US government says ALL phone calls and texts are hacked

Raphael Satter and AJ Vicens

By Raphael Satter and AJ Vicens

WASHINGTON (Reuters) -The U.S. government is urging senior government officials and politicians to ditch phone calls and text messages following intrusions at major American telecommunications companies blamed on Chinese hackers.

Right now.

In written guidance released on Wednesday, the Cybersecurity and Infrastructure Security Agency said "individuals who are in senior government or senior political positions" should "immediately review and apply" a series of best practices around the use of mobile devices.

The first recommendation: "Use only end-to-end encrypted communications."

End-to-end encryption - a data protection technique which aims to make data unreadable by anyone except its sender and its recipient - is baked into various chat apps, including Meta Platforms' WhatsApp, Apple's iMessage, and the privacy-focused app Signal. Corporate offerings which allow end-to-end encryption also include Microsoft's Teams and Zoom Communications' online meetings.

Neither regular phone calls nor text messages are end-to-end encrypted, which means they can be monitored, either by the telephone companies, law enforcement, or - potentially - hackers who've broken into the phone companies' infrastructure.

That's what happened in the case of the cyber spies dubbed "Salt Typhoon," a group that U.S. officials have said is being run by the Chinese government.

Beijing routinely denies allegations of cyberespionage.

Speaking earlier this month, a senior U.S. official said that "at least" eight telecommunications and telecom infrastructure firms in the United States were compromised by the Salt Typhoon hackers and that "a large number of Americans' metadata" had been stolen in the surveillance sweep.

Last week, Democratic Senator Ben Ray Lujan said the wave of intrusions "likely represents the largest telecommunications hack in our nation's history" and it's not clear that American officials have figured out how to defeat the hackers' spy campaign.

Jeff Greene, CISA's executive assistant director for cybersecurity, told reporters Wednesday that the investigation remains ongoing and various targeted agencies and people are at different stages of their response.

The Salt Typhoon compromise "is part of a broader pattern of PRC activity directed at critical infrastructure," Greene said, referring to Chinese-linked cyber operations focused on utilities and other sensitive networks and tracked under the nickname "Volt Typhoon."

"This is ongoing PRC activity that we need to both prepare for and defend against for the long term," Greene said.

Communicating only via end-to-end encryption has long been a recommendation pushed by digital safety experts like those at the Electronic Frontier Foundation, whose senior staff technologist Cooper Quintin welcomed the guidance. Still, he said the idea that the government was steering its own officials away from the regular phone network was worrying.

"It is a huge indictment of the telecoms that run the nation's infrastructure," he said.

Other recommendations include avoiding text messages based on one-time passwords - like the kind often sent by U.S. banks to verify logins - and using hardware keys, which help protect against a password-stealing technique known as phishing.

Tom Hegel, a threat researcher at cybersecurity company SentinelOne, echoed Cooper's endorsement of the CISA guidelines, saying that "Chinese actors aren't the only ones continuing to collect unsecured communications."

A wide variety of spies and hackers "all stand to lose valuable access if their targets adopt these security measures," he said.

(Reporting by Raphael Satter and AJ Vicens; editing by Jonathan Oatis and Diane Craft)US government tells officials, politicians to ditch regular calls and texts

Raphael Satter and AJ Vicens

Updated Wed, December 18, 2024 at 10:52 AM PST·3 min read

7

Technicians install 5G equipment in California

By Raphael Satter and AJ Vicens

WASHINGTON (Reuters) -The U.S. government is urging senior government officials and politicians to ditch phone calls and text messages following intrusions at major American telecommunications companies blamed on Chinese hackers.

Right now.

In written guidance released on Wednesday, the Cybersecurity and Infrastructure Security Agency said "individuals who are in senior government or senior political positions" should "immediately review and apply" a series of best practices around the use of mobile devices.

The first recommendation: "Use only end-to-end encrypted communications."

End-to-end encryption - a data protection technique which aims to make data unreadable by anyone except its sender and its recipient - is baked into various chat apps, including Meta Platforms' WhatsApp, Apple's iMessage, and the privacy-focused app Signal. Corporate offerings which allow end-to-end encryption also include Microsoft's Teams and Zoom Communications' online meetings.

Neither regular phone calls nor text messages are end-to-end encrypted, which means they can be monitored, either by the telephone companies, law enforcement, or - potentially - hackers who've broken into the phone companies' infrastructure.

That's what happened in the case of the cyber spies dubbed "Salt Typhoon," a group that U.S. officials have said is being run by the Chinese government.

Beijing routinely denies allegations of cyberespionage.

Speaking earlier this month, a senior U.S. official said that "at least" eight telecommunications and telecom infrastructure firms in the United States were compromised by the Salt Typhoon hackers and that "a large number of Americans' metadata" had been stolen in the surveillance sweep.

Last week, Democratic Senator Ben Ray Lujan said the wave of intrusions "likely represents the largest telecommunications hack in our nation's history" and it's not clear that American officials have figured out how to defeat the hackers' spy campaign.

Jeff Greene, CISA's executive assistant director for cybersecurity, told reporters Wednesday that the investigation remains ongoing and various targeted agencies and people are at different stages of their response.

The Salt Typhoon compromise "is part of a broader pattern of PRC activity directed at critical infrastructure," Greene said, referring to Chinese-linked cyber operations focused on utilities and other sensitive networks and tracked under the nickname "Volt Typhoon."

"This is ongoing PRC activity that we need to both prepare for and defend against for the long term," Greene said.

Communicating only via end-to-end encryption has long been a recommendation pushed by digital safety experts like those at the Electronic Frontier Foundation, whose senior staff technologist Cooper Quintin welcomed the guidance. Still, he said the idea that the government was steering its own officials away from the regular phone network was worrying.

"It is a huge indictment of the telecoms that run the nation's infrastructure," he said.

Other recommendations include avoiding text messages based on one-time passwords - like the kind often sent by U.S. banks to verify logins - and using hardware keys, which help protect against a password-stealing technique known as phishing.

Tom Hegel, a threat researcher at cybersecurity company SentinelOne, echoed Cooper's endorsement of the CISA guidelines, saying that "Chinese actors aren't the only ones continuing to collect unsecured communications."

A wide variety of spies and hackers "all stand to lose valuable access if their targets adopt these security measures," he said.

(Reporting by Raphael Satter and AJ Vicens; editing by Jonathan Oatis and Diane Craft)