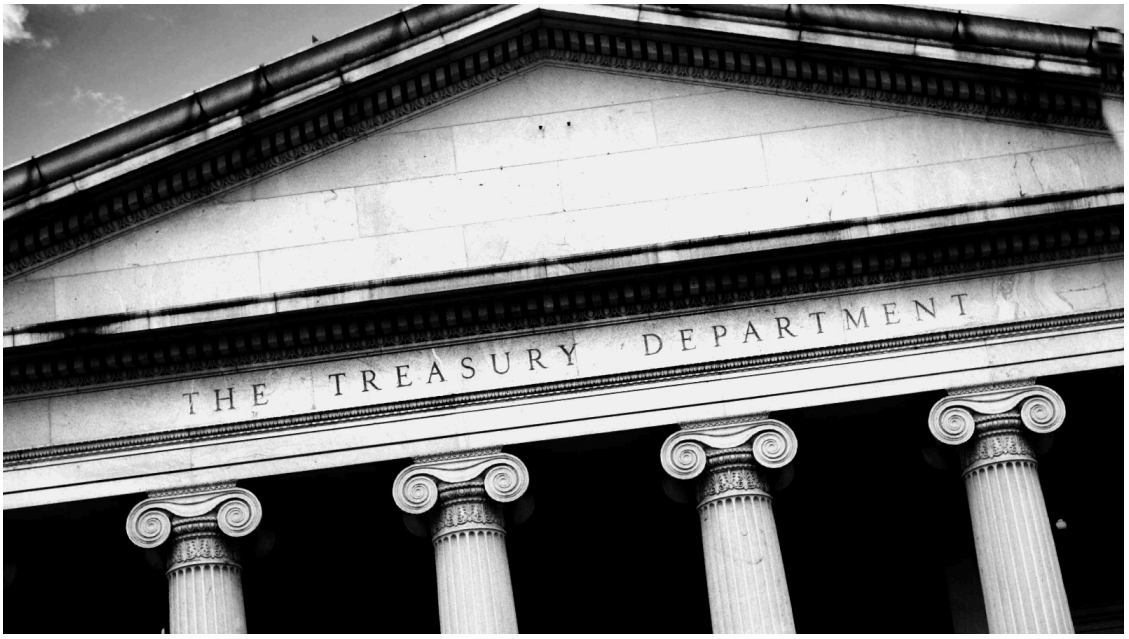
# US Treasury hack linked to Silk Typhoon Chinese state hackers

By Sergiu Gatlan

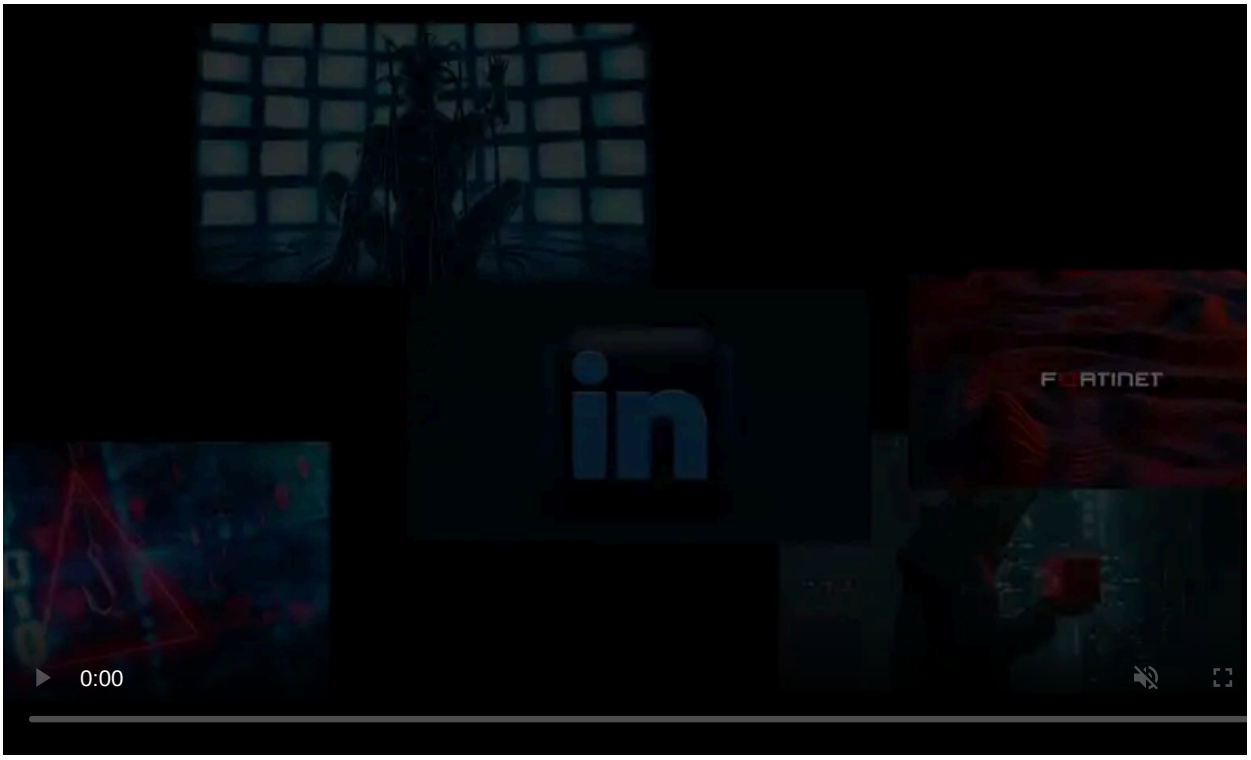
Published: 2025-01-09 · Archived: 2026-04-05 19:09:50 UTC

