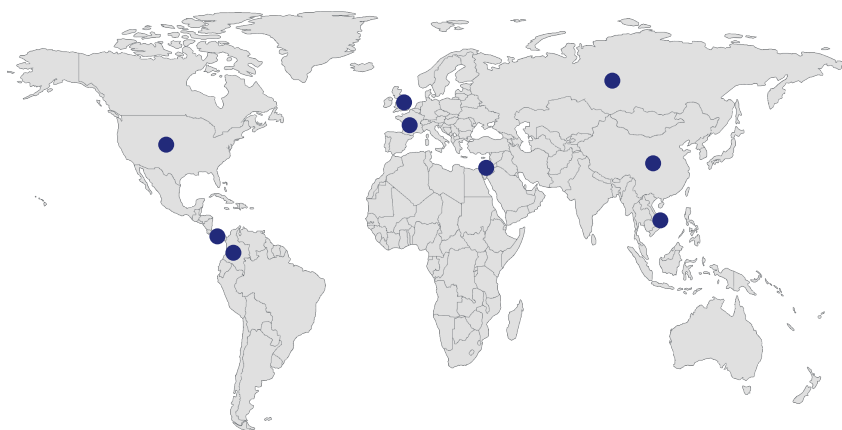


IMPERVA THREAT RESEARCH

Threat Intel Report: September 8-21, 2025

Countries



Top Tags

NoName057(16)

s1ngularity

Shai-Hulud

INC

ShinyHunters

Executive Summary

Actionable Information:

- **Law Enforcement and Hacktivism:** Takedowns like Operation Eastwood show that coordinated international actions can temporarily disrupt hacktivist groups, but these actors often rebound quickly with increased aggression and new alliances. Organizations should expect that disruption operations may reduce activity briefly but rarely neutralize a threat completely.
- **Financial and Identity Exploitation:** Attackers are chaining together weak verification processes, legacy data leaks, and overlooked user interface elements to perform account takeovers and SIM swaps. This highlights the continued fragility of static identifiers (last four digits, SSNs, ID numbers) as authenticators.
- **Software Supply Chain and Developer Risk:** Supply chain compromises (e.g., s1ngularity and Shai-Hulud) and vulnerabilities in developer tools (Cursor) demonstrate how adversaries are systematically targeting developers as an upstream gateway to broader compromise. The ability for malicious code to propagate automatically across repositories and packages amplifies risk across entire ecosystems.
- **Critical Infrastructure and Dependency Risks:** Attacks on aviation systems (Collins Aerospace outage) and vendor platforms (SonicWall) reinforce the fragility of global supply chains. Organizations dependent on third-party services must plan for resilience and fallback procedures.

Outlook:

The overall trend is one of increasing convergence between hacktivism, state-aligned espionage, and cybercrime, with each borrowing tactics from the other. Developers, vendors, and third-party service providers are being targeted at scale, amplifying systemic risk across industries. At the same time, attackers are innovating around authentication bypasses, exploiting the continued reliance on static data and weak identity checks. Looking ahead, organizations should expect more frequent supply-chain compromises, sharper focus on identity

exploitation, and persistent state-linked surveillance campaigns. Building resilience now requires stronger identity verification models, tighter vendor risk oversight, and deeper visibility into upstream code and service dependencies.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 1,381% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via completePath in the ProcessUtilities.outputExecutioner() sink. There is /filemanager/upload (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.

↑ 363% [CVE-2025-22457](#)

- A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.4, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

↑ 231% [CVE-2025-47227](#)

- In the Production Environment extension in Netmake ScriptCase through 9.12.006 (23), the Administrator password reset mechanism is mishandled. Making both a GET and a POST request to login.php is sufficient. An unauthenticated attacker can then bypass authentication via administrator account takeover.

Prolonged Application-Layer DDoS Targets U.S. Food & Beverage Site

+US +Food & Beverage +DDoS

- A US-based food and beverage site was targeted this past week with an application-layer DDoS attack reaching 2.77 million requests per second (RPS). Coming from just 275 IPs, the attack lasted over 17 hours in total, suggesting the attackers had both strong infrastructure control and clear intent to disrupt availability.

Brute-Force Login Surge Targets Colombian Financial Services Site

+Colombia +Financial Services

- A Colombian financial services platform was subjected to a high-volume account takeover (ATO) attempt, registering nearly 1.4 million login requests within a single hour. The attack was entirely brute-force login attempts, indicating that attackers were systematically testing stolen or guessed credentials to gain unauthorized access. Interestingly, the malicious traffic originated primarily from U.S.-based IPs, suggesting the use of compromised infrastructure, residential proxies, or hosting services to obscure the attackers' true location.

