CYBER INSIGHTS DIGEST

June Edition

NEWS BYTES - DOMESTIC

CERT-In Releases Blueprint to Counter AI-Assisted Cyber Threats

CERT-In's blueprint advises organizations to defend against AI-assisted cyber threats through AI asset inventories, stricter patching, deep-fake readiness, vulnerability management, log preservation, and governance for shadow AI usage.

Financial Institutions Report 10,114 Fraud Cases Worth ₹48,021 Crore in FY26

RBI data showed banks and financial institutions reported 10,114 fraud cases involving ₹48,021 crore in FY26. While case counts declined from FY25, fraud value increased, with advances forming the largest value category.

Indian Government, Tech Firms Testing Critical Software Against Mythos AI Risk

Indian authorities and major technology firms reportedly began testing critical financial and government software against risks from Anthropic's Mythos AI. CERT-In is examining key digital infrastructure, including Aadhaar and government login systems.

MHA's I4C and RBI Innovation Hub Sign MoU to Crack Down on Mule Accounts

I4C and RBI Innovation Hub signed an MoU to improve detection of mule accounts using AI-driven systems such as MuleHunter.ai. The collaboration will enable fraud-risk intelligence sharing and strengthen cyber fraud prevention across India's banking and digital payments ecosystem.

66 Held in Hyderabad Police Crackdown on 'Ghost SIM' Cyber Fraud Network

Hyderabad Police arrested 66 people under Operation Octopus 3.0, targeting ghost SIM networks enabling cyber fraud. Police identified 1194 linked SIMs, seized 544 SIM cards, and connected the network to ₹101.87 crore in fraud.

Fake Call Centres Duping US Citizens Busted in Bengaluru

Karnataka State Cyber Command busted fake Bengaluru call centres impersonating a US accounting software firm. The operators allegedly offered fake tax help, licence renewals, and software keys while routing proceeds through shell companies.

NEWS BYTES - INTERNATIONAL

INTERPOL Operation Ramz: 201 Arrests in First MENA Cybercrime Operation

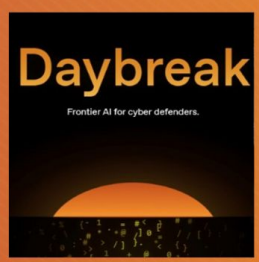
INTERPOL's first large-scale MENA cybercrime operation led to 201 arrests, 382 additional suspects identified, 3,867 victims traced, and 53 servers seized. The operation targeted phishing, malware, and cyber-scam infrastructure across 13 countries.

CISA Adds Two Exploited Microsoft Defender Zero-Days to KEV

CISA added two actively exploited Microsoft Defender flaws to KEV: CVE-2026-41091 for privilege escalation and CVE-2026-45498 for denial-of-service. The alert underscores attacker focus on compromising security tools themselves.

Eurojust & Europol Shut Down Criminal VPN Network "First VPN"

French and Dutch authorities, supported by Eurojust and Europol, dismantled First VPN, a criminal VPN service used to hide ransomware and hacking activity. Authorities took down 33 servers and accessed operational user data before shutdown.

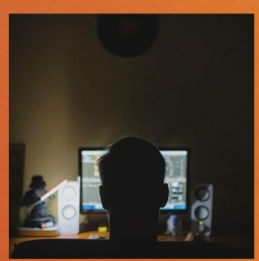


OpenAI Launches Daybreak for AI-Powered Cyber Defence

OpenAI launched Daybreak, combining frontier AI models and Codex Security to help defenders perform secure code review, threat modelling, patch validation, dependency-risk analysis, and remediation guidance earlier in the software development cycle.

Microsoft Exchange Server CVE-2026-42897 Exploited via Crafted Email

Microsoft confirmed active exploitation of CVE-2026-42897 affecting on-prem Exchange OWA. A crafted email opened in Outlook Web Access could execute JavaScript in the browser context; Exchange Online was not impacted.



