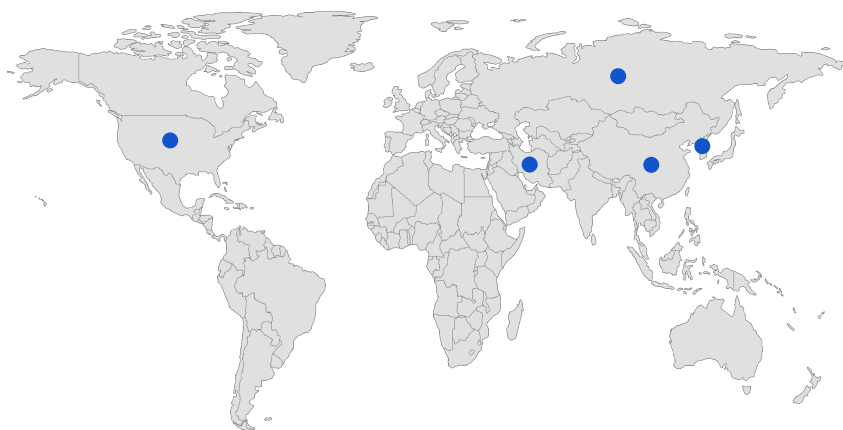


Threat Intel Report: March 17-23, 2025

Countries



Top Tags

Apache

ZDI-CAN-25373

DollyWay

AgeGate

rose87168

Executive Summary

Actionable Information:

- **Exploitation of Open-Source Components Continues to Rise:** Attackers are increasingly targeting widely used open-source software, including web servers and development frameworks. The rapid release of proof-of-concept exploits and the lag in patch adoption create a critical window for exploitation, highlighting the need for organizations to prioritize vulnerability management and monitor third-party dependencies closely.
- **WordPress Ecosystem Remains a Prime Target:** Malware campaigns and plugin-specific vulnerabilities continue to plague WordPress-based websites, especially those tied to e-commerce. Attackers exploit unpatched or misconfigured plugins to gain persistent access or redirect traffic, underscoring the need for tighter security controls, routine plugin updates, and stronger web application firewalls in the CMS ecosystem.
- **State-Sponsored Cyber Activity is Persistent and Strategic:** Long-running campaigns by nation-state actors demonstrate a focus on stealthy exploitation of overlooked or low-profile vulnerabilities. These efforts often go undetected for years and reflect a shift toward long-term access, cyber espionage, and data exfiltration rather than immediate disruption.
- **Blending of Cyber and Physical Threats Increases:** Recent incidents show the use of doxing, public exposure, and politically motivated cyber activity to target individuals and organizations. These tactics blur the lines between online harassment and real-world risk, requiring coordination between cybersecurity, legal, and physical security teams.
- **False Breach Claims and Data Leak Misinformation on the Rise:** The use of fabricated or unverified data breach claims as a tactic for extortion or reputational harm is becoming more common. Organizations must be prepared to investigate and respond quickly to such claims, balancing transparency with a clear assessment of actual risk.

Outlook:

This week's threat landscape shows a convergence of classic attack vectors—unpatched software, supply chain plugins, and state-backed operations—with emerging psychological and reputational threats, including doxing and breach disinformation. Nation-state exploitation of overlooked vulnerabilities, paired with ongoing large-scale WordPress infections, highlights the continued importance of proactive patch management and layered web application defenses. Meanwhile, the abuse of leaked or fabricated data for political messaging or extortion underlines the growing need for coordinated legal, PR, and cybersecurity responses to handle public-facing threats. Expect continued exploitation of open-source component vulnerabilities and further blending of cyber and socio-political campaigns targeting organizations in tech, healthcare, and critical infrastructure.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 152,425% [CVE-2025-29891](#)

- Bypass/Injection vulnerability in Apache Camel. This issue affects Apache Camel: from 4.10.0 before 4.10.2, from 4.8.0 before 4.8.5, from 3.10.0 before 3.22.4. Users are recommended to upgrade to version 4.10.2 for 4.10.x LTS, 4.8.5 for 4.8.x LTS and 3.22.4 for 3.x releases. This vulnerability is present in Camel's default incoming header filter, that allows an attacker to include Camel specific headers that for some Camel components can alter the behaviors such as the camel-bean component, or the camel-exec component.

↑ 7,465% [CVE-2024-11972](#)

- The Hunk Companion WordPress plugin before 1.9.0 does not correctly authorize some REST API endpoints, allowing unauthenticated requests to install and activate arbitrary Hunk Companion WordPress plugin before 1.9.0 from the WordPress.org repo, including vulnerable Hunk Companion WordPress plugin before 1.9.0 that have been closed.

↑ 1,617% [CVE-2024-9463](#)

- An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.

US Entertainment Site Targeted by ATO

+US +Entertainment +ATO

- A US-based entertainment company was recently targeted by account takeover attacks, reaching over 800,000 login attempts in one day. The attacks, which came from 31,000 US-based IPs, were brute force attack attempts targeting login pages.

