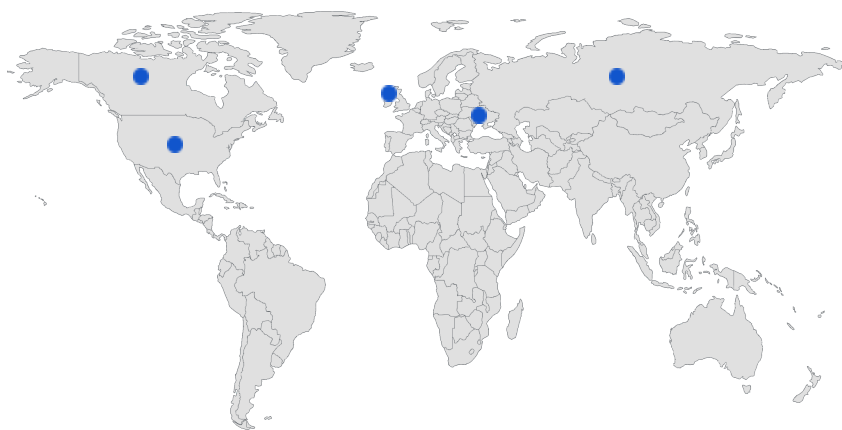


Threat Intel Report: October 23-29, 2023

Countries



Top Tags

Lockbit

Rhysida

iLeakage

Financial Services

Government

Executive Summary

Actionable Information:

- **Geopolitical Cyber Tensions:** The suspected involvement of Ukraine's SBU in the Alfa-Bank hack indicates a rising trend of state-sponsored cyberattacks. Organizations, especially in the financial sector, should be vigilant of potential geopolitical motivations behind cyber threats.
- **Advanced Persistent Threats (APTs):** The exploit by the Winter Vivern APT group on Roundcube webmail servers is a reminder of the sophisticated tactics employed by APTs. Organizations should be proactive in monitoring for such threats and ensuring their systems are updated.
- **Rising DDoS Attacks:** The record-setting DDoS attack emphasizes the evolving nature and scale of denial-of-service threats. Strengthening DDoS protection measures is crucial for online platforms.
- **Emerging Ransomware Tactics:** The introduction of Rhysida, a self-deleting ransomware, indicates a shift in ransomware tactics to hinder post-incident investigations. Regular data backups and updated security solutions are more vital than ever.
- **Browser Vulnerabilities:** The iLeakage vulnerability in Apple's Safari browser emphasizes the need for continuous monitoring and patching of widely-used browsers to protect user data.
- **Critical Infrastructure Threats:** The vulnerability in F5's BIG-IP application delivery controller showcases the risks faced by critical infrastructure components. Immediate patching and continuous monitoring are essential for such systems.

Outlook:

The cyber landscape continues to evolve with threat actors exploiting vulnerabilities across various platforms and sectors. The healthcare sector, in particular, remains a prime target, as evidenced by the Windsor Hospital incident. Financial institutions are also under threat, with the Alfa-Bank incident highlighting potential geopolitical motivations behind cyberattacks. Organizations must remain vigilant, prioritize patching known vulnerabilities, and invest in educating employees about emerging threats. The rise of self-deleting ransomware and sophisticated APT exploits underscores the need for proactive defense strategies and robust backup solutions.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

📈 11% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

📈 2% [CVE-2022-22965](#)

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

📈 4% [CVE-2023-35082](#)

- An authentication bypass vulnerability in Ivanti

Financial Services site experiences 1.2M RPS DDoS attack

+US +Financial Services

- On October 26, a US-based financial services site was hit with a 1.2M RPS application-layer DDoS attack. The attack came from over 7,000 IP addresses and lasted half an hour.

Telecommunications company targeted by SQLi and RCE

+SQL Injection +RCE +Telecommunications

- A telecommunications company was targeted this week by attacks split between SQL injection and remote code execution. The attacks came mainly from Germany, followed by the US and Türkiye.

Recent Cyber Threats

Windsor hospital faces cyber disruption

+Canada +Healthcare

- [Windsor Regional Hospital](#) in Ontario experienced a cyber incident that disrupted its computer systems. The hospital had to revert to manual processes, causing delays in patient care.

Ukraine's SBU suspected in Russian bank hack

+Ukraine +Russia

- Ukraine's Security Service ([SBU](#)) is suspected of involvement in the cyberattack on Russia's Alfa-Bank. The attack led to the leak of confidential client data.

