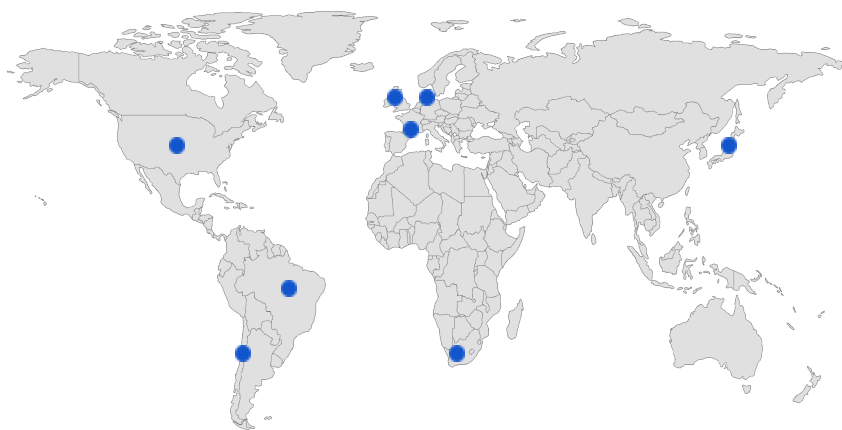


Threat Intel Report: August 21-27

Countries



Top Tags

Luna Grabber

Anonymous Sudan

Rhysida

ALPHV

IOT

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 19% [CVE-2022-21371](#) CVSS Score: 9.8

- A remote directory traversal vulnerability in Oracle WebLogic Server

↑ 15% [CVE-2022-22965](#) CVSS Score: 9.8

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

↓ 22% [CVE-2023-35082](#) CVSS Score: 9.8

- An authentication bypass vulnerability in Ivanti

Largest application layer DDoS attack of 2023 targets Chilean gambling site

+DDoS +Chile +Gambling

- A Chilean gambling site was targeted by DDoS reaching 3M RPS in just six minutes. Attacks came from almost 10,000 IPs, mainly based in the Netherlands and Chile. This attack is the largest application-layer DDoS attack Imperva has seen so far in 2023.

US financial site hit with path traversal attacks

+US +Financial Services +Path Traversal

- A US-based financial site was attacked with path traversal attacks on August 27, reaching almost 1.5M attack attempts. This site has not been targeted before with any notable attacks, and this instance came mainly from Ukraine in a probable targeted attack.

Recent Cyber Threats

New infostealer malware poses as Roblox packages

+Luna Grabber

- A new malware called [Luna Grabber](#) is disguising itself as Roblox packages on the npm platform. The malware is designed to steal sensitive information, including login credentials, from users who download these fake packages.

WinRAR zero-day exploited to spread malware

+Zero-day

- A zero-day vulnerability in [WinRAR](#) is being actively exploited to spread malware. The flaw allows attackers to execute arbitrary code when a user opens a specially crafted RAR archive. Users are advised to update their WinRAR software to the latest version to mitigate the risk.

Openfire serves at risk of code execution

+Code Execution

- Openfire servers are at risk due to a new [exploit](#) that allows attackers to execute arbitrary code. The vulnerability is particularly concerning because Openfire is widely used for XMPP-based messaging services. Users are advised to apply patches as soon as they are available.

Smart light bulbs have several vulnerabilities

+IoT

- Researchers have found vulnerabilities in TP-Link Tapo L530E [smart bulbs](#) that could allow attackers to steal WiFi passwords. The flaws range from improper authentication to lack of encryption, and TP-Link is working on fixes.

Anonymous Sudan targets Twitter

+Anonymous Sudan

- Anonymous Sudan targeted X, formerly Twitter, for a one-hour targeted attack on August 27th. It's unknown why they targeted the site, but reports confirmed outages were reported around that time.

Data Breaches

Rhysida ransomware group threatens to sell over 1TB of healthcare data

+US +Healthcare +Rhysida

- [Prospect Medical Holdings](#), a healthcare services provider, has suffered a data breach by the Rhysida ransomware group, which has threatened to sell stolen data if the ransom of 50 BTC is not paid. The compromised data includes over 500K records including sensitive patient information, SSNs, and more.

Ohio History Connection targeted by ransomware group

+US +Education

- The [Ohio History Connection](#) has experienced a data leak and ransomware attack. The incident has disrupted the website's services and exposed the personal data, including SSNs, of over 7K employees between 2009 and 2023. The organization is currently investigating the breach.

Title lender confirms financial data stolen in recent data breach

+Automotive +US

- Title lender [TMX Finance](#) has revealed that payment card data for over 5M customers was stolen in a recent data breach. The company initially denied that financial data was compromised but has now confirmed the theft.

10M French citizens' data leaked

+France +Government

- A massive data leak has exposed the sensitive information of 10 million [French](#) citizens. The compromised data includes names, email addresses, and phone numbers. The source of the leak is still unknown, and an investigation is underway.

Crypto platform hacked, \$7M stolen

+Financial Services +Cryptocurrency

- The decentralized finance (DeFi) platform [Exactly Harbor Protocol](#) has been hacked, resulting in the theft of millions of dollars in cryptocurrency. The platform has suspended all transactions and is investigating the breach. Users are advised to withdraw their funds from the platform.

Brazilian escort service leaks 14M records of escorts and customers

+Brazil +Adult

- A [Brazilian escort service](#) has inadvertently exposed the personal data of escorts and clients. The exposed data includes over 14M records including names, contact details, and transaction histories. The service has taken steps to secure the data and is investigating the incident.

UK police data leaked, again

+UK +Government

- More [UK police officers](#) have been exposed in a data breach affecting the Metropolitan police division, which serves London and surrounding areas. An IT breach into the company that supplies the division's warrant cards has leaked up to 47K officers' names, ranks, and photos. This breach follows recent police breaches in England and Northern Ireland.

Danish cloud provider loses all data to ransomware attack

+Denmark +Cloud Services

- Danish cloud provider [CloudNordic](#) was hit by a ransomware attack that encrypted all of its servers, including backups. The company is currently working on restoring services but warns that data loss is significant, and it will not pay a ransom. The attack has raised concerns about the vulnerability of cloud service providers to ransomware attacks.

US defense contractor leaks admin credentials and internal data

+Engineering +US

- [Belcan](#), a US defense contractor, experienced a data breach where a Kibana instance was left unsecured. Although the admin passwords were hashed, the leak has put the company's internal systems at risk, and an investigation is underway.

Over 2M Duolingo users' data scraped

+Education

- Data of approximately 2.6 million [Duolingo](#) users has been released on a hacking forum. The data was scraped and includes usernames and hashed passwords. Duolingo is investigating the incident and has urged users to change their passwords.

South African government targeted by Snatch ransomware

+Government +South Africa

- The [Department of Defence in South Africa](#) has been targeted by Snatch ransomware. The attack has compromised sensitive information and disrupted operations. The incident is under investigation, and it's yet another example of how governmental organizations are increasingly becoming targets for ransomware attacks.

Seiko watchmaker breached by ALPHV

+Retail +Japan +ALPHV

- [Seiko](#), a major Japanese watchmaker, has been breached by the ALPHV ransomware gang. The attackers have claimed to have stolen sensitive data, including production plans and technical schematics. Seiko has apologized to its customers and partners and is currently investigating the breach.

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