Salt Typhoon:

China's Persistent Telecom Espionage Campaign

Carl Lochstampfor

Department of Cybersecurity, Old Dominion University,

CS 462, Computer Networking and Cybersecurity

May 3, 2026

Salt Typhoon: China's Persistent Telecom Espionage Campaign

In September 2024, U.S. officials reported that Salt Typhoon, a state-sponsored hacking group linked to the People's Republic of China (PRC), breached major American telecommunications providers, including AT&T, Verizon, T-Mobile, and Lumen Technologies (DiMolfetta, 2025). The breach was unique not because of new hacking techniques but for exploiting known flaws, stealing credentials, and capitalizing on weak security practices that organizations ignored despite available patches (Eclypsium, 2025; More, 2025; Caveza, 2025). This case shows how basic network security lapses enable major espionage campaigns and underscores this paper's central claim: that neglecting simple protections in telecom infrastructure exposes organizations to ongoing, large-scale cyber threats.

Salt Typhoon shows that a cyberattack on critical infrastructure, such as core network nodes or edge routers, can disrupt multiple organizations. Telecommunications providers manage traffic for enterprises, governments, and individuals via protocols such as SIP, BGP, and DNS, so breaches pose national security and privacy risks. To support the claim that persistent threats grow from ignored basic security, this paper analyzes: (1) Salt Typhoon's tactics, techniques, and procedures (TTPs), (2) targeted devices and protocols, (3) campaign and societal impact, and (4) mitigation strategies to reduce the risk of similar advanced persistent threat (APT) attacks.

Background and State Sponsorship

U.S. and allied cyber agencies describe Salt Typhoon as a PRC state-sponsored threat actor engaged in espionage targeting telecommunications and other critical sectors (Cybersecurity and Infrastructure Security Agency [CISA] et al., 2025). Threat intelligence reporting characterizes the

group as a well-resourced advanced persistent threat (APT) focused on maintaining unauthorized, hidden access over long periods rather than launching quick, disruptive attacks (Recorded Future Insikt Group, 2025). Sources consistently portray Salt Typhoon as part of a larger, state-directed intelligence effort. That effort aims to help China gain strategic economic and political advantages by targeting global communications infrastructure.

In January 2025, the U.S. Department of the Treasury sanctioned Sichuan Juxinhe Network Technology Co., Ltd. for its direct role in Salt Typhoon operations, confirming the company's involvement in compromising major U.S. telecommunications and internet service provider networks (U.S. Department of the Treasury, 2025). The action also highlights China's practice of contracting private cybersecurity firms to carry out state-directed operations — a model that explains the scale and endurance of such campaigns. Taken together, Treasury sanctions and independent threat intelligence confirm that Salt Typhoon operates in support of Chinese state objectives rather than for independent criminal gain (U.S. Department of the Treasury, 2025; Recorded Future Insikt Group, 2025).

How the Attack Worked

The six stages of the Salt Typhoon attack sequence are illustrated in Figure 1 (see Appendix A).

Initial Access and Persistence

CVE-2023-20198 provided attackers with a clear technical entry point. This serious flaw in Cisco IOS XE's web interface allows unauthenticated attackers (those not required to log in or verify identity) to create accounts with level 15 privileges, granting them the highest level of administrative control (Eclypsium, 2025). Since many affected devices sit at network edges (the

boundary between a secure internal network and external sources) exploiting one router could give attackers an immediate foothold.

What made CVE-2023-20198 especially dangerous and damaging was how widely it was exploited before organizations responded. Recorded Future's Insikt Group identified Salt Typhoon attempting to compromise over 1,000 internet-facing Cisco devices across six separate targeting campaigns, with telecommunications providers representing a primary focus (Recorded Future Insikt Group, 2025). Although patches had been available since October 2023, unpatched devices were still being successfully compromised months later — a pattern that points to a systemic failure in how enterprises prioritize updates for network edge equipment (More, 2025).

Rather than stopping at one vulnerability, Salt Typhoon layered a second exploit on top of the first. Once administrative access was obtained via CVE-2023-20198, the attackers used CVE-2023-20273 to execute root-level commands, thereby gaining unrestricted control (Eclypsium, 2025). Cisco Talos confirmed that the group relied on stolen credentials and living-off-the-land techniques, with no evidence of zero-day exploits — meaning Salt Typhoon needed no novel capabilities, as everything they required was either already on the device or accessible through long-unpatched flaws (More, 2025). Caveza's analysis reinforced this: ProxyLogon in Microsoft Exchange, another flaw linked to Salt Typhoon, remained unpatched on most exposed systems well after a fix was available (Caveza, 2025). The group's willingness to exploit both old and new vulnerabilities suggests an opportunistic approach: if a device was reachable and unpatched, it was a qualified target (DiMolfetta, 2025).

