Salt Typhoon, the Chinese Telecom Hack: What's Next?

Salt Typhoon, the Chinese Telecom Hack: What's Next?

Cybersecurity 2025 began with the dramatic breaking news of the Chinese Telecom Hack. Although what has been called the Salt Typhoon attack made headlines around the globe, the issue in fact has a complicated history that has been gaining momentum for some time, as we reported in a previous newsletter (CYRIN Newsletter, February 2024 (../cybersecurity-volt-typhoon-and-the-grid/)).

In December 2024, Federal cyber officials held a news briefing stating that Chinese hackers had launched large-scale attacks on several major United States telecom firms including AT&T, Verizon and T-Mobile. The FBI began investigating the “Salt Typhoon” attack in late spring, so the issue had been building for some time. The breach of the cellular data of thousands (possibly millions) of Americans was disclosed by *Politico* (https://www.politico.com/news/2024/11/06/chinese-hackers-american-cell-phones-00187873) in November (other major publications such as *The Wall Street Journal* and *The New York Times* had much of the story in September and October, respectively), and was far from a small scale attack. In addition, early reports indicate that no one really knows how long the attackers have been in the systems and the scope of what they have been doing. According to Cybersecurity Dive (https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576/), Federal officials said at the media briefing in early December that the attacks were “widespread and actively evolving and that officials still don’t know the full extent of damages caused by the global espionage campaign or what remains at risk.”

Unfortunately, there are no official reports indicating how or if the attacks were successful or in what way; if malware was installed; or what information the hackers were seeking and for what purpose. Cybersecurity Dive (https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576/) reports that authorities have confirmed that the group poses a “persistent threat,” and speculated again that “malicious activity is ongoing.” In terms of future risk, Jeff Greene from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) noted that it’s not yet known if the hackers have been completely ejected from the networks, and “we still don’t know the scope of what they’re doing.” In November the FBI and CISA issued a joint statement (https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure) into the ongoing investigation into the hack orchestrated by the People’s Republic of China (PRC) hack and revealed that it was “broad and significant.”

Although CISA, the FBI, the National Security Agency and cyber authorities in Australia, Canada and New Zealand are still in the information gathering stage, and as of this writing have not released any official or definitive information, there has been hardening guidance (https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure) designed to help telecom providers moving forward as details reveal themselves.

This sophisticated hack has raised the alarm as one of the largest in US history. In addition, the United States, Australia, Canada and New Zealand claim it is part of an intelligence operation (https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure) conducted by “PRC affiliated threat actors.” Salt Typhoon has also attacked state entities in Southeast Asia since August of 2024. All in all, Salt Typhoon (https://therecord.media/china-salt-typhoon-targets-southeast-asia-telecom) is considered “one of the most aggressive Chinese state hacker groups.”

Cybersecurity doesn't always make the primetime nightly news, but due to the severity of the event, all the major television networks picked up the story. Homeland Security Secretary Alejandro Mayorkas admitted that the hack is a "very, very serious matter (https://www.nbcnews.com/politics/national-security/vast-chinese-hack-eight-us-telecoms-firms-still-going-official-says-rcna181319)," and "a very sophisticated hack" that was no doubt escalating for some time, with implications for intelligence being particularly alarming.

This breach targeted close to home. According to their representatives the FBI informed the presidential campaigns of Donald Trump and Kamala Harris in October that they were targeted as well as the office of Senate Majority Leader Chuck Schumer, D-N.Y.

As reported by PBS (https://www.pbs.org/newshour/show/chinese-hackers-have-infiltrated-at-least-8-u-s-telecom-companies-white-house-says), Chinese hackers had infiltrated at least eight communications firms in the United States and over the last one to two years — quote — "dozens" of telecommunications companies across Asia and Europe, and the hack was ongoing, according to Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger.

Why does this matter?

The eight targeted US telecommunications firms are not the only ones struggling to defend their networks. Advanced Persistent Threats (APTs) possibly linked to Salt Typhoon have compromised telecommunications firms (https://www.trendmicro.com/en_us/research/24/k/earth-estries.html) in the Asia-Pacific (APAC) and the Middle East and North Africa (MENA) regions as well. In 2022, a Chinese APT group (https://www.darkreading.com/cyberattacks-data-breaches/governments-telcos-chinas-hacking-typhoons) called Daggerfly and Evasive Panda hacked systems at a telecommunications organization in Africa. Experts speculate that telecommunications networks are strategic targets for malicious actors, in part, as they can kickstart a geopolitical strategy. China's infiltration of worldwide networks may be part of such a strategy to destabilize and gather sensitive information about a country's citizens.

