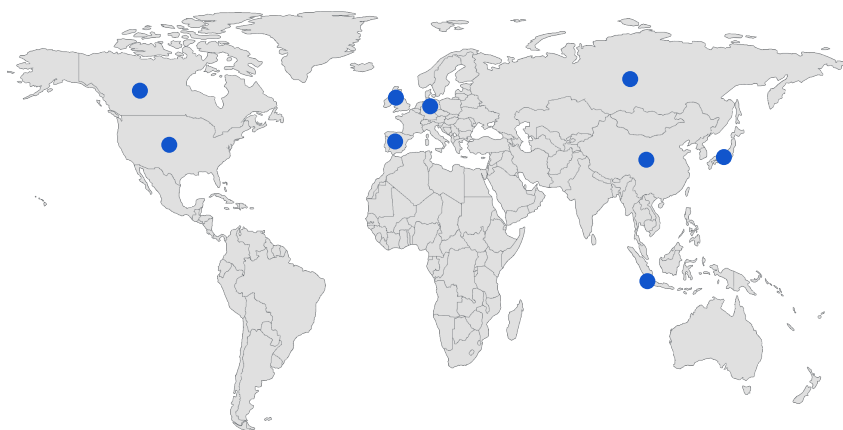


Threat Intel Report: January 6-12, 2025

Countries



Top Tags

WordPress

PhishWP

BARWM

MirrorFace

Silent Crow

Executive Summary

Actionable Information:

- **Increase in Sophisticated Phishing and Malware Attacks:** Cybercriminals continue to refine their tactics, with phishing campaigns like the one exploiting Social Security Administration branding to distribute RATs, and increasingly sophisticated credit card skimmers targeting WordPress sites. These attacks are often difficult for users to detect, using legitimate-looking interfaces or stealthy methods such as database injections and file obfuscation to steal sensitive information.
- **Critical Vulnerabilities in Widely-Used Platforms:** WordPress plugins, such as Fancy Product Designer, continue to be a prime target for attackers. Unpatched vulnerabilities like SQL injection and arbitrary file uploads in such plugins expose WooCommerce sites to significant risks. Site administrators must remain vigilant, applying security updates promptly and securing user input to mitigate these threats.
- **Ongoing Exploitation of IoT Devices and Critical Infrastructure:** The Mirai botnet's exploitation of industrial routers with zero-day vulnerabilities underscores the ongoing risk posed by internet-exposed devices. Additionally, cyber-espionage groups like MirrorFace continue to target critical infrastructure, such as Japan's national security and technological sectors, using sophisticated malware to exfiltrate sensitive data.
- **Location Data Breaches and Data Exposure:** The breach at Gravy Analytics, revealing precise location data of millions, and other recent data leaks, highlight the significant risks associated with geolocation data. Both individuals and organizations must take steps to secure their data, especially when dealing with third-party data brokers who may not prioritize security.

Outlook:

The cybersecurity landscape in 2025 is defined by the increasing sophistication of cyberattacks, which are becoming harder to detect and mitigate. Phishing, social engineering, and malware delivery methods are being refined to bypass

security measures and deceive even savvy users. Critical vulnerabilities in widely used platforms, especially plugins for popular content management systems like WordPress, are being exploited by attackers to target e-commerce and other business-critical operations. Moreover, the rise in attacks targeting IoT devices and the exploitation of critical infrastructure suggests a growing trend in cyber-espionage and DDoS attacks on industrial and governmental targets. Moving forward, it is crucial for organizations to prioritize vulnerability management, user awareness, and encryption of sensitive data to protect against an increasingly aggressive and sophisticated threat landscape.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 550% [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.

📈 234% [CVE-2024-9465](#)

- An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys.

📈 62% [CVE-2024-7593](#)

- Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel.

Massive DDoS Attack Targets Indonesian Government Site

+Indonesia +Government +DDoS

- An Indonesian government site was recently targeted by a huge DDoS attack, at almost 10M RPS. The application-layer attack, which lasted 14 hours, came from 5,300 IPs—a comparatively low number for the scale of the attack.

Account Takeover Attack Targets US Automotive Site

+US +Automotive +ATO

- A United States automotive site was the target of an account takeover attack reaching over 2M logins. The attacks came primarily from IP addresses based in the US and Germany, and attackers mainly leveraged basic bots and bots disguised as browsers.

Recent Cyber Threats

Social Security Administration Spoofed to Deliver RAT

+RAT +Phishing +US +Government

- Hackers have exploited [Social Security Administration](#) (SSA) branding to distribute the ConnectWise Remote Access Tool (RAT) through phishing emails. This campaign, active since September 2024, mimics official SSA communications to trick victims into downloading malware. Once installed, the RAT allows attackers to steal sensitive data, including Social Security Numbers, credit card details, and phone carrier PINs. The attackers

use dynamic DNS services and attacker-hosted domains to evade detection, making the campaign highly deceptive and effective.

PhishWP Plugin Enables Sophisticated Payment Page Scams

[+Phishing](#) [+PhishWP](#) [+WordPress](#) [+eCommerce](#)

- Cybercriminals are leveraging the [PhishWP](#) plugin to create counterfeit payment pages that closely mimic legitimate payment processors, making it challenging for users to detect the deception. This plugin allows attackers to craft highly customizable checkout pages, collect one-time passwords (OTPs) to bypass security measures, and transmit stolen data directly to attackers via Telegram. The widespread use of this tool poses a significant threat to e-commerce platforms and their customers.

