Taiwan Web Infrastructure targeted by APT UAT-7237 with custom toolset

Data: 2025-08-16 07:40:06

Autor: Inteligência Against Invaders

Taiwan Web Infrastructure targeted by APT UAT-7237 with custom toolset

APT group UAT-7237, linked to UAT-5918, targets web infrastructure in Taiwan using customized open-source tools to maintain long-term access.

A Chinese-speaking advanced persistent threat (APT) group, tracked as UAT-7237, has been observed targeting web infrastructure entities in Taiwan using customized versions of open-sourced tools with an aim to establish long-term access within high-value victim environments.

UAT-7237 has been active since at least 2022, the researchers found significant overlaps with UAT-5918, which is an info-stealing threat actor active since 2023 and known for using web shells and open-source tools for persistence and credential theft. Talos experts believe that UAT-7237 is a subgroup of 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.” reads the report *published by Talos.*

“UAT-7237 aims to establish long-term persistence in high-value victim environments.”

Talos researchers observed the UAT-7237 APT group using a customized Shellcode loader tracked as “SoundBill.” SoundBill can be employed to decode and load any shellcode, including Cobalt Strike.

UAT-7237 exploits unpatched servers for initial access, then performs rapid reconnaissance using commands like nslookup, systeminfo, and ping before establishing persistence via SoftEther VPN and RDP rather than web shells.

They move through networks using SMB shares and check for domain admins and controllers. They also use built-in Windows tools like SharpWMI and WMICmd to run commands, gather system info, and prepare for further attacks.

After compromising systems, UAT-7237 deploys custom and open-source tools to maintain access and steal data. Their custom loader, SoundBill, decodes and executes shellcode from files like ptiti.txt, running payloads ranging from Mimikatz to Cobalt Strike for credential theft and long-term access. SoundBill has two built-in programs from QQ, a Chinese messaging app, likely used as decoys in phishing attacks.

They also use JuicyPotato for privilege escalation and modify Windows settings, like disabling UAC and enabling cleartext password storage.

Credentials are primarily harvested with Mimikatz, sometimes embedded in SoundBill, and through LSASS dumping (Project1.exe) or registry searches for VNC credentials. Extracted data is compressed for exfiltration, enabling attackers to pivot, escalate privileges, and maintain persistence.

The threat actor spreads in networks using tools like FScan and SMB scans to find accessible systems. They pivot using stolen credentials and maintain long-term access via SoftEther VPN, with configurations in Simplified Chinese, indicating operator proficiency. Their VPN setup was active from Sept 2022 to Dec 2024, showing extended use.

Talos published IOCs for this research on GitHub.

Follow me on Twitter:@securityaffairsandFacebookandMastodon

PierluigiPaganini

(SecurityAffairs–hacking,China)