ICICI Lombard

CYBER INSIGHTS DIGEST

April Edition

NEWS BYTES - DOMESTIC

Critical PHP RCE Vulnerability Mass Exploited

Mass exploitation of a critical PHP remote code execution (RCE) vulnerability has been observed in new attacks. This vulnerability allows attackers to execute arbitrary code on affected systems, leading to significant security breaches and potential data loss.

New Android Malware Campaigns Evading Detection Using Cross-Platform Framework .NET

New Android malware campaigns are evading detection by using the cross-platform framework .NET MAUI. These campaigns are increasing the threat landscape by making it harder for traditional security measures to detect and mitigate the malware.

SideWinder APT Targets Maritime, Nuclear, and IT Sectors

The SideWinder advanced persistent threat (APT) group has been targeting maritime, nuclear, and IT sectors across Asia, the Middle East, and Africa. These attacks pose a significant threat to critical infrastructure and sensitive information in these regions.

APT36 Spoofs India Post Website to Infect Windows and Android Users with Malware

APT36 group with ties to Pakistan has been attributed to the creation of a fake website masquerading as India's public sector postal system (India Post) as part of a campaign designed to infect both Windows and Android users in the country.

Hackers Exploit Severe PHP Flaw to Deploy Quasar RAT and XMRig Miners

Hackers are exploiting a severe PHP flaw to deploy Quasar RAT and XMRig miners. This exploitation allows attackers to gain control over affected systems, using them for remote access and cryptocurrency mining. Surge in exploitation attempts since late last year, with a significant concentration reported in Taiwan (54.65%), Hong Kong (27.06%), Brazil (16.39%), Japan (1.57%), and India (0.33%).

Vo1d Malware Botnet Grows to 1.6 Million Android TVs Worldwide

A new variant of the Vo1d malware botnet has grown to 1,590,299 infected Android TV devices across 226 countries, recruiting devices as part of anonymous proxy server networks. The researchers report that the botnet has had notable infection surges, like going from 3,900 to 217,000 bots in India within just three days.

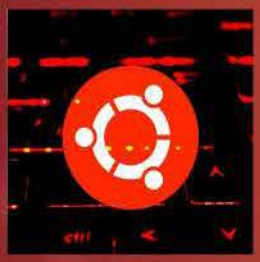
NEWS BYTES - INTERNATIONAL

Lucid: The Rising Threat of Phishing-as-a-Service

Lucid has emerged as a rising threat in the form of phishing-as-a-service. This service facilitates widespread phishing attacks by providing tools and resources to cybercriminals, making it easier to launch sophisticated phishing campaigns.

Hackers Repurpose RansomHub's EDRKillShifter in Medusa, BianLian, and Play Attacks

Hackers have repurposed RansomHub's EDRKillShifter tool in attacks involving Medusa, BianLian, and Play ransomware. This tool enhances the effectiveness of these ransomware attacks by disabling endpoint detection and response (EDR) systems, making it harder to detect and mitigate the threats.



New Ubuntu Linux Security Bypasses Require Manual Mitigations

New security bypasses in Ubuntu Linux have been discovered, requiring manual mitigations. These vulnerabilities allow attackers to bypass security measures, potentially leading to unauthorized access and data breaches. Users are advised to implement the recommended mitigations promptly.

New Morphing Meerkat Phishing Kit Mimics Brands

The new Morphing Meerkat phishing kit mimics 114 brands using victims' DNS email records. This sophisticated phishing kit enhances the effectiveness of phishing attacks by making them appear more legitimate, increasing the likelihood of victims falling for the scams.

Ghostscript Nightmare: Critical Severity Vulnerabilities Put Users at Risk

Critical severity vulnerabilities in Ghostscript have been identified, putting users at risk. These vulnerabilities can be exploited to execute arbitrary code, leading to potential data breaches and system compromises. Users are urged to apply the necessary patches to protect their systems.

Adversaries Target AI Users with Fake Sponsored Ads to Deliver Malware

DeepSeek users with fake sponsored Google ads to deliver malware. This tactic exploits user trust in sponsored ads, leading to malware infections and potential data theft. Users are advised to be cautious and verify the authenticity of ads before clicking.

ICICI Lombard

KEY TRENDS

$ 10.5T

The Review Hive

Global cybercrime costs are projected to reach $10.5 trillion annually by 2025, up from $8 trillion in 2023, driven by increased attack frequency and sophistication

3179

CVE Details

3179 CVEs (Common Vulnerabilities and Exposures) created in April.

91%

Version-2

91% of security teams utilize generative AI, though 65% acknowledge limited understanding of its implications

$10M

The Review Hive

Healthcare organizations are predicted to remain prime targets for cybercriminals in 2025, with the average cost of a data breach in this sector likely exceeding $10 million.

703%

NuCamp

Credential theft has increased by 703%, highlighting the growing threat to user credentials.

2200

NuCamp

Approximately 2,200 cyber attacks happen every single day, averaging one attack every 39 seconds.

CYBER INCIDENT ANALYSIS

Healthcare Sector Ransomware Attack

INDUSTRY

- Healthcare / Medical Services

BRIEF SUMMARY

- A healthcare organization faced a severe Medusa ransomware attack via a compromised RDP service. Attackers exploited weak authentication, gaining unauthorized access and manually deploying ransomware, encrypting critical patient data, including medical records, billing information, and administrative files.