TeamPCP Targets Open-Source Software and AI Tools

Researchers profiled TeamPCP, a financially motivated group linked to repeated software supply-chain attacks against open-source tools, developer extensions, and AI-adjacent ecosystems. The coverage highlights rising risk from poisoned packages and compromised developer tooling.

KEY TRENDS

2,055

Checkpoint

Organizations faced an average of 2,055 cyberattacks per week in May 2026.

3670

CVE Details

3670 CVEs (Common Vulnerabilities and Exposures) created in May 2026.

48%

Checkpoint

Ransomware incidents surged 48% year-on-year in May 2026.

1 IN 25

Checkpoint

Check Point found that 1 in every 25 GenAI prompts from enterprise networks carried high risk of sensitive data leakage.

646

BreachSense

Breachsense tracked 646 ransomware victims across leak sites in May 2026.

96%

BlackFrog

Ransomware data exfiltration occurred in 96% of attacks in Q1 2026. That figure has held at critically high levels since 2025

CYBER INCIDENT ANALYSIS

Fake Support Centre Impersonation → Cross-Border Payment Fraud

INDUSTRY

- IT-enabled Services / BPO Operations

BRIEF SUMMARY

- A technology-support services setup was misused to run fraudulent outbound calls targeting overseas customers. Call agents impersonated a reputed accounting/software support provider and offered fake tax assistance, licence renewals, and software keys. Victims were induced to pay "service charges," while proceeds were routed through shell entities and multiple bank accounts. The incident came to light after cyber police raids in May 2026 uncovered multiple fake call-centre locations, scripts, devices, and suspected payment-routing infrastructure.

ROOT CAUSE ANALYSIS

- Weak governance over call-centre operations and client-verification processes.
- Use of scripted impersonation and fake identities to gain customer trust.
- Lack of monitoring over employee calling activity, call scripts, and payment collection channels.
- Shell entities and layered bank accounts used to obscure fund movement.
- Inadequate internal red-flag monitoring for unusual call volumes and overseas payment patterns.

LOSS CATEGORIES TO VICTIM

- Legal & Regulatory Exposure, Investigation Costs, Reputational Damage, Potential Financial Loss

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensic review of endpoints, call records, scripts, CRM tools, and payment-routing logs.
- Legal support for regulatory and law-enforcement engagement.
- Crisis communication support to manage stakeholder and customer-facing impact.
- Assistance in mapping fund flows and identifying suspicious accounts or entities.
- Advisory on strengthening governance, employee monitoring, and fraud-prevention controls.

LOSS INCURRED

- IR / Forensics Services, Legal Costs, Monetary Loss

RECOMMENDED PREVENTIVE MEASURES

- Conduct enhanced due diligence on all clients, campaigns, and outsourced calling mandates.
- Implement call recording, keyword monitoring, and approval controls for customer-facing scripts.
- Restrict collection of payments through unapproved accounts or shell entities.
- Perform employee background checks and enforce access controls on calling tools.
- Monitor anomalous call volumes, repeated overseas targeting, and high-risk payment patterns.
- Establish internal whistleblower and escalation channels for suspected fraud activity.

CYBER INCIDENT ANALYSIS

Ghost SIM Network Abuse → Cyber Fraud Enablement

INDUSTRY

- Telecom Distribution / Digital Payments Ecosystem

BRIEF SUMMARY

- A telecom-linked fraud network allegedly enabled cybercriminals by supplying "ghost SIMs" used to conceal identities. Fraudulent SIMs were activated through misuse of customer eKYC, mobile number portability workflows, and bulk SIM distribution channels. These SIMs were later used to create fake social media accounts, receive OTPs, support mule-account operations, and facilitate cyber fraud. In May 2026, police identified 194 ghost SIMs linked to cybercrime, seized 544 SIM cards, and connected the network to fraud cases worth over ₹101 crore.

