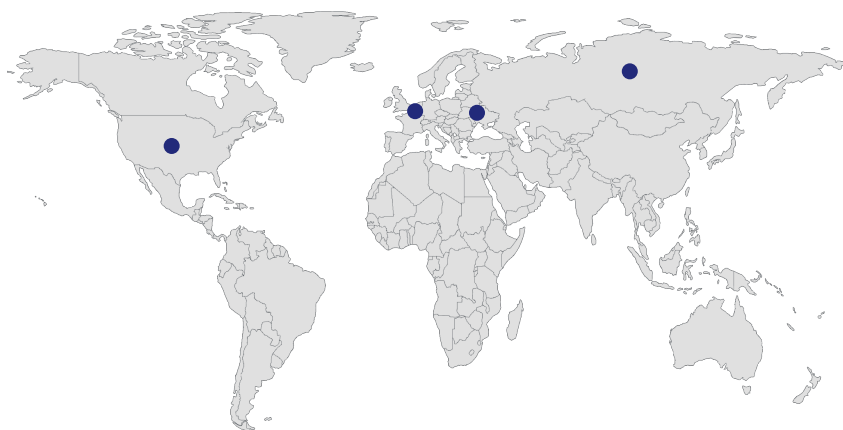


IMPERVA THREAT RESEARCH

Threat Intel Report: May 19-31, 2026

Countries



Top Tags

GREYVIBE

Glassworm

Silent Ransom

TanStack

ShinyHunters

Executive Summary

Actionable Information:

- **AI adoption is expanding both attacker capabilities and available attack surfaces.** Threat actors are increasingly integrating generative AI into multiple stages of cyber operations while simultaneously exploiting user trust in AI platforms for malware delivery and social engineering. As AI tools become embedded into daily workflows, attackers are finding new opportunities to abuse legitimate features, trusted domains, and rapidly adopted technologies that may not have mature security controls.
- **Developer ecosystems remain a primary target for scalable compromise.** Attackers continue to focus on source-code platforms, browser and IDE extensions, package repositories, and self-hosted development infrastructure because these environments provide access to credentials, proprietary code, and downstream organizations. Compromise of a single trusted component can enable broader supply-chain attacks, allowing threat actors to bypass traditional perimeter defenses by abusing legitimate developer workflows.
- **Threat actors are increasingly targeting trusted infrastructure and administrative platforms.** Security tools, endpoint management systems, SaaS environments, and authentication platforms remain attractive targets because they often have elevated privileges and broad organizational access. Successful compromise of these systems can allow attackers to blend into normal operations, steal credentials, or move deeper into enterprise environments through channels already trusted by defenders.
- **Extortion operations continue shifting toward identity theft, social engineering, and data-focused attacks.** Criminal groups are moving beyond traditional ransomware encryption by targeting high-value repositories of customer, employee, and business data. Campaigns increasingly rely on phishing, credential theft, SaaS compromise, and even physical intrusion attempts to obtain sensitive information while reducing the operational complexity associated with deploying ransomware.

Outlook:

Recent activity highlights the continued evolution of cyber threats away from isolated technical exploits and toward attacks against the interconnected systems organizations rely on every day. AI platforms, development pipelines, cloud services, identity providers, and security management tools are increasingly viewed as high-value access points that can produce widespread impact from a single compromise. Threat actors are also demonstrating greater flexibility, combining traditional malware, social engineering, supply-chain abuse, and legitimate platform functionality to evade defenses and maximize reach. Organizations should expect continued targeting of trusted ecosystems and prioritize securing third-party integrations, developer environments, identity controls, and administrative tools as attackers increasingly focus on the relationships between systems rather than only individual vulnerabilities.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 1,672% [CVE-2026-1492](#)

- The User Registration & Membership – Custom Registration Form Builder, Custom Login Form, User Profile, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to improper privilege management in all versions up to, and including, 5.1.2. This is due to the plugin accepting a user-supplied role during membership registration without properly enforcing a server-side allowlist. This makes it possible for unauthenticated attackers to create administrator accounts by supplying a role value during membership registration.

