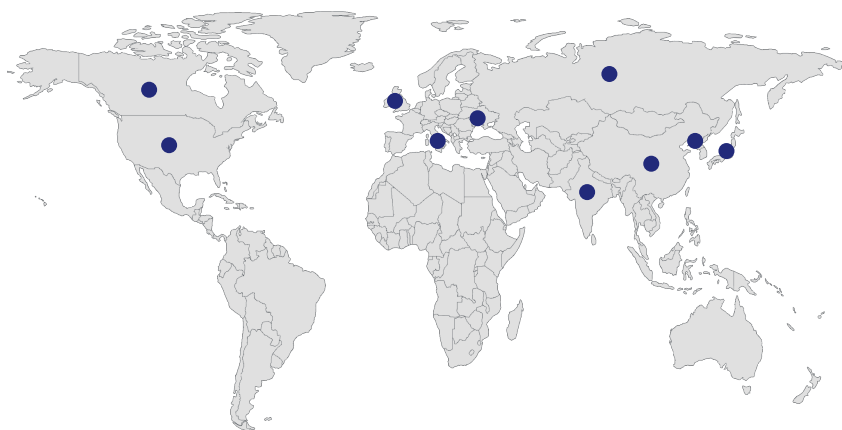


IMPERVA THREAT RESEARCH

Threat Intel Report: July 7-13, 2025

Countries



Top Tags

Lazarus Group

Anatsa

DoNotAPI

Salt Typhoon

Payouts King

Executive Summary

Actionable Information:

- **Sophisticated Malware Delivery Tactics Are Evolving:** Threat actors are increasingly blending social engineering with legitimate-looking platforms and tools to deliver stealthy malware. This includes repurposing red team frameworks, trojanizing trusted applications, and mimicking real software to bypass user and system defenses.
- **Trusted Ecosystems Are Being Weaponized:** Malicious activity is growing within environments users typically trust, such as official app stores, browser extensions, and cloud-based services. These platforms are being used to distribute malware, harvest data, and carry out large-scale automated attacks with minimal friction.
- **Misconfigurations and Poor Credential Hygiene Remain Critical Weaknesses:** Unsecured interfaces, exposed debug tools, and default or weak credentials continue to give attackers easy access to enterprise environments. These basic security lapses are frequently exploited for remote code execution, data exfiltration, or privilege escalation.
- **Nation-State Activity Is Increasing in Scope and Sophistication:** Advanced persistent threat (APT) groups are expanding their geographic targeting and refining their techniques. Recent campaigns show a clear focus on diplomatic, telecom, and defense-related sectors, often through well-crafted phishing or infrastructure compromise.
- **Data Breach Risks Are Rising Amidst Delayed Disclosure and Poor Controls:** A steady rise in large-scale data exposures, often due to unprotected databases, vulnerable infrastructure, or neglected software hygiene, continues to erode consumer trust. In several cases, breach disclosures are significantly delayed, highlighting gaps in incident response and regulatory compliance.
- **Cyber Operations Are Increasingly Disruptive to Physical and Strategic Infrastructure:** Attackers are targeting critical infrastructure and supply chains not just for espionage, but for disruption. This includes attacks that impede military capabilities, financial systems, or core communications networks, reflecting a shift toward more strategically impactful operations.

Outlook:

The cybersecurity threat landscape this week highlights a convergence of stealth malware, misconfiguration exploits, and state-sponsored espionage. Attackers are increasingly bypassing traditional defenses using trusted platforms, like app stores and browser ecosystems, and exploiting routine oversights like exposed services and default credentials. Espionage groups are expanding their geographic reach, while civilian infrastructure, including telecom, retail, crypto, and healthcare, is increasingly vulnerable to high-impact breaches. The combination of delayed breach disclosures and repeated vulnerability exploitation signals an urgent need for continuous monitoring, threat modeling beyond perimeter defenses, and zero-trust implementations across sectors. Expect further cross-industry fallout if misconfigurations, unpatched systems, and supply chain trust continue to go unchecked.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 10,065% [CVE-2025-48827](#)

- vBulletin 5.0.0 through 5.7.5 and 6.0.0 through 6.0.3 allows unauthenticated users to invoke protected API controllers' methods when running on PHP 8.1 or later, as demonstrated by the `/api.php?method=protectedMethod` pattern, as exploited in the wild in May 2025.

