Feb 05 2024

NETMANAGEIT

Intelligence Report

New Information on Cyberespionage Attacks against Myanmar Military Junta

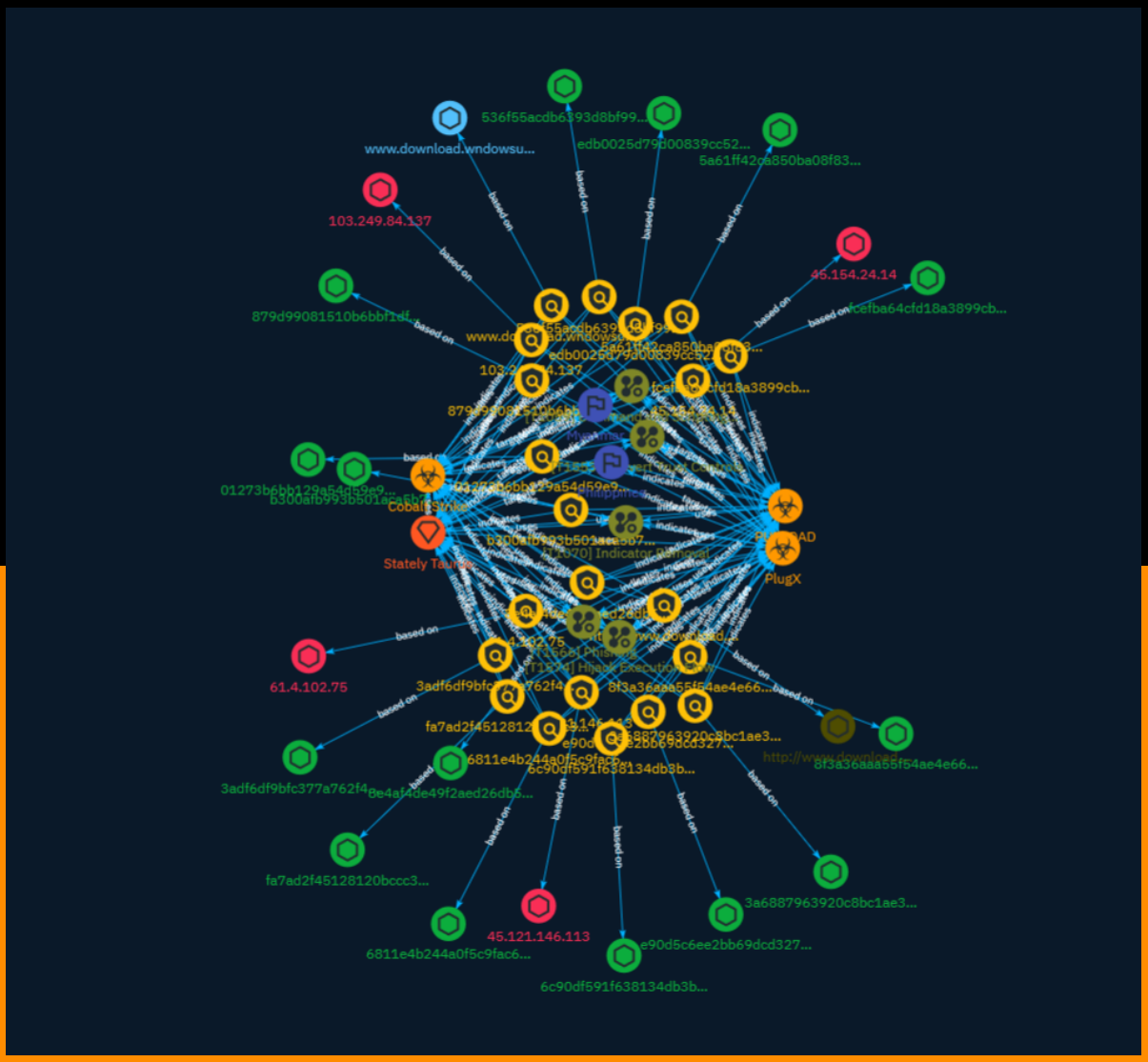

Table of contents

Overview

Entities

Observables

External References

Overview

Description

All newly discovered campaigns have taken place in between the originally discussed campaigns on November 9th, 2023 and January 17th, 2024. Employment of previously seen techniques such as DLL Search Order Hijacking and leveraging publicly documented malware such as PUBLOAD show a consistent intrusion set. However, deviations like the use of Cobalt Strike beacons and infostealers showcase variability in modus operandi.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

www.download.wndowsupdate.com

Pattern Type

stix

Pattern

[hostname:value = 'www.download.wndowsupdate.com']

Name

http://www.download.wndowsupdate.com

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 hours ago', 'timestamp': 1707145699, 'iso': '2024-02-05T10:08:19-05:00'} - **IPQS: Domain:** download.wndowsupdate.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://www.download.wndowsupdate.com']

Name

61.4.102.75

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 61.4.102.75 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Wilayah Persekutuan Kuala Lumpur - **City:** Kuala Lumpur - **Latitude:** 3.14 - **Longitude:** 101.69

Pattern Type

stix

Pattern

[ipv4-addr:value = '61.4.102.75']

Name

45.154.24.14

Description

- **Zip Code:** N/A - **ISP:** Siamdata Communication Co. - **ASN:** 56309 - **Organization:** Siamdata Communication Co. - **Is Crawler:** False - **Timezone:** Asia/Bangkok - **Mobile:** False - **Host:** 45.154.24.14 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:**

Premium required. - **Country Code:** TH - **Region:** Nonthaburi - **City:** Nonthaburi - **Latitude:** 13.62 - **Longitude:** 100.55

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.154.24.14']

