# Telecom giant Viasat breached by China's Salt Typhoon hackers

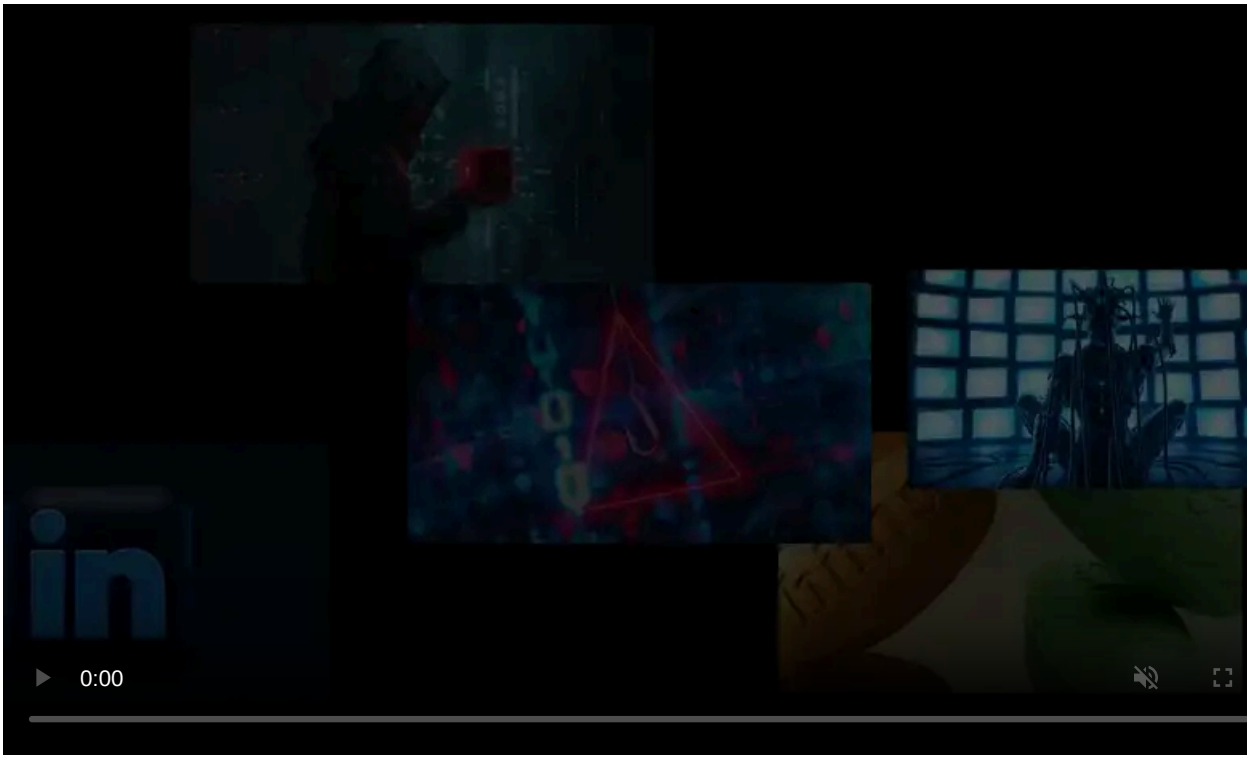
By Sergiu Gatlan

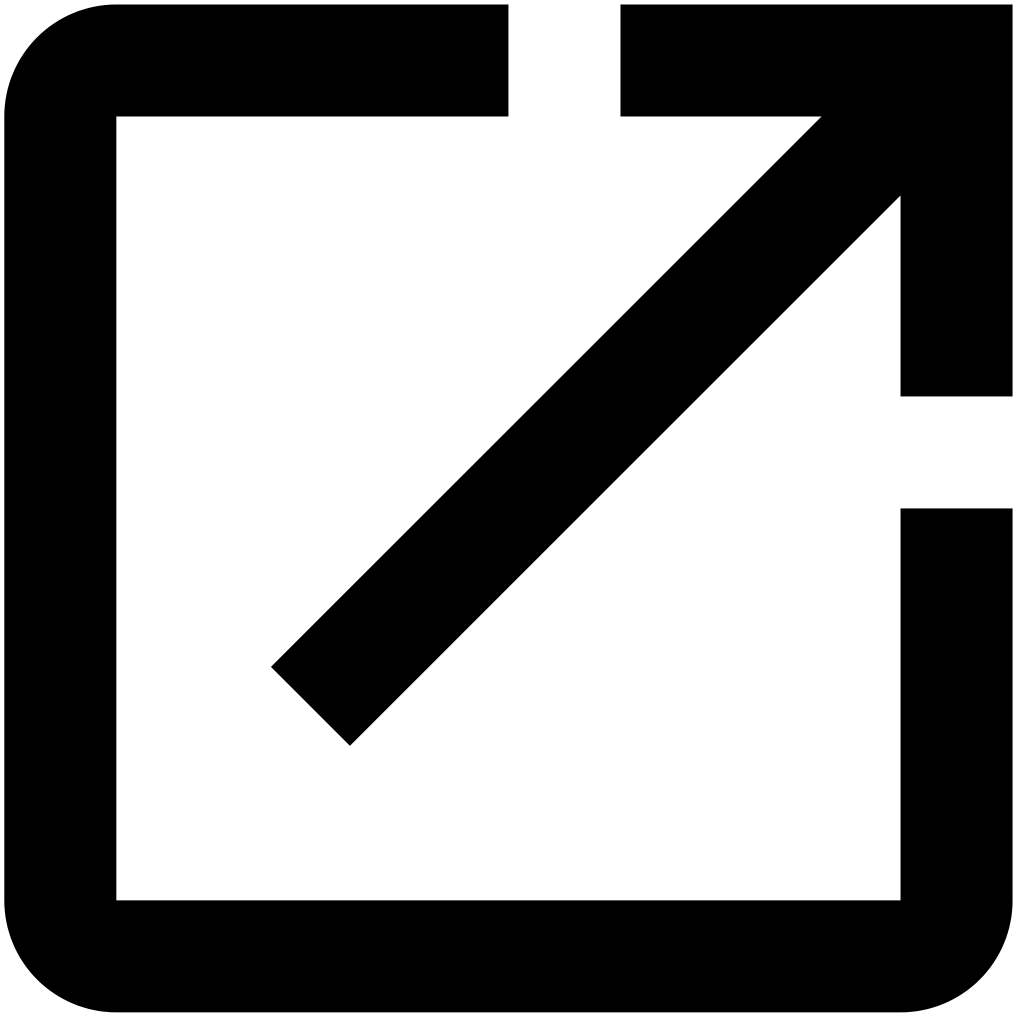
Published: 2025-06-19 · Archived: 2026-04-05 15:33:32 UTC


Satellite communications company Viasat is the latest victim of China's Salt Typhoon cyber-espionage group, which has previously hacked into the networks of multiple other telecom providers in the United States and worldwide.

Viasat provides satellite broadband services to governments worldwide and aviation, military, energy, maritime, and enterprise customers. Last month, the telecom giant told shareholders that it had approximately 189,000 broadband subscribers in the United States.

The company discovered the Salt Typhoon breach earlier this year and has been working with federal authorities to investigate the attack, as Bloomberg first reported.


0:00



"Viasat and its independent third-party cybersecurity partner investigated a report of unauthorized access through a compromised device. Upon completing a thorough investigation, no evidence was found to suggest any impact to customers," Viasat told BleepingComputer.

"Viasat engaged with government partners as part of its investigation. Due to the sensitive nature of information sharing with government partners, we are unable to provide further details. Viasat believes that the incident has been remediated and has not detected any recent activity related to this event."

BleepingComputer first contacted Viasat in February with questions regarding a potential breach, but received no reply at the time.

Russian hackers also breached Viasat's KA-SAT consumer-oriented satellite broadband service in February 2022, wiping satellite modems using AcidRain data wiper malware roughly one hour before Russia invaded Ukraine.

The 2022 cyberattack impacted tens of thousands of broadband customers in Ukraine and Europe, including modems controlling roughly 5,800 wind turbines in Germany.

## Salt Typhoon telecom breaches

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

While inside U.S. telecom 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.

Earlier this month, NSA and CISA officials also tagged Comcast and Digital Realty as potentially compromised in Salt Typhoon's telecom attacks.

Salt Typhoon has been breaching government organizations and telecom companies since at least 2019 and kept actively targeting telecoms between December 2024 and January 2025, breaching more telecommunications providers worldwide via unpatched Cisco IOS XE network devices.

---