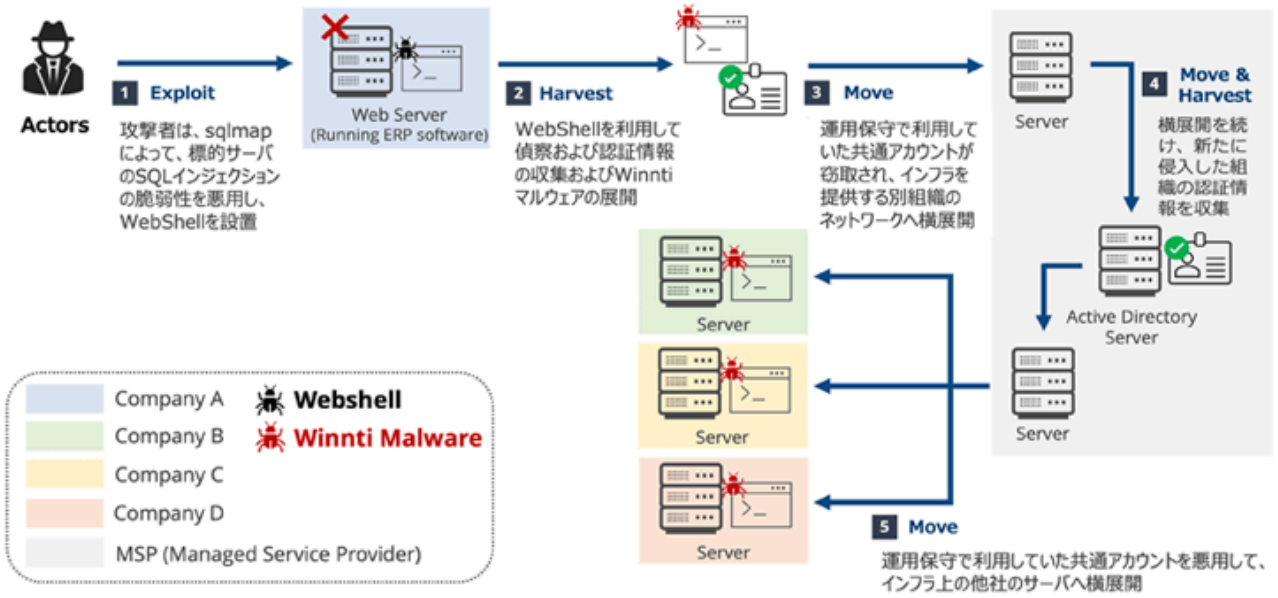
Winnti APT41 Targets Japanese Firms in RevivalStone Cyber Espionage Campaign

By The Hacker News

Published: 2025-02-18 · Archived: 2026-04-05 14:40:41 UTC



The China-linked threat actor known as Winnti has been attributed to a new campaign dubbed **RevivalStone** that targeted Japanese companies in the manufacturing, materials, and energy sectors in March 2024.

The activity, detailed by Japanese cybersecurity company LAC, overlaps with a threat cluster tracked by Trend Micro as Earth Freybug, which has been assessed to be a subset within the APT41 cyber espionage group. It's also monitored by Cybereason under the name Operation CuckooBees, and by Symantec as Blackfly.

APT41 has been described as a highly skilled and methodical actor with the ability to mount espionage attacks as well as poison the supply chain. Its campaigns are often designed with stealth in mind, leveraging a bevy of tactics to achieve its goals by using a custom toolset that not only bypasses security software installed in the environment, but also harvests critical information and establishes covert channels for persistent remote access.

