Feb 01 2024

NETMANAGEIT

Intelligence Report

Evolution of UNC4990: Uncovering USB Malware's Hidden Depths

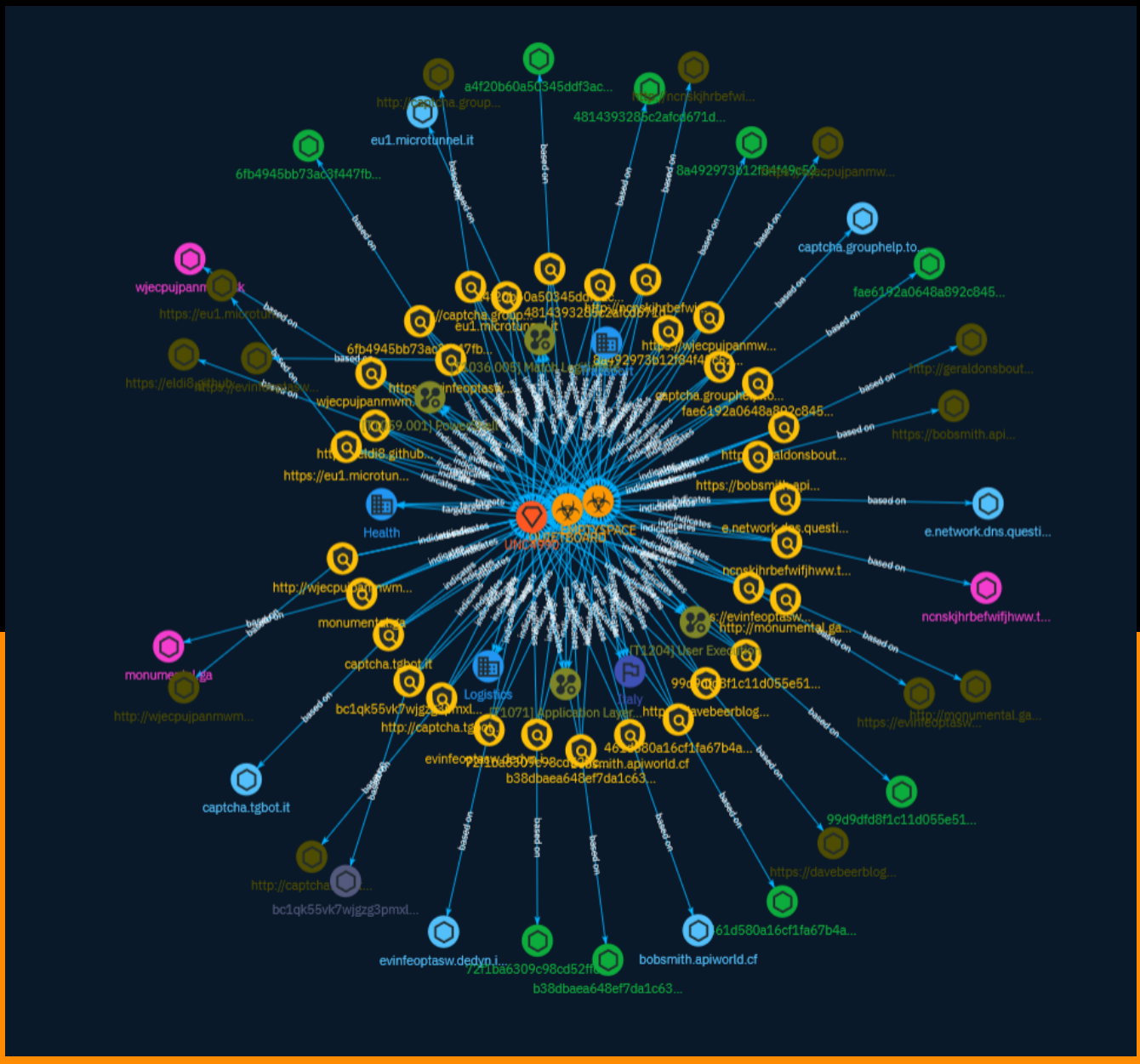

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 35
- Intrusion-Set 36
- Attack-Pattern 37
- Country 43
- Sector 44

