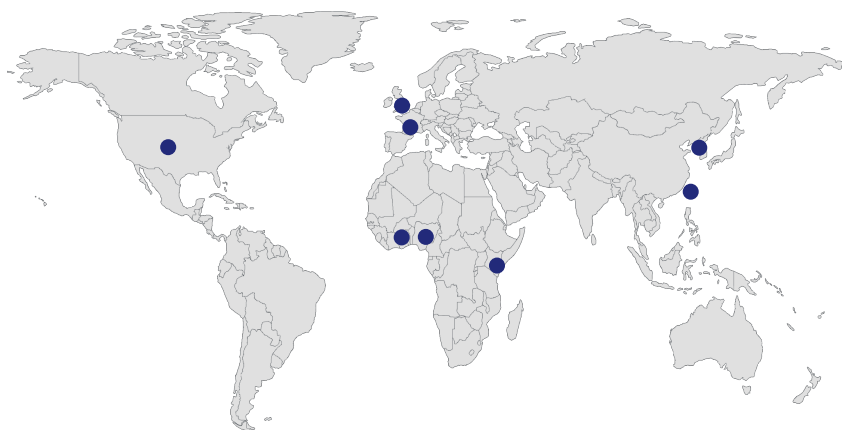


IMPERVA THREAT RESEARCH

Threat Intel Report: June 23-29, 2025

Countries



Top Tags

Androxxgh0st

ALPHV

Qilin

Anubis

Lazarus

Executive Summary

Actionable Information:

- **Ransomware continues to disrupt critical sectors**, with attacks affecting healthcare, logistics, and entertainment operations.
- **Nation-state activity remains high**, with Russian and North Korean groups conducting cyberespionage and financially motivated attacks.
- **Attackers are increasingly abusing trusted infrastructure**, including AI-generated content, search engines, and education networks, to deliver malware and steal credentials.
- **Financial institutions in emerging markets face targeted phishing campaigns**, capitalizing on weaker cybersecurity postures.
- **Malware targeting eCommerce platforms is on the rise**, exploiting popular CMS plugins to steal payment data and hijack SEO.

Outlook:

The past week reflects a cyber threat landscape where attackers are blending old tactics with new vectors, amplifying their reach and impact. Ransomware remains the most damaging threat, now extending its consequences beyond data loss to physical harm. Nation-state groups are simultaneously advancing strategic goals and generating revenue, while criminal actors leverage underprotected infrastructure and content manipulation to evade detection. As geopolitical tensions and global digitization continue to rise, organizations should anticipate more cross-sector targeting, faster malware evolution, and increasingly blurred lines between cybercrime and cyberwarfare.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 2,641% [CVE-2024-34102](#)

- Adobe Commerce versions 2.4.7, 2.4.6-p5, 2.4.5-p7, 2.4.4-p8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by sending a crafted XML document that references external entities. Exploitation of this issue does not require user interaction.

↑ 1,711% [CVE-2024-7928](#)

- A vulnerability, which was classified as problematic, has been found in FastAdmin up to 1.3.3.20220121. Affected by this issue is some unknown functionality of the file /index/ajax/lang. The manipulation of the argument lang leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.4.20220530 is able to address this issue. It is recommended to upgrade the affected component.

↑ 1,642% [CVE-2024-13159](#)

- Absolute path traversal in Ivanti EPM before the 2024 January-2025 Security Update and 2022 SU6 January-2025 Security Update allows a remote unauthenticated attacker to leak sensitive information.

Recent Cyber Threats

Russian APT Hits Ukrainian Government Networks with Malware

+Russia +Ukraine +Gamaredon

- Ukrainian government systems were targeted in a recent wave of attacks attributed to Russian-aligned threat group [Gamaredon](#), reportedly using phishing emails and malware implants. The campaign aimed at data exfiltration and continued cyber disruption of Ukraine's digital infrastructure. The attacks align with ongoing hybrid warfare strategies.