Android Apps Targeted by Steganography Backdoor Attacks

[+Android](#) [+BARWM](#) [+Steganography](#) [+Backdoor](#)

- A new technique called [BARWM](#) leverages DNN-based steganography to embed imperceptible backdoors in Android apps, allowing attackers to silently manipulate real-world deep learning models. This stealthy attack method avoids detection by generating sample-specific triggers, making it harder to spot and mitigate. When applied to Android apps, the attack successfully bypasses security measures and compromises the app's integrity. Research shows that this method outperforms traditional backdoor attacks, achieving higher success rates and better stealth.

Mirai Botnet Targets Industrial Routers with Zero-Day Exploits

[+Mirai](#) [+Botnet](#) [+China](#) [+US](#) [+Germany](#) [+UK](#)

- A new [Mirai](#)-based botnet has been exploiting zero-day vulnerabilities in industrial routers and smart home devices, including the Four-Faith industrial router and Neterbit routers. This botnet, which has been active since early 2024, is used to launch DDoS attacks, causing disruptions for its targets. The botnet's exploit mix includes both public and private vulnerabilities, allowing it to infect a variety of internet-exposed devices. Attacks have exceeded 100 Gbps in traffic, targeting organizations worldwide, particularly in China, the US, Germany, and the UK.

Critical Vulnerabilities in Fancy Product Designer Plugin Impact WooCommerce Sites

[+WordPress](#) [+Plugin](#) [+SQLi](#)

- The [Fancy Product Designer](#) plugin for WordPress, used by over 20,000 sites, contains two unpatched critical vulnerabilities: an unauthenticated arbitrary file upload flaw and an unauthenticated SQL injection vulnerability. These flaws, identified as CVE-2024-51919 and CVE-2024-51818, allow attackers to execute remote code and potentially compromise databases. Despite being notified in March 2024, the vendor has not released patches, leaving WooCommerce sites vulnerable to exploitation. Administrators are urged to restrict file uploads and sanitize user inputs to mitigate risks.

Credit Card Skimmer Targets WordPress Checkout Pages via Database Injection

[+Malware](#) [+Skimmer](#) [+WordPress](#)

- A new credit card skimmer malware has been identified targeting [WordPress](#) checkout pages, using a stealthy method of injecting malicious JavaScript into the site's database. This skimmer only activates on checkout pages, either hijacking existing payment fields or creating a fake form to capture sensitive payment data. The malware uses Base64 encoding and AES-CBC encryption to obfuscate and exfiltrate the stolen data to remote servers. This attack method avoids detection by common file-scanning tools, making it particularly dangerous for WordPress eCommerce sites.

MirrorFace Campaign Targets Japan's National Security and Technology

[+MirrorFace](#) [+China](#) [+Japan](#) [+APT10](#)

- [MirrorFace](#), a Chinese-linked cyber-espionage group, has been targeting Japanese organizations since 2019. The group, operating under APT10, has conducted spear-phishing campaigns and exploited vulnerabilities in various devices to breach networks in sectors like semiconductor manufacturing, aerospace, and media. Tools like ANEL and NOOPDOOR have been used to exfiltrate sensitive national security and technological data. The attacks, characterized by stealthy execution techniques such as running malware in Windows Sandboxes, have been ongoing, with campaigns aimed at critical infrastructure and high-value targets in Japan.

Data Breaches

PowerSchool Data Breach Exposes Sensitive Information of Students and Staff

+US +Canada +Education

- [PowerSchool](#), a K-12 educational technology company, experienced a data breach affecting schools across the United States and Canada. The breach potentially exposed personal information of students and staff, including names, addresses, Social Security numbers, medical information, and grades. PowerSchool has notified affected individuals and is working to enhance security measures to prevent future breaches.

Massive Data Breach Exposes Precise Locations for Users of Popular Apps

+Geolocation

- [Gravy Analytics](#), a location data broker, experienced a significant data breach potentially exposing precise location data of millions of individuals. The breach affected users of popular mobile applications, including dating apps, games, and health trackers. The exposed data included sensitive locations such as users' homes and workplaces. Gravy Analytics is investigating the breach and working to mitigate potential misuse of the exposed data.

Hackers Breach Russian State Agency Managing Property and Land Records

+Silent Crow +Russia +Government

- A hacker group known as [Silent Crow](#) has claimed responsibility for breaching Rosreestr, the Russian state agency responsible for property and land records. The breach resulted in the exposure of sensitive personal information, including names, addresses, and contact details of Russian citizens. Rosreestr is investigating the incident and has temporarily suspended access to certain records to mitigate potential misuse.

Hackers Breach Telefónica's Network, Leak 2.3 GB of Data Online

+Telecommunications +Spain

- [Telefónica](#), a Spanish multinational telecommunications company, confirmed a data breach involving its internal Jira ticketing system. Hackers using compromised employee credentials accessed and leaked approximately 2.3 GB of internal data, including documents and tickets. The breach is linked to the Hellcat Ransomware group, known for targeting large organizations. Telefónica is investigating the incident and has taken steps to prevent further unauthorized access.

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.