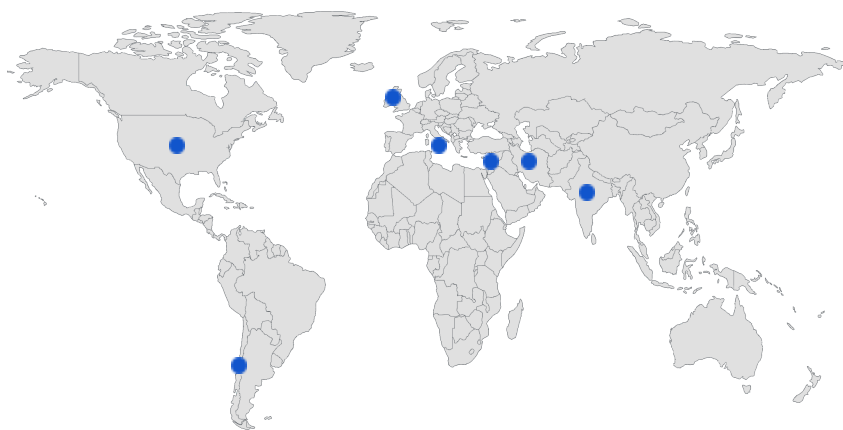


Threat Intel Report: July 31-August 6

Countries



Top Tags

Anonymous Sudan

NoName05716

Mysterious Team Bangladesh

Cyber Avengers

AlphV

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 1% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↓ 30% [CVE-2022-22965](#)

- a RCE vulnerability in Spring programs ("Spring4Shell")

↑ 65% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

SSRF spike targets US-based sites

+SSRF +US +Travel +Financial Services +Business +Telecommunications

- Server-side request forgery, or SSRF, spiked on August 3 at 236% over the average. Attacks primarily targeted US-based sites in the travel, financial services, business, and telecommunications industries. Attacks came from almost 31K distinct IPs, and SSRF rates have since gone down to pre-attack levels.

Short but intense DDoS attack hits UK computing site

+UK +Computing +DDoS

- A UK computing site was attacked on August 4 by application-layer DDoS. The attack lasted only 7 minutes, but was able to reach 750K RPS, pointing to a targeted attack by an advanced attacker with significant resources, like large botnets, at their disposal.

Recent Cyber Threats

NoName targets Italian sites

+NoName05716 +Italy +Financial Services +Government +Business +Hacktivism

- Pro-Russian hacking group [NoName05716](#) has taken responsibility for last week's cyberattacks on various Italian entities, including banks, businesses, and government agencies. The group targeted several websites, including that of Intesa Sanpaolo, Italy's largest bank, and criticized Italian officials for their support towards Ukraine.

Mysterious Team Bangladesh has conducted many DDoS attacks since 2022

+Mysterious Team Bangladesh +Hacktivism +Israel +India +Government +Logistics +Financial Services

- A hacktivist group named "[Mysterious Team Bangladesh](#)" has been associated with over 750 DDoS attacks and 78 website defacements since June 2022, primarily targeting logistics, government, and financial sectors in India and Israel. The group, believed to be Bangladeshi, is driven by religious and political motives, with a focus on supporting Palestine and opposing Israel.

Anonymous Sudan focuses on Nigeria and France

+Anonymous Sudan +Nigeria +France +Government +Telecommunications

- Hacking group [Anonymous Sudan](#) has targeted Nigerian sites for the past week, especially telecommunications company MTN. As of August 5, the group is now pivoting to threatening attacks against French government sites, including the French tax system.

CISA cybersecurity advisory lists top 12 CVEs of 2022

+US +Government +CVEs

- A [cybersecurity advisory](#), released by the Cybersecurity and Infrastructure Security Agency (CISA), FBI, and NSA, highlighted the most exploited vulnerabilities of 2022, which include Log4Shell, Proxy Shell, and Fortinet vulnerabilities. [CVE-2018-13379](#), a VPN credential exposure vulnerability in FortiOS and FortiProxy, topped the list.

