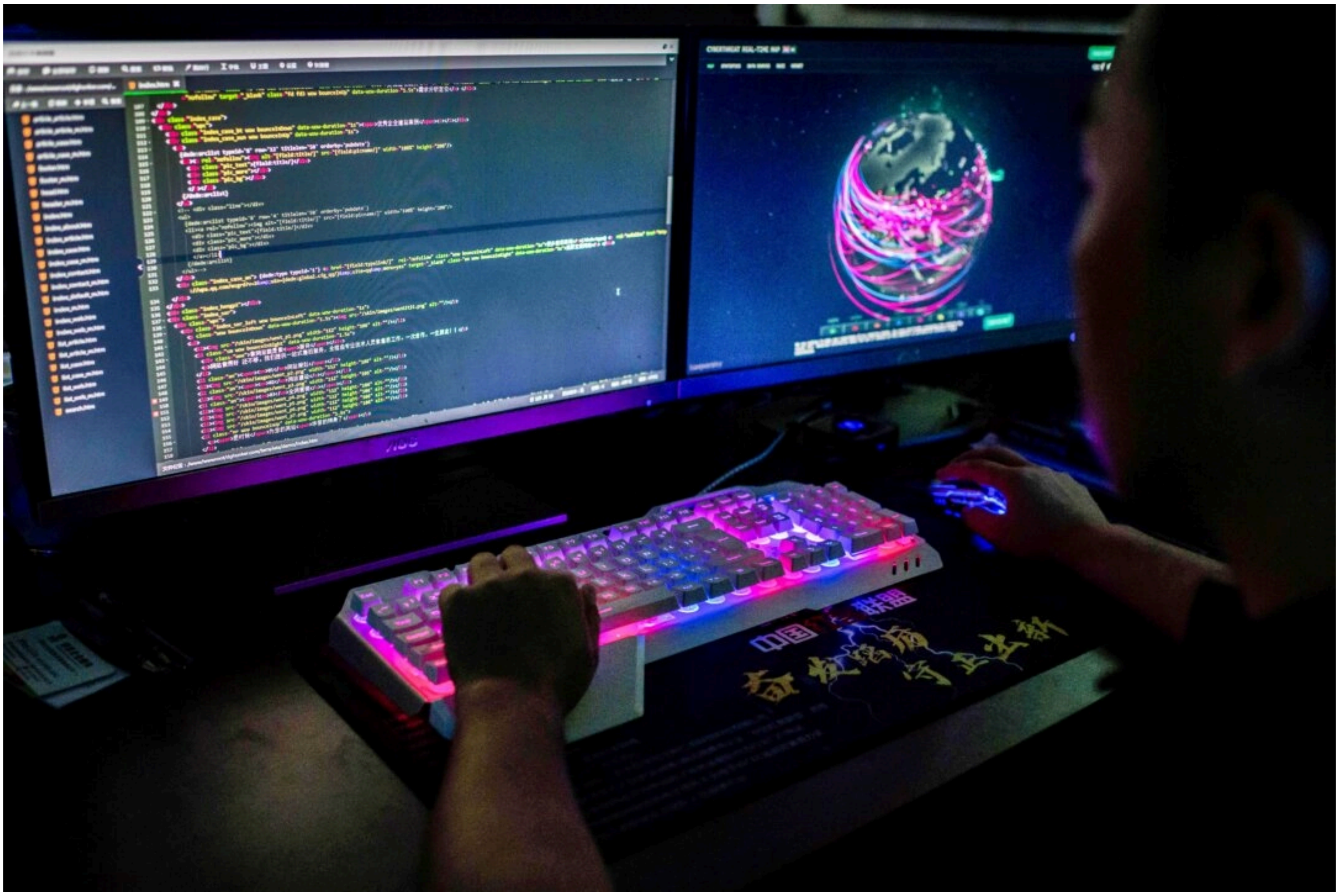
FBI, NSA Ask US Telecom Companies to Boost Security Following Chinese Hacking Incident

The latest breach ‘will go down as maybe one of the most significant cyberattacks’ the United States has ever faced, Sen. Mark Warner (D-Va.) said.

0 1 Save



A hacker uses his computer in Dongguan, Guangdong Province, China, on Aug. 4, 2020. Nicolas Asfouri/AFP via Getty Images

By Naveen Athrappully
12/4/2024 Updated: 12/4/2024

Print

Multiple intelligence agencies are recommending that telecommunication companies boost communications infrastructure security in the aftermath of a Chinese hacking campaign that targeted the sensitive sector.

