Treasury Sanctions Cybersecurity Company Involved in Compromise of Firewall Products and Attempted Ransomware Attacks

Published: 2026-02-13 · Archived: 2026-04-05 23:11:06 UTC

WASHINGTON — Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) is sanctioning cybersecurity company **Sichuan Silence Information Technology Company, Limited** (Sichuan Silence), and one of its employees, **Guan Tianfeng** (Guan), both based in People's Republic of China (PRC), for their roles in the April 2020 compromise of tens of thousands of firewalls worldwide. Many of the victims were U.S. critical infrastructure companies.

Malicious cyber actors, including those operating in China, continue to be one of the greatest and most persistent threats to U.S. national security, as highlighted in the 2024 Annual Threat Assessment released by the Office of the Director of National Intelligence.

"Today's action underscores our commitment to exposing these malicious cyber activities—many of which pose significant risk to our communities and our citizens—and to holding the actors behind them accountable for their schemes," said Acting Under Secretary of the Treasury for Terrorism and Financial Intelligence Bradley T. Smith. "Treasury, as part of the U.S. government's coordinated approach to addressing cyber threats, will continue to leverage our tools to disrupt attempts by malicious cyber actors to undermine our critical infrastructure."

Today, the Department of Justice (DOJ) unsealed an indictment on Guan for the same activity. Additionally, the U.S. Department of State announced a Rewards for Justice reward offer of up to $10 million for information about Sichuan Silence or Guan.

April 2020 Firewall compromise

Guan Tianfeng discovered a zero-day exploit in a firewall product. A zero-day exploit is a previously unknown vulnerability in a computer software or hardware product that can be used in a cyberattack. Between April 22 and 25, 2020, **Guan Tianfeng** used this zero-day exploit to deploy malware to approximately 81,000 firewalls owned by thousands of businesses worldwide. The purpose of the exploit was to use the compromised firewalls to steal data, including usernames and passwords. However, Guan also attempted to infect the victims' systems with the Ragnarok ransomware variant. This ransomware disables anti-virus software and encrypts the computers on a victim's network if they attempt to remedy the compromise.

More than 23,000 of the compromised firewalls were in the United States. Of these firewalls, 36 were protecting U.S. critical infrastructure companies' systems. 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. One victim was a U.S. energy company that was actively involved in drilling operations at the time of the compromise. If this

compromise had not been detected, and the ransomware attack not been thwarted, it could have caused oil rigs to malfunction potentially causing a significant loss in human life.

Guan Tianfeng and sichuan silence

Guan is a Chinese national and was a security researcher at **Sichuan Silence** at the time of the compromise. Guan competed on behalf of Sichuan Silence in cybersecurity tournaments and posted recently discovered zero-day exploits on vulnerability and exploit forums, including under his moniker GbigMao. Guan was responsible for the April 2020 firewall compromise.

Sichuan Silence is a Chengdu-based cybersecurity government contractor whose core clients are PRC intelligence services. Sichuan Silence provides these clients with computer network exploitation, email monitoring, brute-force password cracking, and public sentiment suppression products and services. Additionally, Sichuan Silence provides these clients with equipment designed to probe and exploit target network routers. A pre-positioning device used by Guan in the April 2020 firewall compromise was in fact owned by his employer, Sichuan Silence.

OFAC is designating Sichuan Silence and Guan pursuant to Executive Order (E.O.) 13694, as amended by E.O. 13757, for being responsible for or complicit in, or having engaged in, directly or indirectly cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector.

SANCTIONS IMPLICATIONS

As a result of today's action, all property and interests in property of the designated persons described above that are in the United States or in the possession or the control of U.S. persons are blocked and must be reported to OFAC. In addition, any entities that are owned, directly or indirectly, individually or in the aggregate, 50 percent or more by one or more blocked persons are also blocked. Unless authorized by a general or specific license issued by OFAC, or exempt, OFAC's regulations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons.

In addition, financial institutions and other persons that engage in certain transactions or activities with the sanctioned entities and individuals may expose themselves to sanctions or be subject to an enforcement action. The prohibitions include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any designated person, or the receipt of any contribution or provision of funds, goods, or services from any such person.

The power and integrity of OFAC sanctions derive not only from OFAC's ability to designate and add persons to the Specially Designated Nationals and Blocked Persons (SDN) List, but also from its willingness to remove persons from the SDN List consistent with the law. The ultimate goal of sanctions is not to punish, but to bring about a positive change in behavior. For information concerning the process for seeking removal from an OFAC

list, including the SDN List, please refer to OFAC's Frequently Asked Question 897 here. For detailed information on the process to submit a request for removal from an OFAC sanctions list, please click here.

Click here for more information on the individuals and entities designated today.

###
