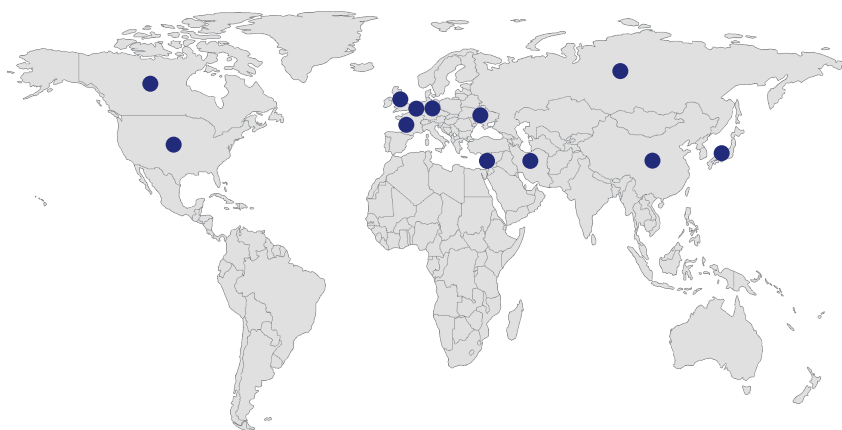


Threat Intel Report: August 17-23, 2026

Top Tags



MoYu

Executive Summary

- **Critical infrastructure and operational technology remain under direct pressure from both state-linked and criminal activity.** This week included disruption of a U.K. power-generation facility, AI-assisted attacks against Siemens PLCs, and continued ransomware targeting of U.S. critical infrastructure. The common thread is increasing attacker willingness to move beyond enterprise IT and target systems with real-world operational consequences.
- **Attackers are increasingly abusing trusted enterprise and software ecosystems to gain scale.** Supply-chain compromise affected Rust packages and automotive update infrastructure, while campaigns involving Microsoft Teams, cloud credentials, and third-party software demonstrate that legitimate platforms are being used as delivery, persistence, and access mechanisms. These attacks are particularly difficult to detect because they exploit trust relationships rather than obviously malicious infrastructure.
- **Identity and credential theft continue to underpin both espionage and financially motivated intrusion.** SynkLoader uses help-desk impersonation to capture credentials, ToxicPanda targets financial authentication data, and long-lived AWS keys remain valid years after exposure. At the same time, threat actors such as Cavern Manticore and Medusa are pairing credential access with persistent espionage or extortion objectives.
- **Data breaches are increasingly creating secondary risk through concentrated identity, healthcare, government, and cloud data.** The French Education Ministry, Sakura Internet, CareCloud, Philips, and SickKids incidents show how a single compromise can expose large populations or sensitive organizational information, while attacker claims involving Azure identities demonstrate the monetization value of aggregated workforce data. These incidents create follow-on risk for phishing, credential abuse, fraud, and targeted social engineering even when core systems remain operational.

Outlook:

The dominant trend this week is the continued convergence of operational disruption, identity compromise, and trusted-platform abuse. State-linked and criminal actors alike are increasingly targeting infrastructure that offers leverage beyond a single endpoint, including PLCs, software update mechanisms, collaboration platforms, cloud credentials, and centralized enterprise services. At the same time, the persistence of ransomware, mobile banking malware, and large-scale data theft suggests that attackers will continue to blend espionage, extortion, and fraud rather than operate within clearly separated categories. Looking ahead, organizations should expect faster exploitation of exposed infrastructure, more abuse of legitimate software and SaaS ecosystems, and greater use of stolen identity data to support follow-on attacks across both IT and operational environments.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,016% [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.

↑ 384% [CVE-2025-8943](#)

- The Custom MCPs feature is designed to execute OS commands, for instance, using tools like ``npx`` to spin up local MCP Servers. However, Flowise's inherent authentication and authorization model is minimal and lacks role-based access controls (RBAC). Furthermore, in Flowise versions before 3.0.1 the default installation operates without authentication unless explicitly configured. This combination allows unauthenticated network attackers to execute unsandboxed OS commands.

↑ 104% [CVE-2026-3055](#)

- Insufficient input validation in NetScaler ADC and NetScaler Gateway when configured as a SAML IDP leading to memory overread.

