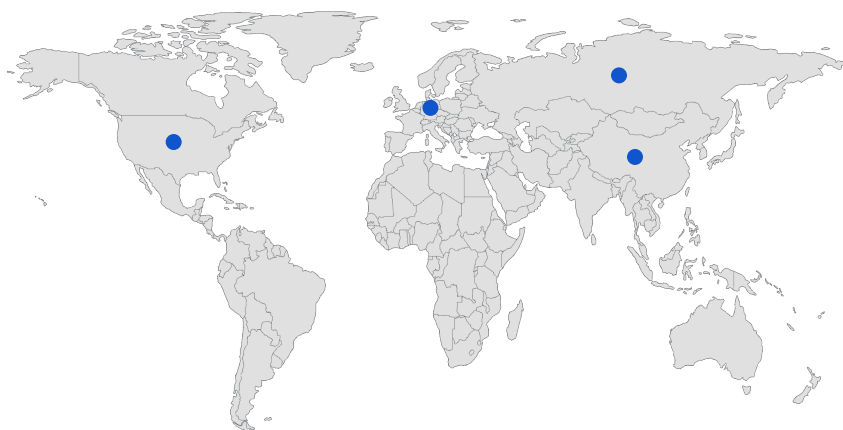


Threat Intel Report: February 10-16, 2025

Countries



Top Tags

Flesh Stealer

nullifAI

8Base

Malware

Magento

Executive Summary

Actionable Information:

- **Increased Supply Chain Vulnerabilities:** Threat actors are increasingly targeting software supply chains, including machine learning models, gaming platforms, and third-party tools, highlighting the need for robust validation and continuous monitoring of external dependencies.
- **Persistent Data Breaches Across Industries:** Critical sectors such as government, healthcare, and IoT manufacturing are experiencing frequent data breaches, exposing sensitive personal and operational data, which increases the risks of identity theft, espionage, and unauthorized access.
- **Ransomware Disruption but Evolving Malware:** While law enforcement operations have successfully disrupted some ransomware operations, cybercriminals continue to innovate, with new malware strains targeting browsers, messaging apps, and financial data through diverse delivery methods.
- **Exploitation of Misconfigurations and Legacy Systems:** Attackers are actively exploiting misconfigured APIs, outdated web infrastructure, and exposed cryptographic keys, emphasizing the importance of securing application frameworks, rotating sensitive keys, and maintaining up-to-date systems.

Outlook:

The cybersecurity landscape continues to evolve with attackers diversifying their methods, from supply chain compromises to large-scale data breaches and innovative malware. While international collaboration has led to notable successes against ransomware groups, emerging threats, especially those exploiting misconfigurations and unprotected systems, will likely increase. Organizations must adopt proactive defenses, particularly around API security, supply chain vetting, and secure key management, to mitigate the expanding attack surface.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,914% [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.

↑ 114% [CVE-2024-12987](#)

- A vulnerability, which was classified as critical, was found in DrayTek Vigor2960 and Vigor300B 1.5.1.4. Affected is an unknown function of the file /cgi-bin/mainfunction.cgi/apmcfupload of the component Web Management Interface. The manipulation of the argument session leads to os command injection. It is possible to launch the attack remotely.

↑ 94% [CVE-2024-45195](#)

- Direct Request ('Forced Browsing') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.16.

CVE-2024-53704 Attacks on the Rise

+CVE +US +Financial Services +Computing +Business

- Attacks targeting CVE-2024-53704—a recently released improper authentication vulnerability in the SSLVPN authentication mechanism—spiked last week, reaching almost 14,000 attack attempts in one day. Attacks targeted US-based sites across several industries, including Financial Services, Computing, and Business.

German Financial Services Site Targeted by Automated Attacks

+Germany +Automated Attack +Financial Services

- Automated attacks targeted a German Financial Services site, reaching 3.5 million requests over two days. Attacks came primarily from IPs based within Germany, and had an average risk score of 60%.

