

'Major incident'

China-backed hackers breached US Treasury workstations

BY MATT EGAN
CNN

The US Treasury Department notified lawmakers on Monday that a China state-sponsored actor infiltrated Treasury workstations in what officials are describing as a "major incident."

In a letter reviewed by CNN, a Treasury official said it was informed by a third-party software service provider on Dec. 8 that a threat actor used a stolen key to remotely access certain Treasury workstations and unclassified documents.

"Based on available indicators, the incident has been attributed to a Chinese

state-sponsored Advanced Persistent Threat (APT) actor," Aditi Hardikar, assistant secretary for management at the US Treasury, wrote in the letter.

A Treasury spokesperson said in a statement to CNN that the compromised service has been taken offline and officials are working with law enforcement and the Cybersecurity and Infrastructure Security Agency (CISA).

"There is no evidence indicating the threat actor has continued access to Treasury systems or information," the Treasury spokesperson said.

Treasury officials plan



Chip Somodevilla/Getty Images via CNN NewsSource

The US Treasury Department notified lawmakers on Dec. 30 that a China state-sponsored actor infiltrated Treasury workstations, and pictured is the U.S. Department of Treasury building.

to hold a classified briefing about the breach next week with staffers from the House Financial Services Committee, a senior committee staffer told CNN. The exact timing of the briefing has not been scheduled yet.

According to the letter to Senate Banking Committee leadership, the third-party software service provider, BeyondTrust, said hackers gained access to a key used by the vendor to secure a cloud-based ser-

vice that Treasury uses for technical support.

"With access to the stolen key, the threat actor was able to override the service's security, remotely access certain Treasury [Departmental Office] user workstations, and access certain unclassified documents maintained by those users," the Treasury letter said.

BeyondTrust did not immediately respond to a request for comment.

It's not clear exactly how many workstations were infiltrated. However, the Treasury spokesperson said in the statement that "several" Treasury user workstations were accessed.

Hardikar said in the letter that based on Treasury policy, intrusions attributed to advanced persistent

threat actors are considered a "major cybersecurity incident." Treasury officials are required to provide an update in a 30-day supplemental report.

It's not clear if Treasury has fully determined the extent of the damage caused by the breach.

Hardikar wrote in the letter that, in an effort to "fully characterize the incident and determine its overall impact," Treasury has been working with CISA, the FBI, US intelligence agencies and third-party forensic investigators.

"CISA was engaged immediately upon Treasury's knowledge of the attack, and the remaining governing bodies were contacted as soon as the scope of the attack became evident," the letter said.

McCRACKEN CO. | GRAVES CO. | MARSHALL CO. | LYON CO. | CALDWELL CO. | MASSAC CO.

CLASSIFIEDS

CALL 1-800-599-1771 OR EMAIL: classifieds@paducahsun.com

LOG ON TO CREATE YOUR OWN: PaducahSun.com (click Classifieds at the top of the page)



Buy and sell across Western Kentucky & Southern Illinois in one location. Your ad will appear in 6 newspapers!

Find it!
In the Classifieds!

FOR SALE
Spacious home on sprawling acreage.

0900 LEGALS

Local contractor seeking qualified DBE, MBE & WBE subcontractors & suppliers for work relating to civil construction in the Western Kentucky area. Email info@yecllc.com or call 270-247-1400 to request information regarding the project.

The adopted budget for FY 2024-25 and the financial statements and audit for 2023-24 of the Electric Plant Board of the City of Paducah d/b/a Paducah Power System (PPS) may be viewed at the PPS office located at 1500 Broadway, Paducah, KY and on the PPS website: www.paducahpower.com



Browse It.
paducahsun.com

The Paducah Sun

is currently accepting applications for:

FULL-TIME OFFICE DELIVERY AGENT

Duties will include delivery of newspaper routes, making of new delivery tapes, delivery of missed papers of home delivery subscribers, assist with kiosk and increase circulation sales.

Company vehicle provided. \$12/hour.

Send Resumes to jhall@paducahsun.com

For more information contact Tonya Dickey at 270-575-8792

The Paducah Sun is an equal opportunity employer and does not discriminate on the basis of race, religion, color, sex, national origin or disability.

To apply, call Tonya at 270-575-8792