US agencies confirm Beijing-linked telecom breach involving call records of politicians, wiretaps

By Jonathan Greig

Published: 2024-11-14 · Archived: 2026-04-06 00:26:24 UTC

U.S. law enforcement agencies confirmed on Wednesday previous reports that hackers connected to the People's Republic of China (PRC) breached the systems of commercial telecommunications infrastructure in order to steal the call record data of prominent politicians.

The FBI and Cybersecurity and Infrastructure Security Agency (CISA) said in a statement that an investigation that began in late October has revealed a “broad and significant cyber espionage campaign.”

“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,” the agencies said.

The Wall Street Journal and New York Times reported weeks ago that a Chinese government group called Salt Typhoon breached systems at AT&T, Verizon and Lumen — specifically targeting the systems U.S. law enforcement agencies use for wiretaps.

The news outlets reported that Salt Typhoon used their access to telecommunications giants like Verizon to target data from phones used by President-elect Donald Trump, Vice President-elect JD Vance and staff members of Vice President Kamala Harris.

Politico first reported that Salt Typhoon hackers gained access to Call Detail Records — which provide granular data on who a person spoke to, when, for how long, and where they were when they took the call.

The Wednesday statement says the FBI and CISA expect their understanding of the campaign “to grow as the investigation continues.”

“FBI and CISA continue to render technical assistance, rapidly share information to assist other potential victims, and work to strengthen cyber defenses across the commercial communications sector,” the agencies said. “We encourage any organization that believes it might be a victim to engage its local FBI Field Office or CISA."

In addition to Trump, Vance and Harris, law enforcement agencies told outlets that other high-ranking officials from both political parties were targeted as part of the campaign. The Wall Street Journal reported that beyond AT&T, Verizon and Lumen, several other telecoms were targeted.

In the letter to FCC Chair Jessica Rosenworcel and DOJ Attorney General Merrick Garland, U.S. Senator Ron Wyden, (D-Ore) wrote that the incident should “serve as a major wake-up call to the government.”

“The outdated regulatory framework and DOJ’s failed approach to combating cyberattacks by protecting negligent corporations must be addressed,” he said. “The security of our nation's communications infrastructure is paramount, and the government must act now to rectify these longstanding vulnerabilities.”

Retired Gen. Paul Nakasone recently spoke to the Click Here podcast and explained that the Salt Typhoon campaign was a far different effort than Volt Typhoon — where Chinese hackers placed themselves on critical infrastructure in ways that could cause destructive actions.

Nakasone, the former head of U.S. Cyber Command and the National Security Agency, said the Salt Typhoon effort resembled previous Chinese hacking efforts like the 2015 Office of Personnel Management hack and warned that U.S. officials need to be much more sophisticated in the way that they communicate.

“[Salt Typhoon’s hack] is about scope and scale. This is intelligence gathering. This is not what we saw with Volt Typhoon, which was clearly designed to create some type of outcome in a crisis or conflict. This is to gather intelligence. Should we be surprised? That unencrypted communications are being intercepted by an adversary? No, we shouldn't. Uh, but the scale of it is what is concerning,” he said.

“The scale of being in American telecommunications companies. So this portends, what are we going to do now that we've discovered them? And this is really the next step that our government, the private sector, needs to come together to be able to act on.”

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.
