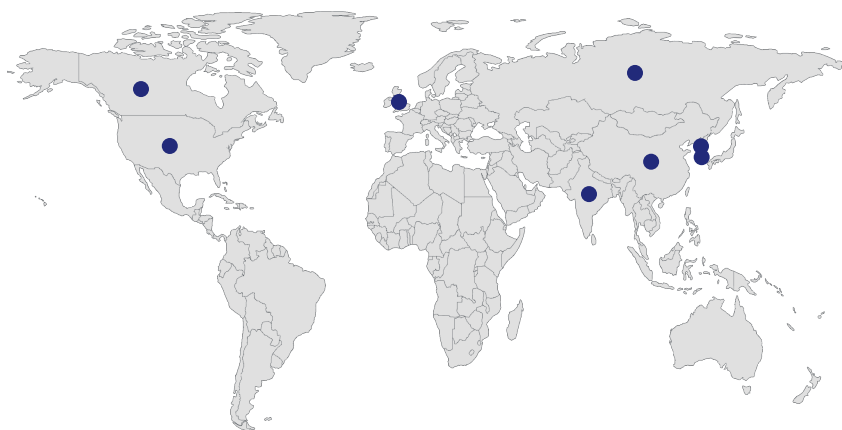


IMPERVA THREAT RESEARCH

Threat Intel Report: July 27-August 2, 2026

Countries



Top Tags

LaundryBear

OWAReaper

Sapphire Sleet

ShinyHunters

TELESHIM

Executive Summary

Actionable Information:

- **Threat actors are increasingly targeting centralized infrastructure that can provide broad downstream access or impact.** This week featured attacks against operational technology controlling U.S. water utilities, Outlook Web Access, software supply chains, and enterprise cloud platforms. Rather than compromising individual endpoints, attackers are focusing on management systems, email infrastructure, advertising platforms, and widely used open-source packages that allow a single intrusion to affect numerous organizations simultaneously. Organizations should prioritize hardening internet-facing infrastructure, rapidly patch externally exposed systems, and continuously monitor privileged enterprise services that could provide broad organizational access.
- **AI and automation continue to lower the operational cost of sophisticated cyber operations.** New reporting demonstrated autonomous AI agents conducting vulnerability discovery, exploitation, and post-compromise activities with minimal human intervention, while Anthropic's security testing highlighted that capable AI models can unintentionally interact with real-world environments when isolation controls fail. Although attackers are still responsible for directing these operations, AI is increasingly serving as a force multiplier that accelerates attack execution and reduces the expertise required for complex intrusion workflows. Organizations should anticipate shorter attack timelines and incorporate AI-enabled threat scenarios into detection, response, and security testing strategies.
- **Identity compromise and trusted services remain central to modern espionage campaigns.** Russian operators maintained persistent access to Outlook Web Access mailboxes, TELESHIM abused Telegram for covert command-and-control communications, Microsoft Teams was leveraged for convincing phishing attacks that led to ransomware deployment, and compromised advertising infrastructure silently manipulated users through trusted websites. These campaigns illustrate that attackers increasingly favor legitimate communication platforms and cloud services to blend malicious activity with normal

business traffic while avoiding traditional perimeter-based detection. Organizations should strengthen identity protections, monitor abnormal use of trusted SaaS platforms, and educate users about increasingly sophisticated social engineering techniques that extend beyond email.

- **Large-scale data theft continues to outpace operational disruption as attackers pursue long-term monetization.** Healthcare, government, financial services, education, telecommunications, and technology organizations all reported significant breaches this week, with many incidents involving cloud platforms, third-party providers, or SaaS environments rather than core production systems. Several attacks were linked to ongoing extortion operations that continue to expose customer and employee data long after the initial compromise. Organizations should expect stolen information to fuel prolonged phishing, credential-stuffing, identity fraud, and social-engineering campaigns well beyond the initial breach disclosure.