 1,159% [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.

 1,019% [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/. If PUT requests were also enabled then malicious files could be uploaded leading to remote code execution. PUT requests are normally limited to trusted users and it is considered unlikely that PUT requests would be enabled in conjunction with a rewrite that manipulated the URI. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.10, from 10.1.0-M1 through 10.1.44, from 9.0.0.M11 through 9.0.108. The following versions were EOL at the time the CVE was created but are known to be affected: 8.5.6 through 8.5.100. Other, older, EOL versions may also be affected.

Recent Cyber Threats

ChatGPT Share Links Abused to Deliver Malware

+AI +Malware

- Threat actors abused [ChatGPT's](#) share-link feature to host fake OpenAI outage pages that pushed malware disguised as the ChatGPT desktop application. The campaign exploited user trust in OpenAI-branded infrastructure and used a legitimate sharing mechanism to make malicious pages appear more credible. This reflects a broader shift in phishing and malware delivery, where

attackers are increasingly weaponizing trusted SaaS and AI platforms rather than relying only on lookalike domains. The incident also highlights how AI ecosystem adoption is creating new social-engineering surfaces, especially as users become accustomed to downloading AI tools, browser extensions, and desktop apps.

Dutch Authorities Disrupt 17 Million-Device Malware Botnet

+Netherlands

- Dutch authorities took offline a [malware botnet](#) affecting roughly 17 million devices and seized more than 200 servers hosted at a local provider supporting the operation. The disruption followed an investigation by Dutch police and the National Cyber Security Centre, showing the role of coordinated law enforcement and national cyber agencies in dismantling large-scale criminal infrastructure. The scale of the infected device population indicates the botnet had significant potential for credential theft, proxy abuse, spam, fraud, or distributed attacks. The operation also demonstrates how hosting providers and regional infrastructure can become central choke points for global cybercrime ecosystems.

GREYVIBE Uses Generative AI Across Ukraine-Linked Operations

+GREYVIBE +Russia +Ukraine

- [GREYVIBE](#), a Russia-nexus threat group, has been seen targeting Ukraine and Ukraine-related entities since at least August 2025. Researchers said the group showed strong evidence of systematic generative AI and LLM use across its operations, including development and operational phases, while also showing ties to the broader cybercrime ecosystem. The activity aligns with Russian state interests but does not yet have definitive links to a previously tracked group. GREYVIBE is notable because it shows AI moving beyond isolated phishing assistance and into repeatable operational support for state-aligned campaigns.

FortiClient EMS Flaw Exploited to Deploy EKZ Infostealer

+CVE +EKZ +Credential Stealer

- Attackers exploited [CVE-2026-35616](#), an authentication bypass vulnerability in FortiClient Enterprise Management Server, to deliver an undocumented credential stealer called EKZ. The malware was disguised as a Fortinet endpoint update and executed through VPN scripting workflows managed by FortiClient, making the attack especially concerning for environments that use endpoint and VPN tooling as trusted management channels. Because EMS systems often sit close to endpoint administration workflows, compromise can provide attackers with a strong position for credential theft and follow-on access. The campaign reinforces the risk of exploitation against security management platforms that have broad trust and deployment reach inside enterprise networks.

Gogs Zero-Day Enables RCE on Internet-Facing Git Servers

+Gogs +RCE

- Researchers disclosed an unpatched zero-day vulnerability in [Gogs](#), a self-hosted Git service commonly used as an alternative to GitHub Enterprise or GitLab. The flaw can allow attackers to gain remote code execution on internet-facing instances, creating direct risk to source-code repositories and developer infrastructure. Because Gogs is frequently exposed online for remote collaboration, vulnerable deployments could give attackers access not only to servers but also to sensitive code, credentials, and development workflows. The issue fits a broader pattern of attackers targeting software development environments as a path to supply-chain compromise.

