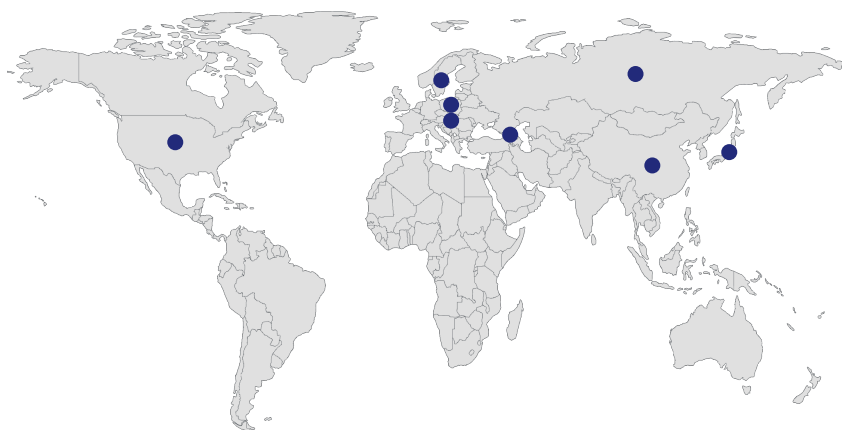


IMPERVA THREAT RESEARCH

Threat Intel Report: November 3-9, 2025

Countries



Top Tags

Airstalk

Cavalry Werewolves

Curly COMrades

NGate

Akira

Executive Summary

Actionable Information:

- **Supply-chain & developer ecosystem risk is high:** Threat actors are increasingly targeting the software development and distribution pipeline, embedding malicious code or exploiting trusted tools to gain downstream access. Organizations should prioritize code integrity checks, dependency monitoring, and continuous assessment of third-party development platforms.
- **EDR evasion via virtualization is growing:** Adversaries are leveraging virtual environments and containerized workloads to hide persistence mechanisms and evade endpoint detection. Enhanced visibility into virtual infrastructure and behavioral analytics around system isolation tools are becoming essential.
- **Geopolitical sabotage vs. crime differentiation:** Nation-state operations and financially motivated groups continue to diverge in tactics, with the former favoring destructive or espionage-driven campaigns and the latter focusing on data theft and monetization. Maintaining geopolitical threat awareness and robust incident containment processes is critical.
- **Consumer and public-sector data exposure continues at scale:** Large-scale breaches across industries show persistent weaknesses in vendor security and data handling practices. Strengthening third-party risk management, data minimization, and breach response readiness remains a top priority.
- **Financial theft via novel vectors:** Attackers are diversifying their monetization methods, from exploiting digital payment systems to abusing emerging technologies like decentralized finance. Financial and fintech organizations should enhance transaction monitoring, anomaly detection, and customer verification safeguards.
- **Collaboration trust erosion:** Vulnerabilities and misuse of communication platforms are enabling impersonation and fraud within trusted environments. Stronger user awareness, verification protocols, and secure communication policies are needed to preserve organizational trust.

Outlook:

Expect continued pressure on the software supply chain and enterprise tooling, with attackers favoring low-friction entry via developer environments, MDM interfaces, and official app marketplaces rather than perimeter exploits. Operational security evasion will lean on virtualization, living-off-the-land services, and collaboration platforms to blend into normal workflows. In parallel, state-aligned actors are likely to intensify destructive or disruptive operations tied to geopolitical objectives, while financially motivated groups probe contactless payment/ATM and DeFi edge cases for rapid monetization. Organizations that combine strong third-party governance, developer environment hardening, hypervisor visibility, and resilient recovery (tested backups + rapid comms) will be best positioned to absorb this blend of espionage, disruption, and fraud in the weeks ahead.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 138,730% [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.

↑ 1,050% [CVE-2024-53675](#)

- An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.

↑ 525% [CVE-2024-9463](#)

- An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.

