Feb 20 2024

NETMANAGEIT

Intelligence Report

Earth Preta Campaign Uses DOPLUGS to Target Asia

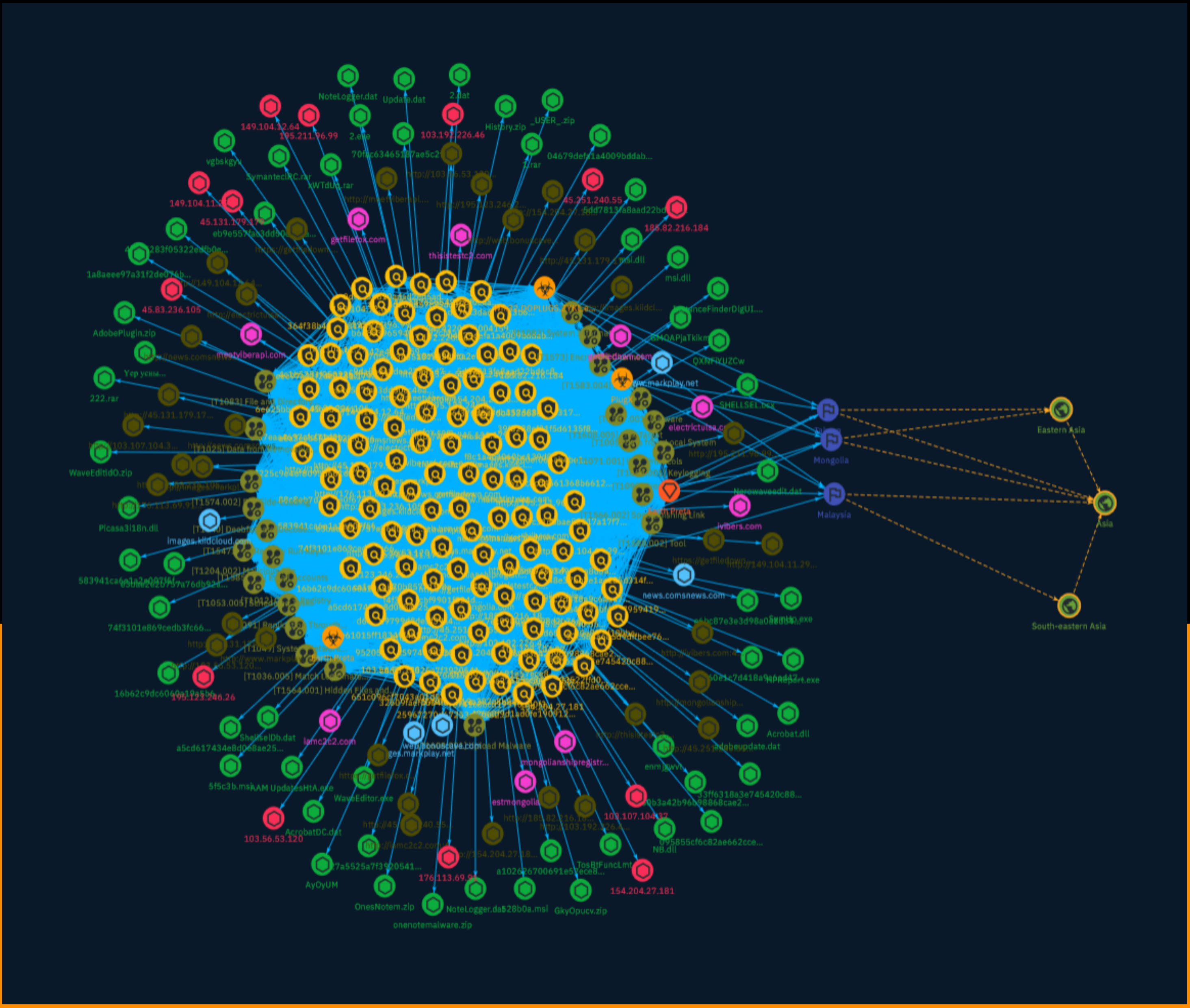

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor group called Earth Preta has been running a campaign targeting Asia using a malware called DOPLUGS to infect victims via phishing emails. DOPLUGS serves as a downloader to retrieve a more advanced PlugX malware strain. The campaign has focused on government entities in Taiwan, Vietnam, Malaysia, and other Asian countries. DOPLUGS has constantly evolved since 2022, integrating features like the KillSomeOne USB worm module.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name

www.markplay.net

Pattern Type

stix

Pattern

[hostname:value = 'www.markplay.net']

