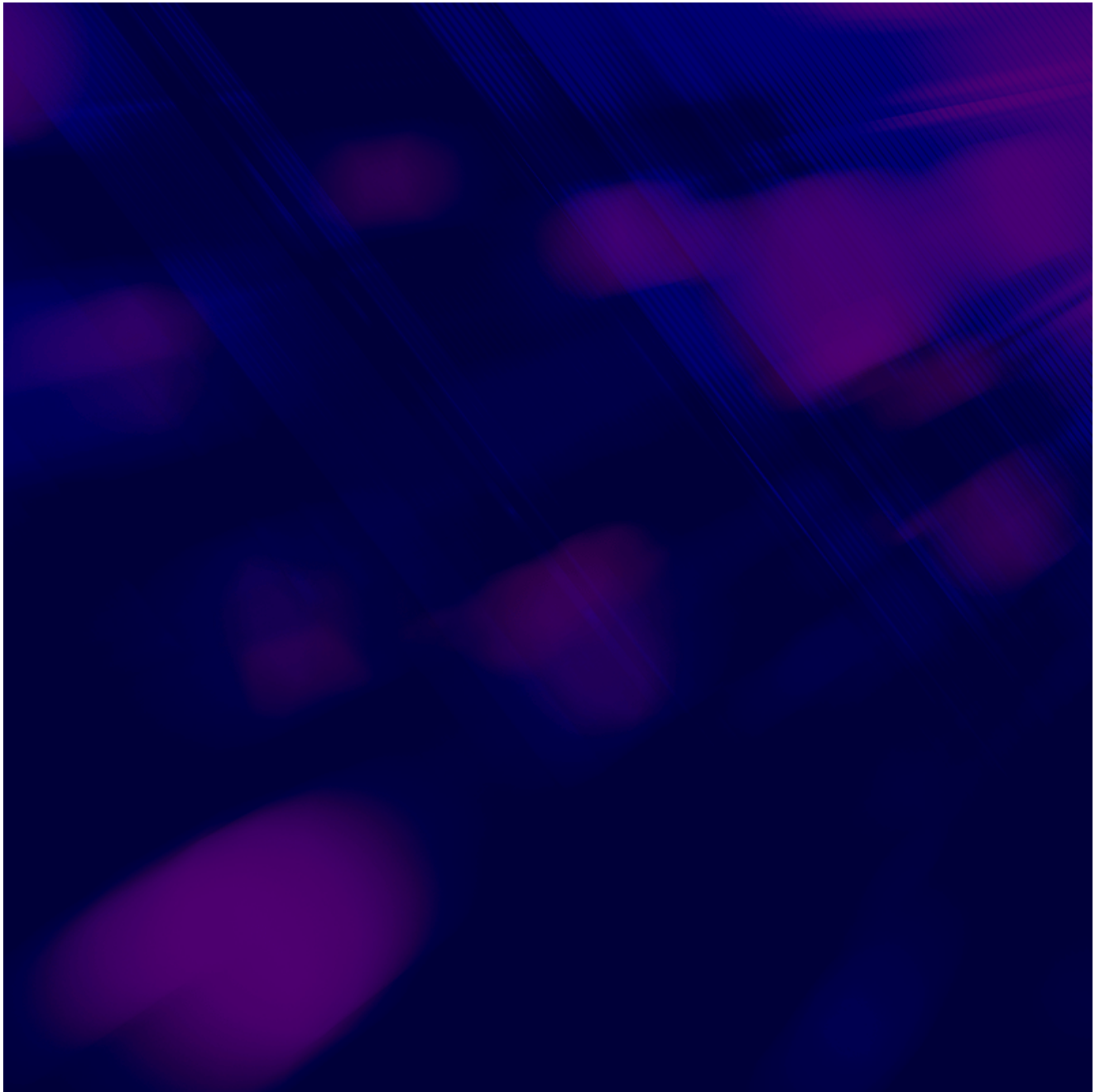


Chinese Cyberespionage Group BRONZE SILHOUETTE Targets U.S. Government and Defense Organizations

[Sw secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations](https://secureworks.com/blog/chinese-cyberespionage-group-bronze-silhouette-targets-us-government-and-defense-organizations)

Secureworks Counter Threat Unit



Direct observations of multiple intrusions reveal that the group focuses on operational security. Wednesday, May 24, 2023 By: Secureworks Counter Threat Unit

