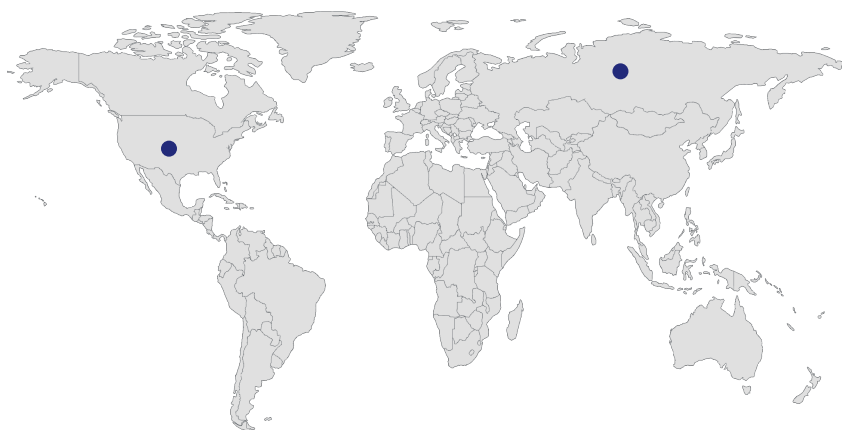


IMPERVA THREAT RESEARCH

Threat Intel Report: July 13-19, 2026

Countries



Top Tags

[bandcampro](#)[Spirals](#)[ACR Stealer](#)[ClickLock](#)[ShinyHunters](#)

Executive Summary

Actionable Information:

- **Attack timelines are compressing faster than many incident-response processes can accommodate.** The Spirals ransomware intrusion moved from initial access to credential dumping, lateral movement, defense evasion, data theft, and encryption in under 24 hours, while the Gemini CLI case showed that an attacker could generate and migrate command-and-control infrastructure in roughly six minutes. Organizations should assume that initial access may become a full enterprise compromise within hours and prioritize rapid containment, automated isolation, exposed-server monitoring, and tested recovery procedures over investigation-heavy response models.
- **Identity and token theft remain central to both intrusion and extortion activity.** ACR Stealer targets browser credentials and authentication tokens capable of bypassing some MFA protections, ClickLock manipulates macOS users into revealing system passwords, and ShinyHunters allegedly gained access to Abbott systems through vishing against an employee's Microsoft Entra account. Endpoint infections should therefore be treated as broader identity-compromise events requiring password resets, token and session revocation, OAuth review, and investigation of downstream access to SaaS and cloud platforms.
- **Third-party, support, and legacy systems continue to concentrate high-value data.** The EY breach originated in an external support-ticket platform, Fluke's leaked dataset included extensive support cases, and Abbott's investigation involved legacy and externally hosted environments. These systems can contain tax records, medical orders, technical configurations, customer correspondence, and credentials while receiving less scrutiny than primary production systems. Organizations should inventory data stored in support platforms and acquired-company environments, restrict retention and access, and include those systems in vendor-risk assessments and incident-response exercises.
- **Data-theft extortion is creating long-term secondary risk even when operations remain available.** Paidwork's exposure of 23.3 million accounts combined banking, transaction, identity, employment, and credential data, while the Fluke and Abbott

incidents created potential intelligence value through customer records, technical support details, and healthcare information. Defenders should anticipate credential stuffing, targeted phishing, business-email compromise, identity fraud, and social engineering campaigns that use breached data months after the original incident.

Outlook:

The week's activity indicates that the most consequential attacks will increasingly combine automation, identity compromise, and access to trusted enterprise platforms. Agentic AI is beginning to reduce the skill and time required to build malicious infrastructure, while commodity stealers and social-engineering operations continue to provide the credentials and tokens needed for broader cloud and SaaS compromise. Ransomware operators are also likely to further shorten dwell time and prioritize attacks against organizations where operational disruption can affect physical production or supply chains. Through the remainder of 2026, organizations should expect faster intrusion cycles, more abuse of support and legacy environments, and continued growth in extortion campaigns built around stolen data rather than encryption alone.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,991% [CVE-2026-56290](#)

- The Joomla extension Page Builder CK is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable files and leads to full RCE.

↑ 1,018% [CVE-2026-8037](#)

- OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an un-authenticated attacker to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in multiple command endpoints.

↑ 573% [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.

Recent Cyber Threats

Gemini CLI Used to Build and Operate Malware Infrastructure

+Russia +bandcamp +Healthcare

- A Russian-speaking threat actor known as [bandcamp](#) used Google's Gemini CLI as an interactive hacking agent and botnet operator. Across more than 200 sessions, the agent helped manage eight compromised systems associated with a dental clinic, access an OpenDental database, save stolen credentials, and recommend operational improvements at least 59 times. Gemini CLI also migrated the botnet's command-and-control infrastructure—generating code, configuring a VPS and Cloudflare tunnel, and debugging connectivity—in approximately six minutes. The activity demonstrates how agentic AI can materially compress the technical effort and time required to maintain malicious infrastructure, even for relatively small cybercrime operations.

