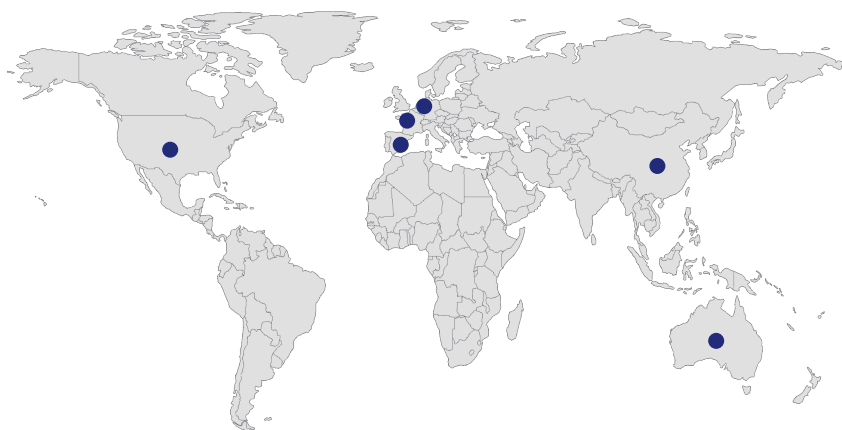


IMPERVA THREAT RESEARCH

Threat Intel Report: June 30 - July 6, 2025

Countries



Top Tags

AI

APT31

BrakTooth v2

Crypto

Dark Angels

Executive Summary

Actionable Information:

- **State-Backed Exploits Target Critical Infrastructure:** Nation-state actors, particularly APT31 from China, continue to exploit high-impact zero-days, targeting government networks to conduct cyber espionage and disrupt operations.
- **Supply Chain Risks Expand Across Industries:** Multiple incidents this week highlight the persistent risk of supply chain attacks, with breaches affecting payroll providers, loyalty program contractors, and software distribution channels, leading to significant data exposures.
- **Consumer-Facing Technologies Under Attack:** Attackers are increasingly abusing trusted consumer platforms, such as Bluetooth firmware, crypto browser extensions, and signed installers, to conduct stealthy attacks aimed at eavesdropping, credential theft, and malware deployment.
- **Healthcare and Retail Sectors Face Large-Scale Breaches:** Healthcare providers and retailers reported major breaches involving hundreds of thousands to millions of affected individuals, with stolen data ranging from personal identifiers to payment and medical records.
- **Resurgence of High-Impact Data Leaks:** Threat actors continue to leak stolen corporate and government data, increasing the risk of secondary attacks, fraud, and geopolitical tension, as seen with the International Criminal Court and telecom giant Telefónica.

Outlook:

The cybersecurity threat landscape remains highly active, with a clear uptick in sophisticated nation-state attacks targeting sensitive government and legal institutions, as well as rampant supply chain breaches affecting industries from healthcare to retail and travel. Attackers are leveraging both high-profile zero-days and softer supply chain vectors to maximize impact and evade detection. The frequency of credential harvesting campaigns, combined with widespread data leaks, suggests a heightened risk of phishing and fraud in the months

ahead, particularly as more stolen data circulates across underground forums. Organizations must prioritize software supply chain security, vendor risk management, and robust incident response capabilities to mitigate growing risks across all sectors.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 4,280% [CVE-2024-10924](#)

- The Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress are vulnerable to authentication bypass in versions 9.0.0 to 9.1.1.1. This is due to improper user check error handling in the two-factor REST API actions with the 'check_login_and_get_user' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, when the "Two-Factor Authentication" setting is enabled (disabled by default).

↑ 938% [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.

↑ 447% [CVE-2025-34028](#)

- The Commvault Command Center Innovation Release allows an unauthenticated actor to upload ZIP files that represent install packages that, when expanded by the target server, are vulnerable to path traversal vulnerability that can result in Remote Code Execution via malicious JSP. This issue affects Command Center Innovation Release: 11.38.0 to 11.38.20. The vulnerability is fixed in 11.38.20 with SP38-CU20-433 and SP38-CU20-436 and also fixed in 11.38.25 with SP38-CU25-434 and SP38-CU25-438.

