

IMPERVA THREAT RESEARCH

Threat Intel Report: September 29-October 5, 2025

Countries



Top Tags

Crimson Collective

Medusa

MatricPDF

IoT

Malware

Executive Summary

Actionable Information:

- **Ransomware & Data Theft:** Threat actors are increasingly targeting sensitive corporate and operational data for exfiltration and extortion, moving beyond simple encryption to maximize financial and reputational impact.
- **Supply Chain & Vendor Risk:** Breaches continue to exploit third-party and vendor ecosystems, highlighting the importance of auditing, monitoring, and segmenting external partners.
- **Exploitation of Platforms & Software:** Unpatched systems, misconfigurations, and legacy infrastructure remain key avenues for attackers to access critical networks and sensitive data.
- **Phishing & Malware Evolution:** Attackers are leveraging legitimate platforms, applications, and document formats to deliver malware and conduct phishing campaigns while evading traditional detection methods.
- **Data Privacy & IoT Exposure:** Gaps in data isolation, encryption, and privacy controls in both enterprise software and consumer IoT devices are creating opportunities for unauthorized access and tracking.
- **Operational Disruption:** Beyond data loss, cyberattacks are increasingly causing measurable disruptions to operations and service availability, affecting business continuity.

Outlook:

This week's activity underscores a widening attack landscape that blends traditional data extortion with emerging abuse of legitimate platforms. Ad networks, cloud analytics tools, and consumer IoT devices are all proving attractive vectors for cybercriminals seeking scale, stealth, and persistence. The ongoing targeting of telecom, government, and aviation entities reinforces that trusted infrastructure providers remain prime entry points for both financially motivated and opportunistic attackers. Over the coming months, expect more

hybrid attacks combining social engineering with supply chain compromise, as threat groups diversify methods to circumvent stronger perimeter defenses and exploit weaknesses in trust-based systems.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 397% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

↑ 354% [CVE-2024-12987](#)

- A vulnerability, which was classified as critical, was found in DrayTek Vigor2960 and Vigor300B 1.5.1.4. Affected is an unknown function of the file `/cgi-bin/mainfunction.cgi/apmcfgupload` of the component Web Management Interface. The manipulation of the argument session leads to os command injection. It is possible to launch the attack remotely.

↑ 150% [CVE-2025-10035](#)

- A deserialization vulnerability in the License Servlet of Fortra's GoAnywhere MFT allows an actor with a validly forged license response signature to deserialize an arbitrary actor-controlled object, possibly leading to command injection.

Global Brute-Force Campaign Targets German Telecom Provider

+Germany +Telecommunications

- A German telecommunications company was targeted by account takeover attacks in a five-day onslaught, averaging 25 million login attempts per day. The attacks came from over 50 countries, and were almost entirely brute-force in nature.

Recent Cyber Threats

Hijacked Ads Push Malware via Phony TradingView Offers

+Malware +Trojan

- Researchers warn of an evolving campaign in which malicious actors use hijacked Google Ads and YouTube channels to promote [fake "TradingView Premium"](#) offers. The operators commandeer verified accounts, clone the real branding, and push unlisted videos that lure victims into downloading a spyware Trojan (Trojan.Agent.GOSL). The expansion from Facebook into Google and YouTube increased reach dramatically, exposing more users to credential theft, personal data and crypto wallet compromise.

Unencrypted Tile Broadcasts Expose Users to Persistent Tracking

+IoT

- Researchers have discovered that [Tile tracking tags](#) broadcast unencrypted MAC addresses and device IDs, allowing observers or malicious parties in range to trace a user's movement over time. The system also uploads unmasked identifiers to Tile servers in plaintext, giving Tile (or third parties) visibility into location data despite claims otherwise. Weaknesses in the anti-stalking and anti-theft features further allow attackers to spoof or replay broadcasts, potentially framing others or evading detection.

MatrixPDF Tool Transforms PDFs Into Stealth Phishing & Malware Vectors

+Phishing +Malware +MatrixPDF

- A new toolkit called [MatrixPDF](#) has been discovered that enables attackers to embed obfuscated overlays, JavaScript actions, and fake prompts into otherwise benign PDF files. The malicious features only trigger when a user clicks, helping evade static email scanners and bypass Gmail filters. The builder is sold to threat actors via cybercrime forums and Telegram, potentially lowering the bar for advanced phishing campaigns.

Adobe Analytics Bug Causes Cross-Tenant Data Leakage

+Software

- A deployment mistake in [Adobe Analytics](#) introduced a bug on September 17 that caused customer tracking data to bleed into other tenants' analytics environments. The issue persisted until September 18 and affected approximately 3–5% of data. Adobe assures no malicious intent, but clients are instructed to purge impacted datasets (including backups and downstream systems) to avoid retention of others' sensitive fields.

Data Breaches

Comcast Held for Ransom With 834 GB Data at Stake

+Medusa +Telecommunications

- The Medusa ransomware group claims to have breached [Comcast's](#) internal systems, exfiltrating ~834 GB of data and publishing screenshots and file listings to support its demands. It is asking for \$1.2 million to either delete or release the stolen data. The exposed file paths suggest access to actuarial, financial modeling, and product-management datasets, raising sensitive business and regulatory risks.

Cyber Attack Silences Asahi's Distribution Systems

+Japan +Food & Beverage

- Japan's [Asahi Group](#) reported a system failure triggered by a cyberattack which forced shutdowns of its distribution networks and call centers. The company says no customer or commercial data appears to have been stolen so far, but operations within Japan remain severely disrupted with no timeline for full recovery. Given Asahi's scale in domestic markets, the blackout of internal systems likely inflicts material revenue and reputational damage.

Citrix Breach Leaks FEMA & CBP Employee Data

+US +Government

- A breach originating from an exploited Citrix vulnerability enabled attackers to access [FEMA](#) servers (Region 6) and exfiltrate employee data, including those tied to U.S. Customs and Border Protection. The compromise, traced back to June, triggered terminations of IT staff at FEMA and forced remedial changes to Zscaler policies and access controls. The event underscores how legacy infrastructure and weak segmentation can amplify impact in federal environments.

WestJet Breach Exposes Passports of 1.2M Travelers

+Aviation

- [WestJet](#) confirmed that a cyberattack in June compromised personal data of ~1.2 million customers, including passports, government IDs, names, dates of birth, and travel histories. The intrusion was executed via a social engineering attack to reset an employee's password and access the network through Citrix. Although credit card and password data were not exposed, the breach poses high identity theft and regulatory risk given the sensitivity of the data.

Red Hat Consulting GitLab Instance Hit, Internal Data Stolen

+Crimson Collective

- [Red Hat](#) confirmed that a third-party GitLab instance used by its consulting arm was breached by the group "Crimson Collective," who claim to have stolen ~570 GB of compressed data across 28,000 private repositories. The theft reportedly included source code, credentials, configurations, internal communications, and customer engagement reports. While Red Hat says their main services and open source supply chains remain unaffected, up to 800 Red Hat customers—including major enterprises and U.S. government agencies—may have had data involved.

Third-Party Breach Impacts Renault UK Customer Records

+Automotive +UK

- [Renault U.K.](#) disclosed that a breach of a third-party supplier exposed personal data of its customers, including details like contact and vehicle information. The automaker urged affected customers to remain vigilant and updated, stating that the compromised data did not include payment card or highly sensitive financial details. The incident emphasizes the risks posed by vendor ecosystems and the importance of third-party security oversight.

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.