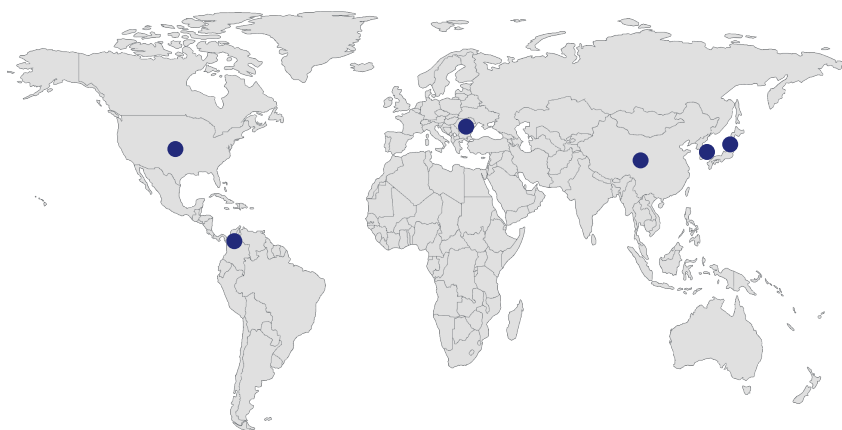


IMPERVA THREAT RESEARCH

Threat Intel Report: December 15-28, 2025

Countries



Top Tags

BlindEagle

LongNosedGoblin

INC

Play

CI0p

Executive Summary

Actionable Information:

- **Trust boundaries are the primary attack surface:** Attacks increasingly abuse trusted artifacts, like developer notebooks, open-source repos, browser extensions, Group Policy, and third-party APIs, rather than exploiting perimeter weaknesses. Security controls must assume that “legitimate” tools can be weaponized.
- **Ransomware is now predominantly data-centric, not encryption-centric:** Across multiple sectors, attackers focused on data exfiltration, public shaming, and regulatory pressure. Backup integrity and recovery no longer mitigate extortion risk if sensitive data is accessible.
- **Public sector and education remain high-yield targets:** Government agencies, libraries, utilities, and universities continue to suffer outsized impact due to large identity datasets, slower patch cycles, and complex vendor ecosystems.
- **Credential abuse and insider risk are persistent enablers:** Several incidents stemmed from compromised subcontractor credentials, internal account misuse, or over-privileged access, reinforcing the need for stronger identity governance, least privilege, and behavioral monitoring.
- **IoT and consumer devices are becoming attack force multipliers:** The Kimwolf botnet demonstrates that unmanaged Android and IoT devices are no longer edge risks but core components of global DDoS capacity.

Outlook:

Looking ahead, organizations should expect continued blending of malware, extortion, and abuse of legitimate enterprise mechanisms, with attackers favoring low-friction access paths that evade traditional security tooling. Software supply chains, analytics platforms, identity providers, and administrative controls will remain prime targets, particularly where monitoring assumes benign use. As ransomware groups further specialize by industry and data type, regulatory exposure and reputational damage, not downtime, will

drive attacker leverage. Defenders should prioritize visibility into trusted workflows, enforce zero-trust principles around internal tooling, and treat identity and data access as the primary battleground for 2026.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 5,300% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via completePath in the ProcessUtilities.outputExecutioner() sink. There is /filemanager/upload (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.

↑ 2,938% [CVE-2025-55183](#)

- An information leak vulnerability exists in specific configurations of React Server Components versions 19.0.0, 19.0.1 19.1.0, 19.1.1, 19.1.2, 19.2.0 and 19.2.1, including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. A specifically crafted HTTP request sent to a vulnerable Server Function may unsafely return the source code of any Server Function. Exploitation requires the existence of a Server Function which explicitly or implicitly exposes a stringified argument.