WordPress and WooCommerce Sites Compromised by Multifaceted Malware

+eCommerce +Retail +Malware

- A sophisticated malware campaign is targeting [WordPress and WooCommerce websites](#), infecting thousands of sites globally. The attackers inject malicious code to hijack search engine rankings and steal credit card data via fake checkout pages. The malware continuously evolves to evade detection and abuses legitimate plugins.

Androxgh0st Botnet Exploits University Servers for Cloud Credential Theft

+Androxgh0st +Botnet +US +Education

- The [Androxgh0st](#) botnet has expanded its operations by compromising U.S. university servers to steal cloud credentials and environment variables. The botnet leverages known vulnerabilities in Laravel, ThinkPHP, and Apache frameworks, using infected machines to scan for further targets. Its ultimate goal is hijacking cloud services for data theft and spam distribution.

Malicious SEO Campaign Uses AI to Spread Malware via Search Results

+SEO Poisoning +Malware +AI

- Threat actors are using [AI-generated blog content](#) to poison search engine results, tricking users into downloading malware disguised as legitimate software. The campaign targets tools like AnyDesk and Cisco Webex by mimicking their official download pages. Researchers warn this tactic is increasingly effective at driving organic traffic to malicious payloads.

Cybercriminals Target African Financial Institutions in Coordinated Campaign

+Nigeria +Ghana +Kenya +Phishing

- A financially motivated campaign has hit businesses and financial institutions across [Africa](#), deploying phishing emails with malicious attachments to gain access to sensitive systems. The attacks are believed to be part of a broader trend targeting emerging markets with weaker cyber defenses. Affected countries include Nigeria, Ghana, and Kenya.

Data Breaches

Estes Express Confirms Ransomware Attack, Ransomed Data Leaked

+Logistics +ALPHV

- Freight forwarding giant [Estes Express Lines](#) confirmed a data breach following an October 2023 ransomware attack, which was later claimed by the ALPHV/BlackCat group. The attackers exfiltrated sensitive employee data, including Social Security numbers and banking information. Victims are now being notified, months after the breach occurred.

Ransomware Attack Tied to NHS Delays That Contributed to Patient Death

+UK +Healthcare +Qilin

- The ransomware attack on NHS provider [Synnovis](#) in London led to the disruption of critical pathology services, delaying cancer diagnoses and surgeries. According to the UK Health Security Agency, the delay contributed to at least one patient death. Qilin, a known ransomware group, took credit for the attack.

Mainline Health Systems Breach Impacts Over 100,000 Patients

+Healthcare +US

- [Mainline Health Systems](#), a rural healthcare provider in Arkansas, suffered a data breach affecting over 100,000 individuals. Exposed data included medical information, financial account details, and Social Security numbers. The attack began with unauthorized access to email accounts and escalated into a broad compromise of patient records.

Airline Employee Data Breached in Isolated Incident

+Travel

- [Hawaiian Airlines](#) disclosed a cyberattack that compromised employee data but did not impact flight operations or customer systems. The breach stemmed from unauthorized access to internal files containing employee information. The company is notifying affected individuals and offering identity protection services.

Disneyland Paris Appears on Anubis Ransomware Leak Site

+Anubis +France

- Anubis ransomware operators have listed [Disneyland Paris](#) as a victim on their leak site, threatening to release allegedly stolen internal documents and employee records. Disneyland Paris has not confirmed the breach publicly, but the listing suggests a possible compromise of sensitive corporate data.

Lazarus Group Linked to \$11M BitoPro Crypto Theft

+Lazarus +North Korea +Taiwan +Crypto +Financial Services

- [BitoPro](#), a Taiwanese crypto exchange, attributed a recent \$11 million heist to North Korean threat actor Lazarus Group. The hackers used spearphishing and malware to compromise a wallet, stealing millions in various cryptocurrencies. This attack adds to a string of financially motivated operations linked to Lazarus.

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.