Observables

- Url 46

- Hostname 48
- Domain-Name 49
- StixFile 50
- Cryptocurrency-Wallet 52

External References

- External References 53

Overview

Description

This report provides an analysis of the threat actor group UNC4990, which has been conducting campaigns since at least 2020 primarily targeting organizations in Italy across industries like health, transportation, and logistics. The group relies heavily on USB-based malware for initial infection, using malicious shortcut files that execute PowerShell scripts to download additional payloads. The report tracks the evolution of the group's tactics, techniques, and procedures over time, including their shift from using text files to abusing legitimate services like GitHub and Vimeo to host encoded payloads. Their toolset includes the EMPTYSPACE downloader and the QUIETBOARD backdoor, which have modular components to expand functionality. The report provides technical details on the capabilities of these tools as well as opportunities for detection based on forensic artifacts.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

https://davebeerblog.eu.org/wp-admin.php

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': '1 day ago', 'timestamp': 1706693932, 'iso': '2024-01-31T04:38:52-05:00'} - **IPQS: Domain:** davebeerblog.eu.org

Pattern Type

stix

Pattern

[url:value = 'https://davebeerblog.eu.org/wp-admin.php']

Name

https://eldi8.github.io/src.txt

Description

- **Unsafe:** False - **Server:** GitHub.com - **Domain Rank:** 133 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & Internet - **Domain

Age:** {'human': '11 years ago', 'timestamp': 1362769968, 'iso': '2013-03-08T14:12:48-05:00'} - **IPQS: Domain:** eldi8.github.io - **IPQS: IP Address:** 185.199.110.153

Pattern Type

stix

Pattern

[url:value = 'https://eldi8.github.io/src.txt']

Name

http://geraldonsboutique.altervista.org/updater.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1518 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** ISP - **Domain Age:** {'human': '23 years ago', 'timestamp': 977508339, 'iso': '2000-12-22T13:05:39-05:00'} - **IPQS: Domain:** geraldonsboutique.altervista.org - **IPQS: IP Address:** 52.49.51.252

Pattern Type

stix

Pattern

[url:value = 'http://geraldonsboutique.altervista.org/updater.php']

Name

evinfeoptasw.dedyn.io

Pattern Type

stix

Pattern

[hostname:value = 'evinfeoptasw.dedyn.io']

Name

eu1.microtunnel.it

Pattern Type

stix

Pattern

[hostname:value = 'eu1.microtunnel.it']

Name

e.network.dns.questions.name

Pattern Type

stix

Pattern

[hostname:value = 'e.network.dns.questions.name']

Name

captcha.tgbot.it

Pattern Type

stix

Pattern

[hostname:value = 'captcha.tgbot.it']

Name

captcha.grouphelp.top

Pattern Type

stix

Pattern

[hostname:value = 'captcha.grouphelp.top']

Name

bobsmith.apiworld.cf

Pattern Type

stix

Pattern

[hostname:value = 'bobsmith.apiworld.cf']

Name

wjecpujpanmwm.tk

Description

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

Pattern Type

stix

Pattern

[domain-name:value = 'wjecpujpanmwm.tk']

Name

https://wjecpujpanmwm.tk/updater.php?from=USB1

Description

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

Pattern Type

stix

Pattern

[url:value = 'https://wjecpujpanmwm.tk/updater.php?from=USB1']

Name

ncnskjhrbefwifjhww.tk

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:** ncnskjhrbefwifjhww.tk - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'ncnskjhrbefwifjhww.tk']

Name

monumental.ga

Pattern Type

stix

Pattern

[domain-name:value = 'monumental.ga']

Name

https://evinfeoptasw.dedyn.io/updater.php?from=USB1

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 84783 - **DNS Valid:** True - **Parking:** False - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9

years ago', 'timestamp': 1433494554, 'iso': '2015-06-05T04:55:54-04:00'} - **IPQS: Domain:** evinfeoptasw.dedyn.io - **IPQS: IP Address:** 188.114.97.14

Pattern Type

stix

Pattern

[url:value = 'https://evinfeoptasw.dedyn.io/updater.php?from=USB1']

Name

https://bobsmith.apiworld.cf/license.php

Description

- **Unsafe:** False - **Server:** cloudflare - **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:** bobsmith.apiworld.cf - **IPQS: IP Address:** 172.67.193.47

