CYBER INSIGHTS DIGEST

July Edition

NEWS BYTES - DOMESTIC

APT36 Targets Indian Defense with Credential-Stealing Malware

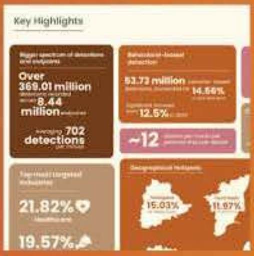
APT36, a Pakistan-linked threat group, is targeting Indian defense personnel using phishing emails containing malware-laced documents to steal credentials. The campaign leverages spoofed government domains and malicious executables, posing a serious cyber espionage threat to India's defense sector.

DoT Releases Draft Telecom Cybersecurity Policy for Public Feedback

A major cyber breach at the Bengaluru Water Supply and Sewerage Board (BWSSB) exposed over 2.9 lakh citizens' records. The leaked data includes Aadhaar, phone numbers, and addresses. Experts highlight negligence in cybersecurity practices.

Updated DRAT Malware Resurfaces in TAG-140's Cyber Arsenal

TAG-140, linked to Chinese state interests, is using an updated DRAT v2 malware variant for cyber espionage. The malware features improved evasion, reconnaissance, and data exfiltration capabilities, posing increased risks to government and defense entities in South and Southeast Asia.



DSCI Releases India Cyber Threat Report 2025 Highlighting Key Risks

The India Cyber Threat Report 2025 reveals a surge in ransomware, phishing, and APT attacks targeting critical infrastructure, government, and enterprises. It emphasizes the need for stronger cybersecurity frameworks, threat intelligence, and public-private collaboration to counter evolving digital threats.

Cybersecurity Dialogue Held in Mumbai Amid Rising National Cyber Threats

A new variant of the 'Tarbot' Android banking trojan is targeting over 750 apps, including banking and crypto wallets. It captures credentials and bypasses multi-factor authentication using overlay attacks.

India, UAE Strengthen Cybersecurity Ties Through Strategic Collaboration

India and the UAE signed a Memorandum of Understanding to enhance cooperation in cybersecurity, focusing on information sharing, capacity building, and joint research. The partnership aims to bolster national cyber resilience and address evolving global cyber threats collaboratively.

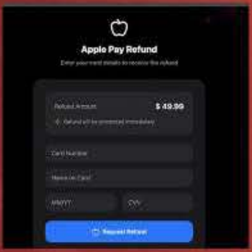
NEWS BYTES - INTERNATIONAL

Stealthy WordPress Malware Drops Windows Trojan via PHP Backdoor

A stealthy malware campaign targets WordPress sites using a PHP backdoor to deploy Windows trojans. The attack enables remote access, data theft, and system compromise, highlighting the importance of securing web servers and regularly monitoring for unauthorized changes.

ConnectWise ScreenConnect Abused to Deploy Malware in Targeted Attacks

Cybercriminals are abusing ConnectWise ScreenConnect to distribute malware in targeted attacks. The remote access tool is exploited to install backdoors and surveillance software, enabling persistent access to victim systems. Organizations are urged to monitor remote tools and apply strict access controls.



Apple Pay Refund

Enter your card details to receive the refund

Refund Amount $ 49.99

Refund will be processed immediately

Card Number

Name on Card

MM/YY

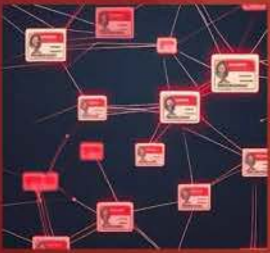
CVV

CapCut-Themed Apple Phishing Scam Steals Card Data via Fake Refunds

A phishing campaign uses fake Apple refund alerts tied to CapCut to trick users into submitting credit card details. The scam employs realistic pages and urgency tactics, targeting mobile users and aiming for financial fraud through credential and card data theft.

Top VPN Apps May Enable Chinese State Surveillance

VPN apps on Apple and Google platforms may be compromised to enable Chinese state surveillance. Researchers warn of potential data interception and user tracking, raising privacy concerns amid tightening regulations and increased scrutiny of foreign tech services.



Over 2,000 Devices Compromised via Weaponized Social Security Documents

Hackers exploited fake Social Security documents to deliver malware, compromising over 2,000 devices. The campaign uses phishing emails with malicious attachments to gain unauthorized access, steal data, and execute remote commands, posing serious threats to personal and organizational cybersecurity.

Hackers Breach Norwegian Dam, Force Valve Open at Full Capacity

Hackers breached a Norwegian hydroelectric dam's control system, forcing a critical valve open at full capacity. While no damage occurred, the incident highlights the vulnerability of industrial control systems to cyberattacks with potentially catastrophic consequences

KEY TRENDS

2200

Astra

Number of cyber attacks per day globally.

2911

Simplilearn

2911 CVEs (Common Vulnerabilities and Exposures) created in June.

57%

Zscaler

57% of ransom demands, in the previous year, were for $1 million or more.

