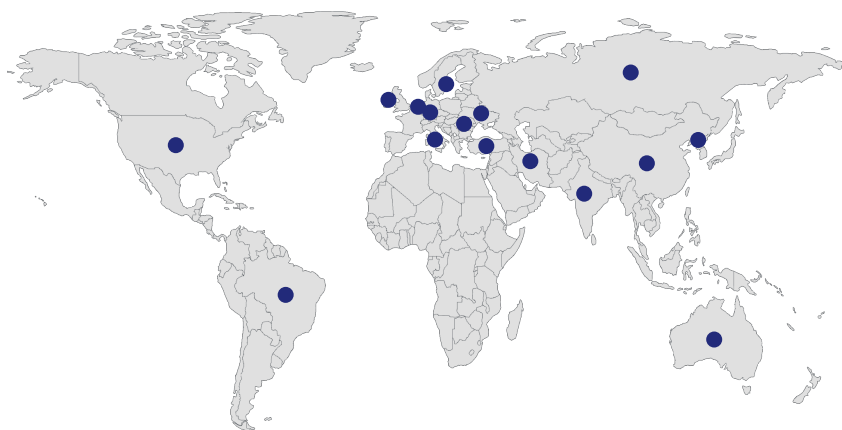


IMPERVA THREAT RESEARCH

# Threat Intel Report: October 27-November 2, 2025

## Countries



## Top Tags

BlueNoroff

UNC6384

CoPhish

Everest

SafePay

## Executive Summary

### Actionable Information:

- **Protocol and Platform Exploitation:** Core internet and software protocols remain high-risk vectors; attackers are exploiting overlooked behaviors in developer tools, cloud agents, and AI-integrated browsers. Vigilance at the protocol and runtime layer is critical.
- **Mass-Market and Mobile Software Risks:** Widely used apps, mobile ecosystems, and developer frameworks are increasingly weaponized, from RATs to NFC and input-mimicking malware, emphasizing the need for secure app vetting, runtime monitoring, and strict permission enforcement.
- **Abuse of Trusted Services and Agents:** Legitimate SaaS agents, cloud integrations, and workflow tools are being manipulated for token theft, data exfiltration, and account takeover, highlighting the importance of identity hygiene, OAuth oversight, and conditional access.
- **OT and Critical Infrastructure Risk:** Internet-facing industrial control systems remain highly vulnerable to opportunistic and hacktivist exploitation; network segmentation, secure remote access, and monitoring of operational anomalies are essential to prevent disruption.

### Outlook:

Overall, recent intelligence highlights an increase in automation-driven social engineering, stealthy malware, and exploitation of trusted platforms. Threat actors continue to combine traditional IT, mobile, cloud, and OT attack surfaces, using low-noise techniques and leveraging legitimate tools to maintain persistence and scale impact. AI is being operationalized by sophisticated adversaries to craft high-fidelity lures and automate operations, while the rise of malware-as-a-service and novel phishing methods is lowering the barrier for less skilled attackers to launch high-impact campaigns.

---

## Threat Activity in Imperva

### Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 216% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction. Exploitation of this issue requires the admin panel be exposed to the internet.

↑ 129% [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.

↑ 97% [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.

---

## Recent Cyber Threats

### Unchecked Compose YAML Lets Host Files Be Overwritten

+[Path Traversal](#) +[Docker](#)

- A serious path-traversal vulnerability ([CVE-2025-62725](#)) was discovered in Docker Compose versions prior to 2.40.2, allowing attackers to escape the local cache directory and write arbitrary files on the host machine simply by referencing a malicious remote OCI artifact. The flaw can be triggered even by “read-only” commands like `docker compose ps` if a crafted YAML file and OCI layer annotation are used, making it especially stealthy. Organizations running development, CI/CD pipelines or cloud workspaces that use Compose should patch immediately and scrutinize any remote-artifact use in workflows.

### Fake Telegram X App Spreads Backdoor on Android

+[Baohuo](#) +[Backdoor](#)

- A new Android backdoor dubbed [Baohuo](#) masquerades as the legitimate Telegram X client; once installed it hijacks Telegram accounts, enabling full control of chats and data. The malware has infected over 58,000 devices so far, primarily in India and Brazil. Users are lured via fake app versions and once permissions are granted, attackers pivot to account takeover and data theft.

