TLP: Amber + Strict: (*Means: restricted to your organisation only and information requires your support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of your organization – not for posting in public domain nor circulating on social media*).

CERT-In Advisory - CIAD-S-2025-03

Original Issue Date: May 07, 2025

Severity Rating: Critical

Urgent Advisory from CERT-In for Cyber Crisis Management

In view of the emerging heightened cyber incidents and global geo-political developments CERT-In is issuing this advisory.

Cyber crisis is a situation wherein security characters of information are compromised as a result of failure of an IT system or network of IT systems, due to technical reasons, intentional acts, leading to consequences that may threaten lives, organisations trust, national security and public confidence.

1. What are the immediate events / crisis to be alert to and aware of:

i. Surge in Scanning, Probing of Networks and IT Infrastructure

ii. Large scale spam, phishing emails

iii. Large scale defacement and attacks on websites,

iv. Large scale mis-information on websites and social media

v. Malware outbreak , ransomware attacks on your organisation

vi. Attacks on Power generation, transmission, distribution systems, Activation of malware in IoT, Industrial control systems.

vii. Attacks on Financial Sectors and Digital payment ecosystem – NPCI, UPI fintech providers, SWIFT, ATM networks, banks, Stock exchanges

viii. Distributed Denial of service attacks for disruption of websites / applications

ix. Compound attacks – By combining different attack methods, hackers could launch an even more destructive attack. The Compound

attacks magnify the destructiveness of a physical attack by launching coordinated cyber attack.

x. Attacks on Telecom infrastructure – DNS Hijacking and BGP route hijacking (prefix hijacking): The attacker announces the more specific prefixes of intended target network to reroute traffic through itself. Once successful, the hijacker could then perform Man-in-the-middle attacks, eavesdropping, modify or block the traffic.

xi. High Energy Radio Frequency Attacks

xii. Hybrid Threats & Influencing – Fake news, Manipulating human Psychology

2. What are some of the observations:

i. Phishing campaigns directed towards users
ii. Website defacements
iii. Distributed Denial of Service Attacks
iv. Malware infections, data breaches and credential compromises

3. What are some of the reasons for carrying out such incidents:

There could be multiple objectives such as:

i. To undermine public trust
ii. Undermine government's ability to deliver public services
iii. Steal sensitive information
iv. Conduct disruptive and destructive cyber attacks
v. Dissemination of propaganda and psychological operations

4. What sort of behaviour / tactics / techniques could be expected from the adversary:

Some of the behaviour / tactics / techniques could be:

i. Pre-positioning themselves in the ICT infrastructure
ii. Initial disruptive operations of the ICT infrastructure
iii. Sustained targeting and attacks of the ICT infrastructure
iv. Maintaining foot hold for extended operations within the ICT infrastructure

v. Conduct possible destructive activities of the ICT infrastructure

5. What actions can you take / what checklist can you follow:

Immediate actions:

i. Create a 24x7 control room or virtual connect systems with key officers, point of contacts along with their contact numbers (incident response teams, CERT-In, vendors, ISPs, utilities, etc)
ii. Increase vigil on your networks
iii. Monitor your bandwidth speed round the clock
iv. Ensure redundant Internet connections
v. Monitor availability of websites, applications and integrity of information being provided
vi. Create offline backups of your important data
vii. Conduct cyber threat hunting
viii. Ensure all systems are patched with latest updates
ix. Review your contingency plan
x. Review Business Continuity Plan and Disaster Recovery plan
xi. Watch for alerts from CERT-In (Cyber Swachhta Kendra, Threat Intel, NCCC) as well as from Police and MHA
xii. Act immediately on the advisories from CERT-In
xiii. Ensure multi-factor authentication for all systems
xiv. Maintain contacts of community centres, Resident Welfare Associations, Transport facilities

6. In case of a cyber incident / cyber crisis situation:

i. Report the incident or sign of crisis to CERT-In immediately and remain continuous touch with CERT-In
ii. Preserve the logs for investigation purposes and root cause analysis
iii. Prepare your crisis communication and media management plans in consultation with Cert-In
iv. Prepare an improvement plan and strengthen security controls

Responding to Cyber Threats on Industrial Control Systems implementations

Description

The potential for cyberattacks increases with industrial control systems (ICS) becoming more interconnected through the Internet of Things (IoT) and cloud-based systems. Adversaries often infect systems and silently monitor traffic, observe the activities and wait for months or even years before taking any action. This allows them to strike when they can cause the maximum damage.