Pattern Type

stix

Pattern

[url:value = 'https://bobsmith.apiworld.cf/license.php']

Name

https://eu1.microtunnel.it/c0s1ta/index.php

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686003948, 'iso': '2023-06-05T18:25:48-04:00'} - **IPQS: Domain:** eu1.microtunnel.it - **IPQS: IP Address:** 104.21.55.19

Pattern Type

stix

Pattern

[url:value = 'https://eu1.microtunnel.it/c0s1ta/index.php']

Name

http://monumental.ga/wp-admin.php

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': '1 day ago', 'timestamp': 1706693871, 'iso': '2024-01-31T04:37:51-05:00'} - **IPQS: Domain:** monumental.ga - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://monumental.ga/wp-admin.php']

Name

http://wjecpujpanmwm.tk/updater.php

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': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** wjecpujpanmwm.tk

Pattern Type

stix

Pattern

[url:value = 'http://wjecpujpanmwm.tk/updater.php']

Name

http://ncnskjhrbefwifjhww.tk/updater.php

Pattern Type

stix

Pattern

[url:value = 'http://ncnskjhrbefwifjhww.tk/updater.php']

Name

http://captcha.tgbot.it/updater.php

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': '1 day ago', 'timestamp': 1706693863, 'iso': '2024-01-31T04:37:43-05:00'} - **IPQS: Domain:** captcha.tgbot.it

Pattern Type

stix

Pattern

[url:value = 'http://captcha.tgbot.it/updater.php']

Name

http://captcha.grouphelp.top/updater.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 634515 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '7 years ago', 'timestamp': 1478119147, 'iso': '2016-11-02T16:39:07-04:00'} - **IPQS: Domain:** captcha.grouphelp.top - **IPQS: IP Address:** 104.21.10.16

Pattern Type

stix

Pattern

[url:value = 'http://captcha.grouphelp.top/updater.php']

Name

fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4']

Name

b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1']

Name

a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40']

Name

99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6']

Name

72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be']

Name

6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c09008860954361l4a17443

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c0900886095436114a17443']

Name

8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d']

Name

4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8']

Name

461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3']

Name

bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w']

Name

https://evinfeoptasw.dedyn.io/updater.php

Description

zgRAT payload delivery URL (confidence level: 100%)

Pattern Type

stix

Pattern

[url:value = 'https://evinfeoptasw.dedyn.io/updater.php']

Name

https://davebeerblog.eu.org/wp-admin.php

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': '1 day ago', 'timestamp': 1706693932, 'iso': '2024-01-31T04:38:52-05:00'} - **IPQS: Domain:** davebeerblog.eu.org

Pattern Type

stix

Pattern

[url:value = 'https://davebeerblog.eu.org/wp-admin.php']

Name

https://eldi8.github.io/src.txt

Description

- **Unsafe:** False - **Server:** GitHub.com - **Domain Rank:** 133 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '11 years ago', 'timestamp': 1362769968, 'iso': '2013-03-08T14:12:48-05:00'} - **IPQS: Domain:** eldi8.github.io - **IPQS: IP Address:** 185.199.110.153

Pattern Type

stix

Pattern

[url:value = 'https://eldi8.github.io/src.txt']

Name

http://geraldonsboutique.altervista.org/updater.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1518 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** ISP - **Domain Age:** {'human': '23 years ago', 'timestamp': 977508339, 'iso': '2000-12-22T13:05:39-05:00'} - **IPQS: Domain:** geraldonsboutique.altervista.org - **IPQS: IP Address:** 52.49.51.252

Pattern Type

stix

Pattern

[url:value = 'http://geraldonsboutique.altervista.org/updater.php']

Name

evinfeoptasw.dedyn.io

Pattern Type

stix

Pattern

[hostname:value = 'evinfeoptasw.dedyn.io']

Name

eu1.microtunnel.it

Pattern Type

stix

Pattern

[hostname:value = 'eu1.microtunnel.it']

Name

e.network.dns.questions.name

Pattern Type

stix

Pattern

[hostname:value = 'e.network.dns.questions.name']

Name

captcha.tgbot.it

Pattern Type

stix

Pattern

[hostname:value = 'captcha.tgbot.it']

