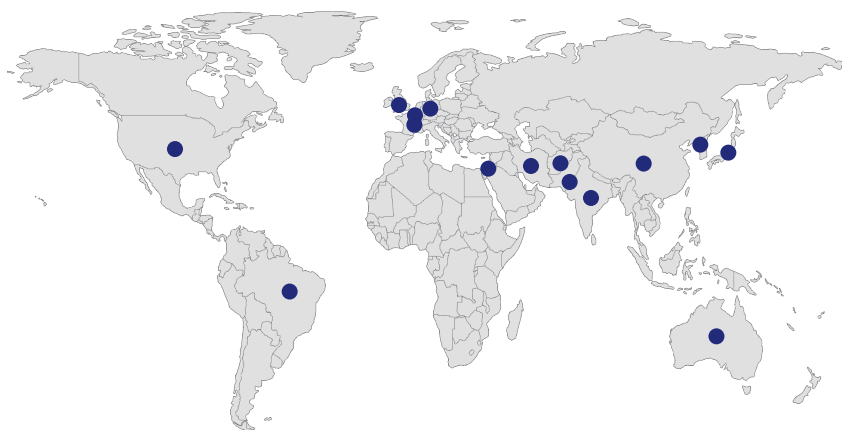


IMPERVA THREAT RESEARCH

Threat Intel Report: September 14-20, 2026

Countries



Top Tags

WaterPlum

Handala Hack

Transparent Tribe

FamousSparrow

ShinyHunters

Executive Summary

Actionable Information:

- High-leverage infrastructure remains a primary target. Active exploitation affected virtualization, identity, remote-management, and edge platforms, including VMware vCenter, Cisco ISE, and ScreenConnect, while supply-chain activity involving Brevo and npm packages extended risk into customer and developer environments.
- State-aligned operations remain geographically broad and technically diverse. North Korean WaterPlum activity combined fake recruitment, malware, and cryptocurrency theft at global scale, while Iran-linked, China-linked, and Pakistan-aligned actors continued espionage operations targeting dissidents, governments, defense organizations, and regional institutions.
- Trusted platforms and legitimate workflows are increasingly being used as delivery and persistence mechanisms. This week's activity included GitHub-hosted malware, Cloudflare Worker abuse, Telegram-based command-and-control, private GitHub repositories, browser extensions, and compromised third-party services, allowing malicious activity to blend with normal enterprise traffic.
- Data breaches continue to concentrate sensitive identity and operational information in third-party and centralized services. Incidents affecting Gyazo, Japan's Digital Agency, Revolut, CenterPoint Energy, RNLI, and Oceania Hotels exposed combinations of identity documents, government personnel data, financial records, customer information, and travel details.

Outlook:

The week's activity points to continued convergence between rapid exploitation of high-leverage infrastructure, state-aligned espionage, supply-chain compromise, and identity-focused data theft. Attackers are increasingly using legitimate cloud, developer, communications, and administrative platforms to reduce visibility while expanding the downstream impact of a single compromise. The near-term outlook is

for continued exploitation of edge and management systems, broader abuse of trusted software ecosystems, and more follow-on phishing, fraud, and extortion enabled by large identity-rich data exposures.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,898% [CVE-2026-21627](#)

- The vulnerability was rooted in how the Tassos Framework plugin handled specific AJAX requests through Joomla's com_ajax entry point. Under certain conditions, internal framework functionality could be invoked without proper restriction.

↑ 1,405% [CVE-2025-32432](#)

- Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

↑ 313% [CVE-2026-18072](#)

- The Advanced Responsive Video Embedder for Rumble, Odysee, YouTube, Vimeo, Kick ... plugin for WordPress is vulnerable to Authentication Bypass via a Hardcoded Backdoor in version 10.8.7. The vulnerability exists because the `\_arve\_uc\_init()` function — registered on WordPress's `init` hook at priority 1 so that it runs before any authentication checks on every request — reads an attacker-supplied token from the `\_wlogin` (or `\_wpm`) parameter and compares it against a hardcoded SHA-256 hash embedded directly in the plugin source, with no nonce verification, no capability check, and no password validation anywhere in the flow.

Recent Cyber Threats

North Korean WaterPlum Campaign Compromises 30,000 Devices Worldwide

+North Korea +WaterPlum +Cryptocurrency +Contagious Interview +Supply Chain

- A joint advisory from Japanese, U.S., Australian, and German authorities attributed a global malware campaign to North Korean threat group [WaterPlum](#), which compromised at least 30,000 devices across roughly 100 countries between December 2025 and July 2026 and transferred more than \$10.7 million in stolen cryptocurrency to North Korea. The operation is associated with the Contagious Interview campaign, using fake recruiting and freelance opportunities to direct developers toward malicious coding projects or npm packages. Authorities linked the campaign to more than 7,000 compromised cryptocurrency wallets, while stolen credentials and personal information have also supported fraudulent North Korean employment operations.