Name

web.bonuscave.com

Pattern Type

stix

Pattern

[hostname:value = 'web.bonuscave.com']

Name

images.markplay.net

Pattern Type

stix

Pattern

[hostname:value = 'images.markplay.net']

Name

news.comsnews.com

Pattern Type

stix

Pattern

[hostname:value = 'news.comsnews.com']

Name

images.kiidcloud.com

Pattern Type

stix

Pattern

[hostname:value = 'images.kiidcloud.com']

Name

thisistestc2.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '20 minutes ago', 'timestamp': 1708424164, 'iso': '2024-02-20T05:16:04-05:00'} - **IPQS: Domain:** thisistestc2.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'thisistestc2.com']

Name

mongolianshipregistrar.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Shopping - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686725693, 'iso': '2023-06-14T02:54:53-04:00'} - **IPQS: Domain:** mongolianshipregistrar.com - **IPQS: IP Address:** 172.67.188.118

Pattern Type

stix

Pattern

[domain-name:value = 'mongolianshipregistrar.com']

Name

meetviberapi.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1693987784, 'iso': '2023-09-06T04:09:44-04:00'} - **IPQS: Domain:** meetviberapi.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'meetviberapi.com']

Name

ivibers.com

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'ivibers.com']

Name

iamc2c2.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '20 minutes ago', 'timestamp': 1708424159, 'iso': '2024-02-20T05:15:59-05:00'} - **IPQS: Domain:** iamc2c2.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'iamc2c2.com']

Name

getfilefox.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1694053204, 'iso': '2023-09-06T22:20:04-04:00'} - **IPQS: Domain:** getfilefox.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'getfilefox.com']

Name

estmongolia.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686725692, 'iso': '2023-06-14T02:54:52-04:00'} - **IPQS: Domain:** estmongolia.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'estmongolia.com']

Name

getfiledown.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1691393939, 'iso': '2023-08-07T03:38:59-04:00'} - **IPQS: Domain:** getfiledown.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'getfiledown.com']

Name

electrictulsa.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 years ago', 'timestamp': 1660062671, 'iso': '2022-08-09T12:31:11-04:00'} - **IPQS: Domain:** electrictulsa.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'electrictulsa.com']

Name

https://getfilefox.com/enmjgwvt

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:**

True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1694053204, 'iso': '2023-09-06T22:20:04-04:00'} - **IPQS: Domain:** getfilefox.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'https://getfilefox.com/enmjgwvt']

Name

https://getfiledown.com/vgbskgyu

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1691393939, 'iso': '2023-08-07T03:38:59-04:00'} - **IPQS: Domain:** getfiledown.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'https://getfiledown.com/vgbskgyu']

Name

https://getfiledown.com/utdkt

Description
- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1691393939, 'iso': '2023-08-07T03:38:59-04:00'} - **IPQS: Domain:** getfiledown.com - **IPQS: IP Address:** N/A
Pattern Type
stix
Pattern
[url:value = 'https://getfiledown.com/utdkt']
Name
http://www.markplay.net:8080
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1684207667, 'iso': '2023-05-15T23:27:47-04:00'} - **IPQS: Domain:** markplay.net - **IPQS: IP Address:** 140.82.57.219
Pattern Type
stix
Pattern
[url:value = 'http://www.markplay.net:8080']

Name

http://web.bonuscave.com:8080

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 years ago', 'timestamp': 1639841756, 'iso': '2021-12-18T10:35:56-05:00'} - **IPQS: Domain:** web.bonuscave.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://web.bonuscave.com:8080']

Name

http://thisistestc2.com:443

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '19 minutes ago', 'timestamp': 1708424164, 'iso': '2024-02-20T05:16:04-05:00'} - **IPQS: Domain:** thisistestc2.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://thisistestc2.com:443']

Name

http://news.comsnews.com:5938

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Personal Websites and Blogs - **Domain Age:** {'human': '1 year ago', 'timestamp': 1664961581, 'iso': '2022-10-05T05:19:41-04:00'} - **IPQS: Domain:** news.comsnews.com - **IPQS: IP Address:** 107.161.23.204

Pattern Type

stix

Pattern

[url:value = 'http://news.comsnews.com:5938']

Name

http://mongolianshipregistrar.com:443

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Shopping - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686725693, 'iso': '2023-06-14T02:54:53-04:00'} - **IPQS: Domain:** mongolianshipregistrar.com - **IPQS: IP Address:** 104.21.8.133

