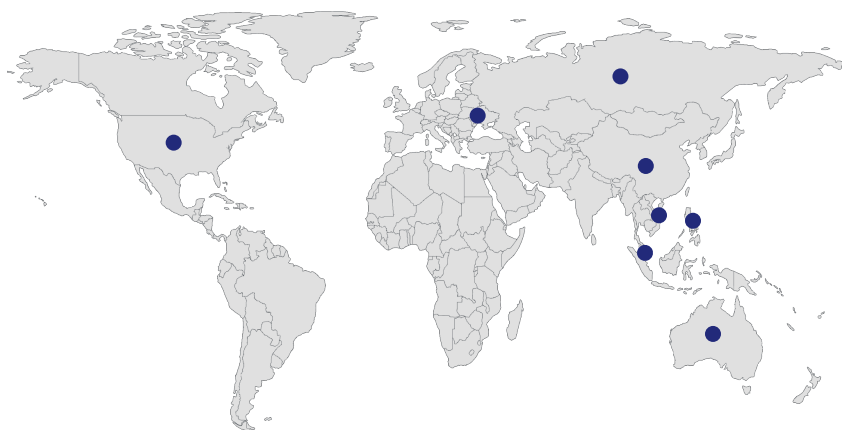


IMPERVA THREAT RESEARCH

Threat Intel Report: September 7-13, 2026

Countries



Top Tags

ShinyHunters

APT29

APT31

UNC3569

TheGentlemen

Executive Summary

Actionable Information:

- **Enterprise infrastructure and identity systems continue to be attacked in parallel, creating multiple paths to broad downstream compromise.** This week included exploitation of Adobe Commerce/Magento, MikroTik routers, JFrog Artifactory, GitLab, and N-able N-central, alongside Microsoft 365 phishing campaigns that bypass MFA by stealing authenticated sessions. The common pattern is attacker focus on platforms that sit at control points for software delivery, remote administration, routing, and cloud identity, where a single compromise can expose many systems or users rather than one endpoint.
- **AI is increasingly being used to sustain and accelerate real-world cyber operations.** A Russia-linked espionage cluster used Claude to automatically modify and redeploy malware after detection, while other campaigns this week combined AI-assisted vulnerability discovery or exploitation with conventional offensive tooling. The significance is not simply faster malware development, but greater operational resilience and reduced human effort across reconnaissance, exploitation, and evasion.
- **Cloud identity compromise and social engineering remain central to both espionage and extortion.** BigBear 2.0 stole more than 5,000 Microsoft 365 credentials across 258 organizations, while ShinyHunters, Helix, Falcon, and related groups used passkey-, SSO-, and MFA-themed lures to capture session tokens and enumerate enterprise cloud environments. These campaigns show that attackers are adapting to stronger authentication by manipulating trusted workflows and stealing valid sessions rather than attempting to defeat authentication mechanisms directly.
- **Large-scale data exposure is increasingly concentrated in identity, healthcare, travel, and third-party platforms.** The IDScan incident involved a claimed 153 million driver's-license records, a Vietnam-linked passenger database exposed roughly 220 million travel records, and healthcare breaches affected millions of patients at AdaptHealth and McKesson. Third-party access also featured prominently in the AdaptHealth, Brevo, Veradigm, and Trezor-related incidents, reinforcing the role of vendors and external platforms as aggregation points for sensitive data.

Outlook:

The dominant trend this week is the convergence of high-leverage infrastructure exploitation, cloud identity compromise, and AI-assisted operations. Threat actors are increasingly targeting platforms that provide administrative or downstream access—such as DevOps systems, routers, remote-management tools, and Microsoft 365—while using automation and AI to shorten operational cycles and maintain persistence after detection. At the same time, large breaches involving identity, healthcare, and travel data continue to expand the pool of information available for follow-on phishing, impersonation, and extortion. Looking ahead, the most significant risk is likely to come from attacks that combine these elements: rapid exploitation of trusted infrastructure, theft of valid identities or sessions, and increasingly automated post-compromise activity.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

 6,234% [CVE-2026-82329](#)

- JFrog Artifactory contains an authentication weakness that, under default configuration, may allow an unauthenticated attacker with network access to obtain administrative privileges.