On May 24, 2023, the U.S. National Security Agency (NSA) issued a joint cybersecurity advisory highlighting a cluster of activity it attributes to a People's Republic of China (PRC) state-sponsored threat group. Secureworks® Counter Threat Unit™ (CTU) researchers attribute this activity to BRONZE SILHOUETTE (referred to in the advisory as Volt Typhoon) and have observed the threat group conducting network intrusion operations against U.S government and defense organizations since 2021. The tactics, techniques, and procedures (TTPs) and victimology observed during Secureworks incident response (IR) engagements suggest BRONZE SILHOUTTE targets organizations for intelligence-gathering purposes that are in alignment with the requirements of the PRC. The threat group has demonstrated careful consideration for operational security such as the use of preinstalled binaries to “live off the land,” incorporation of defense evasion techniques, and reliance on compromised infrastructure to prevent detection and attribution of its intrusion activity, and to blend in with legitimate network activity.

June 2021 IR engagement

During a June 2021 engagement, Secureworks incident responders discovered that BRONZE SILHOUETTE had gained initial access to the compromised organization's single-factor Citrix environment via a domain administrator account. It is unclear how the threat actors obtained these credentials. BRONZE SILHOUETTE moved laterally to another web server and dropped a simple Java-based web shell (AuditReport.jspx). Secureworks incident responders observed the threat actors execute a series of reconnaissance commands via the web shell (see Figure 1).



```
* cmd /C whoami (2021-06-06)
* cmd /C "ping [redacted] -n 1" (2021-06-06)
* cmd /C "net group [redacted] (2021-06-06)
* cmd /C "net user [redacted] (2021-06-06)
* cmd /C "net user [redacted] (2021-06-06)
* cmd /C "net use \\ [redacted] \admin$ (2021-06-06)
* cmd /C "dir \\ [redacted] \C$" (2021-06-06)
* cmd /C "dir \\ [redacted] \inetpub" (2021-06-06)
* cmd /C "dir \\ [redacted] \inetpub\wwwroot" (2021-06-06)
```

Figure 1. Reconnaissance commands issued through Java-based web shell. (Source: Secureworks)

BRONZE SILHOUETTE then wrote Base64-encoded text to C:\Windows\Temp\ntuser.ini and decoded it to C:\Windows\Temp\iisstart.aspx via the certutil command (see Figure 2).

- Used Windows Management Instrumentation (WMI) to execute the Ntdsutil Active Directory (AD) management tool on the domain controller (see Figure 4). This command creates a copy of the ntds.dit AD database for credential attacks such as pass the hash or offline password hash cracking.

```
cmd /C "wmic /node: [REDACTED] /password: [REDACTED] process call create "cmd.exe /c mkdir C:\Windows\Temp\pro & ntdsutil \ac i ntds\ ifm \create full C:\Windows\Temp\pro\ q q"" (2021-06 [REDACTED])"
```

Figure 4. Credential dumping using Ntdsutil. (Source: Secureworks)

- Copied the ntds.dit database to the web server via xcopy, compressed the database as a multi-volume password-protected archive via 7-Zip, and saved the volumes to a public-facing directory on the same server with legitimate-sounding filenames and a .gif extension.
- Used the rd command with the /S switch to delete the threat actors' working directories and files.

The threat actors then exfiltrated the dumped AD database to an external IP address. This IP address belonged to a compromised server at an organization in the same vertical as the compromised organization.

September 2021 IR engagement

BRONZE SILHOUETTE reappeared in a September 2021 Secureworks IR engagement against an organization in the U.S. The threat actors gained initial access by exploiting a vulnerability in an internet-facing ManageEngine ADSelfService Plus server (likely CVE-2021-40539). BRONZE SILHOUETTE deployed a web shell (ReportGenerate.jsp) and interacted with it to run reconnaissance commands using built-in Windows tools such as net user, nltest, netstat, and systeminfo (see Figure 5).