Pattern Type

stix

Pattern

[url:value = 'http://mongolianshipregistrar.com:443']

Name

http://news.comsnews.com:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Personal Websites and Blogs - **Domain Age:** {'human': '1 year ago', 'timestamp': 1664961581, 'iso': '2022-10-05T05:19:41-04:00'} - **IPQS: Domain:** news.comsnews.com - **IPQS: IP Address:** 45.128.135.122

Pattern Type

stix

Pattern

[url:value = 'http://news.comsnews.com:443']

Name

http://meetviberapi.com:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1693987784, 'iso': '2023-09-06T04:09:44-04:00'} - **IPQS: Domain:** meetviberapi.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://meetviberapi.com:443']

Name

http://ivibers.com:443

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://ivibers.com:443']

Name

http://images.markplay.net:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9 months ago', 'timestamp': 1684207667, 'iso': '2023-05-15T23:27:47-04:00'} - **IPQS: Domain:** images.markplay.net - **IPQS: IP Address:** 140.82.57.219

Pattern Type

stix

Pattern

[url:value = 'http://images.markplay.net:443']

Name

http://images.kiidcloud.com:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1662914041, 'iso': '2022-09-11T12:34:01-04:00'} - **IPQS: Domain:** images.kiidcloud.com - **IPQS: IP Address:** 185.195.236.16

Pattern Type

stix

Pattern

[url:value = 'http://images.kiidcloud.com:443']

Name

http://iamc2c2.com:443

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '19 minutes ago', 'timestamp': 1708424159, 'iso': '2024-02-20T05:15:59-05:00'} - **IPQS: Domain:** iamc2c2.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://iamc2c2.com:443']

Name

http://electrictulsa.com:443

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 years ago', 'timestamp': 1660062671, 'iso': '2022-08-09T12:31:11-04:00'} - **IPQS: Domain:** electrictulsa.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://electrictulsa.com:443']

Name

http://45.251.240.55:8080

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.251.240.55 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://45.251.240.55:8080']

Name

http://45.83.236.105:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.83.236.105 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://45.83.236.105:443']

Name

http://45.131.179.179:5938

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.131.179.179 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://45.131.179.179:5938']

Name

http://45.251.240.55:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/

A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.251.240.55 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://45.251.240.55:443']

Name

http://45.131.179.179:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.131.179.179 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://45.131.179.179:443']

Name

http://195.211.96.99:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 195.211.96.99 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://195.211.96.99:443']

Name

http://45.131.179.179:22

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 45.131.179.179 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://45.131.179.179:22']

Name

http://195.123.246.26:22

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 195.123.246.26 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://195.123.246.26:22']

Name

http://185.82.216.184:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 185.82.216.184 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://185.82.216.184:443']

Name

http://176.113.69.91:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 176.113.69.91 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://176.113.69.91:443']

Name

http://154.204.27.181:80

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 154.204.27.181 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://154.204.27.181:80']

Name

http://154.204.27.181:110

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 154.204.27.181 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://154.204.27.181:110']

Name

http://149.104.12.64:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/

A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 149.104.12.64 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://149.104.12.64:443']

Name

http://149.104.11.29:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 149.104.11.29 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://149.104.11.29:443']

Name

http://103.56.53.120:8080

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.56.53.120 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.56.53.120:8080']

Name

http://103.56.53.120:80

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[url:value = 'http://103.56.53.120:80']

Name

http://103.192.226.46:443

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.192.226.46 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.192.226.46:443']

Name

45.83.236.105

Description

CC=US ASN=AS6134 XNNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.83.236.105']

Name

f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5']

Name

f4f36c78cbf9901f224de427f42b390c83190c7c1cc4bce8b66f596e62df02d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'f4f36c78cbf9901f224de427f42b390c83190c7c1cc4bce8b66f596e62df02d0']

Name

eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13']

Name

e6bc87e3e3d98a0a8db4fcd7cd5a9b89d4a7b125de450dfb8f387d2a9e09face

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e6bc87e3e3d98a0a8db4fcd7cd5a9b89d4a7b125de450dfb8f387d2a9e09face']

Name

e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280']

Name

dca39474220575004159ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'dca39474220575004159ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c']

Name

d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'd64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4']

Name

d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc']

Name

cd60e1c7d418a9c6ad4705d315f8ace2cdc3fd0528e71064dd80bbbd51bc2b76

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cd60e1c7d418a9c6ad4705d315f8ace2cdc3fd0528e71064dd80bbbd51bc2b76']