16B

CVE Details

16 Billion Credentials Leaked in Historic Data Dump.

7.4M

Strobes

Leak of data belonging to 7.4 million Paraguayans traced back to infostealers.

92%

Security Magazine

92% of malware was delivered via emails.

CYBER INCIDENT ANALYSIS

Ransomware Attack on a Legal Firm

INDUSTRY

- Professional Services / Legal & Consulting

BRIEF SUMMARY

- A legal and consulting firm suffered a ransomware attack by Luna Moth, which exfiltrated sensitive data without encryption. Using phishing emails and remote access tools, attackers infiltrated the network, stole data, and demanded ransom-impacting operations and exposing confidential client information.

ROOT CAUSE ANALYSIS

- Phishing emails mimicked tools like DocuSign and Zoom to install RATs.
- Poor email filtering and awareness enabled credential theft and device compromise.
- Limited egress monitoring delayed detection of significant data loss.

LOSS CATEGORIES TO VICTIM

- Data Exposure, Compliance Risk, Reputational Damage, Financial Loss

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensics identified tools, attacker movement, and data accessed during breach.
- Legal support ensured regulatory compliance and managed client confidentiality fallout.
- Ransom experts assessed threat credibility and handled extortion negotiations.

LOSS INCURRED

- Legal Fees, Regulatory Penalties, Forensics Cost, Revenue Loss

RECOMMENDED PREVENTIVE MEASURES

- Use phishing protection and real-time email sandboxing to block malicious content.
- Enforce MFA across all systems and remote access applications.
- Conduct regular phishing simulations and company-wide security training sessions.
- Develop and rehearse breach response plans for ransomware and extortion scenarios.

CYBER INCIDENT ANALYSIS

Data Leakage in a Fintech Organization

INDUSTRY

- Financial Services / Fintech

BRIEF SUMMARY

- An investment firm faced a major data breach due to insecure mobile APIs. Lacking proper authentication and object-level authorization, attackers accessed sensitive customer data, raising concerns over security, privacy, and compliance.

ROOT CAUSE ANALYSIS

- APIs lacked authentication and object-level authorization controls, exposing sensitive endpoints.
- IDOR vulnerabilities allowed attackers to manipulate inputs, retrieving other users' data.
- Tokens issued via unregistered numbers and exposed keys were abused using automation.

LOSS CATEGORIES TO VICTIM

- Data Exposure, Reputational Damage, Compliance Risk, Operational Disruption

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Legal team managed notifications and ensured compliance with privacy regulations.
- Funding allocated for patching, redesign, and third-party security assessments.

LOSS INCURRED

- Forensic Analysis, Application Reengineering, Reputation Recovery Costs, Potential Regulatory Fines

RECOMMENDED PREVENTIVE MEASURES

- Implement robust authentication and authorization for all API endpoints.
- Conduct regular SAST, DAST, and VAPT to detect and fix vulnerabilities.
- Deploy API gateways with access control and threat anomaly detection features.
- Validate all tokens, and avoid exposing secrets or static keys publicly.
- Apply zero trust model for mobile and backend application interactions.
- Develop comprehensive incident response plans with periodic breach simulations.

ADVISORIES

ADVISORY : MATTERMOST SECURITY ADVISORY (AV25-364)

- **Multiple Vulnerabilities Identified:** The advisory highlights multiple security vulnerabilities affecting Mattermost versions prior to 9.5.2, 9.4.6, and 9.3.8, including issues that may allow privilege escalation or unauthorized access.
- **Potential Exploitation Risks:** Successful exploitation could enable attackers to execute arbitrary code, perform actions on behalf of other users, or access sensitive data without proper authorization, impacting confidentiality and integrity.
- **Recommended Action Update:** Administrators are strongly urged to upgrade Mattermost to the latest secure versions immediately to mitigate these risks and ensure the protection of communication and collaboration environments.
- **Additional Mitigation Measures:** The Canadian Centre for Cyber Security also recommends reviewing logs for unusual activity and implementing proper access controls and monitoring to detect any exploitation attempts post-update.

Read more at: Mattermost Security Advisory (AV25-364)

ADVISORY : CISA GUIDANCE AND STRATEGIES TO PROTECT NETWORK EDGE DEVICES

- **CISA Releases Protective Guide:** CISA published a detailed guide to help organizations secure internet-exposed systems, aiming to reduce the attack surface exploited by threat actors in real-world incidents
- **Focus on Common Misconfigurations:** The guide highlights frequently observed misconfigurations such as weak authentication, exposed management interfaces, and default credentials that make systems vulnerable to compromise.
- **Mitigation Recommendations Provided:** CISA offers actionable recommendations, including enforcing multi-factor authentication, using network segmentation, and disabling unused services to enhance overall cybersecurity posture.
- **Targets Public and Private Sectors:** The guidance is intended for both public and private organizations, especially IT teams and defenders, to proactively identify, assess, and remediate internet-facing security weaknesses.

Read more at: CISA Guidance and Strategies to Protect Network Edge Devices

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.com