Recent Cyber Threats

Iran-Linked Cyberattack Shuts Down U.K. Power Plant for Four Days

+United Kingdom +Iran +Energy +Critical Infrastructure +Operational Technology

- A cyberattack attributed in media reporting to [Iran-linked hackers](#) forced a small U.K. power-generation facility offline for four days in July, with the incident publicly disclosed on August 23. The U.K. government confirmed that a small-scale generator was affected but said the attack never threatened the wider national energy system; the government and NCSC have since engaged energy operators on defensive measures. Officials have not publicly identified the facility, technical intrusion vector, or responsible actor, and the U.K. government has not formally attributed the attack to Iran. The incident is nevertheless significant because it demonstrates successful cyber disruption of physical energy production amid heightened geopolitical tensions involving Iran and Western governments.

Iranian Cavern Framework Expands Espionage Operations Against Israel

+Israel +Iran +Cavern +Cavern Manticore +Cyber Espionage

- Researchers detailed continued evolution of the [Cavern](#) command-and-control framework used by Iranian state-linked operators against Israeli entities. New components dynamically choose between direct HTTPS and Google Apps Script relays based on DNS A-record responses, while the related HOLLOWGRAPH module abuses Microsoft 365 calendar events and Graph API traffic as a covert two-way channel for commands and encrypted data exfiltration. Kaspersky linked the framework to Cavern Manticore, an

Iran MOIS-affiliated cluster overlapping MuddyWater and OilRig/Lyceum, while also observing modules for Active Directory reconnaissance, SQL enumeration, LDAP brute forcing, SOCKS5 tunneling, and file operations. The use of Microsoft and Google infrastructure allows malicious communications to blend into legitimate enterprise SaaS traffic and complicates network-based detection.

AI-Generated Exploit Scripts Target Siemens PLCs in Critical Infrastructure

+AI +Siemens +PLC +United States +Critical Infrastructure +OT

- The NSA, CISA, FBI, Department of Energy, and EPA jointly warned of ongoing attacks using [AI-generated scripts](#) against Siemens S7 Series programmable logic controllers deployed in U.S. critical infrastructure. The agencies said targeting extends beyond Siemens devices and affects PLC environments across critical manufacturing, energy, water and wastewater, chemical, food and agriculture, and commercial facilities. PLCs directly control physical machinery and industrial processes, giving successful attackers a potential path from cyber compromise into operational disruption. The advisory is a notable example of generative AI being used to accelerate attacks against operational technology rather than conventional enterprise endpoints.

Medusa Ransomware Has Hit More Than 500 U.S. Critical Infrastructure Organizations

+Medusa +Ransomware +United States +Critical Infrastructure

- CISA, the FBI, and the Department of Health and Human Services said [Medusa](#) ransomware actors have compromised more than 500 U.S. critical-infrastructure organizations since June 2021, up from approximately 300 reported in a March 2025 advisory. Affected sectors include healthcare and public health, the defense industrial base, critical manufacturing, government services and facilities, information technology, and financial services, with additional victims in education, legal, insurance, technology, and manufacturing. The operation uses ransomware and data-extortion tactics to pressure organizations following network compromise. The updated victim count demonstrates Medusa's sustained ability to penetrate high-value organizations across multiple regulated industries.

Hackers Poison Popular Rust Packages in Software Supply-Chain Attack

+Rust +Supply Chain +arrayref +Infostealer +Open Source

- Attackers compromised a maintainer account and published malicious versions of [three Rust crates](#)—arrayref, append-only-vec, and internment—within a 23-minute window. Arrayref alone recorded more than 53 million downloads during the preceding 90 days and is used in cryptography, graphics, and blockchain projects. The malicious releases introduced a dependency named proc-macro1, typosquatting the legitimate proc-macro2 package, which executed information-stealing malware during compilation while otherwise leaving upstream source code largely intact. The incident demonstrates the disproportionate reach available when attackers compromise trusted developer accounts within widely used open-source ecosystems.

SynkLoader Uses Microsoft Teams Help-Desk Phishing to Steal Credentials

+SynkLoader +Microsoft Teams +Phishing +Credential Theft +Social Engineering

- Researchers identified a previously undocumented malware family called [SynkLoader](#) being distributed through Microsoft Teams by attackers impersonating corporate IT help desks. Victims are directed to install a fake “PowerShell Cleaner” MSI hosted on Microsoft Azure, after which the malware displays a counterfeit Windows lock screen designed to capture credentials. File metadata indicates the malware was first compiled and distributed around July 28, while the attack method builds on the growing use of Teams chat and voice interactions for interactive social engineering. Hosting the payload on Azure and impersonating internal IT personnel increases the perceived legitimacy of the attack chain.

