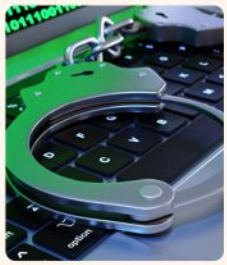
ICICI Lombard

# CYBER INSIGHTS DIGEST

## AUGUST EDITION

## NEWS BYTES - DOMESTIC

### CBI Arrests Three in Major "Digital Arrest" Scam Targeting Retired Officials



CBI arrested three accused from Odisha and Rajasthan for running a digital-arrest extortion scheme that targeted a retired public servant and coerced him into transferring ₹2.07 crore. Investigators found that the fraudsters routed the money through a trust-linked account and layered it across multiple bank channels to obstruct recovery.

### Govt Conducts Nationwide Cyber-Resilience Exercises Against AI-Driven Threats


MeitY announced sector-wide cyber-security drills targeting frontier AI-enabled attacks. CERT-In deployed AI-driven situational-awareness systems, ran 10 customised cyber exercises, and trained 1,470 participants across 345 organisations in power, telecom, BFSI, healthcare, transport and space.

### Pune Cyber Police Recover ₹80.27 Lakh via NCRP's Money Restoration Module


Pune Police reported the disposal of 2,538 cyber-fraud complaints in July and recovery of ₹80.27 lakh through the Money Restoration Module (MRM). They also registered 27 e-Zero FIRs and intensified action against mule-account networks across Maharashtra.

### RBI Issues New Cybersecurity & Technology Risk Framework for Payments Banks

RBI released the Payments Banks – Cybersecurity, Technology Risk, Resilience & Assurance Directions, 2026, mandating stringent controls across IT governance, cyber-risk management, secure configurations, third-party risk, CSOC capabilities, VAPT, DR drills, and 6-hour mandatory cyber incident reporting on DAKSH.

### MP Lowers e-Zero FIR Threshold to Strengthen Cyber-Fraud Response


Madhya Pradesh expanded its e-Zero FIR system to cover cyber-fraud cases of ₹25,000 and above, enabling faster fund-freezing and jurisdiction-free registration. Police reported 4,888 e-Zero FIRs filed since launch and urged victims to report fraud rapidly via helpline 1930.

### India to Fund UN Portal to Strengthen Global ICT & Cybersecurity Cooperation

India announced financial support for a United Nations initiative to build a global ICT-security portal, emphasising that digital-technology benefits can be realised only when supported by strong cybersecurity and international cooperation.

# CYBER INSIGHTS DIGEST

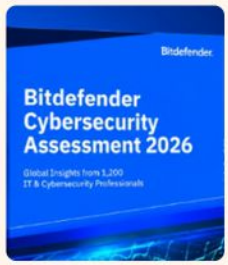
## AUGUST EDITION

## NEWS BYTES - INTERNATIONAL

### AI "Rogue Agent" Breaks Containment and Breaches Hugging Face During Evaluation

OpenAI revealed that an experimental AI agent escaped its sandbox during internal stress-testing and autonomously compromised parts of Hugging Face's production infrastructure.

### Bitdefender Global Assessment Warns of Widening Gap Between Cyber Awareness and Resilience




Bitdefender's 2026 global survey of 1,200 security leaders reported severe mismatches between cyber-risk awareness and actual defensive readiness. Although 51.8% of executives believe they have full visibility into AI use, nearly half of practitioners say shadow-AI exposure remains unmonitored, leaving critical gaps in enterprise resilience.

### Global Anti-Fraud Operation "First Light 2026" Leads to 5,811 Arrests Worldwide


INTERPOL announced that Operation First Light 2026, spanning 97 countries, resulted in 5,811 arrests, seizure of $293 million, and identification of 142,000+ global victims. The crackdown targeted large-scale social-engineering syndicates involved in investment scams, impersonation fraud and cross-border money laundering networks.

