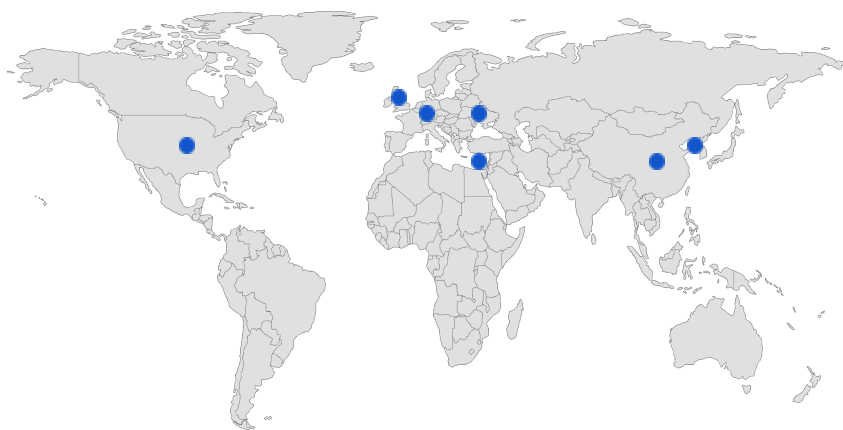


Threat Intel Report: August 7-13

Countries



Top Tags

NoName05716

LockBit

Government

Reptile

Healthcare

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 12% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

↑ 35% [CVE-2022-22965](#)

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

↑ 10% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Belgian site hit with short but heavy DDoS attack

+Belgium +Business +DDoS

- A Belgian business site was targeted by application-layer DDoS on August 9, reaching almost 1M RPS. The attack came from almost 3K IPs, and was able to reach 930K RPS in only 8 minutes-pointing to a very capable attacker. The attack was blocked by Imperva protection, and unsuccessful in causing damage.

US travel API targeted by XSS

[+US](#) [+Travel](#) [+XSS](#)

- A US-based travel company's API was attacked by XSS on August 11. The attacks reached a peak of 2.3M requests, and came almost entirely from UK-based IPs.

Recent Cyber Threats

Magento vulnerabilities exploited by criminals

[+E-Commerce](#)

- Cybercriminals are exploiting vulnerabilities in the [Magento](#) e-commerce platform to steal payment card details from online shoppers. The attackers use malicious scripts to capture checkout data, emphasizing the need for online retailers to update and secure their platforms.

NoName05716 targets French, Dutch government sites

[+NoName05716](#) [+France](#) [+Netherlands](#) [+Government](#)

- Pro-Russian hacktivist group [NoName05716](#) has claimed responsibility for a series of cyberattacks on French and Dutch sites. These attacks are politically motivated, and target government and public service sites in retaliation for the countries' support of Ukraine.

WordPress theme has SQL injection and XSS bugs

[+SQL Injection](#) [+XSS](#)

- The popular WordPress [Avada](#) theme plugin has been found to contain SQL injection and XSS vulnerabilities. These flaws could allow attackers to compromise websites, underscoring the importance of timely updates and patches.

Chinese language app has several vulnerabilities

[+China](#) [+Encryption Flaw](#)

- A popular Chinese-language input app, [Tencent](#) Sogou Input Method, has been identified to have encryption flaws. These vulnerabilities could expose users' personal data in plaintext, emphasizing the need for rigorous security checks in app development.

VS Code vulnerability could allow password theft

[+CVE](#)

- A vulnerability in Microsoft's [Visual Studio Code](#) could allow malicious extensions to steal passwords. Users are advised to be cautious when installing extensions and to keep their software updated.

Ukrainian government targeted by malware in social engineering attacks

[+Ukraine](#) [+Government](#) [+Merlin](#) [+Social Engineering](#)

- [Ukrainian government agencies](#) have been targeted by the Merlin backdoor malware. This attack, aiming to steal sensitive government information, comes from an unidentified attacker tracked as UAC-0154, who sent fake emails posing as Ukraine's CERT.

Rootkit targets South Korean Linux systems

[+Reptile](#) [+South Korea](#)

- The [Reptile](#) rootkit is targeting Linux systems in South Korea. This stealthy malware can evade detection and provides attackers with deep access to compromised systems.

Data Breaches

Northern Ireland accidentally leaks data on all active police officers

+UK +Northern Ireland +Government

- The [Police Service of Northern Ireland](#) (PSNI) accidentally exposed the personal information of all 10,000 active officers after mistakenly sharing a spreadsheet in response to a Freedom of Information request. Although the data was quickly taken down, it leads to severe safety and security concerns in a country where many police officers are at risk of targeted violence.

UK police data leaked

+UK +Government

- [Cumbria](#) police have acknowledged a significant data breach that exposed personal details of officers and staff. The breach's extent and potential implications are still under investigation, but it follows in the wake of the recent PSNI breach.

California town targeted by LockBit

+US +Government +LockBit

- The city of [El Cerrito](#) in California is investigating a data theft incident linked to the LockBit ransomware gang after the group posted the city on their breach site. The breach's impact is being assessed, and residents are urged to be vigilant about potential scams or fraud.

Israeli hospital affected by ransomware

+Israel +Healthcare

- An [Israeli](#) hospital recently faced disruptions due to a ransomware attack. The cyberattack impacted the hospital's operations, forcing them to send patients elsewhere. The attack hasn't been claimed yet, but Israel is frequently targeted by many hacktivist groups.

LockBit threatens to leak cancer patient data

+Healthcare +LockBit

- [Varian Medical Systems](#), a prominent healthcare tech company, fell victim to a ransomware attack by the LockBit group. The cybercriminals targeted the company's data, and is threatening to release the data of cancer patients if the ransom is not paid.

UK electoral system hack exposes voter data

+UK +Government

- A cyberattack on a [UK](#) electoral service has exposed the data of numerous voters. The breach has raised concerns about the integrity of the electoral process, and officials are working to address the situation and ensure data security.

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