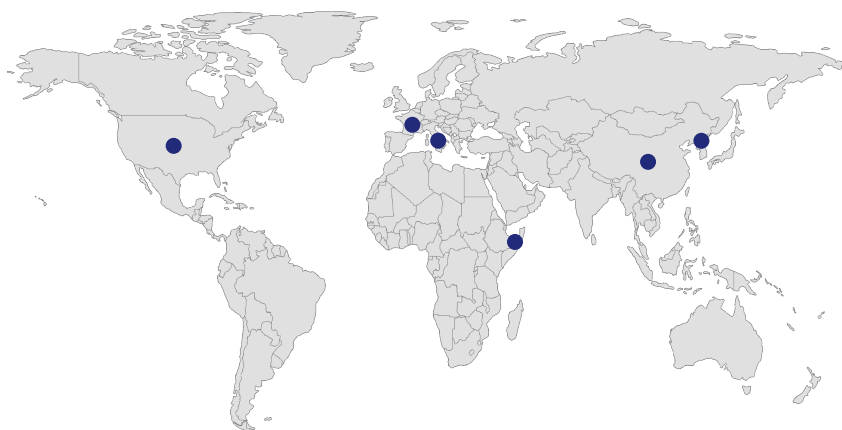


IMPERVA THREAT RESEARCH

Threat Intel Report: November 10-16, 2025

Countries



Top Tags

Whisper Leak

KONNI

Phishing

CI0p

Government

Executive Summary

Actionable Information:

- **AI is now a fully operational attack enabler:** Threat actors are using AI systems for autonomous reconnaissance and exploitation, while new side-channels show that even encrypted interactions with AI services can leak sensitive information.
- **Supply-chain and platform abuse is escalating:** Attackers increasingly compromise software ecosystems, service providers, and platform features to impact thousands of downstream users at once.
- **Identity compromise remains the most reliable entry point:** Social engineering, phishing at scale, and abuse of legitimate administrative tools continue to be key drivers of breaches across sectors.
- **Critical infrastructure and government systems are high-value targets:** Weakly protected national systems, telecom/energy providers, and public-sector platforms remain vulnerable to data exposure and operational disruption.
- **Zero-day exploitation fuels high-impact data theft:** Attackers continue to weaponize enterprise application flaws to access sensitive financial, personal, and operational data.

Outlook:

This week's activity reinforces a maturing threat landscape where automation, supply-chain leverage, and identity compromise converge to produce higher-impact intrusions. As AI becomes both an attack vector and a force multiplier, defenders should expect faster, more adaptive campaigns requiring real-time monitoring and traffic analysis. Supply-chain compromises and platform-level abuse suggest that even well-secured organizations can be exposed through trusted services, making third-party risk a persistent priority. Critical infrastructure and government entities will likely face sustained pressure as attackers pursue targets with broad systemic value. Looking forward, organizations should prepare for increasingly automated, multi-stage intrusions, where preventing credential compromise, auditing service dependencies, and hardening enterprise applications will be the most effective defenses.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 498% [CVE-2024-7399](#)

- Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1050 allows attackers to write arbitrary file as system authority.

↑ 280% [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.

↑ 140% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via `completePath` in the `ProcessUtilities.outputExecutioner()` sink. There is `/filemanager/upload` (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.

Application-Layer DDoS Hits US Food & Beverage Site

+US +Food & Beverage +DDoS

- A US-based food and beverage company faced a sustained application-layer DDoS attack this week, peaking at 2.4 million requests per second over a 23-hour period. The prolonged volume indicates a highly coordinated effort aimed at overwhelming site functionality and disrupting services.

US Telecom Targeted by Large-Scale Account Takeover

+US +Telecommunications +ATO

- A US telecommunications site experienced a major account takeover campaign this week, peaking at 5.2 million login attempts in a single day. The brute-force activity was driven entirely by Apple-based automated clients originating from US IPs, indicating a coordinated, high-volume credential-testing effort.

Recent Cyber Threats

AI-Agent Led Espionage Campaign Disrupted

+AI +China

- Anthropic detected in mid-September 2025 an espionage campaign in which a China-linked actor abused its [Claude AI](#) system not just as a support tool but as an autonomous attacker agent. The campaign hit large tech companies, financial institutions and government agencies globally, executing reconnaissance, exploitation and lateral movement with minimal human oversight.

