T-Mobile confirms it was hacked in recent wave of telecom breaches

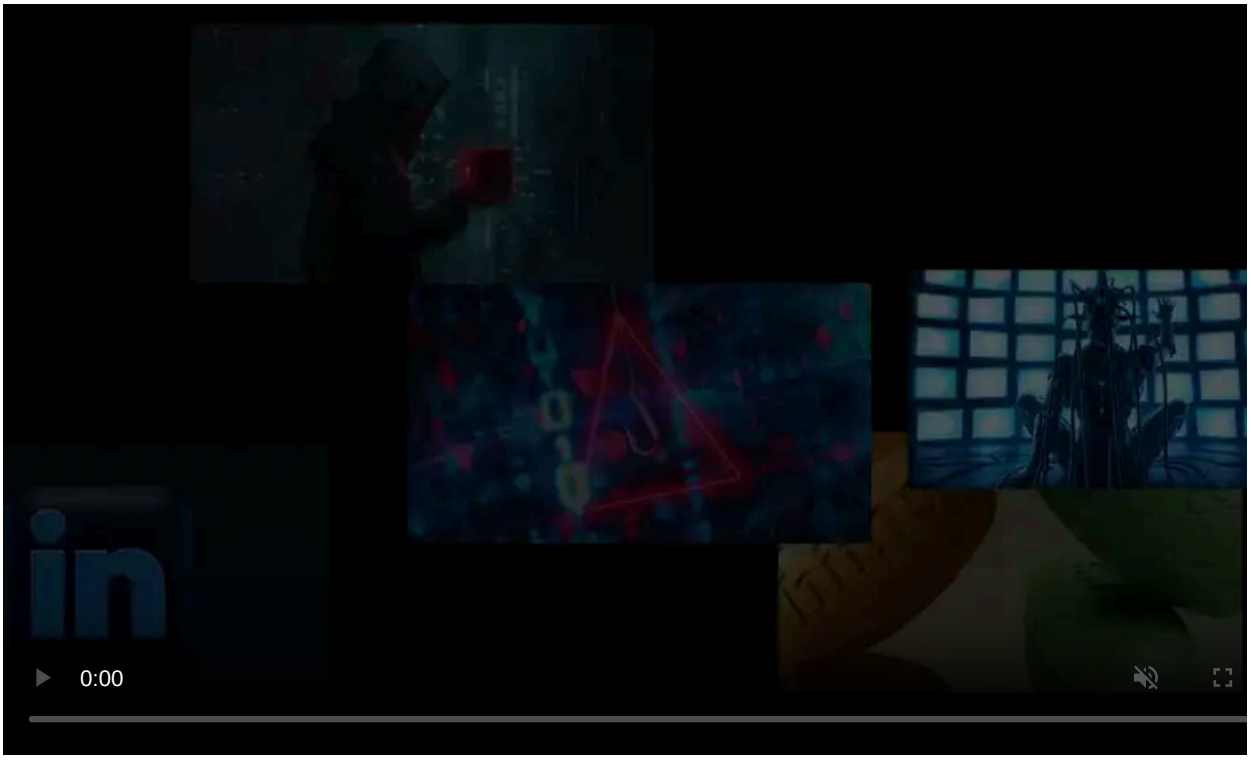
By Lawrence Abrams

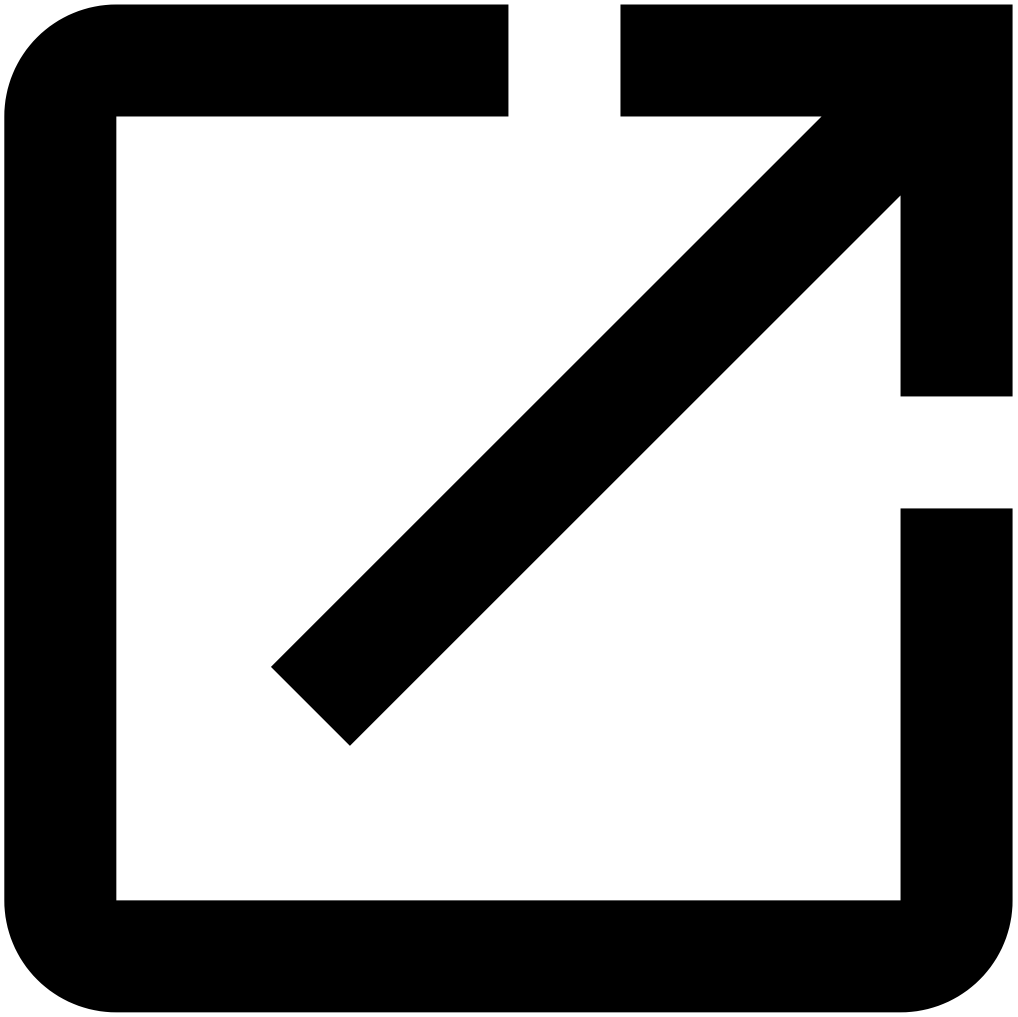
Published: 2024-11-16 · Archived: 2026-04-05 18:26:09 UTC

T-Mobile confirms it was hacked in the wave of recently reported telecom breaches conducted by Chinese threat actors to gain access to private communications, call records, and law enforcement information requests.

"T-Mobile is closely monitoring this industry-wide attack, and at this time, T-Mobile systems and data have not been impacted in any significant way, and we have no evidence of impacts to customer information," T-Mobile told the Wall Street Journal, which first reported about the breach.

"We will continue to monitor this closely, working with industry peers and the relevant authorities."


0:00



T-Mobile shared a similar statement with BleepingComputer, stating it has found no evidence of any customer data being accessed or exfiltrated.

"Due to our security controls, network structure and diligent monitoring and response we have seen no significant impacts to T-Mobile systems or data," T-Mobile told BleepingComputer after the publishing of this story.

"We have no evidence of access or exfiltration of any customer or other sensitive information as other companies may have experienced."

Last month, The Wall Street Journal reported that Chinese state-sponsored threat actors known as Salt Typhoon had breached multiple U.S. telecommunication companies, including AT&T, Verizon, and Lumen.

Salt Typhoon (aka Earth Estries, FamousSparrow, Ghost Emperor, and UNC2286) is a sophisticated Chinese state-sponsored hacking group active since at least 2019 and typically focuses on breaching government entities and telecommunications companies in Southeast Asia.

WSJ reports that the hacking campaign allowed the threat actors to target the cellphone lines of senior U.S. national security and policy officials across the U.S. government to steal call logs, text messages, and some audio.