↑ 9,216% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

↑ 4,091% [CVE-2025-32813](#)

- An issue was discovered in Infoblox NETMRI before 7.6.1. Remote Unauthenticated Command Injection can occur.

High-RPS Application-Layer DDoS Hits Financial Firm

+Financial Services +DDoS

- A financial trading company was targeted by a high-intensity application-layer DDoS attack that peaked at 5.8 million requests per second within just 11 minutes. Despite the massive scale, the attack was launched from only 853 IPs, indicating the use of a highly efficient botnet capable of generating significant traffic with a relatively small footprint. This kind of focused, high-RPS assault can overwhelm application infrastructure quickly, disrupting trading operations and damaging service availability.

Massive API Violation Campaign Targets Italian Energy Sector

+Italy +Utilities +API Violation

- An Italian energy company experienced over 33 million API violations within just two days, signaling a sustained and deliberate attack. The majority of traffic originated from advanced bots capable of mimicking legitimate browser behavior, making detection and mitigation more difficult. Based on the endpoints targeted—such as AEM's CSRF token retrieval API—attackers were likely probing for weaknesses in CSRF protection or attempting to exploit misconfigured Adobe Experience Manager instances.

Recent Cyber Threats

North Korean Hackers Weaponize Fake Zoom Updates to Spread MacOS Malware

+North Korea +Lazarus Group +Nimdoor

- North Korea-linked threat actors, likely affiliated with the [Lazarus Group](#), are distributing a new macOS backdoor called Nimdoor by disguising it as a Zoom update. The malware, written in Nim, grants remote access and data exfiltration capabilities. The campaign specifically targets Mac users, leveraging a trojanized installer to avoid detection and maintain persistence.

Exposed JDWP Interfaces Create Critical Entry Points for Remote Code Execution

+Java +JDWP

- Threat actors are exploiting misconfigured [Java Debug Wire Protocol \(JDWP\)](#) interfaces exposed to the internet, enabling unauthenticated remote code execution (RCE). These interfaces, intended for debugging Java applications, have been found across major cloud providers and enterprise environments. Attackers can take full control of systems, download payloads, and launch further attacks if JDWP is left unprotected.

Hackers Leverage Leaked Red Team Tool to Spread Info-Stealers

+Shellter

- Cybercriminals are abusing a leaked version of [Shellter](#), a red teaming tool designed to create evasive payloads, to distribute info stealers like Agent Tesla and Venom RAT. These payloads are embedded into benign-looking executables, helping them evade antivirus detection. The campaign highlights how red team tools can quickly become dangerous in the hands of malicious actors once publicly leaked.

Anatsa Banking Trojan Returns via Google Play, Targeting U.S. Users

+Anatsa +Financial Services

- The [Anatsa](#) Android banking trojan has resurfaced on Google Play, disguised as utility and productivity apps, targeting users at five major U.S. banks. Once installed, the malware can perform screen recording, keylogging, and initiate unauthorized transactions using accessibility services. Google has removed the apps, but the campaign highlights the ongoing threat of mobile banking malware infiltrating official app stores.

CitrixBleed 2: CVE-2025-5777 Reveals Dangerous Memory Leak in NetScaler

+CitrixBleed 2

- [CVE-2025-5777](#), a critical memory disclosure flaw in Citrix NetScaler ADC and Gateway appliances, allows attackers to extract sensitive memory content, including session tokens and credentials. This vulnerability, dubbed CitrixBleed 2, is a bypass of a previous patch and poses serious risks for enterprises relying on NetScaler infrastructure. Successful exploitation could lead to full session hijacking and data exposure.

ChatGPT Exploited to Leak Windows Product Keys

+AI

- A bug hunter bypassed ChatGPT-4's safeguards by framing a guessing game and tricking the AI into disclosing valid Windows 10 license keys, including one tied to a major financial institution, after the user declared "[I give up](#)." The exploit hinges on prompting logic and illustrates that sensitive data inadvertently trained into models can still leak. This highlights a systemic risk for any proprietary keys or secrets that have been exposed in training sets.