↑ 273% [CVE-2025-61882](#)

- Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: BI Publisher Integration). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in takeover of Oracle Concurrent Processing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

Recent Cyber Threats

Hidden Code Execution in Jupyter Exports

+Jupyter

- Imperva Threat Research identified a vulnerability in how [Jupyter Notebook](#) exports can be abused on Windows: malicious notebooks or configuration files can trigger arbitrary code execution when exporting notebooks containing SVG output. This issue stems from insecure search paths in the nbconvert tool, meaning a crafted batch script can be executed during a routine export process, potentially leading to workstation compromise. Organizations that process notebooks from external sources are at risk of executing untrusted code, underscoring the need for stricter controls on shared notebooks and dependency hygiene.

PyStoreRAT Spread Through Fake GitHub Projects

+RAT +Python +Javascript

- Researchers highlighted a campaign where malicious Python and JavaScript loaders on GitHub, disguised as OSINT utilities and developer tools, delivered a modular remote access trojan dubbed [PyStoreRAT](#). These repos, often appearing legitimate and trending due to artificial metrics, fetch and execute an HTA payload that stages additional modules and a follow-on information stealer called Rhadamanthys. The technique leverages developer trust in open-source repositories and social promotion on forums to gain traction, making it a stealthy infection vector among analysts and developers.

Chrome Extension With Millions of Users Harvests AI Chat Data

+AI

- A widely installed [Chrome extension](#), marketed as a free VPN, was found to intercept and exfiltrate users' AI chatbot conversations from services like ChatGPT, Claude, Gemini, and others. The extension and related titles (with millions of installations) contained JavaScript that rerouted API requests and silently sent full prompt/response data to third-party analytics servers. The abuse of the Chrome Web Store "Featured" badge increased user trust and scale, showing how marketplace trust signals can be leveraged for mass data collection.

BlindEagle Targets Colombian Government With Multi-Stage Malware

+BlindEagle +Colombia +Government

- In a sophisticated spear-phishing campaign attributed to the South American threat actor [BlindEagle](#), attackers targeted a Colombian government agency under the Ministry of Commerce, Industry and Tourism. Using a compromised internal email account, they delivered a crafted SVG attachment that launched a multi-stage chain: JavaScript/PowerShell bootstrap, Caminho downloader, and final payload DCRAT, a remote access trojan capable of persistence and control. The operation underscores a trend toward nested scripting, steganography, and multi-vector delivery to bypass defenses within government networks.

Kimwolf Botnet Amasses 1.8M Android Devices for DDoS

+Kimwolf +AISURU +Botnet +DDoS

- Security researchers uncovered the [Kimwolf](#) botnet, a massive distributed network of at least 1.8 million infected Android-based TVs, set-top boxes, and tablets leveraged for large-scale DDoS attacks. Over a three-day window in late November 2025, the botnet issued approximately 1.7 billion attack commands, and its infrastructure briefly ranked among the most accessed domains worldwide. The campaign appears linked to the previously identified AISURU botnet family and demonstrates increasing focus on consumer IoT devices as DDoS infrastructure.

China-Aligned APT Exploits Group Policy to Deploy Espionage Malware

+China +LongNosedGoblin

- Researchers revealed a previously undocumented China-aligned threat group dubbed [LongNosedGoblin](#), which leverages Windows Group Policy to distribute malware across compromised networks belonging to governmental organizations in Southeast Asia and Japan. After initial access, the actor abuses trusted administrative mechanisms to propagate tools for surveillance, data theft, and broader foothold, including use of cloud services like OneDrive and Google Drive for command delivery. The group's use of Group Policy objects for lateral movement represents a strategic blending of legitimate enterprise tools with stealthy persistence and espionage objectives.

Data Breaches

ClOp Exploits CentreStack for Data Theft and Extortion

+ClOp +Software

- The ClOp ransomware gang has actively scanned and compromised internet-exposed [Gladinet CentreStack](#) file-sharing servers, leveraging known and potentially zero-day flaws to steal sensitive files and issue extortion demands. CentreStack is widely used by enterprises for secure remote access to file servers, making successful breaches particularly impactful for organizations that have not applied recent patches. ClOp's focus on data theft and public pressure for payment continues its shift from pure encryption to extortion via stolen data publication.