After gaining full control, Salt Typhoon configured Generic Routing Encapsulation (GRE) tunnels (data channels that encapsulate and transmit packets across networks) between compromised devices and attacker-controlled infrastructure (CISA et al., 2025). Because GRE is

a legitimate and commonly used tunneling protocol in enterprise networking, Salt Typhoon could blend in with ordinary traffic if organizations did not closely monitor device configurations. This aided their persistence, allowing attackers to retain access even after defenders changed passwords or removed suspicious accounts.

Lateral Movement and Evasion

With a foothold established, Salt Typhoon sought deeper access into their victims' networks. The method was simple yet effective: by intercepting TACACS+ (Terminal Access Controller Access-Control System Plus, a protocol for authenticating network administrators) authentication traffic on compromised devices, the attackers captured network administrators' credentials during routine, daily work (CISA et al., 2025). Those stolen credentials then unlocked additional routers, switches, and network segments, enabling lateral movement without requiring new vulnerabilities to be exploited at each step.

Covering their tracks was just as deliberate as the intrusion itself. A custom malware tool called JumbledPath, disclosed by Cisco Talos in February 2025, routed attacker commands through chains of compromised Cisco devices, making it difficult to trace their origin (Wright, 2025). Additionally, Salt Typhoon routinely erased logs on devices they accessed — and in many cases, victim organizations had not retained sufficient logs to assist investigations, leaving little evidence to reconstruct events afterward (CISA et al., 2025). The attackers also exploited Cisco's built-in Guest Shell feature, a separate lightweight virtual Linux environment on Cisco devices, to run their tools in a space not typically monitored by security teams (CISA et al., 2025).

Devices and Protocols Targeted

Salt Typhoon primarily targeted network edge devices, such as routers, firewalls, VPN gateways (devices that create secure connections for remote access), and related management infrastructure (Eclypsium, 2025). These devices are attractive targets because they sit between internal systems and outside traffic, carry broad visibility into communications, and typically receive slower patching updates than standard servers and workstations. Cisco IOS XE devices were central to Salt Typhoon's campaign, though official and industry reporting confirms that other exposed edge technologies and management services were also involved (CISA et al., 2025; DiMolfetta, 2025).

At the protocol level, the campaign focused on the systems administrators use to control critical infrastructure. TACACS+ and SSH were primary targets because compromising them meant compromising the people managing the network, not just the devices themselves (CISA et al., 2025). GRE served a different purpose: rather than being exploited as a vulnerability, it was weaponized as a persistence mechanism, allowing attackers to blend their own tunneled traffic into what appeared to be normal network operations (CISA et al., 2025). Perhaps most concerning was Salt Typhoon's reported access to lawful intercept systems maintained under the Communications Assistance for Law Enforcement Act (CALEA) — infrastructure designed to support government surveillance that, once compromised, could expose the targets and methods of active domestic investigations (DiMolfetta, 2025).

Societal Impact

The Salt Typhoon campaign had serious effects, targeting systems that handle everyday communication. Public reports confirm that several major U.S. telecommunications providers were compromised, raising the risk that communications of businesses, government officials, and ordinary users could be exposed to foreign intelligence (DiMolfetta, 2025; CISA et al., 2025). The situation became more troubling when Salt Typhoon reportedly accessed lawful intercept systems. If foreign intelligence learns who is under surveillance and how investigations are conducted, the risk extends well beyond data theft — ongoing operations and the identities of sources, targets, and detection methods could all be exposed (DiMolfetta, 2025).

The damage was not limited to commercial networks either. A 2025 Department of Homeland Security memo revealed that a state Army National Guard network was severely compromised, exposing administrative credentials and network diagrams (Riotta, 2025). By early 2026, the same group was linked to breaches of congressional staff email systems supporting national security committees — confirming that Salt Typhoon's ambitions spanned military, legislative, and intelligence environments, not just private industry (Riotta, 2026).

Proposed Solutions

Patch Management and Hardening

Timely patching is the first and best defense against this type of malicious campaign. Cisco had already released fixes for CVE-2023-20198 and CVE-2023-20273, and other exploited vulnerabilities had also been patched long before many victims responded (Eclypsium, 2025; DiMolfetta, 2025). Caveza's analysis shows that organizations kept systems exposed and

unpatched for years after fixes were available, especially for ProxyLogon, a set of vulnerabilities in Microsoft Exchange email servers (Caveza, 2025). Unpatched, internet-facing devices become long-term entry points for advanced threat actors and should be treated as a critical remediation priority.

