Chinese hackers also breached Charter and Windstream networks

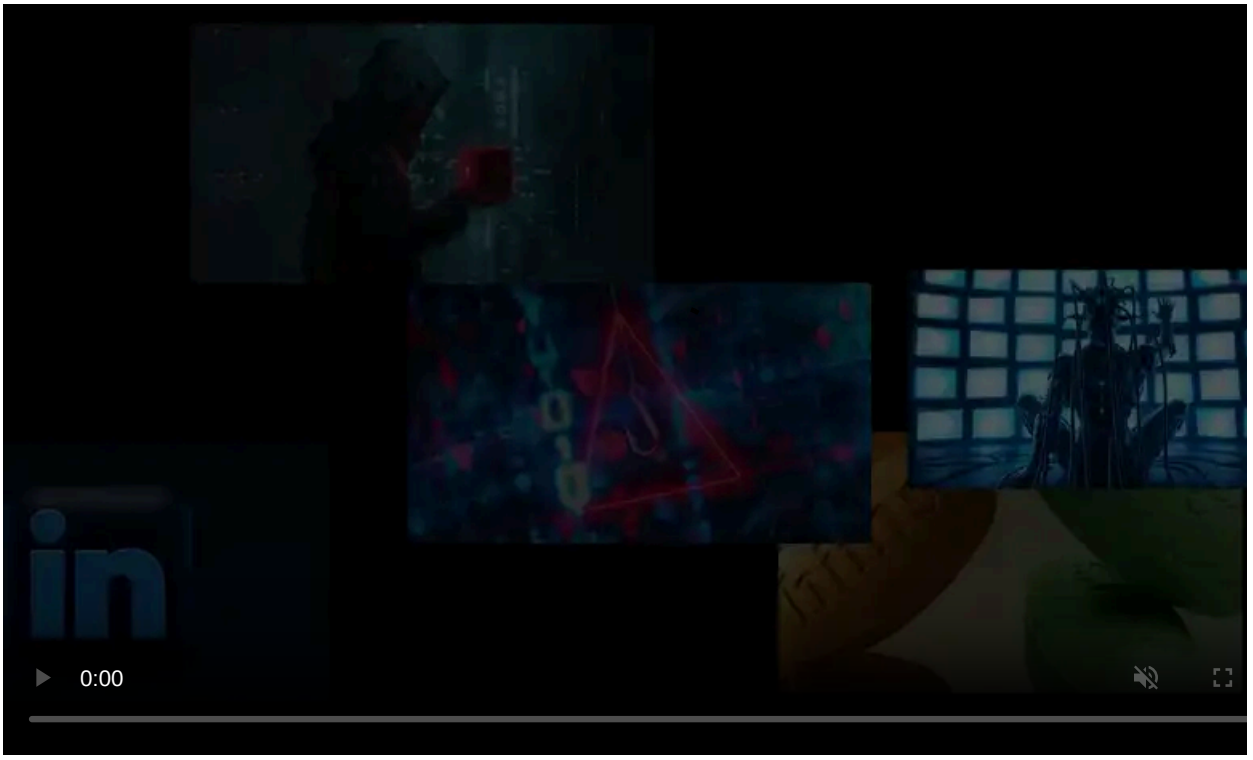
By Sergiu Gatlan

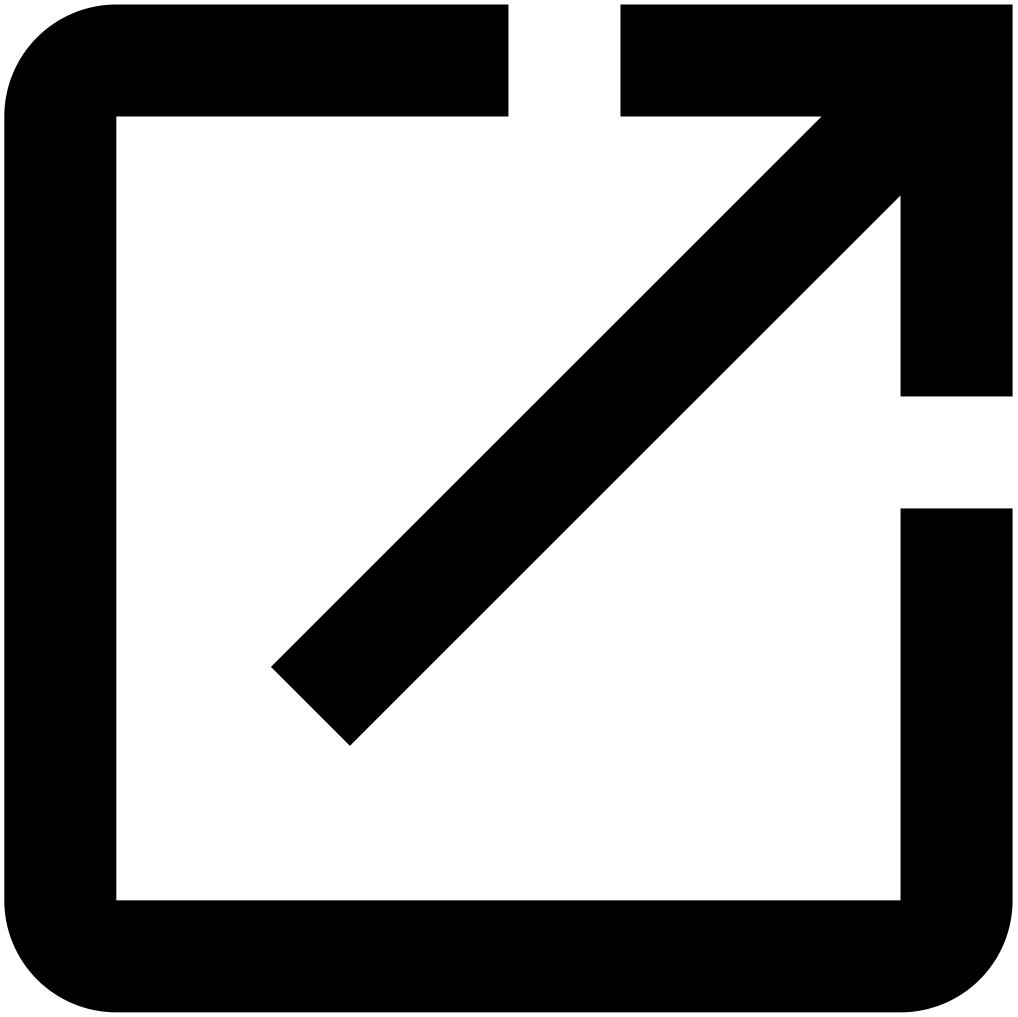
Published: 2025-01-06 · Archived: 2026-04-05 16:34:56 UTC