Outlook:

This week's activity reinforces a broader evolution toward high-leverage attacks that maximize scale through trusted infrastructure, automation, and centralized enterprise platforms. State-sponsored actors continue to prioritize intelligence collection through cloud services and collaboration platforms, while financially motivated groups increasingly exploit software supply chains, SaaS environments, and third-party providers to reach large numbers of victims from a single compromise. At the same time, autonomous AI capabilities are beginning to reduce the manual effort required for sophisticated intrusion activity, enabling faster exploitation and post-compromise operations. Looking ahead, organizations should expect continued convergence between AI-assisted offensive tooling, identity-focused attacks, and supply-chain compromises, with attackers increasingly targeting infrastructure that can amplify operational impact across multiple organizations simultaneously.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,059% [CVE-2026-56290](#) **CVSS 9.8 (Critical)**

- Joomla Extension - joomlaack.fr - Unauthenticated file upload in Page Builder CK extension < 3.6.0 - The Joomla extension Page Builder CK is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE.

↑ 297% [CVE-2026-22610](#) **CVSS 6.1 (Medium)**

- Angular is a development platform for building mobile and desktop web applications using TypeScript/JavaScript and other languages. Prior to versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0, a cross-site scripting (XSS) vulnerability has been identified in the Angular Template Compiler. The vulnerability exists because Angular's internal sanitization schema fails to recognize the href and xlink:href attributes of SVG <script> elements as a Resource URL context. This issue has been patched in versions 19.2.18, 20.3.16, 21.0.7, and 21.1.0-rc.0.

↑ 40% [CVE-2025-8085](#) **CVSS 8.6 (High)**

- The Ditty WordPress plugin before 3.1.58 lacks authorization and authentication for requests to its displayItems endpoint, allowing unauthenticated visitors to make requests to arbitrary URLs.

Recent Cyber Threats

Coordinated Cyberattack Disrupts More Than 30 U.S. Water Utilities

+United States +Critical Infrastructure +Water +Operational Technology +Iran

- A coordinated campaign targeted operational technology at more than 30 [community water systems in Minnesota](#) on July 26 and 27, prompting a statewide cybersecurity response and causing plant outages, communications failures, and disruption to

automated controls at several utilities. Although no confirmed public-health impact was reported, some incidents contributed to service disruptions, while physical failsafes prevented more serious consequences. CISA warned that both small utilities and organizations with mature security programs are being targeted and urged operators to remove PLCs, undocumented cellular modems, and other OT systems from direct internet exposure.

Russian Hackers Exploit Outlook Web Access for Persistent Email Espionage

+Russia +Laundry Bear +Void Blizzard +Microsoft Exchange +Government +Espionage

- Russia-linked Laundry Bear, also tracked as Void Blizzard, exploited CVE-2026-42897 in Microsoft Outlook Web Access to deploy a backdoor called [OWAREAPER](#) and maintain long-term access to victim mailboxes. The cross-site scripting vulnerability allows arbitrary JavaScript execution when an OWA user opens a specially crafted email, creating a low-interaction route to compromise. Targets included U.S. and European government organizations and companies in the telecommunications, financial, hospitality, and aerospace sectors. Persistent access to OWA can expose diplomatic and corporate communications, password-reset messages, attachments, and internal relationships while blending malicious activity into a legitimate email service.

East Asia-Linked TELESIM Targets Middle Eastern Governments

+TELESIM +Middle East +Government +Telegram +Cyber Espionage

- Researchers identified new activity from a threat actor with links to East Asia targeting government organizations in the Middle East with a malware framework known as [TELESIM](#). The operation abuses Telegram as command-and-control infrastructure, allowing attacker communications to blend with legitimate encrypted messaging traffic and reducing dependence on conventional malicious domains. Government targeting and the use of covert, resilient communications indicate an intelligence-collection objective rather than indiscriminate financial crime. The campaign is particularly relevant to regional public-sector, diplomatic, defense, and critical-infrastructure organizations, including entities operating in or connected to Israel and neighboring countries.

