China-linked Actors Maintain Focus on Organizations Influencing U.S. Policy

Recent compromise of a non-profit organization reflects continued interest in U.S. policy.

- **The TTPs have previously been linked to multiple Chinese actors such as Kelp, Space Pirates, and APT41.**
- **APT41 is one of the longest-running Chinese espionage groups.**
- **Attackers were aiming to establish a persistent and stealthy presence on the network. They gained access for several weeks in April 2025.**

China-linked actors continue to show interest in U.S. organizations with links to or involvement in policy issues, including an intrusion earlier this year into a U.S. non-profit organization that is active in attempting to influence U.S. government policy on international issues.

The threat actors appeared determined to establish persistence and maintain long-term access to the network when they gained access to it for several weeks in April 2025. Evidence of various techniques, including the use of a legitimate vetysafe.exe component to sideload a malicious DLL (sbamres.dll.), point to the attackers being based in China. A copy of this malicious DLL was previously used in attacks linked to the China-based threat actors known as Space Pirates. A variant of this component, with a different filename, was also used by the Chinese APT group Kelp (aka Salt Typhoon) in a separate incident. Additionally, the technique was also used by Earth Longzhi, which is believed to be a subgroup of the long-standing Chinese threat group APT41.

The attackers here also used Imjpuexc on the targeted network, which is a legitimate Microsoft file that is used to allow keyboard input from East Asian language scripts, such as Chinese, Japanese, and Korean.

Attack Chain

The first malicious activity occurred on April 5, 2025, when a mass scan was performed against a server attempting various well-known exploits - such as Atlassian OGNL Injection (CVE-2022-26134), Log4j (CVE-2021-44228), Apache Struts (CVE-2017-9805), and GoAhead RCE (CVE-2017-17562), among many others.

There was then a gap in activity until April 16, when a flurry of attacker activity occurred on the network.

At 1.21am local time, several suspicious curl commands were executed:

```
curl -I -k “https://www.google.com”

curl -I -k “https://www.google.com”

curl -I -k “https://www.google.com”

curl -I -k “https://www.microsoft.com”

curl -I -k “https://www.bing.com”

curl -I -k “httos://192.0.0.88”

curl -I -k “https://192.0.0.88”

curl -I -k 192.0.0.88:443

curl -I http://www.goog.elcom

curl -I http://www.google.com

curl -I http://www.google.com
```

These were used to test internet connectivity, before pinging internal systems that may have been of interest to the attackers. The attackers tried multiple different ways to connect to the system they appeared to be interested in (192.0.0.88). They initially tried to connect via HTTPS, then over port 443, followed by google.com pings. Trying all these different methods suggests that the attackers may have been having some issues connecting to the particular machine they were interested in.

Shortly after this initial activity, the attackers executed the Windows command-line tool netstat to collect network configuration information. This was used to list all active connections and their associated processes. It's likely these attackers were mainly interested in TCP connections. Transmission Control Protocol (TCP) is a communications standard that allows application programs and computing devices to exchange messages over a network.

The attackers then created a scheduled task, which was used to ensure persistence:

```
schtasks /create /tn \Microsoft\Windows\Ras\Outbound /tr
"CSIDL_WINDOWS\microsoft.net\framework\v4.0.30319\msbuild.exe
c:\programdata\microsoft\rac\outbound\outbound.xml" /sc minute /mo 60 /ru system
```

A legitimate version of msbuild.exe was then used to launch and execute the contents of an unknown xml file, which was presumably used to launch the following file:

csidl_profile\documents\msoutbound

The schtask command was used to create a new scheduled task called "\Microsoft\Windows\Ras\Outbound", which was configured to run every 60 minutes as a high-privileged SYSTEM user. This was used for persistence and to execute the following command:

```
"CSIDL_WINDOWS\microsoft.net\framework\v4.0.30319\msbuild.exe"
CSIDL_COMMON_APPDATA\microsoft\rac\outbound\outbound.xml
```

After msbuild.exe was launched, we believe it executed the contents of the unknown outbound.xml file, which in turn was used to load and inject unknown code into csc.exe, which was observed connecting to a malicious command and control server (C&C):

hxxp://38.180.83[.]166/6CDF0FC26CDF0FC2

Then at 2.50am, a custom loader (SHA256: f52b86b599d7168d3a41182ccd89165e0d1f2562aa7363e0718d502b7e3fcb69) was executed, passing an encrypted file on the command line, which is decrypted and loaded into memory.

```
CSIDL_SYSTEMX86\msascui.exe MicrosoftRuntime
```

While the payload was unavailable for analysis, it’s likely this was used by the attackers to load a remote access tool (RAT). It’s unclear if this was successful.

Additionally, a legitimate VipreAV component (vetysafe.exe) was used by the attackers for DLL-sideloading to install a loader (sbamres.dll). This technique was previously used by China-linked threat actors including Space Pirates and Earth Longzhi (an APT41 sub-group). The VipreAV component was signed by "Sunbelt Software, Inc." DLL sideloading is a technique where the attackers use the DLL search order mechanism in Windows to plant and then invoke a legitimate application that executes a malicious DLL payload.

