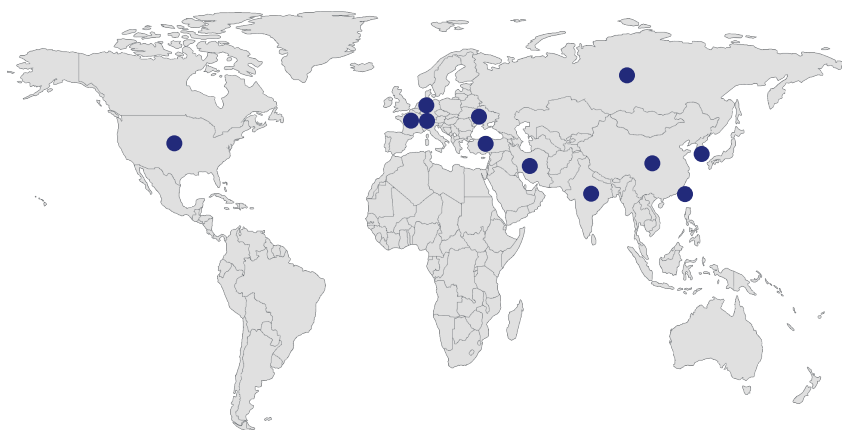


IMPERVA THREAT RESEARCH

Threat Intel Report: August 10-16, 2026

Countries



Top Tags

Gunra

Conti

ShinyHunters

ClOp

ExfilSquad

Executive Summary

Actionable Information:

- **AI-enabled intrusion activity is moving from experimentation toward operational use.** Taiwan's government reported a campaign in which multiple autonomous agents performed reconnaissance, vulnerability research, exploitation, and tactical adaptation in parallel, while other reporting this week showed threat actors using AI-assisted workflows to increase the speed and scale of attacks. Defenders should assume that attacker dwell time will continue to shrink and prioritize rapid exposure management, automated containment, and monitoring for machine-speed reconnaissance and exploitation behavior rather than relying on human-paced response assumptions.
- **Enterprise platforms, software supply chains, and privileged infrastructure remain high-leverage targets.** Active exploitation of VMware vCenter and campaigns against Salesforce, ServiceNow, open-source dependencies, and trusted recruitment or communications workflows show attackers concentrating on systems that provide broad access or downstream reach. This trend increases the importance of hardening externally exposed management platforms, reviewing SaaS and portal configurations for anonymous data exposure, and treating third-party and open-source dependencies as part of the core attack surface.
- **Identity theft, social engineering, and trusted-service abuse continue to converge.** Sandworm's recruitment lures, RecruitTrap's browser-in-the-browser phishing, and broader abuse of legitimate cloud and collaboration services demonstrate that attackers are increasingly blending malicious activity into normal business workflows. Organizations should strengthen phishing-resistant MFA, monitor for anomalous use of trusted SaaS platforms, and train users to treat recruitment, collaboration, and support interactions as potential attack vectors rather than focusing primarily on email-based phishing.
- **Data breaches are increasingly creating durable secondary risk through third parties and extortion ecosystems.** This week's incidents exposed tax, customer, shipping, energy, and enterprise data across France, the U.K., and global organizations, while ShinyHunters, ClOp, and ExfilSquad continued to monetize stolen information through leak and extortion campaigns.

Organizations should expect exposed data to support follow-on phishing, fraud, credential abuse, and highly targeted social engineering long after the initial breach, particularly when logistics providers, SaaS platforms, and other third parties are involved.

Outlook:

The dominant theme this week is the continued shift toward high-speed, high-leverage attacks that combine automation, identity compromise, and trusted infrastructure. AI-assisted operations are beginning to compress reconnaissance and exploitation timelines, while attackers continue to favor centralized enterprise platforms, third-party providers, and supply-chain dependencies that can expose large numbers of organizations from a single compromise. At the same time, data-theft extortion remains a persistent monetization model, with stolen information retaining value well beyond the original incident. Looking ahead, organizations should expect more autonomous attack activity, faster exploitation of newly disclosed vulnerabilities, and increasing abuse of legitimate cloud, SaaS, and software ecosystems to evade detection and maximize downstream impact.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 3,023% [CVE-2025-3248](#)

- Langflow versions prior to 1.3.0 are susceptible to code injection in the `/api/v1/validate/code` endpoint. A remote and unauthenticated attacker can send crafted HTTP requests to execute arbitrary code.

↑ 1,488% [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.

↑ 1,447% [CVE-2026-48939](#)

- A vulnerability in the iCagenda extension for Joomla allows the upload of arbitrary files in the file attachment feature, ultimately resulting in PHP code upload and execution.

Recent Cyber Threats

VMware vCenter RCE Campaign Compromises Systems Across 47 Countries

+Germany +US +Turkey +Iran +France

- Attackers are actively exploiting [CVE-2026-59310](#), a critical VMware vCenter Syslog Server vulnerability, to establish persistent remote access using a reverse-SSH utility. Researchers identified compromises at 361 IP addresses across 47 countries, with more than half located in Germany, the United States, Turkey, Iran, and France. Compromising vCenter is particularly significant because the platform centrally manages virtualization infrastructure and may give attackers visibility or control across large numbers of virtual machines. The geographically dispersed victim set demonstrates that exploitation has moved beyond isolated probing into a broad international campaign.

