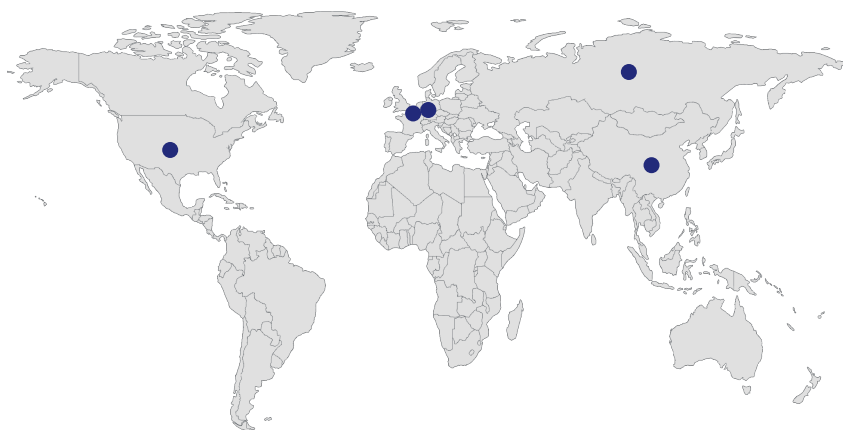


IMPERVA THREAT RESEARCH

Threat Intel Report: July 28-August 3, 2025

Countries



Top Tags

Houdini

Cobalt Strike

LightBasin

BlackSuit

ShinyHunters

Executive Summary

Actionable Information:

- **AI development tools and browser extensions are emerging as major attack surfaces**, with recent exploits showing how easily attackers can hijack trust in AI outputs and DOM environments.
- **Trusted platforms and services continue to be weaponized for malware delivery**, including GitHub, Quora, Discord, and even Salesforce via OAuth abuse.
- **Physical and hardware-based intrusions are growing more advanced**, with attackers planting rogue devices inside networks to bypass traditional security perimeters.
- **Ransomware and data extortion remain pervasive across industries**, with utilities, media, and CRM users among recent victims.
- **Misconfigured systems and human error continue to drive data exposure**, including internal mishandling of sensitive government and institutional records.
- **Financial and healthcare sectors are facing sustained pressure**, as both banking malware and critical service disruptions hit targets in multiple regions.

Outlook:

The cyber threat landscape this week underscores an accelerating convergence between trusted technologies and attacker operations. AI platforms, CRM systems, developer tools, and national infrastructure components are all being abused as delivery vectors or entry points—exploiting user trust, inadequate controls, and insecure defaults. While ransomware and data extortion continue to dominate breach disclosures, we're seeing a parallel rise in stealthy operations that blend hardware access, social engineering, and creative malware staging. The expanding attack surface across industries, particularly utilities, finance, telecom, and healthcare, calls for more proactive threat modeling and scenario testing, especially in environments where AI, cloud tools, and user-installed extensions are prevalent.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

2,120% [CVE-2025-34300](#)

- A template injection vulnerability exists in Sawtooth Software's Lighthouse Studio versions prior to 9.16.14 via the `ciwwweb.pl` `http://ciwwweb.pl/` Perl web application. Exploitation allows an unauthenticated attacker to execute arbitrary commands.

635% [CVE-2024-10924](#)

- The Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress are vulnerable to authentication bypass in versions 9.0.0 to 9.1.1.1. This is due to improper user check error handling in the two-factor REST API actions with the `'check_login_and_get_user'` function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, when the "Two-Factor Authentication" setting is enabled (disabled by default).

113% [CVE-2025-47812](#)

- In Wing FTP Server before 7.4.4, the user and admin web interfaces mishandle `'\0'` bytes, ultimately allowing injection of arbitrary Lua code into user session files. This can be used to execute arbitrary system commands with the privileges of the FTP service (root or SYSTEM by default). This is thus a remote code execution vulnerability that guarantees a total server compromise. This is also exploitable via anonymous FTP accounts.

US Computing Site Hit by 3.3 Million RPS DDoS Attack

+US +Computing +DDoS

- A U.S.-based computing site was hit with a 3.3 million RPS application-layer DDoS attack in late July, ramping to full intensity within just nine minutes—a sign of a highly coordinated botnet. Notably, its parent company was also targeted three hours earlier with a 1.6 million RPS assault, suggesting a deliberate campaign aimed at disrupting the broader organization's digital infrastructure. The back-to-back nature of the attacks may indicate strategic targeting of shared services or infrastructure dependencies.

Recent Cyber Threats

Silent Execution via Gemini CLI Exploit

+AI +Google

- A critical flaw in Google's [Gemini CLI](#) AI coding assistant allowed attackers to execute malicious code on users' systems without their knowledge. The issue stemmed from the way Gemini fetched and executed AI-generated suggestions, which could be manipulated to include unauthorized code execution through model-generated paths. Google has since patched the flaw, which raised concerns about the broader risks of integrating AI directly into development workflows.

Malicious Mouse Config Tool Delivered Backdoor

+Houdini +Germany

- The [Endgame Gear XM1](#) mouse configuration tool was found to be infected with a malicious update that installed the Houdini RAT and additional malware on users' devices. The compromised software was hosted on the official vendor site and appears to have been tampered with in May 2024, potentially affecting hundreds of users before being taken down. German authorities and CERTs are investigating, but the attackers remain unidentified.

