SECURITY

U.S. officials urge Americans to use encrypted apps amid unprecedented cyberattack

FBI and CISA officials said it was impossible to predict when the telecommunications companies would be fully safe from interlopers.

Dec. 3, 2024, 4:01 PM EST

By Kevin Collier

Amid an unprecedented cyberattack on telecommunications companies such as AT&T and Verizon, U.S. officials have recommended that Americans use encrypted messaging apps to ensure their communications stay hidden from foreign hackers.

The hacking campaign, nicknamed Salt Typhoon by Microsoft, is one of the largest intelligence compromises in U.S. history, and it has not yet been fully remediated. Officials on a news call Tuesday refused to set a timetable for declaring the country's telecommunications systems free of interlopers. Officials had told NBC News that China hacked AT&T, Verizon and Lumen Technologies to spy on customers.

A spokesperson for the Chinese Embassy in Washington denied the country was behind the hacking campaign, telling NBC News in an email that "China firmly opposes and combats all kinds of cyber attacks."

In the call Tuesday, two officials – a senior FBI official who asked not to be named and Jeff Greene, executive assistant director for cybersecurity at the Cybersecurity and Infrastructure Security Agency – both recommended using encrypted messaging apps to Americans who want to minimize the chances of China's intercepting their communications.

"Our suggestion, what we have told folks internally, is not new here: Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication. Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible," Greene said.

The FBI official said, "People looking to further protect their mobile device communications would benefit from considering using a cellphone that automatically receives timely operating system updates, responsibly managed encryption and phishing resistant" multi-factor authentication for email, social media and collaboration tool accounts.

The scope of the telecom compromise is so significant, Greene said, that it was "impossible" for the agencies "to predict a time frame on when we'll have full eviction."

The hackers generally accessed three types of information, the FBI official said.

One type has been call records, or metadata, showing the numbers that phones called and when. The hackers focused on records around the Washington, D.C., area, and the FBI does not plan to alert people whose phone metadata was accessed.

The second type has been live phone calls of some specific targets. The FBI official declined to say how many alerts it had sent out to targets of that campaign; the presidential campaigns of Donald Trump and Kamala Harris, as well as the office of Senate Majority Leader Chuck Schumer, D-N.Y., told NBC News in October that the FBI had informed that they had been targeted.

The third has been systems that telecommunications companies use in compliance with the Communications Assistance for Law Enforcement Act (CALEA), which allows law enforcement and intelligence agencies with court orders to track people's communications. CALEA systems can include classified court orders from the Foreign Intelligence Surveillance Court, which processes some U.S. intelligence court orders. The FBI official declined to say whether any classified material was accessed.

Privacy advocates have long advocated using end-to-end encrypted apps. Signal and WhatsApp automatically implement end-to-end encryption in both calls and messages. Google Messages and iMessage also can encrypt calls and texts end to end.

The FBI and other federal law enforcement agencies have a complicated relationship with encryption technology, historically advocating against full end-to-end encryption that does not allow law enforcement access to digital material even with warrants. But the FBI has also supported forms of encryption that do allow some law enforcement access in certain circumstances.

Even though the hacking campaign was first publicly disclosed in the lead-up to the election, the U.S. believes it was not an attempt to sway results, the FBI official said, but instead a massive but traditional espionage operation by China to gather intelligence on American politics and government.

"We see this as a cyberespionage campaign, not dissimilar to any other approaches. Certainly the way they went about it was very, very specific about the telcos and the ISPs, but it fits into the cyberespionage bucket," the FBI official said.

In a statement to NBC News, Ron Wyden, D-Ore, one of the Senate's fiercest privacy advocates, criticized America's reliance on CALEA as it leaves such sensitive information unencrypted.

"Whether it's AT&T, Verizon, or Microsoft and Google, when those companies are inevitably hacked, China and other adversaries can steal those communications," he said.

CORRECTION (Dec. 4, 2024, 5:30 PM ET): A previous version of this article misstated what the acronym CALEA stands for. It is the Communications Assistance for Law Enforcement Act, not the Commission on Accreditation for Law Enforcement Agencies.

Kevin Collier

Kevin Collier is a reporter covering cybersecurity, privacy and technology policy for NBC News.