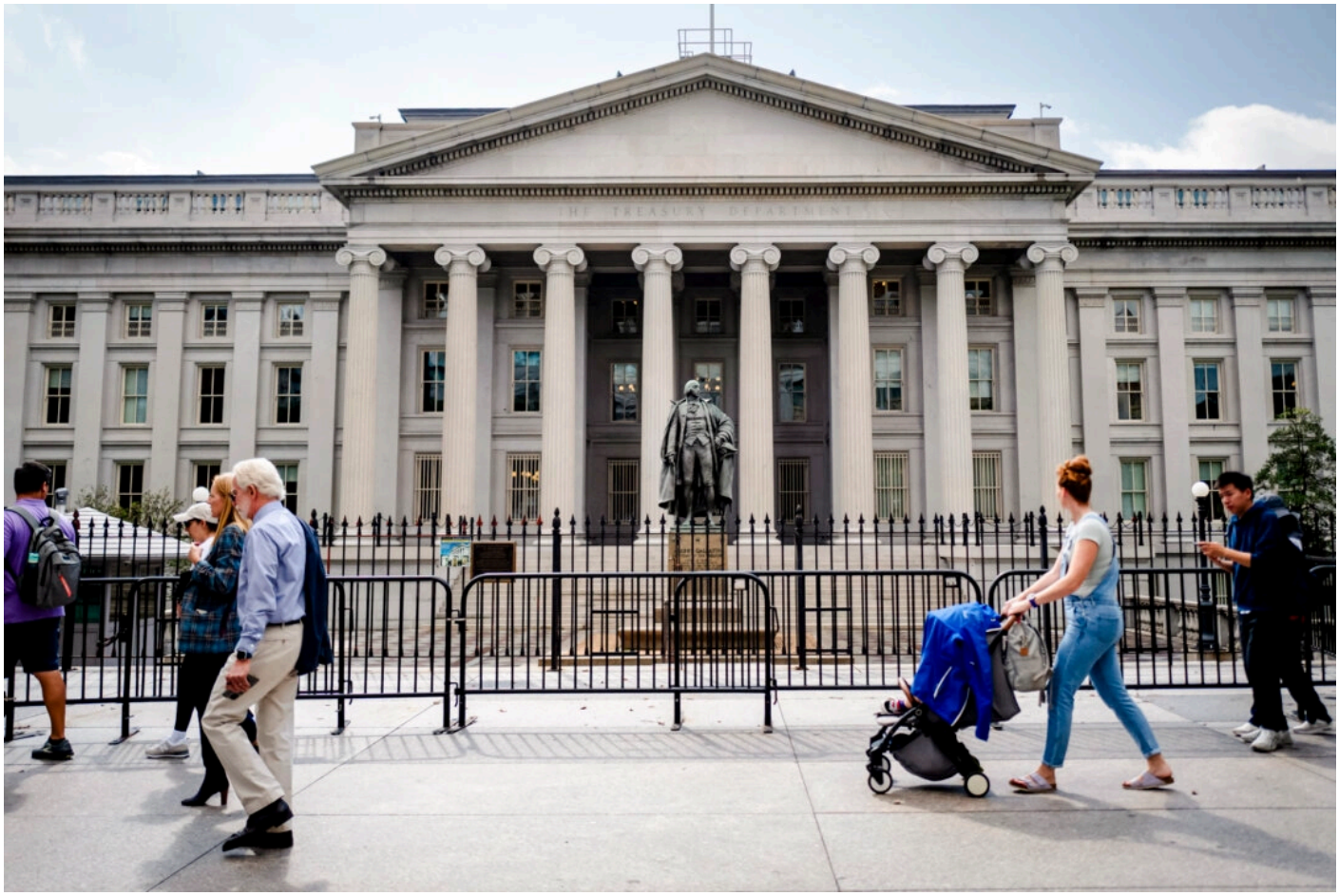
US Sanctions Chinese Company, Indicts Hacker Over Cyberattacks

The State Department announced a $10 million bounty on the Chinese hacker and others who have compromised US critical infrastructure.