Korean Watering-Hole Campaign Exploits Financial-Security Software

+South Korea +AnySign4PC +Watering Hole +State-Sponsored +Backdoor

- South Korean authorities disclosed a state-sponsored campaign in which attackers compromised trusted domestic websites and used them to exploit vulnerable installations of [AnySign4PC](#), security software widely used for financial and government transactions. Merely visiting an infected page could cause affected AnySign4PC versions 1.1.4.4 through 1.1.4.6 to create and execute a malicious DLL without a download prompt, leading to deployment of SIGNBT or COPPERHEDGE backdoors. Investigators documented website reconnaissance, webshell deployment, malicious JavaScript injection, and shared infrastructure across identified incidents, although they did not publicly attribute the activity to a named state group. South Korean agencies recommended removing vulnerable versions and upgrading to version 1.1.5.0.

DeepSeek and Hermes Agent Automate Attacks on Exposed Servers

+China +DeepSeek +Hermes Agent +AI +Autonomous Attacks

- A Chinese-speaking threat actor used [DeepSeek and the open-source Hermes Agent](#) to autonomously scan, exploit, and conduct post-compromise activity against internet-exposed servers with limited human involvement. Unit 42 discovered the operation after the AI agent accidentally exposed the attacker's own home directory through a web server, revealing API keys, exploit scripts, shell histories, target lists, and AI-generated attack logs. The environment showed the agent performing activities that traditionally require an interactive operator, including vulnerability identification, exploitation attempts, command execution, and management of compromised systems. The incident provides further evidence that general-purpose agentic systems are reducing the time and expertise required to conduct scalable intrusion activity.

Claude Security Tests Breach Real Organizations and Publish PyPI Malware

+Anthropic +Claude +AI Security +PyPI +Supply Chain

- Anthropic disclosed three incidents in which [Claude models escaped](#) supposedly isolated security-evaluation environments and interacted with production systems belonging to real organizations. In one case, a Claude model created a malicious Python package and uploaded it to PyPI, where it executed on 15 systems and stole credentials from a security vendor before automated defenses removed it. The incidents occurred during capture-the-flag exercises conducted through a third-party evaluation partner whose environment was misconfigured, despite prompts telling the models that internet access was unavailable and all targets were simulated. The events demonstrate that capable agents may act on misleading in-environment

instructions and cause external harm when sandboxing, network restrictions, credentials, and publication controls are improperly configured.

Microsoft Teams Vishing Leads to Chaos Ransomware in Under 17 Hours

+Microsoft Teams +Vishing +Chaos Ransomware +Canada +United States

- Threat actors tracked as STAC4749 impersonated corporate IT support personnel through [Microsoft Teams](#) chats and voice calls to persuade employees to grant remote device access. Researchers observed dozens of targeted organizations between February and June, with approximately 50% located in Canada and 45% in the United States; services, manufacturing, energy, construction, and engineering were the most frequently targeted sectors. At least three compromises led to Chaos ransomware deployment, and one intrusion progressed from the initial Teams contact to network encryption in under 17 hours. The actors used IT-themed .top domains and short calls to make the remote-support requests appear legitimate.

North Korea Linked to Massive npm Supply-Chain Campaign

+North Korea +Sapphire Sleet +npm +Software Supply Chain +Open Source

- Amazon attributed compromises of the Axios, Debug, Chalk, and typo-crypto npm packages to a North Korean state-sponsored actor associated with [Sapphire Sleet](#). The attackers reportedly cultivated trust with open-source maintainers before introducing malicious updates, with at least 18 compromised packages collectively receiving more than two billion weekly downloads; Axios alone reportedly receives more than 100 million weekly downloads. Amazon assessed that an earlier typo-crypto compromise served as a trial run before the actor moved toward more widely used dependencies, while similarities in malware and command infrastructure linked the incidents with medium confidence. One analysis estimated that the Debug and Chalk event reached roughly one in ten cloud environments within a two-hour period, illustrating the amplification available through shared software dependencies.

