Oct 10 2023

NETMANAGEIT

Intelligence Report

Grayling: Previously Unseen Threat Actor Targets Multiple Organizations in Taiwan

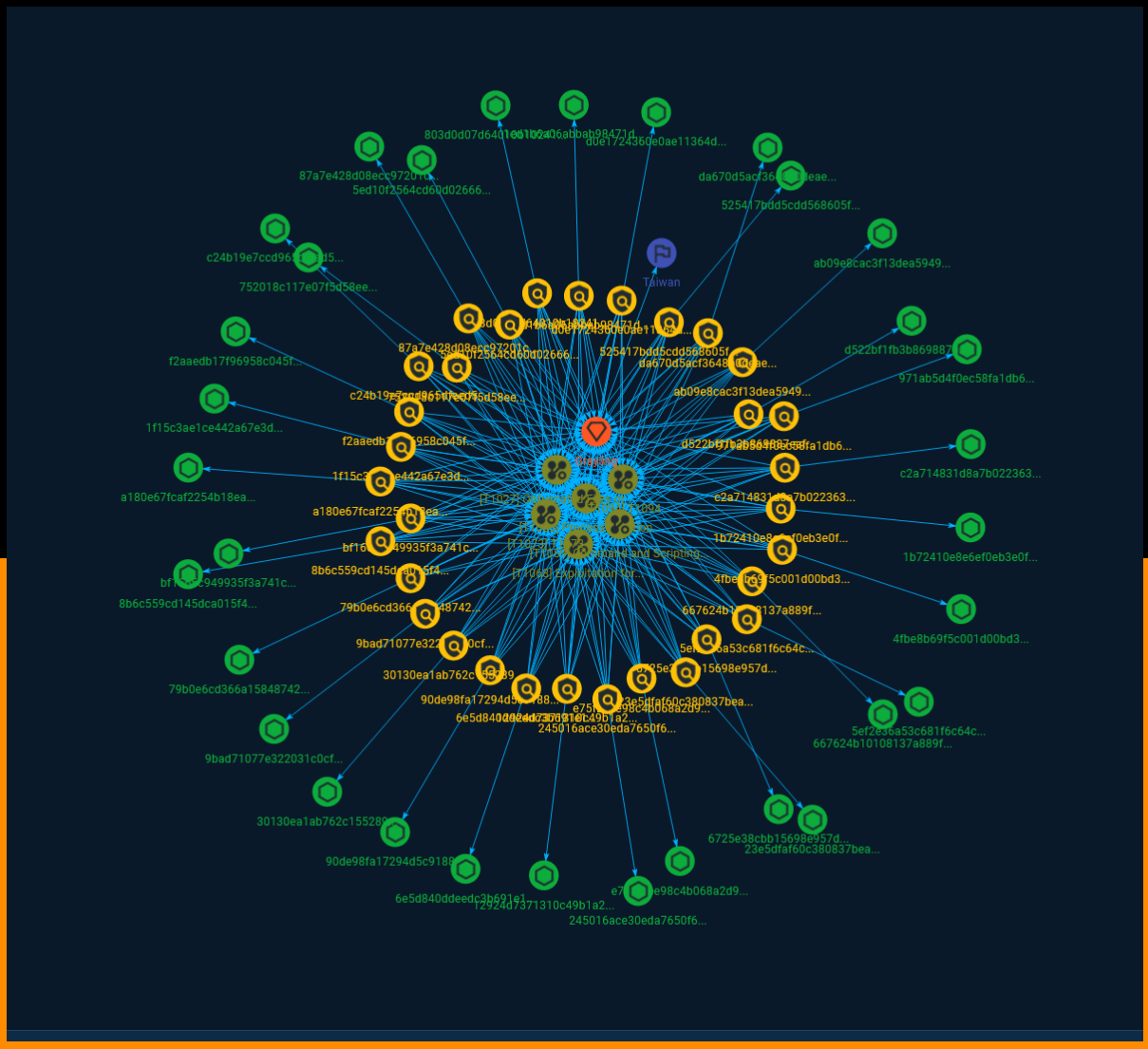

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A previously unknown advanced persistent threat (APT) group used custom malware and multiple publicly available tools to target a number of organizations in the manufacturing, IT, and biomedical sectors in Taiwan.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Process Injection
ID
T1055
Description
Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.
Name
Exploitation for Privilege Escalation
ID
T1068

Description

Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid

detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [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) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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
T1073

ID
T1073

Name
T1094

ID
T1094

Indicator

Name
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b']
Name
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f']
Name

12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746']

Name

752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea']

Name

667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c']

Name

79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17']

Name

525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9']

Name

e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3']

Name

1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce']

Name

d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c']

Name

90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0']

Name

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721']

Name

5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec']

Name

da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9']

Name

245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa']

Name

87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8']

Name

1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9']

Name

9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739']

Name

1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91']

Name

6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50']

Name

a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe']

Name

971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f']

Name

6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068']

Name

5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970']

Name

4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba']

Name

8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2']

Name

d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29']

Name

23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae']

Name

c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5']

Name

c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3']

Name

30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6']

Intrusion-Set

Name
Grayling

Country

Name
Taiwan

StixFile

Value
e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3
5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2
971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f
c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3
245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581
1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce
da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9
d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721

79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17

4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba

6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50

23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae

bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec

6e5d840ddeedc3b691e11a286acd7b6c087a91af27c00044dd1d951da5893068

1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9

752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea

c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5

30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6

12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746

f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b

ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f

d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29

87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8

667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c

1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91

a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe

External References

- https://otx.alienvault.com/pulse/65257b05864d3e1624233f65
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/grayling-taiwan-cyber-attacks