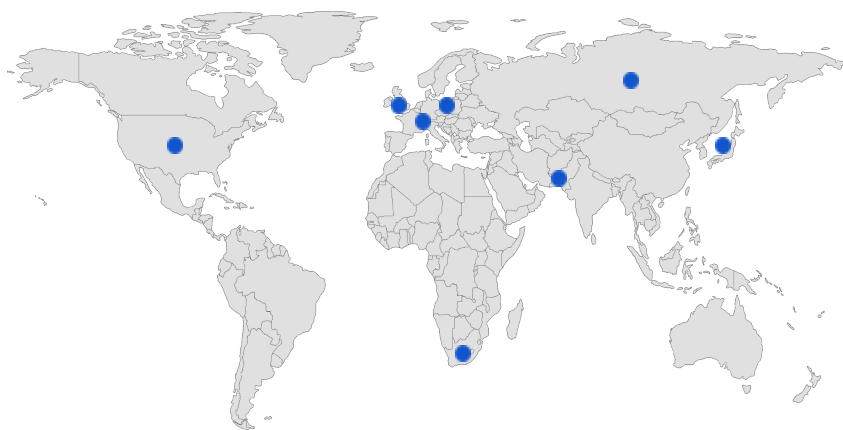


Threat Intel Report: August 14-20

Countries



Top Tags

ALPHV

NoEscape

Black Basta

Anonymous Italia

MoveIT

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 19% [CVE-2023-21371](#)

- a remote directory traversal vulnerability in Oracle WebLogic Server

⬇ 1% [CVE-2022-22965](#)

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

⬆ 17% [CVE-2023-30185](#)

- A file upload vulnerability in some CRMEB versions

Pakistani financial site experiences >1M RPS DDoS attack

+Pakistan +Financial Services +DDoS

- A Pakistani financial site was targeted on August 20 by an application-layer DDoS attack reaching over 1M RPS. The attack lasted over 8 hours, and came from over 2500 distinct IPs, which points to attackers' use of a wide botnet.

Polish computing site attacked by bots

+Poland +Ireland +South Africa +Computing

- A Polish computing site was targeted by bots on August 18, at rates 7K times higher than the average. The attacks came mainly from Ireland and South Africa.

Recent Cyber Threats

WinRAR vulnerability poses risk

+WinRAR

- A flaw in [WinRAR](#), a popular file compression tool, allows attackers to execute malicious programs simply by having users open a specially crafted RAR archive. This vulnerability poses a significant risk as users might inadvertently run malicious software without any additional interaction.

ALPHV ransomware group releases new ransomware

+ALPHV +Sphynx

- The ALPHV ransomware group released a new ransomware variant named [Sphynx](#), which incorporates tools from the Impacket library and RemCom for its operations. This combination allows the ransomware to execute commands remotely and spread laterally within networks.

New Apple exploit can be exploited without user interaction

+Apple +Technology

- A newly discovered [exploit](#) in Apple's iOS 16 enables attackers to bypass security mechanisms and gain unauthorized access to user data. The vulnerability is particularly concerning as it can be exploited without any user interaction.

Duke ransomware targets victims via decoy PDFs

+Duke +Russia +Government

- Cyber attackers have been using decoy PDFs, seemingly from the German embassy, to distribute the [Duke](#) malware, which is believed to be linked to Russian threat actors. The campaign targets specific individuals, aiming to compromise their systems for espionage purposes.

Ford vulnerability does not pose a safety risk

+Automotive +Wi-Fi Vulnerability

- [Ford](#) has acknowledged a Wi-Fi vulnerability in some of its vehicles but asserts that it does not pose a safety risk to drivers or passengers. The company is likely to address the issue in future updates, emphasizing that the flaw doesn't impact the vehicle's primary functions.

ATM software vulnerability could lead to remote hacking

+Financial Services

- Vulnerabilities in Ilogona's [ScrutisWeb](#) software could expose ATMs to potential remote hacking attempts. If exploited, attackers could gain unauthorized access to ATM operations and potentially compromise customer data.

Data Breaches

Germany bar association targeted by NoEscape ransomware

+Germany +NoEscape +Legal

- The [German National Bar Association](#) is currently investigating an attack from NoEscape ransomware. The extent of the breach and the data affected are still being determined.

Illinois hospital alerts current and former patients and employees about breach

+Healthcare +US

- An [Illinois-based hospital](#) has notified its patients and employees about a recent cyber incident. The specifics of the breach, including the data compromised, are still under review.

NC organization targeted by Black Basta ransomware

+US +Government +Black Basta

- The [Raleigh Housing Authority](#) has fallen victim to a ransomware attack by the Black Basta ransomware group, who have released SSNs and passport information from some victims. The attackers have made demands, and the authority is working to address the situation.

NYC Finance Department leaks personal information of all employees

+Financial Services +Government +US

- New York City's [Department of Finance](#) inadvertently exposed personal information of its staff due to a failed emergency alert test. The exposed data included sensitive details, and the issue has since been addressed.

QR code phishing attacks target US energy organization

+US +Energy

- A major [US energy organization](#) was targeted in a sophisticated QR code-based phishing attack. The attackers aimed to steal credentials and gain unauthorized access.

Clorox responding to recent security breach

+Manufacturing

- [Clorox](#), the cleaning products company, is addressing a security breach that impacted its systems. The company is working to determine the extent of the breach and the data affected.

US hospital alerts affected individuals one year later

+US +Healthcare

- A [Georgia healthcare system](#) has notified 180,000 individuals about a cyberattack that occurred a year ago. The delay in notification has raised concerns, and the affected individuals are being provided with guidance on protective measures.

UK police forces have third and fourth data breaches in recent weeks

+UK +Government

- Police forces in [Norfolk and Suffolk](#) have identified a data breach that compromised sensitive information as part of a mishandled Freedom of Information request. These breaches follow Northern Ireland and Cumbria police data mishandling incidents in the past weeks.

Colorado alerts 4M people affected by MoveIT data breach

+US +Government

- The state of [Colorado](#) has issued a warning to 4 million individuals about a data breach linked to the IBM MoveIT software. The breach exposed sensitive data, and affected individuals are being provided with guidance and support.

Anonymous Italia attacks Japanese government

+Anonymous Italia +Japan +Government

- [Anonymous Italia](#) has claimed responsibility for a cyberattack on the Japanese government in retaliation for wastewater release in the Fukushima power plant. The attackers aimed to disrupt government operations and raise awareness about the issue.

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