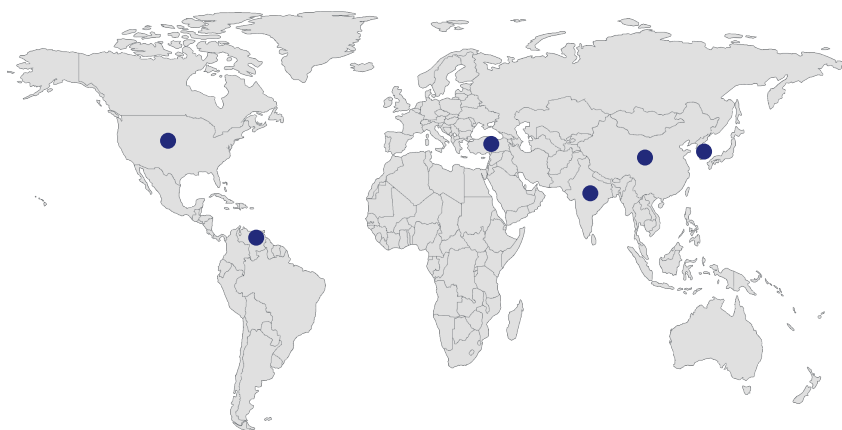


IMPERVA THREAT RESEARCH

Threat Intel Report: December 29, 2025-January 4, 2026

Countries



Top Tags

Evasive Panda

MgBot

1011

Qilin

Crypto

Executive Summary

Actionable Information:

- **Supply chain and third-party compromise** remains a dominant multiplier across industries, affecting crypto, aviation, financial services, healthcare, food delivery, and entertainment platforms, even where primary environments were not breached.
- **Trusted infrastructure abuse is escalating**, including DNS poisoning, legitimate subdomains, and vendor-managed environments, allowing attackers to blend into normal traffic and communications.
- **Data exposure without direct system compromise** is increasingly “good enough” for attackers, enabling phishing, identity theft, and financial fraud at scale.
- **Ransomware impact continues to expand post-incident**, with revised disclosures showing breach scopes growing by orders of magnitude months after initial notifications.
- **Development and test environments are a growing weak point**, both technically and reputationally, as attackers exploit lower controls and later weaponize claims publicly.

Outlook:

Looking ahead, defenders should expect continued growth in indirect compromise paths, with attackers favoring vendors, platforms, and infrastructure layers that sit just outside traditional security ownership boundaries. Espionage actors will further refine low-noise, long-dwell techniques such as DNS manipulation and update-chain abuse, while financially motivated actors will keep exploiting third-party access to maximize victim counts per intrusion. At the strategic level, the normalization of cyber operations as enablers of real-world force will raise the stakes for critical infrastructure protection, particularly in politically sensitive regions. Organizations that cannot rapidly validate trust across suppliers, environments, and communications channels will remain disproportionately exposed in 2026.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,305% [CVE-2025-53772](#)

- Deserialization of untrusted data in Web Deploy allows an authorized attacker to execute code over a network.

↑ 350% [CVE-2025-40598](#)

- A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.

↑ 51% [CVE-2025-8085](#)

- The Ditty WordPress plugin before 3.1.58 lacks authorization and authentication for requests to its displayItems endpoint, allowing unauthenticated visitors to make requests to arbitrary URLs.

Recent Cyber Threats

Poisoned DNS, Silent Implant

+China +Türkiye +India +Evasive Panda +MgBot

- China-linked APT [Evasive Panda](#) ran a targeted espionage campaign that used DNS poisoning to redirect legitimate software update traffic and deliver MgBot. The activity spanned Nov 2022–Nov 2024, with telemetry showing victims in Türkiye, China, and India, and some systems reportedly compromised for over a year. Operators used multi-stage loaders, encrypted components delivered via DNS responses, and in-memory injection/DLL sideloading to keep implants stealthy and persistent. Initial access relied on fake updaters impersonating trusted apps (e.g., a SohuVA update) to execute malware while appearing legitimate.

“10x Bitcoin” Grift via Real Grubhub Subdomain

+Food & Beverage +Crypto

- [Grubhub](#) merchant partners received emails pitching a “Holiday Crypto Promotion” that promised to return 10x the Bitcoin sent to a specified wallet, a classic “send funds, get more back” fraud. The messages appeared credible because they came from b.grubhub.com, a legitimate Grubhub subdomain used for business communications, and some included recipients’ names. Grubhub has investigated and contained the issue, and noted the intrusion originated from an account used by a third-party support services provider.