Name

ca1ada6770b85771f98e5c02310449ab73231034cfa78b8861850368208c7698

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ca1ada6770b85771f98e5c02310449ab73231034cfa78b8861850368208c7698']

Name

c9da5b0a8dee27fbf5d7bbb4c9b9b38d8c0c547479d315efd62599a3c5d9cb13

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9da5b0a8dee27fbf5d7bbb4c9b9b38d8c0c547479d315efd62599a3c5d9cb13']

Name

c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1']

Name

http://103.107.104.37:443

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.107.104.37 - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://103.107.104.37:443']

Name

b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb']

Name

c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692']

Name

b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177']

Name

abd6521990e88bd18bbcba063744efe0ccac23063bb340720cc3f610d9b1c770

Description

Other:Malware-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'abd6521990e88bd18bbcba063744efe0ccac23063bb340720cc3f610d9b1c770']

Name

a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f']

Name

a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916']

Name

a102626700691e57ece83a4ce24d995e57449508238eb5688954b78448be9172

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a102626700691e57ece83a4ce24d995e57449508238eb5688954b78448be9172']

Name

a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129']

Name

9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58']

Name

95205b92d597489b33854e70d86f16d46201803a1a9cb5379c0d6b7c0784dbc7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'95205b92d597489b33854e70d86f16d46201803a1a9cb5379c0d6b7c0784dbc7']

Name

8e4a4d202d57c79dc0f40ae032f9d7b0ea7ce5024128a2aa227decc228e16113

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e4a4d202d57c79dc0f40ae032f9d7b0ea7ce5024128a2aa227decc228e16113']

Name

8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be']

Name

88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b']

Name

908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8']

Name

7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b']

Name

45.131.179.179

Description

CC=US ASN=AS6134 XNNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.131.179.179']

Name

77a49637bf4047959419c41867437957619d03059b5d3f8d9af26e6ae2347db6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77a49637bf4047959419c41867437957619d03059b5d3f8d9af26e6ae2347db6']

Name

74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1']

Name

70fac63465187ae5c2f057efc291bc34987dff46bec565a7e8f07f9899527224

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'70fac63465187ae5c2f057efc291bc34987dff46bec565a7e8f07f9899527224']

Name

71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787']

Name

6e625bbcecc45b6b556141eef37ffd31aa4861ce4debca6500be72364172ffc7

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'6e625bbcecc45b6b556141eef37ffd31aa4861ce4debca6500be72364172ffc7']

Name

67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6']

Name

651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859']

Name

195.211.96.99

Description

CC=US ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.211.96.99']

Name
60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797']
Name
583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83']
Name
5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914']

Name

5700535f19a382c8b84db6bff3a077e15269df0ec10ea6257e2fa203720356b4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5700535f19a382c8b84db6bff3a077e15269df0ec10ea6257e2fa203720356b4']

Name

4c1b5283f05322edfb0ef8b9d5cf75b62b558fcaefed921f1143765a3bd6248e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c1b5283f05322edfb0ef8b9d5cf75b62b558fcaefed921f1143765a3bd6248e']

Name

48e37bb7e1ac185d314f262894014e1337a3c14455cd987dd83ac220bae87b3a

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'48e37bb7e1ac185d314f262894014e1337a3c14455cd987dd83ac220bae87b3a']

Name

471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132']

Name

42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5']
Name
42663f9d1ad0fe190912800b92c64d38b6f74fac23281b87180a4fef5bc2efd6
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '42663f9d1ad0fe190912800b92c64d38b6f74fac23281b87180a4fef5bc2efd6']
Name
3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' =
'3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b']

Name

39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a']

Name

32609faef0b04f0c37c4cf081c147872a45c59d7c4fbca35deb40d144b0226ad

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'32609faef0b04f0c37c4cf081c147872a45c59d7c4fbca35deb40d144b0226ad']

Name

364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321']

Name

33ff6318a3e745420c884f35709f2799f2fe461a6a5bb5b1e3166b9ab2ff142f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '33ff6318a3e745420c884f35709f2799f2fe461a6a5bb5b1e3166b9ab2ff142f']

Name

195.123.246.26

Description

CC=CZ ASN=AS204957 Green Floid LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.123.246.26']

Name

26b1d37ea3da6a6213b65b000dbb39575d858fa274aea895cc3bf62e706fce5d

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '26b1d37ea3da6a6213b65b000dbb39575d858fa274aea895cc3bf62e706fce5d']

