ASEAN Entities in the Spotlight: Chinese APT Group Targeting

Executive Summary

Over the past 90 days, Unit 42 researchers have identified two Chinese advanced persistent threat (APT) groups conducting cyberespionage activities against entities and member countries affiliated with the Association of Southeast Asian Nations (ASEAN):

- The first APT group, Stately Taurus, created two malware packages we believe targeted entities in Myanmar, the Philippines, Japan and Singapore. The timing of these campaigns coincided with the ASEAN-Australia Special Summit, held March 4-6, 2024.
- The second Chinese APT group compromised an ASEAN-affiliated entity. This APT group has targeted various Southeast Asia government entities including Cambodia, Laos and Singapore in recent months.

Stately Taurus (aka Mustang Panda, BRONZE PRESIDENT, Red Delta, LuminousMoth, Earth Preta and Camaro Dragon) has been operating since at least 2012. We assess this to be a Chinese APT group that routinely conducts cyberespionage campaigns. This group has historically targeted government entities and nonprofits, as well as religious and other nongovernmental organizations across North America, Europe and Asia.

We recently identified network traffic from the aforementioned ASEAN-affiliated entity to the malicious infrastructure associated with the second Chinese APT group, which indicated the entity's environment had been compromised. ASEAN-affiliated entities are attractive targets for espionage operations due to their role in handling sensitive information regarding diplomatic relations and economic decisions in the region.

Palo Alto Networks customers are better protected from this malicious infrastructure through our Prisma Cloud Defender agents with WildFire integration, as well as DNS Security and Advanced URL Filtering.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics	**China**, **APAC**

Stately Taurus Activity

During the ASEAN-Australia Special Summit held in March 2024, Unit 42 researchers identified two Stately Taurus malware packages that we assess were leveraged to target Asian countries. Threat actors created malware for these packages on March 4-5, 2024, coinciding with the ASEAN-Australia Special Summit (March 4-6, 2024).

Package 1: Talking_Points_for_China.zip

Attackers created the first package on March 4, 2024, as a ZIP archive. Entities located in the Philippines, Japan and Singapore saw it the next day (evidenced by the samples they uploaded to communal databases). Extracting the contents of the `Talking_Points_for_China.zip` archive reveals two files, as shown in Figure 1.

Figure 1. `Talking_Points_for_China.zip`.

The executable `Talking_Points_for_China.exe` is actually a renamed copy of the signed anti-key logging program `KeyScrambler.exe` developed by QFX Software Corporation. Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply that the legitimate product is flawed or malicious.

Upon executing this binary, it sideloads the malicious DLL `KeyScramblerIE.dll` and copies it to the directory `C:\Users\Public\Libraries\SmileTV\KeyScramblerIE.dll` with an autorun registry key of the same location established for persistence.

The code then decrypts shellcode that we assess is PubLoad malware. This malware then attempts to establish a connection to `103.27.109[.]157:443`.

This package displays strong overlap with the sample described by CSIRT-CTI in their post's section entitled Campaign #4 – Talking Points for China.zip. These similarities include:

- The archive filename
- The magic bytes to initiate the payload (`17 03 03`)
- Using a signed binary from QFX Software Corporation
- The execution characteristics of PubLoad malware

Package 2: Note PSO.scr

Threat actors created the second package on March 5, 2024, as a screensaver executable (SCR extension) file, which an entity located in Myanmar saw the same day (evidenced by an upload to a malware repository). Given the filename (`Note PSO.scr`), we suspect that PSO is likely a reference to the title of Personal Staff Officer, a rank in the Myanmar military.

We observed Stately Taurus switching tactics, techniques and procedures (TTPs) for this malicious package. Instead of their typical choice of relying on file archive formats (ZIP, RAR, ISO) for delivery, this time Stately Taurus employed an executable with a screensaver (SCR) file extension for initial infection. This approach resulted in the download of malicious code from the IP address `123.253.32[.]71`.

