PRESS RELEASE

China-Based Hacker Charged for Conspiring to Develop and Deploy Malware That Exploited Tens of Thousands of Firewalls Worldwide

Tuesday, December 10, 2024

For Immediate Release

Office of Public Affairs

Note: View the indictment here and FBI Wanted Poster here.

A federal court in Hammond, Indiana, unsealed an indictment today charging Guan Tianfeng, a citizen of the People's Republic of China (PRC) for his involvement in a conspiracy to hack indiscriminately into firewall devices worldwide in 2020. Guan and his co-conspirators worked at the offices of Sichuan Silence Information Technology Co. Ltd. to discover and exploit a previously-unknown vulnerability (an "0-day" vulnerability) in certain firewalls sold by U.K.-based Sophos Ltd. (Sophos) – an information technology company that develops and markets cybersecurity products. The malware that exploited the vulnerability discovered by Guan was designed to steal information from infected computers and to encrypt files on them if a victim attempted to remediate the infection. 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.

"The defendant and his co-conspirators exploited a vulnerability in tens of thousands of network security devices, infecting them with malware designed to steal information from victims around the world," said Deputy Attorney General Lisa Monaco. "Today's indictment reflects the Justice Department's commitment to working with partners across government and across the globe to detect and hold accountable malicious cyber actors based in China or elsewhere who pose a threat to global cybersecurity."

"The defendant and his conspirators compromised tens of thousands of firewalls and then continued to hold at risk these devices, which protect computers in the United States and around the world," said Assistant Attorney General for National Security Matthew G. Olsen. "The Department of Justice will hold accountable those who contribute to the dangerous ecosystem of China-based enabling companies that carry out indiscriminate hacks on behalf of their sponsors and undermine global cybersecurity."

"Our law enforcement actions, technical expertise, and enduring partnerships with private companies, like Sophos, demonstrate the reputation of the FBI as being a reliable and effective partner for stopping this malicious activity," said Assistant Director Bryan Vorndran of the FBI's Cyber Division. "Complementary actions prevented further victimization of U.S. businesses and individuals while contributing to the safety of U.S. citizens as they use the internet."

"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."

"The zero-day vulnerability Guan Tianfeng and his co-conspirators found and exploited affected firewalls owned by businesses across the United States, including in Indiana," said Special Agent in Charge Herbert J. Stapleton of the FBI Indianapolis Field Office. "If Sophos had not rapidly identified the vulnerability and deployed a comprehensive response, the damage could have been far more severe. Sophos's efforts combined with the dedication and expertise of our cyber squad formed a powerful partnership resulting in the mitigation of this threat."

The Conspiracy to Exploit Common Vulnerabilities and Exposures (CVE) 2020-12271

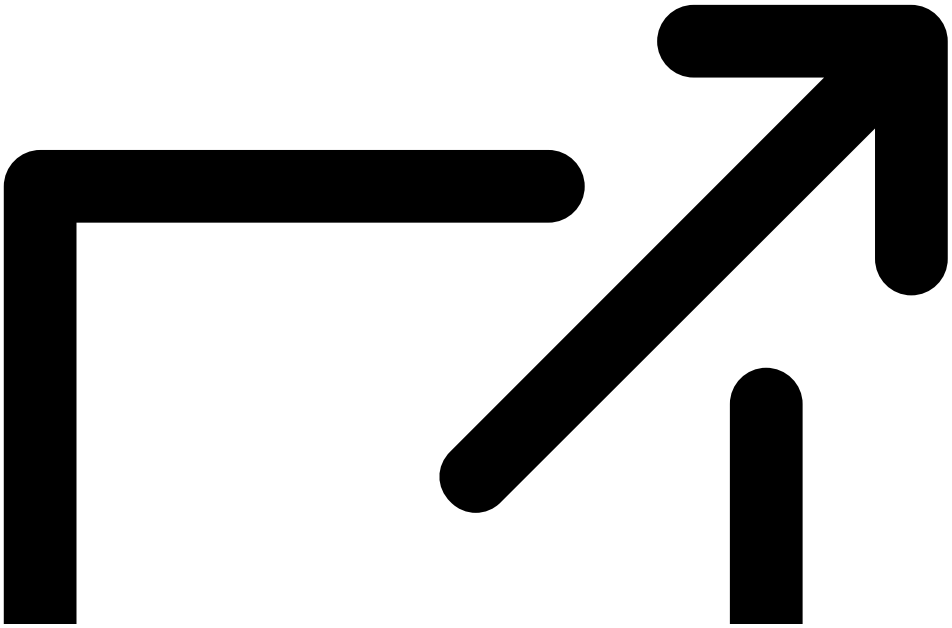
As alleged in the indictment, in 2020, Guan and his co-conspirators developed, tested, and deployed malware that targeted approximately 81,000 Sophos firewalls using a 0-day vulnerability that existed on those devices. The 81,000 Sophos firewalls were located throughout the world, including within victim organizations located in the Northern District of Indiana. The vulnerability was later designated CVE 2020-12271.

Guan and his co-conspirators designed the malware to steal information from firewalls. To better hide their activity, Guan and his co-conspirators registered and used domains designed to look like they were controlled by Sophos, such as sophosfirewallupdate.com. Sophos discovered the intrusion and remediated its customers' firewalls in approximately two days, which caused the co-conspirators to modify their malware. As modified, the malware was designed to deploy encryption software from a ransomware variant in the event the victims attempted to remove the malware. Their encryption efforts did not succeed, but demonstrated the conspirators' disregard for the harm that they would cause to victims.

