Cyber Cert Labs

Situational Report:
ICBC FS Ransomware Nov 2023

16.11.2023 TLP: Green

cybercertlabs.com

Situational Report

On the 8th of November the Industrial and Commercial Bank of China Financial Services ("ICBC FS") a wholly owned subsidiary of Industrial and Commercial Bank of China Limited ("ICBC") headquartered in New York notified the Securities Industry and Financial Markets Association in New York that it was experiencing a ransomware attack.

Impact Analysis

- The attack affected computer systems used as part of the banks treasury clearing service and as a result the ICBC FS was unable to settle treasury trades on behalf of clients and third parties[1].
- ICBC had to inject capital into its ICBC FS to settle $9 billion in unsettled trades with BNY Mellon and hired a cybersecurity firm for recovery[2].
- ICBC informed market participants about the incident in a SIFMA-organized call, isolating its systems from Wall Street and implementing alternative manual trading systems[3].
- The attack affected ICBC's role in the U.S. Treasuries market but caused limited overall market disruption.

Technical Analysis

- The ransomware attack was claimed by Lockbit[4]. The suspected entry point for the attack was an unpatched Citrix server vulnerability (CVE-2023-4966, 'CitrixBleed'), which allowed unauthorized network access[5].
- A security researcher Kevin Beaumount posted[6] details of a Citrix Netscaler Gateway tied to a ICBC FS domain that may have been vulnerable to this remote exploit as of the 6th of November. The information provided may only be coincidental as forensic details of the incident have not been made public yet.
- However, there is evidence that this vulnerability[7] has been targeted by threat actors seeking financial reward either through extortion, ransomware attacks or in some cases both.

---

[1] https://www.darkreading.com/attacks-breaches/treasury-markets-disrupted-from-icbc-ransomware-attack

[2] https://www.reuters.com/technology/cybersecurity/icbc-ransomware-attack-triggers-global-regulator-trader-scrutiny-2023-11-10/

[3] https://www.reuters.com/technology/cybersecurity/icbc-ransomware-attack-triggers-global-regulator-trader-scrutiny-2023-11-10/

[4] https://www.ft.com/content/8dd2446b-c8da-4854-9edc-bf841069ccb8

[5] https://www.computerweekly.com/news/366559013/Ransomware-attack-on-major-Chinese-lender-disrupts-financial-markets

[6] https://cyberplace.social/@GossiTheDog/111382220085861321

[7] https://unit42.paloaltonetworks.com/threat-brief-cve-2023-4966-netscaler-citrix-bleed/

ICBC Response and Market Reactions

- ICBC informed market participants about the incident in a SIFMA-organized call, isolating its systems from Wall Street and implementing alternative manual trading systems.
- The incident slightly affected ICBC's Hong Kong-listed shares.
- Top executives from ICBC flew to the U.S. to manage the fallout, but a full restoration of operations had not been achieved[8].
- However, there is evidence that this vulnerability[9] has been targeted by threat actors seeking financial reward either through extortion, ransomware attacks or in some cases both.

Threat Actor Details

- Lockbit ransomware was first discovered in 2020 and the group behind the malware are believed to operate out of Russia and eastern Europe.
- In 2022, LockBit was the most active global ransomware group and RaaS provider in terms of the number of victims claimed on their data leak site[10].
- LockBit claimed to have received a ransom payment from ICBC[11].

Ongoing Impact and Recovery Efforts

- The attack's disruption extent was unclear, though it affected Treasury market liquidity. ICBC worked with U.S. banks to clear transactions amid cybersecurity issues[12].
- Discussions occurred about hiring Mandiant for incident response, but no agreement was reached. Full recovery could take weeks.

Recommended Actions

- Irrespective of the speculation regarding the CitrixBleed vulnerability role in the ICBC FS ransomware attack organisations should rapidly assess their exposure to this vulnerability.
- Isolate and patch all vulnerable systems immediately.
- Begin a full historical log search to identify any potential or actual exploit attempts.
- Begin threat hunting across the network to identify any evidence of actual exploitation and any persistence activities.

---

[8] https://www.scmp.com/business/banking-finance/article/3241445/icbc-flies-top-executives-us-race-contain-fallout-hack-ransomware-gang-lockbit

[9] https://unit42.paloaltonetworks.com/threat-brief-cve-2023-4966-netscaler-citrix-bleed/

[10] https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022

[11] https://www.scmp.com/business/banking-finance/article/3241445/icbc-flies-top-executives-us-race-contain-fallout-hack-ransomware-gang-lockbit

[12] https://www.scmp.com/business/banking-finance/article/3241445/icbc-flies-top-executives-us-race-contain-fallout-hack-ransomware-gang-lockbit