AT&T, Verizon reportedly hacked to target US govt wiretapping platform

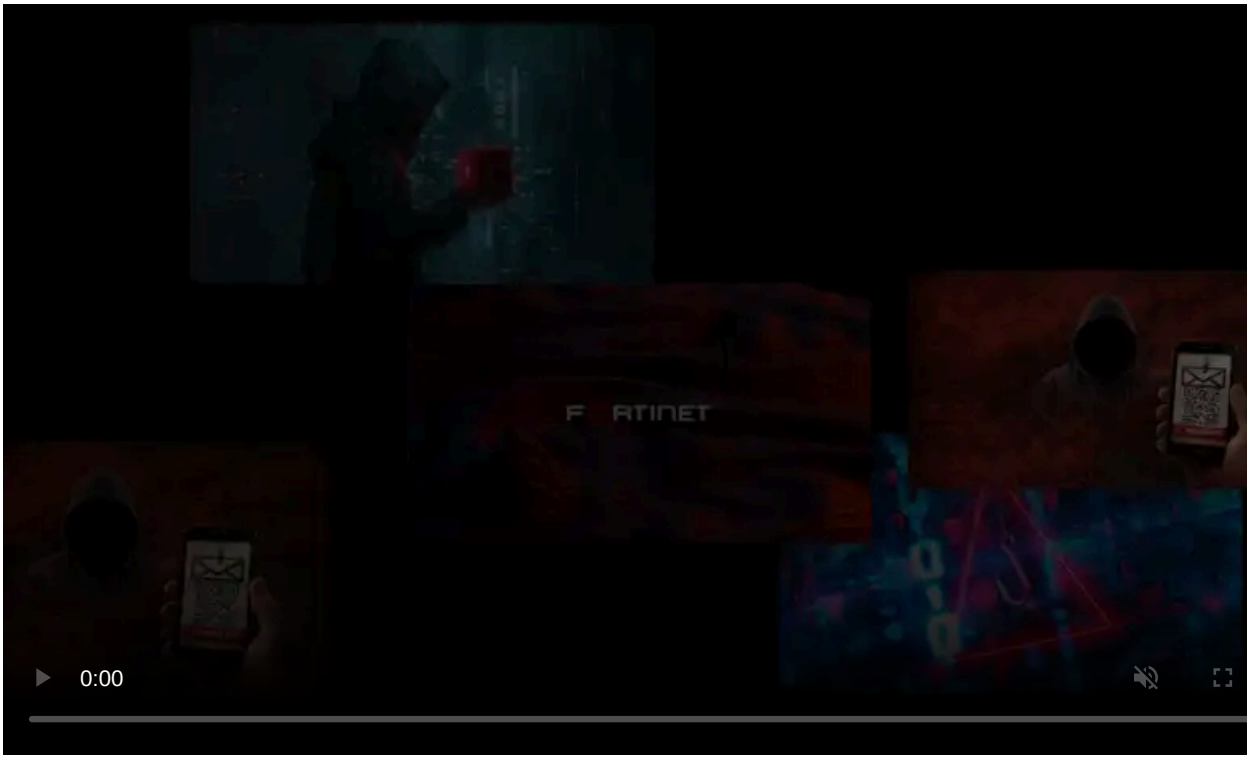
By Ionut Ilascu

Published: 2024-10-07 · Archived: 2026-04-05 21:28:49 UTC

Multiple U.S. broadband providers, including Verizon, AT&T, and Lumen Technologies, have been breached by a Chinese hacking group tracked as Salt Typhoon, the Wall Street Journal reports.

The purpose of the attack appears to be intelligence collection as the hackers might have had access to systems used by the U.S. federal government for court-authorized network wiretapping requests.

It is unclear when the intrusion occurred, but WSJ cites people familiar with the matter, saying that "for months or longer, the hackers might have held access to network infrastructure used to cooperate with lawful U.S. requests for communications data."


F RTINET
0:00

Salt Typhoon is the name that Microsoft gave to this particular China-based threat actor. Other cybersecurity companies are tracking the adversary as Earth Estries (Trend Micro), FamousSparrow (ESET), Ghost Emperor (Kaspersky), and UNC2286 (Mandiant, now part of Google Cloud).

Capturing sensitive traffic

According to the WSJ, the attack was discovered in recent weeks and is being investigated by the U.S. government and security experts in the private sector.

The impact of the attack - amount and type of observed and exfiltrated data - is still being assessed, people with information about the intrusion told WSJ.

“The hackers appear to have engaged in a vast collection of internet traffic from internet service providers that count businesses large and small, and millions of Americans, as their customers” - Wall Street Journal

Apart from breaching service providers in the U.S. Salt Typhoon may have hacked similar entities in other countries, too.

Salt Typhoon has been active since at least 2019 and is considered a sophisticated hacking group focusing on government entities and telecommunications companies typically in the Southeast Asia region.

Security researchers also found that the threat actor attacked hotels, engineering companies, and law firms in Brazil, Burkina Faso, South Africa, Canada, Israel, France, Guatemala, Lithuania, Saudi Arabia, Taiwan, Thailand, and the United Kingdom.

The hackers usually obtain initial access to the target network by exploiting vulnerabilities, such as the ProxyLogon vulnerabilities in Microsoft Exchange Server (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065).

In previous attacks attributed to Salt Typhoon/Ghost Emperor, the threat actor used a custom backdoor called SparrowDoor, customized versions of the Mimikatz tool for extracting authentication data, and a Windows kernel-mode rootkit Demodex.

Investigators are still looking for the initial access method for the recent attack. The WSJ says that one avenue being explored is gaining access to Cisco routers responsible for routing internet traffic.

However, a Cisco spokesperson told WSJ that the company was looking into the matter but had received no indication that Cisco networking equipment was involved in the breach.

BleepingComputer contacted AT&T about the alleged breach and was told they "are not commenting on the WSJ report." Lumen also declined to comment.

Verizon has not responded to our emails, and we will update the story if we receive a reply.

Chinese APT hacking groups have been increasingly targeting U.S. and European networking devices and ISPs in cyberespionage attacks.

In August, cybersecurity researchers at Lumen's Black Lotus Labs disclosed that the Chinese threat actors known as "Volt Typhoon" exploited a zero-day flaw in Versa Director to steal credentials and breach corporate networks. During these attacks, the threat actors breached multiple ISPs and MSPs in the U.S. and India, which is not believed to be related to the recent breaches.

In September, Black Lotus Labs and law enforcement disrupted a massive Chinese botnet named "Raptor Train" that compromised over 260,000 SOHO routers, IP cameras with malware. This botnet was used by the "Flax Typhoon" threat actors for DDoS attacks and as a proxy to launch stealthy attacks on other organizations.

While these attacks have been attributed to different Chinese hacking groups, they are believed to operate under the same umbrella, commonly sharing infrastructure and tools.

Source: https://www.bleepingcomputer.com/news/security/atandt-verizon-reportedly-hacked-to-target-us-govt-wiretapping-platform/