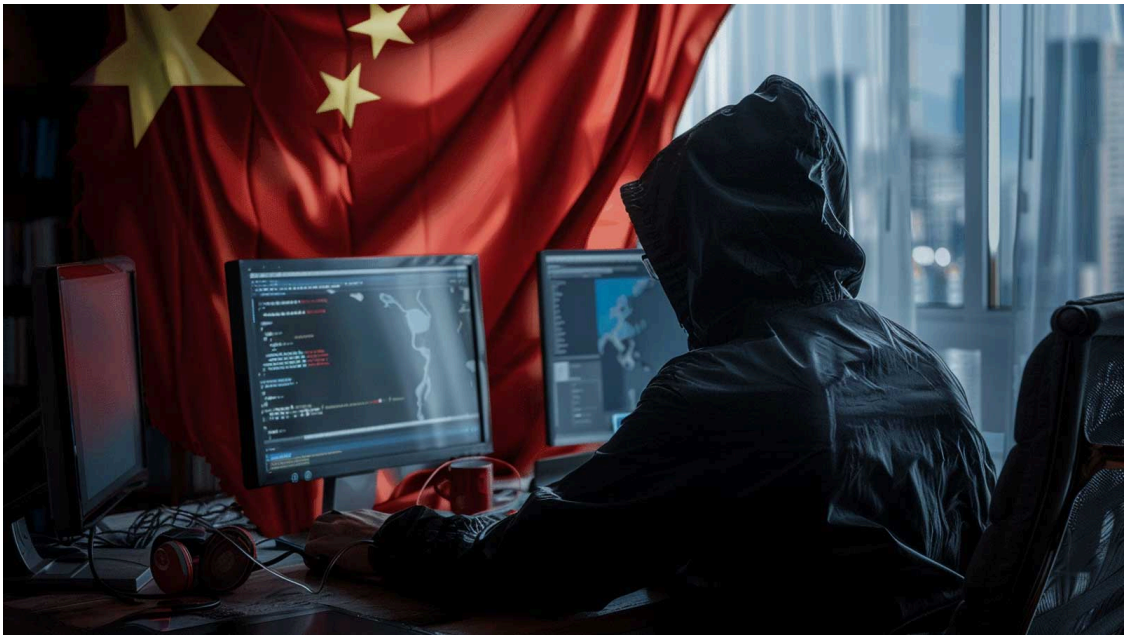
Chinese hackers breached National Guard to steal network configurations

By Lawrence Abrams

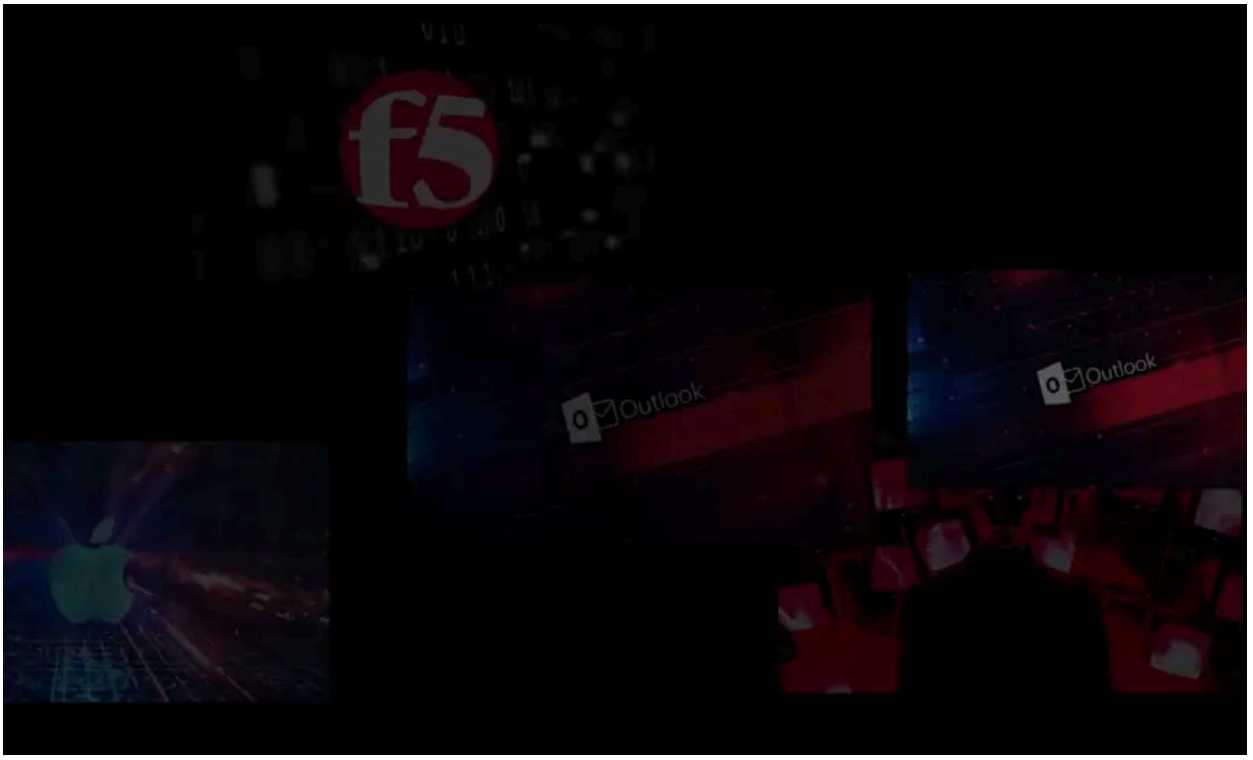
Published: 2025-07-17 · Archived: 2026-04-02 10:37:32 UTC



