CYBER INSIGHTS DIGEST

May Edition

NEWS BYTES - DOMESTIC

CERT-In Flags High-Severity AI Cyber Risks for Organisations and MSMEs

CERT-In warned that frontier AI can automate vulnerability discovery, exploit chaining, reconnaissance, and multilingual phishing at scale. The advisory urges organisations and MSMEs to strengthen monitoring, patching, access controls, and cyber resilience

India's Cybersecurity Market Projected to Reach $15.06 Billion by 2031

Industry officials said India's cybersecurity market may grow from $6.56 billion in 2026 to $15.06 billion by 2031, driven by digitisation, AI-enabled threats, and rising investment in advanced defence solutions.

Operation Octopus 2.0: 52 Arrested in Pan-India Cyber Fraud Crackdown

Hyderabad Police arrested 52 people, including 32 bank officials, across nine States. Investigators linked around 350 bank accounts to nearly 850 cybercrime cases involving approximately ₹150 crore in transactions.

Delhi Police Bust ₹300 Crore International Cyber Fraud Syndicate

Delhi Police busted a cyber fraud syndicate linked to over 2,500 complaints and ₹300 crore in scams. The network used fake trading apps, mule accounts, shell firms, and Cambodia-linked operators.

WhatsApp Says 9,400 Accounts Banned After Digital Arrest Probe

WhatsApp told the Supreme Court it banned 9,400 accounts linked to "digital arrest" and law-enforcement impersonation scams. The platform said government inputs were used to map and disrupt wider scam networks.

Gemini to Meta: Deepfake Gang Used AI to Hijack Identities in Gujarat

Ahmedabad Police arrested four accused for using AI-generated deepfake videos to bypass Aadhaar-linked liveness checks, change mobile numbers, access DigiLocker, and open fraudulent bank accounts and loans

NEWS BYTES - INTERNATIONAL

Europol Releases IOCTA 2026 Highlighting AI-Driven Cybercrime Surge

Europol's flagship IOCTA report warns that AI, encryption, and cybercrime-as-a-service are accelerating global cybercrime. It highlights a widening "velocity gap" where automated attacks outpace law-enforcement capabilities.

April 2026 Cyber Update Flags Surge in Zero-Day Exploits and Hacktivism

Global cyber activity was marked by critical zero-day vulnerabilities (e.g., Chrome CVE-2026-5281) and rising hacktivist activity targeting 16 countries, with DDoS, defacement, and "hack-and-leak" operations escalating.

CISA Issues Advisory on Iranian APT Targeting Industrial Control Systems

The joint advisory warns of Iran-linked actors exploiting PLC devices across U.S. critical infrastructure. The attacks manipulate HMI/SCADA systems, causing operational disruption and potential financial loss.

Global Cybersecurity Incidents Report Highlights Rise in Transnational Cyber Fraud

The report emphasises the growing cross-border nature of cyber fraud operations involving coordinated networks across Asia and Europe, reinforcing the need for international law-enforcement collaboration.

Cyber Threats Spike Globally in April as Attack Volumes Rise

Analysis shows global cyber-attacks rose to ~2,201 weekly incidents per organisation, up 10% MoM. Education, government, and telecom sectors were most targeted amid growing ransomware and AI-driven threat activity.

CISA Expands Known Exploited Vulnerabilities (KEV) Catalogue Amid Rising Threat Activity

CISA expanded its KEV catalogue with multiple actively exploited vulnerabilities, issuing strict remediation timelines. The move highlights escalating global threat activity and increasing urgency for rapid patch management across organisations

ICICI Lombard

KEY TRENDS

2,201

Checkpoint

Organizations faced an average of 2,201 cyberattacks per week in April 2026

6455

CVE Details

6455 CVEs (Common Vulnerabilities and Exposures) created in April 2026.

105

Flashpoint

At least 105 publicly disclosed ransomware attacks were recorded in April, the highest April level since 2020.

4,946

Checkpoint

The education sector recorded 4,946 weekly attacks per organisation, making it the most targeted industry globally.

70

BreachSense

Over 70 active ransomware groups operated globally during April 2026.

$10.5T

CybelAngel

Global cybercrime costs are projected to exceed $10.5 trillion in 2026, making cybercrime the world's third-largest "economy."

CYBER INCIDENT ANALYSIS

Unauthorized Cloud Storage Upload → Customer Data Exposure Risk

INDUSTRY

- Insurance / Digital Policy Platform

BRIEF SUMMARY

- An attacker exploited misconfigured S3 bucket on a cloud function used for user-uploaded documents. They uploaded a malicious archive and gained access to sensitive customer information (IDs, claim forms). The issue was detected after abnormal file-read spikes triggered cloud monitoring alerts.

ROOT CAUSE ANALYSIS

- Incomplete bucket access permissions allowed unauthenticated upload/download.
- No validation processes on uploaded files or source origins.
- Weak cloud monitoring and alerting thresholds for file-access anomalies.
- No separation between testing and production storage; cloud IAM roles overly permissive.

