Chinese hackers breached T-Mobile's routers to scope out network

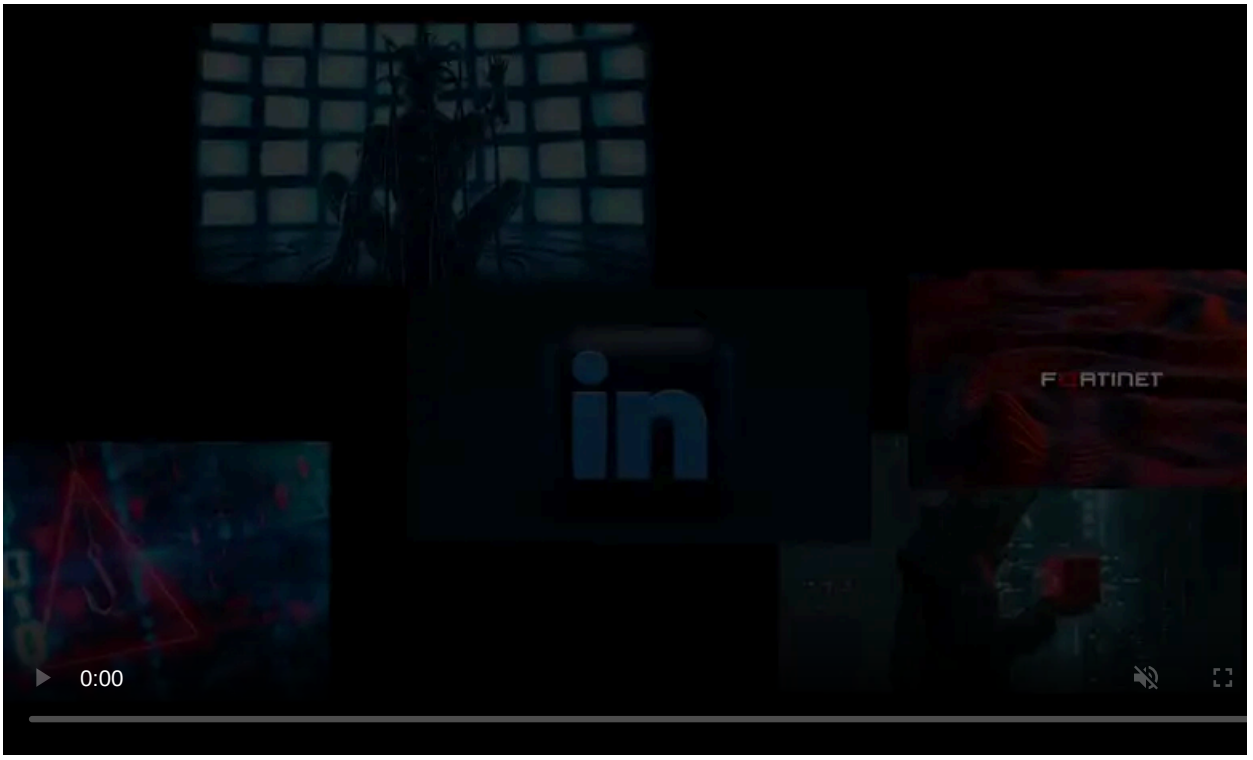
By Sergiu Gatlan

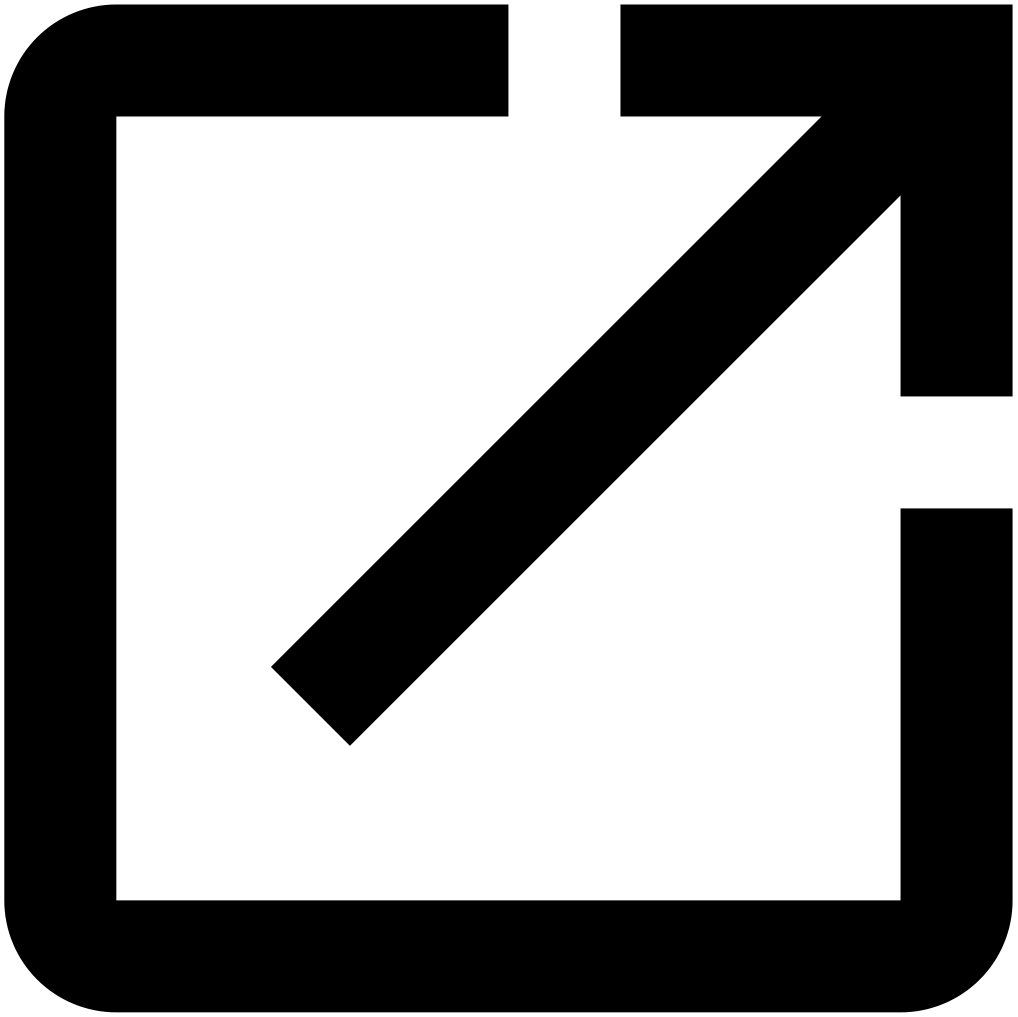
Published: 2024-11-27 · Archived: 2026-04-05 20:12:34 UTC

T-Mobile says the Chinese "Salt Typhoon" hackers who recently compromised its systems as part of a series of telecom breaches first hacked into some of its routers to explore ways to navigate laterally through the network.

However, the company says its engineers blocked the threat actors before they could spread further on the network and access customer information.

Also tracked as Earth Estries, FamousSparrow, Ghost Emperor, and UNC2286, this Chinese state-sponsored threat group has been active since at least 2019 and typically focuses on breaching government entities and telecommunications companies in Southeast Asia.


0:00



Jeff Simon, the company's Chief Security Officer, shared in a blog post published on Wednesday that the threat actors' attack—originating from a connected wireline provider's network—was stopped by T-Mobile's cyber defenses, including proactive monitoring and network segmentation.

The company discovered the breach after detecting suspicious behavior, including commands usually used in the reconnaissance stage of cyberattacks being run on some of its routers and commands matching indicators of compromise previously linked to Salt Typhoon, as Simon told Bloomberg.

"Many reports claim these bad actors have gained access to some providers' customer information over an extended period of time – phone calls, text messages, and other sensitive information, particularly from government officials. This is not the case at T-Mobil," Simon said.

