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

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.

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.

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.

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.

Dated 10th December, 2024