Industrial router has several severe vulnerabilities with no patches

+ICS +CVEs

- Security researchers have identified multiple vulnerabilities in the [Milesight UR32L industrial router](#), which could be exploited to execute arbitrary code or commands. The most severe vulnerability, [CVE-2023-23902](#), is a buffer overflow in the router's HTTP server login functionality, leading to potential remote code execution. No software updates have been released to address these issues, despite being reported in February.

SpyNote malware used in European bank fraud

+SpyNote +Financial Services +Europe

- Since the start of the year, there has been a noticeable surge in [SpyNote](#) activity, which, although typically used for data collection and espionage, is now being employed to commit bank frauds against European banking customers. The attack often begins with a smishing campaign where victims are told to install a certified banking app, which eventually grants the attackers remote access to the victim's device and allows them to deploy the malware.

Call of Duty servers taken offline after worm targets PC game

+Gaming +Worm

- The servers for "[Call of Duty: Modern Warfare 2](#)" were taken offline by Activision on July 26th, 2023, after concerns arose about a self-spreading worm virus targeting the PC version of the game. Players had detected unusual

behavior, and upon investigation, it was found that the servers were compromised by a worm virus identified as Trojan:Win32 Wacatac.B!ml.

Data Breaches

Israeli oil refinery attack claimed by Iranian hacking group

+Israel +Iran +Cyber Avengers +Hacktivism

- The website of Israel's largest oil refinery operator, [BAZAN Group](#), became inaccessible globally after a cyberattack, although it remained accessible within Israel. An Iranian hacktivist group named 'Cyber Avengers' claimed responsibility for the attack and shared alleged screenshots of BAZAN's SCADA systems, however, BAZAN dismissed these as fake.

Tempur Sealy attack claimed by AlphV hacking group

+AlphV +Manufacturing

- [Tempur Sealy](#), one of the world's leading mattress sellers, experienced a cyberattack that necessitated the shutdown of portions of its IT infrastructure. Although the company did not specify the nature of the attack, the AlphV ransomware group later claimed responsibility, claiming possession of sensitive documents from high-ranking officials.

US emergency rooms closed over computer system incident

+US +Healthcare

- A widespread cyberattack affected [hospital computer systems](#) throughout the US, leading to the closure of emergency rooms in multiple states and the diversion of ambulances. The incident, which began at facilities run by Prospect Medical Holdings based in California, prompted the company to take its systems offline and initiate an investigation with cybersecurity specialists. No further information is known about this attack currently, as the investigation is ongoing.

US government employee data compromised in MoveIT breach

+US +Government +MoveIT

- US government contractor [Serco Inc.](#) reported a data breach where attackers accessed the personal data of over 10,000 individuals from a third-party vendor's MoveIT managed file transfer server. The breach, which originated from the company's benefits provider, compromised data such as names, U.S. Social Security Numbers, dates of birth, addresses, and selected health benefits.

Imperva customers are protected against the MoveIT vulnerability.

US, Chile astronomical observatories shut down in cyberattack precautionary measure

+US +Chile

- The [Gemini North](#) observatory in Hawai'i recently suspended its operations due to a cyberattack. While the attack did not cause any damage, both the Gemini North in Hawai'i and its counterpart in Chile were shut down as a precautionary measure.

UK special needs school targeted by LockBit ransomware

+LockBit +UK +Education +Ransomware

- The [LockBit](#) ransomware group targeted West Oaks School in Leeds, England, a school for children with special educational needs. The school was given a two-week ultimatum to pay a ransom or face the publication of potentially stolen data, although it remains unclear what specific information was compromised.

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.



By Phone:
650-345-9000



By Fax:
888-611-7282

By mail:

Imperva Headquarters
One Curiosity Way, Suite
203 San Mateo, CA 94403