



CYBER INSIGHTS DIGEST

SEPTEMBER EDITION

NEWS BYTES - DOMESTIC

ED Arrests Two in ₹30,000-Crore Pan-India Cyber-Fraud & Digital-Arrest Network



Enforcement Directorate arrested two individuals in Mumbai for their role in a massive cyber-fraud and digital-arrest syndicate involving ₹27,000 crore in suspected bank transactions and ₹3,000 crore in cash dealings. ED investigations revealed over 300 victim complaints and 150–160 FIRs linked to the network across 20 States.

India Orders Google to Takedown Firebase Infrastructure Used in Banking Malware Campaigns



India's I4C directed Google to remove 57 Firebase-hosted malicious websites and databases used by cybercriminals to impersonate Indian banks (SBI, ICICI, Axis) and government schemes. The malware campaigns targeted Android users to steal banking credentials, highlighting shifts towards abuse of legitimate cloud infrastructure.

Supreme Court Issues Fresh Directions to Curb Digital-Arrest Scams



Supreme Court mandated new safeguards for cyber-fraud victims, including faster restoration of defrauded funds and a uniform SOP for banks to temporarily hold suspicious mule-linked accounts. The Court noted fraud recoveries of ₹18.05 crore across 36,290 cases via national restoration mechanisms.

India Introduces New Cybersecurity Regulations for Power-Sector OT/IT Systems



Central Electricity Authority (CEA) issued India's new cybersecurity framework for the power sector, mandating OT-focused controls, network segregation, trusted procurement, incident reporting, asset inventories, and mandatory cybersecurity audits for power-generation, transmission, and distribution firms.

India's Cybersecurity Threat Surface Expands Amid 265 Million Annual Attacks



New national threat-intelligence reporting highlighted India's exposure to 265 million cyberattack attempts and 369 million malware detections in 2025. CERT-In handled 29.44 lakh cyber incidents, underscoring a rapidly growing attack surface driven by UPI expansion, Aadhaar authentication, and large-scale digital-public-infrastructure growth.

SEBI Launches IT Resilience Index to Strengthen Market Infrastructure Institutions' Cyber Posture



SEBI introduced a new IT Resilience Index (ITRI) for Market Infrastructure Institutions (MIIs) to quantify cyber readiness. SEBI emphasized that disruptions in core IT systems can jeopardize national market stability, making board-level oversight mandatory.



CYBER INSIGHTS DIGEST

SEPTEMBER EDITION

NEWS BYTES - INTERNATIONAL

U.S. Agencies Warn of AI-Powered Attacks Targeting Siemens Industrial PLCs



U.S. federal agencies warned that attackers are using AI-generated scripts to compromise Siemens S7 Series PLCs deployed across critical infrastructure such as water, energy, and industrial manufacturing. Threat actors used tools like Censys and ZoomEye to locate exposed PLCs and leveraged read-access to map environments for future disruptive write operations.

Global AI Regulation Tightens: EU AI Act High-Risk Systems Enforced



The EU activated new AI transparency obligations requiring providers and deployers to clearly label AI-generated or AI-manipulated content. Enforcement will be carried out by national market-surveillance authorities, the EU AI Office, and the European Data Protection Supervisor, with penalties up to €15 million or 3% of global turnover.

GitLab CVE-2026-19478 (CVSS 9.4) Actively Exploited to Rewrite Public Projects



Researchers confirmed active exploitation of CVE-2026-19478, a critical GitLab code-injection flaw enabling attackers to modify or delete public repositories without authentication. The vulnerability allows manipulation of project data with no user interaction, posing high risk for supply-chain contamination and open-source ecosystem compromise.

Oracle PeopleSoft Zero-Day Exploited by ShinyHunters



The U.S. President issued a memorandum directing national agencies to integrate private-sector offensive cyber capabilities into efforts against transnational cyber-enabled crime. The policy aims to counter large organized fraud networks by leveraging industry tools, intelligence pipelines, and coordinated federal oversight.

