ICICI Lombard

CYBER INSIGHTS DIGEST

January Edition

NEWS BYTES - DOMESTIC

CERT-In Releases Critical Alert for Google Chrome Desktop Users

CERT-In flagged multiple high-severity vulnerabilities in Google Chrome. These flaws could let an attacker execute arbitrary code, steal sensitive information, escalate privileges, or bypass security restrictions, typically by luring a user to a specially crafted web page. Users / organizations are advised to update Chrome to the latest vendor-fixed version

Makop Ransomware Actively Targeting Indian Businesses (55% Victims in India)

Acronis reports Makop continues to compromise victims via exposed RDP. The campaign frequently involves reconnaissance, lateral movement tooling, and attempts to disable defenses before encryption, with India representing ~55% of observed victims, indicating concentrated targeting of Indian organizations.

CERT-In Issues High-Severity Vulnerability Alert in Microsoft Products

The linked CERT-In advisory covers multiple high-severity vulnerabilities in Microsoft products which could enable remote code execution, privilege escalation, information disclosure, security bypass, spoofing, or denial of service. CERT-In notes at least one listed vulnerability is being exploited in the wild and recommends applying Microsoft security updates from the official release notes/update guide

CERT-In warns of WhatsApp account takeover campaign "GhostPairing"

CERT-In warned of GhostPairing, a social-engineering campaign abusing WhatsApp's device-linking flow to silently add attacker devices, enabling message access and impersonation without SIM swaps or password theft. Users should avoid suspicious links and regularly review Settings -Linked Devices to remove unknown sessions.

Telangana Logged 17,000 Ransomware Hits in 2025

Telangana's IT Minister stated the state recorded ~17,000 ransomware incidents in 2025, highlighting the scale of cyber risk for institutions and private enterprises. The remarks were made at a cybersecurity conclave, alongside broader national cyber-attack volume references and calls for stronger, technology-enabled policing and prevention systems.

CERT-In alerts on surge in attacks targeting Palo Alto Networks firewall devices

CERT-In reported a critical spike in coordinated scanning and exploitation attempts against Palo Alto Networks firewall devices, with observed targeting across PAN-OS versions, especially in India's BFSI environments. Recommended actions include urgent patching, restricting management access, blocking suspicious IPs, and enhanced monitoring/threat hunting

NEWS BYTES - INTERNATIONAL

WARP PANDA Targets VMware vCenter & Cloud Environments

CrowdStrike identified a China-nexus actor "WARP PANDA" targeting VMware vCenter/ESXi environments, deploying BRICKSTORM and additional implants to maintain stealthy, long-term access and stage data for exfiltration, raising risk for virtualized and hybrid cloud estates.

SMS Phishers Pivot to Fake Tax Refunds, Rewards & Retailer Lures

Krebs reported SMS phishing groups expanding beyond "parcel/toll" lures into tax-refund and rewards-point scams, mass-registering domains to harvest card data and OTPs—often converting stolen cards into Apple/Google mobile wallets for rapid monetization.

GOLD BLADE / STAC6565 Evolves Into Hybrid Espionage + Ransomware (QWCrypt)

Sophos observed STAC6565 (linked to GOLD BLADE/RedCurl) shifting from cyber-espionage to a hybrid model combining data theft with selective QWCrypt ransomware deployment, including novel delivery via recruitment platforms and BYOVD-style defense evasion.

Nomani Investment Scam Surges 62% Using AI Deepfake Ads on Social Media

ESET findings show "Nomani" investment fraud increasing sharply, using more realistic AI deepfake testimonials and short-lived ad campaigns across platforms, pushing victims into fake investment flows and extracting additional fees plus identity/payment details.

HoneyMyte (Mustang Panda) Adds Kernel-Mode Rootkit to Deliver ToneShell

Kaspersky reported HoneyMyte using a signed malicious mini-filter driver to protect tooling and inject an updated ToneShell backdoor, enabling stealthy persistence and remote shell capability, with targeting focused on government environments across Southeast/East Asia.

