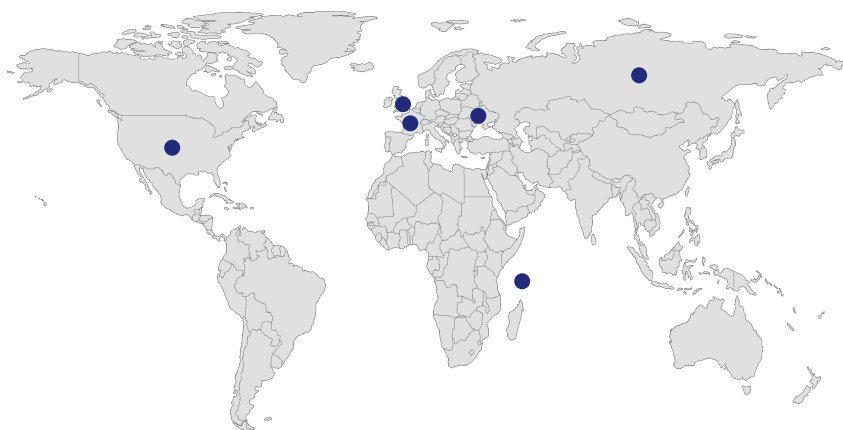


IMPERVA THREAT RESEARCH

Threat Intel Report: July 14-20, 2025

Countries



Top Tags

APT28

RansomHub

DragonForce

Scattered Spider

Van Helsing

Executive Summary

Actionable Information:

- **AI-driven threats are accelerating**, with attackers increasingly using large language models to craft dynamic, real-time payloads or manipulate trusted features in enterprise tools.
- **Supply chain and open-source ecosystems remain vulnerable**, as attackers exploit popular development packages and third-party dependencies to distribute malware and steal data.
- **Web infrastructure attacks are becoming stealthier**, using novel techniques like ZIP-based file inclusion and prompt injection to evade detection and compromise systems.
- **Data breaches continue across sectors**, with healthcare, education, retail, and crypto all experiencing significant incidents—driven by both misconfigurations and targeted ransomware.
- **Ransomware groups and data extortion actors show persistent activity**, leveraging both traditional and emerging vectors to breach sensitive environments and leak stolen data.

Outlook:

The threat landscape this week highlights a growing convergence between advanced attack techniques and traditional data theft. AI is not only a tool for defenders—it's now being adopted by threat actors to enhance speed and stealth. Meanwhile, widespread breaches underscore the ongoing need for stronger third-party risk management, cloud and infrastructure hardening, and cross-sector data protection strategies. We expect AI abuse, open-source compromise, and healthcare-targeted extortion to remain prominent through Q3.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 14,100% [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.

↑ 93% [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.

↑ 83% [CVE-2025-20029](#)

- Command injection vulnerability exists in iControl REST and BIG-IP TMOS Shell (tmsh) save command, which may allow an authenticated attacker to execute arbitrary system commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

Surge in ATO Attacks on South American Finance Sector

+Financial Services +South America +ATO

- A South American financial services company was targeted by account takeover this week, in an attack that reached 1.2 million login attempts in a single day. The attack, which targeted the site's authentication portals, came from entirely US-based IPs.

Automated Attack Targets French Retailer

+France +Retail +Automated Attack

- A French retail website experienced over 1.5 million automated requests in a single day, likely aimed at probing for vulnerabilities or harvesting data. The attack traffic originated entirely from scanning tools hosted in Germany, highlighting the continued use of commercial scanners and cloud-based infrastructure in retail-targeted reconnaissance campaigns.

Recent Cyber Threats

Gemini Prompt Injection Enables Phishing Summaries

+AI +Prompt Injection +Phishing

- Security researchers demonstrated how hidden HTML/CSS in emails can hijack Google Gemini's [Summarize this email](#) feature to inject fake security alerts and phishing prompts. The technique exploits invisible directives that Gemini dutifully displays—even though no real links are present—raising significant risks for Gmail Workspace users. Google is rolling out mitigations, but users should treat AI-generated summaries cautiously.

