ICICI Lombard

CYBER INSIGHTS DIGEST

November Edition

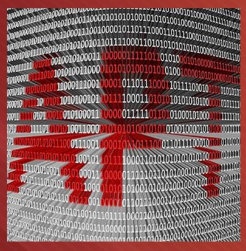
NEWS BYTES

Malware attack on State Data Center in India puts some citizen services at a standstill

A malware attack on Uttarakhand's State Data Center has disrupted several critical services, including government websites and the Chief Minister's helpline. The state is collaborating with cybersecurity experts to restore services and strengthen security measures.

WazirX moved over $73 million crypto after data breach: CoinSwitch

Following a security breach resulting in the theft of $230 million, WazirX transferred over $73 million worth of cryptocurrency to exchanges like Bybit and KuCoin. This move comes as the company faces liabilities totaling $546.5 million.



New China-Nexus APT Group IcePeony Targeting Asian Nations

The advanced persistent threat (APT) group IcePeony, reportedly linked to China, has been targeting government agencies, academic institutions, and political organizations in countries including India, Mauritius, and Vietnam. Their attacks involve sophisticated techniques such as SQL injection and a custom malware called 'IceCache.'

IRDAI tightens fraud rules post hacking incidents

The Insurance Regulatory and Development Authority of India (IRDAI) has introduced stricter guidelines to combat online fraud in the insurance sector following recent hacking incidents. These measures aim to strengthen security and protect policyholders from cyber threats.

Indian companies struggle to stop ransomware attacks

Indian businesses, banks, and public services are increasingly targeted by ransomware, with a 46% year-on-year rise in cyberattacks. Many companies are paying ransoms to recover data, underscoring the urgent need for stronger cybersecurity measures.

Rashtriya Raksha University Leads the Way in Cybersecurity with the Cyber Commando Training Program

On October 1, 2024, Rashtriya Raksha University (RRU), in collaboration with the Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs, launched the prestigious Cyber Commando Training Program, marking a major milestone in strengthening India's cybersecurity infrastructure.

NEWS BYTES

Massive PSAUX ransomware attack targets 22,000 CyberPanel instances

A critical vulnerability in CyberPanel allowed the PSAUX ransomware to target and encrypt files on 22,000 servers. The attack exploited an authentication bypass flaw, leading to significant disruptions.

AI scammers target Gmail accounts, say they have your death certificate

Scammers are using AI-generated voices to impersonate Google Support, falsely claiming that a death certificate has been issued for the victim. They deceive users into clicking 'Yes, it's me' on a fake account recovery screen, leading to account compromise.

'CrossBarking' Attack Targeted Secret APIs, Exposing Opera Browser Users

Researchers have discovered a new attack called 'CrossBarking' that exploits private APIs in the Opera browser. This vulnerability allows attackers to execute malicious code, alter settings, hijack accounts, and disable security extensions.

Fake WordPress Plugins on 6,000 Sites Prompt Users to Install Malware

Over 6,000 websites have been compromised by fake WordPress plugins in the ClickFix campaign. These plugins, installed using stolen credentials, prompt users to install malware through fake browser update notifications.

Lazarus Group Exploits Chrome Zero-Day in Latest Campaign

North Korea's Lazarus Group is exploiting a Chrome zero-day vulnerability and a fake game website to target cryptocurrency investors. The campaign uses AI-generated content and professional LinkedIn accounts to lure victims.

Independent Russian news site rides out a week of DDoS incidents

The independent Russian news site Novaya Gazeta Europe was hit by multiple large-scale DDoS attacks, temporarily taking its website offline. The attacks, which peaked at 12 million junk page requests per minute, originated from multiple data centers.

ICICI Lombard

KEY TRENDS

70

Infosecurity Magazine

Researchers have discovered over 70 zero-day vulnerabilities at Pwn2Own Ireland.

3612

CVE Details

A total of 3,612 CVEs (Common Vulnerabilities and Exposures) were created in October.

17T

CISO Economic Times

India is expected to face nearly 17 trillion cyberattacks by 2047.

400

TheRecord.Media

Nearly 400 US healthcare institutions were hit with ransomware over the past year, according to Microsoft.

19 CR

Business Standard

The average cost of a data breach reached Rs 19 crore in 2024.

175M

Bleeping Computer

Amazon reports that 175 million customers now use passkeys to log in.

CYBER INCIDENT ANALYSIS

Cyber Incident in the Transportation Sector

INDUSTRY

- Transportation

BRIEF SUMMARY

- A fraudster, posing as a staff accountant, emailed a client requesting urgent payment for an invoice. The client's Accounts Payable (AP) Manager communicated with the imposter and forwarded the request to the vendor setup team, who subsequently approved it.