The U.S. Department of the Treasury in Washington on Oct. 3, 2024. Madalina Vasiliu/The Epoch Times

By Catherine Yang

12/10/2024 Updated: 12/10/2024

The Treasury Department on Dec. 10 sanctioned a Chinese cybersecurity company and one of its employees for compromising tens of thousands of firewalls worldwide, including those of U.S. critical infrastructure companies.

The cyberattack involving Sichuan Silence Information Technology Company occurred in April 2020, according to a department statement.

The Justice Department on Tuesday unsealed an indictment against Guan Tianfeng, a Chinese citizen and employee of the cybersecurity company that was involved in the cyberattack.

Sichuan Silence's core customers are Chinese intelligence agencies, according to the Treasury Department, and the company has advertised a product that could be used to scan and detect overseas network targets to obtain intelligence information, crack passwords, and suppress public sentiment.

A grand jury indictment charges Guan with conspiracy to commit computer fraud and conspiracy to commit wire fraud.

According to law enforcement, Guan and unnamed coconspirators created malware that exploited a new vulnerability in firewalls sold by UK-based Sophos.

The UK company said in an October report that China-based actors have persistently targeted its networking appliances for five years. Cooperation between U.S. law enforcement and Sophos led to Guan's indictment.

The malware used by Guan was allegedly designed to steal information from infected computers and included "ransomware" functions that would encrypt the files on infected devices if a victim tried to fix the issue.

Guan was a security researcher at Sichuan Silence who recently posted about the similar exploits on a forum, according to officials,

and a device he used in the 2020 hack was owned by Sichuan Silence.

The widespread attack is estimated to have affected 81,000 devices worldwide, according to officials. More than 23,000 of those were in the United States, including 36 protecting U.S. critical infrastructure, one U.S. energy company, and one U.S. agency.

Sophos released patches, and clients were able to remedy the intrusion about two days after the attack. According to the indictment, Guan and the coconspirators sought to circumvent the update but were prevented.

“If any of these victims had failed to patch their systems to mitigate the exploit, or cybersecurity measures had not identified and quickly remedied the intrusion, the potential impact of the Ragnarok ransomware attack could have resulted in serious injury or the loss of human life,” the Treasury Department stated.

The State Department has put up a $10 million reward for information leading to the location of Guan or any person who has targeted U.S. critical infrastructure through cyber activities under the direction of a foreign government.

According to the Washington-based think tank Institute for Security and Technology, ransomware attacks sharply increased by 73 percent from 2022 to 2023; last year, more than 2,800 of the 6,670 incidents occurred in the United States. Sophos estimates that 59 percent of organizations were hit with ransomware in 2023

According to the Office of the Director of National Intelligence, China state-backed cyber actors are “the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.”

FBI Director Christopher Wray has warned in public speeches over the past year about the Chinese cyber threat, testifying that Chinese cyber actors outnumber that of the FBI “at least 50 to one” and that Chinese hackers have infiltrated U.S. critical infrastructure and are prepositioned to deal a “devastating blow.”

The Wall Street Journal was the first to report earlier this year that among the critical infrastructure infiltrated were major American telecommunications companies, and that Chinese actors had access for at least months.

The FBI and Cybersecurity and Infrastructure Security Agency (CISA) confirmed an investigation into the hacks in October, and the White House and Congress have held multiple briefings with telecom executives and the intelligence community since.

In a joint statement update on Nov. 13, the FBI and the CISA described the Chinese hacking campaign as "broad and significant cyber espionage."

White House officials have confirmed that the hackers breached eight telecom companies and stated that they appeared to be targeting the communications of senior political figures.

Catherine Yang
Author

Catherine Yang is a reporter for The Epoch Times based in New York.

Author's Selected Articles

Senator Introduces Bill to End Hong Kong's Special Status Over CCP Interference
Dec 10, 2024

US Sanctions Chinese, Russian Tech Companies for Human Rights Violations
Dec 10, 2024

Beijing to Sanction US Government Personnel Over Hong Kong

Dec 10, 2024

TikTok Asks Court to Pause Ban as App Seeks Supreme Court Appeal

Dec 09, 2024