In a joint statement from the FBI and CISA earlier this week, the U.S. government confirmed that the threat actors stole call data, communications from targeted people, and information about law enforcement requests submitted to telecommunication companies.

"Specifically, we have identified that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders,," reads the joint statement.

"We expect our understanding of these compromises to grow as the investigation continues."

These attacks were reportedly conducted through vulnerabilities in Cisco routers responsible for routing internet traffic. However, Cisco previously stated there were no indications that their equipment was breached during these attacks.

This breach is the ninth T-Mobile suffered since 2019, with the other incidents being:

- In 2019, T-Mobile exposed the account information of an undisclosed number of prepaid customers.
- In March 2020, T-Mobile employees were affected by a data breach exposing their personal and financial information.
- In December 2020, threat actors accessed customer proprietary network information (phone numbers, call records).
- In February 2021, an internal T-Mobile application was accessed by unknown attackers without authorization.
- In August 2021, hackers brute-forced their way through the carrier's network following a breach of a T-Mobile testing environment.
- In April 2022, the Lapsus$ extortion gang breached T-Mobile's network using stolen credentials.
- In January 2023, T-Mobile confirmed attackers stole the personal information of 37 million customers by abusing a vulnerable Application Programming Interface (API) in November 2022.
- In May 2023, T-Mobile disclosed a breach impacting only 836 customers, but that exposed sensitive information.

Update 11/16/24: Added statement from T-Mobile.

Source: https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/