Recent Cyber Threats

Airstalk Supply Chain Spyware Uncovered

+Airstalk

- Researchers discovered a new malware family, [Airstalk](#), used in a likely supply-chain attack to compromise enterprise environments. Airstalk abuses the AirWatch/Workspace ONE MDM API to create a covert command-and-control channel, harvesting browser cookies, history, bookmarks, and screenshots from compromised systems. The attack is believed to primarily target business-process-outsourcing (BPO) firms, enabling the attacker to gain access across multiple downstream client networks.

Phishing-Led Campaign Against Russian Institutions

+Cavalry Werewolf +Russia +Kyrgyzstan

- Between May and August 2025 the [Cavalry Werewolf](#) cluster ran a focused cyber-espionage campaign against Russian state agencies and critical-industry firms, using highly targeted spear-phishing emails that impersonated Kyrgyz government ministries (and in at least one case used a legitimately compromised government account). Victims received password-protected RAR attachments that deployed two bespoke toolsets which provide remote command execution, file upload/download and data

exfiltration (often via Telegram bots). Researchers observed customized filenames mimicking official documents, multi-language tool variants, and additional utilities such as reverse SOCKS agents, indicating a well-resourced operator focused on intelligence collection rather than commodity crime.

Hyper-V Virtualization Abuse by Russian Hackers

+Curly COMrades +Russia +Georgia

- The Russian-linked [Curly COMrades](#) group has been abusing Microsoft Hyper-V virtualization in Windows to install lightweight Alpine Linux VMs that host malware, thus evading traditional endpoint detection. In one campaign they targeted Georgian government/judiciary and Moldovan energy firms, deploying implants named CurlyShell and CurlCat for remote access. By tunneling malicious network traffic through the VM and default switch, they masked network origin and bypassed normal defenses.

NGate NFC Relay Attack Drains Polish ATMs

+Ngate +Poland

- A new malware campaign named [NGate](#) uses an Android-based NFC relay approach to let attackers withdraw cash from ATMs in Poland without physically taking victims' cards. The attackers leverage social engineering to get the victim's phone near an NFC-enabled ATM and then relay the transaction remotely. The technique allows cash to be stolen covertly from bank customers' accounts.

AI-Generated VS Code Extension Sneaks in Ransomware

+AI +Code Extension

- A malicious extension called [susvsex](#) was published on Microsoft's official VS Code marketplace, claiming in its description to "automatically zip, upload, and encrypt files" from a user's system. The extension was apparently created using AI ("vibe-coded"), used GitHub for command-and-control, and was downloaded by developers before being removed. The incident raises concerns about how development platforms and marketplaces can be used for malicious distribution to the developer community.

Destructive Wiper Campaign Hits Ukraine's Grain Exports

+Sandworm +Russia +Ukraine

- [Sandworm](#) has deployed multiple data-wiping malware strains (ZEROLOT and Sting) since June-September 2025 across Ukraine's grain, energy, logistics, and government sectors, aiming to undermine the country's export infrastructure and wartime economy. The destructive attacks followed initial intrusions by another actor, UAC-0099, then handed off to Sandworm for execution. Using wipers instead of ransomware signals strategic disruption rather than financial extortion.

Developer Toolchain Exposed via CLI Flaw

+npm

- A critical vulnerability ([CVE-2025-11953](#), CVSS 9.8) in the widely used npm package "@react-native-community/cli" allows unauthenticated remote attackers to send specially crafted POST requests to the included Metro development server, which by default binds to all network interfaces, and thereby execute arbitrary OS commands on developer machines. The flaw affects versions 4.8.0 through 20.0.0-alpha.2 and has been patched in version 20.0.0. Because this CLI tool is downloaded millions of times weekly, development environments worldwide may have been exposed.

