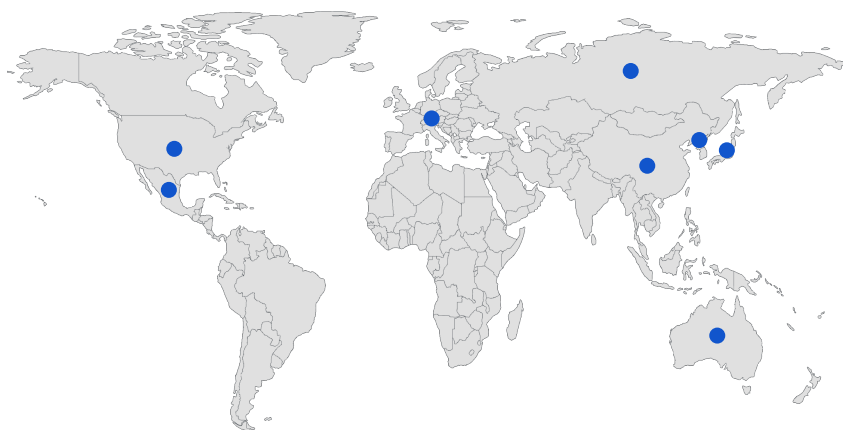


Threat Intel Report: March 10-16, 2025

Countries



Top Tags

Lazarus

Ballista

PlayPraetor

APT37

Lumma Stealer

Executive Summary

Actionable Information:

- **Supply Chain and Open-Source Exploitation on the Rise:** Attackers are increasingly targeting open-source ecosystems and supply chains, leveraging vulnerabilities in npm, GitHub repositories, and WordPress plugins to distribute malware and gain unauthorized access.
- **Persistent Remote Code Execution (RCE) and IoT Threats:** Unpatched software and IoT devices remain prime targets for botnets and cyber espionage, with RCE vulnerabilities in web applications, routers, and industrial systems being actively exploited.
- **Growing Threat from Nation-State and Financially Motivated Attacks:** State-sponsored cyber actors, particularly from North Korea, continue targeting developers and mobile users for espionage, while financially motivated threat actors exploit businesses, education institutions, and online gambling platforms for profit.
- **Malware and Phishing Tactics Becoming More Sophisticated:** Cybercriminals are refining their attack techniques, using fake CAPTCHAs, AI-generated repositories, and malicious mobile apps to bypass traditional security measures and steal sensitive data.

Outlook:

The cybersecurity landscape continues to evolve, with adversaries exploiting vulnerabilities in widely used open-source frameworks, IoT devices, and enterprise networks. Nation-state actors remain a persistent threat, particularly in espionage-driven campaigns targeting developers and mobile ecosystems. Meanwhile, financially motivated attacks are broadening in scope, hitting industries beyond traditional finance and retail, such as consulting firms, online casinos, and public education. Organizations must adopt proactive security measures, including stricter patch management, enhanced monitoring of supply chain dependencies, and improved user awareness to combat these emerging threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,466% [CVE-2024-25600](#)

- Improper Control of Generation of Code ('Code Injection') vulnerability in Codeer Limited Bricks Builder allows Code Injection. This issue affects Bricks Builder: from n/a through 1.9.6.

↑ 795% [CVE-2024-55956](#)

- In Cleo Harmony before 5.8.0.24, VLTrader before 5.8.0.24, and LexiCom before 5.8.0.24, an unauthenticated user can import and execute arbitrary Bash or PowerShell commands on the host system by leveraging the default settings of the Autorun directory.

↑ 452% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction. Exploitation of this issue requires the admin panel be exposed to the internet.

US Beverage Company Targeted by Application DDoS

+US +Germany +Food & Beverage +DDoS

- A popular US food & beverage company was attacked by application layer (L7) DDoS this past week, reaching almost 1.5 million requests in just over three hours. Attacks came from over 10,000 IPs, based in the US and Germany, that had an average risk score of 60%.

Travel Company Targeted by Advanced Bots

+US +Russia +Travel +Account Takeover

- A travel company was recently targeted in a large account takeover attack, reaching 1.3 million login attempts in one day. The attacks were primarily conducted by advanced bots with the ability to act like a human user and came from US and Russia-based IPs.

Recent Cyber Threats

Imperva Shields Against Apache Camel Header Injection Flaw

+Apache Camel +Header Injection

- A vulnerability identified as [CVE-2025-27636](#) in the Apache Camel framework allows attackers to bypass header filtering using miscased headers. This flaw specifically affects configurations utilizing HTTP server components in combination with the camel-bean component on beans implementing multiple methods. Imperva has implemented protections against this vulnerability to safeguard affected systems.

Hidden Commands Uncovered in Widely Used Bluetooth Chip

+IoT +Backdoor

- Researchers have discovered 29 undocumented commands in the [ESP32](#) microchip, produced by Espressif and embedded in over a billion IoT devices. These hidden commands can be exploited for memory manipulation, device impersonation, and packet injection, potentially leading to unauthorized data access and

persistent threats. Espressif has not publicly documented these commands, raising concerns about their intentional or accidental inclusion.

PHP-CGI Flaw Exploited in Attacks on Japanese Sectors

+Japan +Cobalt Strike +Powershell +Mimikatz +Telecommunications +Entertainment +Education +eCommerce

- Threat actors have exploited a remote code execution vulnerability, [CVE-2024-4577](#), in the PHP-CGI implementation on Windows systems to infiltrate organizations in [Japan](#). Post-exploitation activities include deploying Cobalt Strike, executing PowerShell scripts, and employing tools like Mimikatz for credential theft. The attackers have targeted various sectors, including technology, telecommunications, entertainment, education, and e-commerce, indicating a broad and potentially espionage-driven campaign.

