KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | CDSL hit by malware attack: SEBI, CERT-In investigates the incident

Tracker ID: TN1126 **Date:** 25/Nov/2022 **Category:** Incident **Industry:** Finance **Region**: Asia

Background

On November 18, 2022, Central Depository Services Limited (CDSL), India's second-largest depository, revealed malware on a "few internal machines", according to a disclosure filed with the India's National Stock Exchange, and as a precaution, the company promptly isolated the machines and disconnected itself from other constituents of the capital market. CSDL is still investigating the incident and has not provided any details about the malware.

According to preliminary findings, it states that no confidential information or investment data has been compromised as a result of the incident. The CDSL team has reported the incident to the competent authorities, like the Securities and Exchange Board of India (SEBI) and the Computer Emergency Response Team (CERT-In), the central agency to assess cyber threats, and is investigating the attack.

In response to exchange notice no. 20221119-2 dated November 19, 2022, citing the delay in settlements seen due to malware in CDSL, the Bombay Stock Exchange (BSE) issued an additional malware advisory for stockbrokers, trading members, and clearing members on November 20, 2022, and urged the members to take the necessary steps concerning malware detection at CDSL.

India had a 51% increase in reported ransomware instances in 2022-H1 compared to the previous year. Majority of the attacks were observed in the data centers, IT, and ITeS sectors, followed by the manufacturing and finance sectors. In India during H1 2022, prominent ransomware families observed included Djvu/Stop for citizen-centric attacks, Lockbit [2.0 and 3.0] and the Hive group for targeted attacks, and Phobos for both citizen-centric and targeted threat campaigns. Aside from these, ALPHV, Ragnar, Locker, Makop, ReVil, and Conti variations were reported in H1 2022.

Threat actors are continuing to use known vulnerabilities, compromised credentials of remote access services, and phishing operations to gain initial access to enterprises' and citizens' infrastructures. The increased ransomware activity in Indian cyberspace is of grave concern. While the results of the CDSL attack investigation are still awaited and analyzing the ongoing chatter in cyberspace we request organizations to refer to our recent advisory on “Ruthless QBot Campaign and Black Basta Ransomware targets victims worldwide” and take the appropriate action to gear up against such actors. Users are requested to be vigilant, and administrators are advised to protect and prioritize patching of critical assets proactively to identify the threat actor before they infiltrates.

Indicators of Compromise

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Prioritize patching of any existing vulnerabilities and harden the applications and infrastructure.
- Enforce periodic password changes and key rotation for critical assets and remote access services [VPN and RDP]. Make sure the credentials are complex, unique, and not reused on another platform.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | CDSL hit by malware attack: SEBI, CERT-In investigates the incident

Tracker ID: TN1126 **Date:** 25/Nov/2022 **Category:** Incident **Industry:** Finance **Region**: Asia

- Implement regular phishing awareness and training throughout the workplace. Make sure employees are aware of any active phishing threats.
- Verify the email sender and content before downloading attachments or selecting embedded links from emails. Hover the pointer above embedded links to show the link's target.
- Consider enabling multi-factor authentication, especially for public facing services or remote access applications.
- Implement Privileged Access Management (PAM) in devices. Ensure security software components are enabled on all systems and that a policy is in place requiring the administrator password to be entered in the event of attempts to disable protection.
- Continuously monitor network traffic and logs for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Deploy appropriate security controls such as latest AV/EDR, Firewall, IDS for monitoring and mitigating the cyber threats.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.
- Implement proper network segmentation with controlled access to services and applications and disable unnecessary services and ports.
- Establish a data recovery strategy and routinely backup your files to a secure offsite location, where the ability to rescue your data after a ransomware assault is guaranteed by routine data backups.
- In case of a compromise, consider resetting all the account credentials that are possibly compromised and implement.

References

- ET Bureau, Clearing at CDSL back to normal post cyber attack, Economic Times, 21st November 2022, External Link (economictimes.indiatimes.com).
- NSE Archives - CDSL, Central Depository Services (India) Limited, Listing Compliance Department, National Stock Exchange of India Ltd, 18th November 2022, External Link (archives.nseindia.com).
- TeamLease RegTech, BSE issued additional malware advisory for Stockbrokers, Trading Members, and Clearing Members, Legal Research Team, 21st November 2022, External Link (www.teamleaseregtech.com).
- CERT-In, India Ransomware Report, H1-2022, 2022, External Link (www.csk.gov.in).
- KPMG Internal Sources.

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

idual or entity. Although we endeavour to provide accurate and timely e accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia