Treasury hackers also breached US foreign investments review office

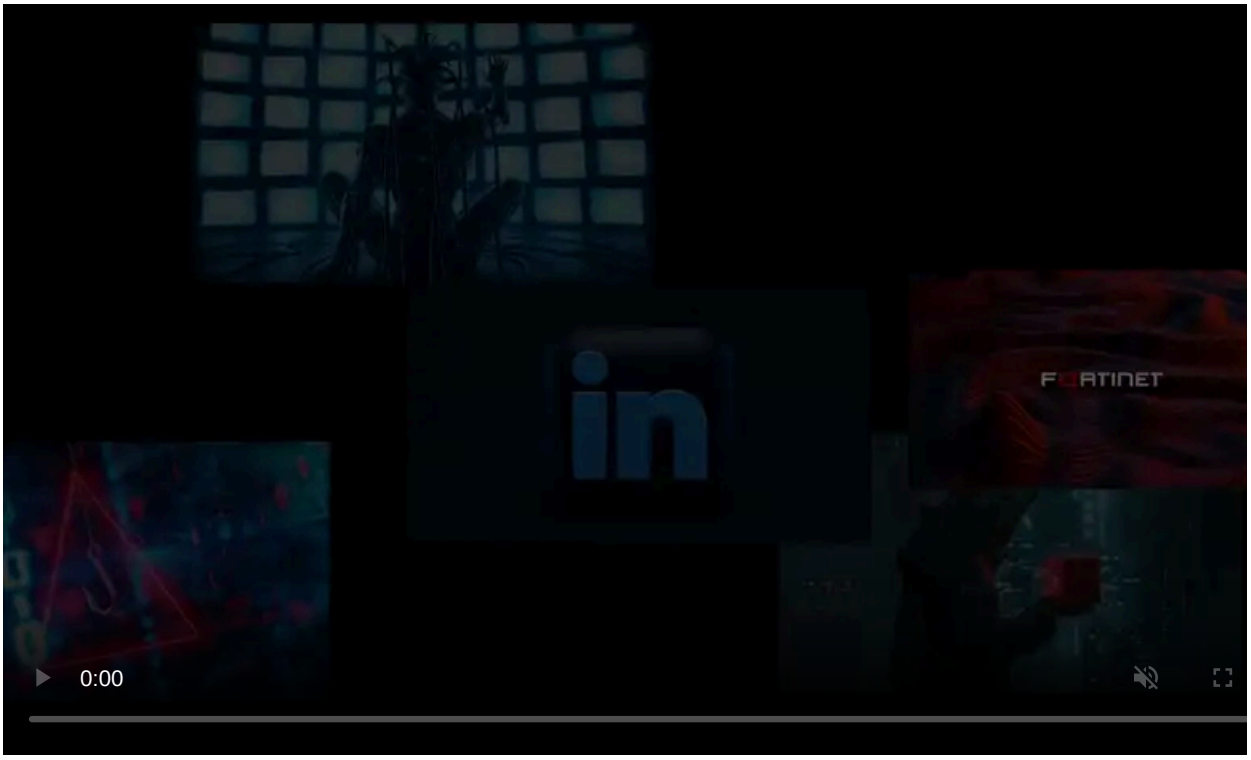
By Sergiu Gatlan

Published: 2025-01-10 · Archived: 2026-04-05 20:01:11 UTC

Silk Typhoon Chinese state-backed hackers have reportedly breached a Treasury Department office that reviews foreign investments for national security risks.

CNN reported on Friday, citing U.S. officials familiar with the matter, that the attackers gained access to the Committee on Foreign Investment in the United States (CFIUS) systems.

The CFIUS is a government office and interagency committee authorized to review foreign investment and real estate transactions to determine their effect on U.S. national security.


0:00

The same attackers also breached the Office of Foreign Assets Control (OFAC), another Treasury Department office that administers trade and economic sanctions programs, using a stolen BeyondTrust Remote Support SaaS API key to breach the department's network.

Since then, U.S. officials revealed that the threat actors specifically targeted OFAC—which administers and enforces trade and economic sanctions programs—and likely aimed to collect intelligence on Chinese individuals and organizations the U.S. might consider sanctioning.

On Monday, CISA said the Treasury Department breach did not impact other federal agencies, followed by a Wednesday Bloomberg report attributing the attack to the Silk Typhoon hacking group.

The report confirmed the intelligence theft hypothesis and said that, according to people familiar with the incident, the group is believed to have used the stolen BeyondTrust digital key "to access unclassified information relating to potential sanctions actions and other documents."

Silk Typhoon (Hafnium) also hacked the Treasury's Office of Financial Research. However, the impact of this incident is still being assessed, and investigators have yet to find evidence that the Chinese hackers maintained access to the Treasury systems after the breached BeyondTrust instance was shut down.

This Chinese nation-state hacking group is known for attacking a wide range of organizations in the United States, Australia, Japan, and Vietnam, ranging from defense contractors, policy think tanks, and non-governmental organizations (NGOs) to healthcare, law firms, and higher education entities.

The state-backed hacking group's cyberespionage campaigns mainly focus on reconnaissance and data theft, using zero-day software vulnerabilities and hacking tools like the China Chopper web shell.

Silk Typhoon became widely known in early 2021 after exploiting the ProxyLogon zero-day flaws impacting Microsoft Exchange Server, compromising an estimated 68,500 servers before security patches were released.

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.
