

Threat Intel Report: September 16-22, 2024

Countries



Top Tags

HTTP

INC

GitHub

eCommerce

Crypto

Executive Summary

Actionable Information:

- **Emerging Exploitation of HTTP Headers:** Attackers are increasingly abusing HTTP headers to inject malicious payloads for lateral movement within enterprise environments. This highlights the need for stricter HTTP security measures and real-time monitoring to detect anomalous traffic patterns.
- **E-commerce Targeted via Sophisticated Skimmers:** A WooCommerce skimmer is stealing payment details by embedding malicious code into style tags, bypassing traditional security. E-commerce platforms must enhance detection measures, including server-side integrity checks and regular code audits.
- **High-Risk Vulnerabilities in Core Systems:** Critical vulnerabilities such as CVE-2024-6091 (AutoGPT) and CVE-2024-40711 (Veeam Backup & Replication) expose systems to remote code execution and potential ransomware attacks. Both vulnerabilities are rated 9.8 CVSS, making immediate patching essential, especially for industries reliant on AI or backup infrastructure.
- **Rising Threat of Supply Chain and Third-Party Breaches:** Incidents at Salesforce (public link manipulation), Harvey Nichols (third-party supplier), and GitHub (malware scanner) underline how supply chain vulnerabilities are becoming a significant attack vector. Organizations must enforce stricter security practices with third-party vendors and review their software dependencies for potential malware.
- **Nation-State Espionage and Ransomware Escalation:** North Korean hackers continue to target critical infrastructure, including the energy and defense sectors, while a new ransomware group, INC, is ramping up attacks on U.S. businesses. These campaigns emphasize the need for enhanced defenses against both espionage and ransomware, particularly in high-risk industries.

Outlook:

The recurring themes this week revolve around critical vulnerabilities, supply chain threats, and targeted attacks from both cybercriminals and nation-states. As attackers increasingly exploit weaknesses in infrastructure and third-party systems, organizations must prioritize patch management, vendor risk assessments, and advanced threat detection. Looking ahead, we can expect ransomware gangs to further leverage unpatched critical vulnerabilities, while nation-state actors continue focusing on espionage against key industries. The growing sophistication of skimming and malware techniques also suggests that sectors like e-commerce and open-source development will face heightened risks in the near future.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 345% [CVE-2024-4885](#)

- An unauthenticated Remote Code Execution vulnerability in Progress WhatsUpGold.

📈 288% [CVE-2023-34362](#)

- A SQL injection vulnerability in the Progress MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database.

📈 244% [CVE-2023-49070](#)

- Pre-authentication RCE in Apache Ofbiz due to XML-RPC no longer maintained but still present.

Canadian Rewards Site Faces Bot-Driven Business Logic Attacks Targeting Authentication

+Canada +Rewards +Business Logic

- This week, a Canadian rewards site was targeted by business logic attacks, reaching over 12 million requests in one day. The attacks came from bots, and targeted the site's authentication portal, likely in an attempt to exploit weaknesses in the site's authentication workflows, and allow bots to exploit discount systems, redeem points fraudulently, or even lock legitimate users out of their accounts.

US Financial Services Site Hit by Mobile-Based Account Takeover Attempts

+US +Financial Services +ATO

- A US financial services site was attacked by account takeover attempts this week, coming entirely from clients listed as mobile browsers. The attack attempts reached 15 million requests over two days, and targeted the mobile version of the site, probably in an attempt to evade detection and take advantage of the site's mobile-specific business logic, such as weaker session management or less stringent rate limits.

Recent Cyber Threats

Attackers Exploit HTTP Headers for Lateral Movement

+HTTP

- Cybercriminals are abusing [HTTP headers](#) to inject malicious payloads into target systems, enabling lateral movement and data theft. By manipulating these headers, attackers bypass traditional detection mechanisms and escalate their privileges within networks, posing a significant threat to enterprise environments. This technique has been seen across multiple industries, emphasizing the need for stricter HTTP security measures.

WooCommerce Skimmer Steals Credit Card Data via Style Tags

+eCommerce +Skimmer

- A new [WooCommerce](#) skimmer is stealing credit card details by embedding malicious code in style tags and fake image extensions. The skimmer loads silently on compromised sites, harvesting customer payment data during checkout. This attack is highly sophisticated, bypassing many traditional detection methods and potentially affecting thousands of e-commerce websites globally.