Name

45.121.146.113

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 45.121.146.113 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Selangor - **City:** Cyberjaya - **Latitude:** 2.92 - **Longitude:** 101.65

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.121.146.113']

Name

fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64']

Name

fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1']

Name

edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361']

Name

e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641']

Name

b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995']

Name

103.249.84.137

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 103.249.84.137 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Kuala Lumpur - **City:** Kuala Lumpur - **Latitude:** 2.97 - **Longitude:** 101.65

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.249.84.137']

Name

8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6']

Name

879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f']

Name

8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf']

Name

6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02']

Name

5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3']

Name

6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614']

Name

3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1']

Name

536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745']

Name

3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d']

Name

01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935']

Name

www.download.wndowsupdate.com

Pattern Type

stix

Pattern

[hostname:value = 'www.download.wndowsupdate.com']

Name

http://www.download.wndowsupdate.com

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 hours ago', 'timestamp': 1707145699, 'iso': '2024-02-05T10:08:19-05:00'} - **IPQS: Domain:** download.wndowsupdate.com - **IPQS: IP Address:** 127.0.0.1

Pattern Type

stix

Pattern

[url:value = 'http://www.download.wndowsupdate.com']

Name

61.4.102.75

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 61.4.102.75 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Wilayah Persekutuan Kuala Lumpur - **City:** Kuala Lumpur - **Latitude:** 3.14 - **Longitude:** 101.69

Pattern Type

stix

Pattern

[ipv4-addr:value = '61.4.102.75']

Name

45.154.24.14

Description

- **Zip Code:** N/A - **ISP:** Siamdata Communication Co. - **ASN:** 56309 - **Organization:** Siamdata Communication Co. - **Is Crawler:** False - **Timezone:** Asia/Bangkok - **Mobile:** False - **Host:** 45.154.24.14 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** TH - **Region:** Nonthaburi - **City:** Nonthaburi - **Latitude:** 13.62 - **Longitude:** 100.55

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.154.24.14']

Name

45.121.146.113

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 45.121.146.113 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Selangor - **City:** Cyberjaya - **Latitude:** 2.92 - **Longitude:** 101.65

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.121.146.113']

Name

fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64']

Name

fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1']

Name

edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361']

Name

e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641']

Name

b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995']

Name

103.249.84.137

Description

- **Zip Code:** N/A - **ISP:** Gigabit Hosting Sdn Bhd - **ASN:** 55720 - **Organization:** Gigabit Hosting Sdn Bhd - **Is Crawler:** False - **Timezone:** Asia/Kuala_Lumpur - **Mobile:** False - **Host:** 103.249.84.137 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:**

False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** MY - **Region:** Kuala Lumpur - **City:** Kuala Lumpur - **Latitude:** 2.97 - **Longitude:** 101.65

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.249.84.137']

Name

8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6']

Name

879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f']

Name

8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf']

Name

6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02']

Name

5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3']

Name

6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614']

Name

3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1']

Name

536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745']

Name

3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d']

Name

01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935']
```

Malware

Name
PUBLOAD

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

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)

Name
PUBLOAD

Name
Cobalt Strike

Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

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
Stately Taurus

Name
Stately Taurus

Attack-Pattern

Name
Subvert Trust Controls
ID
T1553
Description
Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)
Name
Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may

attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Hijack Execution Flow

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution.

(Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Country

Name
Philippines
Name
Myanmar
Name
Philippines
Name
Myanmar

Hostname

Value
www.download.wndowsupdate.com
www.download.wndowsupdate.com

Url

Value
http://www.download.wndowsupdate.com
http://www.download.wndowsupdate.com

IPv4-Addr

Value
61.4.102.75
45.154.24.14
45.121.146.113
103.249.84.137
61.4.102.75
45.154.24.14
45.121.146.113
103.249.84.137

StixFile

Value
fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64
fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1
edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361
e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641
b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995
8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6
8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf
879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f
6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02
6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614
5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3
3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1
536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745

3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d

01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935

fcefba64cfd18a3899cb5c87328eabad18a0efebfb5d8f8e774c570cad332e64

fa7ad2f45128120bccc33f996f87a81faa2e9c1236666dd69b943a755f332eb1

edb0025d79d00839cc52d6b750d845c37ffd5a882c81e7979e2594a7f6c6d361

e90d5c6ee2bb69dcd327ca344263ce1e033a04c6e054c69c46b01236691b7641

b300afb993b501aca5b727b1c964810345cfa5b032f5774251a2570a3ae16995

8f3a36aaa55f54ae4e665a3c4213dec1f16912bf5ed2f0ff5ff9d08a84a451a6

8e4af4de49f2aed26db54ac90acf72edf5aa83f0aa38d262a95c653106a56acf

879d99081510b6bbf1df105bca85087edadcc3b235fb1e358194892cae2b034f

6c90df591f638134db3b48ff1fd7111c366ec069c69ae28ee60d5cdd36408c02

6811e4b244a0f5c9fac6f8c135fcfff48940e89a33a5b21a552601c2bceb4614

5a61ff42ca850ba08f835e3a960d87450c2d6557f5fa65dd006c00eda1ab45a3

3adf6df9bfc377a762f4cebe9e5b5e7d7a823de03f6bfe8efa8ed5473ce10bc1

536f55acdb6393d8bf9976cc3ba1e64280c8f8c26463a139354e53991dd87745

3a6887963920c8bc1ae35fdca69af2c0865f8b5c6ef90b4db91fa152bc56050d

01273b6bb129a54d59e91c389a71add9892d392ea5f145169ae628ec99eda935

External References

- https://csirt-cti.net/2024/02/01/stately-taurus-continued-new-information-on-cyberespionage-attacks-against-myanmar-military-junta/
- https://otx.alienvault.com/pulse/65c0f530b6c8fe662e3a7326