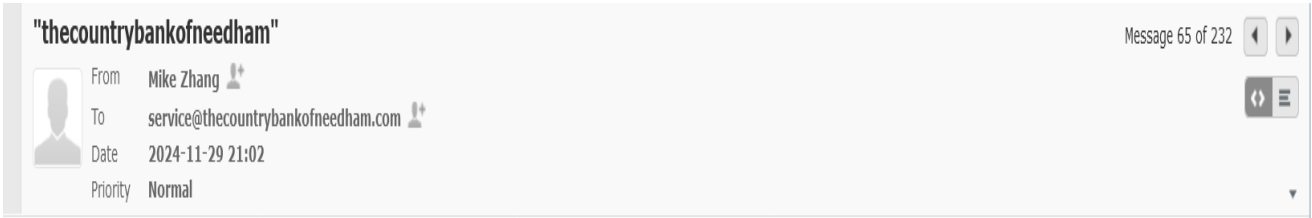


Dear CEO,

(It's very urgent, please transfer this email to your CEO. If this email affects you, we are very sorry, please ignore this email. Thanks)

We are a Network Service Company which is the domain name registration center in China.
We received an application from Kai Rui Ltd on November 25, 2024. They want to register " thecountrybankofneedham " as their Internet Keyword and " thecountrybankofneedham .cn "、" thecountrybankofneedham .com.cn " 、" thecountrybankofneedham .net.cn "、" thecountrybankofneedham .org.cn " domain names. But after checking it, we find " thecountrybankofneedham " conflict with your company name or trademark. In order to deal with this matter better, so we send you email and confirm whether this company is your distributor or business partner in China or not?

Best Regards

****

Mike Zhang | Service Manager

China Name Registry (Head Office)

No. 300, Xuanhua Road, Changning District, Shanghai200050, China

Tel: +86-2161918696 | Fax: +86-2161918697 | Mob: +86-1582177 1823

Web: www(dot)chinanameregistry(dot)cn

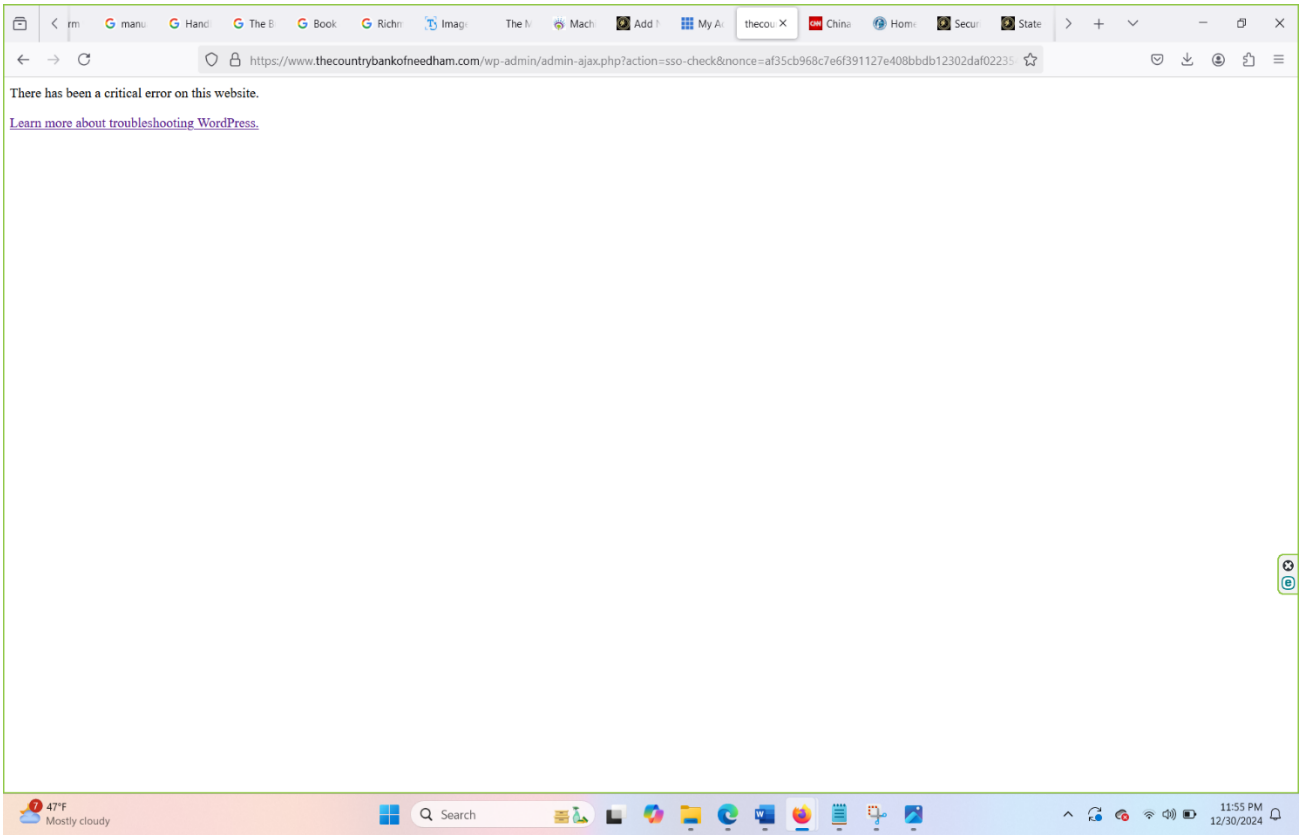
****

RECORDING OF CORPUS: US TREASURY STOLEN DOCUMENTS
[Thecountrybankofneedham.com]

