ICICI Lombard

CYBER INSIGHTS DIGEST

January Edition

NEWS BYTES - DOMESTIC

LNK Files and SSH Commands: The New Arsenal of Advanced Cyber Attacks

A report reveals that cybercriminals are increasingly using LNK files and SSH commands for advanced attacks. These methods enable them to bypass security measures, maintain persistence, and execute complex attack chains, particularly targeting high-value sectors such as defense and aerospace.

ElizaRAT Exploits Instant Messaging and other services For C2

Recent developments in the Elizarat malware have improved its command and control (C2) communication methods. These enhancements enable more effective data exfiltration and evasion of detection, posing greater challenges for cybersecurity defenses.

New Android Banking Trojan Targets Indian Users Through Fake Apps

A new Android banking Trojan is targeting users in India through fake applications. This malware deceives users into divulging sensitive information, putting their financial security at risk. The threat underscores the need for heightened vigilance and stronger security measures among mobile users.

India on high alert as hacker group plans 'Cyber Party' targeting critical digital infrastructure

India is on high alert following reports of a hacker group planning a 'cyber party' to target critical digital infrastructure. Authorities are ramping up security measures to safeguard essential services and prevent potential disruptions from these cyber threats.

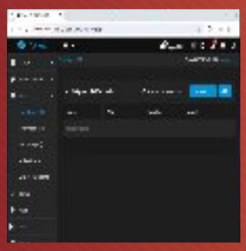
API Security flaw that exposed data of users and drivers

A security flaw exposed the personal data of over 1,800 users and drivers, including names, email addresses, and phone numbers. The vulnerability, associated with an API used for feedback collection, has been patched to prevent potential scams and data breaches.

Unveiling India's Cyber Threat Landscape: Data, Trends, and Resilience

Ransomware attacks were particularly prevalent in the manufacturing sector, which accounted for 30.14% of all attacks targeting India. The most active ransomware group, LockBit 3.0, was responsible for over 61% of these incidents.

NEWS BYTES - INTERNATIONAL



TrueNAS CORE Vulnerability Let Attackers Execute Remote Code

A critical vulnerability in TrueNAS Core has been identified, which allows unauthorized access to sensitive data. Users are strongly urged to update their systems promptly to mitigate potential risks and protect against exploitation by malicious actors.

New 'OtterCookie' malware used to backdoor devs in fake job offers

North Korean threat actors are deploying a new malware variant, OtterCookie, in a campaign targeting software developers with fake job offers. This malware, part of the ongoing Contagious Interview operation, enables data theft and exfiltration of sensitive information. Developers are advised to verify job offers carefully and exercise caution when executing code during interviews.

Dozens of Browser Extensions Vulnerable, Exposing Millions of Users to Data Theft

A phishing attack has compromised at least 35 browser extensions, putting over 2.6 million users at risk of data theft and credential exposure. Attackers injected malicious code into legitimate extensions, allowing them to steal sensitive information such as cookies and access tokens.

Mobile Spear Phishing Targets Executive Teams

Sophisticated mobile spear-phishing campaigns are increasingly targeting corporate executives, using social engineering tactics and impersonating trusted platforms. Recent attacks leveraged fake DocuSign documents and advanced redirection techniques to harvest sensitive credentials, underscoring the need for enhanced mobile security measures..

Critical SSRF Vulnerability (CVE-2024-53353) Found in Invoice Ninja

A critical Server-Side Request Forgery (SSRF) vulnerability (CVE-2024-53353) has been discovered in Invoice Ninja, allowing attackers to access sensitive files on the host server. This flaw can be exploited by both local and low-privileged users during PDF generation, potentially exposing critical information such as database credentials. Users are advised to apply security updates promptly to mitigate the risk.

Thousands Download Malicious npm Libraries Impersonating Legitimate Tools

Threat actors have uploaded malicious typosquats of legitimate npm packages, such as typescript-eslint, resulting in thousands of downloads. These counterfeit versions are designed to install trojans and fetch additional malicious payloads, underscoring the urgent need for enhanced supply chain security in software development.

KEY TRENDS

11

Hindu Business Line

11 Cyber Threats Every Second: India's Digital Expansion Increases the Attack Surface.

2904

CVE Details

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

5.2B

Business Standard

With 5.2 billion encrypted cyberattacks, India ranks second globally.

190K

Security Week

A botnet of 190,000 BadBox-infected Android devices has been discovered.

761

India Today

India detected an average of 761 cyberattacks per minute in 2024.

10.5T

Cobalt.io

Cybercrime costs are projected to rise to $10.5 trillion by 2025.

CYBER INCIDENT ANALYSIS

Data Breach in Healthcare Sector

INDUSTRY

- Healthcare Services

BRIEF SUMMARY

- A cyberattack infiltrated the client's systems via Remote Desktop Protocol (RDP) and used port scanning for reconnaissance. The attacker created a new user account, deployed ransomware, and exfiltrated sensitive data, leading to a major data breach.