Tomiris Shifts to Telegram / Discord-Based C2 for Stealthier Government Targeting

Reporting based on Kaspersky research highlights Tomiris increasing use of public services (e.g., Telegram/Discord) for C2 to blend malicious traffic with legitimate platforms, while delivering multi-stage tooling via spear-phishing against high-value government targets.

KEY TRENDS

107

BleepingComputer

Google's December 2025 Android Security Bulletin patched 107 vulnerabilities, including two high-severity flaws flagged as exploited in targeted attacks.

5381

CVE Details

5381 CVEs (Common Vulnerabilities and Exposures) created in December 2025.

39080

MITRE CWE

39,080 CVE records analyzed in MITRE's 2025 Top 25 dataset.

62%

The Hacker News

The Nomani investment scam activity rose 62%, driven by increasingly realistic AI deepfake ads.

724

Saptang Labs

~724 ransomware disclosures across 40+ active groups in December 2025.

1.82T

Vercara (DigiCert)

1.82 trillion web requests processed, with ~464 billion flagged as malicious, showing continued massive automated and exploit traffic against web apps.

ICICI Lombard

CYBER INCIDENT ANALYSIS

Sinobi Ransomware via Firewall Vulnerability

INDUSTRY

- Leading Industrial Distributor

BRIEF SUMMARY

- Organization was hit by Sinobi ransomware after attackers exploited a firewall vulnerability to bypass defenses and gain internal access. Attackers encrypted critical files and used double extortion, threatening to leak exfiltrated data unless ransom was paid. Incident was detected through monitoring, but delayed response increased impact on confidentiality, integrity, and availability.

ROOT CAUSE ANALYSIS

- Unpatched firewall vulnerability exploited: CVE-2024-40766 (SonicOS Improper Access Control).
- Privilege escalation and lateral movement enabled by credential stuffing/brute-force against weak passwords; tools such as PsExec and WMI used to spread.
- Data exfiltration occurred alongside encryption; threats issued to leak sensitive customer data.
- Delayed detection due to insufficient monitoring and lack of anomaly detection for unusual network behavior.

LOSS CATEGORIES TO VICTIM

- Operational disruption, Data breach, Reputational damage

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Digital forensics and threat analysis to identify attack origin and scope.
- Regulatory compliance support for notifications/reporting coordination.
- Ransom payment guidance and risk-benefit assessment (including negotiation support if applicable).
- Remediation and recovery support (patching, control enhancements, restoration, firewall/VPN reconfiguration).
- Security posture review including segmentation, endpoint security, and threat detection (third-party red team).

LOSS INCURRED

- Incident Response Cost, Legal/Compliance Penalties, Data Restoration Costs

RECOMMENDED PREVENTIVE MEASURES

- Regular firewall configuration audits and timely patch management to prevent exploitation of known flaws.
- For CVE-2024-40766: apply updates; restrict management access via ACL/IP allowlisting; disable unused services; enforce least privilege; refine firewall rules and zone policies.
- Enhanced network segmentation to limit lateral movement and isolate sensitive systems/data.
- Regular vulnerability scanning and penetration testing to identify exploitable gaps early.
- Ransomware response playbook development and testing to reduce response time and disruption.
- Backup strategy with regular restore testing to validate recovery capability.
- Continuous monitoring and behavior analytics with alerts for anomalous access, encryption activity, and exfiltration attempts.

ICICI Lombard

CYBER INCIDENT ANALYSIS

Typosquatting Phishing → Credential Theft → Unauthorized ACH Transfers

INDUSTRY

- Media

BRIEF SUMMARY

- A phishing campaign used a typosquatted domain to impersonate internal communications and trick employees into entering credentials on a fake login page. With stolen credentials, attackers accessed internal systems and initiated unauthorized ACH transactions to external accounts. Incident was detected after unusual transaction patterns were flagged by fraud detection systems.