ROOT CAUSE ANALYSIS

- The adversary gained access to the accountant's email through phishing techniques and emailed the AP Manager to register a new vendor.
- The attacker then sent a second email to the AP Manager with a fraudulent invoice, claiming it was due for payment.
- The AP Manager sought CFO approval for the payment, and the attacker provided a fake email. Believing it was legitimate, the AP Manager forwarded it to the AP Administrator to process the payment.
- Unaware of the fraudulent request, the real Staff Accountant contacted the AP Manager. During their conversation, they uncovered the fraud and halted the payment just in time.

LOSS CATEGORIES TO VICTIM

- Brand Reputation, Forensics Cost, and Potential Financial Loss

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- The insurer assisted the organization in coordinating with a digital forensics and incident response expert to assess the impact of the incident and provide remediation recommendations.
- Additionally, the insurer helped appoint legal counsel to assist with cross-border regulatory reporting.

LOSS INCURRED

- Forensic Cost and Legal Cost

RECOMMENDED PREVENTIVE MEASURES

- It is recommended to implement Exchange Online Protection (EOP) and Advanced Threat Protection (ATP) as an additional layer of security on the tenant. Implement a multi-step verification process and establish clear communication protocols.
- Enable external email warnings to alert users about potential phishing emails. Monitor logs for inbox rule creation and foreign account activity. Monitor and review financial transactions regularly.
- Enable DLP services in M365 and encrypt emails when sharing externally

CYBER INCIDENT ANALYSIS

Cyber Incident in the IT Sector

INDUSTRY

- IT and Digital Solutions Company

BRIEF SUMMARY

- The client was alarmed upon receiving an urgent notification from a regulatory body, warning of potential reconnaissance activity on their network. The alert revealed that credentials linked to the client had been found on the dark web, suggesting a serious security breach. This discovery indicated that cybercriminals might be probing their defenses, possibly planning a more significant attack.

ROOT CAUSE ANALYSIS

- Cybercriminals exploited a vulnerability in the SMBv1 (Server Message Block version 1) protocol to harvest sensitive credentials from the client's network. This well-known flaw enabled attackers to infiltrate the system and access critical information.

LOSS CATEGORIES TO VICTIM

- Brand Reputation, Forensic Cost, and potential Confidentiality Compromise

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- The insurer assisted the organization in coordinating with a digital forensics and incident response expert to assess the impact of the incident and provide remediation recommendations.
- Additionally, the insurer helped appoint legal counsel to support cross-border regulatory reporting.

LOSS INCURRED

- Forensic Cost

RECOMMENDED PREVENTIVE MEASURES

- Ensure SMBv1 is fully disabled across all systems, as it is no longer supported by modern operating systems.
- Deploy advanced intrusion detection systems, network monitoring tools, and dark web monitoring to detect suspicious activities and credential exposure in real-time. Regularly update and patch systems and protocols.
- Enhance credential practices by implementing regular password updates, using strong, unique passwords, and enabling multi-factor authentication (MFA), especially for privileged accounts.

ADVISORIES

FOREIGN THREAT ACTOR CONDUCTING LARGE-SCALE SPEAR-PHISHING CAMPAIGN WITH RDP ATTACHMENTS

- A foreign threat actor is conducting a large-scale spear-phishing campaign using malicious RDP files to gain access to networks. The campaign targets various sectors, including government and IT, by impersonating trusted entities to deceive recipients.
- To minimize exposure to cyber threats, forbid or significantly restrict outbound RDP connections. Implement controls to block the execution of RDP files by users, which is crucial in reducing the risk of exploitation.
- Implement multi-factor authentication (MFA) wherever feasible to add an essential layer of security for remote access. Avoid using SMS-based MFA whenever possible. Establish a user education program to teach how to identify and report suspicious emails. Strong user education can help mitigate the threat of social engineering and phishing attacks.
- Evaluate, alongside EDR solutions, the deployment of anti-phishing and antivirus tools to strengthen defenses against emerging threats.

Read more at: Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments | CISA

ORACLE CRITICAL PATCH UPDATE ADVISORY

- Oracle's October 2024 Critical Patch Update addresses 329 new security patches across various Oracle products, including Oracle Database Server, Oracle Application Express, and Oracle Blockchain Platform.
- Given the threat posed by a successful attack, Oracle strongly recommends that customers apply the Critical Patch Update security patches as soon as possible. Until the patches are applied, customers may reduce the risk of a successful attack by blocking network protocols required for the attack.
- Some vulnerabilities can be exploited remotely without authentication, highlighting the urgency of taking immediate action. Several vulnerabilities addressed in this Critical Patch Update impact multiple products.

Read more at: Oracle Critical Patch Update Advisory - October 2024