Industrial and Commercial Bank of China dealing with LockBit ransomware attack

By Jonathan Greig

Published: 2023-11-09 · Archived: 2026-04-05 23:17:21 UTC

One of the world's largest banks is dealing with a ransomware attack, according to media reports on Thursday.

The Financial Times first reported that the state-owned Industrial and Commercial Bank of China (ICBC) — China's biggest, with revenues of $214.7 billion in 2022 — was hit with ransomware this week.

The Securities Industry and Financial Markets Association, a trade group representing securities firms, banks, and asset management companies, reportedly sent a message to its members about the incident after certain trades on the U.S. Treasury market were unable to clear.

ICBC, the Securities Industry and Financial Markets Association and the U.S. Treasury Department did not respond to requests for comment.

Sources told Financial Times that the LockBit ransomware gang was behind the attack. The group has carried out several large attacks on governments, companies and organizations throughout 2023, far outpacing any other ransomware gang currently operating.

Bloomberg reported that the bank told several clients that a cybersecurity issue would require them to reroute some trades. ICBC said the attack started on Wednesday evening, the outlet reported.

Several cybersecurity researchers said reports of the attack had been floating around for days. Experts at the malware research platform vx-underground said they were informed of equity traders who were unable to place trades or clear previous ones through ICBC.

The bank allegedly sent out an emergency notice saying the incident is "impacting all of ICBC's clearing customers" and that due to the attack, they were temporarily not accepting orders.

Cybersecurity expert Kevin Beaumont shared a Shodan search showing that ICBC had a Citrix Netscaler box that was unpatched for CVE-2023-4966 — a bug known by experts as "CitrixBleed" that affects NetScaler ADC and NetScaler Gateway appliances. The products are used by companies to manage network traffic.

Beaumont said the box is now removed from the internet but noted that ransomware gangs are exploiting the issue because it "allows complete, easy bypass of all forms of authentication." More than 5,000 organizations have yet to patch the vulnerability, he added.

"It is as simple as pointing and clicking your way inside orgs - it gives attackers a fully interactive Remote Desktop PC the other end," Beaumont explained.

Jon Miller, CEO of Halcyon, told Recorded Future News that the alleged attack on ICBC “has the potential to have a serious impact on worldwide financial markets, as US Treasuries are central to the global banking and finance system.”

“Critical infrastructure providers like the financial, manufacturing, healthcare and energy sectors remain top targets for ransomware operators because the pressure to quickly resolve the attacks and resume operations increases the chances victim organizations will pay the ransom demand,” he said.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