Financial Services Site Targeted in Automated Attacks

+US +Financial Services +Automated Attack +Path Traversal

- A US-based financial services site was targeted by automated attacks and path traversal last week, reaching almost 4 million attack attempts in one day. Attacks came from just 37 US-based IPs with an average risk score of 44%.

Recent Cyber Threats

Active Exploitation of Apache Tomcat's CVE-2025-24813 Uncovered

+[Apache Tomcat](#) +[CVE](#) +[Remote Code Execution](#)

- Security researchers have identified active exploitation of CVE-2025-24813, a critical remote code execution vulnerability in [Apache Tomcat](#). Attackers are using proof-of-concept exploits published shortly after the flaw's disclosure, sending base64-encoded serialized Java payloads via PUT requests to gain control over unpatched servers. Imperva customers are protected against this vulnerability out-of-the-box.

Apache Camel's CVE-2025-29891 Vulnerability

+[Apache Camel](#) +[CVE](#) +[Header Injection](#)

- A high-severity vulnerability, CVE-2025-29891, has been disclosed in [Apache Camel](#), allowing attackers to inject malicious headers and manipulate application behavior. The flaw affects several HTTP components, including camel-servlet and camel-jetty. This issue affects configurations using HTTP server components combined with the camel-bean component. Imperva customers are protected against this vulnerability out-of-the-box.

Sophisticated Malware Targets WordPress E-commerce Sites

+[WordPress](#) +[WooCommerce](#) +[Credit Card Skimmer](#) +[Backdoor](#)

- Researchers have uncovered a complex malware infection on a [WordPress](#) e-commerce site, featuring a credit card skimmer, a hidden PHP file manager backdoor, and a reconnaissance script. Designed specifically for WooCommerce platforms, the attack aims for financial gain and long-term control by stealing payment information and maintaining persistent access. The malware communicates with malicious domains, now blocklisted, highlighting the need for robust security measures on e-commerce websites.

Unpatched Windows Zero-Day Exploited by Multiple Nation-State Actors

+[ZDI-CAN-25373](#) +[China](#) +[Iran](#) +[North Korea](#) +[Russia](#) +[Windows](#) +[Zero-Day](#)

- An unpatched Windows zero-day vulnerability, identified as [ZDI-CAN-25373](#), has been actively exploited since 2017 by 11 state-sponsored groups from China, Iran, North Korea, and Russia. Attackers leverage crafted Windows Shortcut (.LNK) files with hidden command-line arguments to execute malicious payloads, facilitating data theft and cyber espionage. Despite its active exploitation, Microsoft has classified the issue as low severity and does not plan to release a fix.

DollyWay Malware Campaign Compromises Over 20,000 WordPress Sites

+[WordPress](#) +[DollyWay](#)

- Since 2016, the [DollyWay](#) malware operation has compromised over 20,000 WordPress sites globally, redirecting users to malicious destinations. The campaign exploits vulnerabilities in plugins and themes, employing advanced evasion and re-infection techniques. Web administrators are advised to update their WordPress installations and plugins to prevent exploitation.

Critical Vulnerability in WordPress Age Gate Plugin Exposes Over 40,000 Sites

+[WordPress](#) +[AgeGate](#) +[LFI](#)

- A critical vulnerability, [CVE-2025-2505](#), has been identified in the Age Gate plugin for WordPress, affecting over 40,000 websites. The flaw allows unauthenticated remote code execution via a Local PHP File Inclusion vulnerability through the 'lang' parameter. Site administrators are strongly encouraged to update to the patched version 3.5.4 to mitigate potential exploits, and Imperva customers are protected against this vulnerability out-of-the-box.

Data Breaches

Oracle Refutes Hacker's Claim of 6 Million Record Breach

+[rose87168](#) +[SSO](#)

- A threat actor known as rose87168 claimed to have stolen 6 million records from [Oracle Cloud's](#) Single Sign-On (SSO) platform, offering data including encrypted passwords and key files for sale. Oracle has denied any breach of its cloud services, stating that the published credentials are not from Oracle Cloud and that no customer data has been compromised. The hacker attempted to provide proof by uploading a text file to Oracle's server, but Oracle maintains its systems remain secure.

DogeQuest Website Doxes Tesla Owners Amid Rising Tensions

[+Automotive](#) [+DOGE](#)

- A website named [DogeQuest](#) has emerged, publishing personal information of Tesla owners and employees of the Department of Government Efficiency (DOGE), led by Elon Musk. The site features an interactive map displaying names, addresses, and contact details, with a Molotov cocktail cursor, highlighting Tesla dealerships and Supercharger stations. This development coincides with escalating protests against Musk's political involvement and recent budget cuts by DOGE, leading to increased harassment and vandalism targeting Tesla assets and owners.

OrthoMinds Data Exposure Potentially Affects Thousands

[+Healthcare](#) [+US](#)

- [OrthoMinds](#), a provider of orthodontic practice management software based in Georgia, announced a security incident that may have exposed patients' protected health information (PHI). Between November 17 and 27, 2024, parts of its network were accessible to unauthorized external parties. Compromised data includes names, dates of birth, medical and health insurance information, payment card details, and Social Security numbers.

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.