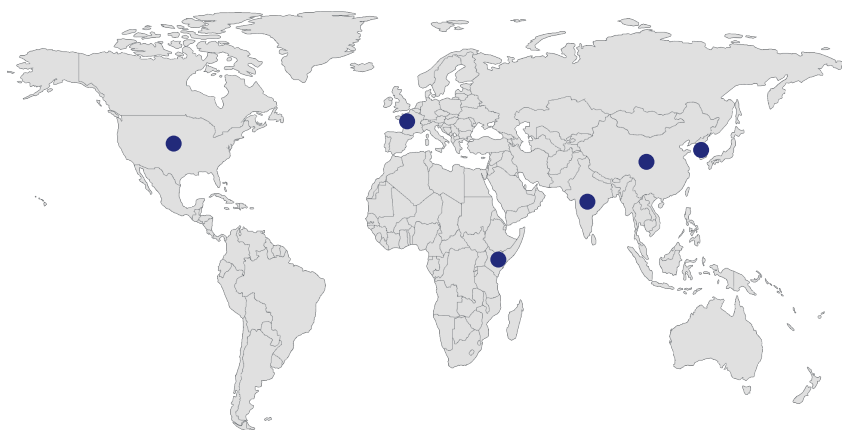


IMPERVA THREAT RESEARCH

Threat Intel Report: November 17-30, 2025

Countries



Top Tags

Lazarus

Everest

PCP@Kenya

Akira

INC

Executive Summary

Actionable Information:

- **Growing reliance on legitimate services to hide malicious infrastructure:** Threat actors are increasingly abusing trusted developer, storage, and cloud platforms to host payloads or route command-and-control traffic. This trend significantly erodes the effectiveness of domain-reputation and static-indicator-based defenses, requiring stronger behavioral and runtime telemetry.
- **Rise in highly convincing social-engineering operations:** Multiple campaigns this week highlight how attackers continue to prioritize deception over technical exploitation, leveraging fake updates, screen-sharing scams, and voice-phishing to compromise users and administrators. Organizations should assume that user-driven attacks will bypass technical controls and invest in layered identity-verification and least-privilege models.
- **Botnets and malware adopting decentralized and resilient C2 models:** Adversaries are experimenting with blockchain-based infrastructure, cross-platform runtimes (e.g., Node.js), and modular loaders to evade takedowns, accelerate payload delivery, and persist long-term in enterprise environments. Defenders should prioritize detection of unusual process runtimes, script execution, and outbound network patterns.
- **Financially motivated scams scaling with consumer behavior cycles:** Fraud campaigns tied to holiday shopping, customer support impersonation, and digital-payment abuse are rising sharply, exploiting periods of high transaction volume and user distraction. Financial institutions and e-commerce platforms should expect seasonal spikes and deploy adaptive fraud analytics.
- **Large-scale data exposure through both direct compromise and third-party supply-chain weaknesses:** Breaches across retail, education, public services, manufacturing, and government agencies underscore how adversaries target both primary

organizations and their vendors. Continuous third-party risk monitoring and incident-response integration with suppliers remain critical.

- **Critical infrastructure increasingly targeted or disrupted by ransomware and ideological actors:** Attacks on emergency-alert systems, transportation sectors, and government web platforms show the operational and societal impact of cyber disruptions. Resilience planning, segmentation, and offline communication backups are essential.

Outlook:

This week's activity reflects a maturing threat landscape where adversaries combine technical innovation, legitimate-service abuse, and highly targeted social-engineering to bypass conventional security controls. Emerging trends—such as decentralized botnet command structures, AI-enabled espionage tooling, and cross-platform loader ecosystems—signal that threat actors are investing in scalable, resilient operations that are harder to disrupt. At the same time, widespread data leaks and supply-chain breaches demonstrate that even organizations with strong internal security face elevated systemic risk through partners and vendors. Looking ahead, defenders should anticipate continued blending of espionage-grade tradecraft with financially motivated attacks, alongside increasing focus on critical-infrastructure targets and mobile-communication channels. Proactive monitoring, user-centric security design, and integrated vendor-risk governance will be essential to mitigate the next wave of threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 6,200% [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.

↑ 489% [CVE-2025-40598](#)

- A Reflected cross-site scripting (XSS) vulnerability exists in the SMA100 series web interface, allowing a remote unauthenticated attacker to potentially execute arbitrary JavaScript code.

↑ 350% [CVE-2025-31324](#)

- SAP NetWeaver Visual Composer Metadata Uploader is not protected with a proper authorization, allowing unauthenticated agent to upload potentially malicious executable binaries that could severely harm the host system. This could significantly affect the confidentiality, integrity, and availability of the targeted system.