Recent Cyber Threats

Operation Eastwood: Long-Term Disruption or Temporary Pause for NoName057(16)?

+NoName057(16) +Russia

- In July 2025, Europol, Eurojust, and partner law enforcement agencies launched [Operation Eastwood](#), targeting NoName057(16) — a pro-Russian hacktivist group known for DDoS attacks on government and public infrastructure. The operation seized over 100 servers, arrested key members in France and Spain, and disrupted the group's support infrastructure (DDoS bots, volunteers). While the group tried to downplay the impact, there was a noticeable operational pause, followed by a rebound: after regrouping, they increased their attack rate by ~80%, expanding target numbers and forming new alliances under hacktivist

coalitions (e.g. Z-Alliance). The report concludes that Eastwood was a tactical win but not sufficient to eliminate the threat permanently.

The Hidden Last-Four: Google Pay, Bots & SIM Swaps Exploitation

+Israel +SIM Swap

- [Imperva researchers show](#) how a chain of weak linkages—old data leaks, lax SIM verification, and a vulnerability in the Google Pay “Pay” button iframe—can be exploited to facilitate SIM-swap and account takeover fraud. The Google Pay button, when a card is saved, reveals the last four digits of the card inside an iframe; attackers can crop and style this to look like a CAPTCHA challenge, harvesting those digits from unsuspecting users. Combined with static leaked personally identifying information (names, IDs) and loose telecom verification practices (in some countries), that bit of information becomes sufficient to bypass authentication systems or obtain SIM swaps. Imperva reported that Google removed the last-four-digits display in that button after being notified, but warns that many institutions still rely on similarly exposed static data, meaning this attack model could be quite broadly applicable.

“S1ngularity” Supply-Chain Attack Hits Thousands of GitHub/NPM Repos

+s1ngularity

- A supply chain attack dubbed [s1ngularity](#) compromised the Nx project by abusing a flawed GitHub Actions workflow, allowing a malicious version of an NPM package to be published. The injected malware (“telemetry.js”) stole credentials from Linux and macOS systems (GitHub tokens, SSH keys, etc.), and pushed the stolen secrets into public GitHub repositories. The attack affected 2,180 GitHub accounts and 7,200 repositories, many secrets still valid, and has prompted revocations of tokens, package takedowns, and tighter publishing controls.

Cursor Editor Flaw Permits Silent Repo-Triggered Code Execution

+Cursor +AI +Vibe coding

- A vulnerability in the [Cursor AI code editor](#) allows malicious repositories to trigger code execution automatically when a folder is opened. The issue arises because Cursor ships with Workspace Trust disabled by default, and certain repository tasks (via .vscode/tasks.json) configured with “runOn: folderOpen” can execute without user confirmation. This could result in credential theft, file modification, or further compromise, particularly in developer and CI/CD environments.

French Users Warned of Spyware Campaigns via Apple & CERT-FR

+France +iCloud

- [Apple](#), working with France’s CERT-FR, has issued multiple warnings this year (including September 3) to French users whose devices linked to iCloud may have been compromised. The attacks in question are highly sophisticated, often using zero-day vulnerabilities or requiring no interaction from the victim (zero-click). The targeted profiles include journalists, activists, lawyers, politicians, senior government officials, and similarly high-risk persons.

Shai-Hulud Worm Infects 180+ NPM Packages, Spreads Automatically

+Shai-Hulud +Worm +npm

- A self-replicating worm named [Shai-Hulud](#) has compromised over 180 npm packages, some with millions of downloads weekly. Once an infected package is installed, the worm harvests developer credentials (npm tokens, cloud API keys, etc.), exfiltrates them (including publishing them to public GitHub repos), then uses stolen credentials to infect other packages maintained by the same authors. The campaign marks a dangerous escalation: autonomous spread + code-supply chain compromise impacting a large part of the JavaScript ecosystem.

Data Breaches

Airport Check-in Systems Crippled by Collins Aerospace Outage

+Aviation

- A cyber-related disruption to [Collins Aerospace’s MUSE software](#) — used for electronic check-in, baggage drop, and boarding pass generation — forced major European airports (Heathrow, Brussels, Berlin, Dublin, etc.) to revert to manual processing.

Hundreds of flights were delayed or cancelled, with long queues and travel chaos over several days. The outage exposed a dependency risk on third-party systems for critical airport operations.