OAuth login vulnerability

+CVE +Account Takeover

- A vulnerability in [OAuth](#) login can lead to full account takeovers, affecting millions of users. The flaw can be exploited by attackers to bypass authentication processes.

Winter Vivern APT exploit

+Zero-day +Winter Vivern

- The [Winter Vivern](#) APT group exploited a zero-day vulnerability in Roundcube webmail servers. This allowed them to access sensitive email content.

Record HTTP2 DDoS attack

+DDoS

- A massive [DDoS attack](#), reaching 100 million RPS, targeted an undisclosed online platform. This attack set a new record in terms of its scale and intensity.

Rhysida self-deleting ransomware

+Rhysida +Ransomware

- A new ransomware strain named [Rhysida](#) has been discovered, which uniquely deletes itself after encrypting victim's files. This self-deletion feature makes post-incident investigations challenging.

FakeUpdater campaign targets Russian-speaking users

+Russia +Trojan

- The [FakeUpdater.ru](#) campaign tricks users into downloading a fake Chrome update, which in turn spreads Trojan malware. The campaign targets Russian-speaking users and has been active since early 2023.

iLeakage Safari vulnerability

+Apple +iLeakage

- A new attack technique named "[iLeakage](#)" can steal emails and passwords from Apple's Safari browser. The vulnerability affects even the latest versions of Safari.

F5 BIG-IP vulnerability protected by Imperva

+CVE +F5

- [F5](#) has issued a warning about a critical vulnerability in its BIG-IP application delivery controller. The flaw can allow attackers to execute arbitrary system commands, leading to potential system takeover.

Imperva customers are protected against this vulnerability.

Data Breaches

CoinFlip data breach

+Social Engineering +Financial Services

- [CoinFlip](#) experienced a breach as a result of a social engineering attack targeting a CoinFlip employee, leading to unauthorized access to certain systems. The compromised data includes full names, dates of birth, and either a driver's license, state-issued identification card, or passport number.

D.C voter data exposure

+DC +Government

- The personal information of D.C. voters may have been exposed in a data breach earlier this month. The [D.C. Board of Elections](#) discovered that a breached server, owned by DataNet Systems, contained a copy of the board's voter roll, potentially exposing partial Social Security numbers, driver's license numbers, dates of birth, and contact information.

Police portal accessed by unauthorized users

+Government

- Unauthorized access to Facebook and Instagram's [police portal](#) was detected. The portal, used by law enforcement agencies, was accessed using valid credentials, but by unauthorized individuals.

Irish Police Service data leak

+Ireland

- The [Irish National Police Service's](#) internal portal was unintentionally exposed online, revealing sensitive information. The leak was due to a misconfiguration and exposed data including operational plans and member details.

SBU targets Russian bank

+Ukraine +Russia +Financial Services

- Ukraine's Security Service ([SBU](#)) was allegedly involved in the cyberattack on Russia's Alfa-Bank. The bank faced disruptions, and the SBU's involvement is seen as a significant escalation in cyber warfare.

Russian state organizations hacked

+Russia +Backdoor +Government

- Hackers have infiltrated [Russian state industrial organizations](#) using backdoors for data theft. The cyber-espionage campaign targeted specific data and intellectual property from these organizations.

New England Biolabs data leak

+US +Healthcare

- [New England Biolabs](#) inadvertently leaked sensitive data online. The exposed data included customer information, and the company is working to address the issue.

Airbnb data breach data for sale

+Travel

- [Airbnb](#) experienced a significant data breach with millions of user records now available for sale on the dark web. The breach exposed sensitive information, including personal details and transaction histories, putting users at risk of potential scams and identity theft.

Radcliffe Labs leaks 7TB database

+Healthcare

- [Redcliffe Labs](#) suffered a data leak, exposing a staggering 12 million records and a 7TB database. The exposed data includes sensitive patient information, which could have severe implications for the affected individuals.

Hello Alfred accidentally leaks user data

+Database Misconfiguration

- The [Hello Alfred](#) app, designed to assist users with daily tasks, inadvertently leaked user data due to a misconfigured database. The exposed data includes personal details, potentially putting thousands of users at risk.

Lockbit gang claims Boeing hack

+Lockbit +Aerospace

- The Lockbit ransomware gang claims to have hacked aerospace giant [Boeing](#), threatening to release a vast amount of sensitive data unless their demands are met. As of now, Boeing has not publicly responded, and no data samples have been released by the ransomware group.

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 mail:

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