

Threat Intel Report: July 8-14, 2024

Countries



Top Tags

Mallox

jQuery

Gh0st RAT

XMRig

NullBulge

Executive Summary

Actionable Information:

- *Increasing Exploitation of Software Vulnerabilities:* There is a clear trend of attackers exploiting critical vulnerabilities across various platforms and software. Organizations must prioritize timely patching and updates to mitigate these risks.
- *Sophisticated Malware and Ransomware Attacks:* The use of advanced evasion techniques and the targeting of multiple operating systems, such as Linux and Windows, are becoming more common. Enhanced malware detection and response strategies are crucial.
- *Supply Chain and Third-Party Risks:* The persistent distribution of trojanized software packages indicates a growing threat to supply chains. Rigorous vetting and monitoring of third-party components are essential to secure development environments.
- *Data Breaches and Information Exposure:* The frequent occurrence of data breaches underscores the need for robust data protection measures and incident response plans to safeguard sensitive information.

Outlook:

The landscape of cyber threats continues to evolve, with attackers increasingly targeting critical infrastructure and exploiting software vulnerabilities. The trend towards more sophisticated and targeted attacks, such as the coordinated exploitation of multiple vulnerabilities in platforms like ServiceNow and the use of advanced evasion techniques in malware, indicates a growing need for comprehensive and proactive security measures. The increased focus on supply chain attacks, as evidenced by the trojanized NPM packages, highlights the necessity for rigorous vetting of third-party components. Organizations must prioritize patch management, strengthen their cybersecurity frameworks, and ensure



rapid response capabilities to mitigate the impact of these persistent and complex threats. Looking forward, we anticipate a continued rise in targeted ransomware attacks and data breaches, necessitating an ongoing commitment to cybersecurity vigilance and innovation.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 736% [CVE-2023-28770](#)

- A sensitive information exposure vulnerability in Zyxel

📈 411% [CVE-2023-40044](#)

- A deserialization of untrusted data vulnerability in WS_FTP server

📈 365% [CVE-2023-49070](#)

- A code injection vulnerability in Apache OFBiz

German Telecom Company Hit By 1M RPS DDoS Attack

+Germany +Telecommunications +DDoS

- A German telecommunications company was hit by a 1M requests per second (RPS) application-layer DDoS attack this week, coming from 3,500 distinct IPs. Such attacks on telecom companies are often motivated by attempts to disrupt critical communication services and cause operational chaos, highlighting the strategic importance of these targets for malicious actors.

Account Takeover Attack Targets US FSI Site

+US +Financial Services +ATO

- This week, a US financial services site was targeted by account takeover in a two-day attack, leveraging bots to conduct brute force attempts. Such attacks aim to gain unauthorized access to user accounts, highlighting the critical need for enhanced security measures like multi-factor authentication to protect sensitive financial data.

Recent Cyber Threats

ServiceNow Vulnerability Exposes All Data

+CVE +Unauthorized Access

- Researchers have discovered a critical chain of three vulnerabilities in [ServiceNow](#) that allow unauthorized access to all data in the platform. The vulnerabilities include an authentication bypass, privilege escalation, and arbitrary data access. These flaws were found during an audit of publicly accessible ServiceNow instances.

New Malware Variant Evades Wordfence

+Malware +WordPress

- Researchers identified a new malware variant capable of evading [Wordfence](#), a popular WordPress security plugin. The malware uses obfuscation techniques to bypass detection and infect websites. This discovery highlights the evolving sophistication of malware targeting WordPress sites.

Mallox Ransomware Targets Linux Systems

+Mallox +Ransomware +Linux

- A new variant of [Mallox](#) ransomware has been discovered targeting Linux systems, expanding its previous focus on Windows environments. The ransomware encrypts files and demands a ransom for decryption, posing a threat to businesses using Linux. This marks a significant expansion in the attack surface for the Mallox group.

Trojanized jQuery Found in NPM Packages

[+jQuery](#) [+NPM Packages](#) [+Trojan](#)

- Recently, researchers uncovered a persistent campaign distributing trojanized versions of [jQuery](#) through NPM packages. These malicious packages include backdoors that can compromise development environments. The campaign has been ongoing for months, affecting numerous developers.

WordPress Calendar Plugin Exploited

[+WordPress](#)

- Hackers are actively exploiting vulnerabilities in the WordPress [Simple Calendar](#) plugin, which is used by over 150,000 sites. The vulnerabilities allow for unauthorized access and potential data breaches. Users are urged to update their plugins to mitigate these risks.

OpenSSH Flaw CVE-2024-6409 Exploited

[+OpenSSH](#) [+RCE](#) [+CVE](#)

- A new critical vulnerability in [OpenSSH](#), CVE-2024-6409, is being actively exploited by attackers. This flaw allows for remote code execution, potentially compromising secure shell communications. Users are advised to apply patches immediately to secure their systems.

Universal Code Execution via Browser Extensions

[+XSS](#)

- A vulnerability in browser extensions has been discovered that allows for [universal code execution](#) across different browsers. This flaw can be exploited through malicious extensions, posing a significant risk to users. The discovery underscores the need for enhanced security measures in browser extension development.

PHP Flaw CVE-2024-4577 Actively Exploited

[+PHP](#) [+CVE](#) [+Malware](#)

- The [PHP vulnerability](#) CVE-2024-4577, a critical flaw allowing attackers to execute arbitrary code on affected web servers, is being actively exploited in the wild. Multiple threat actors are exploiting this vulnerability to deliver multiple malware families, including Gh0st RAT, RedTail cryptominers, and XMRig.

Cyberattack Disrupts Macau Government Websites

[+Macau](#) [+Government](#)

- Several [Macau](#) government websites were hit by a DDoS attack, causing significant disruptions. The attack targeted critical infrastructure, impacting public services and information access. Authorities are investigating the breach to determine the extent of the damage and prevent future incidents.

Data Breaches

AT&T Breach Linked to American Hacker, \$370K Ransom Paid

[+Telecommunications](#) [+US](#)

- [AT&T](#) experienced a data breach orchestrated by an American hacker, leading the telecom giant to pay a \$370,000 ransom to secure their data. The breach exposed sensitive customer information, including names, social security numbers, and account details.

Disney Slack Data Leak Exposes Internal Information

[+Entertainment](#) [+NullBulge](#)

- A hacker group known as NullBulge accessed and leaked internal communications from [Disney's](#) Slack channels. The breach exposed sensitive information about upcoming projects, internal processes, and employee discussions. The leaked data included details on unreleased content and internal Disney strategies, potentially impacting the company's operations and competitive standing.

Rite Aid Cybersecurity Breach Exposes Customer Data

+US +Healthcare

- [Rite Aid](#) disclosed that customer data was accessed in a cybersecurity breach that occurred in June. The breach compromised personal information, including names, addresses, and prescription details of an undisclosed number of customers. The incident underscores the ongoing vulnerability of personal data in the retail and healthcare sectors and the need for robust security measures.

Philadelphia City Data Breach Affects 35,000 Email Accounts

+US +Government

- A data breach in [Philadelphia's](#) city email system affected approximately 35,000 email accounts, exposing sensitive information. The compromised data included personal details of city employees and communications containing confidential information. The breach has significant implications for the city's operations and employee privacy, prompting an urgent review of security protocols and response measures.

Imperva Protection

Imperva provides comprehensive digital security solutions, including protection against threats to web applications and APIs— including security vulnerabilities, fraud, and bad bots, data security solutions, and security against disruptive network- and application-level DDoS attacks.