Name

25967270d67253c72532a7e0416eb27ff249bc17dc1d7cded0148f8f4b932789

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '25967270d67253c72532a7e0416eb27ff249bc17dc1d7cded0148f8f4b932789']

Name

1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c']

Name

13c31dbbae53517a17f7e6c99031480babe2bd8a07151dbb7f344ab620f3ac11

Description

SUSP_XORed_Mozilla

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '13c31dbbae53517a17f7e6c99031480babe2bd8a07151dbb7f344ab620f3ac11']

Name

16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe']

Name

0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4']

Name

095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1']

Name

17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82']

Name

04679defa1a4009bddab2a5d81be747b51a7f0f7aa5e7ebb937b40379a6a4690

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '04679defa1a4009bddab2a5d81be747b51a7f0f7aa5e7ebb937b40379a6a4690']

Name

176.113.69.91

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[ipv4-addr:value = '176.113.69.91']

Name

149.104.11.29

Description

CC=HK ASN=AS6134 XNNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.104.11.29']

Name

12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd']

Name

103.56.53.120

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.56.53.120']

Name

103.192.226.46

Description

CC=HK ASN=AS6134 XNNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.192.226.46']

Name

103.107.104.37

Description

CC=HK ASN=AS135330 ADCDATA.COM

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.107.104.37']

Name

149.104.12.64

Description

CC=HK ASN=AS6134 XNNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.104.12.64']

Name

154.204.27.181

Description

CC=HK ASN=AS131685 Sun Network Hong Kong Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.204.27.181']

Name

185.82.216.184

Description

CC=BG ASN=AS59729 ITL LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.82.216.184']

Name

45.251.240.55

Description

PlugX botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.251.240.55']

Malware

Name
Earth Preta
Name
Win32.DOPLUGS.ZYKL.enc
Name
PlugX
Description
[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

Intrusion-Set

Name
Earth Preta

Attack-Pattern

Name

Hidden Files and Directories

ID

T1564.001

Description

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files either via a series of Graphical User Interface (GUI) prompts or with command line switches (`dir /a` for Windows and `ls –a` for Linux and macOS). On Linux and Mac, users can mark specific files as hidden simply by putting a “.” as the first character in the file or folder name (Citation: Sofacy Komplex Trojan) (Citation: Antiquated Mac Malware). Files and folders that start with a period, ‘.’, are by default hidden from being viewed in the Finder application and standard command-line utilities like “ls”. Users must specifically change settings to have these files viewable. Files on macOS can also be marked with the UF_HIDDEN flag which prevents them from being seen in Finder.app, but still allows them to be seen in Terminal.app (Citation: WireLurker). On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace. For example, SSH utilities create a .ssh folder that’s hidden and contains the user’s known hosts and keys. Adversaries can use this to their advantage to hide files and folders anywhere on the system and evading a typical user or system analysis that does not incorporate investigation of hidden files.

Name
DLL Side-Loading
ID
T1574.002
Description
Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s). Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)
Name
Web Protocols
ID
T1071.001
Description
Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as HTTP/S(Citation:

CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

Name

Query Registry

ID

T1012

Description

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. The Registry contains a significant amount of information about the operating system, configuration, software, and security.(Citation: Wikipedia Windows Registry) Information can easily be queried using the [Reg](https://attack.mitre.org/software/S0075) utility, though other means to access the Registry exist. Some of the information may help adversaries to further their operation within a network. Adversaries may use the information from [Query Registry](https://attack.mitre.org/techniques/T1012) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

Name

Tool

ID

T1588.002

Description

Adversaries may buy, steal, or download software tools that can be used during targeting. Tools can be open or closed source, free or commercial. A tool can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Tool acquisition can involve the procurement of commercial software licenses, including for red teaming tools such as [Cobalt Strike](https://attack.mitre.org/software/S0154). Commercial software may be obtained through purchase, stealing licenses (or licensed copies of the software), or cracking trial versions.(Citation: Recorded Future Beacon 2019) Adversaries may obtain tools to support their operations, including to support execution of post-compromise behaviors. In addition to freely downloading or purchasing software, adversaries may steal software and/or software licenses from third-party entities (including other adversaries).

