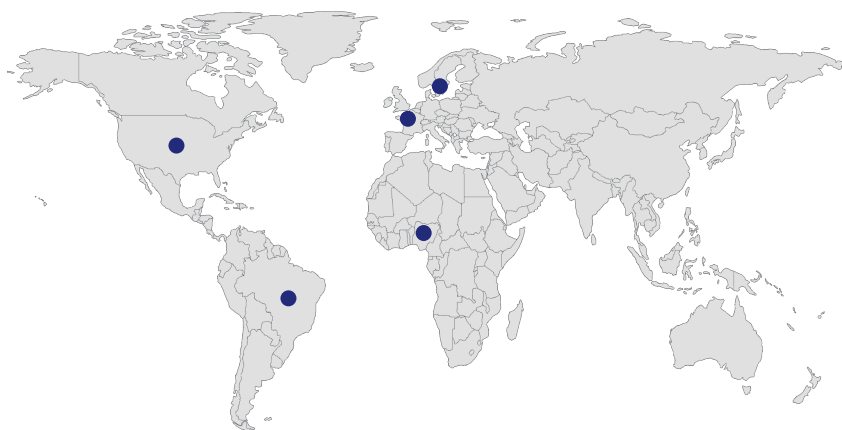


IMPERVA THREAT RESEARCH

Threat Intel Report: August 25-September 7, 2025

Countries



Top Tags

Lazarus

ShinyHunters

Financial Services

Crypto

SQLi

Executive Summary

Actionable Information:

- **Third-party and supply-chain exposure is a leading multiplier of risk.** Breaches increasingly originate from vendors, SaaS integrations, and code repositories, highlighting the need for vendor risk management, continuous monitoring of external dependencies, and clear contingency planning for supplier outages.
- **Financially motivated campaigns are escalating in both sophistication and ambition.** Attackers are leveraging zero-days, custom malware, and social engineering to target high-value industries, while also attempting direct monetization through large-scale fraud and payment system abuse.
- **Consumer communication platforms remain priority targets.** Messaging apps and account-linking features are under heavy exploitation pressure, showing how widely trusted platforms can be repurposed for account takeovers, espionage, and fraud at scale.
- **Common web vulnerabilities continue to drive compromise.** Despite advances in defense, basic flaws such as SQL injection are still pervasive, demonstrating the importance of secure development practices and layered protections such as WAFs.
- **Credential and token hygiene remains a weak point.** Secrets embedded in development pipelines and cloud platforms continue to be a high-value target, requiring systematic scanning, rotation, and least-privilege access enforcement.

Outlook:

Looking ahead, organizations should anticipate an intensified focus on supply-chain and vendor ecosystems as attackers exploit the “weakest link” to achieve broad impact. Financial services and payment systems will remain primary targets, with adversaries blending technical exploits and social engineering to maximize payout opportunities. Messaging and collaboration platforms will likely see ongoing zero-click and account takeover attempts, reflecting their role as gateways to both individuals and enterprises. At the same time, legacy

vulnerabilities in web applications and poor credential hygiene will ensure a steady stream of opportunistic attacks. The overall trend points toward convergence of data theft, fraud, and operational disruption, requiring a balanced defense strategy that combines preventative controls, real-time monitoring, and resilience planning.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 324% [CVE-2024-56145](#)

- Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Users of affected versions are affected by this vulnerability if their php.ini configuration has `register\_argc\_argv` enabled. For these users an unspecified remote code execution vector is present. Users are advised to update to version 3.9.14, 4.13.2, or 5.5.2.

 104% [CVE-2024-36680](#)

- In the module "Facebook" (pkfacebook) <=1.0.1 from Promokit.eu for PrestaShop, a guest can perform SQL injection. The ajax script facebookConnect.php have a sensitive SQL call that can be executed with a trivial http call and exploited to forge a SQL injection.

 94% [CVE-2024-50623](#)

- In Cleo Harmony before 5.8.0.21, VLTrader before 5.8.0.21, and LexiCom before 5.8.0.21, there is an unrestricted file upload and download that could lead to remote code execution.

Retaliatory Cyberattacks Target Nigerian Financial Sector

+Financial Services +Nigeria

- Over a five-day period, Nigerian financial institutions and some local business sites were hit with a wave of coordinated cyberattacks. Targets faced API abuse, large-scale automated probing, path traversal, authentication bypass, and remote code execution attempts, suggesting an organized campaign to exploit vulnerabilities across accounts. The timing is notable: just one day earlier, Nigeria deported 51 Chinese and Tunisian nationals in a nationwide crackdown on cybercrime. The immediate surge of attacks against core industries strongly points to retaliatory action.

Recent Cyber Threats

Lazarus Unleashes Triple-RAT Zero-Day Assault

+RAT +Lazarus +Financial Services +Crypto

- Over the past two years, researchers have observed a sophisticated [Lazarus](#) subgroup exploiting an unpatched zero-day vulnerability to deploy three different Remote Access Trojans (RATs) against financial and cryptocurrency organizations. The campaign is multi-staged and appears highly targeted, with attackers posing as legitimate trading firm employees through Telegram and counterfeit Calendly-style websites to lure victims. These operations demonstrate Lazarus's continued refinement of social engineering combined with technical exploitation to achieve persistent access.