Iran-Linked MOIS Actors Deploy CHOSEN BRICK Spyware Against Dissidents and Journalists

+Iran +MOIS +CHOSEN BRICK +Cyber Espionage +United States +United Kingdom

- U.S., U.K., and Dutch authorities warned that actors linked to Iran's Ministry of Intelligence and Security are deploying [CHOSEN BRICK](#) spyware against dissidents, activists, journalists, and other targets worldwide. Operators establish trust through WhatsApp and Telegram before sending malicious Windows files disguised as material such as medical records; successful infections can steal communications, contacts and social-media information, capture screen content, and access device microphones. Authorities said stolen information has subsequently appeared on pro-Iranian leak sites, linking the surveillance operation to both intelligence collection and public exposure of targeted individuals.

Handala Hack Uses HEAVYGRAM Backdoor for Telegram-Based Espionage

+Iran +Handala Hack +HEAVYGRAM +Cyber Espionage +Israel

- Researchers linked the Iran-aligned Handala Hack persona to [HEAVYGRAM](#), a surveillance backdoor that uses Telegram infrastructure for command-and-control and supports remote command execution, system and process discovery, screenshot capture, DLL sideloading, persistence, and theft of files and Telegram sessions. A companion Delphi utility called CRUDEEXCLUDE prepares compromised Windows systems for later payloads by configuring Microsoft Defender exclusion paths. The findings add technical detail to Handala's broader operations, which have prominently targeted Israeli organizations and individuals.

Transparent Tribe Deploys New Rust Backdoor Against India and Afghanistan

+Pakistan +APT36 +Transparent Tribe +India +Afghanistan +Cyber Espionage

- Pakistan-aligned Transparent Tribe, also tracked as APT36, launched Operation [RapidRust](#) against government and defense organizations in India and Afghanistan using four previously undocumented tools: RUSTYSHADE, RUSTYMOVE, PSNATCH, and BASHNATCH. RUSTYSHADE is a Rust-based backdoor that abuses private GitHub repositories for command-and-control, while the supporting toolset provides persistence, reconnaissance, and data-theft capabilities. The activity continues the group's sustained focus on South Asian government, defense, telecommunications, and critical-infrastructure targets.

China-Linked FamousSparrow Deploys New SparroWocky Backdoor

+China +FamousSparrow +SparroWocky +Latin America +Cyber Espionage

- China-aligned [FamousSparrow](#) deployed a previously undocumented C++ backdoor named SparroWocky against government organizations across multiple Latin American countries. ESET found that the malware replaces the group's older SparrowDoor implant and uses extensive anti-analysis techniques and Windows internals knowledge, indicating continued investment in custom espionage tooling. FamousSparrow overlaps with other China-linked activity, including Earth Estries and Salt Typhoon, although the clusters are not necessarily synonymous.

Brevo Supply-Chain Attack Injects Malware Through Customer Websites

+France +Brevo +Supply Chain +ClickFix +Cloudflare +WordPress

- France-based marketing and CRM provider [Brevo](#) confirmed that attackers stole a long-lived Cloudflare API key with full account permissions and used it to modify web content at the CDN edge for approximately 5.5 hours on September 14. A malicious Cloudflare Worker altered Brevo websites and JavaScript components embedded on customer sites, displaying fake Cloudflare verification pages that directed Windows users through ClickFix malware execution. On WordPress sites, the malicious JavaScript also identified logged-in administrators and attempted to install a backdoored plugin disguised as Web Media Optimizer.

Rapuncel Campaign Impersonates 40 Software Brands and Disables 145 Security Products

+Rapuncel +LastPass +GitHub +Infostealer +BYOVD

- An ongoing malware campaign is using SEO-optimized [GitHub repositories](#) impersonating LastPass and at least 39 other software companies to distribute the Rapuncel information stealer. Victims are redirected through fake repositories to oversized ZIP archives intended to evade scanning, after which a renamed Microsoft Visual Studio debugger sideloads a malicious DLL. The campaign also deploys a legitimate Microsoft-signed kernel driver that can be abused to disable 145 antivirus and endpoint detection and response products.

KREMLIN Banking Malware Forces Malicious Extensions Into Chrome and Edge

+Brazil +KREMLIN +Banking Malware +Chrome +Edge +Credential Theft

- A Brazilian banking-malware operation active since mid-2025 is using a toolkit called [KREMLIN](#) to force malicious extensions into Chrome and Edge while bypassing Chromium integrity protections. The campaign begins with JavaScript files disguised as bank receipts, invoices, payment records, or business documents, then downloads Node.js, establishes scheduled-task persistence, and retrieves additional payload locations through an Ethereum smart contract. The extensions can steal credentials, authenticated session tokens, and other sensitive browser data; research has linked the toolkit to at least seven campaigns since May 2025.