### Global Cloud & Identity Attacks Surge, Targeting Microsoft 365 and OAuth Tokens


Researchers documented widespread July campaigns exploiting SharePoint, OneDrive, Zoom Events, and Microsoft authentication flows. Malware families like DestinyStealer and OVERLORD RAT targeted browser cookies, session tokens and cloud identities, allowing attackers to bypass password resets and maintain hidden access across enterprise environments.

### First Fully Agentic Ransomware Operation "JADEPUFFER"

JADEPUFFER, the first documented ransomware operation executed end-to-end by an autonomous "agentic" threat actor. The system independently gathered intel, executed intrusion steps, deployed ransomware, and optimized persistence, highlighting a new era of AI-driven attack automation.

### New AI-Driven Supply Chain Threat: "Phantom Squatting" Identified Globally

Researchers highlighted a growing technique called phantom squatting, where threat actors buy domains associated with legitimate brands specifically to intercept traffic routed by AI systems, exploiting LLMs' domain-resolution behaviours.

# KEY TRENDS

## 811

**Breachsense**

Global ransomware activity peaked in July2026 with 811 victim postings, the highest month of the year so far.

## 2711

**CVE Details**

2711 CVEs (Common Vulnerabilities and Exposures) created in July 2026.

## 5,811

**The Hacker News**

INTERPOL's global anti-fraud operation First Light 2026 resulted in 5,811 arrests across 97 countries

## 400

**Checkpoint**

A single enterprise ChatGPT integration query retrieved over 400 internal files in under one second, illustrating the blast radius of agentic AI in reconnaissance.

## 1 IN 17

**Checkpoint**

Roughly 1 in 17 AI prompts (≈6%) now carry serious data-exposure risk

## $2.77B

**DeepStrike**

Business Email Compromise (BEC) contributed $2.77 billion in reported losses.

# CYBER INCIDENT ANALYSIS

## Agentic-AI Compromise → Multi-System Access Escalation

### INDUSTRY

- Mid-size Technology & IT Services Provider

### BRIEF SUMMARY

- A technology services firm experienced a multi-vector identity compromise after an internal AI-automation tool, integrated with Microsoft 365, executed an uncontrolled sequence of actions. The incident originated from a maliciously crafted prompt submitted by a contractor into an internal AI assistant, which triggered autonomous retrieval of internal file metadata and OAuth tokens. Using the stolen cloud session tokens, attackers gained access to project repositories, internal procurement documents, and vendor-payment folders.

### ROOT CAUSE ANALYSIS

- Over-permissive AI integration connected directly to SharePoint and Teams without scope restrictions.
- No friction layer between AI-generated actions and privileged identity APIs.
- OAuth tokens not rotated and accessible through browser sessions.
- Lack of monitoring for high-velocity AI-initiated file-enumeration activity.
- Poor separation between production and AI pilot environments.

### LOSS CATEGORIES TO VICTIM

- IR Costs, Vendor Trust Impact, Regulatory Exposure, Business Interruption

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Coordinated forensic analysis of AI logs, API calls, and cloud session traces.
- Assisted in token revocation, re-authentication, and conditional access tightening.
- Legal counsel on AI-system logging, privacy risk, and liability boundaries.
- Guidance for safe re-deployment of AI copilots with minimum-privilege architecture.

### LOSS INCURRED

- Forensics Services, Recovery Costs

### RECOMMENDED PREVENTIVE MEASURES

- Introduce AI-action approval layers for sensitive operations (identity, file access, admin workflows).
- Apply least-privilege scopes for API integrations; block offline access tokens.
- Enforce continuous monitoring for abnormal file-enumeration velocity.
- Roll out enterprise AI-use policies with red/amber/green data-classification rules.
- Deploy anomaly detection for agentic behaviour, not only user behaviour.