Name

Registry Run Keys / Startup Folder

ID

T1547.001

Description

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. (Citation: Microsoft Run Key) These programs will be executed under the context of the user and will have the account's associated permissions level. The following run keys are created by default on Windows systems: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce` Run keys may exist under multiple hives.(Citation: Microsoft Wow6432Node 2018)(Citation: Malwarebytes Wow6432Node 2016) The `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx` is also available but is not created by default on Windows Vista and newer. Registry run key entries can reference programs directly or list them as a dependency.(Citation: Microsoft Run Key) For example, it is possible to load a DLL at logon using a "Depend" key with RunOnceEx: `reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"` (Citation: Oddvar Moe RunOnceEx Mar 2018) Placing a program within a startup folder will also cause that program to execute when a user logs in. There is a startup folder location for individual user accounts as well as a system-wide startup folder that will be checked regardless of which user account logs in. The startup folder path for the current user is `C:\Users\\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`. The startup folder path for all users is `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp`. The following Registry keys can be used to set startup folder items for persistence: * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders` * `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` The following Registry keys can control automatic startup of services during boot: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce` * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices` Using policy settings to specify startup programs creates corresponding values in either of two Registry keys: * `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` * `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` Programs listed in the load value of the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows` run automatically for the currently logged-on user. By default, the multistring `BootExecute` value of the registry key `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` is set to `autocheck autochk *`. This value causes Windows, at startup, to check the file-system integrity of the hard disks if the system has been shut down abnormally. Adversaries can add other programs or processes to this registry value which will automatically launch at boot. Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots. Adversaries may also use [Masquerading](https://attack.mitre.org/techniques/T1036) to make the Registry entries look as if they are associated with legitimate programs.

Name

Link Target

ID

T1608.005

Description

Adversaries may put in place resources that are referenced by a link that can be used during targeting. An adversary may rely upon a user clicking a malicious link in order to divulge information (including credentials) or to gain execution, as in [Malicious Link](https://attack.mitre.org/techniques/T1204/001). Links can be used for spearphishing, such as sending an email accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser. Prior to a phish for information (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003)) or a phish to gain initial access to a system (as in [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002)), an adversary must set up the resources for a link target for the spearphishing link. Typically, the resources for a link target will be an HTML page that may include some client-side script such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) to decide what content to serve to the user. Adversaries may clone legitimate sites to serve as the link target, this can include cloning of login pages of legitimate web services or organization login pages in an effort to harvest credentials during [Spearphishing Link](https://attack.mitre.org/techniques/T1598/003).(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) Adversaries may also [Upload Malware](https://attack.mitre.org/techniques/T1608/001) and have the link target point to malware for download/execution by the user. Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure ([Domains](https://attack.mitre.org/techniques/

T1583/001)) to help facilitate [Malicious Link](https://attack.mitre.org/techniques/T1204/001). Link shortening services can also be employed. Adversaries may also use free or paid accounts on Platform-as-a-Service providers to host link targets while taking advantage of the widely trusted domains of those providers to avoid being blocked. (Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing)(Citation: Intezer App Service Phishing) Finally, adversaries may take advantage of the decentralized nature of the InterPlanetary File System (IPFS) to host link targets that are difficult to remove. (Citation: Talos IPFS 2022)

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Email Accounts

ID

T1585.002

Description

Adversaries may create email accounts that can be used during targeting. Adversaries can use accounts created with email providers to further their operations, such as leveraging them to conduct [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) Adversaries may also take steps to cultivate a persona around the email account, such as through use of [Social Media Accounts](https://attack.mitre.org/techniques/T1585/001), to increase the chance of success of follow-on behaviors. Created email accounts can also be used in the acquisition of infrastructure (ex: [Domains](https://attack.mitre.org/techniques/T1583/001)).(Citation: Mandiant APT1) To decrease the chance of physically tying back operations to themselves, adversaries may make use of disposable email services.(Citation: Trend Micro R980 2016)

Name

Server

ID

T1583.004

Description

Adversaries may buy, lease, or rent physical servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Adversaries may use web servers to support support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations. Instead of compromising a third-party [Server](https://attack.mitre.org/techniques/T1584/004) or renting a [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may opt to configure and run their own servers in support of operations. Adversaries may only need a lightweight setup if most of their activities will take place using online infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems.(Citation: NYTStuxnet)