Netherlands Implements New National Cybersecurity Act (CbW) Aligning with NIS2



covering August enforcement, the Netherlands' new Cyberbeveiligingswet (CbW) formally came into effect on 15 August 2026 with no grace period. The Act transposes NIS2 into Dutch law and introduces stricter organisational obligations for entities in finance, telecom and critical infrastructure.

Suspected China-Nexus APT Exploits VMware vCenter CVE-2026-59310 (CVSS 9.8)



a China-linked APT exploited a newly patched directory-traversal flaw in VMware vCenter, deploying Babuk-derived ransomware as a "smokescreen" to hinder forensics. The attack chain included default credential abuse, reverse SSH channels, and privilege escalation.

KEY TRENDS

2,422

Checkpoint

Organisations experienced an average of 2,422 cyberattacks per week in August, up 4% from July and 22% year-on-year

3201

CVE Details

3201 CVEs (Common Vulnerabilities and Exposures) created in August 2026.

1,042

Checkpoint

1,042 ransomware attacks in August, an 8% monthly increase and almost double the August 2025 level

1 IN 112

Checkpoint

Email phishing frequency increased to approximately 1 in every 112 emails in August

83

Breachsense

Breachsense tracked 83 active ransomware groups, up sharply from 66 in July

369M

ET Government

India recorded approximately 369 million malware detections across 8.44 million endpoints

CYBER INCIDENT ANALYSIS

Third-Party AI Support Tool Misconfiguration → Customer Information Exposure

INDUSTRY

- Insurance / Financial Services

BRIEF SUMMARY

- An insurer deployed an AI-enabled customer-support platform integrated with its CRM, policy-administration system, and internal knowledge base. A configuration change granted the AI tool wider access than intended, allowing users to retrieve information from unrelated customer cases. A specially constructed query caused the platform to return policy summaries, claim references, and internal service notes outside the requester's authorized scope. Monitoring detected unusually high-volume retrieval activity, prompting suspension of the integration and revocation of affected API credentials.

ROOT CAUSE ANALYSIS

- Excessive API permissions granted to the AI support platform.
- Inadequate segregation between customer records and internal knowledge repositories.
- No output-level access validation before information was presented to users.
- Third-party configuration changes were deployed without security review.
- Limited logging of AI-initiated retrievals and machine-identity activity.

LOSS CATEGORIES TO VICTIM

- Potential Customer Data Exposure, Temporary Disruption, Legal & Regulatory Assessments, Reputational Exposure

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Engaged cloud and AI-forensics specialists to review prompts, API logs, and retrieved records.
- Supported token revocation, permission reduction, and isolation of the affected integration.
- Assisted legal counsel in determining the notification population and regulatory implications.
- Coordinated third-party vendor engagement and preservation of relevant evidence.

LOSS INCURRED

- Forensic Costs, Legal Expenses, Customer Support Disruption, AI-Platform Remediation

RECOMMENDED PREVENTIVE MEASURES

- Apply least-privilege access to AI tools, plugins, APIs, and service accounts.
- Enforce record-level authorization independently of the AI model's output.
- Separate customer data, internal documentation, and public knowledge sources.
- Introduce human approval for sensitive searches and bulk information retrieval.
- Monitor AI agents for abnormal query velocity, data volume, and access patterns.
- Include AI security, audit rights, incident reporting, and indemnity provisions in vendor contracts.

CYBER INCIDENT ANALYSIS

AI-Assisted Vendor Impersonation → High-Value Payment Diversion

INDUSTRY

- Engineering & Infrastructure Services

BRIEF SUMMARY

- A finance employee received messages impersonating the company's managing director, requesting an urgent payment for a confidential acquisition-related transaction. The attackers used publicly available executive information, a cloned profile image, and AI-generated voice messages to strengthen the impersonation. The employee transferred funds to a newly added beneficiary after receiving fabricated supporting documents and approval messages. The fraud was detected when the genuine executive denied authorizing the transaction. Rapid reporting enabled the bank to freeze a substantial portion of the transferred funds.