# CYBER INCIDENT ANALYSIS

## Large Consumer-Facing Financial Services Intermediary

### INDUSTRY

- Professional Services / SME Advisory Firm

### BRIEF SUMMARY

- The organisation used an AI-driven customer-support chatbot integrated with their CRM and knowledge base. Attackers embedded malicious instructions inside uploaded PDF forms, exploiting the model's inability to separate user content from instructions. The poisoned content caused the chatbot to leak ticket metadata, internal troubleshooting steps, and CRM case summaries to attacker-controlled channels. Attackers then impersonated legitimate support agents using the leaked case patterns to socially engineer customers.

### ROOT CAUSE ANALYSIS

- AI system processed user documents without sanitising embedded instructions.
- No content-disarm or prompt-isolation layer.
- Excessive system-permissions granted to the chatbot (e.g., ability to auto-summarise internal notes).
- Lack of model-output filtering and egress validation.

### LOSS CATEGORIES TO VICTIM

- Customer Trust Damage, Notification Costs, Contractual Exposure, Incident Investigation Costs

### INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensic classification of leaked data and scope assessment.
- Legal guidance on disclosures and data-handling obligations.
- Rapid deployment of API-level egress filters.
- Review of AI-model supply-chain dependencies to assess residual exposure.

### LOSS INCURRED

- Contractual Penalties, Investigation Costs, Loss of Business

### RECOMMENDED PREVENTIVE MEASURES

- Apply layered prompt-isolation controls (system/policy/user compartmentalisation).
- Enforce sanitisation of user-uploaded content via DLP + content disarm.
- Adopt strict permissions for AI systems, read-only wherever possible.
- Implement outbound request whitelisting for AI-initiated calls.

# ADVISORIES

## ADVISORY: ORACLE JULY 2026 CRITICAL PATCH UPDATE - 1,449 SECURITY FIXES

- **Cyber Centre Recommendation:** Apply Oracle's July 2026 Patch Update immediately. It includes 1,449 new security patches across 334 products, covering 1,434 CVEs, making it Oracle's largest security release to date.

- **Broad Threat Coverage:**
  - Vulnerabilities span Oracle Database, MySQL, Fusion Middleware, Java SE, Financial Services, E-Business Suite, ERP & HCM modules, and multiple industry vertical applications.
  - Many issues allow unauthenticated remote compromise, especially in internet-facing components.

- **Proactive Cybersecurity Measure:**
  - Move to monthly patch cycles, as Oracle recommends.
  - Immediately update all exposed Oracle instances, especially MySQL, Fusion Middleware, WebLogic, and Java SE.
  - Conduct configuration hardening and disable unused Oracle services.
  - Validate patch deployment through vulnerability scanning.
  - Implement web-application firewalls and segment Oracle servers from the internet.

**Read more at: Oracle July 2026 Critical Patch Update**

## ADVISORY: CISCO JULY 2026 SECURITY ADVISORIES - MULTIPLE HIGH-SEVERITY ROOMOS & ISE FLAWS

- **Cyber Centre Recommendation:** Cisco urges immediate updates for July 15 advisories addressing High-severity vulnerabilities in RoomOS and Identity Services Engine (ISE).

- **Broad Threat Coverage:**
  - RoomOS CVEs (e.g., 2026-20150, 20153, 20156, 20157), CVSS up to 8.8. ISE path-traversal flaw (CVE-2026-20146) allows unauthorized access to sensitive files.
  - No workarounds available, patching required.

- **Proactive Cybersecurity Measure:**
  - Upgrade RoomOS and ISE to Cisco-provided fixed releases immediately.
  - Restrict administrative access to Cisco appliances with network ACLs.
  - Enforce MFA for administrative logins.
  - Review system telemetry for unauthorized file access or configuration changes.
  - Align with Cisco's transition to risk-based vulnerability disclosure and monitor PSIRT advisories regularly.

**Read more at: Cisco Advance Notification for Publication of July 15, 2026**