### HyperRat: Android Spy-Tool Offered As-a-Service

+[HyperRat](#) +[MaaS](#)

- Security researchers uncovered a new Android remote access trojan named [HyperRat](#) that is marketed on cybercrime forums as a “ready-made” malware-as-a-service (MaaS). It allows attackers with little to no code-writing ability to remotely control infected devices, steal sensitive data, and launch mass phishing campaigns from the compromised Android device. This lowers the barrier to entry for mobile threat actors and increases the volume of potential campaigns.

### Atlas Browser Vulnerable to Prompt Injection via URL Bar

+[AI](#) +[Prompt Injection](#)

- [Atlas browser](#), the new AI-driven browser developed by OpenAI, is vulnerable to a novel form of prompt injection: malicious commands hidden in URLs entered into its “Omnibox” can cause the AI agent to execute unintended actions like navigating to a user’s cloud storage and deleting files. This risk underscores the broader dangers of agentic browsers which integrate autonomous AI actions with standard browsing, especially when they interpret ambiguous input as trusted commands.

## Herodotus Trojan Types Like a Human to Stay Hidden

+Herodotus +Trojan +Android +Italy +Brazil

- Researchers have discovered the Android banking Trojan [Herodotus](#) which mimics genuine human typing behavior, randomly delaying between keystrokes (0.3–3 seconds) to evade behavioral detection systems. Currently spotted in active campaigns in Italy and Brazil, and sold on underground forums as a malware-as-a-service (MaaS) offering, it enables full device takeover via accessibility abuse and overlay screens. Security teams should monitor for anomalous input timing on mobile endpoints and enforce least-privilege controls for Accessibility and overlay permissions.

## AI-Driven Executive Baiting by Crypto-Focused APT

+North Korea +BlueNoroff +GhostCall +GhostHire +India +Türkiye +Australia

- The North Korean-linked threat actor [BlueNoroff](#) (aka APT38/Sapphire Sleet) has expanded its operations with two campaigns dubbed “GhostCall” and “GhostHire” that leverage AI tools to craft highly targeted lures aimed at crypto- and Web3-industry executives on Windows and macOS platforms. Victims are enticed via fake investor meetings or bogus recruiter tests, which deliver malware or initiate account takeover; operations have spread across India, Türkiye, Australia and other regions since at least April 2025. The shift underscores how AI is being operationalized by sophisticated state-actors to automate social engineering, reduce footprint and scale out high-value targeting.

## Hacktivists Hijack Internet-Connected OT in Canadian Critical Infrastructure

+Canada +ICS

- The Canadian Centre for Cyber Security (CCCS) issued an alert warning that hacker groups are exploiting internet-accessible [industrial control systems \(ICS\) in Canada’s water, oil & gas and agricultural sectors](#). Documented incidents include tampering with water-pressure valves at a Canadian facility, raising false alarms at an oil & gas plant, and altering temperature/humidity at a grain-drying silo. The alert emphasizes that insecure ICS exposure can serve as a media-seeking tool for hackers, besides being a public-safety hazard, and urges improved segmentation, MFA, VPN use and asset inventory.

## Wave of NFC-Relay Malware Hits European Android Payment Users

+Android +NFC

- Researchers have uncovered a dramatic surge in [Android apps implementing Near-Field Communication \(NFC\) relay malware](#): over 760 malicious apps in recent months are targeting European users to steal payment-card info by relaying NFC transactions. The technique allows attackers to effectively impersonate NFC taps or nearby transactions inside compromised devices, enabling fraudulent use of cards at POS or ATMs without physical cloning. This rising threat emphasizes the mobile-payment ecosystem’s exposure and the need for mobile-app ecosystem vigilance.

