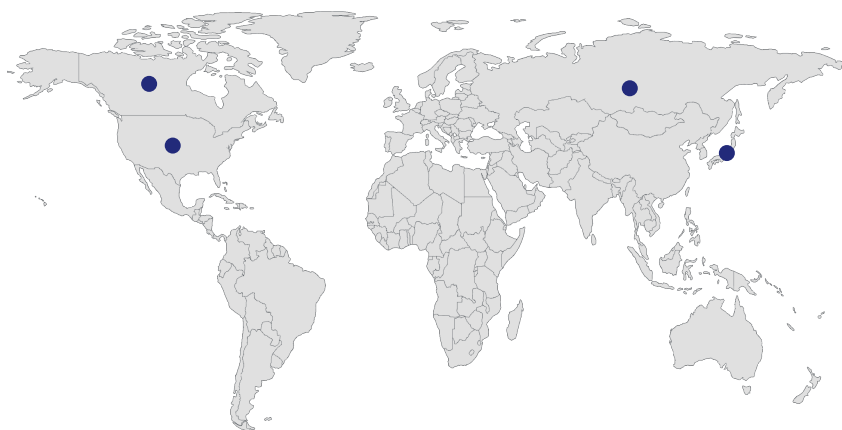


IMPERVA THREAT RESEARCH

Threat Intel Report: October 20-26, 2025

Countries



Top Tags

Lumma Stealer

ClickFix

AI

Medusa

Genesis

Executive Summary

Actionable Information:

- **Supply Chain and Trust Exploitation:** Attackers are increasingly targeting dependencies, open-source components, and third-party providers to gain access indirectly. Strengthening supply chain visibility and vendor risk management is essential.
- **Ransomware Expansion and Fragmentation:** The ransomware ecosystem continues to diversify, with new groups emerging and established ones evolving. Organizations should assume continuous exposure and emphasize resilience and rapid recovery.
- **Platform and Interface Manipulation:** Threat actors are shifting toward abusing trusted platforms and interfaces, from social media networks to AI assistants, to deliver malware and deceive users. Enhanced user awareness and integrity controls are needed to counter this shift.
- **AI as a Growing Attack Surface:** The rapid integration of AI tools introduces new security gaps, including data exposure through automated behaviors and prompt manipulation. Enterprises should treat AI ecosystems as high-risk assets requiring dedicated safeguards.
- **Persistent Public-Sector Vulnerability:** Local governments and smaller agencies remain frequent targets due to limited defenses and high operational impact, underscoring the need for improved baseline security and coordinated response frameworks.

Outlook:

This week's activity points to a fragmented but intensifying threat landscape where trust abuse and third-party compromise are as dangerous as direct exploits. Ransomware groups continue to proliferate, with new players like Genesis emerging even as established names rebrand or implode, suggesting a churn that keeps the overall ecosystem resilient. The blending of AI-driven interfaces and social engineering marks a turning point: attackers are adapting faster than technical defenses by hijacking user trust and automation. Expect increased cross-platform manipulation (browser extensions, AI assistants, content-sharing platforms) and deeper infiltration through

supply chains in Q4 2025. Organizations should prioritize visibility across dependencies, validation of digital trust boundaries, and user-interface security as key defenses against the next wave of cyberattacks.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,933% [CVE-2024-9463](#)

- An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.

↑ 109% [CVE-2025-47227](#)

- In the Production Environment extension in Netmake ScriptCase through 9.12.006 (23), the Administrator password reset mechanism is mishandled. Making both a GET and a POST request to login.php is sufficient. An unauthenticated attacker can then bypass authentication via administrator account takeover.

↑ 90% [CVE-2024-53675](#)

- An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.

Recent Cyber Threats

Underground Dox Slows Lumma Stealer Market

+Lumma Stealer

- Rival threat actors published a targeted doxxing campaign exposing alleged core members and operational details of the [Lumma \(aka Water Kurita / LummaC2\) info-stealer service](#), prompting a sharp drop in Lumma activity and a migration of customers to competing stealers. Security vendors and reporting say the leaks revealed personal and infrastructure data that forced Lumma operators to change comms and infrastructure, disrupting their malware-as-a-service business. The incident follows earlier takedowns and legal actions against Lumma and underscores how underground rivalry and OPSEC failures can blunt a prolific info-stealer's operations.

NuGet Homoglyph Package Steals Crypto Keys

+NuGet +Crypto

- Researchers discovered a [malicious NuGet package impersonating Nethereum](#) by swapping an ASCII "e" for a Cyrillic homoglyph; the package contained code that decodes a C2 endpoint and exfiltrates mnemonic phrases, private keys and keystore data to the attacker. The malicious package (Nethereum.All) artificially inflated download counts to appear popular and boost search ranking, enabling developers to accidentally pull the backdoored library into projects. NuGet removed the packages after disclosure; researchers warn that NuGet's permissive naming allows Unicode homoglyph abuse and that devs must verify publishers and unusual download surges.