WhatsApp Device-Link Scam Hijacks Accounts

+Messaging +Scam

- Attackers exploit [WhatsApp's](#) device-link feature, tricking victims into entering Facebook credentials that enable the attacker to link a malicious device and seize full control over the user's account. Once hijacked, victims' contacts, chat histories, and media

are accessible and used to propagate further scams or malware. The deception is particularly dangerous due to its seamless, zero-click nature and reliance on trusted-looking credential prompts.

SQLi Warning for WordPress Membership Plugin

+SQLi +WordPress

- A critical unauthenticated SQL injection vulnerability (CVE-2025-49870) was discovered in the widely used “Paid Member Subscriptions” [WordPress](#) plugin (affecting versions up to 2.15.1). The flaw allows attackers to manipulate SQL queries via unsanitized PayPal IPN data, potentially exposing sensitive user information like email addresses and hashed passwords. With over 10,000 sites impacted, the risk includes phishing, credential stuffing, or full account compromise—making immediate updating to version 2.15.2 essential.

WhatsApp Seals Zero-Click Zero-Day Hole (CVE-2025-55177)

+CVE +Zero-Click +Messaging

- [WhatsApp](#) patched a critical zero-day, zero-click vulnerability (CVE-2025-55177) that allowed attackers to bypass proper authorization during linked-device synchronization and potentially execute code on users' devices without interaction. The flaw was believed to be actively exploited in advanced spyware campaigns, prompting urgent remediation. The complex nature of the exploit, involving WhatsApp's linkage mechanism, underscores the evolving attack vectors in trusted messaging infrastructures.

Data Breaches

TransUnion Breach Compromises 4.4M Customer Records via Vendor Access

+Financial Services +US +ShinyHunters

- [TransUnion](#) reported a breach exposing personal information of over 4.4 million individuals due to unauthorized access through a third-party application on July 28 and discovered two days later. Although credit report data was reportedly unaffected, data breached likely included names, email addresses, birthdates, SSNs, and possibly transaction details, with the threat heavily tied to ShinyHunters' broader Salesforce-linked intrusion campaign. TransUnion is cooperating with law enforcement, offering 24 months of identity-theft protection, and warning users to monitor for phishing and freeze credit if needed.

Auchan Loyalty Data Exposed in Massive Retail Breach

+France +Retail

- French retail giant [Auchan](#) has confirmed a cyberattack affecting several hundred thousand loyalty account holders. Exposed data includes full names, titles, client statuses, postal and email addresses, phone numbers, and loyalty card numbers; however, bank data, passwords, and PINs remain secure. The incident raises concerns for identity theft, phishing, and fraud, as well as potential reputational damage and heightened regulatory scrutiny under GDPR.

Farmers Insurance Vendor Breach Hits Over 1 Million Customers

+Financial Services +US

- [Farmers Insurance](#) and its affiliated firms disclosed that over 1.1 million customers were impacted by a breach stemming from a third-party vendor's system, discovered May 30 and publicly revealed in late August. Compromised data includes names, addresses, birthdates, driver's license numbers, and partial Social Security numbers. The breach is linked to a broader wave of Salesforce-related attacks using malicious OAuth apps, prompting Farmers to offer two years of identity-theft protection and to urge customer vigilance against phishing and fraud.

Ransomware Cripples HR Systems Across 200 Swedish Municipalities

+Sweden +Government

- A ransomware assault on [Miliödata](#)—an IT provider managing HR and sick-leave systems for about 80% of Swedish municipalities—has knocked offline critical admin services in nearly 200 municipal governments. The attack was detected on August 23 and triggered national response from CERT-SE and Swedish civil defense, with a ransom demand of approximately 1.5 bitcoin (~\$163,000). While no known threat group claimed responsibility, the incident underscores the escalating threat to public infrastructure via supply-chain attacks.

Fintech Breach Triggers \$130M Heist Attempt via Brazil's Pix System

+Financial Services +Brazil

- Hackers compromised the systems of [Sinqia S.A.](#), Evertec's Brazilian subsidiary, and attempted to orchestrate unauthorized \$130 million transactions over Brazil's Pix real-time payments network. The attack involved access to the fintech platform and was likely orchestrated via illicit transfers between financial institutions. Financial watchdogs are analyzing the breach to tighten real-time payment system security in this major attempted heist.

GhostAction Strikes GitHub—Thousands of Secrets Plucked from Repos

+GhostAction +GitHub

- The [GhostAction](#) supply-chain campaign has breached 817 GitHub repositories, extracting 3,325 credentials, including npm, PyPI, and DockerHub tokens. Though technical methodology remains unclear, the attack carries medium severity, risking unauthorized access to cloud services, databases, and internal systems. The breadth across European repositories raises heightened GDPR and regulatory concerns for affected 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.