Ransomware Linked to Washington Library Compromises 340K+

+US +Government +INC

- A cyberattack on the [Pierce County Library System](#) in Washington state compromised personal data for more than 340,000 patrons and staff after threat actors accessed systems between April 15 and 21, forcing a complete shutdown of the library's IT infrastructure. Stolen information ranges from names and birthdates of patrons to Social Security numbers, passport details, financial and health insurance data for current and former employees. The INC ransomware-as-a-service group claimed responsibility, highlighting ongoing risks to public sector digital services and the potential for extensive identity exposure in government-affiliated systems.

700Credit Breach Exposes Millions of Consumer Records

+Financial Services

- Credit reporting and identity verification provider [700Credit](#) confirmed a major data breach affecting at least 5.6–5.8 million individuals, where attackers accessed sensitive personal information, including names, addresses, dates of birth, and Social Security numbers, via a compromised third-party API tied to its web application. The breach persisted from July through October 2025 before detection, exposing records gathered from automotive dealerships and related service providers. 700Credit is notifying affected parties and offering credit monitoring, underscoring how deeply embedded service providers in the financial and automotive sectors are now attractive targets for large-scale personal data theft.

Askul Confirms RansomHouse Attack Stole 740K Records

+Japan +Logistics +RansomHouse

- Japanese office supplies and logistics firm [Askul](#) disclosed that roughly 740,000 customer and business partner records were stolen following a RansomHouse ransomware attack in October 2025. Attackers initially used compromised subcontractor credentials to infiltrate Askul's network, deployed multiple ransomware variants that evaded EDR detection, and deleted backups to stymie recovery, causing significant operational disruption. Although payment data was reportedly not accessed, exposed records and the ongoing restoration process highlight both credential misuse and ransomware commercialization as persistent threats to retail and e-commerce infrastructure.

Ransomware Breach at NYC/DC Real Estate Firm Exposes Personal Records

+US +Real Estate +Play +Ransomware

- [Rockrose Development Corp.](#), a real-estate developer operating in New York City and Washington, D.C., disclosed that unauthorized actors compromised internal systems in a July 2025 breach, affecting 47,392 individuals. Play ransomware claimed responsibility on its data leak site, asserting that sensitive personal data, including SSNs, tax IDs, driver's licenses, passports, financial account info, health insurance, medical data, and credentials, was exfiltrated. Rockrose is offering identity protection services to affected individuals and has not confirmed ransom payment details; regulatory notifications have been submitted.

University of Phoenix Data Theft Part of Large Oracle EBS Exploitation

+US +Education +CI0p

- The [University of Phoenix](#) confirmed a major data breach impacting nearly 3.5 million individuals after attackers exploited a zero-day vulnerability in Oracle's E-Business Suite, part of a broader campaign against hundreds of organizations. The CI0p ransomware group is tied to the campaign, exfiltrating sensitive personal and financial information such as names, dates of birth, Social Security numbers, and bank details. The incident was discovered in November 2025, though data was accessed in mid-August, and the university is offering identity protection services.

Ransomware Attack Disrupts Romanian Water Authority IT Systems

+Romania +Ransomware +Utilities

- Romania's national water management authority, [Administrația Națională Apele Române](#), suffered a ransomware attack beginning December 20, 2025, that compromised approximately 1,000 IT systems across central and regional offices. The attackers used Windows BitLocker to encrypt servers (GIS, database, email, web, workstations) and issued a ransom demand; authorities have not publicly attributed the campaign to a known group and advise against negotiating. Crucially, operational technology controlling water infrastructure remained intact, so essential services continued.

Shinhan Card Employee-Linked Merchant Data Leak

+Financial Services +South Korea

- South Korea's [Shinhan Card](#) reported a breach affecting around 192,000 merchant representatives' records, primarily mobile phone numbers and limited personal details, due to alleged internal misconduct by staff rather than an external cyberattack. The firm notified the Personal Information Protection Commission after its internal investigation concluded an employee improperly transmitted merchant data for sales purposes; no evidence has emerged that credit card numbers or bank account details were exposed. Shinhan is strengthening controls and working with regulators.

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.