US Treasury Says It Was Breached by Chinese Hacker

Photo: yinance.yahoo.com

The U.S. Treasury Department has reported a significant cybersecurity breach attributed to a Chinese state-sponsored actor, as outlined in a letter sent to Congress. This incident, described as a “major cybersecurity incident,” was facilitated through a third-party software provider, BeyondTrust Inc.

Key Points of the Incident:

Breach Discovery: The Treasury was alerted on December 8, 2024, by BeyondTrust, which indicated that a hacker had gained access to a key used to secure a cloud-based service for remote technical support.

Access Details: The hacker was able to remotely access certain Treasury workstations and unclassified documents maintained by those users.

Response and Investigation: The Treasury is collaborating with the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and third-party forensic investigators to assess the breach. BeyondTrust has taken the compromised service offline and is cooperating with law enforcement.

Chinese Government's Denial: The Chinese embassy in Washington has rejected the allegations, calling them a "smear attack" and urging the U.S. to stop spreading disinformation regarding Chinese hacking threats.

Ongoing Cyber Espionage Concerns: This breach is part of a larger investigation by the White House into a cyber-espionage campaign targeting U.S. telecommunications companies, attributed to a group known as Salt Typhoon. Reports suggest that hackers spent months infiltrating telecom networks and gathering sensitive information, including communications of high-profile individuals.

Impact on U.S.-China Relations: The breach and ongoing cyber threats occur amid a period of fluctuating U.S.-China relations, which had seen some recent diplomatic engagement, including meetings between President Biden and Chinese leader Xi Jinping.

The incident underscores the persistent threat posed by state-sponsored cyber actors and raises significant concerns about the security of sensitive government information. The U.S. government is likely to take further actions to address these cybersecurity challenges and hold foreign actors accountable for such breaches.