Guan Tianfeng's Employment and Sichuan Silence's Relationship with the PRC Government

According to court documents, Guan worked for Sichuan Silence, a PRC-based private company that has provided services to the PRC Ministry of Public Security, among other PRC organizations. According to Sichuan Silence's website, it developed a product line which could be used to scan and detect overseas network targets in order to obtain valuable intelligence information.

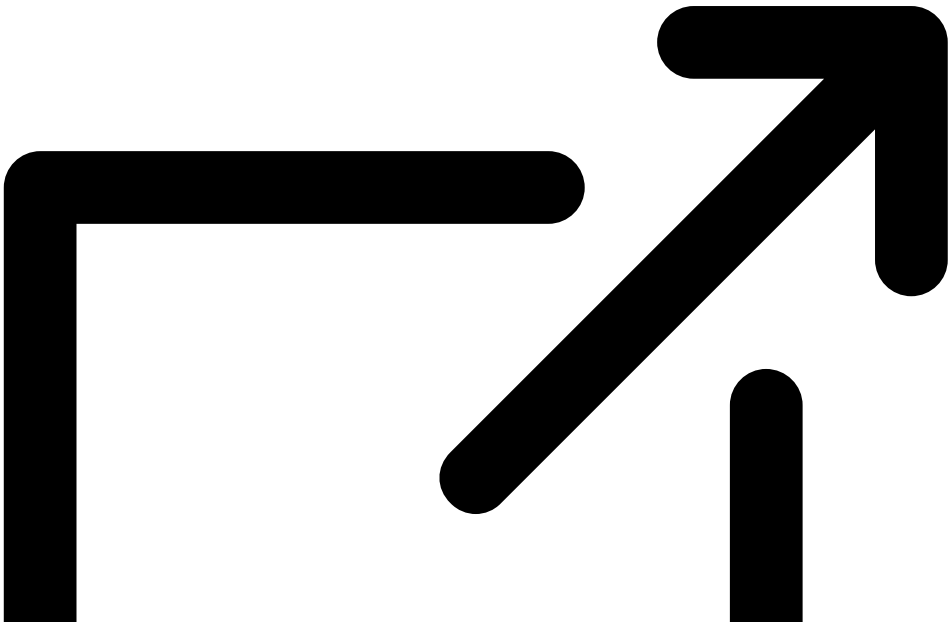
In October, Sophos released a number of articles chronicling its separate long-running investigation, "Pacific Rim



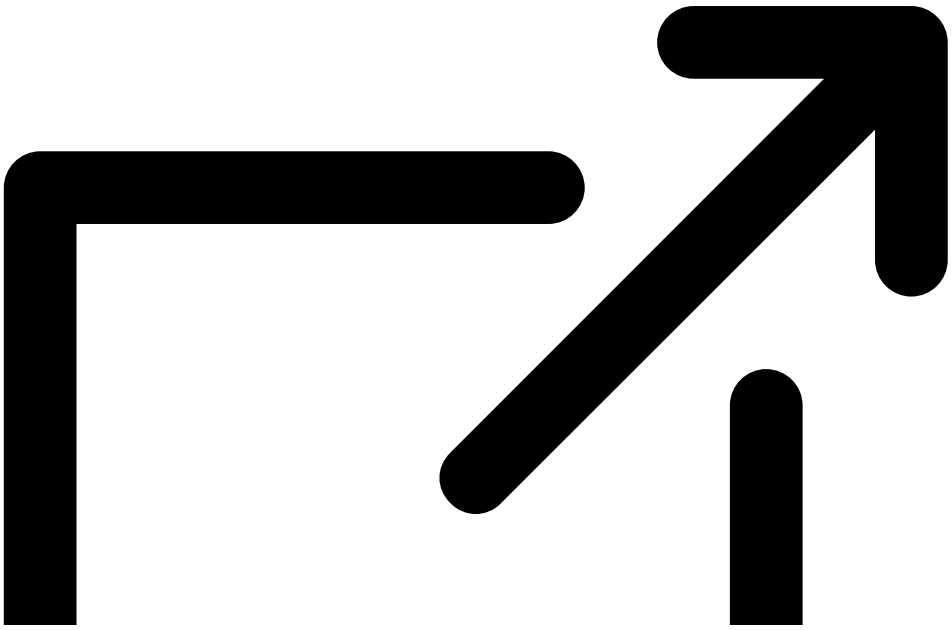
." Sophos detailed PRC-based advanced persistent threat groups targeting its networking appliances for over five years, which it described as "unusually knowledgeable about the internal architecture of the device firmware." One of the attacks described in the Pacific Rim report involved CVE-2020-12271.

Soon after the Sophos announcements in October, the FBI issued a call for information regarding computer intrusions into Sophos edge devices. The FBI continues to solicit information on PRC-sponsored malicious actors targeting edge devices and network security appliances.

The U.S. Department of State also announced



rewards today 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.

Trial Attorneys Jacques Singer-Emery and George Brown of the National Security Division's National Security Cyber Section and Assistant U.S. Attorney Steven J. Lupa for the Northern District of Indiana are prosecuting the case.

The FBI continues to investigate Sichuan Silence's hacking activities and intrusions into various edge devices.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Updated February 6, 2025