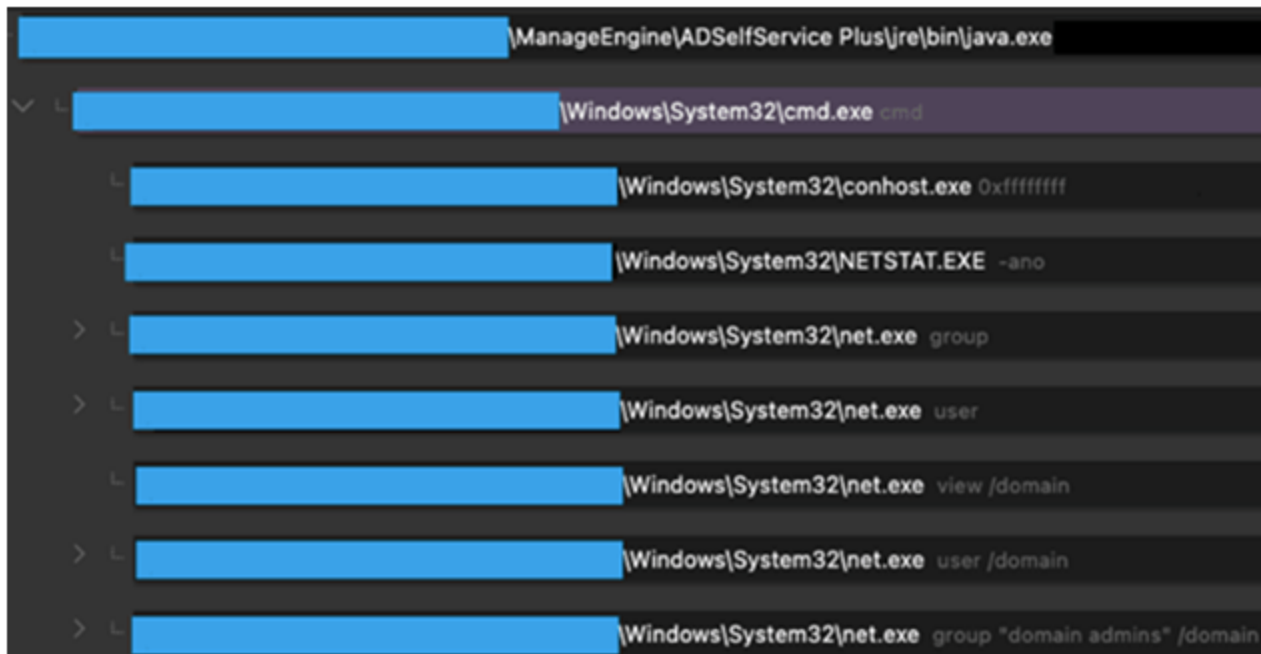


Figure 5. BRONZE SILHOUETTE reconnaissance commands. (Source: Secureworks)

Secureworks incident responders observed the threat actors executing ADSSPlus.exe, which is a renamed csvde.exe file. The csvde.exe command-line utility provides import and export functionality for Lightweight Directory Access Protocol (LDAP) repositories. The threat actors used the '-f' switch, which exports a list of AD objects to the ADSSPlus.dat file (see Figure 6).

```
ADSSPlus.exe -f "C:\ManageEngine\ADSelfService Plus\bin\ADSSPlus.dat"
```

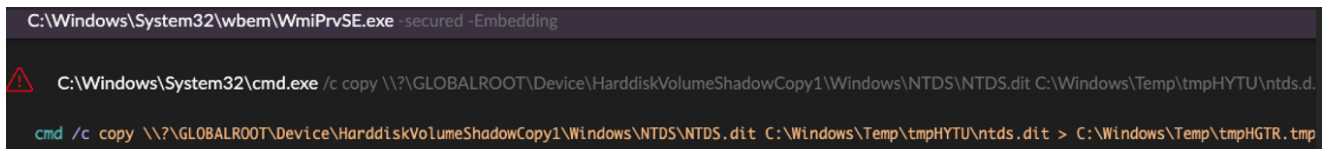
Figure 6. Threat actor command to export AD objects to ADSSPlus.dat. (Source: Secureworks)

BRONZE SILHOUETTE used the Windows makecab command to compress the ADSSPlus.dat file into a cabinet (.cab) file, but Secureworks incident responders did not observe the threat actor exfiltrating the file.

June 2022 IR engagement

During a June 2022 engagement, Secureworks incident responders discovered that BRONZE SILHOUTTE had deployed a single web shell to multiple servers across the environment after likely exploiting an internet-facing PRTG Network Monitor server. The web shell was also a derivative of the Awen web shell but included key modifications such as the addition of AES encryption and decryption for command and control (C2) communications. Based on web shell file creation timestamps, the network was likely compromised in May 2021.