The Chinese state-sponsored hacking group known as Salt Typhoon breached and remained undetected in a U.S. Army National Guard network for nine months in 2024, stealing network configuration files and administrator credentials that could be used to compromise other government networks.

Salt Typhoon is a Chinese state-sponsored hacking group that is believed to be affiliated with China's Ministry of State Security (MSS) intelligence agency. The hacking group has gained notoriety over the past two years for its wave of attacks on telecommunications and broadband providers worldwide, including AT&T, Verizon, Lumen, Charter, Windstream, and Viasat.

The goal of some of these attacks was to gain access to sensitive call logs, private communications, and law-enforcement wiretap systems used by the U.S. government.


f5
Outlook
Outlook

National Guard network breached for nine months

A June 11 Department of Homeland Security memo, first reported by NBC, says that Salt Typhoon breached a U.S. state's Army National Guard network for nine months between March and December 2024.

During this time, the hackers stole network diagrams, configuration files, administrator credentials, and personal information of service members that could be used to breach National Guard and government networks in other states.

"Between March and December 2024, Salt Typhoon extensively compromised a US state's Army National Guard's network and, among other things, collected its network configuration and its data traffic with its counterparts' networks in every other US state and at least four US territories, according to a DOD report," reads the memo.

"This data also included these networks' administrator credentials and network diagrams—which could be used to facilitate follow-on Salt Typhoon hacks of these units."

The memo further states that Salt Typhoon has previously utilized stolen network topologies and configuration files to compromise critical infrastructure and U.S. government agencies.

"Salt Typhoon has previously used exfiltrated network configuration files to enable cyber intrusions elsewhere," continued the memo.

"Between January and March 2024, Salt Typhoon exfiltrated configuration files associated with other U.S. government and critical infrastructure entities, including at least two U.S. state government agencies. At least one of these files later informed their compromise of a vulnerable device on another U.S. government agency's network."

Network configuration files contain the settings, security profiles, and credentials configured on networking devices, such as routers, firewalls, and VPN gateways. This information is valuable to an attacker, as it can be used to identify paths to and credentials for other sensitive networks that are typically not accessible via the Internet.

The DHS warns that between 2023 and 2024, Salt Typhoon stole 1,462 network configuration files associated with approximately 70 U.S. government and critical infrastructure entities from 12 sectors.

While it was not disclosed how Salt Typhoon breached the National Guard network, Salt Typhoon is known for targeting old vulnerabilities in networking devices, such as Cisco routers.

The DHS memo shared the following vulnerabilities that Salt Typhoon leveraged in the past to breach networks:

- **CVE-2018-0171:** A critical flaw in Cisco IOS and IOS XE Smart Install that allows remote code execution via specially crafted TCP packets.
- **CVE-2023-20198:** A zero-day affecting Cisco IOS XE web UI that permits unauthenticated remote access to devices.
- **CVE-2023-20273:** A privilege escalation flaw also targeting IOS XE that allows hackers to execute commands as root. This flaw has been seen chained with CVE-2023-20198 to maintain persistence.
- **CVE-2024-3400:** A command injection vulnerability in Palo Alto Networks' PAN-OS GlobalProtect, which allows unauthenticated attackers to execute commands on devices.

DOH also shared the following IP addresses that have been used by Salt Typhoon when exploiting the above vulnerabilities:

```
 43.254.132[.]118
146.70.24[.]144
176.111.218[.]190
113.161.16[.]130
23.146.242[.]131
58.247.195[.]208
```

In previous attacks, the hackers exploited unpatched Cisco routers in telecom environments to gain access to infrastructure. The attackers used this access to spy on communications of U.S. political campaigns and lawmakers.

As part of these attacks, the threat actors deployed custom malware named JumblePath and GhostSpider to surveil telecom networks.

The DHS memo urges National Guard and government cybersecurity teams to ensure these flaws have been patched and to turn off unnecessary services, segment SMB traffic, implement SMB signing, and enforce access controls.

A National Guard Bureau spokesperson confirmed the breach to NBC but declined to share specifics, stating that it had not disrupted federal or state missions.

China's embassy in Washington did not deny the attack but stated the U.S. had not provided "conclusive and reliable evidence" that Salt Typhoon is linked to the Chinese government.

Source: https://www.bleepingcomputer.com/news/security/chinese-hackers-breached-national-guard-to-steal-network-configurations/