Caracas Blackout Precedes Maduro Capture

+US +Venezuela +Cyber Operations

- [U.S. cyber operations](#) were reportedly used to disrupt power and communications across Caracas ahead of a coordinated military raid that resulted in the capture of Venezuelan President Nicolás Maduro and his wife, Cilia Flores. The blackout, which plunged large parts of the capital into darkness, is believed to have been caused by targeted cyber interference with Venezuela’s electricity and communications infrastructure, creating operational cover for U.S. special forces and aircraft entering Venezuelan airspace.

Data Breaches

Payment Processor Breach Exposes Ledger Users

+Crypto

- [Ledger](#) confirmed that the personal data of some customers was exposed after its third-party payment processor, Global-e, suffered an unauthorized access to parts of its cloud infrastructure that handles order processing. The breach exposed names and contact details of customers who transacted via Global-e, although no wallet credentials, seed phrases, payment card data, or account passwords were accessed, and Ledger's own systems were not breached. Ledger and Global-e engaged forensic investigators to contain the access and notify affected users, but the incident underscores continued risk tied to payment partners and supply chain data exposure in crypto services. Customers have been warned to remain vigilant for phishing and social engineering attempts using the leaked contact information.

Korean Air Staff Data Exposed via Supplier Hack

+Aviation +South Korea

- A breach of [Korean Air's](#) former in-flight catering and duty-free supplier, KC&D, has resulted in exposure of personal information for about 30,000 Korean Air employees. The compromise stems from a hack of KC&D, which handled sensitive employee data, illustrating how third-party vendors can propagate risk to major carriers even after divestiture. While specifics on the threat actor group or initial intrusion vector were not detailed in public reports, the incident was disclosed by an employee and subsequently acknowledged, triggering internal reviews and likely regulatory notifications. The event highlights the enduring challenges of securing interconnected enterprise ecosystems and vendor networks across aviation and travel sectors.

Marquis Software Ransomware Fallout Expands to More Banks

+US +Financial Services

- Credit unions and community banks continue to disclose impacts from the [Marquis Software Solutions](#) breach tied to a ransomware attack that exploited a vulnerability in a SonicWall firewall. Recent notifications from Artisans' Bank and VeraBank reveal that names, Social Security numbers, addresses, taxpayer IDs, and other personal data were stolen from Marquis's systems and exposed, even though the banks' own networks were not directly breached. The incident, first discovered in August and attributed to ransomware, has now affected tens of thousands of individuals across multiple financial institutions' customer bases, reinforcing the systemic threat posed by vendor-side compromises in critical financial services support infrastructure.

NordVPN Refutes Breach Claims, Says Data Was Test

+1011 +Software

- A threat actor using the handle 1011 claimed to have breached a [NordVPN](#) internal development server, posting alleged database dumps containing Salesforce API keys, Jira tokens, and source code on a cybercrime forum. NordVPN has categorically denied the breach, stating the data was "dummy" or test information from a temporary third-party environment used during trial testing, not connected to its production infrastructure, and that no sensitive customer data or real credentials were exposed. The company's forensic analysis found no evidence of production compromise, but the episode highlights the risk linked to development/test environments on third-party platforms and the broader perception and PR challenges when breach claims surface online.

Covenant Health Patient Data Breach Nearly 478,000 Affected

+Healthcare +US +Qilin

- [Covenant Health](#) of New England revealed that a May 2025 ransomware breach impacted 478,188 individuals, a dramatic increase over its initial disclosure of around 7,800. The Russian-speaking Qilin ransomware group claimed responsibility for the attack, saying it stole more than 1.3 million files (about 850 GB) from Covenant's systems. Exposed data includes names, addresses, Social Security numbers, medical record numbers, health insurance details, and treatment information, raising heightened risk for medical identity theft and fraud and prompting the organization to offer credit monitoring services to victims. The breach underscores persistent threats to healthcare IT environments, where sensitive patient information remains a high-value target.

Weverse Fan Platform Leak Highlights K-Pop Data Risks

+South Korea +Entertainment

- A data leak at [Weverse](#), the fan engagement platform operated by South Korean entertainment giant Hybe, has exposed user data tied to its global fan community and interactive "fansign lottery" system. The incident reignited concerns about transparency and privacy practices within high-traffic digital fan ecosystems, where personal information and transactional

interactions are stored and often monetized. Although details on the scale or specific data elements exposed were not fully disclosed, the event has prompted renewed scrutiny of how platforms supporting major entertainment franchises manage and protect user information against unauthorized access or leaks.

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.