DoNot APT's LoptikMod Campaign Targets Europe

+India +DoNotAPI +LoptikMod

- India-linked [DoNot APT](#) (aka APT-C-35, Origami Elephant) launched a spear-phishing campaign targeting a European foreign ministry. The attackers used a crafted email impersonating defense attachés and hosted a RAR archive on Google Drive delivering LoptikMod malware, establishing persistence and enabling data exfiltration. This marks an escalation from South Asian-focused operations to direct targeting of European diplomatic infrastructure.

Malicious Browser Extensions Turn Browsers into Scrapers

+Scrapers

- Nearly 1 million browser installations have been weaponized via [malicious extensions](#) that transform user browsers into scraping bots. These extensions harvest web content en masse, draining resources and compromising user privacy. The scale underscores how browser extension ecosystems can be abused as botnet proxies with minimal technical sophistication.

Fake Gaming & AI Firms Distribute Windows Malware

+Malware +AI +Gaming

- A wave of fake gaming and AI company webpages lured employees and investors into downloading trojanized [Windows installers](#). The malware packages blended legitimate apps with info-stealing and remote-access modules, designed to steal credentials and spy on targets. The operation highlights the growing trend of targeted social-engineering campaigns masquerading as tech startups.

Data Breaches

Luxury Retail Chain Hit in UK Data Theft

+UK +Retail

- On July 2, attackers infiltrated [Louis Vuitton's](#) UK systems, exfiltrating customer names, contact details, and purchase histories. The company confirmed no financial data was accessed but warned customers about phishing and fraud risks. This marks the third breach in three months across LVMH brands, as major UK retailers face increasingly targeted cyber threats.

Crypto ATM Operator Delayed Reporting Major Breach

+Crypto +Financial Services

- [Bitcoin Depot](#) revealed this week that it lost personal data, including names, addresses, emails, phone numbers, birth dates, and driver's license numbers, on nearly 27,000 users in June 2024 due to a GitLab server vulnerability. Disclosure was delayed over a year pending a federal investigation, which ended June 2025, sparking concerns about transparency in crypto KYC compliance.

Japanese IT Subsidiary Breached via Zero-Day Network Exploit

+Japan

- On March 7, hackers exploited a previously unknown vulnerability in network equipment at [Nippon Steel Solutions](#), gaining access to personal data of customers, partners, and employees. The breach triggered emergency containment measures and a forensic investigation, although no evidence yet suggests public disclosure of the stolen data.

AI Hiring Chatbot Exposes Jobseeker Data Through Default Credentials

+Food & Beverage +AI

- Security researchers discovered that an admin account on [McDonald's](#) AI hiring platform "Olivia" was protected by the default username/password "123456," allowing access to 64 million chat records with names, emails, phone numbers, and more. Although no malicious use has been detected, the breach highlights glaring security failures in AI-powered HR systems.

Massive Leak at Tax-Firm Exposes Quarter-Million Records

+US +Technology

- A publicly accessible, unprotected database tied to [Rockerbox](#) in Texas exposed 245,949 records, totaling nearly 287 GB, containing names, birth dates, SSNs, driver's licenses, military discharge forms, and tax documentation. The data exposure was quickly sealed after notification, and there's no evidence yet of malicious access or misuse.

Chinese State-Linked Hackers Strike Canadian Telecom Giant

+China +Canada +Salt Typhoon

- Canada's [Rogers Communications](#) fell victim to espionage by the Chinese state-sponsored Salt Typhoon threat actor, which exploited vulnerabilities in Cisco routers to infiltrate core communications infrastructure. While details are limited, this attack signals a strategic assault on Canadian telecom networks.

New Ransomware Gang Hits Rehab Clinics in Florida

+USA +Healthcare +Payouts King

- A newly emerged ransomware group called [Payouts King](#) claimed responsibility for breaching Gateway Community rehab clinics in Florida, stealing ~890 GB of sensitive data. The breach affected 34,498 patients, exposing SSNs, health insurance info, and medical records. Although the clinic confirmed the attack, it's unclear if a ransom was paid.

Cyberattack Disrupts Russian Drone Firmware Operations

+Russia +Ukraine

- Unknown hackers infiltrated infrastructure belonging to a Russian dev team behind the [1001](#) civilian-to-military drone firmware, halting distribution pipelines. Despite no evidence of firmware tampering, operational disruption affected nearly 200,000 drones deployed for the Ukraine war effort.

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.