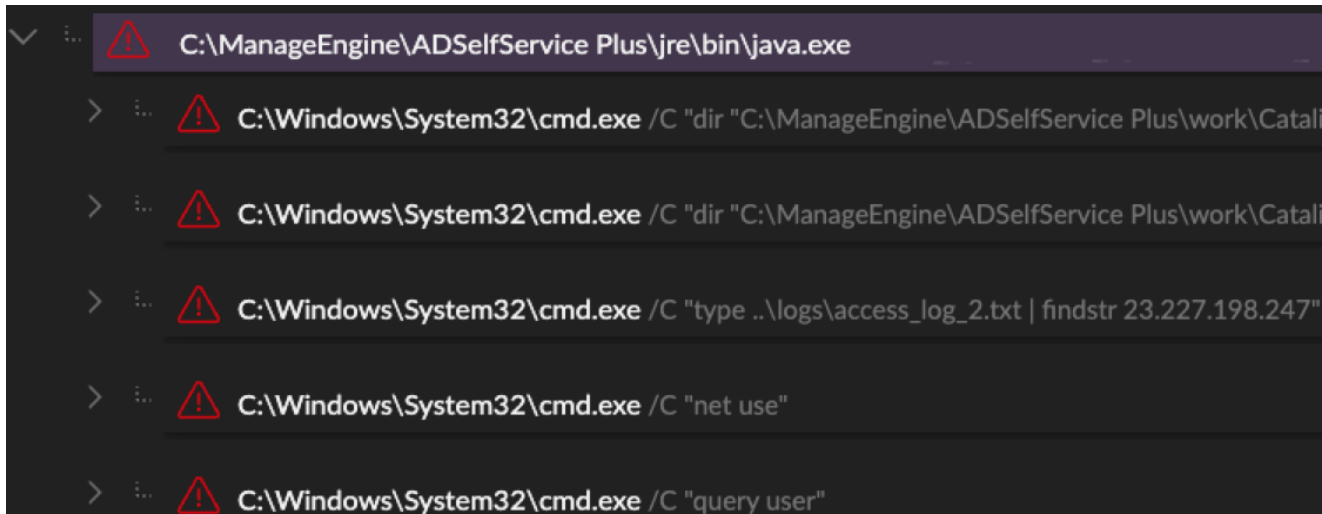
The threat actors used WMI to execute the native vssadmin command on a domain controller to create a volume shadow copy (see Figure 7). They then extracted the ntds.dit AD database and the SYSTEM registry hive from the volume shadow copy (see Figure 7).



```
C:\Windows\System32\wbem\WmiPrvSE.exe -secured -Embedding
C:\Windows\System32\cmd.exe /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\Windows\Temp\tmpHYTU\ntds.d
cmd /c copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\Windows\Temp\tmpHYTU\ntds.dit > C:\Windows\Temp\tmpHGTR.tmp
```

Figure 7. Threat actor WMI commands to extract the ntds.dit database. (Source: Secureworks)

Secureworks incident responders observed the threat actors using 7-Zip to create an archive file containing the SYSTEM registry hive and ntds.dit, likely for exfiltration. A few days later, the threat actors moved laterally to a ManageEngine ADSelfService Plus server and ran reconnaissance commands. One command revealed BRONZE SILHOUETTE searching for one of its C2 IP addresses (see Figure 8).



```
C:\ManageEngine\ADSelfService Plus\jre\bin\java.exe
C:\Windows\System32\cmd.exe /C "dir "C:\ManageEngine\ADSelfService Plus\work\Catali
C:\Windows\System32\cmd.exe /C "dir "C:\ManageEngine\ADSelfService Plus\work\Catali
C:\Windows\System32\cmd.exe /C "type ..\logs\access_log_2.txt | findstr 23.227.198.247"
C:\Windows\System32\cmd.exe /C "net use"
C:\Windows\System32\cmd.exe /C "query user"
```

Figure 8. Threat actor commands run under the ManageEngine Java process. (Source: Secureworks)

A CTU investigation into the attacker-controlled C2 infrastructure revealed at least three PRTG servers belonging to other organizations. This discovery suggests that BRONZE SILHOUETTE targets vulnerable PRTG servers for initial access into a target environment and to establish its C2 infrastructure.

BRONZE SILHOUETTE: A member of the new wave of Chinese threat groups?

CTU analysis of the direct observations from BRONZE SILHOUETTE intrusions reveals a threat group that favors web shells for persistence and relies on short bursts of activity primarily involving living-off-the-land binaries to achieve its objectives. For example, the June 2021 IR engagement determined that the threat actors were inside the compromised network

for only 90 minutes before obtaining the ntds.dit AD database. The threat actors also take steps to identify and remove evidence of their presence on a network, such as inspecting server logs for their C2 IP address and deleting files used during their intrusions.

BRONZE SILHOUETTE's use of other organizations' compromised servers in its C2 proxy network may help obfuscate the source of the intrusion activity and make attribution more challenging. In some intrusions, the C2 communications could blend in with legitimate business network traffic to reduce the likelihood of detection.