Dark Reading (https://www.darkreading.com/cyberattacks-data-breaches/governments-telcos-chinas-hacking-typhoons) speculates that the Salt Typhoon attacks may lead to one positive outcome: encouraging citizens and governments to use encryption more widely. It's certainly true that telecommunications providers – private and state-owned – require more robust security. "The global attacks on telecommunications technology demonstrate that even nations with well-considered, strict privacy laws are not safe havens," says Gregory Nojeim, senior counsel and director of the security and surveillance project at the Center for Democracy and Technology, a digital-rights group.

Next steps

Clearly, the large scale and sophisticated Salt Typhoon attack is of critical and ongoing concern to US officials; this is further complicated by the ongoing tensions between Washington and Beijing over cyber-espionage and other high-stakes national security issues.

The United States continues to be in conversation with House and Senate intelligence committees, and cybersecurity teams. Cybersecurity experts (https://www.cnn.com/2024/10/05/politics/chinese-hackers-us-telecoms/index.html) from Microsoft and Google-owned firm Mandiant are also assisting the investigation into the hack. People probing the attacks have been impressed by the skill, persistence and ability of Salt Typhoon hackers to imbed in computer networks.

CYRIN can help

Training or lack of has consequences. According to some estimates (https://securityintelligence.com/articles/ai-reduces-data-breach-lifecycles-and-costs/), organizations can significantly reduce the cost of a breach by an average of $232,867 through cybersecurity training for their employees.

CYRIN can help on several fronts. For the education market, we consistently work with colleges and universities both large and small to create realistic training to meet the environment students will encounter when they graduate and enter the workforce.

For industry we continue to work with our partners to address major challenges including incident response, ransomware, and phishing and set up realistic scenarios that allow them to train their teams and prepare new hires for the threats they will face. Government agencies have been using CYRIN for years, training their front-line specialists on the real threats faced on their ever-expanding risk surface.

A full-blown cyberattack is not something you can prepare for after it hits. The best time to plan and prepare is before the attack.

Our training platform teaches fundamental solutions that integrate actual cyber tools from CYRIN’s labs that allow you to practice 24/7, in the cloud, no special software required. Cyber is a team effort; to see what our team can do for you take a look at our course catalog (https://cyrin.atcorp.com/catalog/), or better yet, contact us for further information and your personalized demonstration of CYRIN. Take a test drive and see for yourself!

< Read other CYRIN Newsletters (..)

Contact Us for details or to Set Up a CYRIN Demo
+1-800-850-2170 (tel:+1-800-850-2170) • sales@cyrintraining.com

Watch CYRIN: The Next-Generation Cyber Range (https://youtu.be/smokjaL2aCw)

Learn More About How CYRIN Online Training Can Benefit You (https://cyrin.atcorp.com/)

Follow what we're up to:

(https://www.facebook.com/ArchitectureTechnologyCorporation/)

(https://x.com/JobsATC)

(https://www.linkedin.com/company/architecture-technology-corporation)

(https://www.youtube.com/@atcorp)

About ATCorp (/about/)

Our Story (/about/our-story/)
Publications (/about/publications/)
Patents (/about/patents/)
Careers (/about/careers/)
Contact Us (/about/contact/)
Search (/search/)

Products (/products/)

CYRIN Cyber Range (/products/cyrin/)
CRR-1000 Tactical Router (/products/crr-1000/)

R&D (/r-and-d/)

Trestle Framework (/r-and-d/trestle/)
USB Sentry (/r-and-d/usbsentry/)
Advanced Routers (/r-and-d/advanced-routers/)

Engineering Services (/services/)

Air Transportation Systems Engineering (/services/air-transportation-systems-engr/)
Bandwidth Optimized Collaboration (/services/bandwidth-optimized-collaboration/)
Custom Code Profiling Solutions (/services/custom-code-profiling/)