Name

Upload Malware

ID

T1608.001

Description

Adversaries may upload malware to third-party or adversary controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content. Adversaries may upload malware to support their operations, such as making a payload available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server. Malware may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Malware can also be staged on web services, such as GitHub or Pastebin, or hosted on the InterPlanetary File System (IPFS), where decentralized content storage makes the removal of malicious files difficult.(Citation: Volexity Ocean Lotus November 2020)(Citation: Talos IPFS 2022) Adversaries may upload backdoored files, such as application binaries, virtual machine images, or container images, to third-party software stores or repositories (ex: GitHub, CNET, AWS Community AMIs, Docker Hub). By chance encounter, victims may directly download/install these backdoored files via [User Execution](https://attack.mitre.org/techniques/T1204). [Masquerading](https://attack.mitre.org/techniques/T1036) may increase the chance of users mistakenly executing these files.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Data from Local System

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://

attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

Replication Through Removable Media

ID

T1091

Description

Adversaries may move onto systems, possibly those on disconnected or air-gapped networks, by copying malware to removable media and taking advantage of Autorun features when the media is inserted into a system and executes. In the case of Lateral Movement, this may occur through modification of executable files stored on removable media or by copying malware and renaming it to look like a legitimate file to trick users into executing it on a separate system. In the case of Initial Access, this may occur through manual manipulation of the media, modification of systems used to initially format the media, or modification to the media's firmware itself. Mobile devices may also be used to infect PCs with malware if connected via USB.(Citation: Exploiting Smartphone USB) This infection may be achieved using devices (Android, iOS, etc.) and, in some instances, USB charging cables.(Citation: Windows Malware Infecting Android)(Citation: iPhone Charging Cable Hack) For example, when a smartphone is connected to a system, it may appear to be mounted similar to a USB-connected disk drive. If malware that is compatible with the connected system is on the mobile device, the malware could infect the machine (especially if Autorun features are enabled).

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

Spearphishing Link

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Name

Malicious File

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or

Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Name

Malware

ID

T1587.001

Description

Adversaries may develop malware and malware components that can be used during targeting. Building malicious software can include the development of payloads, droppers, post-compromise tools, backdoors (including backdoored images), packers, C2 protocols, and the creation of infected removable media. Adversaries may develop malware to support their operations, creating a means for maintaining control of remote machines, evading defenses, and executing post-compromise behaviors.(Citation: Mandiant APT1)(Citation: Kaspersky Sofacy)(Citation: ActiveMalwareEnergy)(Citation: FBI Flash FIN7 USB) As with legitimate development efforts, different skill sets may be required for developing malware. The skills needed may be located in-house, or may need to be contracted out. Use of a contractor may be considered an extension of that adversary's malware development capabilities, provided the adversary plays a role in shaping requirements and maintains a degree of exclusivity to the malware. Some aspects of malware development, such as C2 protocol development, may require adversaries to obtain additional infrastructure. For example, malware developed that will communicate with Twitter for C2, may require use of [Web Services](https://attack.mitre.org/techniques/T1583/006).(Citation: FireEye APT29)

Name

Match Legitimate Name or Location

ID

T1036.005

Description

Adversaries may match or approximate the name or location of legitimate files or resources when naming/placing them. This is done for the sake of evading defenses and observation. This may be done by placing an executable in a commonly trusted directory (ex: under System32) or giving it the name of a legitimate, trusted program (ex: svchost.exe). In containerized environments, this may also be done by creating a resource in a namespace that matches the naming convention of a container pod or cluster. Alternatively, a file or container image name given may be a close approximation to legitimate programs/images or something innocuous. Adversaries may also use the same icon of the file they are trying to mimic.

Name

Data from Removable Media

ID

T1025

Description

Adversaries may search connected removable media on computers they have compromised to find files of interest. Sensitive data can be collected from any removable media (optical disk drive, USB memory, etc.) connected to the compromised system prior to Exfiltration. Interactive command shells may be in use, and common functionality within [cmd](https://attack.mitre.org/software/S0106) may be used to gather information. Some adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on removable media.

Name

Keylogging

ID

T1056.001

Description

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of capturing credentials quickly, an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems. (Citation: Talos Kimsuky Nov 2021) Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include: * Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data. * Reading raw keystroke data from the hardware buffer. * Windows Registry modifications. * Custom drivers. * [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

Name

Scheduled Task

ID

T1053.005

Description

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task. The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though `at.exe` can not access tasks created with `schtasks` or the Control Panel. An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent) Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

Country

Name
Malaysia

Name
Taiwan

Name
Mongolia

Region

Name
South-eastern Asia

Name
Eastern Asia

Name
Asia

Hostname

Value
www.markplay.net
web.bonuscave.com
images.kiidcloud.com
news.comsnews.com
images.markplay.net