Leak Reveals China Selling Censorship Tech Globally

+China

- Over 500 GB of internal files from [Chinese entities](#) (including Geedge Networks and the MESA Lab) have been leaked, revealing how China's Great Firewall technology is being packaged and exported to other authoritarian regimes. The leaked material includes source code, technical documentation, and internal communications. This demonstrates not just domestic censorship but a global trade in censorship and surveillance technologies.

Nexar Dashcam Video Database Breached

+Software +AWS

- [Nexar's](#) systems were compromised through an improperly secured AWS bucket, exposing over 130 TB of video data from dashcams, including footage with identifiable faces and inside-vehicle views. The breach revealed that a high-privileged embedded key in each dashcam granted access to vast amounts of user data. Companies and public entities that subscribed to Nexar's data services (e.g. mapping, AI partners) may also be affected. Nexar has since secured the vulnerability.

Hello Gym Exposes Over 1 Million Audio Recordings Publicly

+Fitness

- A database managed by [Hello Gym](#), serving gyms and fitness centers, had over 1.6 million audio files (voicemails, calls) exposed without password protection. The recordings include personally identifiable information like names, phone numbers, reasons for calls, and span recordings from 2020-2025. The database was secured only after being externally reported, so duration and extent of malicious access are uncertain.

LunaLock's New Ransom Extortion: Art + AI Training Threat

+LunaLock +AI

- LunaLock targeted the [Artists&Clients](#) platform, stealing digital art and source code, and encrypted its data. Their ransom demand is ~\$50,000, but what makes it unusual is the added threat: if the ransom is not paid, stolen art will be used as AI-training data and public leaks will follow. This introduces a novel extortion vector, leveraging concerns over AI training and copyright, especially in creative communities.

Jaguar Land Rover Hit by Disruptive Cyberattack, Data Stolen

+Automotive +UK

- [Jaguar Land Rover \(JLR\)](#) suffered a cyberattack that forced shutdowns across its production lines and operations. The company confirmed some amount of data was stolen, though full details of which data or how many customers/suppliers are affected remain undisclosed. The attack also caused significant disruption to its supply chain and has triggered regulatory notifications.

French Healthcare Agencies Hit in Coordinated Regional Intrusions

+France +Healthcare

- Three [French regional healthcare agencies](#) (Hauts-de-France, Normandy, Pays de la Loire) have reported cyberattacks targeting servers holding patient identity data. The incidents compromised personally identifiable information (names, email addresses, etc.), but there is no confirmed evidence that clinical or medical records were accessed. The attacks appear coordinated or similar in nature across the regions.

Massive CIC Breach in Vietnam Exposes Credit Data on National Scale

+Vietnam +Government +Financial Services +ShinyHunters

- [Vietnam's National Credit Information Center \(CIC\)](#), operated by its central bank, was breached, with ShinyHunters claiming to have stolen over 160 million records—well beyond the country's population—suggesting inclusion of historical records or multiple entries per person. Authorities confirmed unauthorized access aiming at personal data, and have launched investigations. The service remains operational despite the breach.

Panama Finance Ministry Targeted by Ransom Group INC

+Panama +Government +INC

- [Panama's Ministry of Economy and Finance \(MEF\)](#) disclosed that a workstation in its infrastructure was compromised by the INC ransomware group. The attackers claim to have stolen over 1.5 TB of internal data—emails, financial documents, budgets—and

threatened to publish more unless contacted. Critical systems were not affected, and the breach was contained via security protocols.

Luxury Brands' Customer Data Compromised in ShinyHunters Attack

+[ShinyHunters](#) +[Retail](#) +[Luxury](#)

- ShinyHunters breached [Kering](#), parent company of Gucci, Balenciaga, Alexander McQueen, among others, accessing personal information (names, email addresses, phone numbers, home addresses, and spending history) for approximately 7.4 million customers. Financial data such as credit card info were reportedly not accessed. The breach raises concerns about risk of downstream phishing or identity misuse particularly among high-spending customers.

SonicWall MySonicWall Service Breach Exposes Firewall Config Backups

+[Firewall](#)

- SonicWall confirmed that attackers used brute-force attacks to access backup configuration files stored in its cloud backup service ([MySonicWall](#)) for a subset of its firewall customers (estimated <5% of install base). Though credentials in those files were encrypted, other details (network rules, service credentials, VPN configurations, etc.) may allow attackers to understand network topology or misuse configuration info for further attacks. The company is urging affected customers to reset credentials.

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.