At least 8 US telcos, dozens of countries impacted by Salt Typhoon breaches, White House says

By Jonathan Greig

Published: 2024-12-04 · Archived: 2026-04-05 12:56:13 UTC

The scope of the Chinese government hacking campaign came into further focus on Wednesday, as senior White House officials revealed that eight telecommunications giants in the U.S. were breached and that companies in multiple other countries were also hacked.

The breaches are part of the Salt Typhoon campaign, which first came to light after threat actors intercepted the correspondence of senior officials within both presidential campaigns, including from President-elect Donald Trump and his running mate JD Vance.

Anne Neuberger, the U.S. deputy national security adviser for cyber and emerging technologies, reiterated to reporters on Wednesday that Chinese actors are still inside the breached systems.

Neuberger said President Joe Biden has been briefed on the incident several times, and the White House has created a Unified Coordination Group that meets daily to discuss the issue.

The campaign “has been underway … likely one to two years” and has compromised telecoms in the Indo-Pacific region, Europe and elsewhere.

“Our understanding is that a couple dozens of countries were impacted,” she said. “We believe this is intended as a Chinese espionage program focused, again, on key government officials, key corporate IP, so that will determine which telecoms were often targeted, and how many were compromised as well.”

Neuberger added that the “Chinese access was broad in terms of potential access to communications of everyday Americans” but she said the hackers only targeted prominent individuals.

“As you know, the communications of US government officials relies on these private sector systems, which is why the Chinese were able to access the communications of some senior US government and political officials. At this time, we don't believe any classified communications have been compromised,” she said.

As the Cybersecurity and Infrastructure Security Agency (CISA) and FBI said Tuesday, the companies have not been able to fully remove the hackers from their systems so, Neuberger said, “there is a risk of ongoing compromises to communications until U.S. companies address the cybersecurity gaps.”

The agencies published guidance to help engineers and network defenders identify and remove Salt Typhoon actors. They told reporters that one complicating factor is that the hackers likely breached companies through different vectors, and also had broad aims and targets.

Read More: Cyber incident board’s Salt Typhoon review to begin within days, CISA leader says

Officials with the National Security Council did not respond to several questions about how senior officials are communicating with one another safely if Chinese actors are still in each network, or whether telecommunications companies will notify every American who may have had their data caught up in the incident.

But Neuberger said the agency believes “a large number of Americans' metadata was taken as part of a campaign to identify the specific individuals that the Chinese government was really interested in actually gaining particular access to individual calls, listening to those calls, etc."

She urged the affected telecom giants — which allegedly include Verizon, AT&T, T-Mobile, Lumen and others — to work together and share information they may be seeing in systems both in the U.S. and abroad.

At a recent meeting with the heads of those companies, senior U.S. officials stressed that each of them needed to take a range of steps to further harden their systems against compromise and “make real changes to architect telecom networks to be able to look for the unexpected and reduce the blast radius of events,” Neuberger said.

She noted that several departments within the government, most notably the Commerce Department, are coordinating to help telecom companies respond to the incident.

Neuberger went on to compare the incident to the ransomware attack on Colonial Pipeline and said it should spur a similar regulatory push for minimum cybersecurity standards that telecommunications companies must abide by.

“To prevent ongoing intrusions, we need to require similar minimum cybersecurity practices at telecoms … That’s what other countries are doing, from Australia to the UK, mandating cybersecurity practices for the most critical companies to defend against Chinese and other sophisticated cyber programs,” she said.

“We believe that if the companies had in place minimum practices — secure configurations, up-to-date patching, architecting to monitor for anomalous behavior that would have detected this earlier, managing administrator accounts with multi-factor authentication — that would make it far riskier, harder and costlier for the Chinese to gain access and maintain access.”

The international community also needs to come together to have “open, honest discussions about the PRC’s [People’s Republic of China] destabilizing behavior in cyberspace and steps the global community can take to strengthen its defenses and ultimately influence the PRC to end its destabilizing behavior.”

‘No accountability’

Also on Wednesday, a swath of agencies briefed senators on the incident. Director of National Intelligence Avril Haines spoke alongside the FBI, Federal Communications Commission, NSC and the Cybersecurity and Infrastructure Security Agency, after which several senators criticized the Biden administration for not having enough answers on the incidents.

“There's no accountability. We have not heard a plan of how they're going to fix it. That's unacceptable,” said Sen. Rick Scott (R-FL).

Sen. Ron Wyden (D-OR) told reporters that he is now working on legislation to address the Salt Typhoon campaign but declined to explain what would be in the bill or how it would address the cybersecurity of telecom companies.

Wyden and another senator sent a letter on Wednesday asking the Defense Department's top watchdog to scrutinize how the agency is shoring up its communications against spying in light of the Salt Typhoon breaches.

Mike Rounds (R-S.D.), who is expected to lead the Senate Armed Services Committee's cyber sub-panel next Congress, said one difficulty is that the country's telecommunications systems were "built for efficiency."

"They were not built for security necessarily," he said, adding that it will take "months" for the government to give direction on the changes that need to be made.

He backed calls for cybersecurity standards governing the telecoms industry but said senators are still working out the best way for them to be enacted in a feasible way.

"The challenge is, how do we go about affecting that with private telecom companies and how quickly can they put those security measures in place?" he said. "We are not talking about a short period of time because of the amount of work it's going to take to actually go through and to impact stuff. It's not like getting a new phone. It's a structure that these cell phone systems have been built on."

As he walked out of the briefing room, Senate Intelligence Committee Chair Mark Warner (D-VA), a former telecommunications executive, told reporters the incident is "far and away the worst telecom hack."

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Martin Matishak

is the senior cybersecurity reporter for The Record. Prior to joining Recorded Future News in 2021, he spent more than five years at Politico, where he covered digital and national security developments across Capitol Hill, the Pentagon and the U.S. intelligence community. He previously was a reporter at The Hill, National Journal Group and Inside Washington Publishers.