Securing an ICS from cyberattacks requires a comprehensive strategy that addresses various vulnerabilities and strengthens defences. Here are key best practices for improving ICS cybersecurity:

1. Review ICS component access control; overlapping of authentication credentials for different ICS components should be avoided. Restrict user privileges to only those that are required to perform each person's job. File access should be restricted to those who require access. If network access to a file is necessary, restrict access as much as possible.

2. Unless required by the control systems software, default passwords should always be changed to robust, unpublished passwords.

3. Enhance login security across ICS platforms by requiring multiple verification forms. Use of Multi-Factor Authentication (MFA) adds an extra layer of protection against unauthorized access.

4. Examine network activity inside the enterprise's industrial network and on its boundaries. Eliminate any network connections found with other adjoining information networks that are not required by the industrial process. Ensure ICS networks are isolated from business IT networks. This separation reduces the risk of lateral movement by attackers and protects critical control systems from broader network threats.

5. Check that remote access to the industrial network is provided securely; place special emphasis on ensuring that multiple DMZs are set up in accordance with IT security requirements.

6. Implement network traffic monitoring and cyber attack detection tools on industrial networks. Control system traffic should be monitored and rules should be developed that allow only necessary access. Any exceptions created in the firewall rule set should be as specific as possible, including host, protocol and port information.

7. Misconfigurations can occur during standard operations, be introduced by the system integrator or a managed service provider, or originate from the default product settings established by the system manufacturer. Engaging with the appropriate teams to resolve these issues can help prevent the emergence of future unintended vulnerabilities.

8. Monitor security policy compliance by suppliers, vendors of ICS systems and components, that perform work on the enterprise's industrial control system and that have access to the industrial network's components.

9. Adopt comprehensive supply chain security practices, including validating the authenticity of hardware and software, performing routine security assessments, and ensuring vendors adhere to stringent cybersecurity standards.

10. Establish a process for regular briefings and periodical training of employees. Place particular emphasis on the most popular infection and attack methods, including social engineering techniques.

Organisations are requested to strictly monitor their ICT infrastructure. If any suspicious activity found, preserve all logs as per CERT-In directions of April 28, 2022, take containment measures and report with all relevant logs to CERT-In (at incident@cert-in.org.in) immediately without any delay.

For the Financial Sector, CSIRT-Fin has published a detailed advisory:

CSIRT-Fin Advisory- 251500052501

Urgent Cybersecurity Advisory: Responding to Immediate Cyber Threats in the BFSI Sector

Original Issue Date: May 01, 2025
Severity Rating: Critical ; TLP Rating: Amber

Overview

CERT-In/CSIRT-Fin have intelligence regarding an imminent and coordinated cyber threat campaign specifically targeting Indian organizations operating within the Banking, Financial Services, and Insurance (BFSI) sector. Threat actors are reportedly preparing to launch high-impact cyber-attacks such as ransomware, supply chain intrusions, DDoS attacks, website defacement, data breach and malware attacks. These vectors, whether executed individually or in combination, present a serious threat to the integrity, confidentiality, and availability of BFSI systems and services.

Description

There is a significant likelihood of threat actors leveraging supply chain attack vectors, wherein they may exploit trusted relationships between organizations and their Third-Party Service Providers (TSPs). Such trust-based access makes it increasingly difficult to detect malicious activity originating from these providers. Moreover, the threat is not confined to direct TSPs; attacks may also originate from secondary or “fourth-party” suppliers and service providers. This layered structure of interdependencies introduces considerable complexity in both detection and mitigation, making supply chain attacks particularly challenging and dangerous to defend against.

Further there is increased likelihood of sophisticated ransomware attacks and data breaches across the financial sector. Threat actors may

use advanced tactics such as double extortion, data exfiltration, and exploitation of unpatched vulnerabilities, targeting both large institutions and less-secured entities. These potential attacks pose serious risks to data confidentiality, integrity and operational continuity across the BFSI sector.

Indian BFSI entities are advised to follow the recommendations outlined in “CERT-In Advisory CIAD-2022-0023 titled "Responding to Ransomware Attacks” for corrective and protective measures specifically targeting ransomware threats, “CERT-In Advisory CIAD-2021-0004 titled "Preventing Data Breaches / Data leaks" for strategies to mitigate the risks associated with data breaches, and “CERT-In Advisory CIAD-S-2025-01 titled "Cyber-attack campaigns against Indian websites and ICT infrastructure" for comprehensive guidance on defending against DDoS attacks, website defacement, and malware infections. These advisories provide detailed actions to strengthen defences, minimize potential damage, and enhance overall cybersecurity resilience. However these advisories are not to be considered as a substitute for 24x7 heightened vigilance in your Security Operation Centre and Network Operation Centre. In addition, you are encouraged to ensure that your business continuity plans and disaster recovery plans are in place to ensure business resilience. Further, mitigation measures for supply chains attacks are below.