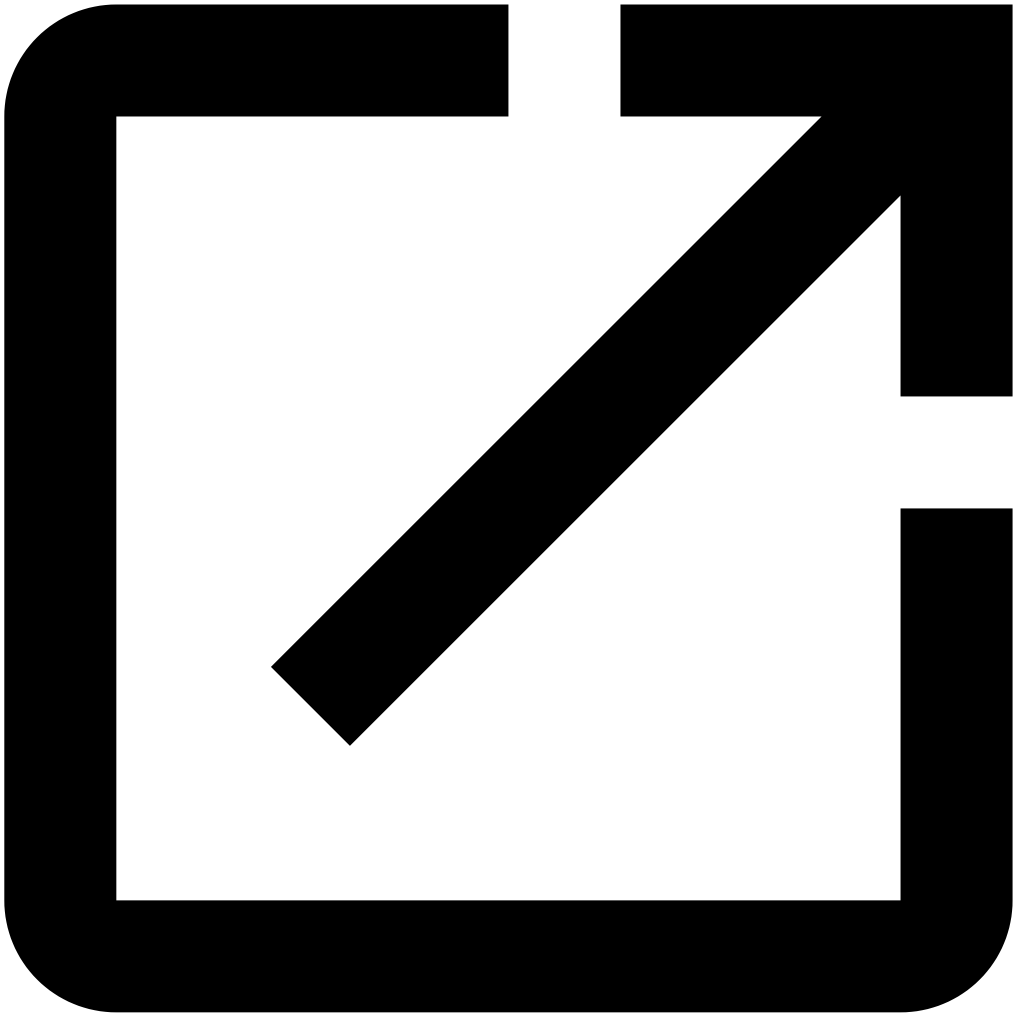



Chinese state-backed hackers, tracked as Silk Typhoon, have been linked to the U.S. Office of Foreign Assets Control (OFAC) hack in early December.

Last month, BleepingComputer reported that the Treasury disclosed a significant cybersecurity incident. The attackers used a stolen Remote Support SaaS API key to compromise a BeyondTrust instance used by the Treasury, allowing them to breach the department's network.

The threat actors also hacked the Treasury's Office of Financial Research, but the impact of this breach is still being assessed. However, there was no evidence that the Chinese hackers maintained access to the Treasury systems after the compromised BeyondTrust instance was shut down. CISA also said on Monday that the Treasury Department breach did not impact other federal agencies.


0:00



In a letter sent to Congress last week, the Treasury said its remote support provider, BeyondTrust, first notified it of the security breach on December 8th. Since then, U.S. officials revealed that the hackers specifically targeted OFAC—which administers and enforces trade and economic sanctions programs—and were likely aiming to collect intelligence on what Chinese individuals and organizations the U.S. might consider sanctioning.

On Wednesday, a Bloomberg report confirmed this hypothesis and attributed the attack to the Silk Typhoon hacking group. According to two people familiar with the matter, the group is "believed to have stolen a digital key from BeyondTrust Inc., a third-party service provider, and used it to access unclassified information relating to potential sanctions actions and other documents."

Silk Typhoon (also known as Hafnium) is a Chinese nation-state hacking group known for attacking a wide range of targets in the United States, Australia, Japan, and Vietnam, including defense contractors, policy think tanks, and non-governmental organizations (NGOs) as well as healthcare, law firms, and higher education organizations.

This Advanced Persistent Threat (APT) group's cyberespionage campaigns mainly focus on data theft and reconnaissance, using zero-day vulnerabilities and tools like the China Chopper web shell.

Hafnium became more widely known in 2021 after exploiting Microsoft Exchange Server zero-day flaws (collectively known as ProxyLogon), compromising an estimated 68,500 Exchange servers by the time security patches were released.

According to the same Bloomberg report, the Biden administration is also developing an executive order to strengthen the U.S. government's cybersecurity defenses.

The order would require implementing "strong identity authentication and encryption" and developing new guidelines for cloud service providers. These guidelines would mandate using multifactor authentication, complex passwords, and storing cryptographic keys using hardware security keys.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---