

IMPERVA THREAT RESEARCH

Threat Intel Report: January 12-25, 2025

Countries



Top Tags

Python

AI

Crypto

StealC

Everest

Executive Summary

Actionable Information:

- **Trust abuse is the dominant theme:** AI model loaders, browser extensions, calendar assistants, CMS platforms, and SharePoint links were all leveraged as high-trust execution or access points, enabling code execution, credential theft, or data exfiltration without traditional exploits.
- **Supply chain risk is expanding beyond software updates:** AI models, cloud test apps, and IT distributors now represent viable upstream compromise points, with downstream blast radius affecting enterprises, regulators, and consumer brands.
- **Opportunistic exploitation remains rapid and global:** Trivially exploitable vulnerabilities (e.g., unauthenticated proxy flaws, exposed servers) triggered immediate large-scale scanning and exploitation attempts across dozens of industries.
- **Ransomware continues to favor scale and leverage:** Attacks on conglomerates, distributors, and consumer franchises reinforce the shift toward dual extortion, where operational disruption is paired with large-volume data theft.
- **Espionage and hacktivism remain active alongside cybercrime:** China-linked zero-day exploitation and politically motivated broadcast hijacking demonstrate parallel nation-state and activist activity exploiting nontraditional infrastructure.
- **Criminal ecosystems show fragility:** XSS exposure in infostealer admin panels reveals persistent weaknesses in MaaS platforms, even as credential theft volumes continue to grow.

Outlook:

The threat landscape is increasingly defined by abuse of legitimate functionality rather than overt exploitation, with attackers embedding themselves inside normal enterprise workflows, like AI inference, cloud collaboration, browser automation, and third-party infrastructure. As organizations accelerate AI adoption and cloud experimentation, control-plane security, deserialization safety, extension governance, and exposure management will become critical defensive priorities. In parallel, ransomware actors will continue

targeting high-leverage nodes in supply chains and consumer ecosystems, while nation-state actors favor stealthy zero-day access for long-term positioning. Expect continued pressure on defenders to detect abuse that looks operationally “normal” rather than overtly malicious.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 984% [CVE-2026-23550](#)

- Incorrect Privilege Assignment vulnerability in Modular DS allows Privilege Escalation.

↑ 759% [CVE-2025-59718](#)

- A improper verification of cryptographic signature vulnerability in Fortinet FortiOS allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML response message.

↑ 364% [CVE-2025-34028](#)

- The Commvault Command Center Innovation Release allows an unauthenticated actor to upload ZIP files that represent install packages that, when expanded by the target server, are vulnerable to path traversal vulnerability that can result in Remote Code Execution via malicious JSP.

Thai Travel API Overwhelmed by Sustained Business Logic Abuse

+Thailand +Travel

- A Thailand-based travel company experienced a sharp surge in business logic attacks against its public API beginning mid-month, underscoring how automated abuse can quickly escalate and then settle into a persistent baseline. Over a four-day period, attack traffic peaked at approximately 70 million requests per day, before dropping and stabilizing at a still-elevated rate of roughly 10 million daily requests. The activity was highly concentrated geographically, with the vast majority of requests originating from Singapore-based IP addresses, suggesting centralized automation rather than organic customer demand. While the initial spike appears opportunistic, the sustained volume indicates ongoing exploitation attempts aimed at inventory scraping, pricing abuse, or transaction manipulation rather than short-lived reconnaissance.

Recent Cyber Threats

Model Metadata Turns Into a Code Execution Vector

+Python

- Several widely used [AI/ML Python](#) model formats allow executable objects to be embedded in model metadata, enabling remote code execution when models are loaded. The issue stems from unsafe deserialization and dynamic object instantiation during configuration parsing, allowing attackers to trigger functions such as `eval()` or OS commands. An attacker could distribute a trojanized model or fork that appears legitimate but executes arbitrary code at load time. Hundreds of publicly available models use affected formats, making this a high-risk AI supply-chain weakness despite no confirmed exploitation at the time of reporting.

Unauthenticated Proxy Requests Expose Oracle Server Backends

+Oracle +HTTP

- A critical unauthenticated vulnerability in [Oracle HTTP Server and WebLogic](#) proxy plug-ins allows attackers to send crafted HTTP requests that bypass proxy enforcement and directly impact backend applications. Successful exploitation can enable

unauthorized creation, modification, or deletion of data, with potential full compromise of exposed services. Following disclosure, large-scale scanning and exploitation attempts were observed globally, with activity concentrated in the US and spanning nearly 20 industries. The flaw is trivial to exploit and immediately attractive to opportunistic attackers targeting enterprise infrastructure.

Browser Extension Quietly Grants Itself Withdrawal Power

+Crypto

- A [malicious Chrome extension](#) posing as a crypto-trading automation tool abuses authenticated browser sessions to silently generate new exchange API keys with withdrawal permissions enabled. The extension hides permission changes from the user interface and exfiltrates API credentials to attacker-controlled infrastructure, enabling direct fund theft without passwords or MFA. Because the abuse occurs via legitimate session context, victims may not see login alerts or security warnings. The campaign highlights the growing use of browser extensions as high-trust malware delivery mechanisms in crypto theft.