NightmareStresser DDoS-for-Hire Platform Seized by FBI

+NightmareStresser +DDoS +United States +Botnet +Cybercrime

- The FBI seized the domains of [NightmareStresser](#), a long-running DDoS-for-hire platform linked to thousands of attacks. The booter advertised 24/7 access to botnets composed of compromised routers and IoT devices and previously had more than 566,000 registered users and 52 dedicated servers. Earlier analysis found the service could generate attacks reaching 200 Gbps across both Layer 4 TCP/UDP and Layer 7 application protocols.

Malicious npm Package Hides Malware in Normal Runtime Behavior

+npm +Supply Chain +JavaScript +Cryptocurrency +Open Source

- Researchers identified an ongoing npm supply-chain campaign involving [indexed-btree](#), a package designed to impersonate the legitimate sorted-btree library, which receives roughly 2 million weekly downloads. Rather than relying on install scripts, the malicious package hides its payload in normal runtime behavior, allowing execution after developers import it into an application. The operation has been linked to a cryptocurrency wallet containing 109 ETH, although researchers did not establish that the funds were stolen through the campaign.

Data Breaches

ShinyHunters Breaches CIOp Leak Site and Steals Ransomware Infrastructure Data

+ShinyHunters +CIOp +Ransomware +Extortion +Cybercrime

- [ShinyHunters](#) compromised the Tor data-leak site operated by the CIOp ransomware group, defacing the service and claiming to have stolen server data and the private keys controlling its onion address. The intrusion represents direct conflict between two major extortion ecosystems rather than conventional victim targeting, with ShinyHunters threatening to use stolen information against CIOp itself. Theft of Tor private keys could allow control or impersonation of infrastructure used to publish victim data and conduct extortion.

Gyazo Breach Exposes 23.6 Million Users and 490 Million Image Metadata Records

+Japan +Gyazo +Technology +Cloud +Credentials

- Image-sharing and screen-capture platform [Gyazo](#) confirmed attackers exploited a server vulnerability on September 11 and stole approximately 23.62 million user records. Exposed information may include names, email addresses, password hashes, user and device IDs, login-session IDs, X integration tokens, Google SSO email addresses, profile information, and subscription data. Attackers additionally accessed 490 million image-metadata records, including image IDs, IP addresses, User-Agent strings, EXIF location data, OCR-extracted text, source URLs, and hashed passphrases for private images.

Japan Government VPN Breach Exposes 246,000 Personnel Records

+Japan +Government +VPN +Digital Agency +Public Sector

- Japan's [Digital Agency](#) disclosed that exploitation of a vulnerability in a VPN device used by the Government Solution Service may have exposed approximately 246,000 rows of personal information belonging to government employees, officials, and associated organizations. Potentially affected information includes approximately 236,000 names, 231,000 email addresses, 94,000 telephone numbers, and 1,000 physical addresses. The agency began investigating after detecting large-scale file access through a maintenance employee's account and determined that an external actor had exploited the VPN device to enter the environment.

CenterPoint Energy Confirms Theft of Customer Data

+United States +Energy +CenterPoint Energy +Critical Infrastructure +Data Breach

- U.S. utility [CenterPoint Energy](#) confirmed that an attacker stole customer information after investigating claims involving 7.49 million records allegedly taken from the company. The threat actor claimed the dataset contained names, phone numbers, service and billing addresses, account numbers, billing amounts, and partial Social Security numbers. CenterPoint serves approximately 7 million metered customers across Indiana, Minnesota, Ohio, and Texas; the attacker's claimed 7.49-million-record total had not been independently confirmed at publication.

RNLI Supporter Data Exposed Through Beacon CRM Breach

+United Kingdom +RNLI +Beacon CRM +Third-Party Risk +Nonprofit

- The U.K.'s [Royal National Lifeboat Institution](#) notified supporters that their personal information may have been stolen through a July cyberattack against third-party customer-relationship-management provider Beacon CRM. Potentially compromised information includes names, contact information, and records describing supporters' interactions with the charity; Beacon is used by approximately 1,500 charities, creating potential exposure beyond the RNLI. Beacon said the incident did not appear to specifically target the lifeboat charity.

Oceania Hotels Customers Exposed Through Reservation Provider Breach

+France +Oceania Hotels +Hospitality +Third-Party Risk +Customer Data

- French hotel group [Oceania Hotels](#) notified customers that an unauthorized party accessed reservation information through the third-party provider hosting its online booking engine. The compromised information relates to stays scheduled between August

2026 and July 2027 and includes names, email addresses, telephone numbers, reservation numbers, and detailed stay information. Oceania said its own information systems were not compromised and that the vulnerability at the external provider had since been corrected.

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.