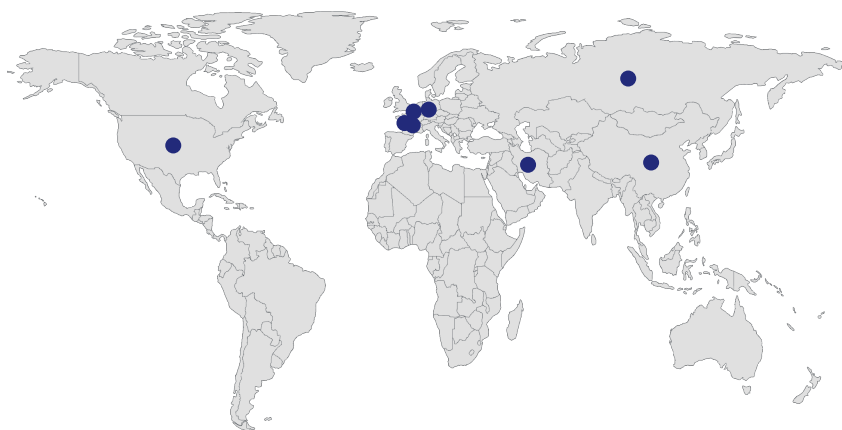


IMPERVA THREAT RESEARCH

Threat Intel Report: April 13-26, 2026

Countries



Top Tags

ShinyHunters

breach3d

Pegglecrew

313 Team

DDoS

Executive Summary

Actionable Information:

- **Identity-layer compromise is overtaking traditional exploitation:** Attacks are increasingly targeting authentication flows (phishing, vishing, SSO abuse) rather than software vulnerabilities, enabling access to high-value systems without needing technical exploits.
- **DDoS activity is shifting toward emerging platforms and influence targets:** Coordinated disruption campaigns are focusing on newer or decentralized services and political infrastructure, where resilience and mitigation maturity lag behind legacy platforms.
- **AI is accelerating both attack execution and defender workload:** AI-driven tooling is enabling rapid vulnerability discovery and multi-step exploitation, while simultaneously overwhelming security teams with increased detection volume and triage complexity.
- **Supply chain compromise remains a systemic risk multiplier:** Breaches of vendors, developer tooling, and third-party environments continue to create cascading exposure across downstream customers, particularly in critical infrastructure and software ecosystems.
- **Data breaches are increasingly monetized through extortion and secondary use:** Large-scale theft of PII is consistently followed by “pay-or-leak” tactics, with stolen data fueling follow-on phishing, fraud, and credential abuse campaigns.
- **Critical and high-visibility sectors remain primary targets:** Government, healthcare, utilities, and media organizations are consistently targeted due to the combination of sensitive data, operational impact, and reputational leverage.

Outlook:

The current threat landscape reflects a structural shift from isolated incidents to interconnected attack chains, where initial access—often through identity compromise or supply chain exposure—enables scalable downstream exploitation. The growing role of AI will likely compress the timeline between vulnerability discovery and exploitation, forcing organizations to prioritize speed of remediation and identity security over perimeter defenses alone. At the same time, disruptive operations such as DDoS and hacktivist activity are expected to continue targeting platforms with high visibility but uneven defensive maturity, particularly in politically sensitive contexts. Overall, organizations should expect higher attack velocity, increased reliance on social engineering, and broader blast radius from single compromises, making resilience and response coordination as critical as prevention.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

221% [CVE-2025-30208](#)

- Vite, a provider of frontend development tooling, has a vulnerability in versions prior to 6.2.3, 6.1.2, 6.0.12, 5.4.15, and 4.5.10. `@fs`` denies access to files outside of Vite serving allow list. Adding `?raw??`` or `?import&raw??`` to the URL bypasses this limitation and returns the file content if it exists. This bypass exists because trailing separators such as ``` are removed in several places, but are not accounted for in query string regexes. The contents of arbitrary files can be returned to the browser. Only apps explicitly exposing the Vite dev server to the network (using `--host`` or `server.host`` config option) are affected.