ROOT CAUSE ANALYSIS

- Weak oversight of point-of-sale agents and telecom promoters.
- Abuse of eKYC and mobile number portability workflows to activate additional SIMs without customer awareness.
- Poor reconciliation between SIM inventory, activation records, and customer consent logs.
- Limited anomaly detection for bulk activations, repeated Aadhaar-linked activity, and unusual eSIM conversions.
- Inadequate monitoring of downstream SIM usage in fraud-linked platforms and mule networks.

LOSS CATEGORIES TO VICTIM

- Regulatory Exposure, Customer Trust Impact, Legal Costs, Financial Liability

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensic review of SIM activation logs, eKYC records, POS activity, and device-linkage data.
- Legal advisory on customer identity misuse and regulatory reporting obligations.
- Support in coordinating with telecom providers, banks, and law-enforcement agencies.
- Incident response guidance for dealer network suspension, access revocation, and control remediation.
- Assistance in reviewing third-party risk exposure across POS agents and distribution partners.

LOSS INCURRED

- Regulatory Penalties, Regulatory Costs, Monetary Loss

RECOMMENDED PREVENTIVE MEASURES

- Implement dealer-level risk scoring and continuous monitoring of SIM activation behaviour.
- Flag unusual patterns such as bulk SIM activation, repeated eKYC attempts, and rapid eSIM conversions.
- Require stronger customer consent validation for mobile number portability and SIM issuance.
- Conduct periodic audits of POS agents, telecom promoters, and SIM distribution channels.
- Integrate fraud intelligence feeds to detect SIMs linked to mule accounts, OTP abuse, and scam platforms.
- Enforce penalties and access termination for agents violating onboarding or KYC norms.

ADVISORIES

ADVISORY : CRITICAL CPANEL & WHM AUTHENTICATION BYPASS - CVE-2026-41940

- **Cyber Centre Recommendation:** Immediately update all internet-facing cPanel & WHM and WP Squared instances to fixed versions. For systems that cannot be patched immediately, apply vendor-recommended mitigations such as blocking exposed cpsrvd service ports and applying ModSecurity rules.
- **Broad Threat Coverage:**
  - CVE-2026-41940 is a critical authentication-bypass vulnerability in cPanel & WHM's session management layer, allowing unauthenticated attackers to gain unauthorized access to the control panel.
  - The vulnerability carries a CVSS 9.8 Critical rating and affects cPanel & WHM versions after 11.40; CISA added it to the Known Exploited Vulnerabilities (KEV) catalogue on 1 May 2026.
- **Proactive Cybersecurity Measure:**
  - Patch cPanel/WHM immediately and verify version compliance across all hosting assets.
  - Run cPanel's detection script to check for indicators of compromise in session files.
  - Review admin account creation, webroot file changes, backup integrity, and outbound scanning/brute-force activity from affected servers.
  - Restrict cPanel/WHM access to trusted IPs and disable public exposure where not operationally required.

Read more at: cPanel

ADVISORY : ACTIVELY EXPLOITED LANGFLOW & TREND MICRO APEX ONE VULNERABILITIES

- **Cybersecurity Review Recommendation:** Prioritize remediation of exposed Langflow instances and on-premise Trend Micro Apex One servers, especially where these systems store credentials, API keys, security policies, or endpoint-management privileges.
- **Broad Threat Coverage:**
  - CVE-2026-34926 is a directory-traversal issue in Trend Micro Apex One that can allow malicious code injection into agents after server access is obtained, creating downstream endpoint-compromise risk.
  - CVE-2025-34291 is a CVSS 9.4 Langflow origin-validation flaw that can enable arbitrary code execution and full system compromise, with risk of exposing stored access tokens and API keys.
- **Proactive Cybersecurity Measure:**
  - Restrict administrative access to Apex One servers and review server-side integrity for unauthorized changes.
  - Rotate API keys, tokens, and secrets stored in or connected to Langflow workspaces
  - Hunt for suspicious code execution, unusual agent policy changes, unexpected endpoint tasks, and outbound connections from affected platforms.

Read more at: Hacker News