Recent Cyber Threats

Attackers Exploit Exposed ASP.NET Keys for Code Injection

+Code Injection +RCE

- Microsoft warns that attackers are exploiting exposed [ASP.NET](#) machine keys to conduct ViewState code injection attacks, achieving remote code execution on IIS web servers. An attacker used a known key to deliver the Godzilla post-exploitation framework in December 2024. Over 3,000 public keys are at risk, prompting Microsoft to recommend secure key generation and server hardening.

Flesh Stealer Malware Targets Browsers and Messaging Apps

+Flesh Stealer +Russia +Malware

- [Flesh Stealer](#), developed by a Russian-speaking actor, steals credentials from browsers and apps like Signal and Telegram. Active since August 2024, it avoids CIS countries and employs anti-VM/debugging techniques. Promoted on Discord and Telegram, it continuously evolves, now bypassing Chrome's encryption and extracting Wi-Fi credentials.

Google Tag Manager Skimmer Steals Credit Card Data from Magento Site

+eCommerce +Magento +Malware

- Attackers injected a malicious Google Tag Manager script into a [Magento](#) eCommerce site, stealing customers' credit card details. The malware, hidden in the site's database, mimicked legitimate tracking scripts and was linked to Magecart-affiliated attackers. At least six websites were found infected with similar malware, highlighting the ongoing threat to online retailers.

Malicious ML Models Found on Hugging Face Platform

+nullifAI +ML +Malware

- Researchers discovered malware hidden in [machine learning models](#) hosted on Hugging Face, exploiting the Pickle serialization format to execute malicious code. Named *nullifAI*, the attack bypassed Hugging Face's security checks, posing a significant risk to developers using these models. The payload included a reverse shell that connected to a hardcoded IP, highlighting the growing threat of AI supply chain attacks.

Police Dismantle 8Base Ransomware Gang in Operation Phobos Aetor

+Law Enforcement +8Base +Ransomware

- An international law enforcement operation, [Phobos Aetor](#), successfully dismantled the 8Base ransomware gang, known for targeting businesses with double extortion tactics. Authorities arrested key members, seized infrastructure, and disrupted ongoing operations, marking a significant win against ransomware groups. The 8Base gang had been active since 2022, compromising numerous organizations globally.

Malicious Game Removed from Steam Platform

+Gaming +Malware +Steam

- Valve removed the game [PirateFi](#) from its Steam platform after discovering it contained malware that executed on players' systems post-installation. The malware targeted user data and created backdoors for remote access, raising concerns about the security of third-party uploads in digital game marketplaces. Valve advised users who downloaded the game to uninstall it and run antivirus scans.

Data Breaches

Coast Guard Data Breach Exposes Personnel and Pay Information

+US +Government +Military

- A data breach in the [U.S. Coast Guard's](#) Direct Access system exposed sensitive information for over 1,100 personnel, including banking details. The breach delayed payments and prompted the Coast Guard to take the system offline for investigation. Coast Guard Cyber Command and the Investigative Service are working to identify the source and secure systems.

Massive IoT Data Breach Exposes 2.7 Billion Records

+IoT +China

- A major data breach involving [Mars Hydro](#), a Chinese IoT manufacturer, exposed 2.7 billion records, including WiFi network names, passwords, IP addresses, and device identifiers. The breach, discovered in an unprotected database, raises concerns about unauthorized remote access and potential surveillance risks. Security researchers warn that compromised credentials could enable large-scale botnet attacks or network intrusions.

McKinney, Texas Data Breach Exposes Thousands of Residents' Information

+US +Government

- A cyberattack on [McKinney, Texas](#), compromised the personal information of 17,751 residents, including Social Security numbers, driver's licenses, and financial data. The breach occurred on October 31 but was only detected in mid-November. The city has since involved federal authorities and provided identity protection services to affected individuals. No ransomware group has claimed responsibility.

Misconfigured APIs Expose Millions of Medical Records in Diagnostic Chain

+Healthcare

- A major [diagnostic chain](#) exposed millions of patients' personal and medical records due to misconfigured APIs, including exposed authentication tokens and unsecured endpoints. Attackers could access names, contact information, and medical reports, posing risks of identity theft and fraud.

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.