More U.S. companies have been added to the list of telecommunications firms hacked in a wave of breaches by a Chinese state-backed threat group tracked as Salt Typhoon.

This comes after AT&T, Verizon, and Lumen confirmed on December 30 that they have evicted the hackers from their networks. After breaching their networks, the Salt Typhoon hackers gained access to targeted individuals' text messages, voicemails, and phone calls, as well as wiretap information of those investigated by U.S. law enforcement.

T-Mobile also disclosed in November that unknown attackers compromised some of its routers in a network reconnaissance attempt after connecting from a linked wireline provider's network. However, the company's Chief Security Officer, Jeff Simon, didn't link the hack to Salt Typhoon and said the carrier's cyber defenses stopped the attack.


0:00



Visit Advertiser websiteGO TO PAGE

Over the weekend, sources familiar with the matter told the Wall Street Journal that the Chinese hackers have also breached the systems of Charter Communications, Consolidated Communications, and Windstream.

When BleepingComputer reached out earlier today to ask for confirmation, Windstream, Charter, and Consolidated Communications declined to comment.

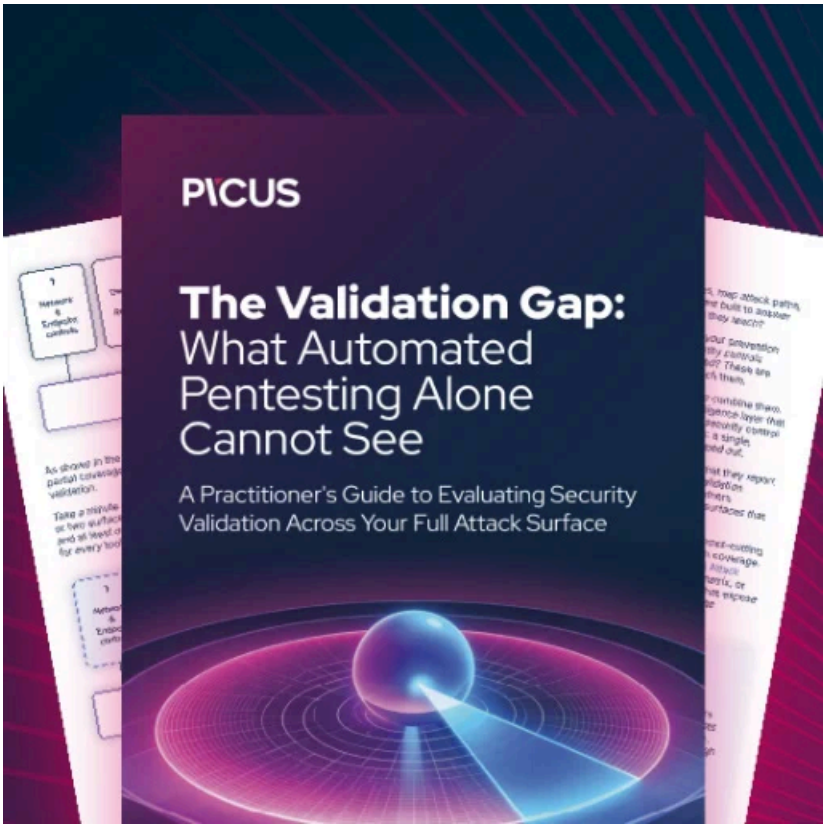
While Anne Neuberger, the White House's deputy national security adviser for cyber and emerging technologies, told reporters on December 27 that the Chinese hackers breached nine U.S. telecoms, it's unknown whether these three carriers are among them or add to the list. Neuberger also said in an early December press briefing that Salt Typhoon had breached telecom companies in dozens of other countries.

Following this wave of telecom breaches that have impacted numerous countries, CISA has advised senior government officials to switch to end-to-end encrypted messaging apps like Signal to mitigate communication interception risks. Additionally, the cybersecurity agency has released guidance to assist telecom administrators and engineers in strengthening their systems against Salt Typhoon attacks.

U.S. Senator Ron Wyden of Oregon also announced a new bill to secure the infrastructure of American telecoms, while FCC Chairwoman Jessica Rosenworcel said the agency would act "urgently" to ensure that U.S. carriers are required to secure their networks against cyberattacks.

In response to these telecom hacks, the U.S. government reportedly plans to ban China Telecom's last active operations in the United States. Additionally, U.S. authorities are considering banning TP-Link routers if ongoing investigations reveal that their use in cyberattacks poses a national security risk.

The Treasury Department also linked Chinese-sponsored hackers last week to a recent breach of the agency's Office of Foreign Assets Control (OFAC), which administers trade and economic sanctions programs, in what it described as a "major cybersecurity incident."



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/charter-and-windstream-among-nine-us-telecoms-hacked-by-china/