Name

captcha.grouphelp.top

Pattern Type

stix

Pattern

[hostname:value = 'captcha.grouphelp.top']

Name

bobsmith.apiworld.cf

Pattern Type

stix

Pattern

[hostname:value = 'bobsmith.apiworld.cf']

Name

wjecpujpanmwm.tk

Description

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

Pattern Type

stix

Pattern

[domain-name:value = 'wjecpujpanmwm.tk']

Name

https://wjecpujpanmwm.tk/updater.php?from=USB1

Description

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

Pattern Type

stix

Pattern

[url:value = 'https://wjecpujpanmwm.tk/updater.php?from=USB1']

Name

ncnskjhrbefwifjhww.tk

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:** ncnskjhrbefwifjhww.tk - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[domain-name:value = 'ncnskjhrbefwifjhww.tk']

Name

monumental.ga

Pattern Type

stix

Pattern

[domain-name:value = 'monumental.ga']

Name

https://evinfeoptasw.dedyn.io/updater.php?from=USB1

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 84783 - **DNS Valid:** True - **Parking:** False - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '9

years ago', 'timestamp': 1433494554, 'iso': '2015-06-05T04:55:54-04:00'} - **IPQS: Domain:** evinfeoptasw.dedyn.io - **IPQS: IP Address:** 188.114.97.14

Pattern Type

stix

Pattern

[url:value = 'https://evinfeoptasw.dedyn.io/updater.php?from=USB1']

Name

https://bobsmith.apiworld.cf/license.php

Description

- **Unsafe:** False - **Server:** cloudflare - **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:** bobsmith.apiworld.cf - **IPQS: IP Address:** 172.67.193.47

Pattern Type

stix

Pattern

[url:value = 'https://bobsmith.apiworld.cf/license.php']

Name

https://eu1.microtunnel.it/c0s1ta/index.php

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686003948, 'iso': '2023-06-05T18:25:48-04:00'} - **IPQS: Domain:** eu1.microtunnel.it - **IPQS: IP Address:** 104.21.55.19

Pattern Type

stix

Pattern

[url:value = 'https://eu1.microtunnel.it/c0s1ta/index.php']

Name

http://monumental.ga/wp-admin.php

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': '1 day ago', 'timestamp': 1706693871, 'iso': '2024-01-31T04:37:51-05:00'} - **IPQS: Domain:** monumental.ga - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://monumental.ga/wp-admin.php']

Name

http://wjecpujpanmwm.tk/updater.php

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': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** wjecpujpanmwm.tk

Pattern Type

stix

Pattern

[url:value = 'http://wjecpujpanmwm.tk/updater.php']

Name

http://ncnskjhrbefwifjhww.tk/updater.php

Pattern Type

stix

Pattern

[url:value = 'http://ncnskjhrbefwifjhww.tk/updater.php']

Name

http://captcha.tgbot.it/updater.php

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': '1 day ago', 'timestamp': 1706693863, 'iso': '2024-01-31T04:37:43-05:00'} - **IPQS: Domain:** captcha.tgbot.it

Pattern Type

stix

Pattern

[url:value = 'http://captcha.tgbot.it/updater.php']

Name

http://captcha.grouphelp.top/updater.php

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 634515 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '7 years ago', 'timestamp': 1478119147, 'iso': '2016-11-02T16:39:07-04:00'} - **IPQS: Domain:** captcha.grouphelp.top - **IPQS: IP Address:** 104.21.10.16

Pattern Type

stix

Pattern

[url:value = 'http://captcha.grouphelp.top/updater.php']

Name

fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4']

Name

b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1']

Name

a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40']

Name

99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6']

Name

72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be']

Name

6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c09008860954361l4a17443

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c0900886095436114a17443']

Name

8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d']

Name

4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8']

Name

461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3']

Name

bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w

Pattern Type

stix

Pattern

[cryptocurrency-wallet:value = 'bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w']

Name

https://evinfeoptasw.dedyn.io/updater.php

Description

zgRAT payload delivery URL (confidence level: 100%)

Pattern Type

stix

Pattern
[url:value = 'https://evinfeoptasw.dedyn.io/updater.php']

Malware

Name
QUIETBOARD
Name
EMPTYSPACE
Name
QUIETBOARD
Name
EMPTYSPACE

Intrusion-Set

Name
UNC4990

Name
UNC4990

Attack-Pattern

Name

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) 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). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols 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. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) 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). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/

techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols 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. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

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.

