What Should the US Do About Salt Typhoon?

By Alexander Culafi

Published: 2025-04-10 · Archived: 2026-04-05 13:22:15 UTC

Source: Daniren via Alamy Stock Photo

Of the countless threat actors, state-sponsored and otherwise, that target the US private and public sectors, few have gained the wide cultural relevance of Salt Typhoon, the Chinese state-sponsored threat actor that has targeted major telecommunications providers in a far-reaching, ongoing espionage campaign.

Discovered last fall, Salt Typhoon has hacked into telecom giants in the US and abroad — including Verizon, AT&T, Lumen Technologies, and others — in a successful effort to access the "lawful intercept" systems law enforcement agencies use for court-authorized wiretapping. In its apparently months-long campaign, Salt Typhoon accessed sensitive data belonging to the Republican and Democratic 2024 presidential campaigns as well as that of other politicians.

Salt Typhoon's activities have continued into the new year and around the world. Although Chinese state-backed espionage against the US is well-established, the telecom-focused attacks reported last fall are a high-profile reminder of how these activities are escalating. The question is, What can the US do about it?

Related:Not Toying Around: Hasbro Attack May Take 'Weeks' to Remediate

Salt Typhoon: Truly an Advanced Threat

CrowdStrike's recent 2025 "Global Threat Report" said China state-backed hacking has reached an "inflection point" and noted a 150% increase in China-nexus activity across all sectors. Beyond espionage, the Chinese government has also shown an interest in pre-positioning itself in critical environments to prepare for possible escalation with adversaries.

Aaron Shraberg, senior intelligence analyst at Flashpoint, tells Dark Reading that on top of aforementioned espionage and pre-positioning activities, the group utilizes a number of sophisticated tactics.

"Salt Typhoon has demonstrated stealth and persistence, meaning it is difficult to identify the threat on networks," Shraberg says. "The group has demonstrated proficiency in various tactics, techniques, and procedures (TTPs), like living off the land (LoTL), to use legitimate tools and blend in with network traffic to avoid discovery."

On April 2, the House Committee on Government Reform dedicated a hearing to Salt Typhoon. During the hearing, state representative and committee chairman William Timmons (R-SC) asked Edward Amoroso, research professor at New York University, whether the US should retaliate for the Salt Typhoon attacks and what kind of response would be justified.

Amoroso did not advocate for "hacking back" (the popular colloquial term for retaliatory offensive cyber activity), instead saying the US should see it as a wake-up call for the country to shore up its defenses and pull together. He said the idea of hacking back "shirks the responsibility" to look inward.

Related:Bank Trojan 'Casbaneiro' Worms Through Latin America

Dark Reading asked four security experts about the US's options for responding to Salt Typhoon, as well as how defenders should protect themselves against APT threats.

The Threat of Salt Typhoon

Asked how much of a threat Salt Typhoon's malicious activities pose to the United States, experts Dark Reading spoke with broadly attested to their significance.

Bobby Kuzma, director of offensive cyber operations at penetration testing and incident response firm ProCircular, says the activity Salt Typhoon engaged in was "pretty bad," noting the reach granted by leveraging the lawful intercept capabilities built into domestic telecommunications providers.

"For every phone company and ISP (not that there’s much of a difference anymore) they have access to, they can intercept everything travelling over the network, including encrypted communications," Kuzma says. "They might not be able to read the content of those communications, but they can certainly look at patterns in who is talking to whom and make educated guesses."

Dave Merkel, co-founder and CEO of managed security services vendor Expel, says it was a huge deal but, notably, nothing new. "China actively goes after US private sector organizations for a number of reasons, relating to counterintelligence, IP theft, you name it," he says.

Related:AI-Powered 'DeepLoad' Malware Steals Credentials, Evades Detection

And to Merkel's point, China's cyber efforts are more or less institutionalized by this point. CrowdStrike, for example, regularly discusses how China's Five-Year Plans should be interpreted from a cyber-focused lens.

This activity doesn't seem to be slowing down. Austin Berglas, global head of professional services at security vendor BlueVoyant as well as former head of cyber for the FBI in New York, says as much.

"Chinese state-sponsored attacks against United States critical infrastructure will continue to occur," Berglas says. "China has been embedding themselves in networks and exploiting supply chains for the purpose of conducting massive data collection activities for years. This is nothing new to the intelligence community."

He continues, "The fact that China is already embedded in US infrastructure is a massive concern. Traditional goals such as intellectual property theft and large-scale intelligence collection pales in comparison to the potential for disruption or takeover of critical services."

US Government Options for Response

Kuzma names "strongly worded diplospeak," expelling members of diplomatic delegations, criminal charges against individual foreign citizens, and sanctions against organizations (which has happened already). "All these are so-called proportionate responses," he says. "It gets scarier from there."

Alon Termin, red team expert at exposure management firm CYE, approached the question of possible responses from a more cyber-focused angle. Namely, shoring up defenses and imposing stronger regulations.

"The US can respond with defensive cyber operations to detect, deter, and neutralize threats," Termin says. "Implementing stricter cybersecurity regulations for critical infrastructure sectors could also help prevent such intrusions."

The FCC proposed regulations last fall requiring communication providers to annually certify, update, and implement cybersecurity risk management plans.

How Should the US Respond to Salt Typhoon?