On Nov. 13, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint statement revealing that hackers linked to China had compromised the networks of several U.S. telecom companies. Hackers stole customer call records, communications of individuals linked to political and government activities, and certain information subject to law enforcement requests, it said.

On Tuesday, the FBI, CISA, National Security Agency (NSA), and international partners published a guide detailing best practices for protecting communications infrastructure. It recommends "actions to quickly identify anomalous behavior, vulnerabilities, and threats, and to respond to a cyber incident," according to a Dec. 3 CISA statement.

"It also guides organizations to reduce existing vulnerabilities, improve secure configuration habits, and limit potential entry points," CISA said.

CISA Executive Assistant Director for Cybersecurity Jeff Greene called the China-backed hackers a "serious threat" to America's critical infrastructure, businesses, and government agencies. The recommendations are expected to help organizations identify and block compromises from cyber actors.

Media reported in October that a China-backed threat actor, Salt Typhoon, had engaged in a widespread hacking campaign in the United States.

In an interview with The Epoch Times last month, Sen. Mark Warner (D-Va.), chair of the Senate Select Committee on Intelligence, said the hacking attempt was “unprecedented in its size and scope.”

Attacks carried out by Salt Typhoon are believed to have affected major telecom networks including Verizon, CenturyLink, and AT&T.

The group also attacked companies and key political figures including 2024 presidential candidates Vice President Kamala Harris and then-former President Donald Trump, now the president-elect. Sen. JD Vance (R-Ohio), now the vice president-elect, had also revealed that his phone had been targeted by Chinese hackers.

Warner said that Salt Typhoon did not specifically target the U.S. elections.

“It has been, unfortunately, going on for some time,” he said. “I believe it begs the fact that we do not have any minimum cybersecurity within our telecom section.

“I think it will go down as maybe one of the most significant cyberattacks we’ve faced in our country.”

During testimony in April, FBI Director Christopher Wray said that Beijing operates the largest hacking network in the world.

“If each one of the FBI’s cyber agents and intelligence analysts focused exclusively on the PRC [People’s Republic of China] threat, the PRC’s hackers would still outnumber FBI cyber personnel at least 50 to 1,” he said.

The Chinese Threat

Last month, national security adviser Jake Sullivan met with executives from the telecom sector to discuss ongoing threats posed by the Chinese Communist regime’s state-sponsored cyber activity.

"The meeting was an opportunity to hear from telecommunications sector executives on how the U.S. Government can partner with and support the private sector on hardening against sophisticated nation-state attacks," he said.

Federal authorities have been combating Chinese cyber infiltrators for quite some time. In September, the U.S. Department of Justice (DOJ) announced that authorities had disrupted a Chinese botnet comprising more than 200,000 devices globally. A botnet refers to a network of devices infected by malware that is controlled by a central authority.

"The botnet devices were infected by People's Republic of China (PRC) state-sponsored hackers working for Integrity Technology Group, a company based in Beijing, and known to the private sector as 'Flax Typhoon,'" the DOJ said.

The botnet, controlled by Integrity, "was used to conduct malicious cyber activity disguised as routine internet traffic from the infected consumer devices," it said.

Washington's enforcement operation took control of hackers' computer infrastructure and subsequently tackled the malware infecting the devices.

According to the FBI, Flax Typhoon has successfully attacked several companies, government agencies, media groups, and universities worldwide.

"The targeted hacking of hundreds of thousands of innocent victims in the United States and around the world shows the breadth and aggressiveness of PRC state-sponsored hackers," U.S. Attorney for the Western District of Pennsylvania Eric G. Olshan said at the time.

Morgan Adamski, executive director of U.S. Cyber Command, said during a security conference last month that hackers affiliated with China were positioning themselves to attack critical IT networks in the United States in the event the two nations engage in a conflict.

U.S. officials had earlier revealed that China-backed threat groups have taken steps to disrupt server systems as well as water and energy controls.

Naveen Athrappully
Author

Naveen Athrappully is a news reporter covering business and world events at The Epoch Times.

Author's Selected Articles

Watch Out for Bad Tax Advice on Social Media: IRS

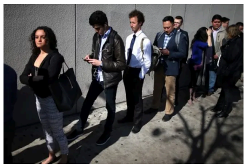
Dec 04, 2024

Planned Parenthood Seeks to Block Arizona Abortion Ban

Dec 04, 2024

California's Unemployment Insurance System Is 'Broken,' Report Finds

Dec 03, 2024



Cucumbers, Salads, Mustard Greens Recalled Across Country

Dec 03, 2024