ICICI Lombard

CYBER INSIGHTS DIGEST

February Edition

NEWS BYTES - DOMESTIC

RedDelta Deploys PlugX Malware in SE Asia and Beyond

RedDelta, a Chinese threat actor, has been targeting organizations in Asia, Europe, and the U.S. with a customized PlugX backdoor. They use spear-phishing and DLL side-loading techniques, and have compromised multiple government entities.

India's Major Cybersecurity Incidents of 2024

India faced a rise in data breaches in 2024, targeting various sectors, with financial losses reaching ₹11,333 crore in the first nine months and projected losses of ₹1.2 lakh crore in 2025. Telecommunications and financial services were prime targets, with vulnerabilities in healthcare and consumer goods sectors also being exploited.

TCS Launches 2025 Cybersecurity Outlook

TCS highlights key technology trends, including GenAI, cloud security, and supply chain resilience, that will help organizations navigate the evolving threat landscape. Seven focus areas were identified to help organizations prioritize security investments and prepare for increasing cyberattacks.

SEBI Announces New Cybersecurity and Cyber Resilience Framework

SEBI's new CSCRF aims to boost cybersecurity for Indian financial market entities, to be implemented in phases starting January 2025. Key features include a Cyber Capability Index (CCI), Market Security Operation Centres (SOCs) for smaller entities, mandatory ISO 27001 certification, and regular cybersecurity audits.

India Proposes Digital Data Rules

India's government has released draft DPDP Rules for public comment, giving citizens more control over their data with options for informed consent, data erasure, and grievance redressal. Companies in India must implement security measures and those that misuse data may face penalties up to ₹250 crore. The Ministry of Electronics and Information Technology (MeitY) seeks public feedback on the draft regulations until February 18, 2025

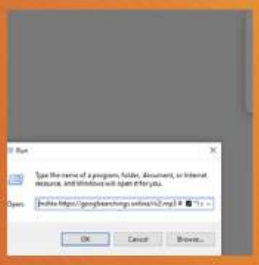
Telecom Department Orders Probe After 750 Million Users' Data Leaked

Following a CloudSEK report claiming 750 million Indian mobile users' data is for sale on the dark web, the Department of Telecom (DoT) has ordered telecom operators to conduct security audits. The leaked database allegedly contains names, numbers, addresses, and Aadhaar details.

NEWS BYTES - INTERNATIONAL

Solana Pump.fun Tool DogWifTool Compromised to Drain Wallets

Hackers compromised DogWifTools, a Solana meme coin promotion tool, via a supply chain attack, draining users' wallets. A malicious actor gained access to the GitHub repository, trojanized versions 1.6.3-1.6.6, and injected a RAT to steal cryptocurrency wallet keys. Losses are estimated to be over $10 million.



Fake CAPTCHA Campaign Spreads Lumma Stealer

A global campaign uses fake CAPTCHA verifications on compromised websites to trick users into running malicious code, delivering the Lumma information stealer. The attack targets various industries, using advanced techniques to bypass security measures.

Phishing Campaign Targets Mobile Users with Fake USPS Messages

A new phishing campaign targets mobile users by using SMS messages with malicious PDF files impersonating the USPS. The PDFs employ novel obfuscation techniques to direct users to phishing pages that steal personal information, potentially impacting organizations across 50+ countries.

GhostGPT: AI Chatbot Malware Assists Cybercriminals

Cybercriminals are selling access to GhostGPT, a malicious generative AI chatbot designed for malware creation, phishing emails, and more. Researchers found it being sold via Telegram, highlighting growing interest among criminals in AI tools for nefarious activities. GhostGPT can quickly create convincing phishing templates and other malicious content.

New "Cookie Sandwich" Technique Allows Stealing of HttpOnly Cookies

The "Cookie Sandwich Attack" exploits cookie parsing inconsistencies to steal sensitive session cookies, even those with the HttpOnly flag. Attackers manipulate HTTP headers, using legacy standards and browser behaviour to expose cookies, enabling access to restricted data via client-side scripts on poorly configured web apps. Web servers must strictly adhere to RFC6265 to prevent such attacks.

