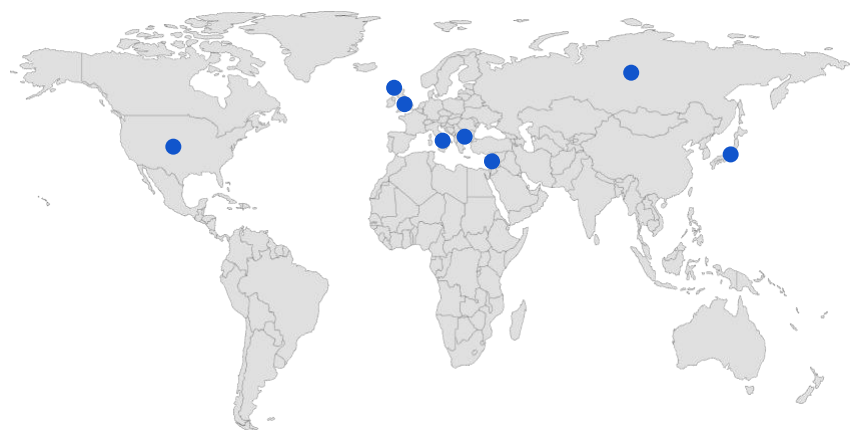


Threat Intel Report: November 25-December 1, 2024

Countries



Top Tags

- Ignoble Scorpius
- Banshee Stealer
- RomCom
- XorBot
- RansomHub

Executive Summary

Actionable Information:

- **Ransomware Prevalence:** Ransomware continues to dominate the threat landscape, with critical sectors like healthcare and high-profile organizations being frequent targets. Attackers are leveraging advanced encryption techniques and demanding increasingly large ransoms.
- **Software and Platform Vulnerabilities:** Critical flaws in widely-used software highlight the need for regular patch management and proactive security measures. These vulnerabilities are being actively exploited to gain unauthorized access and execute malicious actions.
- **Malware and Botnet Threats:** The resurgence of sophisticated botnets and the dissemination of malware source code are enabling less skilled threat actors to launch impactful attacks. IoT devices and platforms with high user engagement remain attractive targets.
- **Sector-Specific Threats:** Certain industries, such as gaming, e-commerce, and healthcare, are seeing tailored attacks that exploit their unique vulnerabilities and dependencies. These sector-specific threats underline the importance of targeted cybersecurity strategies.
- **Evolving Threat Actor Techniques:** Nation-state and advanced persistent threat (APT) groups are employing cutting-edge tactics, such as zero-day vulnerabilities and zero-click exploits, to breach systems with minimal detection.

Outlook:

The cybersecurity landscape is marked by a concerning trend of highly specialized attacks, exploiting both zero-day vulnerabilities and unpatched systems. Ransomware remains a persistent threat, especially in healthcare, while data breaches targeting sensitive personal and financial records are on the rise. Malware source code leaks and botnet evolutions suggest a democratization of cybercrime tools, likely leading to increased attack volumes. Organizations must

adopt proactive defenses, including vulnerability management, advanced threat detection, and sector-specific security frameworks, to mitigate these threats. As the year closes, heightened vigilance is crucial, particularly against ransomware and emerging malware variants.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 3,500% [CVE-2023-26009](#)

- An Improper Privilege Management vulnerability in favethemes Houzez Login Register allows Privilege Escalation.

📈 1,065% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via completePath in the ProcessUtilities.outputExecutioner() sink.

📈 500% [CVE-2023-3460](#)

- The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will.

Largest DDoS Attack Of 2024 Hits Israeli Hospital

[+Israel](#) [+Ireland](#) [+Healthcare](#)

- The largest application-layer (L7) DDoS attack of 2024 targeted an Israeli hospital last month, reaching almost 14 million requests per second (RPS) in just over an hour. Attacking IPs came from both Israel and Ireland.

Japanese Library System Targeted in RCE and SQLi Attacks

[+Japan](#) [+Bulgaria](#) [+Education](#)

- A Japanese metropolitan library system was attacked by remote code execution (RCE) and SQL injection (SQLi) attacks this week, in a one-day onslaught. The attacks came entirely from bots based in Bulgaria.

Recent Cyber Threats

DOJ Shuts Down PopeyeTools Credit Card Marketplace

[+Government](#) [+Marketplace](#) [+PopeyeTools](#)

- The U.S. Department of Justice (DOJ) dismantled [PopeyeTools](#), an illicit online marketplace selling stolen credit card data, and charged three operators with fraud. The operation involved multiple law enforcement agencies and resulted in the seizure of significant infrastructure and assets used by the platform. This marketplace facilitated fraud by offering credit card dumps, impacting individuals and financial institutions globally.