"Our defenses protected our sensitive customer information, prevented any disruption of our services, and stopped the attack from advancing. Bad actors had no access to sensitive customer data (including calls, voicemails, or texts).

"We quickly severed connectivity to the provider's network as we believe it was – and may still be – compromised."

T-Mobile's CSO added that the company no longer sees any attackers active within its network and has shared its findings with the government and industry partners.

Breached in recent Salt Typhoon telecom attacks

T-Mobile's statement from today follows the company's announcement two weeks ago that its systems were compromised in a recent wave of Salt Typhoon telecom breaches.

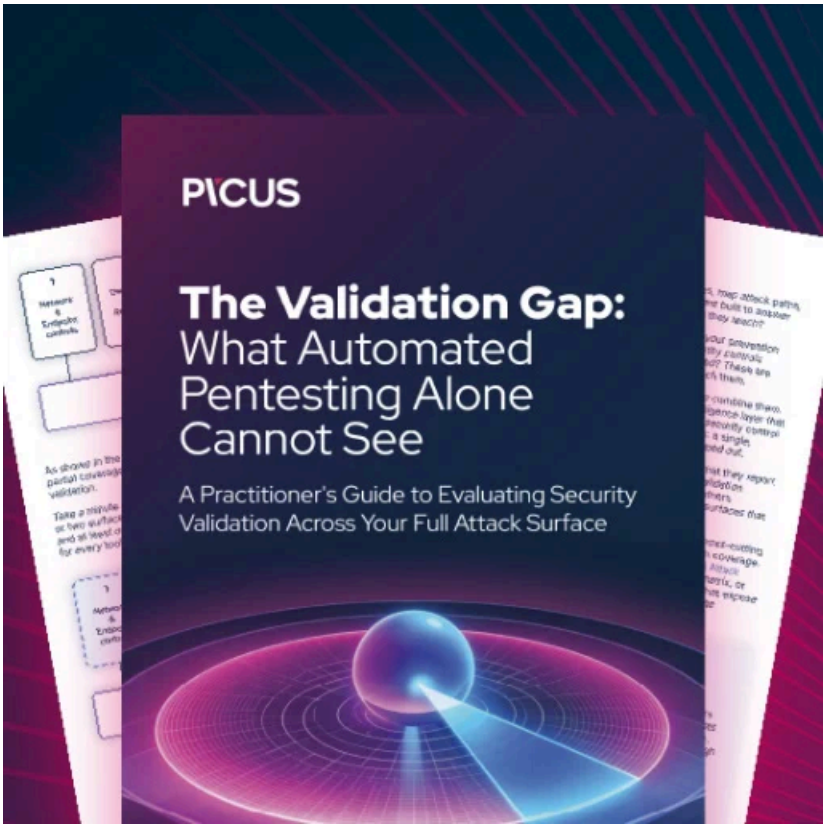
CISA and the FBI confirmed the breaches in late October following reports that the Chinese threat group breached multiple broadband providers, including AT&T, Verizon, and Lumen Technologies.

The two federal agencies later revealed that the attackers compromised the "private communications" of a "limited number" of government officials, stole customer call records and law enforcement request data, and gained access to the U.S. government's wiretapping platform.

Even though it's unknown when the telecom giants' networks were first breached, the Chinese hackers had access "for months or longer," according to a WSJ report. This allowed them to collect and steal vast amounts of "internet traffic from internet service providers that count businesses large and small, and millions of Americans, as their customers," according to people familiar with the matter.

Canada also revealed last month that many of the country's agencies and departments, including federal political parties, the Senate, and the House of Commons, were targeted in broad network scans linked to unnamed Chinese state hackers.

In similar, although likely unrelated attacks, the Volt Typhoon Chinese threat group tracked and hacked multiple ISPs and MSPs in the United States and India after hacking their corporate networks using credentials stolen by in Versa Director zero-day attacks.



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/chinese-hackers-breached-t-mobiles-routers-to-scope-out-network/