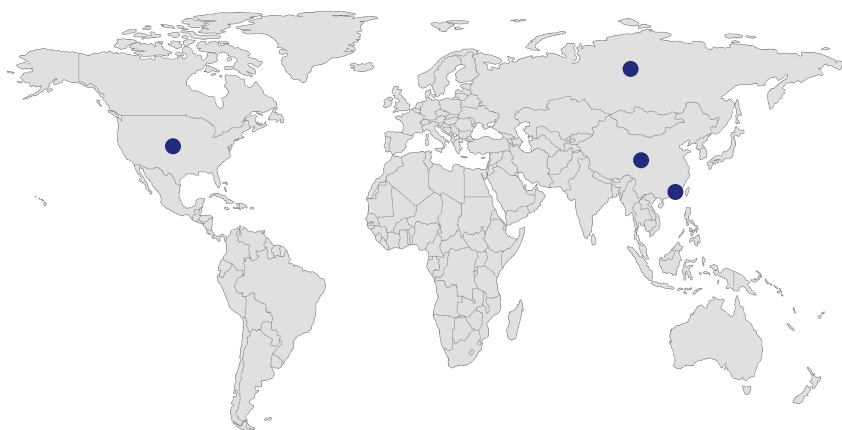


IMPERVA THREAT RESEARCH

Threat Intel Report: December 8-14, 2025

Countries



Top Tags

React2Shell

ChrimeraWire

DroidLock

Qilin

INC

Executive Summary

Actionable Information:

- **Exploitation velocity continues to compress.** The rapid post-disclosure weaponization of the React Server Components vulnerability reinforces a persistent trend: widely deployed frameworks are being scanned and exploited at internet scale within days. Organizations should assume near-immediate exploitation following high-severity disclosures and prioritize virtual patching and compensating controls where remediation timelines lag.
- **Stealth and abuse-of-trust techniques are increasing.** Several incidents this week relied on hiding in plain sight—auto-login backdoors masquerading as JavaScript files, malware simulating legitimate Chrome user behavior, and loaders delivered via fake verification prompts. These techniques bypass traditional signature-based detection and elevate the importance of behavioral analysis and application-layer monitoring.
- **Data exposure risk extends beyond “attacks.”** Misconfigurations and insecure object references drove impact comparable to ransomware and intrusion campaigns, exposing billions of records and sensitive customer data. This highlights that breach risk is increasingly rooted in development and deployment practices, not just external threat actors.
- **Ransomware pressure persists across mid-market and critical sectors.** Healthcare, telecommunications, and life sciences organizations continue to face ransomware incidents involving both encryption and data theft, while hacktivist groups opportunistically target critical infrastructure via exposed services rather than advanced tradecraft.

Outlook:

The current threat landscape reflects a convergence of scale and subtlety: attackers are simultaneously exploiting high-impact vulnerabilities at massive volume while refining quieter techniques that evade conventional controls. Over the near term, organizations should expect continued chaining of newly disclosed vulnerabilities into automated campaigns, broader abuse of trusted web and CMS

components, and sustained data exposure incidents driven by weak access controls and cloud misconfigurations. Defenders that emphasize rapid mitigation, application-layer visibility, and anomaly detection, rather than relying solely on perimeter or malware signatures, will be better positioned to manage both opportunistic and targeted threats as 2025 closes.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 1,130% [CVE-2025-5777](#)

- Insufficient input validation leading to memory overread when the NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.

 615% [CVE-2025-55182](#)

- A pre-authentication remote code execution vulnerability exists in React Server Components versions 19.0.0, 19.1.0, 19.1.1, and 19.2.0 including the following packages: react-server-dom-parcel, react-server-dom-turbopack, and react-server-dom-webpack. The vulnerable code unsafely deserializes payloads from HTTP requests to Server Function endpoints.

 371% [CVE-2025-32432](#)

- Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

Recent Cyber Threats

React2Shell Vulnerability Sparks Global Exploitation Waves

+[React2Shell](#) +[Mirai](#) +[XMRig](#) +[Xnote](#) +[Hong Kong](#) +[China](#)

- Researchers observed hundreds of millions of automated attack attempts leveraging the recently disclosed [React2Shell](#) vulnerability (CVE-2025-55182) in React Server Components. Exploit activity has spawned diverse campaigns, from Chinese cryptomining campaigns and botnets using Mirai and XMRig to targeted remote access trojans like XNote on financial services sites in Hong Kong. The vulnerability's widespread presence in cloud environments has driven opportunistic scanning and exploitation across 128+ countries, underscoring a rapid transition from disclosure to active abuse. Imperva customers are protected against exploitation attempts.