CameraSwarm Compromises More Than 14,500 Dahua Cameras

+CameraSwarm +Dahua +Ukraine +Russia +IoT

- A 35-day campaign dubbed [CameraSwarm](#) compromised more than 14,500 Dahua IP cameras, with the majority located in Ukraine and Russia. The operation ran from June 17 through July 22 and combined vulnerability exploitation, credential brute forcing, and use of offline recovery codes derived from camera serial numbers. Researchers recovered 407 MB of exposed attacker data comprising 2,616 files in 234 directories, including source code, credentials, exploitation results, camera images, logs, and shell history. The scale of the campaign illustrates how internet-facing surveillance infrastructure can be systematically compromised through a mixture of software weaknesses and account-recovery abuse.

Automotive Supply-Chain Attack Turns Android Car Systems Into Proxy Nodes

+China +MoYu +BadBox +Automotive +Supply Chain +Android

- Researchers have uncovered the first documented malware infection chain designed specifically for [Android-based automotive head units](#), targeting devices produced by Chinese vendor DoFun. Attackers associated with the MoYu group compromised the legitimate TWCore update application to distribute JarService malware, which downloads additional payloads and can execute arbitrary modules, perform HTTP requests, and collect device information. The campaign primarily installs a reverse-proxy component that turns vehicle head units into residential proxy nodes and also supports advertising fraud; researchers found no evidence of interference with driving or safety-critical vehicle controls. DoFun told Kaspersky that it had resolved the issue after notification.

ToxicPanda 2.0 Targets 349 Financial Apps Across 16 Countries

+ToxicPanda +Android +Banking Trojan +Mobile +Credential Theft

- The latest [ToxicPanda 2.0](#) Android banking malware targets 349 banking, cryptocurrency, financial, and e-wallet applications across 16 countries and supports 167 remote commands. The malware creates a local VPN interface to block communications with Google Play and Play Services, potentially interfering with Play Protect, application verification, and security updates before installing its payload. It also automates Wireless ADB pairing through Accessibility permissions to obtain shell-level access, harvests device PINs and passwords, and uses invisible overlays against targeted financial applications. A separate PIN-harvesting module targets 140 applications, demonstrating a substantial expansion of the malware's credential-theft and remote-control capabilities.

Thousands of Exposed AWS Keys Still Provide Administrative Cloud Access

+AWS +Cloud Security +Credentials +Secrets +IAM

- Researchers identified more than [9,300 AWS access keys](#) exposed publicly between August 2022 and August 2026 that remained valid at the time of testing. Reporting on the research indicated that hundreds of the credentials were associated with corporate environments, including root and highly privileged IAM keys capable of granting extensive control over AWS resources. Long-lived exposed credentials can allow attackers to access data, create infrastructure, alter permissions, or abuse cloud compute without exploiting a software vulnerability. The findings highlight persistent failures to rotate secrets after public exposure and the continued risk of credentials committed to repositories, development systems, and other public sources.

Berlin Cyberattack Forces Two State Ministries Off Government Network

+Germany +Government +Berlin +Public Sector

- [Berlin](#) disconnected two major Senate departments from the state government's shared IT network after forensic investigators identified a compromise affecting the environment. The departments responsible for urban development, housing, mobility, transport, climate, and environmental policy lost normal internet, email, and remote-work access, forcing employees to rely on alternative communications while investigators contained the incident. Some citizen-facing processes, including housing-benefit and education-assistance applications, were reportedly disrupted because they depend on systems within the isolated environment. Berlin police, prosecutors, the Federal Office for Information Security, and a state crisis team are investigating, while authorities have not yet disclosed the attack vector, attribution, or whether data was exfiltrated.

Data Breaches

French Education Ministry Hackers Claim Data on Millions of Students

+France +Government +Education +ZeroBytes +Data Breach

- [ZeroBytes](#), the group claiming responsibility for the recent French tax-authority breach, said it also obtained information from France's Ministry of Education covering millions of students and tens of thousands of teachers. The group claimed to possess approximately 346 million rows of data spanning more than 20 years, sourced from the Siecle student-management system; samples reviewed by Le Monde reportedly contained recent addresses, email addresses, phone numbers, class information, indicators concerning vulnerable students, teacher comments, and educator records. The incident appears connected to an earlier ministry compromise disclosed in July that authorities initially believed primarily affected employee information. France's Education Ministry is investigating, so the attacker's full figures and nationwide scope should remain characterized as claims rather than confirmed totals.