Patching alone is not enough if the device configuration remains weak. Cisco Talos recommended key hardening steps after the campaign: disable Smart Install where not needed, switch Telnet to SSH for all management sessions, restrict Guest Shell access, and turn off unencrypted web services on exposed devices (Wright, 2025). CISA also advised locking down management interfaces to trusted internal IP ranges and building monitoring capabilities for TACACS+, SSH, SNMP, and GRE traffic (the protocols Salt Typhoon relied on most heavily) (CISA et al., 2025).

Segmentation and Visibility

Another major lesson from Salt Typhoon is that flat networks make lateral movement easier. If one compromised router can lead to stolen administrative credentials and broader network access, organizations must separate sensitive components from normal traffic. Management systems, authentication infrastructure, and lawful intercept environments should be segmented and protected with stricter access controls.

Visibility is the other half of the equation. Many victim organizations did not retain logs long enough or monitor relevant systems closely enough, allowing the intrusion to spread undetected (CISA et al., 2025). Centralized, tamper-resistant logging across routers, authentication systems, and management interfaces — capturing configuration changes, authentication events, and network telemetry — gives defenders the forensic foundation needed to detect and respond to

such campaigns. Proactive threat hunting for anomalous TACACS+ activity, unexpected GRE tunnel configurations, and unauthorized Guest Shell usage should be standard practice in any environment running Cisco infrastructure at scale (CISA et al., 2025).

Conclusion

Salt Typhoon shows how known telecom vulnerabilities can enable large-scale espionage. The attackers exploited well-documented flaws, abused legitimate networking features, stole administrative credentials, and operated for long periods in poorly monitored environments (Eclypsium, 2025; CISA et al., 2025; More, 2025; Caveza, 2025). The campaign's reach and patience were powerful, but the outcome hinged on preventable lapses in basic security.

Salt Typhoon is a clear warning of what can unfold when fundamental security disciplines are continually deprioritized across an entire industry. The path forward requires more than awareness — it demands structural change. Mandatory patching timelines, stronger federal cybersecurity standards for telecommunications carriers, and broader adoption of Zero Trust network architecture are all gaining urgency as a direct result of this campaign (DiMolfetta, 2025). Preventing recurrence demands accelerated patching, stronger device hardening, enforced network segmentation, and vigilant monitoring across every telecom and network-edge environment.

References

Caveza, S. (2025, January 23). Salt Typhoon: An analysis of vulnerabilities exploited by this state-sponsored actor. *Tenable*. https://www.tenable.com/blog/salt-typhoon-an-analysis-of-vulnerabilities-exploited-by-this-state-sponsored-actor

Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, & international partners. (2025, August 27). Countering Chinese state-sponsored actors' compromise of networks worldwide to feed global espionage system (Joint Cybersecurity Advisory AA25-239A). https://www.ic3.gov/CSA/2025/250827.pdf

Eclypsium. (2025, June 24). The Cisco vulnerability Salt Typhoon weaponized against Canadian telcos and Viasat. https://eclypsium.com/blog/cve-2023-20198-cisco-salt-typhoon-viasat-canadian-telcos

DiMolfetta, D. (2025, February 20). Salt Typhoon hackers exploited stolen credentials and a 7-year-old software flaw in Cisco systems. *Nextgov/FCW*. https://www.nextgov.com/cybersecurity/2025/02/salt-typhoon-hackers-exploited-stolen-credentials-and-7-year-old-software-flaw-cisco-systems/403146/

More, A. (2025, February 21). Talos: No Cisco zero days used in Salt Typhoon telecom hacks. BankInfoSecurity. https://www.bankinfosecurity.com/talos-no-cisco-zero-days-used-in-salt-typhoon-telecom-hacks-a-27576

Recorded Future Insikt Group. (2025). RedMike: Salt Typhoon cyber attack on Cisco devices in telecommunications. https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices

Riotta, C. (2025, July 17). Salt Typhoon hit National Guard network in 'extensive' hack. BankInfoSecurity. https://www.bankinfosecurity.com/salt-typhoon-hit-national-guard-network-in-extensive-hack-a-28999

Riotta, C. (2026, January 9). Salt Typhoon hackers hit congressional emails in new breach. BankInfoSecurity. https://www.bankinfosecurity.com/salt-typhoon-hackers-hit-congressional-emails-in-new-breach-a-30484