BRONZE SILHOUETTE has consistently focused on operational security, including a minimal intrusion footprint, incorporation of defense evasion techniques, and use of compromised infrastructure in multiple intrusions. This focus suggests a high level of operational maturity and adherence to a blueprint designed to reduce the likelihood of the detection and attribution of its intrusion activity. This attention to operational security, particularly when targeting Western organizations, is consistent with network compromises that CTU researchers have attributed to Chinese threat groups in recent years. These tradecraft developments have likely been driven by a series of high-profile U.S. Department of Justice indictments of Chinese nationals allegedly involved in cyberespionage activity, public exposures of this type of activity by security vendors, and the consequential likely increased pressure from PRC leadership to avoid public scrutiny of its cyberespionage activity.

BRONZE SILHOUETTE likely operates on behalf the PRC. The targeting of U.S. government and defense organizations for intelligence gain aligns with PRC requirements, and the tradecraft observed in these engagements overlap with other state-sponsored Chinese threat groups.

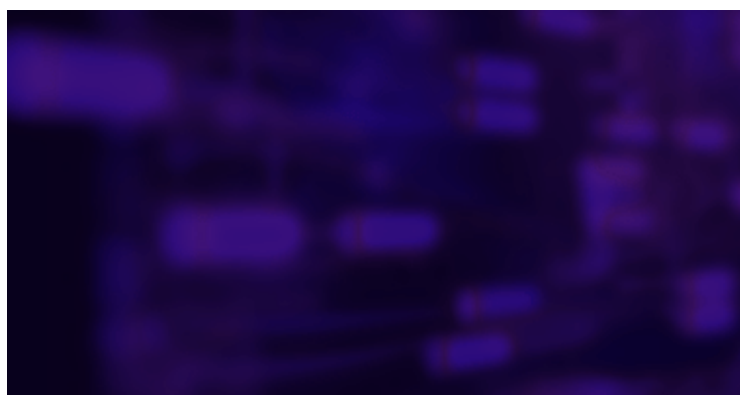
To mitigate exposure to this threat, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The IP addresses may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
006c4a5950f75c2c9049cda1a62c09a0	MD5 hash	Web shell (iisstart.aspx) used by BRONZE SILHOUETTE
4d3572cfc8460fe0299377f6bc05d865a987529f	SHA1 hash	Web shell (iisstart.aspx) used by BRONZE SILHOUETTE
3a9d8bb85fbcfe92bae79d5ab18e4bca9eaf36cea70086e8d1ab85336c83945f	SHA256 hash	Web shell (iisstart.aspx) used by BRONZE SILHOUETTE

Indicator	Type	Context
af3a81605aa8e29c8be9e91d2ce19fc1	MD5 hash	Base64-encoded web shell (ntuser.ini) used by BRONZE SILHOUETTE
a9e32e2bd499c1070f4e0b5a6d85119f1aa0a778	SHA1 hash	Base64-encoded web shell (ntuser.ini) used by BRONZE SILHOUETTE
fe95a382b4f879830e2666473d662a24b34fccf34b6b3505ee1b62b32adafa15	SHA256 hash	Base64-encoded web shell (ntuser.ini) used by BRONZE SILHOUETTE
670545a24a2ce2ac7a0e863790bfe2e1	MD5 hash	Java web shell (AuditReport.jspx) used by BRONZE SILHOUETTE
4ba6b043313c8d163f2ab7c4505c8b9b8cd68061	SHA1 hash	Java web shell (AuditReport.jspx) used by BRONZE SILHOUETTE
ee8df354503a56c62719656fae71b3502acf9f87951c55ffd955feec90a11484	SHA256 hash	Java web shell (AuditReport.jspx) used by BRONZE SILHOUETTE
109.166.39.139	IP address	BRONZE SILHOUETTE C2 server
23.227.198.247	IP address	BRONZE SILHOUETTE C2 server
104.161.54.203	IP address	BRONZE SILHOUETTE C2 server

Table 1. Indicators for this threat.

Read more about Chinese threats in the [2022 State of the Threat report](#). If you need urgent assistance with an incident, contact the [Secureworks Incident Response team](#).



Stay Informed

Get the latest in cybersecurity news, trends, and research

[SEND ME UPDATES](#)



Secureworks Taegis™

Security Analytics +
Human Intelligence
Delivers Better
Security Outcomes

[About Taegis](#)

Latest Report



[Reports](#)

[2022 State of the Threat Report](#)