178% [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.

75% [CVE-2025-54236](#)

- Adobe Commerce versions 2.4.9-alpha2, 2.4.8-p2, 2.4.7-p7, 2.4.6-p12, 2.4.5-p14, 2.4.4-p15 and earlier are affected by an Improper Input Validation vulnerability. A successful attacker can abuse this to achieve session takeover, increasing the confidentiality, and integrity impact to high. Exploitation of this issue does not require user interaction.

SAP Upload Flaw Targeted Across Core Enterprise Systems

+France +Belgium

- Over a three-day period, attackers exploited SAP NetWeaver via CVE-2025-31324, targeting financial, telecom, and business sites in France and Belgium through an unrestricted file upload vulnerability (CVSS 9.8). These platforms are commonly internet-exposed and deeply embedded in backend operations, making them attractive targets for gaining initial access into high-value enterprise environments. Successful exploitation enables remote code execution, providing attackers with a direct path to sensitive data, internal systems, and broader operational disruption.

Recent Cyber Threats

Pro-Iran Hacktivist Group Claims Disruption of Emerging Social Network

+313 Team +Iran +Social Media +DDoS

- [Bluesky](#) experienced a ~24-hour DDoS attack that caused intermittent outages across core features like feeds and notifications. A group calling itself 313 Team, a pro-Iran hacktivist collective, claimed responsibility, though attribution remains unverified.

Bluesky reported no evidence of data access, indicating the attack was purely disruptive. The targeting highlights growing attention on alternative social platforms with comparatively weaker infrastructure defenses.

Decentralized Social Platform Disrupted by Coordinated Traffic Flood

+Social Media +DDoS

- [Mastodon](#) suffered a major DDoS attack targeting its primary server (mastodon.social), causing widespread outages for users. The attack generated millions of malicious requests, temporarily rendering the service inaccessible before mitigation restored access within hours. While no actor claimed responsibility, the incident followed a similar attack on Bluesky, suggesting a broader campaign targeting emerging decentralized platforms. Impact was limited to the main server, with other federated instances remaining operational.

Signal Phishing Campaign Compromises European Officials in Suspected Russian Espionage

+Germany +Netherlands +Russia +Phishing +Government +Journalism

- Authorities in Germany and the Netherlands are investigating a [phishing campaign](#) likely linked to Russia that targeted high-ranking officials via Signal. Attackers used fake “Signal security” messages to trick victims into sharing credentials or linking accounts, compromising ~300 accounts including politicians, military personnel, and journalists. The access enabled attackers to read messages, monitor communications, and potentially impersonate victims. The campaign reflects a shift toward identity-layer compromise of encrypted platforms rather than breaking encryption itself.

AI-Assisted Browser Exploitation Demonstrates Emerging Automated Attack Pathways

+AI

- [Advanced AI models](#) such as GPT-5.4 can be leveraged to identify and exploit browser vulnerabilities, including attacks against Safari. The research demonstrates how AI can chain reconnaissance, vulnerability discovery, and exploitation steps with minimal human input. This significantly lowers the barrier to executing complex attacks and accelerates exploit development timelines. The impact is strategic: AI is transitioning from assistive tooling to semi-autonomous offensive capability.

Data Breaches

Pre-Release Film Leak Exposes Persistent Studio Security Gaps

+Entertainment +Pegglecrew

- An unreleased \$80M [Paramount+](#) film, “Legend of Aang,” was leaked online six months before release, reportedly by the hacker collective Pegglecrew. The breach did not originate directly from Paramount’s systems, highlighting vulnerabilities across third-party and production pipelines. A broader report found 71% of major studios lack basic email spoofing protections, leaving them highly susceptible to impersonation and social engineering. The incident underscores continued systemic weaknesses in Hollywood despite years of high-profile breaches, with direct financial and reputational impact.