Upon opening the SCR file, the threat actor attempts to make network connections to download the benign executable `WindowsUpdate.exe` and malicious DLL `EACore.dll`. These files were hosted at the following locations:

- `hxxp[:]//123.253.32[.]71/WindowsUpdate.exe`
- `hxxp[:]//123.253.32[.]71/EACore.dll`

Threat actors use a benign program they've renamed `WindowsUpdate.exe`, which is actually an older version of `EACoreServer.exe` signed by the reputable video game company Electronic Arts, Inc. They do this to give it an appearance of a trustworthy program while, in the background, they're sideloading their malicious DLL file that they've renamed to overwrite the legitimate `EACore.dll`. This malware then attempts to establish a connection to `www[.]openservername[.]com` at `146.70.149[.]36` for command and control (C2).

Second Chinese APT Group Activity

We recently identified network connections between an ASEAN-affiliated entity and the C2 infrastructure of a Chinese APT group, indicating the entity's environment had been compromised. We have also observed similar activity originating from government entities across ASEAN member states. ASEAN-affiliated entities are attractive targets for espionage operations due to their role in handling sensitive information regarding diplomatic relations and economic decisions in the region.

C2 Infrastructure

Table 1 outlines known target-facing infrastructure used for C2.

IP Address	Target Port	Domain(s)
65.20.103[.]231	80, 81	
139.59.46[.]88	80, 443, 8443, 8080, 9443	
193.149.129[.]93	8443	ai.nerdnooks[.]com
192.153.57[.]98	8080	web.daydreamdew[.]net

Table 1. Known infrastructure.

Activity Timeline: Second Chinese APT Group

Unit 42 researchers identified threat actor activity throughout January and February 2024. We also observed a distinct lull coinciding with the Lunar New Year and the Chinese mandated "Special Working Day" on Feb. 18, 2024, as shown in Figure 2.

Image 2 is a timeline of the working days observed identifying the threat actor from the end of January to the end of
Figure 2. Pattern of life: working days.

We observed a similar pattern of life with this same actor during China's Golden Week in September and October 2023.

Working hours for this actor were also consistent with our prior observations of business hours on weekdays (Monday to Friday) adjusted to UTC +08:00 (China Standard Time), as shown in Figure 3.

Image 3 is a heat map of the pattern of life adjusted to China Standard Time. The vertical axis lists the days of the we
Figure 3. Pattern of life: working hours (+08:00 time adjusted).

Conclusion

Unit 42 has identified two Chinese APTs conducting recent cyberespionage activities against the entities and member countries affiliated with the Association of Southeast Asian Nations (ASEAN). These types of campaigns continue to demonstrate how organizations are targeted for cyberespionage purposes, where nation-state affiliated threat groups collect intelligence of geopolitical interests within the region. We encourage organizations to leverage our findings to inform the deployment of protective measures to defend against these types of threats.

Protections and Mitigations

Palo Alto Networks customers are better protected from the threats discussed above through the following products:

- DNS Security and Advanced URL Filtering classify domains in this article as malicious
- WildFire is a cloud based threat detection engine that classifies the Stately Taurus malware samples in this article as malicious
- Prisma Cloud Defender agents with WildFire integration can detect and prevent malicious execution of the Stately Taurus malware samples in this article on Windows-based VM, container and serverless cloud infrastructure.

If you think you might have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America toll-free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance

.

Indicators of Compromise

Stately Taurus Campaigns

Malware Hashes

- a16a40d0182a87fc6219693ac66428673832922983bd9e70b455f198e124ba2
- 316541143187acff1404b98659c6d9c8566107bd652310705214777f03ea10c8
- 02f4186b532b3e33a5cd6d9a39d9469b8d9c12df7cb45dba6dcab912b03e3cb8
- 5cd4003ccaa479734c7f5a01c8ff95891831a29d857757bbd7fe4294f3c5c126

Infrastructure:

- 103.27.109[.]157
- 123.253.32[.]71
- 146.70.149[.]36
- www.openservername[.]com

ASEAN Affiliated Activity

Infrastructure:

- ai.nerdnooks[.]com
- web.daydreamdew[.]net
- 65.20.103[.]231
- 139.59.46[.]88
- 193.149.129[.]93
- 192.153.57[.]98

Additional Resources

- Intruders in the Library: Exploring DLL Hijacking – Unit 42, Palo Alto Networks

- Stately Taurus Continued – New Information on Cyberespionage Attacks against Myanmar Military Junta – CSIRT-CTI
- Chinese APT Targeting Cambodian Government – Unit 42, Palo Alto Networks