Taiwan Government Hit in Unprecedented AI-Assisted Cyberattack

+Taiwan +AI +China +Government

- [Taiwan](#) confirmed an unusual AI-assisted intrusion campaign after researchers identified attackers using open-source AI agents to automate reconnaissance, vulnerability research, exploitation, and tactical adaptation. Over four days in early July, up to eight

autonomous agents reportedly mapped 21 government systems, compromised at least 85 accounts, and extracted more than 2,500 personnel records before expanding reconnaissance to Taiwan's nuclear safety agency and at least seven energy companies. Researchers did not formally attribute the operation, but Simplified Chinese artifacts led them to assess likely China-linked involvement, while Taiwan said the attacks originated overseas. The incident represents one of the clearest examples to date of AI agents being used in parallel to conduct substantial portions of an intrusion workflow rather than merely generating attack content.

Gunra Ransomware Targets Government and Critical Infrastructure Worldwide

+US +South Korea +Gunra +Conti +Ransomware

- U.S. federal agencies and South Korea's National Policy Agency jointly warned government and critical-infrastructure organizations worldwide about [Gunra](#) ransomware, which first emerged in April 2025 and is derived from leaked Conti source code. The group uses double extortion and has targeted healthcare and public health, financial services, government entities, and other critical sectors. The joint advisory reflects sufficient international activity to prompt coordinated U.S.-South Korean defensive guidance rather than a country-specific alert. Organizations were urged to strengthen access controls, patch exposed infrastructure, and reduce opportunities for lateral movement and ransomware deployment.

City-Forum Campaign Harvests Exposed Salesforce and ServiceNow Data

+City-Forum

- An ongoing campaign dubbed [City-Forum](#) is using custom tooling to systematically collect data exposed to anonymous users through Salesforce Experience Cloud and ServiceNow customer portals. Researchers traced the campaign to a common server and identified targets worldwide across telecommunications, banking and financial services, enterprise software, cybersecurity, privacy, and public-sector organizations. Rather than exploiting the underlying SaaS platforms directly, the campaign identifies customer deployments where portal configuration exposes information without authentication and then harvests it at scale. Researchers said activity was continuing to increase during the reporting period, highlighting configuration exposure as an increasingly valuable cloud attack surface.

Sandworm Targets IT Professionals With Trojanized WireGuard Client

+Russia +Ukraine +Sandworm +UAC-0145

- Russia-linked [Sandworm](#), tracked in this campaign as UAC-0145 and believed to be a sub-cluster of APT44, has targeted system administrators and IT professionals through fake recruitment approaches since at least May. Operators study victims' resumes on employment sites, pose as technology companies or recruiters, and deliver a trojanized WireGuard VPN client as part of the hiring process. Targeting administrators is particularly valuable because their legitimate access may provide direct paths into privileged systems and enterprise infrastructure. Ukraine's CERT attributed the activity and warned that the campaign combines detailed target reconnaissance with trusted software branding to increase execution rates.

China-Linked Jewelbug Combines Government Espionage With Cryptocurrency Fraud

+China +Jewelbug

- China-linked hackers-for-hire group [Jewelbug](#) is using a common infrastructure and malware ecosystem to conduct both state-oriented espionage and financially motivated cryptocurrency theft. Its XG-Web platform turns victim browsers into remote-control channels and supports implants across browsers, Windows systems, Linux servers, and network devices, with researchers identifying government and military targeting across the Middle East, Southeast Asia, and South Asia and more than 90 police and government email addresses in South Asia. The group has developed five generations of command-and-control code, all feeding victim information into a common backend. The blending of intelligence operations with commercial cybercrime complicates traditional actor classification and creates risk across both government and private-sector targets.

Apple Warns Users in 110 Countries About Mercenary Spyware Targeting

+Spyware

- [Apple](#) issued a new wave of threat notifications to users it believes may have been targeted with mercenary spyware, covering an unspecified number of customers across 110 countries. Since launching the notification program in 2021, Apple has warned users in more than 150 countries, illustrating the geographic reach of commercial surveillance operations. The company does not publicly attribute individual notifications to specific spyware vendors, threat actors, or governments because of the sophistication and opacity of the campaigns. The scale of the latest alert reinforces that advanced mobile surveillance is not limited to a small number of countries and remains a global risk for government officials, journalists, executives, activists, and other high-value individuals.

Large-Scale DDoS Campaign Disrupts Swiss Secure Messaging Service Threema

+DdoS +Switzerland +India +China

- A series of large-scale and rapidly changing DDoS attacks disrupted [Threema's](#) hosted secure-messaging infrastructure, temporarily making communications unavailable or significantly delayed during August 11–12. Users in Switzerland, India, and China reported service problems, while organizations using Threema On-Prem remained unaffected because their messaging infrastructure is independently hosted. Threema said the adversary continuously changed attack patterns and also targeted colocation provider Nine, complicating mitigation. The incident demonstrates the operational impact that DDoS attacks can have on privacy-focused communications services even without compromising encryption or user data.

