Published on *The National Law Review* https://natlawreview.com

The U.S. Government Charges China-Based Hacker for Exploiting Zero-Day Vulnerability

Article By:

Trisha Sircar

On December 10, 2024, the federal government unsealed an indictment in federal court in Indiana, charging Chinese national Guan Tianfeng (Guan) for his role in allegedly breaking into thousands of Sophos Ltd. (Sophos) firewall devices globally in 2020. In total, Guan and his co-conspirators infected approximately 81,000 firewall devices worldwide, including a firewall device used by an agency of the United States (U.S.).

According to the indictment, Guan worked at Sichuan Silence Information Technology Company, Limited (Company). According to the Company's website, it developed a product line that could be used to scan and detect overseas network targets to obtain valuable intelligence information. The Federal Bureau of Investigation is investigating the Company's hacking activities and intrusions into various edge devices.

Guan has been charged with conspiracy to commit computer fraud and conspiracy to commit wire fraud. The U.S. Department of State also announced rewards on the same day as the indictment of up to $10 million for information leading to the identification or location of Guan or any person who, while acting at the direction or under the control of a foreign government, engages in certain malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act. The U.S. Department of the Treasury's Office of Foreign Assets Control also announced sanctions on Sichuan Silence and Guan today.

> "Today's indictment underscores our commitment to protecting the public from malicious actors who use security research as a cover to identify vulnerabilities in widely used systems and exploit them," said U.S. Attorney Clifford D. Johnson for the Northern District of Indiana. "Guan Tianfeng and his co-conspirators placed thousands of computer networks, including a network in the Northern District of Indiana, at risk by conducting this attack."
>
> www.justice.gov/...

National Law Review, Volume XIV, Number 358