US Treasury Department breached through remote support platform

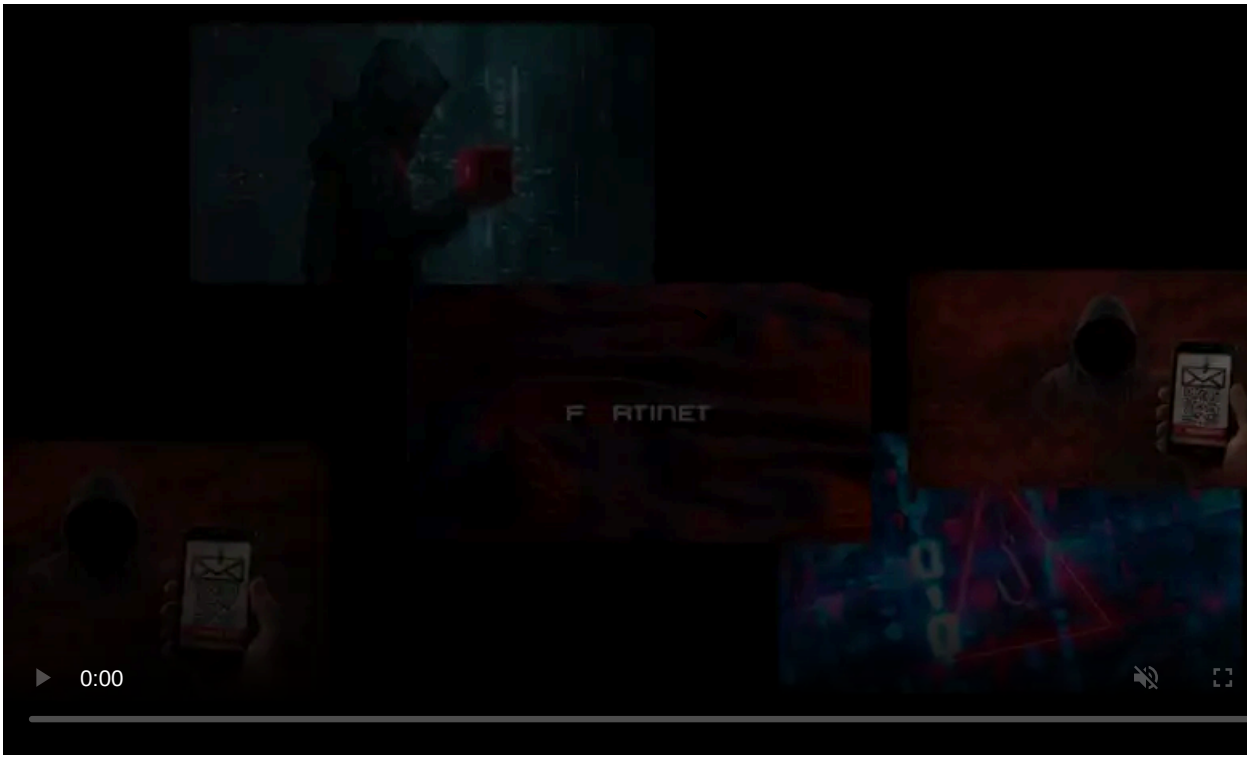
By Lawrence Abrams

Published: 2024-12-30 · Archived: 2026-04-05 21:48:38 UTC

Chinese state-sponsored threat actors hacked the U.S. Treasury Department after breaching a remote support platform used by the federal agency.

In a letter sent to lawmakers and seen by the New York Times, the Treasury Department warned lawmakers it was first notified of the breach on December 8th by its vendor BeyondTrust.

BeyondTrust is a privileged access management company that also offers a remote support SaaS platform that can be used to access computers remotely.


F RTINET
0:00

"Based on available indicators, the incident has been attributed to a China state-sponsored Advanced Persistent Threat (APT) actor," reads the letter seen by the New York Times.

"In accordance with Treasury policy, intrusions attributable to an APT are considered a major cybersecurity incident."

Earlier this month, BleepingComputer reported that BeyondTrust had been breached, with threat actors gaining access to some of the company's Remote Support SaaS instances.

As part of this breach, the threat actors utilized a stolen Remote Support SaaS API key to reset passwords for local application accounts and gain further privileged access to the systems.

After investigating the attack, BeyondTrust discovered two zero-day vulnerabilities, CVE-2024-12356 and CVE-2024-12686, that allowed threat actors to breach and take over Remote Support SaaS instances.

As the Treasury Department was a customer of one of these compromised instances, the threat actors were able to use the platform to access agency computers and steal documents remotely.

After BeyondTrust detected the breach, they shut down all compromised instances and revoked the stolen API key.

The letter says that the FBI and CISA assisted in the investigation into the Treasury Department breach, and there is no evidence that the Chinese threat actors still have access to the agency's computers now that the compromised instances were shut down.

Chinese state-sponsored threat actors named "Salt Typhoon" have also been linked to recent hacks of nine U.S. telecommunication companies, including Verizon, AT&T, Lument, and T-Mobile. The threat actors are believed to have breached telecom firms in dozens of other countries.

The threat actors utilized this access to target the text messages, voicemails, and phone calls of targeted individuals, and to access wiretap information of those under investigation by law enforcement.

Since this wave of telecom breaches, CISA has urged senior government officials to switch to end-to-end encrypted messaging apps like Signal to reduce communication interception risks.

The U.S. government reportedly plans to ban China Telecom's last active U.S. operations in response to the telecom hacks.

BleepingComputer sent further questions to the State Department about the breach but has not received a reply yet.

Source: https://www.bleepingcomputer.com/news/security/us-treasury-department-breached-through-remote-support-platform/