LOSS CATEGORIES TO VICTIM

- Unauthorized Data Exposure, Compliance Penalties, Operational Impact, Customer Trust

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Arranged for forensic review: IAM roles, log collection, and remediation scope.
- Isolated affected buckets, revoked public access, and locked down permissions.
- Guided client on notification requirements and data-subject communication.
- Arranged cloud-architecture hardening and monitoring policy redefinitions.

LOSS INCURRED

- IR / Forensics + Restoration Services, Potential Regulatory Costs, Legal Costs

RECOMMENDED PREVENTIVE MEASURES

- Enforce least-privilege IAM roles; disable public access by default.
- Deploy object-level logging and alert thresholds for anomalous activity.
- Implement pre-processing validation: file-type & size restrictions with antivirus scanning.
- Employ automated compliance scans for bucket configuration drift.
- Conduct periodic pentests and cloud configuration reviews with CI/CD integration.

CYBER INCIDENT ANALYSIS

Deep Fake Enabled KYC Bypass → Fraudulent Loan Origination

INDUSTRY

- NBFC / Digital Lending Platform

BRIEF SUMMARY

- A digital lending platform experienced a fraud incident where threat actors bypassed its remote KYC process using AI-generated deep-fake video identities. Attackers used stolen personal data (PAN/Aadhaar details sourced from prior breaches) to create synthetic onboarding profiles. During video-KYC verification, they deployed deepfake facial overlays to pass liveness checks and complete account onboarding. Multiple unsecured loans were disbursed to mule accounts before anomaly detection flagged unusual borrower behavior and repayment defaults.

ROOT CAUSE ANALYSIS

- KYC verification relied heavily on video-based liveness checks without deepfake-detection capabilities.
- Weak binding between identity (KYC) and device/session used during onboarding.
- Absence of behavioral profiling to flag multiple applications from similar device/IP patterns.
- Delayed detection due to lack of real-time linkage between onboarding and fraud-risk scoring engines.

LOSS CATEGORIES TO VICTIM

- Financial Loss, Credit Risk Inflation, Reputational Impact, Regulatory Exposure

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Conducted forensic review of KYC session recordings and onboarding logs to identify synthetic identity patterns.
- Helped isolate impacted loan accounts and coordinate recovery actions with banking partners.
- Supported enhancement of fraud controls, including deepfake-detection tooling and transaction risk scoring.
- Provided advisory on regulatory exposure related to KYC/AML compliance and audit readiness.

LOSS INCURRED

- Regulatory Penalties, Regulatory Costs, Monetary Loss

RECOMMENDED PREVENTIVE MEASURES

- Deploy deepfake-detection and biometric anomaly detection in video KYC workflows.
- Strengthen identity binding through device fingerprinting, geo-intelligence, and session validation.
- Integrate real-time fraud scoring before loan disbursal, not only post-KYC.
- Implement velocity checks for multiple onboarding attempts across similar identifiers (device/IP/biometrics).
- Introduce step-up authentication (physical verification / small-ticket test disbursement) for high-risk profiles.

ADVISORIES

ADVISORY : CRITICAL CHROME ZERO-DAY EXPLOITED IN THE WILD (CVE-2026-5281)

- **Cyber Centre Recommendation:** Immediately enforce Chrome updates across all enterprise endpoints and restrict usage of outdated browser versions.

- **Broad Threat Coverage:**
  - Google patched a zero-day vulnerability (CVE-2026-5281) on April 1–3, 2026, confirmed as actively exploited in the wild.
  - The flaw enables remote code execution via crafted web pages and was added to the CISA Known Exploited Vulnerabilities (KEV) list with mandatory patch timelines.
  - Risk exposure is massive, affecting Chrome's ~3.5 billion global users, making it one of the highest-impact endpoint vulnerabilities of the month.

- **Proactive Cybersecurity Measure:**
  - Force browser auto-updates via enterprise policy (GPO / MDM).
  - Restrict web access using secure web gateways for unmanaged devices.
  - Monitor unusual browser child-process execution or abnormal scripts.

Read more at: Forbes

ADVISORY : APT TARGETING INDUSTRIAL CONTROL SYSTEMS (ICS/OT)

- **Cybersecurity Review Recommendation:** Immediately isolate OT systems from internet exposure and review PLC network configurations across critical infrastructure.

- **Broad Threat Coverage:**
  - On April 7, 2026, CISA, FBI, NSA, and US Cyber Command jointly issued a high-severity advisory on Iran-affiliated actors targeting PLC devices.
  - Attacks specifically targeted industrial control systems (ICS) used in energy, water, and critical infrastructure.
  - Adversaries manipulated SCADA and HMI systems, resulting in operational disruption and potential physical consequences

- **Proactive Cybersecurity Measure:**
  - Remove direct internet exposure to PLCs and ICS devices.
  - Deploy network segmentation between IT and OT environments.
  - Monitor ICS-specific ports (e.g., 44818, 502, 2222) for anomalous traffic.
  - Validate logs against Indicators of Compromise (IOCs) released in the advisory.

Read more at: CISA Advisory