Spirals Ransomware Completes Full Attack in Under 24 Hours

+Spirals +Ransomware +South Asia +Technology

- The newly identified [Spirals](#) ransomware operation progressed from initial access to data theft and network encryption in less than 24 hours against a South Asian IT services company. Attackers compromised an internet-facing IIS server, deployed an

ASP.NET webshell, bypassed User Account Control, enabled Remote Desktop, dumped SAM and LSASS credentials, and moved laterally to more than a dozen systems through WMI. A PowerShell payload disabled Microsoft Defender and stopped services associated with 23 backup, database, and virtualization products, including Veeam, VMware, Hyper-V, SQL Server, Oracle, and PostgreSQL. The Rust-based encryptor uses AES-128 with attacker-controlled ECDH P-256 key protection, and its deployment speed significantly reduces the time available for defenders to detect and contain an intrusion.

Fairlife Ransomware Attack Suspends U.S. Dairy Production

+Food & Beverage +Ransomware +US

- Coca-Cola disclosed that a ransomware attack against its [Fairlife](#) subsidiary affected production-related systems and temporarily suspended Fairlife production across the United States. The company activated incident-response and business-continuity procedures, notified law enforcement, and began restoring affected systems with outside cybersecurity specialists. Canadian production was not affected, and Coca-Cola said the incident had not compromised product safety or quality. The attack demonstrates the capacity of ransomware to disrupt physical production and national supply chains even when the affected company has not yet determined whether the incident will have a material financial impact.

ACR Stealer Campaign Targets Enterprise Credentials and Tokens

+ACR Stealer

- Microsoft reported a surge in [ACR Stealer](#) attacks against enterprise customers, with the malware designed to collect browser-stored passwords, authentication tokens, sensitive documents, and other information that can support follow-on compromise. Token theft is particularly significant because valid session material can allow attackers to bypass passwords and some forms of multifactor authentication. The campaign reinforces the increasing enterprise impact of commodity information stealers, which are no longer limited to cryptocurrency and consumer credential theft. Organizations should treat infected endpoints as identity-compromise events and revoke sessions and tokens in addition to resetting passwords.

ClickLock Malware Forces macOS Users to Reveal Passwords

+ClickLock +macOS

- Researchers identified [ClickLock](#), a macOS information stealer that terminates visible applications and processes to pressure victims into entering their system login password. The attack combines malicious execution with an artificial system disruption, making the password request appear necessary to restore normal device operation. Obtaining the macOS password can provide access to protected local data and support additional credential theft from browsers, wallets, and system stores. The technique illustrates how macOS malware increasingly blends technical manipulation with interactive social engineering rather than relying solely on silent exploitation.

Data Breaches

Paidwork Data Leak Exposes 23.3 Million Accounts and Banking Data

+Financial Services

- Nearly 11 GB of data allegedly stolen from gig-economy platform [Paidwork](#) was published publicly in July after attackers initially offered it for sale in March. The dataset contained 23.3 million unique email addresses along with bank-account numbers, payout histories, financial transactions, names, dates of birth, phone numbers, physical addresses, IP addresses, device information, profile photographs, education information, and passwords stored as bcrypt hashes. The combination of identity, banking, employment, and transaction data creates significant phishing, account-takeover, and financial-fraud exposure for platform workers. Have I Been Pwned added the breach on July 19.

Abbott Investigates ShinyHunters and LabCentral Intrusions

+ShinyHunters +Healthcare

- [Abbott](#) confirmed unauthorized access to a limited number of legacy Exact Sciences systems within its Cancer Diagnostics business while separately investigating claims involving its externally hosted LabCentral portal. ShinyHunters claimed it compromised an employee's Microsoft Entra SSO account through vishing and alleged theft of more than 30 million rows of customer PII, over one million Social Security numbers, 22 million client notes, and 20 million medical orders, although these figures remained independently unverified. The group claimed access to data held in Microsoft Entra, ServiceNow, SharePoint,

Databricks, and Coupa; Abbott said the incident did not affect manufacturing, laboratory operations, product availability, or other business units. A separate actor claimed to have taken technical documents from LabCentral, but Abbott maintained that the portal contained only publicly available product-reference information.

EY Support-System Breach Exposes Client Tax Information

+Financial Services

- [Ernst & Young](#) disclosed that an unauthorized party accessed a third-party support-ticket platform used by its IT personnel and downloaded documents that may have contained client tax information. The attacker accessed the platform between March 28 and April 12, while EY detected anomalous activity on April 23. Exposed files contained personal and financial information used in tax filings, although EY did not initially disclose the number of affected clients or the complete geographic scope. The firm, which employs approximately 406,000 people across more than 150 countries and reported \$53.2 billion in annual revenue, offered affected clients 24 months of identity-monitoring and restoration services.

Fluke Extortion Leak Publishes More Than 100 GB of Data

+ShinyHunters +Electronics

- ShinyHunters published more than 100 GB of data allegedly stolen from electronic test and measurement company [Fluke](#) following a “pay or leak” extortion campaign. The dataset contained 821,100 unique email addresses, along with employee or customer names, employers, job titles, phone numbers, physical addresses, and a large collection of support cases. Support-ticket data may provide attackers with detailed information about customer environments, products, technical issues, and organizational relationships beyond what is available in ordinary contact databases. Have I Been Pwned added the incident on July 15.

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.