Recruitment Phishing Campaign Uses More Than 3,000 Browser-in-the-Browser Lures

+RecruitTrap +Marketing

- Researchers tracking [RecruitTrap](#) identified more than 3,000 recruitment-themed phishing URLs over two months impersonating hiring processes at more than 50 organizations across 14 sectors. Fake Calendly-style interview pages and branded recruitment portals launch Browser-in-the-Browser login windows designed to steal Google and Facebook credentials, with more advanced infrastructure capable of relaying MFA prompts in real time. Marketing professionals represented the majority of observed targets, likely because compromised accounts can provide access to advertising platforms, corporate social media, customer information, and email. The campaign demonstrates how professional networking and recruitment workflows are increasingly being weaponized for enterprise account compromise.

Data Breaches

French Tax Authority Breach Exposes Data of 678,000 Taxpayers

+France +Government +Financial Services

- [France's Ministry of Economy and Finance](#) confirmed that attackers accessed systems belonging to the General Directorate of Public Finances (DGFIP) and extracted information belonging to 678,000 individuals and professionals. The intrusion reportedly occurred in late June but came to public attention after a threat actor advertised data on a cybercrime forum on August 12. Exposed information included tax-related data such as reference taxable income, family quotient, and withholding-tax rates, while business records included company names and SIREN identifiers. France said affected users would be individually notified and launched further investigations to determine the precise scope of the compromise.

RingCentral Breach Exposes 1.6 Million Accounts

+ShinyHunters

- 1.6 million unique [RingCentral](#) accounts were compromised during a July ShinyHunters pay-or-leak campaign, exposing names, email addresses, phone numbers, and physical addresses. RingCentral provides cloud calling, messaging, and voicemail services to more than 600,000 businesses, increasing the potential value of exposed customer and business-contact information for follow-on phishing and impersonation. ShinyHunters claimed to have stolen approximately 623 GB of information, although RingCentral said the breach affected only a limited portion of customers and did not disrupt its core communications platform. Have I Been Pwned added the breach on August 13, materially clarifying the scale of the previously disclosed incident.

Trezor Shipping-Provider Breach Exposes Nearly 14,000 Customers

+US +UK +Sweden +Colombia +Brazil +Italy +Portugal

- Hardware-wallet company [Trezor](#) disclosed that logistics provider ShipMonk was compromised, exposing order information belonging to 13,689 customers in the United States, United Kingdom, Sweden, Colombia, Brazil, Italy, and Portugal. Of those, 11,742 had names, email addresses, phone numbers, and shipping addresses exposed, while 1,947 had names, cities, and email addresses compromised. Trezor emphasized that its wallets, seed phrases, private keys, passwords, and internal systems were not affected, but warned that the physical-address and crypto-product information could support highly convincing targeted phishing or physical-security scams. The incident again demonstrates the risk introduced when cryptocurrency companies share customer identity and delivery information with logistics providers.

Valve Warns European Steam Hardware Buyers After CEVA Logistics Breach

+Gaming

- [Valve](#) notified European customers who purchased Steam hardware that personal data was stolen following a compromise at shipping partner CEVA Logistics, a subsidiary of France-based CMA CGM. CEVA operates approximately 1,000 warehouses, handled 15 million shipments in 2025, and reported \$18.3 billion in revenue, making it a significant global logistics provider. Valve said exposed information was limited to data available to the shipping provider and did not include Steam passwords, Steam Guard codes, payment information, or unrelated purchase history. The incident is another example of technology companies suffering customer-data exposure through logistics partners rather than compromise of their own core platforms.

Shell Investigates Clop Claim of 89 GB Data Theft

+UK +Energy +Clop

- British energy giant [Shell](#) confirmed it was investigating a potential cyber incident after Clop claimed to have stolen 89 GB of data, including engineering drawings, facility test reports, photographs, and project plans. Shell employs approximately 85,000 people in more than 70 countries and serves more than 20 million customers per day through its global service and charging network. Clop listed Shell among 43 newly claimed victims believed to have been targeted through exposed PTC Windchill and FlexPLM environments. Shell had not confirmed Clop's claimed data volume or the precise intrusion method at publication, so the breach claim should remain characterized as under investigation.

ExfilSquad Claims Data Theft From Global Distributor Wesco

+ExfilSquad

- Global electrical, communications, utility, and supply-chain distributor Wesco confirmed that it was investigating a cybersecurity incident after ExfilSquad claimed to have stolen sensitive company information and published data on its leak site. Wesco's position in industrial, electrical, communications, and utility supply chains increases the potential downstream intelligence value of compromised business and customer records. At publication, Wesco had not confirmed the volume or categories of information allegedly stolen, making the attacker's claims unverified beyond the company's acknowledgment of an incident. The disclosure continues ExfilSquad's 2026 pattern of data-theft extortion without reliance on ransomware encryption.

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.