Collaboration Platform Messaging Flaws Enable Executive Impersonation

+Technology +Business

- Researchers uncovered four critical vulnerabilities in [Microsoft Teams](#) that allow attackers to edit message content without triggering the "edited" label, spoof notifications to appear from trusted contacts, change display names in chats, and even forge identities in audio/video calls. These flaws undermine trust in corporate communications and open a path for phishing, business email compromise, and fraud. All identified issues were patched by Microsoft in October 2025.

Data Breaches

Hungarian Party App Data Spill

+Hungary +Government

- The political party [TISZA Világ](#) in Hungary suffered a breach in late October 2025, exposing roughly 200,000 records including names, email addresses, phone numbers, and physical addresses via their app. The leak raises concerns about political privacy and possible foreign influence given allegations of Russian or Chinese involvement.

Congressional Budget Office Cyber Intrusion

+US +China +Government

- The [U.S. Congressional Budget Office \(CBO\)](#) confirmed a cybersecurity incident in November 2025 that may have exposed internal communications, emails, and chat logs between the CBO and congressional offices. Although the agency hasn't confirmed the attacker's identity, U.S. officials and media reports point to a likely foreign actor, possibly China. The compromise could enable highly targeted phishing and manipulation of legislative policy processes.

Hyundai AutoEver America Sensitive Data Breach

+Automotive +US

- The IT services arm of [Hyundai AutoEver America](#) discovered an intrusion dating to February 2025 that allowed access to names, Social Security numbers, and driver's license information for up to 2.7 million individuals. The breach increases identity theft risk for customers and highlights vulnerabilities in the automotive sector's IT infrastructure.

Nikkei Slack Account Compromise Impacts 17K

+Japan +Media

- Japanese media conglomerate [Nikkei Inc.](#) reported that in September 2025 an employee's Slack credentials were stolen via malware, allowing attackers to access chat histories, email addresses, and names of 17,368 individuals. While no source was confirmed, the incident highlights risks in internal communications systems at major media organizations.

Swedish Software Supplier Breach Hits 1.5M Records

+Sweden +Technology +Government

- A [Swedish IT systems supplier](#) serving roughly 80% of municipalities and other large organizations suffered a breach that exposed records for about 1.5 million individuals, including personal ID numbers, names, and email addresses. The affected dataset also contained references to some military identities. The incident underscores supply chain risk when a vendor is entrusted with citizen data across government and corporate clients.

\$120M Crypto Heist at Balancer DeFi Protocol

+Crypto

- [Balancer](#), an Ethereum-based decentralized finance protocol, was exploited on November 3, 2025, via a rounding error vulnerability in its composable stable pools, resulting in more than \$120 million worth of cryptocurrency drained. The large-scale theft shook market confidence and revealed weaknesses in smart contract validation and DeFi risk management.

Law Enforcement Platform Logins Sold, Surveillance Cameras at Risk

+Government +US

- U.S. lawmakers warned that credentials for [Flock Safety](#) law enforcement customer accounts were stolen and shared online, exposing networks of license plate reader and surveillance camera access. At least 35 accounts were confirmed in public data, with access reportedly offered for sale on a Russian-language forum. The incident raises national security concerns as compromised logins could allow intruders to monitor or disrupt law enforcement operations.

Akira Ransomware Group Breach of Apache OpenOffice

+Akira +Software +Open Source

- The Akira ransomware group announced it breached [Apache OpenOffice](#) systems on October 29, 2025, exfiltrating approximately 23 GB of sensitive corporate data before likely encrypting the network. The attack demonstrates how open-source projects can become valuable targets for ransomware actors seeking to exploit ecosystem trust and supply chain connections.

Massive BPO Vendor Breach Exposes 10M+ Records

+US +Business

- [Conduent](#), a U.S. business services provider serving government agencies and enterprises, confirmed a breach that began in late 2024 and was discovered in January 2025, exposing personal data of more than 10 million individuals. The compromised data included names, Social Security numbers, dates of birth, and health insurance or medical details. The incident highlights the high-value target nature of BPO vendors holding sensitive government and healthcare data.

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.