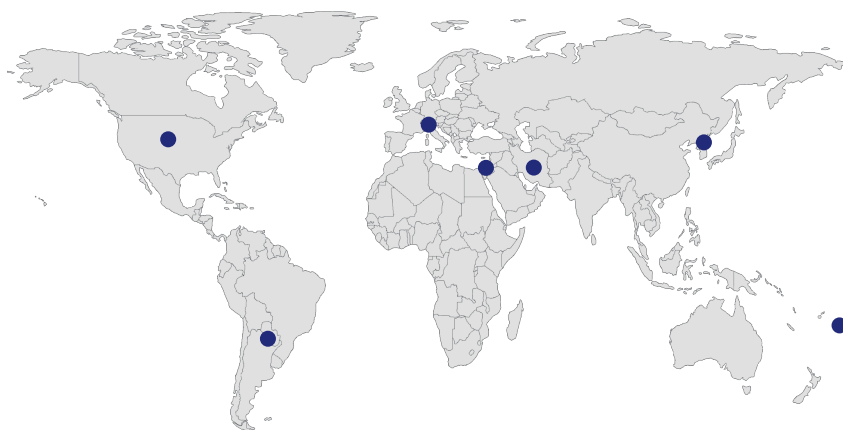


IMPERVA THREAT RESEARCH

Threat Intel Report: June 16-22, 2025

Countries



Top Tags

BlueNoroff

Kairos

Predatory Sparrow

Scattered Spider

BrigadaPMC

Executive Summary

Actionable Information:

- **Surge in Politically Motivated and State-Aligned Attacks:** Cyberattacks linked to nation-state actors intensified this week, notably from BlueNoroff (North Korea) and Predatory Sparrow (Israel). BlueNoroff used deepfake Zoom calls and macOS malware to target cryptocurrency holders, continuing their focus on financial theft through social engineering. Meanwhile, Predatory Sparrow disrupted Iran's Bank Sepah in a destructive attack likely tied to ongoing geopolitical tensions, impacting core banking services and ATM infrastructure.
- **Critical Infrastructure and Government Disruptions:** Government entities and public services remain prime targets. Ransomware incidents affected Taos County, NM and Tonga's Ministry of Health, paralyzing services and pressuring officials with ransom demands. In Paraguay, Brigada Cyber PMC leaked sensitive national data following an extortion attempt. These incidents highlight the vulnerability of under-resourced public-sector entities to high-impact breaches and ransomware.
- **Healthcare and Supply Chains at Risk:** A growing number of attacks hit healthcare and supply-chain infrastructure. World Leaks claimed a large data theft from Freedman HealthCare, potentially exposing sensitive U.S. state data. Separately, a cyberattack on UNFI—the main supplier for Whole Foods—disrupted nationwide food deliveries. These events underscore the ripple effect cyberattacks can have on essential services and consumer access.
- **Credential Leaks and Supply Chain Weaknesses:** Over 16 billion stolen credentials from infostealer logs were discovered online, posing immediate phishing and ATO (Account Takeover) risks. Simultaneously, UBS and Aflac reported data exposures stemming from third-party vulnerabilities and social engineering. These underscore ongoing gaps in vendor risk management and the need for multifactor authentication and continuous credential hygiene.

Outlook:

The cyber threat landscape this week emphasizes a dual challenge: the continued sophistication of nation-state and financially motivated groups, and the vulnerability of critical public infrastructure and supply chains. Threat actors are increasingly blending social engineering, deepfake technologies, and third-party exploitation to breach targets ranging from government agencies to large enterprises. We anticipate persistent and possibly escalating activity targeting healthcare, financial services, and government entities, particularly in geopolitically sensitive regions. Organizations must reinforce social engineering defenses, strengthen supply chain security controls, and prioritize rapid detection and incident response capabilities.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 510% [CVE-2024-8522](#)

- The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection via the 'c_only_fields' parameter of the /wp-json/learnpress/v1/courses REST API endpoint in all versions up to, and including, 4.2.7 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.

↑ 393% [CVE-2025-0107](#)

- An OS command injection vulnerability in Palo Alto Networks Expedition enables an unauthenticated attacker to run arbitrary OS commands as the www-data user in Expedition, which results in the disclosure of usernames, cleartext passwords, device configurations, and device API keys for firewalls running PAN-OS software.

↑ 257% [CVE-2024-53675](#)

- An XML external entity injection (XXE) vulnerability in HPE Insight Remote Support may allow remote users to disclose information in certain cases.

Israeli Websites See 87% Rise in DDoS Attacks

+Israel +Government +Financial Services +DDoS

- Israeli sites have been targeted by application-layer (L7) DDoS attacks this week at rates 87% higher than the previous week. The attacks, which primarily targeted government and financial services sites, were the highest since targeted attacks on a financial services site in late May.