Hackers Use FastHTTP in New High-Speed Password Attacks

Threat actors are using the FastHTTP library to launch high-speed brute-force password attacks against Microsoft 365 accounts. SpearTip discovered the campaign, which began on January 6, 2025, achieving successful account takeovers nearly 10% of the time, with 65% of the malicious traffic originating from Brazil.

KEY TRENDS

510

CyFirma

510 reported ransomware victims globally in January 2025, showing an 82.14% increase from January 2024

3040

CVE Details

3040 CVEs (Common Vulnerabilities and Exposures) created in January.

39

Indus Face

A cybersecurity breach occurs every 39 seconds, contributing to 2,244 daily cyberattacks

3.4B

Get Astra

3.4 billion phishing emails are sent daily, with 1.2% of all emails being malicious

5.6 TBPS

India Today

Cloudflare mitigated a record-breaking 5.6Tbps DDoS attack, indicating an increase in hyper-volumetric DDoS attacks

678B

CEI America

Public spending on cloud services is predicted to grow by 20.4%, reaching $678 billion in 2025

CYBER INCIDENT ANALYSIS

Financial Services Ransomware Attack

INDUSTRY

- Financial Services

BRIEF SUMMARY

- A financial firm suffered a ransomware attack through an exposed RDP. Attackers used Ngrok for stealth, conducted reconnaissance, and deployed remote access tools. They evaded defences, achieved persistence, and encrypted files after exfiltration of data, leaving a ransom note.

ROOT CAUSE ANALYSIS

- **Exposed RDP services without proper security controls (e.g., no MFA).**
- **Weak network segmentation, allowing lateral movement.**
- **Lack of monitoring and detection for tunnelling tools (Ngrok).**
- **Insufficient endpoint security, enabling unauthorized tool execution.**

LOSS CATEGORIES TO VICTIM

- Operational Disruption, Data Breach, Reputational Damage

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Engaged forensic experts to assess impact and containment.
- Facilitated negotiations with ransomware operators.
- Covered costs for data recovery and business continuity efforts.

LOSS INCURRED

- Incident Response Costs, Legal / Compliance Costs, Ransom Payment Consideration

RECOMMENDED PREVENTIVE MEASURES

- **Secure RDP access with multi-factor authentication and IP allow listing.**
- **Monitor for tunnelling tools and block unauthorized remote access software.**
- **Improve network segmentation to limit lateral movement.**
- **Enable advanced logging and monitoring for early threat detection.**
- **Regularly update and test incident response plans for ransomware scenarios.**
- **Implement robust backup strategies, including offline and immutable backups.**

CYBER INCIDENT ANALYSIS

Business Email Compromise in Legal Sector

INDUSTRY

- Legal Services

BRIEF SUMMARY

- A law firm fell victim to a BEC attack where hackers accessed a partner's email through a malicious app, bypassing password changes. They monitored communications, altered payment instructions, and hid security alerts. The fraud was only discovered when clients reported missing payments.

ROOT CAUSE ANALYSIS

- **OAuth Token Abuse: The attacker tricked the user into granting permissions to a rogue third-party app, which remained active even after password resets.**
- **Lack of Conditional Access Policies: No restrictions were in place to prevent login attempts from high-risk locations or untrusted devices.**
- **Email Rule Exploitation: Attackers created inbox rules to auto-delete warnings and forward sensitive data externally.**
- **Insufficient Visibility into OAuth Grants: The security team lacked visibility into third-party app permissions within Microsoft 365.**

LOSS CATEGORIES TO VICTIM

- Financial Loss, Legal / Compliance Risks, Reputational Damage

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Engaged forensic specialists to investigate unauthorized access.
- Assisted in fund recovery efforts through legal channels.