ROOT CAUSE ANALYSIS

- Typosquatted domain closely resembling the legitimate domain exploited user inattention to minor domain differences.
- Executive-impersonation phishing targeted finance/accounting teams with urgency-based ACH authorization requests.
- Credential harvesting occurred via a cloned login portal; compromised credentials enabled access to financial platforms.
- Fraudulent ACH transfers were masked as legitimate vendor payments, delaying early detection.

LOSS CATEGORIES TO VICTIM

- Financial Loss, Credential Compromise, Compliance Exposure

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Incident analysis and forensic investigation (typosquatted domain tracking, compromise analysis, transaction tracing).
- Regulatory compliance and legal support (notifications, compliance assessments, reporting).
- Customer/vendor communication strategy to manage stakeholder messaging and mitigation steps.
- Guidance on handling potential extortion attempts post-incident (even if no ransom was demanded).
- Security posture review focused on email security, finance systems, and authentication.
- Remediation support: MFA rollout, email filtering upgrades, user awareness training, and fraud detection enhancements.

LOSS INCURRED

- Fraud Loss, Forensics Cost, Remediation Costs

RECOMMENDED PREVENTIVE MEASURES

- Domain monitoring and typosquatting protection (monitor and secure commonly mistyped domains).
- Strengthen email security using SPF, DKIM, DMARC; deploy advanced phishing filters and malicious link controls.
- Enforce MFA for all access to sensitive finance systems and transaction platforms.
- Regular phishing awareness training, especially for finance/accounting/HR and high-risk teams.
- Enhance ACH fraud detection and transaction monitoring to flag anomalies in real time.
- Tighten vendor payment controls (second-party verification for high-value transfers).
- Periodic penetration tests and red team exercises to validate controls and readiness.

ADVISORIES

ADVISORY : FORTINET FORTIGATE - 2FA BYPASS OBSERVED IN THE WILD (FG-IR-19-283 / CVE-2020-12812)

- Cyber Centre Recommendation: Validate whether LDAP + local users with 2FA + LDAP group-based policies are configured; treat confirmed bypass as compromise and rotate credentials.
- Broad Threat Coverage: MFA bypass caused by username case-sensitivity mismatch between FortiGate and LDAP directories, allowing authentication without 2FA under specific configurations.
- Proactive Cybersecurity Measure: Upgrade to patched FortiOS (6.0.10+/6.2.4+/6.4.1+ or later as applicable), disable username case-sensitivity where required, restrict VPN/admin access, and review authentication logs for case-variant login attempts.

Read more at: Fortinet FortiGate — 2FA bypass observed in the wild (FG-IR-19-283 / CVE-2020-12812)

ADVISORY : MONGODB — URGENT PATCHING FOR UNAUTHENTICATED REMOTE MEMORY-READ RISK (CVE-2025-14847)

- Cybersecurity Review Recommendation: Immediately verify whether your environment has the specific configuration prerequisites (local users with 2FA referencing LDAP + LDAP group-based auth policies). If suspicious activity is found, treat it as potential compromise and reset credentials (including LDAP/AD binding credentials).
- Broad Threat Coverage:
  - The issue enables 2FA bypass in certain FortiGate LDAP configurations due to username case-sensitivity mismatch between FortiGate and LDAP directories.
  - Attackers can authenticate without the second factor by changing username capitalization, potentially impacting VPN and administrative access workflows.
- Proactive Cybersecurity Measure: Upgrade to patched FortiOS releases (or later versions that include the fix), and enforce the recommended case-sensitivity settings for affected local users. Restrict VPN/admin interfaces to trusted sources, enforce MFA on all privileged paths, and review authentication logs for case-variant login attempts. Validate group-policy design so fallback authentication paths cannot bypass the stronger control.

Read more at: MongoDB — Urgent patching for unauthenticated remote memory-read risk (CVE-2025-14847)