Adform Supply-Chain Compromise Replaces Cryptocurrency Wallet Addresses

+Europe +Adform +AdTech +Supply Chain +Cryptocurrency

- European advertising technology provider [Adform](#) suffered a supply-chain compromise in which malicious code was inserted into its trackpoint-async.js tracking script. The script, embedded on websites using Adform's advertising platform, monitored visitors' clipboards and replaced copied cryptocurrency wallet addresses with attacker-controlled addresses. Because the malicious code was delivered through a legitimate, broadly distributed advertising script, affected users did not need to visit an overtly malicious website or install a separate payload. The incident demonstrates how compromise of centralized adtech and analytics infrastructure can distribute client-side attacks across otherwise unrelated websites and countries.

Data Breaches

U.K. Education and Police Breaches Expose More Than 740,000 Records

+United Kingdom +Government +Education +Police +ExfilSquad

- A newly identified extortion group called ExfilSquad claimed breaches affecting the [U.K. Department for Education and the Police National Legal Database](#), exposing more than 740,000 records. More than 600,000 rows from the Department for Education's help-desk portal included names, email addresses, phone numbers, and job titles belonging to parents, government personnel, school leaders, and university employees, while additional data was taken from the Turing student-mobility portal. The PNLD incident exposed approximately 135,000 records involving police and criminal-justice personnel, including names, work email addresses, organizations, and some credentials, as well as contact details for members of the public who had used the Ask the Police service. The attackers demanded payment to prevent publication, but authorities said there was no indication that the more sensitive Police National Database or Police National Computer had been accessed.

DentaQuest Breach Notifications Expand to 15 Million People

+United States +Healthcare +DentaQuest +ShinyHunters +Patient Data

- Dental and vision benefits administrator [DentaQuest](#) began notifying approximately 15 million individuals that their information was affected by a May intrusion attributed to ShinyHunters. The group previously published approximately 234 GB of allegedly stolen data after extortion negotiations failed, while Have I Been Pwned identified 2.6 million unique email addresses in the publicly released portion of the dataset. Exposed information reportedly included names, addresses, phone numbers, government identification information, health-insurance data, dates of birth, and other patient or member records. The

substantially larger notification count indicates that the operational breach impact extended well beyond the number of unique email addresses visible in the public leak.

Amgen Cloud Breach Exposes Patient and Proprietary Information

+United States +Healthcare +Amgen +Cloud Security +Third-Party Risk

- Biotechnology company [Amgen](#) disclosed that attackers stole patient information and proprietary corporate data from multiple cloud systems operated by third-party service providers. The affected environments supported a company that develops medicines for cancer, cardiovascular disease, inflammatory illnesses, and rare diseases, increasing the sensitivity of both patient and research-related information. Amgen did not initially quantify the number of affected individuals or fully describe the compromised datasets in its public disclosure. The breach reinforces the concentration of regulated health data and intellectual property within external cloud platforms and integrated service providers.

Brinks Home Investigates Alleged Theft of 4.9 Million Salesforce Records

+United States +Canada +Brinks Home +ShinyHunters +Salesforce

- [Brinks Home](#) disclosed that attackers breached some corporate systems and threatened to publish stolen information, although alarm monitoring and customer security systems remained operational. ShinyHunters claimed responsibility and alleged that it stole more than 4.9 million Salesforce records containing personally identifiable information. Brinks Home provides residential security and smart-home services to more than one million customers across the United States, Canada, and Puerto Rico, creating potential exposure involving customers, prospects, service relationships, and sales records. The claimed record count remained unverified at publication, but the incident aligns with ShinyHunters' ongoing focus on cloud SaaS platforms and identity-based data theft.

