US > NATIONAL SECURITY

China-Linked Hackers Targeted ‘Very Senior’ US Political Figures, White House Says

‘We’re still investigating the scope and scale,’ an administration official said.

Anne Neuberger, deputy national security adviser for cyber and emerging technology, speaks with reporters in the James Brady Press Briefing Room at the White House, on Feb. 18, 2022. Alex Brandon/AP Photo

By Frank Fang
12/8/2024 Updated: 12/8/2024

A Print

A top White House official has said that Chinese state-sponsored hackers targeted “very senior” American political figures and recorded their phone calls.

Anne Neuberger, deputy national security adviser for cyber and emerging technologies, told reporters at a security conference in Bahrain that Chinese hacker group “Salt Typhoon” had stolen a large volume of Americans’ metadata.

Copy

The purpose of the operation was more focused,” Neuberger said. We believe ... the actual number of calls that they took, recorded and ook, was really more focused on very senior political individuals.”

he did not name anyone targeted by the Chinese hackers.

Share

We’re still investigating the scope and scale” of the Chinese hacking ampaign, according to Neuberger.

Earlier this week, Neuberger revealed that Salt Typhoon had breached at least eight U.S. telecommunication companies. She also warned at the time that none of the companies had fully removed the hackers from their networks.

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) confirmed the latest breaches in late October, saying at the time that an investigation was underway.

The two agencies provided an update on Nov. 13, stating that Chinese hackers had conducted a “broad and significant cyber espionage campaign” aimed at stealing data from individuals working in government and politics.

On Dec. 4, the FBI, CISA, the National Security Agency, and international partners issued guidance on best practices for protecting

communication infrastructures. Their recommendations include monitoring user account logins for anomalies, patching vulnerable devices, and investigating any configuration modifications to network devices.

Federal Communications Commission (FCC) Chairwoman Jessica Rosenworcel issued a proposal on Dec. 5 that would require communications service providers to submit an annual certification to the agency that they have a cybersecurity plan in place to protect against cyberattacks.

"While the Commission's counterparts in the intelligence community are determining the scope and impact of the Salt Typhoon attack, we need to put in place a modern framework to help companies secure their networks and better prevent and respond to cyberattacks in the future," Rosenworcel said in a statement.

FCC Commissioner Brendan Carr, who has been nominated by President-elect Donald Trump to be the next FCC chair, has said that he would tackle the threats posed by Salt Typhoon.

"The Salt Typhoon intrusion is a serious and unacceptable risk to our national security. It should never have happened," Carr wrote in a post on social media platform X on Dec. 4. "I will be working with national security agencies through the transition and next year in an effort to root out the threat and secure our networks."

On Dec. 6, Rep. Mark Green (R-Tenn.), chairman of the House Committee on Homeland Security, issued a statement in advance of the independent Cyber Safety Review Board's (CSRB) first meeting on Salt Typhoon. The board, established by the Department of Homeland Security in 2022, consists of federal officials and private-sector cybersecurity experts.

Green said that the CSRB's members "have an immense task ahead of them" and that there is bipartisan "frustration" in Congress about the extent of Salt Typhoon's breach.

“There is no doubt that a nation-state sponsored intrusion of this scale and sophistication into internet service providers is unprecedented and unnerving—something hard to say after the discovery of Volt Typhoon, another [Chinese] state-sponsored threat actor,” Green said.

Volt Typhoon, which began targeting a wide range of networks across U.S. critical infrastructure in 2021, was dismantled by a multiagency operation in January.

“I urge affected companies to cooperate in this investigation so we have a comprehensive and thorough understanding of this intrusion, which will position the CSRB to develop potential recommendations for improving overall U.S. telecom network resiliency,” Green said.

He said he will hold a congressional hearing once the board publishes its report on Salt Typhoon.

Green said he aims to advance legislation in both chambers of Congress that will address cyber threats, including a bill (H.R.9770) that would address the shortage of cyber personnel within the U.S. government.

“We face an urgent threat from our adversaries against the technology that underpins our daily lives, and we must be prepared to take decisive action,” he said.

Reuters contributed to this report.

Frank Fang
journalist

Frank Fang is a Taiwan-based journalist. He covers U.S., China, and Taiwan news. He holds a master's degree in materials science from Tsinghua University in Taiwan.

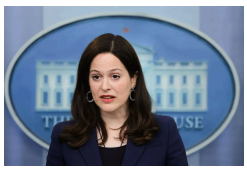
Author's Selected Articles

Trump Nominates Former Senator David Perdue as US Ambassador to China

Dec 05, 2024

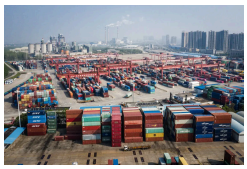
China-Linked Hackers Breached 8 US Telecom Companies, White House Says

Dec 05, 2024



British Companies Face Increasing Challenges in China, Survey Finds

Dec 03, 2024



Philippine President Says Russian Submarine Near His Country 'Very Worrisome'

Dec 02, 2024