Lazarus Group Targets npm with Malicious Packages

+North Korea +Lazarus +npm

- The North Korean state-sponsored [Lazarus Group](#) has introduced six malicious packages into the npm ecosystem, aiming to compromise developer environments. These packages are designed to steal credentials and deploy backdoors, posing significant risks to software supply chains. The discovery underscores the persistent threat posed by Lazarus and the need for vigilance in managing open-source dependencies.

Ballista Botnet Exploits TP-Link Router Vulnerability

+Ballista +US +Australia +China +Mexico

- The [Ballista](#) botnet is actively exploiting an unpatched remote code execution vulnerability, [CVE-2023-1389](#), in TP-Link Archer AX-21 routers. This botnet has infected over 6,000 devices worldwide, targeting sectors such as manufacturing, healthcare, services, and technology across countries including the United States, Australia, China, and Mexico. The malware establishes encrypted command-and-control channels, enabling attackers to execute further malicious activities, highlighting the critical need for timely patch management.

Critical Vulnerability in WooCommerce Plugin Endangers 100,000+ Sites

+WordPress +Plugin +WooCommerce +eCommerce +Retail

- A severe vulnerability, identified as [CVE-2025-1661](#), has been discovered in the "HUSKY – WooCommerce Products Filter Professional" WordPress plugin, affecting over 100,000 online stores. This flaw allows unauthenticated attackers to execute arbitrary files on affected servers, potentially leading to data breaches, site defacement, and full system control. Store owners are strongly advised to update the plugin to version 1.3.6.6 to mitigate this critical risk.

PlayPraetor Malware Masquerades as Legitimate Apps to Target Android Users

+PlayPraetor +Google Play

- The [PlayPraetor](#) malware campaign involves the creation of fake Google Play Store websites that trick users into downloading malicious Android applications. These apps, disguised as legitimate software, are advanced banking Trojans designed to steal sensitive information, including banking credentials and clipboard data. The operation has been linked to over 6,000 fraudulent web pages, primarily targeting users in South-East Asia.

North Korean Spyware 'KoSpy' Infiltrates Google Play Store

+North Korea +APT37 +StarCrufft +KoSpy

- Researchers have uncovered that the North Korean state-sponsored group [APT37](#), also known as ScarCrufft, has been distributing an Android spyware dubbed 'KoSpy' through Google Play and third-party app stores. Masquerading as utility apps like file managers and software updates, KoSpy can collect extensive data, including SMS messages, call logs, location information, files, audio, and screenshots. The spyware has been active for at least three years, targeting both Korean and English-speaking users.

AI-Generated Fake GitHub Repositories Spread Malware

+AI +Malware +Lumma +SmartLoader +GitHub

- A sophisticated malware campaign has been identified, wherein threat actors use AI-generated content to create fake GitHub repositories. These repositories distribute [SmartLoader](#), a loader that subsequently delivers Lumma Stealer and other malicious payloads. The malware is designed to steal sensitive data, including

cryptocurrency wallets, two-factor authentication extensions, and personally identifiable information, leading to identity theft and financial fraud.

Fake CAPTCHA Pages Deploy Malware on Windows Systems

[+Malware](#) [+Lumma](#) [+Vidar](#)

- Cybercriminals are leveraging fake CAPTCHA verification techniques to distribute [malware](#) targeting Windows users. These deceptive CAPTCHA prompts trick users into executing PowerShell commands, initiating a multi-stage attack chain that leads to the deployment of information stealers like Lumma and Vidar. The malware exfiltrates sensitive data and maintains persistence on infected systems, posing significant security risks.

Data Breaches

South Carolina School District Disables Systems Following Cybersecurity Breach

[+US](#) [+Education](#)

- The [Cherokee County School District](#) in South Carolina experienced a network security incident affecting its computer systems. Upon discovery, the district initiated an investigation and is collaborating with the FBI, South Carolina Law Enforcement Division (SLED), and the Cherokee County Sheriff's Office to assess the breach's scope and reinforce security measures. Students and staff have been advised against connecting to the district's network, and upcoming classes will proceed without reliance on technological systems.

Accounting Firm Alerts 217,000 Individuals to Health Data Breach

[+US](#) [+Financial Services](#)

- A US [accounting firm](#) is notifying approximately 217,000 individuals about a data breach that compromised sensitive health information. The breach involved unauthorized access to personal and health data, potentially exposing affected individuals to identity theft and fraud. The firm is offering resources and support to those impacted as it continues to investigate the incident and enhance its security protocols.

Cyberattack Hits Berkeley Research Group Amidst Acquisition Deal

[+US](#) [+Consulting](#) [+Business](#)

- [Berkeley Research Group \(BRG\)](#), a management consulting firm based in Emeryville, California, suffered a cyberattack on March 2, 2025. The attackers claimed to have stolen data and encrypted files within BRG's network, issuing multiple ransomware notices. The incident coincided with BRG's ongoing \$700 million leveraged buyout by TowerBrook Capital Partners, potentially impacting the acquisition process.

Merkur Casino Security Incident Exposes Data of 800,000 Players

[+Germany](#) [+Gambling](#)

- [Merkur Casino](#) experienced a security incident that compromised the personal data of approximately 800,000 players. The breach exposed sensitive information, including names, addresses, and contact details, potentially leading to identity theft and fraud. The company is investigating the breach and has notified affected individuals, advising them to monitor their accounts for suspicious activity.

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.