ICICI Lombard

# CYBER INSIGHTS DIGEST

March Edition

## NEWS BYTES - DOMESTIC


### India Boosts Cybersecurity Budget to ₹1,900 Crore

The Union Budget 2025 has allocated ₹1,900 crore for cybersecurity initiatives, an 18% increase from the previous year. This funding boost aims to combat digital fraud and address rising cybercrime threats to financial and national security

### Mobile Indian Cyber Heist: FatBoyPanel and His Massive Data Breach

Researchers discovered a malware campaign targeting Indian bank users with nearly 900 samples. The attack steals sensitive financial data through fake apps distributed via WhatsApp, exposing approximately 50,000 users' information through unsecured Firebase endpoints.


### New XELERA Ransomware Campaign Spreading Through Malicious Documents

A new ransomware campaign called XELERA is targeting Indian job seekers with fake Food Corporation of India job listings. The attack uses malicious Word documents to deliver Python-based ransomware that steals credentials, corrupts files, and demands Litecoin payments for recovery.

### Cyberattacks to spike in 2025; healthcare and finance sectors at risk: Report

Report warns that Indian healthcare and finance sectors face increased cyber threats in 2025 from AI-powered attacks, deepfakes, and supply chain vulnerabilities. Organizations are urged to enhance cybersecurity with AI-driven threat detection and cyber resilience strategies.


### The Faux SEO Spiderweb: Exploring How Black Hat SEO Has Riddled the Indian Internet Space

Over 150 Indian government websites and educational portals have been compromised by black hat SEO techniques, redirecting users to rummy and investment-focused gambling sites. Attackers use referrer manipulation, cloaking, keyword stuffing, and backlinking to target unsuspecting users.

### Safer Internet Day 2025: Google shares numbers, initiatives and projects taken

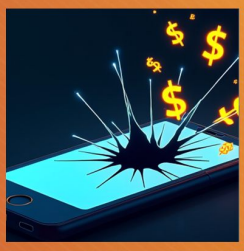
Google has ramped up cybersecurity efforts in India through DigiKavach and "Mauka Gawao" campaigns, Enhanced Play Protect program, and industry collaborations. Since November 2024, they've blocked 13.9 million harmful app installations and prevented Rs 13,000 crores in fraudulent transactions.

Powered by Arete

# NEWS BYTES - INTERNATIONAL


## UK Launches Cyber Severity Scale

The UK's Cyber Monitoring Centre has introduced a severity scale to effectively classify cyber incidents. This new system aims to improve the assessment and response to various cybersecurity threats, enhancing the country's overall cyber defense capabilities



## Android Trojan TgToxic Updates Its Capabilities

Intel 471 researchers discovered the TgToxic Android banking trojan has evolved with new features including screen recording, keylogging, and the ability to bypass two-factor authentication. The malware targets over 450 financial applications and communicates with command-and-control servers via Telegram bots.

## Poseidon Mac Malware Hiding Within PKG Files

A sophisticated macOS trojan called Poseidon uses PKG files with preinstall scripts to infiltrate systems. Active since mid-2024, this 207-byte malware steals credentials, cryptocurrency data, and system files while employing advanced evasion techniques to bypass security measures.

## Attackers exploiting Cisco vulnerabilities tied to Salt Typhoon campaign

GreyNoise researchers detected exploitation of two Cisco vulnerabilities (CVE-2018-0171 and CVE-2023-20198) between December 2024 and January 2025, potentially linked to the Chinese state-sponsored threat group Salt Typhoon, which previously breached major U.S. telecom companies.

## Massive Malware Campaign Exploits Vulnerable Windows Driver to Deploy Gh0st RAT

Attackers created 2,500+ variants of Adlice's vulnerable truesight.sys driver to bypass detection, terminate security software, and deliver Gh0st RAT malware. The campaign primarily targets China and other Asian countries, with Microsoft blocking the driver as of December 2024.


## Have I Been Pwned adds 284M accounts stolen by infostealer malware

Have I Been Pwned added 284 million compromised accounts from infostealer malware found on Telegram's "ALIEN TXTBASE" channel. The collection includes 493 million website-email pairs and 244 million new passwords, helping organizations identify potential security threats.

# KEY TRENDS

## 65.5%

**NDTV**

65.5% of attacks on India were linked to support for Palestine; indicating how global geopolitical tensions affect India's cyberspace.

## 4155

**CVE Details**

4155 CVEs (Common Vulnerabilities and Exposures) created in February.

## 2

**CISA**

CISA Adds Two Known Exploited Vulnerabilities to Catalog.

## 2.7B

**CS Hub**

IoT data breach exposes 2.7 billion records.

## 2200

**KeepNet Labs**

Cyberattacks occur at an alarming rate of over 2,200 times daily, with someone falling victim every 39 seconds.

## 12M

**M Alliance**

Hacker leaks account data of 12 million Zacks Investment users.

ICICI Lombard

# CYBER INCIDENT ANALYSIS

## Cyber Attack in IT Sector

### INDUSTRY

- IT/Software Development

### BRIEF SUMMARY

- Security vulnerability found in popular open-source data visualization platform allowed attackers to exploit plugin system weaknesses, potentially executing arbitrary code. Though quickly patched, organizations using older versions remained at risk of data breaches and system compromise.