ROOT CAUSE ANALYSIS

- **Access via RDP:** Attackers exploited Remote Desktop Protocol (RDP) to gain entry into the network, using legitimate remote execution tools to move laterally across multiple systems.
- **Network Expansion:** This lateral movement enabled them to expand their foothold, compromising additional systems and gaining greater control over the network.
- **Unauthorized Account Creation:** The attackers created an unauthorized administrative account, granting them elevated privileges and access to critical systems.
- **Malicious Activities:** With these heightened privileges, the attackers were able to execute further malicious actions, including accessing additional systems and exfiltrating sensitive data.

LOSS CATEGORIES TO VICTIM

- Brand Reputation, Forensics Cost, Misuse of Resource, Data Loss

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

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

LOSS INCURRED

- Forensic Cost and Legal Cost

RECOMMENDED PREVENTIVE MEASURES

- **Control Remote Access:** Monitor and restrict Remote Desktop Protocol (RDP) access, especially from external IP addresses. Implement strong password policies and enforce frequent credential rotations to enhance security.
- **Implement Security Solutions:** Use Security Information and Event Management (SIEM) for centralized logging, deploy Intrusion Detection/Prevention Systems (IDS/IPS) to detect suspicious activities in real time, and implement Data Loss Prevention (DLP) measures to block unauthorized data transfers.
- **Enhance Network Security:** Limit unnecessary external access, segment networks to protect sensitive systems, disable unused services like FTP and weak SSH, and perform regular secure backups. Regularly test disaster recovery plans to ensure an effective response to breaches.

CYBER INCIDENT ANALYSIS

Malware Incident in Banking Sector

INDUSTRY

- Banking and Financial Services

BRIEF SUMMARY

- On December 15, 2024, unusual network activity indicated a security breach involving ElizaRAT malware. The malware was introduced through a phishing email with a malicious attachment, granting unauthorized access to the network. This compromise resulted in the exfiltration of sensitive client information.

ROOT CAUSE ANALYSIS

- **Triggering Event:** The security incident was triggered when an employee inadvertently opened a malicious attachment in a phishing email, activating the ElizaRAT malware.
- **Bypassing Protections:** This action allowed the malware to bypass inadequate endpoint security measures, enabling its entry into the network.
- **Network Compromise:** Once inside, the malware granted unauthorized access and facilitated the exfiltration of sensitive client data.

LOSS CATEGORIES TO VICTIM

- Brand Reputation, Data Breach, Operational Impact

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- The insurer assisted the organization in liaising with a digital forensics and incident response expert to assess the impact of the incident and provide recommendations for remediation.
- The insurer also facilitated the appointment of legal counsel to assist with cross-border regulatory reporting.

LOSS INCURRED

- Approximately ₹12 crore, including operational recovery and reputational damage management.

RECOMMENDED PREVENTIVE MEASURES

- **Implement Email Protection:** Deploy advanced email filtering systems to effectively block phishing attempts and prevent malicious emails from reaching employees.
- **Regular Employee Training:** Offer ongoing training programs to help staff identify and respond to cyber threats, reinforcing their ability to recognize phishing schemes and other potential attacks.
- **Strengthen Access Security:** Enforce multi-factor authentication (MFA) across all accounts to bolster security and reduce the risk of unauthorized access. Establish strong incident response protocols, regularly tested to ensure readiness.
- **Proactive Cybersecurity Approach:** This incident highlights the critical importance of adopting proactive cybersecurity measures to mitigate risks and ensure business continuity.

ADVISORIES

SUMMARY ON CISA'S ORDER FOR MICROSOFT 365 SECURITY

- **Mandatory Security Measures:** CISA has instructed federal agencies to implement specific security measures to protect their Microsoft 365 tenants from potential cyber threats.
- **Deadline for Compliance:** Agencies must complete these security enhancements by the specified deadline to ensure timely risk mitigation.
- **Focus on Configuration and Access Controls:** The advisory highlights the importance of proper configuration settings and access controls to protect sensitive data within Microsoft 365 environments.
- **Ongoing Monitoring and Assessment:** Agencies are required to establish continuous monitoring and assessment protocols to effectively identify and address vulnerabilities.

Read more at: CISA orders federal agencies to secure Microsoft 365 tenants

CISA ALERT ON FORTINET SECURITY UPDATES

- **Vulnerability Addressed:** Fortinet has released a security update for FortiManager to address a critical vulnerability that could allow remote cyber threat actors to gain control of affected systems.
- **Urgent Action Recommended:** Users and administrators are strongly advised to review the Fortinet Security Bulletin and promptly apply the necessary updates to mitigate risks.
- **Potential Exploitation Risks:** The vulnerability presents significant risks, underscoring the importance of maintaining up-to-date security measures in network management systems.
- **Continuous Monitoring Encouraged:** Organizations should implement continuous monitoring practices to detect any signs of exploitation related to this vulnerability.

Read more at: CISA Alert on Fortinet Security Updates