Glassworm Botnet Disrupted After Developer Supply Chain Campaigns

+Glassworm +Botnet

- Researchers disrupted the [Glassworm](#) botnet after CrowdStrike, Google, and The Shadowserver Foundation cut off four command-and-control channels designed to resist takedown. Glassworm had targeted developers since October 2025 through malicious OpenVSX and Microsoft VS Code extensions used to steal cryptocurrency wallets and developer credentials. Its C2 infrastructure relied on Solana blockchain transactions and the BitTorrent DHT network, reflecting growing experimentation with decentralized infrastructure to make malware operations more resilient. The campaign underscores continued attacker focus on developer tooling, where compromised extensions can harvest credentials and create downstream software supply-chain exposure.

Silent Ransom Group Adds In-Person Data Theft to Extortion Playbook

+Silent Ransom +Social Engineering +US

- The FBI warned that [Silent Ransom Group](#) is targeting U.S. law firms with a social-engineering scheme that can escalate from phone and phishing contact to physical intrusion. Operators pose as IT support, direct employees to grant remote desktop

access, and, if that fails, may send someone to the victim's location to insert a storage device into a company computer. The group, also known as Luna Moth, Chatty Spider, and UNC3753, has targeted legal and financial organizations since at least 2023 and uses stolen data for extortion rather than traditional encryption-based ransomware. The tactic shows how cyber extortion groups are blending digital access attempts with physical security weaknesses to obtain sensitive data.

Data Breaches

GitHub Breach Linked to TanStack Supply Chain Attack

+[TanStack](#) +[Mini Shai-Hulud](#)

- [GitHub](#) confirmed that attackers breached approximately 3,800 internal repositories through a malicious Nx Console VS Code extension tied to the TanStack npm supply-chain attack. The incident was part of the broader Mini Shai-Hulud campaign, which compromised hundreds of npm and PyPI packages through stolen CI/CD credentials and legitimate workflows. GitHub said the breach did not affect production systems, but the exposure of internal repositories highlights the sensitivity of developer environments even when customer-facing systems remain intact. The attack reinforces how malicious extensions and package ecosystem compromises can cascade into source-code exposure across major technology organizations.

Charter Communications Breach Affects 4.9 Million Accounts

+[ShinyHunters](#) +[Voice-phishing](#) +[Telecommunications](#)

- [Charter Communications](#) confirmed a breach after ShinyHunters claimed it compromised the company through a voice-phishing attack against an employee's Microsoft Entra account. Have I Been Pwned reported that 4.9 million accounts were affected, while Charter said no sensitive personal information or customer proprietary network information was exfiltrated. ShinyHunters claimed it used the compromised access to export consumer and business customer records from Charter's Salesforce environment. The breach fits the group's broader pattern of targeting identity platforms, SaaS environments, and CRM data for scalable data theft and extortion.

Carnival Confirms Breach Affecting Nearly 6 Million People

+[ShinyHunters](#) +[Travel](#)

- [Carnival Corporation](#) confirmed a data breach affecting nearly 6 million people after ShinyHunters claimed responsibility for the incident in April. Carnival is the world's largest cruise line operator, with more than 90 ships and about 13.5 million guests served in 2024, making the breach significant because of the volume and sensitivity of travel-related customer data. The incident adds another major travel and hospitality brand to the growing list of ShinyHunters-linked compromises. It also reinforces how large consumer-facing organizations remain attractive extortion targets because they hold high-volume identity and loyalty datasets.

7-Eleven Breach Exposes Personal Information of 183,000+ People

+[ShinyHunters](#) +[Retail](#)

- [7-Eleven](#) confirmed that attackers gained access to systems used to store franchisee documents, with Have I Been Pwned later reporting that personal information for more than 183,000 people was stolen. The breach was claimed by ShinyHunters, continuing the group's campaign against major retail and consumer brands. 7-Eleven operates more than 86,000 stores globally and manages large loyalty programs, making even limited system access relevant because of the brand's scale and partner ecosystem. The incident reflects the ongoing shift toward data theft and extortion campaigns targeting franchise, CRM, and business-document repositories rather than encryption-based disruption.

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.