 469% [CVE-2025-48828](#)

- Certain vBulletin versions might allow attackers to execute arbitrary PHP code by abusing Template Conditionals in the template engine. By crafting template code in an alternative PHP function invocation syntax, such as the "var_dump"("test") syntax, attackers can bypass security checks and execute arbitrary PHP code, as exploited in the wild in May 2025.

 264% [CVE-2025-66039](#)

- FreePBX Endpoint Manager is a module for managing telephony endpoints in FreePBX systems. Versions are vulnerable to authentication bypass when the authentication type is set to "webserver." When providing an Authorization header with an arbitrary value, a session is associated with the target user regardless of valid credentials. This issue is fixed in versions 16.0.44 and 17.0.23.

Recent Cyber Threats

StyleSmuggler Magento Zero-Day Exploited to Backdoor E-Commerce Servers

[+Adobe](#) [+Magento](#) [+CVE-2026-75650](#) [+Zero-Day](#) [+RCE](#) [+Retail](#)

- Adobe issued an emergency fix for [CVE-2026-75650](#), a maximum-severity CVSS 10.0 vulnerability dubbed StyleSmuggler affecting Adobe Commerce and Magento Open Source. Exploitation was observed beginning September 4, with attackers abusing Magento's template system through PHP code injection to achieve arbitrary code execution and install a backdoor disguised behind traffic resembling a normal NTP service. Compromised sites generated distinctive "Payment Transaction Failed Reminder" emails as part of the exploit path. Adobe confirmed active attacks against Commerce merchants when it released patches on September 7.

BlueMoon Exploit Kit Chains Chrome and Windows Zero-Days Across Multiple Espionage Groups

[+China](#) [+APT31](#) [+BlueMoon](#) [+Chrome](#) [+Windows](#) [+Cyber Espionage](#)

- At least four espionage clusters used a previously undocumented exploit kit called [BlueMoon](#), which chains two Chrome V8 vulnerabilities with a Windows ALPC privilege-escalation flaw. Proofpoint first observed China-linked APT31/JungleBamboo deploying the kit on August 28, followed within days by additional China-aligned and unattributed clusters targeting U.S.

aerospace companies, a Vietnamese manufacturer, and government, consulting, and financial organizations in Indonesia and Singapore. The chain combines browser code execution, sandbox escape, and Windows privilege escalation to move from a malicious link to host-level compromise. Two of the Chrome vulnerabilities were effectively patch-gap zero-days because fixes existed upstream in Chromium before reaching stable browser releases.

BigBear Phishing Service Steals 5,000 Microsoft 365 Credentials Across 258 Organizations

+BigBear +Microsoft 365 +AiTM +Phishing +Credential Theft

- The [BigBear 2.0](#) phishing-as-a-service framework was used to bypass MFA at 258 organizations and steal more than 5,000 Microsoft 365 credentials. CloudSEK researchers gained access to the operator panel and identified 42 VPS nodes configured specifically for Microsoft 365 phishing using an Evilginx2-based adversary-in-the-middle architecture. The service proxies victims through legitimate Microsoft authentication, collecting both passwords and authenticated session cookies after MFA is completed. The campaign further demonstrates how commercially available phishing infrastructure is commoditizing session hijacking that can bypass traditional MFA controls.

Passkey-Themed Phishing Drives Microsoft 365 Data Theft and Extortion

+ShinyHunters +Helix +Microsoft 365 +Passkeys +Vishing +Extortion

- Microsoft reported that actors associated with ShinyHunters, Helix, Falcon, and related extortion groups are using passkey-, SSO-, and MFA-themed help-desk [social engineering](#) to compromise enterprise cloud accounts. Victims are directed to adversary-in-the-middle sites or legitimate Microsoft device-code flows, allowing attackers to capture session tokens and subsequently enumerate Entra ID, SharePoint, OneDrive, Exchange, OAuth permissions, roles, authentication methods, and connected SaaS applications. Microsoft observed attackers registering their own MFA methods for persistence and conducting automated data collection over several hours or days while keeping download volumes low enough to blend into normal activity. The campaigns illustrate that passkeys themselves are not being technically broken; instead, attackers are exploiting users' trust in authentication-change workflows.