Recent Cyber Threats

Hijacked Installer Exploited for Stealthy MacOS Attacks

+MacOS +AI +Vulnerability

- Imperva researchers discovered a vulnerability in [Ollama](#), an open-source AI tool for MacOS, allowing attackers to execute arbitrary malicious code during installation. The attack abuses macOS's trust in signed software, allowing malware to bypass security warnings and run stealthily. The malicious installer maintains all legitimate app functionality, making detection difficult.

Chinese Hackers Target French Government via Ivanti Zero-Days

+China +France +APT31 +Government

- Chinese state-sponsored group APT31 exploited multiple Ivanti Connect Secure and Policy Secure VPN zero-days to compromise [French government](#) entities. The attacks involved chaining CVE-2024-21887 and CVE-2023-46805 to gain system control, with exploitation seen as early as March. France publicly attributed the campaign to China, highlighting increasing cyber tensions.

Bluetooth Flaws Expose Devices to Audio Eavesdropping

+Bluetooth +BrakTooth v2

- Researchers revealed multiple vulnerabilities in [Bluetooth](#) firmware across major chipsets, including from Qualcomm and Broadcom, which could let attackers eavesdrop through microphones or crash devices. Dubbed "BrakTooth v2," the flaws impact a wide range of devices like smartphones, laptops, and IoT products, leaving millions potentially at risk. Firmware updates are required for mitigation, but patch availability varies by vendor.

Fake Crypto Wallet Extensions Flood Firefox Store

+Crypto +Firefox

- More than 30 [malicious browser extensions](#) mimicking legitimate crypto wallets like Binance, Bybit, and OKX were found in the Firefox add-ons store, aiming to steal users' wallet credentials. Once installed, these extensions harvest sensitive data and drain crypto funds. Mozilla has removed the add-ons, but similar campaigns continue to emerge.

Data Breaches

Healthcare Breach Exposes Over 263,000 Patients' Data

+US +Healthcare

- [Esse Health](#), a U.S. healthcare provider, disclosed a data breach affecting more than 263,000 patients after attackers accessed sensitive data like Social Security numbers and medical records. The breach occurred in March via unauthorized access to email accounts, raising concerns over patient privacy and phishing risks.

Johnson Controls Notifies Victims of 2023 Data Breach

+Technology +Dark Angels

- [Johnson Controls](#) has begun notifying individuals affected by its September 2023 ransomware attack, which disrupted operations and led to the theft of personal data, including Social Security numbers and banking information. The breach was linked to the Dark Angels ransomware group, with operational losses estimated at \$27 million.

ICC Cyberattack Likely Nation-State Espionage

+Legal +Government

- [The International Criminal Court \(ICC\)](#) confirmed its 2023 cyberattack was likely carried out by a nation-state, though it hasn't attributed responsibility. The attack targeted sensitive documents tied to war crimes investigations, suggesting motives related to espionage or legal obstruction. Forensic analysis confirmed network infiltration and data exfiltration.

2 Million Impacted in Dutch Retail Data Breach

+Food & Beverage +Netherlands +Technology

- [Ahold Delhaize](#), a major European grocery chain, reported a data breach affecting roughly 2 million Dutch customers after hackers accessed data via its loyalty program contractor. Exposed data includes email addresses and phone numbers, raising phishing concerns. The breach is linked to an incident at tech provider NEP Worldwide.

Qantas Data Theft Exposes Frequent Flyer Details

+Australia +Travel

- Australian airline [Qantas](#) disclosed a data breach exposing frequent flyer program member information, including names, statuses, and points balances. The stolen data was shared on a hacking forum, though Qantas says no financial data was involved. Investigations suggest a third-party compromise led to the incident.

Kelly Benefits Supply Chain Breach Affects Dozens of Firms

+US +Financial Services

- [Kelly Benefits](#), a U.S. payroll and benefits firm, confirmed a data breach affecting dozens of corporate clients due to a third-party software vulnerability. Attackers accessed personal and financial data of clients' employees, underlining the risks of vendor-linked supply chain attacks. The breach's full scale remains under investigation.

Hacker Leaks Data Stolen From Telefónica in Alleged New Breach

+Spain +Telecommunications

- A hacker leaked data allegedly stolen from [Telefónica](#), one of Spain's largest telecoms, including employee credentials and network details. Telefónica is investigating the breach, which reportedly stems from unauthorized access to internal systems. The leaked data could facilitate further attacks or fraud.

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.