Unauthorized Access to High-Risk AI Model Raises Offensive Cyber Concerns

+AI +Technology

- Anthropic is investigating unauthorized access to its restricted [Mythos AI](#) model after individuals gained entry through a third-party vendor environment. The model has demonstrated the ability to autonomously execute multi-step cyberattacks and identify vulnerabilities, including completing a 32-step attack chain in testing. Although no malicious use has been confirmed, the breach highlights the risk of advanced AI tools escaping controlled environments. The incident emphasizes supply chain weaknesses and the potential for AI to enable scalable offensive operations.

Mass Identity Data Exposure Hits French Government Systems

+France +Government +breach3d

- France’s national identity agency ([ANTS](#)) confirmed a breach after a threat actor known as “breach3d” claimed to have stolen up to 19 million records and listed them for sale on the dark web. The exposed data includes names, birthdates, addresses, and account metadata tied to official identity services. While attackers did not gain account access, the scale of personal data exposure creates significant risk for phishing, fraud, and identity theft campaigns. The breach represents one of the largest exposures of government-held identity data in France.

Healthcare Giant Confirms Breach Following Mass Data Theft Claims

+Healthcare +ShinyHunters

- [Medtronic](#) confirmed that attackers breached its corporate IT environment and accessed data within internal systems after the extortion group ShinyHunters claimed to have stolen over 9 million records. While the company stated that operations, products, and patient care were not impacted, the scale of the alleged data theft suggests significant exposure of corporate or potentially personal data. The attackers are known for “pay-or-leak” extortion tactics, indicating a high likelihood of data monetization or public release. The incident underscores continued targeting of healthcare organizations for large-scale data exfiltration.

EdTech Platform Targeted in Expanding ShinyHunters Extortion Campaign

+Education +ShinyHunters

- The cybercriminal group ShinyHunters claimed to have breached [Udemy](#), alleging theft of 1.4 million user records containing PII and corporate data. The group issued a “pay or leak” ultimatum with a deadline, consistent with its extortion-driven operations. If validated, the breach would expose users to phishing and credential abuse while continuing a broader campaign targeting SaaS environments. The incident highlights the scalability of identity-focused attacks against large cloud-based platforms.

Home Security Provider Breach Highlights Identity-Based Entry Techniques

+Security +ShinyHunters +Vishing

- [ADT](#) confirmed a cyberattack after ShinyHunters claimed to have stolen millions of customer records, including names, phone numbers, and addresses. Attackers reportedly used a vishing-based compromise of an employee SSO account to access internal systems and exfiltrate data. The group is threatening to leak the data unless a ransom is paid, continuing its “pay or leak” model. The breach underscores the effectiveness of identity-layer attacks against enterprise SaaS environments.

Source Code Repository Breach Extends Supply Chain Fallout

+GitHub

- [Checkmarx](#) confirmed that data from its GitHub repository was posted on the dark web following a March 23 supply chain attack that initially compromised its development environment. Attackers leveraged access to tamper with components tied to developer tooling, part of a broader campaign affecting CI/CD pipelines and open-source dependencies. The incident raised concerns about exposure of sensitive development data and the potential for downstream compromise across organizations using affected tools. It highlights how single points of failure in software supply chains can cascade into widespread risk for developers and enterprises.

Utilities Supply Chain Breach Raises Downstream Infrastructure Risk

+Utilities

- [Itron](#) disclosed a cybersecurity breach impacting its internal systems, though it reported no disruption to operations. As a major provider to utilities globally, the incident raises concerns about potential downstream exposure across energy and water infrastructure customers. The lack of immediate operational impact suggests containment, but the broader risk lies in supply chain access into critical infrastructure environments. Attribution has not been publicly confirmed.

MP Website Redirected and Flooded in Suspected China-Linked Campaign

+China +UK +DDoS +Government

- A website linked to [UK MP David](#) Davis was compromised and then hit by a large-scale DDoS attack, with traffic largely traced to China. Attackers first injected malicious links that redirected visitors to gambling sites before launching a traffic flood of 142 million requests (~800GB) in 24 hours. The incident temporarily took the site offline and was described as interference with parliamentary duties. The attack demonstrates a blend of web compromise and volumetric disruption targeting political infrastructure.

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.