ROOT CAUSE ANALYSIS

- **Exposed RDP & No MFA:** Attackers exploited remote access without multi-factor authentication.
- **Inadequate Monitoring:** Suspicious activity went undetected, enabling ransomware.
- **Weak Segmentation:** Ransomware spread due to poor system isolation.
- **Outdated Systems:** Unpatched vulnerabilities left systems exposed.

LOSS CATEGORIES TO VICTIM

- Operational Disruption, Data Breach, Reputational Damage, Financial Loss

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensic Investigation: Insurer traced intrusion, assessed systems, documented attack.
- Incident Response: Specialists contained threat, began secure restoration.
- Legal Assistance: Counsel guided regulatory notifications, HIPAA compliance.
- Ransom Negotiation: Experts engaged attackers, reduced ransom demands.
- Remediation Funding: Insurer funded recovery, reimaging, patching, MFA, retraining.

LOSS INCURRED

- Legal / Compliance Costs, Ransom Payment, Operational Downtime, Reputation Recovery Costs

RECOMMENDED PREVENTIVE MEASURES

- **Secure Remote Access:** Disable unnecessary services or secure with strong authentication and network restrictions.
- **Enforce MFA:** Implement multi-factor authentication for all remote and privileged accounts.
- **Network Segmentation:** Divide network zones to limit lateral movement and protect sensitive systems.
- **Patch & Response:** Ensure timely software updates, deploy EDR tools, and maintain secure backups and incident response plans.

CYBER INCIDENT ANALYSIS

Phishing Campaign against a Marketing Firm

INDUSTRY

- Social Media Management

BRIEF SUMMARY

- A phishing campaign targeted businesses using Social Media Platform advertising services. Attackers sent emails impersonating Social Media Platform claiming policy violations and threatening suspension. Victims clicked malicious links, interacted with fake chatbots, and provided sensitive information, leading to account hijacking and data compromise.

ROOT CAUSE ANALYSIS

- **Phishing Emails: Attackers sent urgent, fake Social Media Platform emails.**
- **Fake Landing Pages: Links led to convincing fake Social Media Platform pages.**
- **Deceptive Chatbots solicited sensitive data for verification.**
- **Credential Harvesting: Users unknowingly gave attackers account access.**

LOSS CATEGORIES TO VICTIM

- Operational Damage, Financial Loss, Reputational Damage, Data Breach

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- **Forensic Investigation:** Fund digital forensics to assess breach extent.
- **Legal Support:** Provide counsel for breach notification compliance.
- **Crisis Communication:** Develop strategies to inform stakeholders and customers.
- **Remediation Funding:** Support enhanced security measures and training.

LOSS INCURRED

- Revenue Loss, Forensics Costs, Operational Costs

RECOMMENDED PREVENTIVE MEASURES

- **Employee Training:** Educate staff on recognizing phishing attempts, verifying official communications, and securely handling sensitive information.
- **Multi-Factor Authentication:** Implement MFA on all business accounts to add an extra layer of security beyond passwords.
- **Regular Account Audits:** Perform routine reviews of account activities to promptly detect unauthorized actions.
- **Secure Communication Channels:** Use official Social Media Platform channels for all communications and verify the authenticity of messages received.
- **Incident Response Planning:** Develop and regularly update an incident response plan to ensure swift and effective action in case of future security threats.

ADVISORIES

CISA ADVISORY ON INDUSTRIAL CONTROL SYSTEM VULNERABILITIES

- **Critical Security Advisory:** On March 25, 2025, CISA released an advisory regarding vulnerabilities in ABB's RMC-100 and RMC-100 LITE products. These vulnerabilities could allow attackers to exploit the web UI, causing a temporary denial of service.
- **CISA Recommendation:** The Cybersecurity and Infrastructure Security Agency (CISA) strongly advises users to update their systems promptly. ABB has provided updates to mitigate these vulnerabilities and recommends disabling the REST interface when not in use.
- **Affected Products:** The advisory specifically mentions RMC-100 versions 2105457-036 to 2105457-044 and RMC-100 LITE versions 2106229-010 to 2106229-016.
- **Proactive Cybersecurity Measure:** This advisory underscores the importance of maintaining up-to-date systems and proper network segmentation to prevent unauthorized access and potential attacks.

Read more at: CISA Advisory on Industrial Control System Vulnerabilities

ADVISORY : CISA, FBI AND MS-ISAC ADVISORY ON MEDUSA RANSOMWARE

- **Critical Security Advisory:** On March 12, 2025, CISA, in collaboration with the FBI and MS-ISAC, issued a joint advisory on the Medusa ransomware. This ransomware-as-a-service variant has impacted over 300 victims across various critical infrastructure sectors.
- **CISA Recommendation:** The Cybersecurity and Infrastructure Security Agency (CISA) urges organizations to implement the recommended mitigations to reduce the likelihood and impact of Medusa ransomware incidents. Key actions include ensuring systems are patched and up to date, segmenting networks to restrict lateral movement, and filtering network traffic to prevent access from unknown or untrusted origins.
- **Affected Sectors:** The advisory highlights that Medusa ransomware has targeted sectors including medical, education, legal, insurance, technology, and manufacturing.
- **Proactive Cybersecurity Measure:** This advisory emphasizes the importance of maintaining robust cybersecurity practices, such as regular updates and network segmentation, to defend against ransomware threats.

Read more at: CISA, FBI and MS-ISAC Release Joint Advisory