Russian State-Sponsored Group Uses Claude to Automatically Rebuild Detected Malware

+Russia +APT29 +Midnight Blizzard +AI +Cyber Espionage

- Anthropic disrupted an operation attributed to [GTG-20006](#), a Russia-linked espionage cluster whose activity overlaps with APT29/Midnight Blizzard. The actor used Claude to monitor whether deployed malware had been detected and then automatically modify, rebuild, and redeploy components to evade static security detections. Targets included military intelligence entities in Ukraine and European governments, as well as diplomatic, defense, and U.S. foreign-policy organizations. Anthropic's reporting indicates that generative AI is increasingly being used not merely to write malware but to maintain operational resilience during active intrusions.

DoppelCart Operates 119,000 Fake Online Stores to Harvest Payment Cards

+DoppelCart +E-Commerce +Payment Fraud +Phishing +Global

- Researchers identified [DoppelCart](#), a fraud network using more than 119,000 domains to operate counterfeit e-commerce sites designed to steal payment-card information. More than 105,000 shops remained active when scanned, with 96% sharing identical build files and resolving to only 27 commerce backends; the campaign accounts for roughly 2.72% of all .shop domains. The operation copies branding, products, images, and descriptions from legitimate retailers to create convincing storefronts, surpassing the previously documented 75,000-domain BogusBazaar network. Its centralized infrastructure allows operators to create and maintain fraudulent storefronts at industrial scale across multiple countries and retail brands.

China-Linked UNC3569 Exploits Sogou Input Method to Deploy GRAYRABBIT

+China +UNC3569 +GRAYRABBIT +Cyber Espionage +Asia

- China-linked [UNC3569](#) exploited a vulnerability in the widely used Sogou Input Method for Windows to install its GRAYRABBIT backdoor. The group has primarily targeted government, education, technology, and financial organizations across East and Southeast Asia. A crafted link could ultimately give attackers the same level of access as the logged-in victim, making exploitation particularly relevant in environments where Sogou is widely deployed.

Data Breaches

IDScan Confirms Cloud Breach Linked to 153 Million Driver's License Images

+United States +IDScan +Identity Verification +Driver's Licenses +Cloud

- Identity-verification provider [IDScan](#) confirmed unauthorized access to customer data in its cloud environment after a threat actor offered a dataset purportedly containing more than 153 million driver's-license records. Earlier samples associated with the claimed dataset included license images and identity information collected by organizations using IDScan's verification services, making the exposure particularly sensitive because customers may never have had a direct relationship with IDScan itself. The company began investigating after being linked to the database and notified law enforcement. The incident highlights the concentration risk created by identity-verification services that aggregate government-issued identity documents across many downstream customers.

Vietnam-Linked Passenger Database Exposes 220 Million Travel Records

+Vietnam +Aviation +Government +Travel +Data Exposure

- Researchers discovered an exposed [Advance Passenger Information System](#) database containing approximately 220 million passenger and crew records spanning 2017 through 2026. The records included names, passport numbers, dates of birth, nationalities, and detailed flight information, and researchers accessed the system through a cloud-hosted path protected by default credentials. The database was linked to Vietnam's passenger-information ecosystem, although reporting did not establish that all affected travelers were Vietnamese. The combination of passport and travel-history data creates unusually detailed profiles of international travelers and airline personnel.