Whisper Leak: Encrypted AI Chats Exposed

+Whisper Leak +Side-channel +AI

- Researchers revealed a novel side-channel attack dubbed [Whisper Leak](#) where an adversary monitoring encrypted traffic to remote language models can infer the topics of the conversations (such as political dissent, money laundering) by analyzing packet sizes/timings, even though TLS encryption is present. This means clients of streaming AI services may still have sensitive prompts exposed indirectly.

North Korean Spies Redirect Google Tool to Erase Evidence

+North Korea +KONNI

- North Korean state-supported [KONNI](#) attackers hijacked Google Find My Device (Find Hub) features to remotely factory-reset Android phones of South Korean targets, essentially using it as a cover for data-wiping and cleanup after prior intrusions. The campaign shows how mobile device management tools can be weaponized to erase traces and hamper forensic recovery.

Italian Web-Host Customers Phished at Scale

+Italy +Phishing

- A large-scale [phishing campaign](#) targeted customers of one of Italy's largest webhosting/IT providers, impersonating service-expiry/payment notifications to harvest login credentials and payment information. The provider serves over 5.4 million customers, making the potential exposure broad and enabling downstream fraud or access to customer websites.

Phishing via Meta Business Suite Platform

+Phishing

- Researchers uncovered a mass phishing campaign exploiting the [Meta Business Suite](#) invitation feature to send over 40,000 phishing emails to more than 5,000 organizations in North America, Europe and the Asia-Pacific. The attackers created fake Facebook Business pages and used the legitimate facebookmail[.]com domain to send invitations that redirect victims to credential-harvesting sites, bypassing many security filters.

Logic Bombs Hidden in Supply-Chain NuGet Packages

+NuGet +ICS

- Threat researchers identified nine malicious [NuGet packages](#), downloaded nearly 9,500 times, that embed time-delayed "logic bombs" set to trigger in August 2027 or November 2028, sabotaging database operations and industrial-control systems. This illustrates how attackers are weaponizing developer-ecosystems to insert latent threats that may lie dormant for years before activation.

Data Breaches

Nevada State Hit by Ransomware After Employee Download

+US +Government

- In August 2025 the state of [Nevada](#) suffered a ransomware attack that was traced back to a May incident in which a state employee inadvertently downloaded a malware-laced system-administration tool from a spoofed site. The attackers encrypted state systems and issued a ransom note, but the state refused to pay and managed to recover about 90 % of affected data over a 28-day recovery period with the help of insurance and pre-arranged vendor support.

DoorDash Employee Social-Engineering Leads to Data Breach

+Food & Beverage +Social Engineering

- [DoorDash](#) disclosed a breach from October 25, 2025 in which an attacker gained access by tricking an employee via social engineering, then exfiltrated names, emails, physical addresses and phone numbers of customers, delivery workers and merchants. The company has not publicly disclosed the full number affected and asserts that financial credentials or SSNs were not accessed.

The Washington Post Payroll Data of Nearly 10K Staff Exposed

+US +News

- [The Washington Post](#) confirmed that personal and financial information (including Social Security numbers, bank account and routing numbers) of about 9,720 current and former employees and contractors was exposed after attackers exploited a zero-day in Oracle E-Business Suite and exfiltrated data between July and August 2025. The incident highlights how media organizations are vulnerable to enterprise-application exploits and extortion-style data theft.

Logitech Confirms Breach Following CI0p Claim

+CI0p

- [Logitech](#) revealed via an SEC filing that hackers claimed to have stolen data after exploiting a vulnerability in a third-party software platform; the breach was listed on the CI0p gang's leak site and likely tied to the Oracle EBS zero-day campaign. The company said its business operations and products were unaffected, but the incident underscores risk to hardware/tech suppliers of enterprise-application exploits.

Eurofiber France Supply-Chain Breached, Thousands of Clients Affected

+France +Government +Energy +Telecommunications

- [Eurofiber France](#) disclosed a breach discovered November 13, 2025 in which the attacker exploited a vulnerability in its ticket-management and customer-portal systems, and claims surfaced that data of over 3,600 clients (including government, energy, telecoms) might be exposed. The incident is notable as a major compromise of a vendor servicing critical infrastructure, raising systemic supply-chain risk.

Somalia E-Visa Platform Breach Exposes Travel Applicants' Data

+Somalia +Government +Travel

- A breach in [Somalia's](#) electronic-visa system reportedly exposed personal details (names, photos, DOBs, addresses) of at least 35,000 applicants, prompting warnings from U.S. and U.K. authorities due to aviation and migration-security implications. The event highlights risk to national immigration/visa systems in weaker-security jurisdictions.

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.