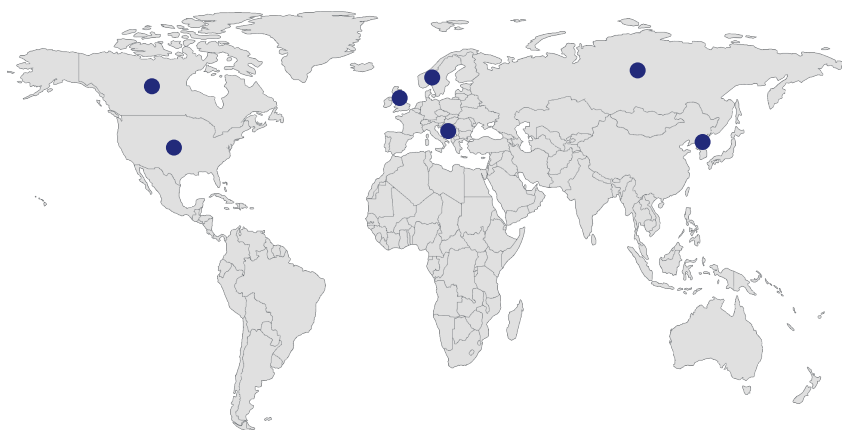


IMPERVA THREAT RESEARCH

Threat Intel Report: August 11-17, 2025

Countries



Top Tags

MadeYouReset

QUICLEAK

Kimsuky

WarLock

RomCom

Executive Summary

Actionable Information:

- **Protocol Exploitation:** Attacks like MadeYouReset (HTTP/2) and QUICLEAK (QUIC) show that flaws in core internet protocols can enable stealthy DoS and service crashes, demanding urgent patching and monitoring at the protocol layer.
- **Mass-Market Software Risks:** Common tools such as WinRAR, WordPress, and SharePoint remain high-value targets, with vulnerabilities exploited at scale by both cybercriminals and state actors.
- **Web & Ad-Based Delivery:** Malvertising and injected JavaScript are being weaponized to deliver multi-stage malware, enabling data theft and persistence through trusted user-facing platforms.
- **Data Exposure Across Sectors:** Sensitive data continues to be exposed across finance, government, and telecom sectors, reflecting weaknesses in third-party systems, cloud storage, and basic credential security.
- **Geopolitical Intrusions:** State-linked groups are escalating operations against Western governments and infrastructure, with disruptive attacks and leaks exposing espionage campaigns.

Outlook:

The current threat landscape underscores an accelerating convergence of state-backed espionage, criminal ransomware, and opportunistic exploitation of mass-market software. Protocol-level flaws (HTTP/2, QUIC) will drive a new wave of stealthy DoS and memory-based attacks that bypass traditional defenses, while common tools like WinRAR and WordPress remain prime entry points due to their ubiquity. Meanwhile, geopolitical tensions are clearly shaping targeting choices, with state actors seeking disruption and influence operations in Western infrastructure and government systems. In the near term, organizations should expect continued cross-pollination between crimeware and nation-state tactics, a rise in large-scale data exposures, and increased exploitation of core internet protocols and trusted platforms as attackers pursue both disruption and long-term access.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 4,679% [CVE-2024-27956](#)

- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Automatic allows SQL Injection. This issue affects Automatic: from n/a through 3.92.0.

↑ 1,850% [CVE-2025-31324](#)

- SAP NetWeaver Visual Composer Metadata Uploader is not protected with a proper authorization, allowing unauthenticated agent to upload potentially malicious executable binaries that could severely harm the host system. This could significantly affect the confidentiality, integrity, and availability of the targeted system.

↑ 1,316% [CVE-2024-5932](#)

- The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.14.1 via deserialization of untrusted input from the 'give_title' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely, and to delete arbitrary files.

2.9M RPS DDoS Hits Entertainment Platform During High-Profile Release

+Entertainment +DDoS

- An entertainment platform was hit with a 2.9 million RPS application-layer DDoS attack that persisted for nearly four hours, pushing sustained volumes well above typical baseline traffic. The assault originated from IPs with an average risk score of 49%, highlighting the use of moderately suspicious but not outright blacklisted infrastructure. The timing aligned with a high-profile content release, suggesting attackers may have been seeking to maximize disruption during peak audience engagement.

Recent Cyber Threats

MadeYouReset: A New Spin on HTTP/2 Resource Abuse

+MadeYouReset +HTTP/2 +DoS

- Researchers at Tel Aviv University and Imperva disclosed [MadeYouReset](#), a novel HTTP/2 DoS attack where the server is tricked into resetting its own streams, resulting in resource exhaustion without violating protocol rules. This attack targets internal discrepancies in stream lifecycle handling and is more stealthy than its predecessor, Rapid Reset, with broad impact across major HTTP/2 implementations.

LiteSpeed QUIC Memory Leak Exposes Pre-Handshake Attack Vector

+QUICLEAK +LSQUIC

- A memory leak in the `lsquic_engine_packet_in` function (prior to version 4.3.1) of the LiteSpeed QUIC (LSQUIC) library, dubbed [QUICLEAK](#), can be exploited during the pre-handshake phase to crash services. The flaw has high severity (CVSS 7.5) and requires no privileges, prompting urgent patching of affected versions.