Traffic Surge Targets Chilean Financial Services Site

+Chile +Financial Services +DDoS

- A Chilean financial services site was hit with a massive application-layer DDoS attack peaking at 1.8 million RPS, far exceeding typical traffic volumes for the region. The campaign originated primarily from IPs in the US, Chile, and Great Britain, suggesting a globally distributed botnet leveraging both local and foreign infrastructure.

Recent Cyber Threats

North Korea repurposes JSON-storage for stealth malware delivery

+North Korea +Lazarus

- Researchers report that the state-linked [Lazarus Group](#) (and related North Korean campaign clusters) have shifted tactics: rather than relying on overt malicious domains, they're embedding malware inside publicly available JSON-storage services. Attackers lure developers, often via fake job/recruiter outreach, into cloning seemingly legitimate repos; the repos contain trojanized code that fetches additional payloads from the JSON services. This vector helps bypass traditional defenses based on domain reputation or signature scanning, making detection harder and enabling supply-chain compromises targeting crypto and Web3 developers.

Fake Windows-Update screens power revived fake-update malware scam

+ClickFix +Infostealer

- A resurgence of the [ClickFix](#) campaign has been observed where attackers show a convincing full-screen fake Windows Update animation in the browser to trick users into pasting malicious commands into cmd/PowerShell. The malicious payloads, including info-stealers such as Rhadamanthys and LummaC2, are hidden via steganography inside PNG images and loaded in memory, circumventing many antivirus defenses. This technique relies heavily on user interaction and deception, highlighting the continuing effectiveness of social-engineering even in advanced malware campaigns.

Spyware tools increasingly targeting messaging-app users worldwide

+Government +Spyware

- The Cybersecurity and Infrastructure Security Agency (CISA) issued a warning that numerous cyber threat actors are now leveraging commercial spyware and remote-access trojans (RATs) to compromise [popular messaging apps](#) such as Signal and WhatsApp. Attack techniques include phishing-style social engineering, malicious QR-code pairing, and even “zero-click” exploits that deliver spyware without user interaction. Victims are often high-value individuals, government or military officials, activists, or executives, across the U.S., Middle East, and Europe, making this a substantial privacy and intelligence-gathering threat.

RomCom's loader lands via SocGholish for first time

+RomCom +SocGholish

- Security researchers report that in September 2025 a U.S.-based [civil-engineering firm](#), linked by past projects to a Ukrainian city, was targeted by RomCom via a fake-update SocGholish campaign. Roughly 10 minutes after initial exploitation, the firm received RomCom's Mythic Agent loader, giving the adversary a powerful post-exploit toolkit capable of remote access, reconnaissance and further payload delivery. This marks the first public instance of RomCom using SocGholish- a significant evolution that lowers the barrier for follow-on ransomware or espionage attacks.

Tsundere botnet weaponizes Node.js and Ethereum smart-contracts to control Windows devices

+Tsundere +Crypto

- Discovered in mid-2025, [Tsundere](#) uses Node.js-based malware whose command-and-control (C2) addresses are stored on the Ethereum blockchain, a novel approach that makes take-down and C2-rotation more resilient. The botnet spreads via disguised MSI installers (often named after popular games) or PowerShell scripts that deploy a full Node.js runtime and run obfuscated JavaScript loaders, sometimes flagged through supply-chain tactics like typosquatting or malicious npm packages. Once active, the bot installs legitimate libraries (e.g. ws, ethers, pm2) to maintain persistence and communicate with its blockchain-derived C2, giving the actor flexibility to push arbitrary code to infected machines. The actor behind it is believed to be a Russian-speaking individual known as “koneko,” which also operates the related 123 Stealer infrastructure.

Massive funds siphoned through WhatsApp screen-sharing scam

+Messaging

- Scammers are exploiting [WhatsApp's](#) screen-sharing feature: they send unsolicited video calls posing as support or bank staff, then trick victims into sharing their screen or installing remote-access tools citing “help” or “security issues.” Once inside, attackers steal one-time passwords and payment credentials, enabling immediate access to accounts and funds— one Hong Kong victim reportedly lost about US \$700,000 in minutes. The technique has appeared across multiple countries, underlining the global and cross-platform nature of this scam.

Holiday-shopping season sees surge in fake-gift ads that empty bank accounts

+Malvertising

- Cybercriminals have launched a large [malvertising campaign](#) impersonating major brands to trick shoppers with “fake gift” offers, especially timed for Black Friday. Victims are redirected through multiple hidden hops to scam landing pages posing as “survey reward” or “free gift” sites, where they are asked to enter payment or personal information, leading to bank-account

emptying or fraud. Because the ads mimic trusted brands and appear during high-traffic retail periods, they are particularly effective and hard to distinguish from legitimate promotions.