AdaptHealth Breach Exposes Data of 4.1 Million Patients

+United States +Healthcare +ShinyHunters +AdaptHealth +Third-Party Risk

- [AdaptHealth](#) confirmed that 4,115,802 individuals were affected by a breach involving cloud-based patient-management, document-storage, and electronic-health-record systems. Attackers gained access after social engineering compromised a privileged account belonging to a third-party contractor, and a threat actor later demanded payment in exchange for withholding the stolen information. Exposed data included names, contact and demographic information, health-insurance data, and health information. The incident was attributed in reporting to ShinyHunters and affected a provider serving millions of patients across all 50 U.S. states.

McKesson Leak Exposes 6.4 Million Email Addresses and Health Data

+United States +Healthcare +McKesson +ShinyHunters +Patient Data

- Have I Been Pwned added 6.4 million unique email addresses from data allegedly stolen from healthcare and pharmaceutical giant [McKesson](#) during an August ShinyHunters pay-or-leak campaign. The exposed corpus contained information associated with patients, employees, healthcare-provider contacts, and marketing recipients, including names, dates of birth, phone numbers, physical addresses, employers, gender, and personal health data. McKesson confirmed unauthorized access to certain third-party applications affecting a subset of customers in its Oncology & Multispecialty and Medical-Surgical units, while stating it had reasonable assurance that unauthorized access was no longer ongoing. HIBP classified the dataset as sensitive because of the medical information involved.

Florida DMV Database Breached Through Stolen Police Credentials

+United States +Florida +Government +ShinyHunters +Identity

- [Florida's Department of Highway Safety and Motor Vehicles](#) confirmed unauthorized access to its DAVID driver-information database using valid credentials belonging to a police-department employee. ShinyHunters had previously claimed to have stolen more than 200,000 driver records from the platform, and state officials subsequently confirmed that the account had been compromised after credentials were stolen from an employee's personal device. DAVID contains sensitive driver's-license and motor-vehicle information used by authorized government and law-enforcement personnel. The incident demonstrates how compromise of one trusted external user can expose a centralized government identity database without requiring direct exploitation of the underlying application.

Mathspace Breach Exposes More Than One Million Students, Parents, and Staff

+Australia +Education +Mathspace +ShinyHunters +Metabase

- Online mathematics-learning platform [Mathspace](#) disclosed that attackers stole data belonging to more than one million students, parents, and staff after breaching its internal Metabase reporting environment. The compromise forms part of a broader campaign in which attackers exploited a critical Metabase SQL-injection zero-day to gain administrator access to

customer instances and steal underlying data. The same campaign affected organizations including Framework, Tally, and logistics provider ShipMonk and has been connected to ShinyHunters extortion activity. The large number of minors potentially represented in the Mathspace dataset makes the breach particularly sensitive within the education sector.

Brevo Breach Enables Phishing Against 347,000 Trezor Customers

[+Trezor](#) [+Brevo](#) [+Cryptocurrency](#) [+Phishing](#) [+Supply Chain](#)

- A separate third-party incident involving email-marketing provider [Brevo](#) exposed Trezor's newsletter infrastructure to an unauthorized actor, enabling phishing messages to be sent to approximately 347,000 email addresses. Around 2,500 recipients clicked the malicious link before the domain was taken down roughly 20 minutes after the campaign began. The emails impersonated Trezor security alerts and claimed a hardware microcontroller vulnerability required customers to download an application and enter their wallet backup phrase. Brevo said the September 9 incident affected 120 customer accounts, making Trezor one of multiple organizations exposed through the provider.

Veradigm Third-Party Breach Exposes Patient Information

[+United States](#) [+Healthcare](#) [+Veradigm](#) [+Ransomware](#) [+Third-Party Risk](#)

- Healthcare technology company [Veradigm](#) disclosed that a cybersecurity incident at a third-party vendor exposed patient personal information. The disclosure followed claims by The Gentlemen ransomware operation, which has increasingly used data theft alongside encryption and operates tooling designed to disable endpoint security controls. Veradigm provides clinical, financial, and data services used across healthcare organizations, increasing the potential downstream sensitivity of compromised patient information. The company had not publicly provided a complete victim count at the time of the September 9 disclosure.

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.