Country

Name
Italy

Name
Italy

Sector

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.
Name
Transport
Description
All entities involved in the movement of people or goods from one place to another.
Name
Logistics
Description
Entities managing the flow of goods, equipment, materials, supplies etc.
Name

Health

Description

Public and private entities involved in research, services and manufacturing activities related to public health.

Name

Transport

Description

All entities involved in the movement of people or goods from one place to another.

Name

Logistics

Description

Entities managing the flow of goods, equipment, materials, supplies etc.

Url

Value
https://davebeerblog.eu.org/wp-admin.php
https://eldi8.github.io/src.txt
http://geraldonsboutique.altervista.org/updater.php
https://wjecpujpanmwm.tk/updater.php?from=USB1
https://evinfeoptasw.dedyn.io/updater.php?from=USB1
https://eu1.microtunnel.it/c0s1ta/index.php
https://bobsmith.apiworld.cf/license.php
http://wjecpujpanmwm.tk/updater.php
http://ncnskjhrbefwifjhww.tk/updater.php
http://monumental.ga/wp-admin.php
http://captcha.tgbot.it/updater.php
http://captcha.grouphelp.top/updater.php
https://evinfeoptasw.dedyn.io/updater.php

https://davebeerblog.eu.org/wp-admin.php

https://eldi8.github.io/src.txt

http://geraldonsboutique.altervista.org/updater.php

https://wjecpujpanmwm.tk/updater.php?from=USB1

https://evinfeoptasw.dedyn.io/updater.php?from=USB1

https://eu1.microtunnel.it/c0s1ta/index.php

https://bobsmith.apiworld.cf/license.php

http://wjecpujpanmwm.tk/updater.php

http://ncnskjhrbefwifjhww.tk/updater.php

http://monumental.ga/wp-admin.php

http://captcha.tgbot.it/updater.php

http://captcha.grouphelp.top/updater.php

https://evinfeoptasw.dedyn.io/updater.php

Hostname

Value
evinfeoptasw.dedyn.io
eu1.microtunnel.it
e.network.dns.questions.name
captcha.tgbot.it
captcha.grouphelp.top
bobsmith.apiworld.cf
evinfeoptasw.dedyn.io
eu1.microtunnel.it
e.network.dns.questions.name
captcha.tgbot.it
captcha.grouphelp.top
bobsmith.apiworld.cf

Domain-Name

Value
wjecpujpanmwm.tk
ncnskjhrbefwifjhww.tk
monumental.ga
wjecpujpanmwm.tk
ncnskjhrbefwifjhww.tk
monumental.ga

StixFile

Value
fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4
b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1
a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40
99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6
461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3
8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d
72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be
6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c09008860954361l4a17443
4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8
fae6192a0648a892c845d9498002ca79497ea58e5315d277f65f7b243f7110e4
b38dbaea648ef7da1c639f4fdaac0d88f03306ea42f0edc9af512c613dbdb7e1
a4f20b60a50345ddf3ac71b6e8c5ebcb9d069721b0b0edc822ed2e7569a0bb40
99d9dfd8f1c11d055e515a02c1476bd9036c788493063f08b82bb5f34e19dfd6

461d580a16cf1fa67b4ac751dfe9d36b2de3f13c97670b3b12641f20246ce4b3

8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d

72f1ba6309c98cd52ffc99dd15c45698dfca2d6ce1ef0bf262433b5dfff084be

6fb4945bb73ac3f447fb7af6bd2937395a067a6e0c09008860954361l4a17443

4814393285c2afcd671dbdd53b3b2021963c32a09745f83ed894e5ae4e2764b8

Cryptocurrency-Wallet

Value
bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w
bc1qk55vk7wjgzg3pmxlh59rv5dlgewd9jem5nrt4w

External References

- https://www.mandiant.com/resources/blog/unc4990-evolution-usb-malware
- https://otx.alienvault.com/pulse/65ba0f6134fcdb7372f30148