YouTube "Ghost Network" of Compromised Channels Removed

+Malware

- Google removed a [large network of YouTube channels that were being used to distribute malware and coordinate malicious campaigns](#), a covert "ghost network" that leveraged the platform's reach to push payloads and command channels. The takedown disrupted the operators' ability to host and promote malicious content through video descriptions, comments, and

linked infrastructure, illustrating continuing abuse of major social/video platforms for large-scale malware distribution. The action reduces an easy, high-visibility vector for operators but highlights that platform misuse remains an ongoing risk.

Spoofed AI Sidebars Trick Atlas/Comet Users into Dangerous Actions

+AI Browsers +AI

- Researchers found [attackers can inject spoofed AI “sidebars” into Atlas and Comet AI assistants’ interfaces](#), tricking users into executing dangerous actions (like exfiltrating secrets or clicking malicious links) by mimicking trusted assistant UI elements. Because the spoofed sidebars closely resemble legitimate assistant controls, users can be fooled into lowering guard and performing sensitive operations, a UI-based social-engineering vector that targets knowledge-worker workflows rather than exploiting software bugs. Developers and users are advised to harden UI isolation, verify provenance of assistant content, and treat in-assistant prompts with the same skepticism as emails or web pages.

“I am not a robot” Clickfix Campaign Evolves

+ClickFix +Russia

- [Russian operators have evolved the “I am not a robot” ClickFix lure](#) by embedding more sophisticated malware payloads in fake CAPTCHA/fix workflows: victims who attempt to interact with ostensibly broken verification widgets receive installers that deploy info-stealers, RATs and other malware families. The campaign uses social engineering to bypass casual defenses, and operators have updated tooling and distribution techniques to increase success rates against a broad set of victims. Security teams should monitor for unusual redirects, unexpected installers after CAPTCHA interactions, and reinforce endpoint controls and browser hygiene.

Shadow-Escape: 0-Click Attack Concept Threatens AI Assistants’ Data Masses

+AI

- Researchers described [a “Shadow Escape” style 0-click attack against AI assistants](#) where malicious inputs or crafted interactions (requiring no explicit user click) could trigger assistants to leak or act on sensitive data, potentially exposing massive aggregated records across services that integrate assistants. The writeups warn that as assistants gain more automatic behaviors and cross-service access, the attack surface for silent exploitation grows, and providers must harden input validation, rate limits, and cross-origin protections to prevent large-scale automated leakage. The analysis frames the risk as systemic: billions/trillions of records could be at risk if such vectors are weaponized at scale

Data Breaches

Massive Data Haul Leaked After Attack on Media Giant

+Medusa +Telecommunications

- [Medusa claims to have stolen approx. 834 GB of data from Comcast Corporation](#) and released roughly 186 GB (compressed) after a failed ransom demand of US \$1.2 million. The files allegedly include internal financial, actuarial and analytics scripts and spreadsheets, indicating deeper business-data access beyond simple customer PII. Comcast has not publicly confirmed the breach, raising concerns about the scope and response from this major media/telecom firm.

Retailer’s Customer Database Compromised in Canada

+Canada +Retail

- [Toys “R” Us Canada disclosed that attackers accessed its customer database](#) and stole names, addresses, emails and phone numbers, though, importantly, they stated no passwords or credit-card/financial information were taken. The breach was discovered after stolen data appeared on an “unindexed internet” repository, and the company is investigating and notifying regulators, but has not released exact numbers or attacker identity. The incident highlights risks even when financial data isn’t taken: the exposed contact/identity info still enables targeted phishing, impersonation and fraud.

New Ransomware Gang “Genesis” Emerges With Multiple Claims

+Genesis +US

- A previously unreported ransomware gang calling itself [Genesis publicly claimed responsibility for nine separate data breaches](#) in the U.S., including at Healthy Living Market & Café (an organic grocery chain) and River City Eye Care (optometrist). They assert

~2.2 TB of stolen data across the nine alleged victims; the two that confirmed breaches report names, SSNs, driver's licence numbers, medical records and payroll info among the data said to have been stolen. Neither company disclosed ransom payments or how much data was exfiltrated, and researchers note that some of Genesis' claims overlap with other groups' claims, suggesting either overlaps, opportunistic claim-making, or impersonation.

Municipal and County Services Hit Across U.S. States

+US +Government

- [Multiple jurisdictions in Texas, Tennessee and Indiana reported cyber incidents this week impacting government services.](#) For example, Kaufman County (TX) detected a cyberattack that disrupted county systems (though emergency services were spared), and in Tennessee, the city of La Vergne experienced a Friday attack that disabled property tax and water-billing systems. These cases reflect a rising trend of public-sector infrastructure being targeted, where the attackers may aim for disruption, ransom or both, and show that local government remains a vulnerable sector.

Global Retailer's Online Store Halts After Supplier Ransomware

+Japan +Retail

- [The Japanese retailer Muji had to suspend its online sales operations after its logistics partner Askul Corporation was hit by a ransomware attack.](#) Askul confirmed the systems outage and that customer ordering, website/app browsing, shipping and catalog services were down while investigation continues into possible data leaks. This incident highlights the risk of third-party/supply-chain dependencies in retail: even if the primary retailer isn't directly breached, a supplier disruption can shut down fulfilment and e-commerce for major brands.

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.