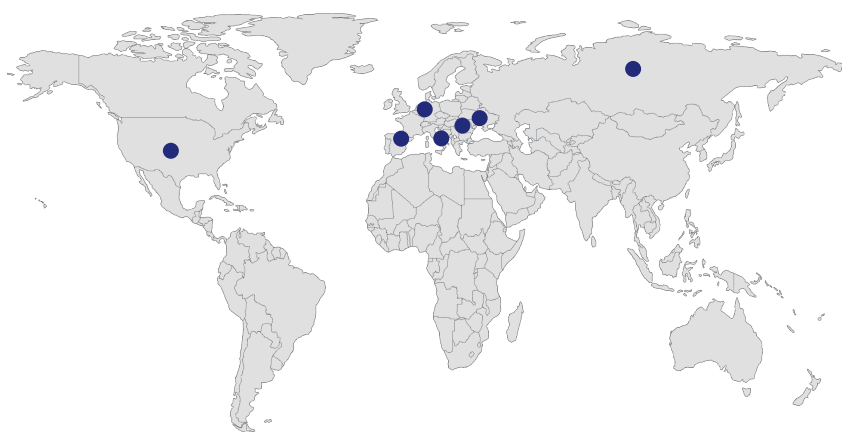


IMPERVA THREAT RESEARCH

Threat Intel Report: February 2-8, 2026

Countries



Top Tags

APT28

ShinyHunters

Bablock

Femwar02

Qilin

Executive Summary

Actionable Information:

- **Geopolitical Targeting of High-Visibility Events:** Nation-state-aligned actors continue to pursue disruption and influence operations around major international events and European public-sector infrastructure, making pre-event hardening and monitoring essential.
- **Rapid Exploitation of Newly Disclosed Vulnerabilities:** Advanced threat groups are weaponizing fresh software flaws within days, shrinking organizational patch and mitigation timelines.
- **Abuse of Trusted Platforms for Malware Distribution:** AI assistant marketplaces, developer repositories, and other legitimate ecosystems are being repurposed as scalable delivery channels that bypass reputation-based defenses.
- **Identity-Centric Data Theft as a Primary Objective:** Recent breaches show attackers prioritizing emails, profiles, and contact data to enable follow-on phishing, impersonation, and extortion campaigns.
- **Cloud Credential Exposure as a High-Speed Breach Vector:** Even limited cloud credentials can be quickly escalated through automated enumeration and privilege abuse, reducing detection windows to minutes.
- **Operational Disruption as a Consistent Impact:** Ransomware and intrusion activity against education, government, and energy organizations continues to cause service outages and business interruption, not just data loss.

Outlook:

In the near term, defenders should expect continued targeting of European institutions and internationally visible events, with rapid exploitation of newly disclosed vulnerabilities remaining a consistent tactic for espionage-focused actors. Simultaneously, financially motivated groups will likely expand their use of trusted platforms—particularly AI and developer ecosystems—as scalable malware distribution and access-broker channels, while monetizing stolen identity datasets through phishing and extortion. As automation and AI

tooling further compress intrusion timelines, the practical window for detection and response will continue to shrink, making credential hygiene, rapid patching, and controls around third-party integrations and remote-access pathways decisive factors in reducing breach impact.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

125% [CVE-2025-55752](#)

- Relative Path Traversal vulnerability in Apache Tomcat. The fix for bug 60013 introduced a regression where the rewritten URL was normalized before it was decoded. This introduced the possibility that, for rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/.

94% [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.

73% [CVE-2025-47812](#)

- In Wing FTP Server before 7.4.4, the user and admin web interfaces mishandle '\0' bytes, ultimately allowing injection of arbitrary Lua code into user session files. This can be used to execute arbitrary system commands with the privileges of the FTP service (root or SYSTEM by default). This is thus a remote code execution vulnerability that guarantees a total server compromise. This is also exploitable via anonymous FTP accounts.

German Food & Beverage Site Targeted by 4.85M RPS DDoS Attack

+Germany +Food & Beverage

- A German food and beverage company was targeted this week by an application-layer DDoS attack, reaching 4.85 million requests per second (RPS) in just 13 minutes. Coming from just 150 IPs, attackers targeted the site in an attempt to disrupt operations and production.

Scalper Bots Drive Massive API Abuse on Gaming Retail Platform

+Retail +Gaming +Scalping

- An online retail site selling popular trading cards experienced high volumes of business logic attacks, reaching over 60 million requests in one day aimed at scalping the popular trading cards. Attacks targeted product APIs, aiming to monitor inventory and detect restocks.

Recent Cyber Threats

Italy Blocks Russian Olympic Disruption Campaign

+Italy +Russia +Olympics

- Italian officials said they thwarted cyberattacks linked to Russia ahead of the [Milano-Cortina Winter Olympics](#) opening ceremony, indicating pre-event targeting of high-visibility international infrastructure. The activity was attributed to Russia-aligned hackers, though specific malware or intrusion details were not publicly disclosed. The attempted operations were likely intended to disrupt or undermine the event's operations and visibility. The incident highlights persistent nation-state interest in major global sporting events as symbolic and geopolitical targets.

Rapid Weaponization of Office Flaw Against European Targets

+Russia +Ukraine +Government +APT28

- Russia-linked APT28 exploited [CVE-2026-21509](#), a high-severity Microsoft Office vulnerability, shortly after disclosure to target Ukrainian government and EU organizations. Malicious Word documents triggered WebDAV connections, dropped payload components, and used COM hijacking to execute code and deploy the Covenant C2 framework. Emails impersonating Ukrainian institutions were sent to dozens of government recipients, indicating coordinated espionage activity. The campaign demonstrates rapid patch-reverse-engineering and continued targeting of European political entities.