Critical AutoGPT Vulnerability Exposes 166K Projects

+CVE +AI

- A critical vulnerability (CVE-2024-6091, CVSS 9.8) has been discovered in [AutoGPT](#), affecting over 166,000 projects. The flaw allows attackers to execute arbitrary code, potentially leading to data loss and system compromises across various industries relying on automated AI systems. This vulnerability underlines the risks of using unvetted AI tools in critical infrastructure.

Critical Veeam Vulnerability Could Be Exploited by Ransomware Gangs

+CVE +Ransomware

- The remote code execution (RCE) vulnerability CVE-2024-40711 in [Veeam Backup & Replication](#) could soon be used by ransomware gangs to target unpatched servers worldwide. The vulnerability, with a CVSS score of 9.8, could allow an attacker to gain full control of a system, manipulate data, and potentially move laterally within a network, making it a high-value target.

Salesforce Public Link Manipulation Puts Data at Risk

+Business

- A vulnerability in [Salesforce](#) public links can be exploited to expose sensitive data by manipulating how shared files are accessed. Attackers can gain unauthorized access to confidential information by adjusting URL parameters, highlighting a major risk for organizations relying on public sharing features in their Salesforce environments.

Construction Industry Software Vulnerability Risks Client Data

+Construction +Financial Services

- A vulnerability in [Foundation Software's](#) accounting tool, used widely in the construction industry, could allow attackers to execute arbitrary code and gain access to sensitive client financial data. Exploiting this flaw could lead to widespread data breaches affecting contractors and their clients, emphasizing the need for immediate patches.

North Korean Hackers Target Energy and Defense Sectors

+North Korea +Energy +Government

- [North Korean hackers](#) are actively targeting energy and defense sectors in an espionage campaign, using spear-phishing techniques to compromise email accounts and gain access to critical information. The campaign aims to steal intellectual property and strategic data, posing a significant threat to national security and global energy infrastructure.

Microsoft Warns of New INC Ransomware Campaign

+INC +Ransomware

- Microsoft has issued a warning about a new ransomware group, [INC](#), which has launched attacks against U.S. businesses, focusing on encrypting corporate networks and demanding high-value payouts. This ransomware exploits vulnerabilities in enterprise systems, disrupting operations and threatening financial stability for the targeted organizations.

GitHub Scanner Campaign Abuses Repositories to Push Malware

+GitHub +Scanner +Malware

- A clever malware campaign is abusing [GitHub repositories](#) to scan for and infect vulnerable projects. By injecting malicious code into legitimate repositories, the attackers aim to compromise the software supply chain, pushing malware to developers who unknowingly integrate infected code into their projects. This campaign highlights the growing risks of open-source software dependencies.

Data Breaches

Dell Suffers Second Security Breach in a Week

[+Computing & IT](#)

- [Dell](#) has experienced a second security breach in the span of a week, exposing customer support data. Attackers exploited vulnerabilities in Dell's internal systems, potentially compromising user information such as service histories and support tickets. The breach raises concerns over Dell's cybersecurity measures and the potential for future, more damaging attacks.

Indodax Crypto Exchange Pledges to Reimburse After Theft

[+Indonesia](#) [+Crypto](#) [+Financial Services](#)

- Indonesia-based [Indodax](#) crypto exchange has promised to reimburse users affected by a recent theft, where attackers managed to steal an undisclosed amount of cryptocurrency. The exchange is working closely with authorities to investigate the breach and strengthen its security protocols to prevent future incidents. The attack highlights ongoing security challenges in the cryptocurrency industry.

Harvey Nichols Faces Data Breach via Third-Party Supplier

[+Retail](#) [+Third-Party](#) [+UK](#)

- High-end retailer [Harvey Nichols](#) has fallen victim to a data breach through a third-party supplier, exposing sensitive customer information. The breach, affecting shoppers' personal and payment data, raises questions about the security of supply chain partners and their role in maintaining robust cybersecurity defenses. This incident adds to the growing number of breaches linked to third-party vendors in the retail industry.

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.