### ROOT CAUSE ANALYSIS

- **Inadequate input validation in the plugin system allowed attackers to send malicious commands through crafted requests, with poor access control increasing exploitation risk.**
- **Vulnerable platform versions enabled security bypass and arbitrary code execution that could compromise servers.**
- **The flaw was discovered during routine security audits and quickly patched once disclosed.**
- **Multiple platform versions were affected, leaving organizations without security updates exposed to attacks.**

### LOSS CATEGORIES TO VICTIM

- Operational Disruption, Forensics Cost, Reputational Damage

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Insurer funded digital forensics to assess exploitation and ensure system security.
- Legal counsel helped navigate regulatory requirements and breach notification procedures.
- Cybersecurity experts assisted with vulnerability patching and security posture improvements.

### LOSS INCURRED

- Forensics Cost

### RECOMMENDED PREVENTIVE MEASURES

- **Update systems regularly to mitigate vulnerabilities and strengthen authentication for admin functions and plugins.**
- **Conduct routine vulnerability scans and penetration testing to identify risks early.**
- **Implement stricter controls for third-party plugins through code reviews and vetting.**
- **Set up enhanced monitoring to detect unusual access or behaviour indicating exploitation attempts.**
- **Train IT staff on timely security patch application and maintaining secure environments.**

ICICI Lombard

# CYBER INCIDENT ANALYSIS

## Cyber Breach in Healthcare Sector

### INDUSTRY

- Healthcare

### BRIEF SUMMARY

- A healthcare provider's EHR system was breached when attackers exploited a vulnerability to bypass authentication. The attack was detected after suspicious logins, but not before patient data including personal, medical, and billing information was compromised.

### ROOT CAUSE ANALYSIS

- **Attackers exploited an unpatched, critical vulnerability in the EHR system's authentication framework, bypassing MFA for privileged accounts due to outdated, poorly encrypted tokens.**
- **The vulnerability was known but not prioritized for remediation due to miscommunication within the IT security team.**
- **Patient data was exfiltrated over several days without detection due to inadequate monitoring of access log and poor anomaly detection.**

### LOSS CATEGORIES TO VICTIM

- Data Loss, Brand Reputation, Forensics Costs, Regulatory Fines, Potential Financial Losses

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Insurer funded forensic investigation of attack vector and compromised data.
- Legal counsel provided guidance on HIPAA and privacy regulation compliance.
- Cybersecurity experts implemented safeguards, patching vulnerabilities and enhancing security.
- Organization notified affected patients and established credit monitoring per breach notification laws.

### LOSS INCURRED

- Forensics Costs, Legal Costs

### RECOMMENDED PREVENTIVE MEASURES

- **Apply immediate patches for known vulnerabilities and maintain regular updates for critical systems.**
- **Strengthen authentication with better token encryption and mandatory MFA for all accounts.**
- **Enhance monitoring of user access patterns and implement anomaly detection for early threat identification.**
- **Encrypt all sensitive data in transit and at rest; develop a comprehensive incident response plan.**
- **Conduct regular security audits and train staff on data protection and phishing awareness.**

# ADVISORIES

## SECURE BY DEMAND: PRIORITY CONSIDERATIONS FOR OPERATIONAL TECHNOLOGY OWNERS

- **Threat Landscape:** Cyber threat actors are targeting specific OT products rather than specific organizations, exploiting common weaknesses such as weak authentication, known software vulnerabilities, limited logging, insecure default settings, and legacy protocols to compromise multiple victims across critical infrastructure sectors.
- **Security by Design Imperative:** The advisory emphasizes shifting the cybersecurity burden from owners/operators to manufacturers by implementing Secure by Design principles in OT products. This approach builds security into products from the beginning rather than requiring costly retrofitting by end users.
- **12 Key Security Elements:** When procuring OT products, owners and operators should select manufacturers who prioritize: Configuration Management, Logging in Baseline Products, Open Standards, Ownership, Protection of Data, Secure by Default configurations, Secure Communications, Secure Controls, Strong Authentication, Threat Modeling, Vulnerability Management, and Upgrade/Patch Tooling.
- **Strategic Impact:** By enforcing purchasing decisions that require these security elements, critical infrastructure organizations can mitigate current and emerging cyber threats, create a path away from legacy environments, and send a clear market signal to manufacturers to stimulate the supply of Secure by Design products

**Read more at: Microsoft Releases January 2025 Security Updates**

## SECURITY CONSIDERATIONS FOR EDGE DEVICES

- **Edge devices like VPNs, firewalls, and routers are primary targets for sophisticated threat actors who exploit vulnerabilities, misconfigurations, and default settings to gain unauthorized network access.**
- **Organizations must implement comprehensive mitigation strategies including timely patching, strong multi-factor authentication, detailed logging of administrative actions, and regular security rule reviews.**
- **Security architecture should incorporate out-of-band management networks, zero trust principles, complete device inventories, and proactive management of end-of-life equipment to reduce attack surfaces.**
- **Device manufacturers should adopt secure-by-design principles throughout development, deliver products in secure default configurations, and provide transparent vulnerability reporting with timely security patches.**

**Read more at: CISA Security Considerations for Edge Devices**