AI Assistant Plugin Ecosystem Turns Into Malware Delivery Channel

+AI +OpenClaw

- Threat actors published over 230 malicious “skills” for the [OpenClaw](#) (formerly Moltbot/ClawdBot) AI assistant on its official registry and GitHub within days. The packages masqueraded as legitimate extensions but delivered password-stealing malware, exploiting the assistant’s deep local-system access and persistent memory features. Researchers also found exposed admin interfaces, increasing the risk of compromise. The activity highlights emerging software-supply-chain risk in rapidly growing AI-agent ecosystems.

Social Engineering Lure Installs Full Remote Access Tools

+Social Engineering +RAT

- Researchers observed a scam using [fake party invitation](#) messages to trick victims into installing remote access tools on Windows systems. Once installed, the software grants attackers full control of the device, enabling surveillance, data access, and further compromise. The campaign relies on familiar social-engineering language to lower suspicion and increase execution rates. The technique reflects continued abuse of legitimate remote-management software for initial access.

Trusted AI Platform Leveraged to Mass-Distribute Android Credential Stealers

+AI +Malware +Android

- Threat actors abused [Hugging Face](#) infrastructure to host thousands of polymorphic Android malware variants delivered through a fake TrustBastion dropper posing as a security app. The payload exploited Accessibility Services to capture screenshots, steal credentials for financial and payment apps, and exfiltrate data to command-and-control servers. Server-side polymorphism generated new samples roughly every 15 minutes to evade detection. The campaign demonstrates how trusted developer platforms are being repurposed as scalable malware distribution channels targeting mobile financial accounts.

Data Breaches

Mass Profile Data Exposure Hits Major Audio Platform

+Media +ShinyHunters

- Hackers exposed personal and contact information tied to roughly 29.8 million [SoundCloud](#) accounts after accessing internal systems and harvesting user data. The dataset included emails, usernames, profile details, and follower information, and researchers linked the activity to the ShinyHunters extortion group. Although passwords and financial data were reportedly not accessed, the breach mapped emails to public profiles, increasing the risk of targeted phishing and impersonation campaigns. The attackers also attempted to extort the company before the data circulated online.

Social Engineering Breach Impacts Robo-Advisor Customer Base

+Financial Services +Social Engineering +ShinyHunters

- Attackers compromised systems tied to the [Betterment](#) investment platform through a social-engineering attack that exposed data from about 1.4 million accounts. Stolen information included names, emails, geographic data, and in some cases addresses or birthdates, while passwords and account logins were not accessed. The intrusion enabled phishing messages (often crypto-themed) to be sent to customers, and threat actors linked to ShinyHunters reportedly claimed responsibility. The incident underscores how credential theft against employees and third-party platforms can cascade into large customer-data exposure.

Restaurant Chain Breach Dataset Leaked After Failed Extortion

+US +Food and Beverage +ShinyHunters

- A data breach at [Panera Bread](#) exposed roughly 5.1 million unique email addresses and associated account details after attackers attempted extortion and later published stolen data. The ShinyHunters group claimed to have taken a broader dataset containing personal information such as names, phone numbers, and physical addresses. The disclosure corrected earlier higher estimates but confirmed significant customer-data exposure. Public release of the dataset increases long-term fraud and phishing risk for affected users.

Eight-Minute Cloud Compromise Highlights AI-Accelerated Intrusions

+Unsecured Credentials +AWS +AI

- Researchers observed an attacker gain full administrative control of a company's [AWS environment](#) in roughly eight minutes after discovering exposed test credentials in a publicly accessible S3 bucket. The intruder used the compromised read-only account to enumerate services such as Secrets Manager, RDS, and CloudWatch, then escalated privileges by injecting code into Lambda functions and hijacking additional accounts. Analysis suggests AI-assisted automation helped accelerate reconnaissance and exploitation, while the attacker attempted to run costly AI workloads and pivot across organizational accounts. The incident underscores how basic credential-exposure errors combined with automated tooling can compress cloud-breach timelines from hours or days to minutes.

Spanish Science Ministry Halts Systems After Suspected Intrusion

+Spain +Government +Science

- [Spain's Ministry of Science](#) partially shut down IT systems after detecting a suspected cyberattack affecting services for citizens and companies. Authorities moved to contain the incident while assessing whether a data breach occurred. The disruption impacted access to government services, illustrating the operational consequences of attacks on public-sector infrastructure. Attribution and technical details have not yet been confirmed.

Europe's Largest University Knocked Offline by Suspected Ransomware

+Italy +Education +Bablock +Femwar02

- Rome's [La Sapienza University](#) shut down large portions of its IT infrastructure after a cyberattack forced administrators to take systems offline to contain the threat. Core digital services, including student management platforms, email, and websites, remained unavailable for days, disrupting exams, administrative tasks, and communications for more than 100,000 students. Italian media reports and external analysis suggest the incident may involve the Bablock ransomware family and a relatively new group known as Femwar02, though officials have not formally confirmed attribution. Recovery efforts relied on backups while national cybersecurity authorities assisted with investigation and restoration.

Ransomware Gang Targets National Oil Pipeline Operator

+Romania +Energy +Qilin

- Romania's national oil pipeline operator [Conpet](#) disclosed a cyberattack that disrupted corporate IT systems and took its website offline while leaving operational pipeline transport unaffected. The Qilin ransomware group claimed responsibility and said it stole nearly 1 TB of internal documents, publishing samples as proof. Authorities were notified and recovery efforts began with national cybersecurity support. The incident highlights continued ransomware pressure on energy and critical-infrastructure organizations.

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.