Prevention and mitigation measures for supply chain attacks

Prevention Measures:

1. Third-Party Risk Management:

- Conduct thorough due diligence when onboarding as well as onboarded vendors and third-party service providers. Assess their cybersecurity posture, data handling practices, and compliance with industry standards (e.g., ISO 27001, SOC 2).

- Implement a vendor risk management program to continuously monitor and assess the security maturity of third-party vendors, including secondary (fourth-party) suppliers.

- Enforce security clauses in contracts requiring vendors to maintain robust cybersecurity measures, including incident reporting, access controls, and regular audits.

2. Limit Vendor Access:

- Implement strict access controls to limit third-party access to only the necessary systems and data required for their operations. Use multi-factor authentication and least privilege access principles to minimize exposure.

- Use segmentation within internal networks to isolate third-party access from critical systems. Restrict vendors' access to sensitive data and infrastructure through secure channels (e.g., VPNs, Zero Trust networks).

3. Supply Chain Monitoring:

- Establish continuous monitoring of vendor and supplier activities, especially focusing on any anomalies in software updates or system configurations.

- Use third-party risk assessment tools to regularly scan and assess the security of supply chain partners, including identifying any known vulnerabilities in their systems or applications.

4. Software Integrity and Code Review:

- Implement code signing for software and updates to ensure the integrity of the code provided by third-party vendors. Any unsigned code should be flagged as potentially malicious.

- Perform regular code reviews and static analysis of third-party applications and components integrated into internal systems to detect any potential vulnerabilities or malicious code.

5. Multi-Factor Authentication (MFA):

- Require MFA for all third-party access, especially for sensitive systems and data. This adds an additional layer of defense, reducing the risk of unauthorized access in case credentials are compromised.

6. Require and Analyze SBOMs from All Vendors:

- Mandate comprehensive, regularly updated SBOMs (Software Bill of Materials) from third-party software providers, and automatically analyze them for known vulnerabilities using trusted databases.

7. Use SBOMs for Continuous Monitoring and Incident Response:

- Maintain an internal SBOM repository to track component dependencies, verify software integrity, and enable rapid impact assessment during supply chain security incidents.

- It is advised to adopt and implement CERT-In's "Technical Guidelines on Software Bill of Materials (SBOM)" (CISG-2024-02) which provides guidance on creating and using SBOMs for better software security and risk management.

Mitigation Measures:

1. Incident Response and Reporting:

- Develop and implement a robust supply chain incident response plan, ensuring all stakeholders, including third-party vendors, know their roles and responsibilities during a breach.

- Create a communication protocol with suppliers for prompt reporting of suspected or confirmed security incidents, including data breaches or compromise of their systems.

2. Timely Patch Management:

- Work with vendors to ensure timely deployment of patches and security updates. Establish a patch management program that prioritizes patches based on risk assessment.

- Monitor vendor-provided updates for any signs of compromise (e.g., trojanized updates) before deployment to internal systems.

3. Network Segmentation and Isolation:

- Segregate critical internal systems from vendor access via network segmentation. This reduces the impact of a compromise on a less critical system from reaching more sensitive infrastructure.

- Consider isolating third-party vendor networks from your core infrastructure using dedicated VLANs or separate subnets, preventing lateral movement if a vendor's system is compromised.

4. Backup and Recovery:

- Regularly back up critical data and ensure backups are stored in a separate location (offline or cloud) with strong encryption. Test backup recovery procedures periodically to ensure rapid restoration in case of a supply chain attack.

- Ensure that backup systems are disconnected from the main network to prevent them from being affected in the event of ransomware or malware attacks.

5. Supply Chain Simulation and Testing:

- Conduct simulated supply chain attack exercises to assess vulnerabilities in your supply chain defence mechanisms. Regularly test response plans and ensure staff are trained to recognize suspicious behaviour from third-party vendors.

- Perform penetration testing that mimics supply chain compromise scenarios, particularly focusing on the weakest links in vendor integrations and third-party software components.

6. Zero Trust Architecture:

- Implement a Zero Trust security model where no entity, whether inside or outside the organization, is trusted by default. Enforce strict identity verification and authorization for every access request, including from vendors.

Organisations are requested to strictly monitor their ICT infrastructure. If any suspicious activity found, preserve all logs as per CERT-In directions of April 28, 2022, take containment measures and report with all relevant logs to CERT-In/CSIRT-Fin (at incident@cert-in.org.in) immediately without any delay.