LOSS INCURRED

- Direct Financial Loss, Incident Response Cost, Operational Impact

RECOMMENDED PREVENTIVE MEASURES

- **Implement OAuth application governance to assess and restrict access to potentially risky third-party applications, ensuring only secure apps are allowed.**
- **Enable Conditional Access policies to automatically block login attempts from high-risk geographic locations, enhancing overall security.**
- **Regularly audit and monitor inbox rules to identify any unauthorized changes or modifications.**
- **Enforce Multi-Factor Authentication (MFA) for user accounts and apply session timeout policies to reduce the risk of unauthorized access.**

ADVISORIES

SUMMARY ON CISA'S ORDER FOR MICROSOFT 365 SECURITY

- **Critical Security Release: On January 14, 2025, Microsoft rolled out a significant set of security updates. These patches address multiple vulnerabilities across various Microsoft products, aiming to close potential loopholes that cybercriminals could exploit to gain unauthorized system access.**
- **CISA Recommendation: The Cybersecurity and Infrastructure Security Agency (CISA) has issued a strong advisory urging users and system administrators to promptly review and apply these updates. This underscores the critical nature of the vulnerabilities being addressed.**
- **Broad Product Coverage: While specific products aren't detailed in the advisory, the updates likely encompass a wide range of Microsoft offerings. This typically includes popular software such as Windows operating systems, Office applications, and various server products.**
- **Proactive Cybersecurity Measure: This release highlights the ongoing importance of maintaining up-to-date software as a key defense against cyber threats. By swiftly addressing known vulnerabilities, organizations and individuals can significantly enhance their cybersecurity posture and reduce the risk of potential attacks.**

Read more at: Microsoft Releases January 2025 Security Updates

CISA ALERT ON FORTINET SECURITY UPDATES

- **CISA and FBI Joint Advisory: On January 22, 2025, they released an alert about threat actors exploiting multiple vulnerabilities in Ivanti Cloud Service Appliances (CSA) during September 2024.**
- **Critical Vulnerabilities: The advisory highlights four critical vulnerabilities in Ivanti CSA, including administrative bypass, SQL injection, and remote code execution flaws.**
- **Exploitation Tactics: Malicious actors chained these vulnerabilities to gain initial access, execute remote code, obtain credentials, and implant webshells on victim networks.**
- **Urgent Recommendations: CISA and FBI strongly advise upgrading to the latest Ivanti CSA version, hunting for malicious activity using provided indicators, and reviewing CISA's vulnerability management resources..**

Read more at: CISA and FBI Release Joint Advisory

The Cyber Incident Analyses have been created by ICICI Lombard GIC Ltd. and Arete-IR LLP ("Arete"). The Analysis is based on information compiled and analysed from various external sources. The above provided content is only for general knowledge and information purposes only and shall not constitute any legal, financial, professional or any other advice by ICICI Lombard GIC Ltd. and Arete. ICICI Lombard GIC Ltd. and Arete make no representation or warranties, express or implied, regarding the accuracy, completeness or reliability of the information contained herein. ICICI Lombard GIC Ltd. and Arete disclaim any liability for reliance placed by any person(s) upon any advice, opinion, statement, memorandum or other information provided herein and the use of such information shall strictly be at his/her/their sole risk. Arete-IR LLP, LLPIN: AAQ-5318, registered office at Unit 200, Maple Celestia, Plot No. 49, Jayabheri Enclave, Gachibowli, Hyderabad, Telangana - 500032. Arete's trademark belongs exclusively to Arete. ICICI trade logo displayed above belongs to ICICI Bank and is used by ICICI Lombard GIC Ltd. under license and Lombard logo belongs to ICICI Lombard GIC Ltd. ICICI Lombard General Insurance Company Limited. Registered Office: ICICI Lombard House, 414, Veer Savarkar Marg, Prabhadevi, Mumbai – 400025. IRDA Reg.No.115. Toll Free 1800 2666. Fax No – 022 61961323. CIN (L67200MH2000PLC129408) customersupport@icicilombard.com. www.icicilombard.comADV/23437