Sophisticated ZIP-based PHP Malware Targets WordPress

+PHP +WordPress +Malware

- A stealthy [PHP malware variant](#) was uncovered that embeds malicious scripts within a win.zip archive, leveraging PHP's zip:// wrapper to dynamically include domain-named payloads. The malware activates silently on WordPress sites, redirecting visitors

to spam or malicious domains after a few seconds. Site owners should audit unusual ZIP-related code and harden PHP file access mechanisms.

Malicious PyPI Package Steals Credit Cards

+PyPI

- Imperva researchers discovered a trojanized PyPI package named [cloudscrapersafe](#), posing as a trusted Cloudflare-bypass library but harboring logic to capture credit card data. Uploaded on July 6 and leveraging over 1.4 million downstream installs of the legitimate cloudscraper package, it exfiltrates stolen billing info to a Telegram bot. Developers are urged to scrutinize package provenance and apply supply-chain security checks.

LameHug Malware Leverages AI for Real-Time Data Theft

+Ukraine +Russia +APT28 +LameHug +Malware +AI

- CERT-UA attributed the newly spotted [LameHug](#) malware to Russian state-linked APT28. The python-based strain uses a large-language model via the Hugging Face API to generate reconnaissance and data-exfiltration commands on compromised Windows hosts in real time. It searches for documents, logs system info, and exfiltrates collected data via SFTP or HTTP POST. This marks a first: malware dynamically crafting attack commands through AI.

Data Breaches

Illinois School District Breach Exposes 11.5K Records

+US +Education +RansomHub

- [Indian Springs School District 109](#) (Chicago area) notified 11,542 individuals that an October 2024 ransomware breach compromised personal records—spanning SSNs, financial accounts, health and IEP info. RansomHub claims they exfiltrated 45 GB of data and published samples to prove the breach. The district is offering credit monitoring while the investigation and any ransom negotiations remain undisclosed.

DragonForce Claims 156 GB Hack on Belk

+Retail +US +DragonForce

- The RaaS-linked group [DragonForce](#) claims responsibility for a May attack on department store chain Belk, stealing approximately 156 GB of internal data. The haul reportedly includes sensitive corporate files and personally identifiable information like SSNs. This marks another in a recent series of retail breaches targeting U.S. brands.

Co-op Reveals 6.5M Customer Records Stolen

+UK +Retail +Scattered Spider

- UK's [Co-op](#) confirmed hackers exfiltrated personal data of all 6.5 million members during an April cyberattack, capturing names, addresses, and contact info, though no financial data was taken. Authorities have arrested four suspects; the hacker group Scattered Spider is believed to be involved. Co-op shut down systems to curb the breach but suffered widespread operational disruptions.

Compumedics Ransomware Leak Hits 320K Patients

+Healthcare +Van Helsing

- Medical tech firm [Compumedics](#) disclosed a ransomware breach in March impacting at least 320,404 individuals across hospitals and clinics, exposing a trove of patient data including SSNs, medical histories, treatment dates, and sleep study results. The Van Helsing group is suspected behind the breach, which spanned multiple facilities.

Gladney Adoption Records Leak Exposes 1.1M Sensitive Profiles

+Healthcare +Non-Profit +Misconfigured Database

- A researcher discovered a misconfigured public database at [Gladney Center for Adoption](#) in Texas, exposing 1.1 million records by late June. The records included sensitive data: children's and parents' identities, medical histories, CPS and court records. The database was secured only after multiple notifications, underscoring the acute risks of misconfiguration in sensitive domains.

Episource Healthcare Breach Impacts 5.4M People

+US +Healthcare +Third-Party

- Medical billing provider [Episource](#) suffered a breach discovered February 6, 2025, where attackers lingered for 10 days and exfiltrated data of 5.4 million individuals, including PHI and PII tied to Medicare/Medicaid. The incident highlights ongoing supply-chain vulnerabilities within healthcare third-party systems.

BigONE Exchange \$27M Crypto Heist from Hot Wallet

+Seychelles +Crypto +Financial Services

- [BigONE](#), a Seychelles-based crypto exchange, suffered a hot wallet attack resulting in theft of around \$27 million in assets including BTC, ETH, USDT, SOL and XIN. The exchange confirmed private keys and personal data weren't compromised and pledged full reimbursement using reserves. It's working to trace the funds.

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.