ROOT CAUSE ANALYSIS

- Payment approval relied on messaging and voice confirmation without independent verification.
- No mandatory callback to a verified number for urgent or confidential transactions.
- Weak controls around first-time beneficiaries and exceptional payment requests.
- Employee training did not sufficiently cover AI-generated voice and executive impersonation.

LOSS CATEGORIES TO VICTIM

- Direct Financial Loss, Legal and Fund Recovery Expenses, Reputational Impact

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Coordinated forensic review of messages, email headers, devices, and payment records.
- Supported immediate escalation to banks and law-enforcement authorities for fund tracing and freezing.
- Engaged crisis and legal advisers to assess notification and governance obligations.
- Assisted with documenting the incident for auditors, the board, and insurers.
- Reviewed payment controls and recommended short-term fraud-prevention measures.

LOSS INCURRED

- Diverted Funds, Forensic and Legal Costs

RECOMMENDED PREVENTIVE MEASURES

- Require out-of-band verification for urgent payments and beneficiary changes.
- Enforce dual approval for high-value, confidential, or first-time transactions.
- Use verified corporate channels and digitally signed approval documents.
- Introduce transaction-risk scoring for abnormal value, timing, and destination.
- Train finance teams to recognise deepfake voice, video, and executive impersonation.
- Maintain a rapid-response process involving the bank, helpline 1930, and law enforcement.

ADVISORIES

ADVISORY: CRITICAL CITRIX NETSCALER AUTHENTICATION BYPASS AND MEMORY OVERFLOW

- **Cyber Centre Recommendation:** Immediately update affected Citrix NetScaler ADC and NetScaler Gateway appliances, prioritising internet-facing VPN, AAA virtual server and SAML-enabled deployments.
- **Broad Threat Coverage:**
 - CVE-2026-19490, rated CVSS 9.3, is an alternate-path authentication bypass affecting certain Gateway, AAA and SAML configurations.
 - CVE-2026-19489, rated CVSS 8.8, is a memory-overflow vulnerability that may cause unpredictable behavior or denial of service.
- **Proactive Cybersecurity Measure:**
 - Upgrade NetScaler 14.1 to 14.1-73.32 or later and 13.1 to 13.1-63.21 or later.
 - Restrict management interfaces to authorised networks.
 - Review Gateway, AAA and SAML configurations and monitor for abnormal authentication activity.
 - Terminate active sessions after patching where operationally feasible.

Read more at: CERT-EU Security Advisory 2026-010

ADVISORY: CRITICAL CISCO CROSSWORK AND SECURE WORKLOAD VULNERABILITIES

- **Cyber Centre Recommendation:** Apply the fixed software released by Cisco on 19 August 2026 for Crosswork and Secure Workload environments. The vendor classified both security-hardening releases as Critical, with maximum CVSS scores of 10.0, and stated that no workarounds were available.
- **Broad Threat Coverage:**
 - The Crosswork release addresses four CVEs, including CVE-2026-20030 and CVE-2026-20357 through CVE-2026-20359.
 - The Secure Workload release addresses five CVEs, including CVE-2026-20231 and CVE-2026-20315 through CVE-2026-20319.
 - Additional August fixes covered BroadWorks, contact-centre products, RoomOS and industrial Ethernet switches.
- **Proactive Cybersecurity Measure:**
 - Upgrade affected Crosswork and Secure Workload deployments immediately.
 - Restrict administrative interfaces through ACLs and trusted management networks.
 - Enforce MFA and review privileged-user activity.
 - Monitor configuration changes, API access and unexpected administrative sessions.

Read more at: Cisco August 19 Security Advisory Publication