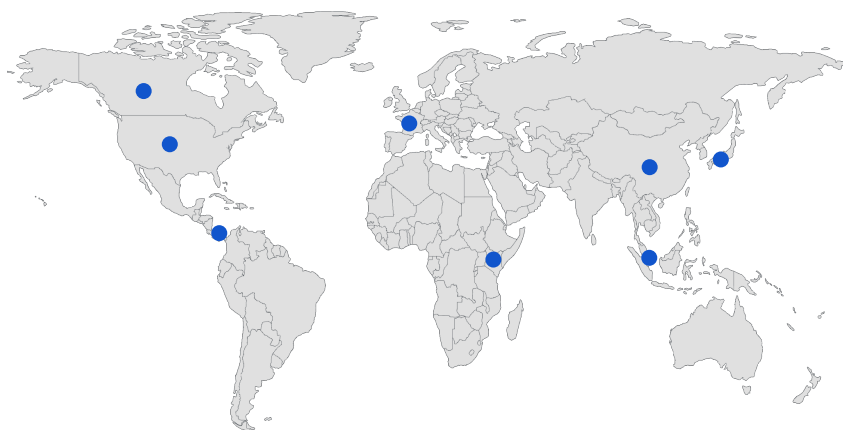


Threat Intel Report: January 27- February 2, 2025

Countries



Top Tags

XWorm RAT

Akira

AI

Crypto

Remote Access

Executive Summary

Actionable Information:

- **Exploitation of Hardware and Software Vulnerabilities:** Attackers are leveraging both hardware flaws and software vulnerabilities to gain unauthorized access to systems, underscoring the need for comprehensive vulnerability management.
- **Deceptive Malware Distribution Tactics:** The use of social engineering tactics, such as fake CAPTCHA verifications, has become prevalent in distributing malware, exploiting users' trust to bypass security measures.
- **Targeted Data Breaches Across Multiple Sectors:** Significant data breaches have impacted various industries, including healthcare and energy, resulting in the exposure of sensitive personal and financial information.
- **Emergence of AI-Enhanced Cyber Threats:** The integration of artificial intelligence (AI) into cyberattacks has led to more sophisticated and effective threat vectors, including advanced phishing schemes and automated exploitation of vulnerabilities.

Outlook:

The cybersecurity landscape continues to evolve, with threat actors employing increasingly sophisticated methods to exploit vulnerabilities across various sectors. Organizations must remain vigilant, adopting a proactive security posture that includes continuous monitoring, regular updates to security protocols, and comprehensive user education to mitigate emerging threats effectively.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 4,650% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.

📈 2,475% [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.

📈 49% [CVE-2024-23897](#)

- Jenkins 2.441 and earlier, LTS 2.426.2 and earlier does not disable a feature of its CLI command parser that replaces an '@' character followed by a file path in an argument with the file's contents, allowing unauthenticated attackers to read arbitrary files on the Jenkins controller file system.

French Retail Site Targeted in 1.5 M RPS DDoS Attack

[+France](#) [+Retail](#) [+Gaming](#)

- A French gaming retail site was targeted by DDoS this week, with an attack reaching 1.5 million requests per second (RPS) and lasting 10 hours. The attack came from 4,000 distinct IPs, and coincided with the release of a popular role-playing gacha video game.

Attackers Try to Scrape Mexican Retail Sites

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

- A Panamanian bank's online login portal was attacked by account takeover attempts, reaching over 1.5 million logins in one day. The attackers leveraged bots across 109 distinct IPs.

Recent Cyber Threats

Subaru Starlink Vulnerability Allowed Remote Vehicle Control

[+Automotive](#) [+Remote Access](#) [+US](#) [+Canada](#) [+Japan](#)

- Security researchers discovered critical vulnerabilities in Subaru's [Starlink](#) system, enabling remote access to vehicle functions such as unlocking doors, starting the engine, and tracking location. These flaws potentially affected millions of vehicles across the U.S., Canada, and Japan. Subaru promptly patched the vulnerabilities upon notification.

Fake CAPTCHA Campaign Distributes Malware

[+Malware](#)

- A deceptive campaign employing fake [CAPTCHA](#) verifications has been identified, where users are tricked into downloading malware. This tactic exploits users' trust in CAPTCHA systems to bypass security measures, leading to unauthorized access and data theft across various industries.

Hackers Exploit Script Kiddies with Trojanized XWorm RAT Builder

[+XWorm RAT](#) [+Telegram](#)

- Cybercriminals distributed a modified [XWorm RAT](#) builder targeting inexperienced hackers, resulting in the compromise of over 18,000 devices worldwide. The malware exfiltrated sensitive information, including browser credentials and system data, using Telegram for command and control operations.

New Side-Channel Attacks Target Apple CPUs

[+Apple](#) [+Side-Channel Attacks](#)

- Researchers have disclosed new side-channel vulnerabilities in modern [Apple](#) processors, stemming from faulty speculative execution implementations. These flaws could allow attackers to steal sensitive information from web browsers, posing significant security risks to users.

Lightning.AI Platform Vulnerability Exposed Users to Remote Code Execution

+RCE +AI

- A critical flaw in [Lightning.AI's](#) development platform was identified, allowing attackers to gain root access and execute arbitrary code. Exploitation could lead to unauthorized control over users' cloud-based studios and connected systems. The vulnerability has since been patched.

Data Breaches

Phemex Cryptocurrency Platform Suffers \$69 Million Theft

+Singapore +Crypto

- Singapore-based cryptocurrency exchange [Phemex](#) experienced a cyberattack resulting in the theft of over \$69 million in various digital assets, including Ethereum and Bitcoin. The breach forced Phemex to temporarily suspend certain operations and implement manual withdrawal reviews. The company is currently working to restore services and has announced plans to compensate affected users.

Mississippi Electric Utility Data Breach Affects 20,000 Residents

+Utilities +Electric +US +Akira

- The Yazoo Valley Electric Power Association, serving multiple counties in [Mississippi](#), suffered a cyberattack in August 2024 attributed to the Akira ransomware group. The breach exposed personal information of over 20,000 residents, including Social Security numbers and financial records. The utility has since restored its systems and is offering identity protection services to the affected individuals.

Kenya's Business Registration Service Breach Exposes High-Profile Data

+Kenya +Business

- [Kenya's](#) Business Registration Service (BRS) confirmed a significant data breach that exposed sensitive information of numerous private companies, including those associated with prominent political figures. The compromised data includes confidential details about company ownership, directorship, and beneficial owners, potentially compromising the privacy and security of high-profile individuals and businesses.

Community Health Center Data Breach Impacts Over 1 Million Patients

+US +Healthcare

- Connecticut-based [Community Health Center](#) (CHC) disclosed a data breach affecting more than 1 million patients. In mid-October 2024, unauthorized individuals accessed CHC's network, compromising personal and health information, including names, addresses, and medical records. The breach did not disrupt daily operations, and CHC is notifying affected individuals while enhancing security measures.

DeepSeek AI Startup Exposes Over 1 Million Sensitive Records

+China +AI

- Chinese AI startup [DeepSeek](#) suffered a significant data breach, leaving a publicly accessible database containing over 1 million sensitive records, including user data, chat histories, API authentication keys, and system logs. The exposed information posed substantial security risks, potentially allowing unauthorized control over the system and privilege escalation. The vulnerability was promptly addressed upon discovery, but it remains unclear if unauthorized access occurred prior to remediation.

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.