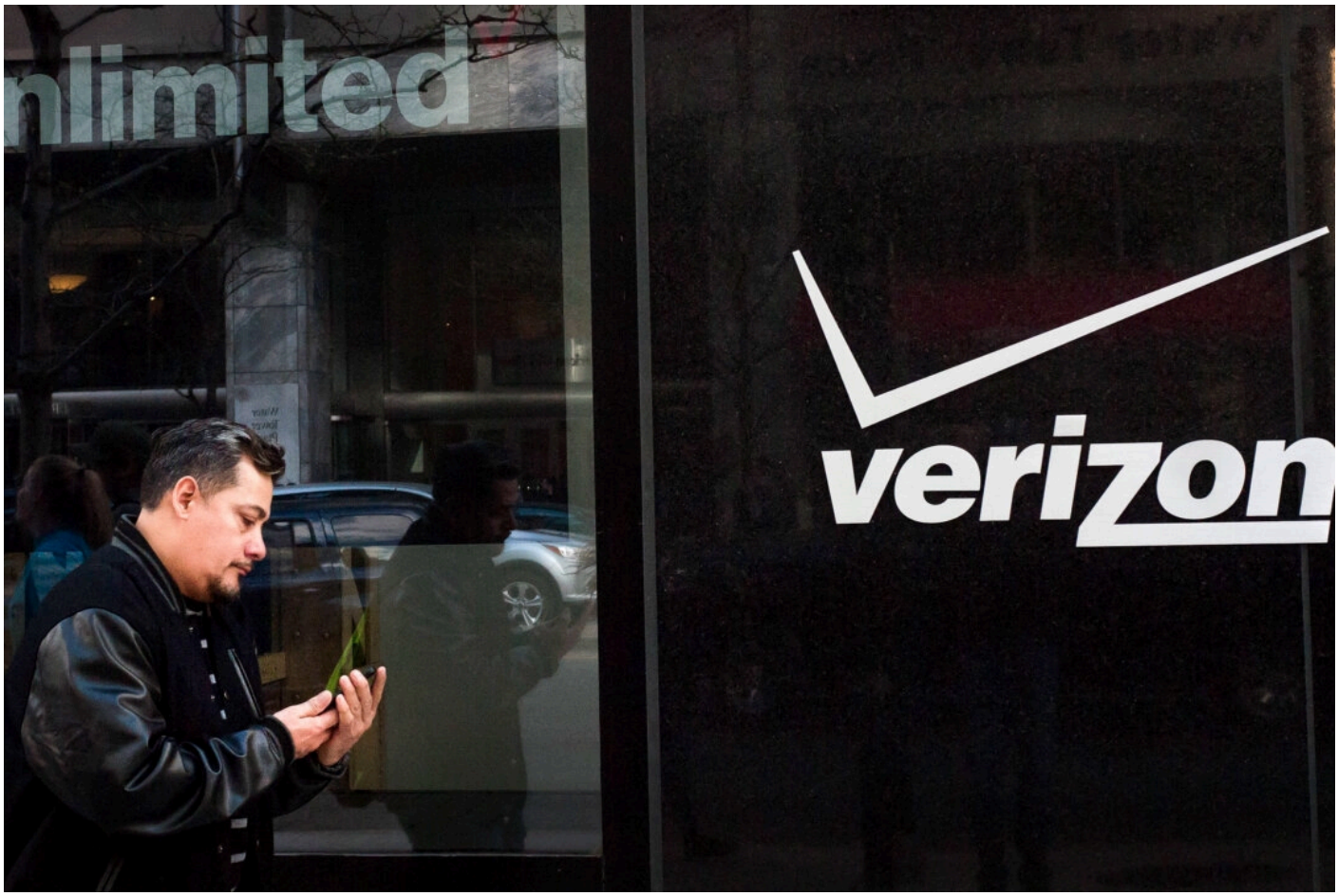
US > NATIONAL SECURITY

China-Backed Salt Typhoon Hacking Group Remains Embedded in US Telecommunications

Chinese state-backed hacking group Salt Typhoon is engaged in an ongoing attack on vast swaths of the U.S. telecommunications infrastructure.

26 10 Save



People pass a Verizon store in Chicago on April 20, 2017. Scott Olson/Getty Images

By Andrew Thornebrooke
12/10/2024 Updated: 12/10/2024

Print

Policymakers are scrambling to find a solution to stop a massive, ongoing hack of U.S. telecommunications networks by a Chinese state-backed cyber group known as Salt Typhoon.

House lawmakers received a classified briefing on the issue from intelligence leaders on Nov. 10, a week after a similar briefing was held for their counterparts in the Senate.

Salt Typhoon has engaged in a wide-ranging espionage campaign since 2022, infiltrating major U.S. telecommunications networks over the years.

