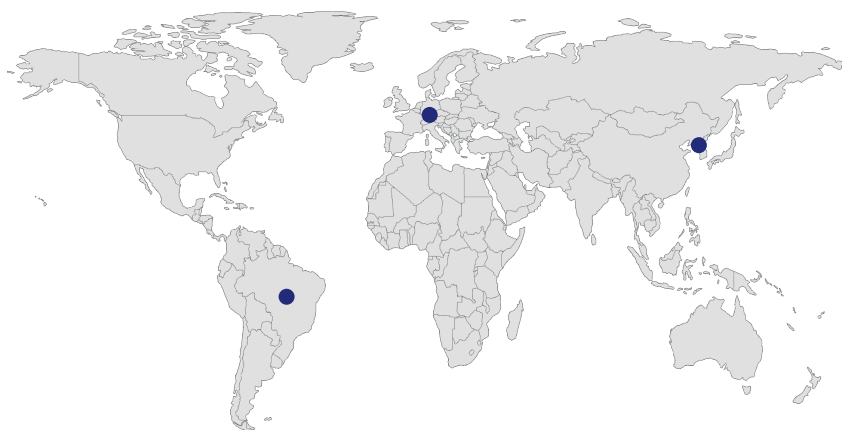


IMPERVA THREAT RESEARCH

Threat Intel Report: October 6-12, 2025

Countries



Top Tags

Malvertising

RondoDox

Qilin

Payouts King

Medusa

Executive Summary

Actionable Information:

- **Automation & Scale:** Several campaigns, including RondoDox and the German telecom brute-force attack, demonstrate the use of automated tools to launch high-volume attacks, targeting IoT devices, user accounts, and enterprise login systems. Organizations should review rate-limiting, MFA, and anomaly detection to mitigate automated threats.
- **Enterprise & ERP Exploits:** Zero-day attacks on Oracle EBS show that ERP and enterprise software remain prime targets for data exfiltration. Timely patching, monitoring of unusual process behavior, and web shell detection are critical.
- **Ransomware & Repeat Attacks:** Ransomware groups like Chaos C, Qilin, Medusa, and Payouts King continue to hit diverse sectors, often following up with repeated attacks if remediation is incomplete. Backups, segmentation, and incident response readiness are essential.
- **Supply Chain & Third-Party Risks:** Breaches affecting Discord support vendors and BK Technologies highlight the continued risk posed by third-party service providers. Vendor risk assessments and least-privilege access are key mitigations.
- **Emerging Attack Vectors:** New trends such as prompt injection targeting AI systems, WhatsApp-propagating malware, and large-scale malvertising campaigns show attackers are exploiting novel technologies and communication platforms. Organizations leveraging AI or social platforms should implement input validation, monitoring, and user awareness training.
- **Identity & Credential Risk:** Credential stuffing and insider-facilitated account compromise remain prevalent, emphasizing the need for strong authentication practices, continuous monitoring, and robust access control.

Outlook:

The current trajectory suggests that attackers will continue blending automated, high-volume campaigns with highly targeted, high-value exploits. The expansion of ransomware tactics, repeated attacks on under-protected systems, and emerging vectors like AI and messaging

platforms point to an increasingly diverse threat surface. Organizations should expect continued pressure on identity systems, third-party vendors, and critical enterprise applications. Proactive defenses—including rapid patching, strong authentication, monitoring of unusual activity, and regular simulation of incident response—will be essential to reducing risk as threat actors leverage both scale and precision in their campaigns.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 7,620% [CVE-2024-50603](#)

- An issue was discovered in Aviatrix Controller before 7.1.4191 and 7.2.x before 7.2.4996. Due to the improper neutralization of special elements used in an OS command, an unauthenticated attacker is able to execute arbitrary code. Shell metacharacters can be sent to /v1/api in cloud_type for list_flightpath_destination_instances, or src_cloud_type for flightpath_connection_test.

 1,005% [CVE-2024-27956](#)

- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Automatic allows SQL Injection. This issue affects Automatic: from n/a through 3.92.0.

 424% [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.

German Telecom Faces Massive Account Takeover Attempt

+Germany +Telecommunications

- A German telecommunications site was targeted by account takeover this week, reaching almost 6 million brute-force login attempts in one day. The campaign targeted customer accounts in an effort to gain unauthorized access, likely using automated credential-stuffing tools.