Sakura Internet Breach Potentially Affects 1.36 Million Accounts

+Japan +Cloud +Sakura Internet +Data Breach +Technology

- Japanese cloud and data-center provider [Sakura Internet](#) disclosed unauthorized access to its sales-management system, potentially affecting 1,360,563 customer and member accounts. Attackers accessed the environment on August 9 during an incident discovered while Sakura was investigating a separate compromise of its rental-server service involving 583 unauthorized account logins and malware installation. The larger system stores customer contract and membership information; Sakura said passwords are hashed and the affected system does not hold payment-card data, while actual exfiltration had not yet been confirmed. Sakura is strategically significant in Japan because it provides hosting, VPS, cloud, data-center, and GPU services and has been selected as a domestic provider for Japan's Government Cloud program.

CareCloud Breach Affects 3.76 Million Patients

+United States +Healthcare +CareCloud +AWS +Patient Data

- Healthcare technology provider [CareCloud](#) reported that 3,756,469 individuals were affected by a March intrusion into one of its AWS environments. Attackers had access between March 10 and March 16 and claimed to have exfiltrated database information, while the incident also caused an approximately eight-hour disruption to one of CareCloud's six electronic-health-record environments. CareCloud provides EHR, medical billing, practice-management, and revenue-cycle services, meaning many affected patients may have had no direct relationship with the company itself. Public notification material confirms exposure of names but does not yet specify the complete set of compromised data fields, and no ransomware or extortion group had publicly claimed responsibility at reporting time.

Philips Confirms Breach as Clop Targets Windchill Customers

+Netherlands +Philips +General Electric +CIoP +Manufacturing

- [Philips](#) confirmed that attackers compromised an enterprise server containing internal information, while General Electric separately said it was investigating Clop's claim that company data had been stolen. Philips said the compromise was contained and did not affect customer environments, while GE had not confirmed the attacker's assertions. Both organizations were named during Clop's broader data-theft campaign against PTC Windchill and FlexPLM deployments, alongside companies including Shell. Researchers subsequently identified a custom Java webshell designed specifically for these platforms, with functionality to decrypt credentials, enumerate Windchill file repositories, and systematically steal files.

Hacker Claims 3.6 Million Azure Identity Records Stolen From Major Companies

+Microsoft Azure +Identity +Cloud +Credential Theft +Data Breach

- A threat actor using the alias [TheHatman](#) offered approximately 3.6 million alleged employee records from multiple major companies for sale after reportedly obtaining access to Azure and Entra environments with compromised credentials. Named organizations included McDonald's, Vodafone, Kyndryl, HCL Technologies, IHG Hotels & Resorts, Gap, Hexaware, and Wyndham, with reported fields including employee names, email addresses, phone numbers, physical addresses, job titles, departments, group memberships, and service or administrator accounts. Researchers reviewing samples assessed that some data appeared authentic but found no indication of a broad Microsoft Azure platform vulnerability, making stolen credentials a more plausible entry vector. Because several organizations had not independently confirmed compromise, the record count and complete victim list should be treated as attacker claims.

SickKids Employee Data Exposed Through Third-Party Software Flaw

+Canada +Healthcare +SickKids +Third-Party Risk

- [Toronto's Hospital for Sick Children](#) disclosed that a vulnerability in an unnamed third-party software application allowed unauthorized access to personal information belonging to some current and former employees and job applicants. SickKids temporarily took its public Careers website offline while investigating but said clinical systems and patient records were not affected. The hospital suggested that the same application is used by other organizations, raising the possibility of a broader campaign against users of the vulnerable software. At publication, SickKids had not disclosed the vulnerability, vendor, number of affected individuals, or complete set of exposed personal information.

Fanlore Breach Exposes 145,000 Accounts and Password Hashes

+Fanlore +OTW +Passwords +Data Breach

- The Organization for Transformative Works identified unauthorized access to its [Fanlore](#) wiki, resulting in exposure of approximately 144,500 unique email addresses. Compromised information included email addresses, usernames, names, and passwords stored using either MD5 or PBKDF2 hashing. OTW supplied the affected dataset directly to Have I Been Pwned, which added the incident on August 19. The presence of older MD5 password hashes increases credential-reuse risk for users whose passwords have not been changed across other services.

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.