SharePoint Lures Enable Rapid Email Infrastructure Takeover

+Energy +AitM

- Attackers compromised multiple [energy-sector organizations](#) by sending phishing emails containing SharePoint links that required authentication, enabling adversary-in-the-middle credential capture. Once mailboxes were compromised, attackers created inbox rules to suppress detection, then used the trusted accounts to distribute hundreds of follow-on phishing emails internally and externally. In at least one case, over 600 phishing messages were sent from a single compromised tenant within days. The campaign demonstrates how cloud collaboration tools can be weaponized to scale phishing from inside trusted environments.

Infostealer Admin Panels Exposed Through XSS Weakness

+StealC +XSS

- A cross-site scripting flaw in [StealC](#) malware control panels allowed attackers to hijack active operator sessions, access stolen credential logs, and observe live campaign activity. The compromised panels revealed large-scale credential theft operations, including millions of cookies and hundreds of thousands of passwords harvested via cracked-software lures. Session data also exposed operational security lapses, including inconsistent VPN use and regionally identifiable infrastructure. The incident underscores persistent weaknesses in criminal SaaS (MaaS) ecosystems and the fragility of attacker tooling.

Calendar Invites Become a Covert Data Exfiltration Channel

+Prompt Injection +AI

- A prompt-injection technique allows attackers to hide malicious instructions inside [calendar invite](#) descriptions that remain dormant until processed by an AI assistant. When users later ask scheduling-related questions, the AI can unintentionally summarize private calendar entries and write the extracted details into newly created events, effectively leaking sensitive meeting data without direct user intent. The attack bypasses traditional access controls by abusing AI interpretation rather than API permissions. This highlights how indirect prompt injection can transform benign enterprise data into an exfiltration vector.

Data Breaches

Exposed Test Apps Open Doors Into Fortune 500 Clouds

+Enterprise +Cloud

- Threat actors are systematically scanning for and exploiting misconfigured security-testing or deliberately vulnerable web applications that have been left publicly accessible on cloud environments tied to [Fortune 500](#) companies and security vendors. Because these apps are intentionally insecure and may run with privileged cloud credentials, attackers leverage them to deploy crypto miners, plant web shells, and pivot deeper into internal systems, achieving unauthorized access without needing initial zero-day exploits. The core failure mode is insecure internet exposure of internal training/testing resources combined with overly permissive cloud roles, turning benign tools into real breach vectors. This pattern highlights a broader issue where internal offensive security tooling doubles as an unintended external attack surface.

Iranian State TV Signal Hijacked for Protest Messaging

+Iran +News +Government

- During a period of political unrest and nationwide internet disruption, unknown attackers briefly interrupted [Iran's](#) state television satellite broadcasts across multiple channels to insert anti-regime content and calls for protest, including footage urging security forces not to use force against civilians. The intrusion was carried over the Badr satellite feed and lasted roughly 10 minutes, overriding scheduled programming. This incident demonstrates that attackers with access to broadcast infrastructure or transmission links can inject arbitrary content into national media, bypassing traditional content control and censorship mechanisms.

Sitecore Zero-Day Used to Establish Stealthy Enterprise Footholds

+China +CMS

- A China-linked threat actor exploited a previously unknown vulnerability in [Sitecore CMS](#) to gain initial access to enterprise and critical-infrastructure environments in North America. After exploitation, attackers conducted credential harvesting, reconnaissance, and persistence establishment, while disabling defensive controls to avoid detection. The campaign shows how widely deployed enterprise platforms remain attractive zero-day targets for long-term access operations. The activity appears focused on espionage rather than immediate disruption.

Kyowon Group Operations Disrupted by Ransomware Attack

+South Korea

- South Korean conglomerate [Kyowon Group](#) confirmed a ransomware attack that spread through internal systems after entering via an externally exposed server. The incident caused widespread operational disruption, forcing system shutdowns across multiple subsidiaries spanning education, publishing, and media services. Authorities warned that millions of customer and employee records could be within the breach scope, though full impact assessment is ongoing. The attack followed a common pattern of lateral movement and potential data exfiltration prior to encryption.

Canadian Investment Regulator Confirms Data Breach

+Canada +Government

- Canada's [Canadian Investment Regulatory Organization \(CIRO\)](#) disclosed a data breach impacting systems that store personal and regulatory information tied to investors and industry participants. The organization stated that sensitive data may have been accessed, prompting notification efforts and coordination with law enforcement and regulators. While no ransomware or threat actor has been publicly named, the breach underscores persistent risks to financial regulatory bodies, which hold centralized, high-value datasets. Investigation into the intrusion vector remains ongoing.

Ransomware Disrupts IT Distributor Ingram Micro

+IT

- Global IT distributor [Ingram Micro](#) reported a ransomware incident that disrupted internal systems and potentially exposed personal information tied to employees and partners. Regulatory filings indicate that data associated with approximately 42,000 individuals may have been impacted. The attack highlights the downstream risk of ransomware in technology supply chains, where disruption or data loss at a distributor can affect a wide ecosystem of vendors and customers. Service restoration and forensic analysis are ongoing.

Everest Ransomware Claims Breach of McDonald's India

+Everest +India +Food & Beverage

- The Everest ransomware group publicly claimed it breached [McDonald's India's](#) systems, asserting the exfiltration of approximately 861 GB of internal documents and customer data (including audit trails, financial reports, and contact records). Screenshots posted on the group's dark-web site show internal artifacts consistent with corporate analytics and business communications, and a two-day deadline was issued as part of extortion pressures. McDonald's India has not yet publicly confirmed or denied the attack; verification is pending. If authentic, this represents a large-scale data theft event on top of ransomware disruption, reflecting the modern emphasis on dual extortion (encryption plus data leak) tactics.

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.