Smart-Bus Systems Left Open to Tracking and Control

+IoT

- Security analysis revealed that [smart buses](#) rely on weak authentication and unencrypted communications, letting attackers track vehicles, control onboard systems, or spy on passengers. The flaws underscore a broader risk in IoT-enabled public transport and the critical need for encrypted, authenticated data flows.

WinRAR Zero-Day Exploited by Multiple Crime Rings

+Russia +RomCom +GOFFEE

- A high-severity zero-day vulnerability in [WinRAR](#) has been exploited in the wild by two independent Russian cybercrime groups (RomCom and GOFFEE) for several weeks, allowing remote attackers to execute arbitrary code when malicious archives are opened.

PS1Bot Malvertising Pushes Multi-Stage Malware via Ads

+PS1Bot +Malvertising

- Researchers uncovered the spread of [PS1Bot](#) via malvertisement campaigns, delivering Node.js-based payloads in multi-stage fashion. Victims are seeded with initial loaders that deploy follow-on modules—enabling stealthy data theft or further system compromise.

Rogue JavaScript Injects Fullscreen iFrame into WordPress Sites

+iFrame +WordPress

- Research has uncovered a campaign where malicious JavaScript forcibly injects fullscreen [iframes](#) into WordPress pages—often to display phishing or ad content overlaying real site UI. These injections exploit plugin or theme vulnerabilities to hijack user sessions, degrade trust, and drive traffic to illicit content.

Data Breaches

Connex Credit Union Breach Exposes 172,000 Members' Personal Data

+Financial Services

- [Connex Credit Union](#) discovered in early June that attackers accessed members' personal and financial data—including SSNs and debit card details—impacting approximately 172,000 people. The breach was detected almost immediately, but notification was delayed to late July. No funds were stolen, though Connex warned of potential phishing attempts using stolen data.

Kimsuky Hackers Turned In by Rogue Duo, 8.9 GB of APT Data Leaked

+Kimsuky +North Korea

- Two dissident hackers exposed 8.9 GB of internal data from North Korea's APT group [Kimsuky](#), unwittingly revealing tooling, stolen emails, phishing kits, and South Korean Ministry of Foreign Affairs source code. The leak, shared on DDoSecrets, may disrupt Kimsuky's ongoing campaigns by revealing infrastructure and methods.

Russian Cyber Espionage Suspected in PACER Court System Breach

+US +Russia +Government +Legal

- Sources say Russian government hackers infiltrated [PACER](#), the U.S. federal court filing system, potentially gaining access to sealed criminal dockets and confidential informant identities. The Judicial Conference confirmed the breach as a "persistent and sophisticated" cyberattack, prompting urgent remediation efforts to safeguard sensitive court records.

Interlock Ransomware Group Claims Massive Utah County Heist

+US +Government +Interlock

- The Interlock ransomware gang claimed responsibility for a cyberattack on [Box Elder County, Utah](#)—alleging theft of 4.5 TB across about 2.1 million files. The county confirmed service disruptions but hasn't yet verified whether the data claim or ransom demand is legitimate, and the investigation remains ongoing.

Croatian Research Institute Falls Victim to SharePoint Exploit

+Croatia +Education +SharePoint

- The [Ruđer Bošković Institute](#) (RBI), a Croatian science and technology research institute, confirmed a ransomware attack leveraging ToolShell SharePoint vulnerabilities, impacting administrative networks and encrypting documents. The institute is

restoring from backups and rebuilding infrastructure without paying ransom, while also investigating potential data exfiltration and notifying relevant authorities.

Pro-Russian Hackers Trigger Dam Water Release in Norway

+Norway +Russia +Infrastructure

- Norway's [Police Security Service](#) (PST) confirmed that pro-Russian hackers manipulated a dam's system to open floodgates, releasing 500 L/s for four hours in April. Though no harm occurred, the incident was most likely intended to demonstrate the attackers' disruptive abilities and send a political message.

Colt Telco Takes Systems Offline amid Cyber Incident

+UK +Telecommunications +WarLock

- UK telecommunications provider [Colt Technology Services](#) shut down internal system, disrupting customer portal and Voice API, as a protective response to a cyber incident. Ransomware group WarLock later claimed to be selling 1 million internal documents for \$200K, though Colt has yet to confirm data exfiltration.

Encrypted Chat App Archive Exposed 410 GB of White House Messages

+US +Government

- [TeleMessage](#), a messaging app used by White House officials, stored messages in plain text on its archive servers due to hardcoded credentials and debug hooks. Researchers accessed and published a 410 GB heap-dump database containing messages from institutions like CBP, JP Morgan, and law enforcement. CISA has since issued warnings and the flaws have been patched.

Canada's House of Commons Breached via Microsoft Vulnerability

+Canada +Government +SharePoint

- Attackers exploited a SharePoint deserialization flaw to breach the Canadian [House of Commons](#) IT system, accessing employee personal and device information. Canada's CSE is investigating, and officials have invoked mitigations—though attribution remains unclear between state or criminal actors.

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.