https://associatetitleagency.thecountrybankofneedham.com

There has been a critical error on this website. Please check your site admin email inbox for instructions. If you continue to have problems, please try the support forums.

Learn more about troubleshooting WordPress.



US Treasury says Chinese hackers stole documents in 'major incident'

By Raphael Satter and A.J. Vicens

December 31, 2024 11:27 AM PST · Updated 4 days ago

https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/

Summary Companies

- US Treasury says Chinese state-sponsored hackers stole documents
- China says it has always opposed all forms of hacker attacks
- Attack follows a pattern of operations by China-linked groups, analyst says

WASHINGTON, Dec 30 (Reuters) - Chinese state-sponsored hackers breached the U.S. Treasury Department's computer security guardrails this month and stole documents in what Treasury called a "major incident," according to a letter to lawmakers that Treasury officials provided to Reuters on Monday.

The hackers compromised third-party cybersecurity service provider BeyondTrust and were able to access unclassified documents, the letter said.

According to the letter, hackers "gained access to a key used by the vendor to secure a cloud-based service used to remotely provide technical support for Treasury Departmental Offices (DO) end users. With access to the stolen key, the threat actor was able to override the service's security, remotely access certain Treasury DO user workstations, and access certain unclassified documents maintained by those users."

"Based on available indicators, the incident has been attributed to a China state-sponsored Advanced Persistent Threat (APT) actor," the letter said.

The Treasury Department said it was alerted to the breach by BeyondTrust on Dec. 8 and that it was working with the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the FBI to assess the hack's impact.

Treasury officials didn't immediately respond to an email seeking further details about the hack. The FBI did not immediately respond to Reuters' requests for comment, while CISA referred questions back to the Treasury Department.

"China has always opposed all forms of hacker attacks," Mao Ning, a spokesperson for China's foreign ministry, told a regular news conference on Tuesday.

A spokesperson for the Chinese Embassy in Washington rejected any responsibility for the hack, saying that Beijing "firmly opposes the U.S.'s smear attacks against China without any factual basis."

A spokesperson for BeyondTrust, based in Johns Creek, Georgia, told Reuters in an email that the company "previously identified and took measures to address a security incident in early December 2024" involving its remote support product. BeyondTrust "notified the limited number of customers who were involved," and law enforcement was notified, the spokesperson said. "BeyondTrust has been supporting the investigative efforts."

The spokesperson referred to a statement posted on the company's website on Dec. 8 sharing some details from the investigation, including that a digital key had been compromised in the incident and that an investigation was under way. That statement was last updated on Dec. 18.

Tom Hegel, a threat researcher at cybersecurity company SentinelOne (S.N), said the reported security incident "fits a well-documented pattern of operations by PRC-linked groups, with a particular focus on abusing trusted third-party services - a method that has become increasingly prominent in recent years," he said, using an acronym for the People's Republic of China."

Reporting by Raphael Satter in Washington, AJ Vicens in Detroit and Akash Sriram in Bengaluru; Additional reporting by Liz Lee in Beijing; Editing by Shinjini Ganguli, Tasim Zahid, Alistair Bell, Rod Nickel, Leslie Adler and Sonali Paul

The Reuters Daily Briefing newsletter provides all the news you need to start your day. Sign up here.

Reporting by Raphael Satter in Washington, AJ Vicens in Detroit and Akash Sriram in Bengaluru; Additional reporting by Liz Lee in Beijing; Editing by Shinjini Ganguli, Tasim Zahid, Alistair Bell, Rod Nickel, Leslie Adler and Sonali Paul

Our Standards: **The Thomson Reuters Trust Principles.**

Suggested Topics: Cybersecurity

Purchase Licensing Rights

Raphael Satter
Thomson Reuters

Reporter covering cybersecurity, surveillance, and disinformation for Reuters. Work has included investigations into state-sponsored espionage, deepfake-driven propaganda, and mercenary hacking.

A.J. Vicens
Thomson Reuters

Cybersecurity correspondent covering cybercrime, nation-state threats, hacks, leaks and intelligence

Recording:335503049585 https://associatetitleagency.thecountrybankofneedham.com for www.thecountrybankofneedham.com and U.S Treasury.