Similarly to Amoroso's answer during the April 2 House Committee on Government Reform hearing, sources broadly responded to the question of what the US government should do by calling for better security hygiene in its most critical institutions. Here's what they said:

- Austin Berglas, BlueVoyant: Our response should be to finally get our own house in order so that we can properly protect the homeland. Private corporations need to learn lessons from failures within the US government. Permitting sensitive and business-related conversations to be conducted on platforms outside of corporate approved networks and devices will only cause problems, and policies and procedures are only useful if enforced and followed. The FCC recently proposed to strengthen rules for telecom providers to secure their environment. This guidance is nothing without action and adoption. Lastly, our adversaries do not need to deploy sophisticated, zero-day exploits to have success. They are capitalizing on patchable, previously identified vulnerabilities. Basic hygiene calls for continuous and complete visibility across your network and monitoring of your most critical supply chain relationships.

- Alon Termin, CYE: The best way to respond is by investing in advanced cybersecurity technologies and practices to protect critical systems.
- Anne An, principal threat intelligence analyst, Trellix: I'd hope that the US government will prioritize the development and deployment of more secure edge devices, such as phones, laptops, and other IoT [Internet of Things] hardware, which are becoming an increasing point of vulnerability. They are often the first line of defense in a network, and as they are more widely used, they become targets for APTs.
- Bobby Kuzma, ProCircular: The US has already exerted pressure on China to make its displeasure known, through sanctions and individual criminal charges against MSS officers linked to the attacks. Another consideration that is on the table, but probably won’t be acted on, is allowing telecom organizations to shut down or remove the lawful intercept capability that acts as an effective backdoor into their infrastructure. There needs to be a balance between convenience to law enforcement for surveillance and having massive backdoors that allow for this exploitation.

Defender Takeaways From Salt Typhoon

Although state-backed espionage may not be something every organization feels it has to worry about, the best practices for defending against an APT are generally good advice, no matter who you are.

Expel's Merkel advises enforcing good cyber hygiene, such as patching quickly, supporting multifactor authentication, and maintaining good asset inventories. He calls this the "bare minimum," and suggests taking a defense-in-depth approach to security and prioritizing strong detection and response.

Flashpoint's Shraberg, meanwhile, calls for enterprises to adopt a "proactive and layered security approach drawing on public and private sector resources and expertise."

"There are many ways to address the multifaced nature of sophisticated threat actors. Technical defenses are very important and should be combined with a level of education of individuals to learn how to do their part to fend off attacks from things like phishing and social engineering, especially as AI tools now find their way into attackers' toolboxes," Shraberg says. "Given the potential for supply chain compromises highlighted with other Chinese APT groups, enterprises should also assess and manage the security risks associated with their vendors and partners, such as those involving networking equipment like routers."

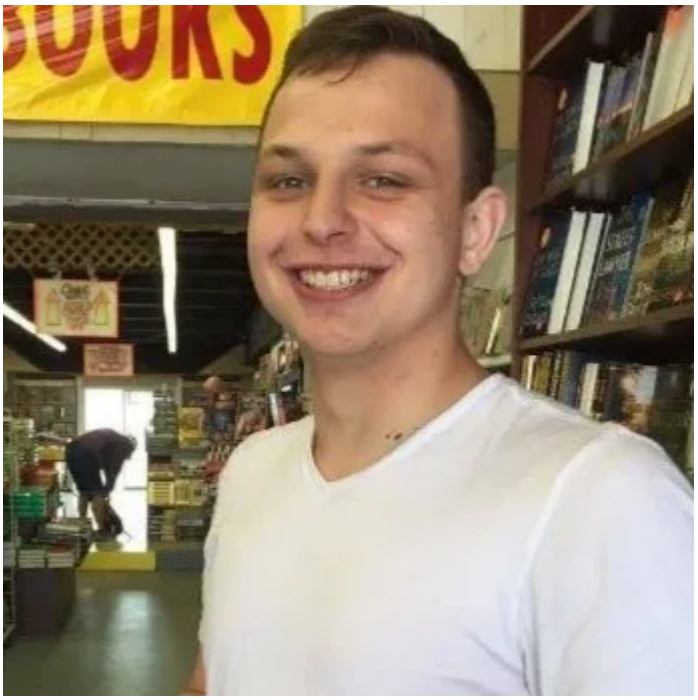
An says that as Salt Typhoon typically uses otherwise legitimate tools like PowerShell and WMI, organizations should monitor for unusual or suspicious activity associated with living off the land, as well as compromised accounts.

"One of the group's most common tactics is to use legitimate credentials and move laterally within the network, so organizations should follow strong monitoring practices to detect and respond to compromised accounts as quickly as possible," An says. "They can do this by implementing and enforcing multifactor authentication, conducting frequent audits, and regularly analyzing login behavior for any signs of irregular activity."

Organizations should also patch public-facing services, VPNs, and legacy systems — common entry points for attackers.

Though a common impulse for the US right now to handle China from a place of escalation and retaliation, Dark Reading sources uniformly do not propose doing something similar on the cyber front. Instead, as Amoroso put it at last week's House committee hearing, "The best defense is a good defense."

About the Author



Senior News Writer, Dark Reading

Alex is an award-winning writer, journalist, and podcast host based in Boston. After cutting his teeth writing for independent gaming publications as a teenager, he graduated from Emerson College in 2016 with a Bachelor of Science in journalism. He has previously been published on VentureFizz, Search Security, Nintendo World Report, and elsewhere. In his spare time, Alex hosts the weekly Nintendo podcast Talk Nintendo Podcast and works on personal writing projects, including two previously self-published science fiction novels.