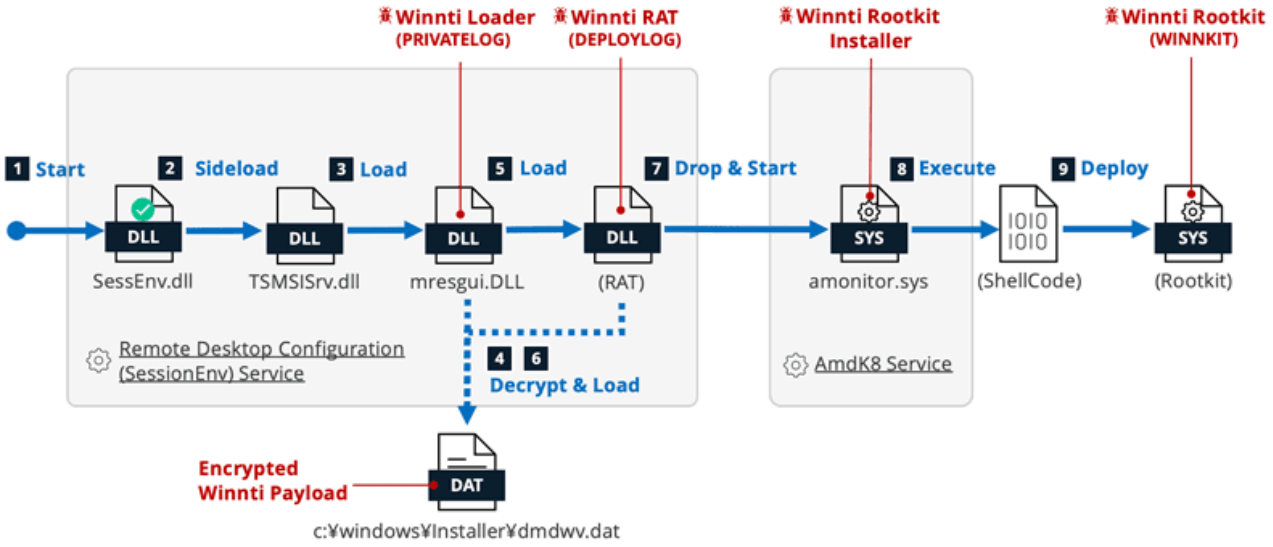
"The group's espionage activities, many of which are aligned with the nation's strategic objectives, have targeted a wide range of public and private industry sectors around the world," LAC said.

"The attacks of this threat group are characterized by the use of Winnti malware, which has a unique rootkit that allows for the hiding and manipulation of communications, as well as the use of stolen, legitimate digital certificates in the malware."

Winnti, active since at least 2012, has primarily singled out manufacturing and materials-related organizations in Asia as of 2022, with recent campaigns between November 2023 and October 2024 targeting the Asia-Pacific (APAC) region exploiting weaknesses in public-facing applications like IBM Lotus Domino to deploy malware as follows -

- **DEATHLOTUS** - A passive CGI backdoor that supports file creation and command execution
- **UNAPIMON** - A defense evasion utility written in C++
- **PRIVATELOG** - A loader that's used to drop Winnti RAT (aka DEPLOYLOG) which, in turn, delivers a kernel-level rootkit named WINNKIT by means of a rootkit installer
- **CUNNINGPIGEON** - A backdoor that uses Microsoft Graph API to fetch commands – file and process management, and custom proxy – from mail messages
- **WINDJAMMER** - A rootkit with capabilities to intercept TCPIP Network Interface, as well as create covert channels with infected endpoints within intranet
- **SHADOWGAZE** - A passive backdoor reusing listening port from IIS web server

The latest attack chain documented by LAC has been found to exploit an SQL injection vulnerability in an unspecified enterprise resource planning (ERP) system to drop web shells such as China Chopper and Behinder (aka Bingxia and IceScorpion) on the compromised server, using the access to perform reconnaissance, collect credentials for lateral movement, and deliver an improved version of the Winnti malware.



The intrusion's reach is said to have been expanded further to breach a managed service provider (MSP) by leveraging a shared account, followed by weaponizing the company's infrastructure to propagate the malware further to three other organizations.

LAC said it also found references to TreadStone and StoneV5 in the RevivalStone campaign, with the former being a controller that's designed to work with the Winnti malware and which was also included in the I-Soon (aka Anxun) leak of last year in connection with a Linux malware control panel.

"If TreadStone has the same meaning as the Winnti malware, it is only speculation, but StoneV5 could also mean Version 5, and it is possible that the malware used in this attack is Winnti v5.0," researchers Takuma Matsumoto and Yoshihiro Ishikawa said.

"The new Winnti malware has been implemented with features such as obfuscation, updated encryption algorithms, and evasion by security products, and it is likely that this attacker group will continue to update the functions of the Winnti malware and use it in attacks."

The disclosure comes as Fortinet FortiGuard Labs detailed a Linux-based attack suite dubbed SSHDInjector that's equipped to hijack the SSH daemon on network appliances by injecting malware into the process for persistent access and covert actions since November 2024.

The malware suite, associated with another Chinese nation-state hacking group known as Daggerfly (aka Bronze Highland and Evasive Panda), is engineered for data exfiltration, listening for incoming instructions from a remote server to enumerate running processes and services, perform file operations, launch terminal, and execute terminal commands.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2025/02/winnti-apt41-targets-japanese-firms-in.html