Recent Cyber Threats

Stealthy Ad Scripts in WordPress Themes

+WordPress +Malvertising

- A global malvertising campaign is injecting PHP into [WordPress theme files](#), fetching external JavaScript that inserts hidden iframes or redirects users to malicious payloads. The injected code mimics Cloudflare challenge paths to evade detection, and at least 17 sites have been linked to attacker infrastructure.

WhatsApp Worm Spreads Banking Malware in Brazil

+SORVEPOTEL +Malware +WhatsApp +Brazil

- A malware strain dubbed [SORVEPOTEL](#) is spreading via WhatsApp by automatically sending malicious ZIP attachments to contacts and groups. Once executed on a Windows system, it runs shellcode, steals data, and continues propagating. The campaign is primarily focused on Brazilian users, leveraging social engineering to boost infection rates.

Oracle EBS Zero-Day Exploited for Data Exfiltration

+CVE

- Attackers are exploiting [CVE-2025-61882](#), an unauthenticated RCE in Oracle E-Business Suite, to deploy web shells and exfiltrate sensitive business data. The threat activity began months before public disclosure, suggesting targeted and opportunistic campaigns against enterprise ERP environments.

Chaos C Ransomware Encrypts Windows Systems

+Chaos C

- A ransomware family named “[Chaos C](#)” is encrypting Windows files and appending a .chaosc extension. Victims receive ransom notes demanding payment for decryption keys. The campaign appears to target a broad range of systems globally, with no single industry focus.

RondoDox Botnet Launches Exploit Shotgun Attacks

+RondoDox

- A botnet dubbed [RondoDox](#) is exploiting 56 disclosed vulnerabilities across DVRs, routers, web servers, and other connected devices. The campaign fires multiple exploit attempts in parallel to maximize infections, showing rapid expansion since mid-year.

Prompt Injection Attacks Target AI Interfaces

+AI +Prompt Injection

- Attackers are abusing prompt injection to manipulate [AI systems](#), forcing models to reveal data or execute unintended actions. These attacks exploit weak input validation and are affecting AI-driven tools across multiple sectors.

North Korean Insider Steals Okta Credentials

+North Korea

- A North Korean IT worker infiltrated global organizations through [Okta](#) infrastructure to steal credentials and access sensitive accounts. The campaign highlights how insider access can be weaponized to compromise identity systems at scale.

Data Breaches

Support Ticket Breach Exposes Discord User Data

+Gaming

- Hackers compromised a third-party customer support vendor used by [Discord](#), stealing support tickets, user names, email addresses, partial payment data, IP addresses, and some government ID images. The breach did **not** directly affect Discord’s core systems, but only users who had interacted with support or age-verification processes. Discord revoked vendor access and is notifying affected users.

Qilin Ransomware Hits Virginia School District

+Education +Qilin

- The Qilin gang infiltrated [Mecklenburg County Public Schools’](#) systems, reportedly encrypting files and claiming to have exfiltrated student and financial records. The school district has declined to pay a ransom while investigating the scope of damage and potential data losses.

171K Patients Affected in Radiology Practice Breach

+Healthcare

- A Florida-based radiology provider, [Doctors Imaging Group](#), revealed that its network was compromised in November 2024 and that attackers copied files containing names, social security numbers, medical and financial data. The firm is still determining exactly what was taken and notifying over 171,000 impacted individuals.

Credential Stuffing Impacts DraftKings Accounts

+Gambling

- [DraftKings](#) reported that fewer than 30 customer accounts were accessed via credential stuffing attacks using credentials obtained elsewhere. The attackers did not breach DraftKings’ internal systems. No financial losses have been confirmed so far, but users are urged to reset passwords and enable multifactor authentication.

Cyber Intrusion Hits Radio Maker for Emergency Services

+Communications

- [BK Technologies](#), a supplier of communications gear for police, fire, and military, acknowledged a cyber break-in performed in September 2025 that impacted internal IT systems. The attacker accessed employee data (past and present) before being ejected. The firm claims operations were not disrupted.

Culinary Institute Hit by SSN-Leak Data Breach

+Payouts King +Education

- The [Institute of Culinary Education](#) disclosed that about 33,342 individuals had their names, SSNs, birth dates, driver's license numbers, and other PII exposed in a breach from May 2025. The ransomware group "Payouts King" claims to have stolen 1.5 TB of data and listed the institute on its leak site.

Medusa Ransoms Distributor Twice in 2025

+Medusa

- [Strategic Retail Partners \(SRP\)](#) was breached in February 2025 by Medusa, who exfiltrated 1.35 TB of data and demanded \$1.2 million. When SRP did not sufficiently remediate, Medusa hit them again in March, issuing a second ransom demand.

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.