This component was also used for DLL sideloading before in conjunction with Deed RAT (aka Snappy Bee), a China-linked remote access Trojan, in activity that was attributed to Kelp (aka Salt Typhoon, Earth Estries). Deed RAT is believed to be shared among multiple Chinese groups.

Kelp came to global prominence in 2024 when it was revealed that the group had compromised the networks of multiple U.S. telecoms companies in the run-up to the 2024 U.S. presidential election and had intercepted the communications of individuals in both the Democratic and Republican presidential campaign camps. That activity was part of a campaign that was believed to have been ongoing for up to two years before its discovery and to have impacted or targeted dozens of countries, including countries in Europe.

APT41 is one of the longest running Chinese espionage groups, and is believed to be composed of multiple sub-groups, including those tracked by the Threat Hunter Team as Blackfly, Grayfly and Redfly. Earth Longzhi was first published about by Trend Micro in 2022, though it documented activity from the group that dated from 2020. At the time Trend said the group had targeted victims in Taiwan, China, Thailand, Malaysia, Indonesia, Pakistan, and Ukraine. Space Pirates are China-linked threat actors that are believed to have been active since at least 2017, and are noted for carrying out attacks against Russian companies.

Also on this network on April 16 was a likely version of Dcsync - a tool used to pretend to be a domain controller (DC) in order to get user credentials from another domain controller via the MS Directory Replication Service Remote Protocol (MS-DRSR):

[i] dcsync: DS Replication Epoch is %u

[x] dcsync: Error in ProcessGetNCChangesReply

[x] dcsync: DRSGetNCChanges, invalid dwOutVersion (%u) and/or cNumObjects (%u)

[x] dcsync: GetNCChanges: 0x%08x (%u)

[x] dcsync: RPC Exception 0x%08x (%u)

The Imjpuexc tool was also seen on the targeted network on 16 April. This was the last attacker activity observed on this machine before all activity ceased completely.

Chinese threat actors remain active

It is clear from the activity on this victim that the attackers were aiming to establish a persistent and stealthy presence on the network, and they were also very interested in targeting domain controllers, which could potentially allow them to spread to many machines on the network.

China-linked groups have always had a focus on espionage activity, and in monitoring foreign governments' attitudes and policies toward China. This attack, and previous activity we documented in December 2024 that targeted a large U.S. organization with a significant presence in China, show that Chinese APT groups continue to take a strong interest in organizations linked to or influential in shaping policy towards China. It is unsurprising in the current geopolitical climate to see these actors taking an interest in U.S.-based institutions.

Also notable in this activity is the use of tools and files that have previously been linked to multiple Chinese actors, such as Kelp, Space Pirates, and APT41. The sharing of tools among groups has been a long-standing trend among Chinese threat actors, making it difficult to say which specific group is behind a set of activities.

Indicators of compromise

51ffcff8367b5723d62b3e3108e38fb7cbf36354e0e520e7df7c8a4f52645c4d – Imjpuexc – csidl_profile\documents\imjpuexc.exe

6f7f099d4c964948b0108b4e69c9e81b5fc5ff449f2fa8405950d41556850ed9 – Unknown – csidl_profile\documents\msoutbound

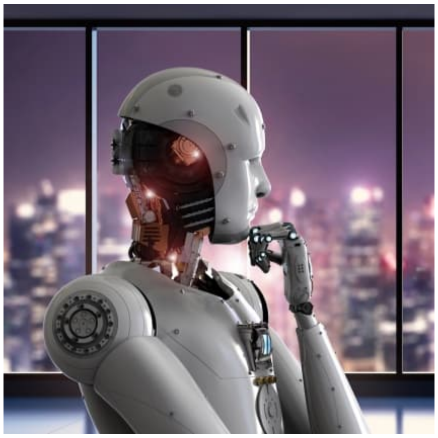
99a0b424bb3a6bbf60e972fd82c514fd971a948f9cedf3b9dc6b033117ecb106 – Same hash also reportedly linked to Space Pirates activity – csidl_profile\ldap_write\documents\sbamres.dll

dae63db9178c5f7fb5f982fbd89683dd82417f1672569fef2bbfef83bec961e2 – Dcsync – csidl_profile\downloads\mmp.exe

e356dbd3bd62c19fa3ff8943fc73a4fab01a6446f989318b7da4abf48d565af2 – Legitimate VipreAV component – csidl_profile\documents\vetysafe.exe

f52b86b599d7168d3a41182ccd89165e0d1f2562aa7363e0718d502b7e3fcb69 – Unknown – csidl_profile\ldap_write\documents\msascui.exe

About the Author



Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

You might also enjoy

U.S. Organization in China Targeted by Attackers

- 5 Dec 2024
- 9 Min Read