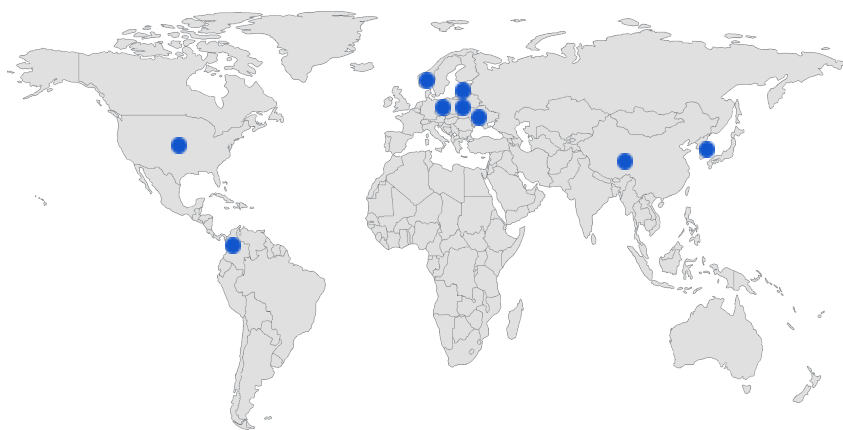


Threat Intel Report: July 10-16

Countries



Top Tags

NATO

MOVEit

NoName05716

CI0p

Government

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 13% [CVE-2023-21371](#)

- A remote directory traversal vulnerability in Oracle WebLogic Server

↓ 18% [CVE-2022-22965](#)

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

↑ 87% [CVE-2022-22963](#)

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

Lithuanian travel site sees bad bot attacks around NATO Summit

+Lithuania +NATO +Travel +NoName05716

- A Lithuanian travel site has been targeted by automated attacks around the country's hosting of the 2023 NATO Summit in Vilnius. The site suffered higher-than-average bot attacks in the week leading up to the Summit, as well as the day of the event. Attacks came from IPs all over Europe, including Russia, and came around [NoName05716's](#) attacks on Lithuanian retail and travel sites, although the group did not claim this attack.

Colombian bank targeted by XSS and path traversal attacks

[+Colombia](#) [+Financial](#) [+Path Traversal](#) [+XSS](#) [+US](#) [+Japan](#)

- A Colombian bank was targeted by path traversal and XSS attacks on July 14, which totaled 2.7M requests in just one day. Attacks came primarily from the US, as well as Japan and the UK, and tried to access the web server via the `/cgi-bin/` directory.

Recent Cyber Threats

Critical RCE bug found in Linux open-source interpreter

[+RCE](#) [+Linux](#)

- A critical RCE bug has been found in the popular Linux open-source interpreter Ghostscript. The bug, known as [CVE-2023-36664](#), has a CVSS score of 9.8, and can trigger code execution when the victim opens a malicious file.

New GhostWriter campaign targets Ukraine and Poland

[+Ukraine](#) [+Poland](#) [+Government](#) [+Belarus](#) [+GhostWriter](#)

- [Ukraine's CERT team](#) has attributed a campaign targeting several government and military entities in Ukraine and Poland to the GhostWriter campaign, linked to the Belarusian government. The attacks primarily hide their payloads in Microsoft Excel and PowerPoint documents, and ultimately install the AgentTesla RAT and Cobalt Strike beacons.

BlackLotus source code posted on GitHub

[+BlackLotus](#)

- Source code for the [BlackLotus](#) bootkit malware has been shared publicly on GitHub, although the shared code has several modifications compared to the original malware. The leaked code has been stripped of an exploit targeting CVE-2022-21894, but contains the rest of the code.

WordPress security plugin found to log plaintext passwords

[+WordPress](#)

- A popular WordPress security plugin known as [All-In-One-Security](#) has been found to log plaintext passwords to log files. The plugin has been updated, but users claim it now breaks sites and doesn't remove the old plaintext password logs.

Large botnet spreads to 20 countries in 2 years

[+Botnet](#) [+AVrecon](#)

- A router botnet known as [AVrecon](#) has spread to 70K devices over 20 countries in just two years. The botnet is one of the largest tracked, and the purpose seems to be enabling criminal activities, like password spraying and fraud.

Data Breaches

Chinese threat actor targets US and EU governments via Outlook vulnerability

[+China](#) [+Storm-0558](#) [+Government](#)

- At least 26 countries have been hit by a Chinese threat actor known as [Storm-0558](#), in attacks that hacked Outlook accounts for espionage and data theft. The attacker has been exploiting a token validation issue in the Outlook program since early May, and has targeted government accounts in the US and Europe.

US software company targeted by unknown nation-state actor

[+US](#) [+Computing & IT](#)

- [JumpCloud](#), a US-based software company, recently announced that intrusion was the work of a sophisticated nation-state actor. This news comes a week after the company reset the API keys of all customers. JumpCloud has yet to reveal the name or origin country of the threat actor.

US healthcare company suffers data breach affecting 11M patients

+US +Healthcare

- US healthcare provider [HCA Healthcare](#) recently announced a breach of 27M records, containing approximately 11M patient's data. The data stolen includes personal information, as well as healthcare data from their last doctor's visit.

Colorado State University impacted by CI0p MOVEit attacks

+US +Education +CI0p +MOVEit

- [Colorado State University](#) recently confirmed that it was impacted in the ongoing MOVEit attacks conducted by the CI0p ransomware gang. The stolen data may include PII and demographic information dating back to at least 2021.

Norwegian Refugee Council suspends attacked refugee database

+Norway +NGO

- The [Norwegian Refugee Council](#) announced that it discovered a cyberattack on a database which contains the personal information of refugees. The Council suspended the database and is conducting an investigation. The organization settled 32,000 people in 2022, including Ukrainian refugees.

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