ChrimeraWire Click-Simulation Trojan Manipulates Web Traffic

+[ChrimeraWire](#) +[Trojan](#) +[Bots](#)

- The [ChrimeraWire](#) Trojan simulates authentic Chrome browsing behavior to artificially inflate search clicks and site engagement metrics, making bot mitigation tools less likely to flag its activity. The malware operates with probabilistic click patterns and random pauses to mimic human interaction, and it can also capture screenshots, fill forms, and read web content. While its primary objective appears to be SEO manipulation or affiliate revenue fraud, additional dormant capabilities suggest potential future expansion into more direct exploitation or data exfiltration.

ClickFix Campaign Fuels Rise in CastleLoader Malware Delivery

+[ClickFix](#) +[CastleLoader](#) +[Malware](#)

- Analysts have documented increased activity combining [ClickFix](#) phishing tactics with delivery of the CastleLoader malware family using a Python-based loader. Infected users lured by fake verification prompts or compromised WordPress sites trigger

multi-stage delivery chains that quietly download and execute in-memory malware without typical user prompts. Once active, CastleLoader can deploy a range of payloads including info-stealers and remote access tools, raising risks to endpoints across sectors.

Stealth Auto-Login Backdoor Hidden as JavaScript Asset

+WordPress +Backdoor

- Researchers uncovered a sophisticated [WordPress backdoor](#) disguised as a seemingly benign JavaScript data file (wp-admin/js/mr_skk/data.php) that, in reality, is PHP code granting attackers automatic administrator login without credentials. Unlike traditional backdoors that create new admin accounts, this variant hijacks existing sessions and yields valid authentication cookies, making detection via user lists or login audits extremely difficult. Attackers who know the file's URL can gain full admin privileges and persistently control the site to install additional malware, modify content, or maintain access even after typical cleanup. This stealth technique blends with normal WordPress request behavior and evades many security detections, highlighting evolving threats against CMS infrastructure.

DroidLock Malware Locks Android Devices and Extorts Ransom

+DroidLock

- Researchers have identified a new Android malware strain called [DroidLock](#) that takes full control of infected phones, locking screens and demanding ransom payments to restore access. Delivered via malicious or phishing sites posing as legitimate apps, DroidLock requests Device Administrator and Accessibility permissions to alter PINs/passwords, intercept data, and display coercive ransom overlays. While not encrypting files traditionally, the malware can threaten data deletion and leverage remote control features to compromise user privacy and device security.

Pro-Russia Hacktivists Target Critical Infrastructure

+Russia +US +Government +Critical Infrastructure

- CISA, FBI, NSA, and allied partners issued advisory [AA25-343A](#) highlighting opportunistic cyber operations by pro-Russia hacktivist collectives against global critical infrastructure. These groups exploit insecure remote access (e.g., poorly secured VNC connections) to gain entry into operational technology environments, resulting in varying degrees of operational disruption. Though less sophisticated than state-sponsored APTs, their activity poses ongoing risks to vital sectors such as utilities and energy.

Data Breaches

Qilin Ransomware Exposes Inotiv Employee and Partner Data

+Qilin +US +Russia +Pharmaceutical +Healthcare

- [Inotiv](#), a US-based pharmaceutical research firm, disclosed a ransomware attack from August 2025 that encrypted its systems and disrupted operations, later confirming a data breach affecting over 9,500 individuals including employees, family members, and partners. The Russia-linked Qilin ransomware group claimed responsibility, alleging theft of roughly 176 GB of internal files and posting proof, though the leak listing was later removed. Stolen data reportedly includes names, addresses, Social Security numbers, financial and medical information, prompting regulatory notifications and identity-theft protection offers.

Petco Pulls Vetco Portal After Major Customer Data Exposure

+Retail +Veterinary +IDOR

- [Petco](#) temporarily took down its Vetco Clinics website after security researchers discovered an Insecure Direct Object Reference (IDOR) flaw that exposed customers' personal information and pets' medical histories without authentication. The vulnerability allowed sequential access to sensitive records by iterating a predictable document ID, potentially affecting large numbers of users and indexing by search engines. This incident represents Petco's third public data exposure in 2025, raising significant privacy and regulatory concerns.

Inc Ransomware Hits Kansas Telecom, Steals 200 GB of Data

+Inc +US +Telecommunications



- The ransomware group Inc publicly claimed responsibility for a cyberattack on [Rainbow Communications](#), a rural broadband and phone provider in northeast Kansas, that began disrupting services mid-November 2025. The group says it exfiltrated approximately 200 GB of accounting, HR, and customer data before systems were restored by November 19. Rainbow has not independently verified the theft, leaving details about the breach vector, ransom demands, and extent of impact unresolved.

Massive 16 TB Database Exposes 4.3 Billion Professional Records

+Unsecured Database

- Security researchers discovered a publicly accessible 16 terabyte MongoDB database containing approximately [4.3 billion professional records](#), including names, emails, phone numbers, employment histories, and profile links, that was left without password protection. The database likely belonged to a lead-generation firm and remained exposed for roughly two days before being secured, though the duration of prior exposure is unknown. Such unprotected repositories create fertile ground for large-scale AI-driven social engineering, business email compromise, and identity fraud campaigns.

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.