Domain-Name

Value
thisistestc2.com
mongolianshipregistrar.com
meetviberapi.com
ivibers.com
iamc2c2.com
getfilefox.com
getfiledown.com
estmongolia.com
electrictulsa.com

Url

Value
https://getfilefox.com/enmjgwvt
https://getfiledown.com/vgbskgyu
https://getfiledown.com/utdkt
http://www.markplay.net:8080
http://web.bonuscave.com:8080
http://thisistestc2.com:443
http://news.comsnews.com:5938
http://news.comsnews.com:443
http://mongolianshipregistrar.com:443
http://meetviberapi.com:443
http://ivibers.com:443
http://images.markplay.net:443
http://images.kiidcloud.com:443

http://iamc2c2.com:443

http://electrictulsa.com:443

http://45.83.236.105:443

http://45.251.240.55:8080

http://45.251.240.55:443

http://45.131.179.179:5938

http://45.131.179.179:443

http://45.131.179.179:22

http://195.123.246.26:22

http://185.82.216.184:443

http://195.211.96.99:443

http://176.113.69.91:443

http://154.204.27.181:80

http://154.204.27.181:110

http://149.104.12.64:443

http://149.104.11.29:443

http://103.56.53.120:8080

http://103.56.53.120:80

http://103.192.226.46:443

http://103.107.104.37:443

IPv4-Addr

Value
45.83.236.105
45.131.179.179
195.211.96.99
176.113.69.91
195.123.246.26
149.104.11.29
103.56.53.120
103.192.226.46
103.107.104.37
149.104.12.64
185.82.216.184
154.204.27.181
45.251.240.55

StixFile

Value
f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5
f4f36c78cbf9901f224de427f42b390c83190c7c1cc4bce8b66f596e62df02d0
eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13
e6bc87e3e3d98a0a8db4fcd7cd5a9b89d4a7b125de450dfb8f387d2a9e09face
e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280
dca39474220575004159ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c
d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc
cd60e1c7d418a9c6ad4705d315f8ace2cdc3fd0528e71064dd80bbbd51bc2b76
d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4
ca1ada6770b85771f98e5c02310449ab73231034cfa78b8861850368208c7698
c9da5b0a8dee27fbf5d7bbb4c9b9b38d8c0c547479d315efd62599a3c5d9cb13
c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1
c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692

b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb

b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177

abd6521990e88bd18bbcba063744efe0ccac23063bb340720cc3f610d9b1c770

a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f

a102626700691e57ece83a4ce24d995e57449508238eb5688954b78448be9172

a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916

a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129

9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58

95205b92d597489b33854e70d86f16d46201803a1a9cb5379c0d6b7c0784dbc7

908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8

8e4a4d202d57c79dc0f40ae032f9d7b0ea7ce5024128a2aa227decc228e16113

88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b

8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be

7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b

77a49637bf4047959419c41867437957619d03059b5d3f8d9af26e6ae2347db6

74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1

71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787

70fac63465187ae5c2f057efc291bc34987dff46bec565a7e8f07f9899527224

6e625bbcecc45b6b556141eef37ffd31aa4861ce4debca6500be72364172ffc7
67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6
651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859
60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797
5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914
583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83
5700535f19a382c8b84db6bff3a077e15269df0ec10ea6257e2fa203720356b4
4c1b5283f05322edfb0ef8b9d5cf75b62b558fcaefed921f1143765a3bd6248e
48e37bb7e1ac185d314f262894014e1337a3c14455cd987dd83ac220bae87b3a
471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132
42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5
42663f9d1ad0fe190912800b92c64d38b6f74fac23281b87180a4fef5bc2efd6
3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b
39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a
364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321
33ff6318a3e745420c884f35709f2799f2fe461a6a5bb5b1e3166b9ab2ff142f
32609faef0b04f0c37c4cf081c147872a45c59d7c4fbca35deb40d144b0226ad
26b1d37ea3da6a6213b65b000dbb39575d858fa274aea895cc3bf62e706fce5d

25967270d67253c72532a7e0416eb27ff249bc17dc1d7cded0148f8f4b932789
1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c
16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe
17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82
13c31dbbae53517a17f7e6c99031480babe2bd8a07151dbb7f344ab620f3ac11
12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd
0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4
095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1
04679defa1a4009bddab2a5d81be747b51a7f0f7aa5e7ebb937b40379a6a4690

External References

- https://www.trendmicro.com/en_us/research/24/b/earth-preta-campaign-targets-asia-doplugs.html
- https://otx.alienvault.com/pulse/65d47ad5998f71d01b635048