Wowza Streaming Engine Vulnerabilities Expose Servers

[+Media](#) [+CVE](#)

- Critical vulnerabilities in the [Wowza Streaming Engine](#), a popular media server software, could allow remote attackers to execute arbitrary code or access sensitive data. Researchers identified that these flaws potentially expose thousands of servers worldwide to exploitation, particularly in media and streaming industries.

Ignoble Scorpious Deploys BlackSuit Ransomware in Fresh Attacks

+Ignoble Scorpious +Blacksuit +Ransomware

- The Ignoble Scorpious threat group has launched new attacks leveraging the [BlackSuit](#) ransomware, primarily targeting entities in critical sectors. The campaign features sophisticated encryption techniques and demands ransoms starting at about 1.5% the company's annual revenue for data decryption.

Critical WordPress Plugin Flaws Threaten 200,000 Sites

+WordPress +CVE +RCE

- Two critical vulnerabilities (CVE-2024-10542 and CVE-2024-10781) in a widely-used WordPress plugin ([Anti-Spam by CleanTalk](#)) expose over 200,000 websites to potential remote code execution and privilege escalation attacks. Exploiting these flaws could allow attackers to take over affected websites.

Banshee Stealer Source Code Leaked Online, Ceases Operations

+Banshee Stealer +Malware

- The source code for [Banshee Stealer](#), a sophisticated malware targeting credentials and sensitive data, has been leaked online. This development raises concerns about an uptick in attacks as the leaked code enables less skilled threat actors to deploy customized variants. Banshee Stealer operators [shut down the malware](#) soon after the code was leaked.

Credit Card Skimmer Targets Magento Checkout Pages

+Skimmer +Magento +eCommerce

- A new wave of credit card skimmer malware has been identified targeting [Magento](#)-based e-commerce sites. The malware injects malicious scripts into checkout pages, harvesting customer payment details. This attack highlights ongoing vulnerabilities in online retail platforms, urging administrators to regularly update and secure their systems.

RomCom APT Exploits Zero-Day and Zero-Click Browser Escapes

+RomCom +CVE +Russia

- [RomCom](#), a Russian APT group, exploited a zero-day vulnerability enabling zero-click browser escapes in Firefox and Tor. The attacks allow complete system compromise without user interaction, posing a severe threat to user privacy and security for the two days this remained unpatched. Mozilla has issued patches, but the incident underscores the importance of timely updates for browser security.

GodLoader Malware Infects Gamers via Godot Scripts

+GodLoader +Gaming

- A newly discovered malware called [GodLoader](#) has infected thousands of gamers through malicious scripts embedded in Godot Engine games. The malware exfiltrates personal information and delivers payloads, exploiting the popularity of indie games developed on this platform.

XorBot Botnet Resurfaces, Threatens IoT Devices

+XorBot +Botnet +IoT

- The [XorBot](#) botnet has re-emerged with advanced evasion techniques and new exploits, specifically targeting IoT devices. Its updated capabilities include scanning for vulnerabilities in connected devices and deploying DDoS attacks or cryptomining malware. The resurgence emphasizes the importance of securing IoT ecosystems against evolving threats.

Data Breaches

Alder Hey Children's Hospital Investigates Ransomware Data Breach

+UK +Healthcare

- [Alder Hey Children's Hospital](#) in the UK is investigating a potential data breach after a ransomware group claimed responsibility for stealing sensitive patient and staff data. The attackers reportedly demanded a ransom to prevent the release of the stolen information. The breach underscores the heightened risk healthcare organizations face from cybercriminals.

Bologna FC Confirms Data Breach After RansomHub Ransomware Attack

+Italy +Sports +RansomHub

- [Bologna FC](#), an Italian Serie A football club, disclosed a data breach caused by a ransomware attack attributed to the RansomHub group. The attackers claim to have stolen sensitive employee and operational data. This incident highlights the growing trend of ransomware groups targeting high-profile organizations in sports.

Over 600,000 Records Exposed in Background Check Data Breach

+US

- A [data breach](#) affecting over 600,000 individuals has been reported, with stolen records including background checks, vehicle registrations, and property details. The exposed data increases the risk of identity theft and fraud for affected individuals. The breach underscores the vulnerabilities in managing sensitive public and private records.

Colonial Behavioral Health Reports Ransomware-Induced Data Breach

+US +Healthcare

- [Colonial Behavioral Health](#), a Virginia-based mental health service provider, reported a data breach following a ransomware attack. The compromised data includes patient records, raising concerns about privacy and compliance with HIPAA regulations.

OnePoint Patient Care Data Breach Exposes Patient Records

+Healthcare +US

- [OnePoint Patient Care](#), a pharmacy provider specializing in hospice care, suffered a data breach exposing sensitive patient information, including health records and contact details. The breach raises significant concerns about privacy and the security of healthcare data.

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.