## Chinese-Linked Zero-Day Weaponized Against European Diplomatic Targets

+China +Hungary +Belgium +Government +UNC6384

- A China-linked hacking group (UNC6384) has actively exploited a zero-day vulnerability in Microsoft Windows to compromise [systems used by European diplomats](#) in Hungary, Belgium and other nations. The exploit enables unauthenticated code execution at system-level privileges and is being used for espionage, underscoring the high-stakes nature of state-actor access to diplomatic networks. Organizations supporting diplomatic missions and international affairs must prioritize immediate patching and isolation of Windows endpoints.

## CoPhish’ Attack Leverages Microsoft Copilot Studio to Hijack OAuth Tokens

+CoPhish

- A novel phishing method dubbed [CoPhish](#) abuses Microsoft Copilot Studio agents hosted on trusted Microsoft domains to present malicious OAuth-consent flows; when users grant access, attackers harvest tokens granting access to e-mail, files and other resources. The use of legitimate enterprise domains and the façade of trusted agents materially increases the risk of large-scale credential/token compromise in enterprise SaaS environments.

## Data Breaches

### Dublin Airport Passenger Data Targeted by Everest Ransomware

+Ireland +Travel +Everest

- The Everest ransomware group has claimed to have stolen more than 1.5 million passenger records from the [Dublin Airport](#), along with personal details of about 18,000 employees of Air Arabia. The records allegedly include names, ticket numbers, seat assignments and device identifiers, raising risks of identity theft and targeted phishing.

### Sweden's Electricity Transmission Operator Reports Major Breach

+Sweden +Everest +Utilities

- State-owned transmission operator [Svenska kraftnät](#) confirmed that it suffered a data breach after the Everest ransomware group claimed to have stolen about 280 GB of internal data via a compromised external file-transfer system. There is no evidence that the power grid operations were impacted.

### Surveillance-Vendor Xortec Hit by Safepay Ransomware Leak Threat

+SafePay +Technology +Germany

- The ransomware group SafePay claimed responsibility for breaching German video-surveillance systems provider [Xortec GmbH](#) and listed the company on its data-leak site with a ransom deadline of 27 October 2025. Xortec supplies IP-cameras, NVRs and access-control hardware to installers and system integrators across the DACH region and internationally.

### Services Giant Conduent Hit by Ransomware-Linked Data Breach

+Technology +US +SafePay

- Technology-services provider [Conduent](#), which supports U.S. state programs including Medicaid, child-support and food-aid, is confirmed to have a breach affecting more than 10.5 million individuals, as claimed by ransomware gang SafePay. The incident highlights risks in large outsourcing firms whose compromise can ripple across many critical public-sector programs.

### Iran's State-Linked Cyber Academy Exposed in Student-Data Leak

+Iran +Government +Education

- [Ravin Academy](#), a cyber-training institution tied to Iran's Ministry of Intelligence, confirmed a breach that exposed names and contact details of students and associates training for state-sponsored cyber operations. The leak highlights operational risk and reputational exposure for Iran's intelligence-cyber ecosystem.

### Resume Bank Leak Exposes Thousands of U.S.-House Applicants

+US +Government

- A publicly accessible database tied to the application portal [DomeWatch](#) (used by U.S. House of Representatives offices) exposed personal data of over 7,000 job-seekers, including interns and staff applicants, raising serious concerns about identity theft and privacy for candidates who'd applied for sensitive roles. The leak included individuals with security clearances ("top secret" or similar) in some cases.

### Russia-Linked Group Uses Legitimate Tools to Infiltrate Ukraine

+Russia +Ukraine +Business +Government

- A cyber-espionage campaign attributed to a suspected Russian-linked group targeted [Ukrainian networks](#) over the summer by using "living off the land" techniques—legitimate administrative tools rather than malware—to breach a large business-services firm and a local government agency. The stealthy approach allowed long-duration undetected access and data theft, illustrating an evolving preference for minimal-footprint intrusion methods.

### Critical Telecom Supplier Ribbon Communications Breached by Nation-State Hackers

+Telecommunications +Government +US

- [Ribbon Communications](#), a U.S. telecom-services firm supporting major carriers and defense customers, disclosed that yet-unnamed nation-state hackers breached its IT network, potentially beginning in December 2024, and accessed older customer files stored outside its main network. The incident underscores how supply-chain and infrastructure vendors are prime targets for long-term espionage in the telecom sector.

---

## 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.