U.S. Department of the Treasury. (2025, January 17). Treasury sanctions company associated with Salt Typhoon and hacker associated with Treasury compromise. https://home.treasury.gov/news/press-releases/jy2792

Wright, R. (2025, February 21). Cisco: Salt Typhoon used new custom malware in telecom attacks. *Cybersecurity Dive.* https://www.cybersecuritydive.com/news/cisco-salt-typhoon-used-new-custom-malware-in-telecom-attacks/740629

Appendix A
Salt Typhoon Six-Stage Attack Sequence

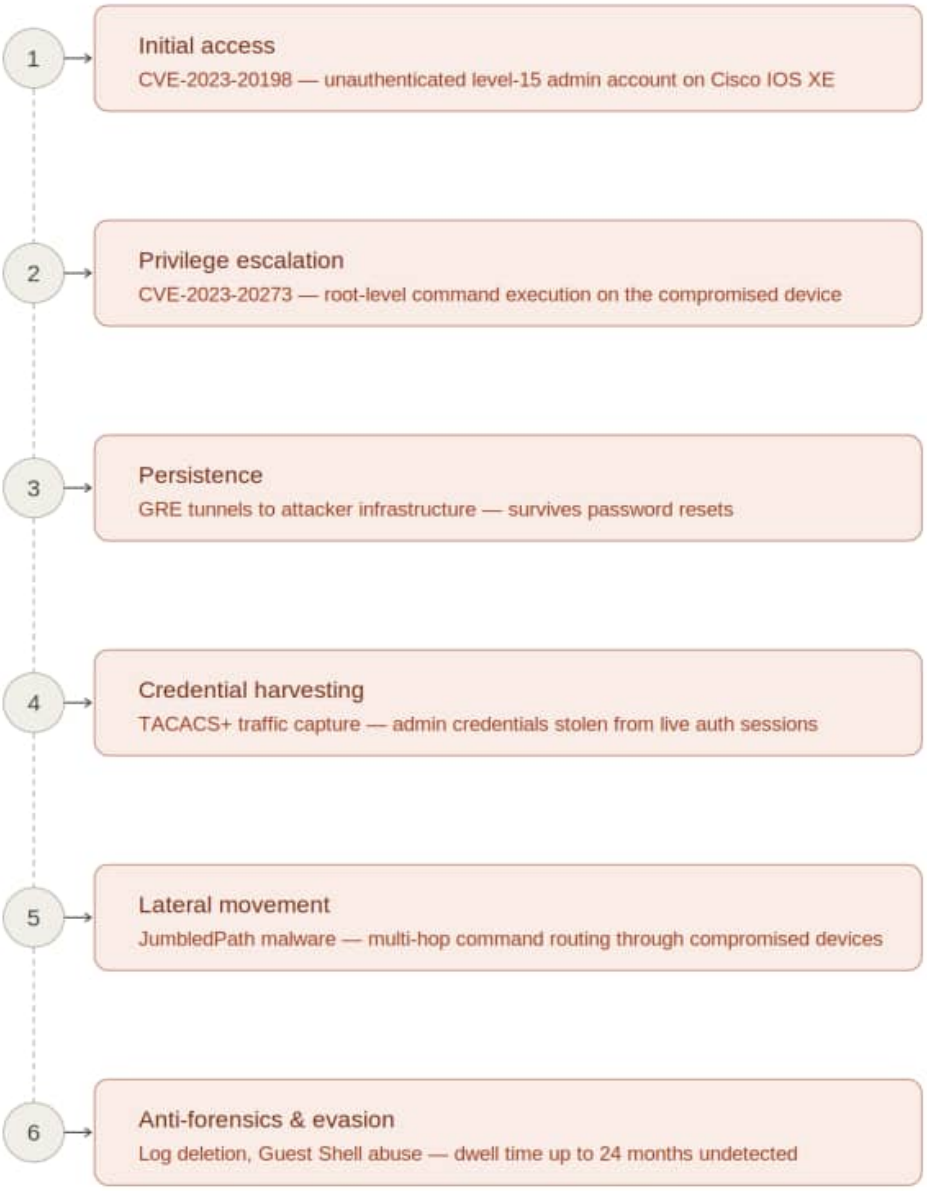

Figure 1. Salt Typhoon six-stage attack sequence (Eclypsium, 2025; CISA et al., 2025; Cybersecurity Dive, 2025)

Figure 1. Salt Typhoon six-stage attack sequence

(Eclypsium, 2025; CISA et al., 2025; Wright, 2025)