Copy

Share

The group has compromised at least eight major telecommunications companies throughout dozens of nations, White House deputy national security adviser Anne Neuberger told reporters on Dec. 4.

Major corporations such as Verizon, AT&T, and CenturyLink are among the companies targeted. The hackers have used persistent access to those companies' infrastructure to collect metadata from a large number of customers, including the dates, times, and recipients of calls and texts made by an unknown number of Americans.

Although the total scale of metadata stolen is not yet known, the hackers also took the actual audio files of calls and content of texts from a smaller group of users, including some at the highest echelons of government.

Shortly after the breach was first publicly acknowledged in October, vice presidential candidate JD Vance, now the vice president-elect, said Salt Typhoon hacked his phone and that he believed that the phone of former President Donald Trump, now the president-elect, was also compromised.

Vance added that he did not believe that the hackers were able to exfiltrate his calls and texts because he was using a third-party app for encryption purposes.

Although the FBI has contacted people whose calls and texts were explicitly targeted by the campaign, the officials have left the responsibility of notifying those whose metadata was compromised to the discretion of the telecommunications companies.

The apparent scope and severity of the Salt Typhoon attack raise questions about the security of the telecommunications infrastructure used by most Americans every day and the policies used by government agencies to collect data on U.S. citizens.

Vance said that Salt Typhoon was able to tap into his phone because the group exploited backdoors in the companies' infrastructure originally established to accommodate the Foreign Intelligence Surveillance Act and the Patriot Act, which granted U.S. intelligence agencies sweeping surveillance powers.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) have since published a guidance document in collaboration with security agencies in New Zealand, Australia, and Canada, acknowledging an ongoing risk to communications infrastructure.

Jeff Greene, CISA executive assistant director, said during a call with reporters that Americans should ensure that they are using an encrypted messaging app to prevent hacking groups from obtaining their calls and texts.

Greene also emphasized that the China-backed hackers are still in U.S. infrastructure and that it is unclear when they will be fully evicted.

Sen. Mark Warner (D-Va.), who chairs the Senate Select Committee on Intelligence, told The Epoch Times shortly after the attack was made public that the breach was unprecedented in size and scope.

"I think it will go down as maybe one of the most significant cyberattacks we've faced in our country," Warner said.

Yet Salt Typhoon is only one part of a suite of Chinese state-backed hacking groups to emerge in the past several years, each of which has aimed to undermine U.S. national security in some way.

While Salt Typhoon appears to have been created for espionage purposes, other programs, including Flax Typhoon and Volt Typhoon, appear to be aimed at infiltrating critical U.S. infrastructure in preparation for a potential armed conflict with the United States.

"These actors put a premium on preparing offensive capability during peacetime, in part by preemptively planting footholds in our infrastructure," Director of National Intelligence Avril Haines said during a congressional hearing on the matter earlier this year.

Flax Typhoon was first revealed by the FBI in September, when the agency announced that it had disrupted a vast Chinese hacking operation that involved the installation of malicious software on more than 200,000 consumer devices, including cameras, video recorders, and home and office routers.

The infected devices were then used to create a massive network of infected computers, or a botnet, that could be used to carry out other cyber crimes, according to the FBI.

Volt Typhoon, on the other hand, has successfully infiltrated thousands of U.S. systems, including critical infrastructure related to U.S. water, gas, energy, rail, air, and ports.

Malware from all three cyber groups remains embedded in some U.S. systems. FBI Director Christopher Wray has said that this is partly because of the decentralized commercial nature of U.S. infrastructure, which makes it difficult to defend, and also because Chinese state-backed hackers outnumber the agency's own cybersecurity personnel 50 to one.

It is unclear at this time what, if any, action the Biden administration will take in response to the sweeping cyberattacks.

Responding to a question from The Epoch Times, State Department spokesman Matthew Miller said that he would not preview any actions that the administration may take against China.

China's ruling Communist Party denies that it engages in espionage against Americans.

Sign up for the Epoch Weekly Debrief newsletter. Get an easy, digestible roundup of 2 to 3 of the most important stories from the past week. Sign up with 1-click >>

Andrew Thornebrooke
National Security Correspondent

Andrew Thornebrooke is a national security correspondent for The Epoch Times covering China-related issues with a focus on defense, military affairs, and national security. He holds a master's in military history from Norwich University.

Author's Selected Articles

Pentagon Adopts New Strategy to Counter Drones
Dec 06, 2024

US Must Do More to Replenish Munitions Stockpiles, Says White House's Sullivan
Dec 05, 2024

Zelenskyy Open to Cease-Fire If NATO Protects Unoccupied Ukrainian Territory
Nov 29, 2024

Trump Nominates Keith Kellogg as Special Envoy for Ukraine–Russia War

Nov 27, 2024

Copyright © 2000 - 2024 The Epoch Times Association Inc. All Rights Reserved.

Cookies Settings