Cobalt Strike Campaigns Masquerade on Quora and GitHub

+Cobalt Strike

- A new campaign abuses legitimate platforms like Quora, GitHub, and Pastebin to deliver [Cobalt Strike](#) beacons, relying on social engineering and obfuscation to evade detection. Victims are lured through fake developer tools or job opportunities, leading to staged infections using compromised cloud storage and developer resources. The approach highlights how attackers continue to weaponize trusted platforms in creative ways to distribute advanced payloads.

Hidden Pi Breach in ATM Network

+LightBasin +Raspberry Pi

- A stealthy backdoor was implanted via a 4G-enabled Raspberry Pi physically connected to a bank's ATM network switch, allowing [LightBasin](#) (also known as UNC2891) to bypass firewalls and gain remote access to internal systems. Using anti-forensics and covert lateral movement, the device provided persistent ingress for long-term surveillance or fraud. The campaign highlights rising sophistication in physical-cyber attacks targeting ATM infrastructures.

Typosquat Phishing Hits Python Developers

+Typosquatting +PyPI

- The Python Software Foundation (PSF) flagged a credential-harvesting campaign targeting Python developers via phishing with a fake PyPI domain (PyPJ[.]org). By impersonating email verification requests, attackers tricked developers into submitting login credentials, risking tainting legit package uploads with malware. PSF responded with warnings on the real platform and cooperation with registrars to shut down phishing domains.

Man-in-the-Prompt: Extension Hijacks AI Sessions

+MITM +Man in the Prompt +AI

- A new attack vector, dubbed [Man in the Prompt](#), leverages malicious or compromised browser extensions to intercept or modify user input and responses within AI tools like ChatGPT and Gemini. These extensions read or inject hidden instructions into the DOM, enabling data exfiltration or unauthorized command injection during AI interactions without user awareness.

DoubleTrouble Variant Spreads via Discord

+DoubleTrouble +Financial Services

- The Android banking trojan [DoubleTrouble](#) has evolved its distribution, using Discord-hosted APKs under false Play-store branding to trick victims into installing malware. Once active, it requests Accessibility permissions, enabling screen recording, advanced keylogging, and overlay UI theft from banking and crypto apps.

Data Breaches

Utility Leak Exposes SSNs via BlackSuit

+US +Utilities +BlackSuit

- [Massachusetts Municipal Wholesale Electric](#) Company (MMWEC) revealed a January 2025 ransomware breach impacting at least 514 individuals. Personal data exposed includes Social Security numbers, taxpayer IDs, and financial account information. The BlackSuit gang claimed responsibility and published MMWEC on its leak site.

GLOBAL GROUP Hits Albavisión, 400 GB Stolen

+US +Media +GLOBAL GROUP

- The nascent [GLOBAL GROUP](#) ransomware operation breached Albavisión, the Miami-based media conglomerate, stealing an alleged 400 GB of data. The group issued a 15-day deadline to negotiate before threatening publication of the stolen files.

Offshore Banks in Seychelles Targeted in Cyber Extortion

+Seychelles

- [Seychelles Commercial Bank](#) confirmed a cybersecurity incident revealing personal banking data of internet-banking clients, including emails, phone numbers and balances—but no funds were withdrawn. This reflects a growing trend of attacks focused on offshore banking platforms for espionage or extortion.

Russian Pharmacy Chains Paralyzed by Cyberattack

+Russia +Healthcare

- A coordinated cyberattack knocked offline IT systems at [major Russian pharmacy chains](#) Stolichki and Neopharm, disrupting cash registers, inventory, and medication reservations across hundreds of outlets. Healthcare access was significantly affected and employees sent home pending restoration over one to two days.

CRM Vishing Breach Taps ShinyHunters in Salesforce Attacks

+ShinyHunters +CRM +Vishing

- A coordinated wave of breaches against major Salesforce CRM customers has been linked to [ShinyHunters](#) (a.k.a. UNC6040) using voice-phishing (vishing). Attackers impersonated internal IT support and tricked employees into installing a rogue OAuth app (My Ticket Portal) via Salesforce Data Loader. The malicious app allowed the theft of Accounts and Contacts data before extortion demands followed.

Everglades Prison Email Misstep Exposes Visitor Details

+US +Government

- At [Everglades Correctional Institution](#) in Florida, a staff email inadvertently sent personal contact details (names, emails, phone numbers) of approved visitors to all inmates via the prison's internal email system. The information was thus accessible by potentially dangerous prisoners through kiosks or secure tablets, prompting fears of targeted extortion or threats. Affected individuals report no official notification or corrective action from the Department of Corrections.

Cyberattack Knocks Out Luxembourg Telecom via Huawei Gear

+Luxembourg +China +Telecommunications

- Luxembourg suffered a deliberate cyberattack that targeted [Huawei](#) enterprise routers in its national mobile infrastructure, causing a 4G/5G outage for over three hours and hampering internet, mobile banking, and emergency services when fallback 2G overloaded. Government investigations stressed the intentional nature of the assault and urged exposure notifications for any entity using Huawei routers. The incident represents a rare westward strike on Chinese telecom infrastructure in Europe.

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.