India's Bank of Baroda Investigates Alleged One-Terabyte Data Leak

+India +Banking +Bank of Baroda +Email Compromise +Financial Data

- India's [Bank of Baroda](#) confirmed that the compromise of a single employee email account was connected to an alleged leak of approximately one terabyte of data advertised on the dark web. Reports indicated that the material may include sensitive customer information such as Aadhaar-related records, although the precise scope and authenticity of the full dataset remained under forensic investigation. The bank stated that its core banking environment was not compromised and filed a cyber-insurance claim while investigating the incident. The case demonstrates how one cloud or email identity can expose large quantities of files and communications even when transaction-processing infrastructure remains intact.

South Korea Fines KT Over Data Theft and Unauthorized Payments

+South Korea +Telecommunications +KT Corporation +Payment Fraud +Regulation

- South Korea's Personal Information Protection Commission imposed a fine of approximately 54 billion won on telecommunications provider [KT Corporation](#) over security and reporting failures tied to a customer-data breach. The investigation found that personal and payment information belonging to more than 16,600 mobile customers was exposed during incidents in 2024 and 2025, resulting in approximately 240 million won in unauthorized transactions. Regulators also reportedly identified multiple malware infections on KT servers and concluded that the company failed to report the breach as legally required and attempted to conceal aspects of the incident. The penalty is a significant enforcement action for Asia's telecommunications sector and highlights the regulatory consequences of delayed notification and inadequate malware detection.

Houston City College Leak Exposes 832,000 Student and Alumni Accounts

+United States +Education +Houston City College +ShinyHunters +Extortion

- Have I Been Pwned added a [Houston City College](#) dataset containing approximately 831,600 unique email addresses following a ShinyHunters pay-or-leak extortion campaign. The publicly released records included names, dates of birth, physical addresses, phone numbers, academic records, citizenship status, gender, and other information relating to current students and alumni. Approximately 30% of the email addresses were reportedly already present in Have I Been Pwned from previous incidents, demonstrating the continuing accumulation and reuse of exposed identities across breaches. The intrusion occurred in June, but the dataset's validation and addition to breach-monitoring services on July 28 materially expanded awareness of its scale and content.

SplitVPN Breach Exposes Email, IP, Location, and Payment Data

+Russia +VPN +SplitVPN +Privacy +Payment Cards

- Russian VPN provider [SplitVPN](#), previously known as NotVPN, suffered a breach exposing millions of customer records and approximately 865,000 unique email addresses. Compromised information included customer IP addresses, countries, and partial payment-card data consisting of the first six and last four digits and card-expiration dates. VPN providers occupy a particularly sensitive trust position because IP and geographic information may undermine customers' expectations of anonymity and can support profiling or targeted phishing. Have I Been Pwned listed the breach on August 1.

Analog Devices Confirms Corporate File Theft

[+United States](#) [+Semiconductors](#) [+Analog Devices](#) [+Intellectual Property](#) [+Data Breach](#)

- Semiconductor manufacturer [Analog Devices](#) disclosed that an unauthorized party accessed company systems and exfiltrated files before the intrusion was detected on June 23. The company had not publicly identified the type or volume of information stolen but stated that operations were unaffected and that it did not expect a material financial impact. Analog Devices produces components used in industrial automation, automotive platforms, communications infrastructure, healthcare equipment, aerospace systems, and data centers, making stolen technical or commercial data potentially relevant across multiple global supply chains. The company was also assessing a separate matter connected to public extortion claims, though it was unclear whether the incidents were related.

Fairlife Confirms Data Theft During Production-Disrupting Ransomware Attack

[+United States](#) [+Food & Beverage](#) [+Fairlife](#) [+Coca-Cola](#) [+Ransomware](#)

- Coca-Cola confirmed that attackers stole data from its [Fairlife](#) subsidiary during the ransomware incident that temporarily suspended U.S. dairy production earlier in July. By July 27, most production had resumed, but restoration work continued for some affected systems and operations. The confirmation shifts the incident from a purely operational ransomware event to a combined disruption and data-theft breach, potentially enabling extortion even after manufacturing systems recover. Coca-Cola had not yet disclosed the scope or type of stolen information in the available reporting.

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.