US Retail Site API Site Targeted

+US +Retail

- A US retail site was targeted by API violations this week, reaching almost 5 million malicious requests in one day. The attacks, which came from bots, leveraged almost 12,000 IPs.
-

Recent Cyber Threats

BlueNoroff Deepfake Zoom Attack on macOS

+BlueNoroff +North Korea

- [BlueNoroff](#), a North Korean threat group, deployed deepfake video calls impersonating company executives on Zoom, delivered via Telegram invites that redirected macOS users to a fake Zoom domain. Once installed, customized Mac malware aimed for crypto theft, continuing their recent campaign targeting cryptocurrency assets.

“Covert Redirector” Malicious WordPress Plugin

+Malware +WordPress

- Researchers have uncovered a fake [WordPress Core](#) plugin that silently redirects visitors to malicious sites after 4–5 seconds, while admins remain unaffected. The covert redirector targets predominantly public-facing sites, injecting harmful URLs and evading detection by isolating its payload from privileged users.

Grocery Chain Hit by Supply-Chain Malware

+Food & Beverage +Supply-Chain +Malware

- On June 5, [United Natural Foods Inc.](#) (UNFI)—the primary distributor for Whole Foods and ~30,000 other grocers—was struck by a cyberattack that severely disrupted deliveries. The attack caused empty shelves at Whole Foods locations nationwide, exposing critical vulnerabilities in retail supply chains.

Predatory Sparrow Disrupts Iran’s Bank Sepah

+Israel +Iran +Predatory Sparrow +Financial Services

- On June 17, the pro-Israel hacker group [Predatory Sparrow](#) claimed and likely executed a destructive cyberattack on Iran’s Bank Sepah, disrupting ATMs, online banking, and card services. They also allegedly destroyed data. The attack is part of an intensifying cyber campaign amid regional conflict.

Data Breaches

Credential Dump Alerts: 16 Billion Logins Exposed

+Infostealer +Credential Dump

- Researchers discovered 30 datasets containing [16 billion login credentials](#)—mostly from infostealer malware logs and old breaches. The data exposed usernames, passwords, and URLs linked to platforms like Apple, Google, and Facebook. Though the datasets were briefly online and likely already in circulation, experts warn of phishing and account takeover risks; users are urged to reset passwords and enable multifactor authentication.

Massive Healthcare Data Heist at Freedman HealthCare

+World Leaks +US +Healthcare

- A new extortion platform, [World Leaks](#), claims to have stolen 52.4 GB (42,204 files) from Freedman HealthCare—a vendor for multiple U.S. state agencies—and threatened to leak the data imminently. The files likely include analytics dashboards, internal credentials, and state contracts, though the firm denies any exposure of protected health info. The breach risks sensitive citizen data across California, Delaware, Rhode Island, and more.

Kairos Ransomware Targets Taos County Government

+Kairos +US +Government

- Ransomware group [Kairos](#) claims it stole 1.94 TB of confidential documents—including records from a child sexual abuse case—from Taos County, New Mexico. They’ve issued a seven-day deadline for ransom payment or will release the data publicly. The county has not officially confirmed the attack, but samples have been released as proof.

Ransomware Shuts Down Tonga’s National Health System

+Tonga

- On June 15, an unnamed ransomware gang crippled [Tonga’s National Health Information System](#), taking down its website, patient records, prescribing tools, and prompting staff to revert to paper systems. The Ministry claims attackers demanded “millions” in ransom and enlisted Australian cybersecurity experts to aid recovery efforts.

Scattered Spider Hits Aflac with Social-Engineering Breach

+Scattered Spider +Financial Services

- [Aflac](#) confirmed it was breached on June 12 by a social engineering attack linked to the Scattered Spider gang. Intruders accessed customer data—potentially including Social Security numbers, claims, and health records—but did not deploy ransomware. The attack was swiftly contained, with Aflac offering credit monitoring and identity theft protection.

Third-Party Breach Exposes 130K UBS Staff Data

+Financial Services +Switzerland

- [UBS](#) confirmed that an external supplier, Chain IQ (with 19 entities affected), was compromised, leading to a leak of info on ~130,000 employees—names, emails, phone numbers, internal codes, and even the CEO's number—on the darknet. No client or account data was exposed, and UBS swiftly contained the incident.

Brigada Cyber PMC Breaches Paraguay Government

+Paraguay +BrigadaPMC +Government

- A cybercrime group exfiltrated PII from [Paraguay's Ministry of Health and Jury of Magistrates](#) on June 14 and posted it on X (formerly Twitter). Although officials claim containment, leaked citizen and magistrate data is already public. Five days earlier, Brigada Cyber PMC demanded \$7.4 million ransom, threatening to publish data on all 7.4 million citizens; the government refused.

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.