Data Breaches

Chinese firm leak reveals Beijing's global hacking toolkit

+China +Technology +AI +India +South Korea

- A leak of more than 12,000 confidential files from Chinese cybersecurity firm [Knownsec](#) (aka Chuangyu) exposed what appear to be state-linked "cyber weapons," internal AI hacking tools, and a sprawling list of targets across over 20 countries. The dump includes sensitive datasets such as 95 GB of Indian immigration records and what may be South Korean telecom call logs, suggesting the operations spanned critical infrastructure, government, and telecom sectors globally. The leak offers rare visibility into how deeply a private firm can be embedded in state-directed hacking programs, potentially reshaping understanding of global cyber-espionage networks.

Sportswear giant allegedly hit by data-extortion group

+Retail +Everest

- The Everest ransomware group claims it breached [Under Armour](#) and exfiltrated 343 GB of sensitive data, including customer PII, purchase histories, product catalogues, and internal company records. In a public post on their dark-web leak site, Everest published sample data and issued a seven-day ultimatum for the company to negotiate- a classic double-extortion move. If verified, the leak could put millions of Under Armour customers at risk of identity theft, fraud, and privacy violations.

Hackers deface Kenyan government sites with racist propaganda

+Kenya +Government +PCP@Kenya

- Multiple official [Kenyan government websites](#), including ministries of interior, health, education, energy, labour, and water, were defaced with white-supremacist messages. The group calling itself "PCP@Kenya" claimed responsibility; the defaced sites remained inaccessible for several hours before restoration. While no sensitive data leak has been reported, the incident disrupted public-facing government services and raises concerns about political or ideological motivations behind digital attacks.

French childcare childcare-payment service suffers major data leak

+France +Financial Services

- The French agency [Pajemploi](#), a social-security service used for parents paying private childcare providers, disclosed a breach affecting up to 1.2 million individuals (workers/employees). Potentially exposed data includes full names, dates and places of birth, postal addresses, social-security numbers, banking-institution names, and employer-service identifiers. Pajemploi said operations continue as normal and that each affected individual will be notified; the breach has been reported to national authorities.

Battery-maker hit by ransomware, 1.7 TB of data claimed stolen

+Energy +Akira

- [LG Energy Solution](#) confirmed a ransomware incident affecting one of its overseas facilities; the attack has since been mitigated and operations restored. Akira group claims to have exfiltrated roughly 1.7 TB of data, including corporate documents, employee records (passports, visas, ID cards), contracts, financials, and SQL databases, and posted the claim on its leak site. Given the company's role in EV-battery production and global supply chains, the breach poses serious risks to client confidentiality, corporate secrets, and potential phishing or identity-theft stemming from exposed PII.

Italy's national railway operator exposed after IT-provider hack

+Italy +Transportation +Government

- Sensitive data belonging to Italy's state-owned railway operator [Ferrovie dello Stato Italiane \(FS\)](#) was reportedly leaked following a breach at its IT-services provider Almagia, holding 2.3 TB of documents. The leak allegedly contains internal corporate plans, confidential contracts (including defense-industry and public-sector deals), financial records, HR data, and even passenger personal data (including passport numbers). This incident highlights the risk of third-party vendor compromise in critical national infrastructure, potentially impacting rail operations, employee privacy, and government/defense contracts.

University affected by vishing attack that exposed alumni & donor data

+US +Education +Vishing

- [Harvard University](#) disclosed that its Alumni Affairs and Development systems were compromised after a voice-phishing (vishing) attack, resulting in exposure of contact information for alumni, donors, staff, and faculty. The breach does not appear to involve sophisticated malware, but exploited human-element weaknesses- underscoring how effective simple social-engineering remains against even top institutions. The data leak raises risks of phishing campaigns, fraud, and reputational damage for the institution and affected individuals.

Ransomware strike hits US emergency alert system, jeopardizing public safety alerts

+US +Government +INC

- The US emergency notification platform OnSolve CodeRED was hit by a ransomware attack, claimed by INC Ransom, on November 1, 2025, with files encrypted by November 10. The breach resulted in the theft of user data including names, physical addresses, phone numbers, email addresses, and even clear-text passwords, which have since been offered for sale online. As a result, many municipalities went offline, residents lost access to timely emergency alerts, and the provider was forced to decommission the legacy system — raising serious concerns over public safety and data security.

OpenAI warns of data exposure after analytics-vendor breach

+AI +API

- On November 9, 2025 Mixpanel, a third-party analytics provider used by [OpenAI's](#) API platform, detected unauthorized access to part of its environment. The attacker exfiltrated a dataset containing limited user profile and analytics data for some OpenAI API users: names, email addresses, coarse location metadata, browser/OS info, referring websites, and user or organization IDs. Critically, no sensitive data was exposed: OpenAI confirmed that chat logs, API keys, payment info, passwords, or other credentials were unaffected.

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.