FBI seeks help to unmask Salt Typhoon hackers behind telecom breaches

By Sergiu Gatlan

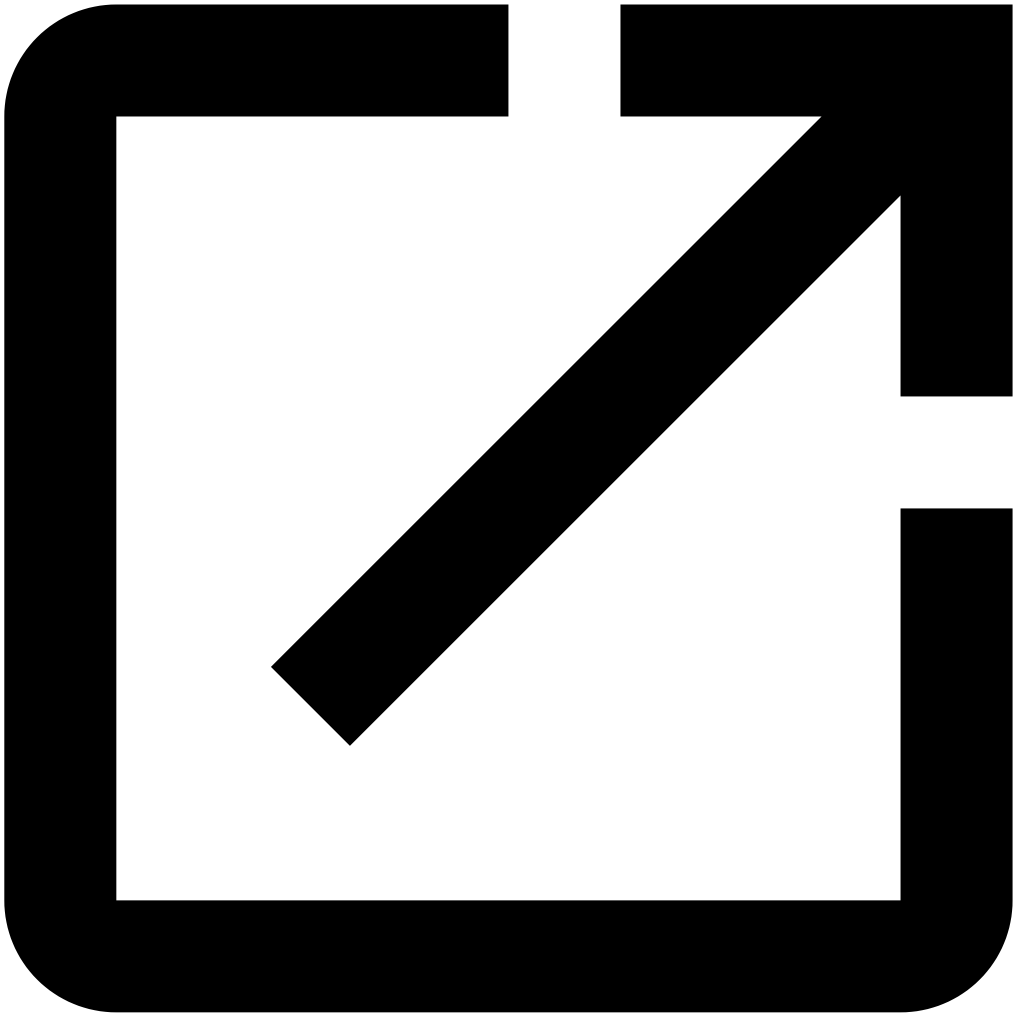
Published: 2025-04-25 · Archived: 2026-04-05 14:08:44 UTC

The FBI has asked the public for information on Chinese Salt Typhoon hackers behind widespread breaches of telecommunications providers in the United States and worldwide.

In October, the FBI and CISA confirmed that the Chinese state hackers had breached multiple telecom providers (including AT&T, Verizon, Lumen, Charter Communications, Consolidated Communications, and Windstream) and many other telecom companies in dozens of countries.

As revealed at the time, while they had access to the U.S. telecoms' networks, the attackers also accessed the U.S. law enforcement's wiretapping platform and gained access to the "private communications" of a "limited number" of U.S. government officials.


DIE LINKE.
0:00



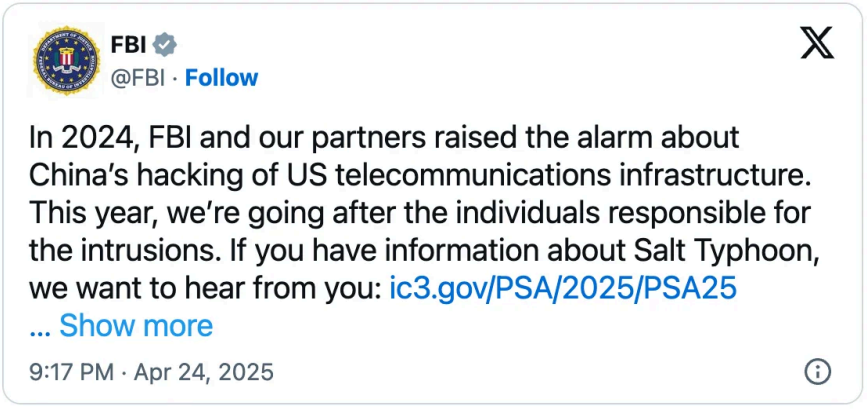
On Thursday, the FBI issued a public service announcement seeking tips that could help identify and locate the Salt Typhoon hackers who targeted US telecommunications infrastructure.

"Investigation into these actors and their activity revealed a broad and significant cyber campaign to leverage access into these networks to target victims on a global scale. This activity resulted in the theft of call data logs, a limited number of private communications involving identified victims, and the copying of select information subject to court-ordered US law enforcement requests," the FBI said.

"FBI maintains its commitment to protecting the US telecommunications sector and the individuals and organizations targeted by Salt Typhoon by identifying, mitigating, and disrupting Salt Typhoon's malicious cyber activity. If you have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you."

In January, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions against Sichuan Juxinhe Network Technology, a Chinese cybersecurity firm believed to be directly involved in the Salt Typhoon telecom breaches.

The FBI also reminded that the U.S. Department of State is offering a reward of up to $10 million through its Rewards for Justice (RFJ) program for information about government-linked foreign hackers linked to malicious cyber activities against U.S. critical infrastructure.



More Salt Typhoon telecom breaches

China's Salt Typhoon Chinese cyber-espionage group (also tracked as Ghost Emperor, FamousSparrow, Earth Estries, and UNC2286) has been breaching government entities and telecom companies since at least 2019.

In recent months, it was also uncovered that this state-backed hacking group is still actively targeting telecoms. Between December 2024 and January 2025, it breached more telecommunications companies worldwide by exploiting privilege escalation and Web UI command injection vulnerabilities in unpatched Cisco IOS XE network devices.

These additional breaches include a U.S. internet service provider (ISP), a U.S.-based affiliate of a U.K. telecommunications provider, an Italian ISP, a South African telecom provider, and a large Thai telecommunications provider.

Cisco has also revealed that the Chinese hackers use a custom JumbledPath malicious tool to stealthily monitor network traffic and likely capture sensitive data from compromised U.S. telecommunication providers' networks.

In response to these breaches, U.S. authorities are considering banning TP-Link routers if an ongoing investigation finds their use in cyberattacks poses a national security risk. They are also reportedly planning to ban China Telecom's last active operations in the United States.
