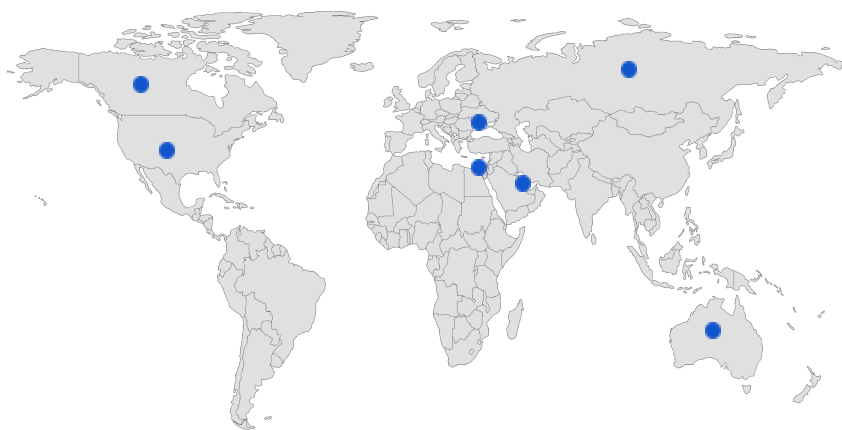


Threat Intel Report: September 25 - October 1

Countries



Top Tags

OilRig

Rhysida

CI0p

Xenomorph

BBTok

Executive Summary

Actionable Information:

- *Cyber-Espionage Campaigns:* There's a noticeable uptick in sophisticated cyber-espionage campaigns targeting specific regions and sectors. Organizations, especially in sensitive industries, should enhance their monitoring and adopt proactive defense strategies.
- *Phishing Campaigns:* The use of unique lures, such as drone manuals, indicates that threat actors are becoming more innovative in their phishing attempts. Continuous employee training on recognizing and reporting suspicious emails is paramount.
- *DDoS Attacks:* Recent disruptions in critical services due to DDoS attacks highlight the need for organizations to bolster their DDoS protection measures and have a response plan in place.
- *Malware Evolution:* The resurgence of known malware strains in evolved forms, targeting specific devices or sectors, underscores the importance of keeping threat intelligence up-to-date and regularly updating security solutions.

Outlook:

The cyber landscape continues to evolve with threat actors employing sophisticated techniques across various sectors globally. The recent surge in ransomware attacks, such as those targeting Sony and Johnson Controls, underscores the need for robust cybersecurity measures and regular backups. Data breaches, as seen with the National Student Clearinghouse and WBSC, highlight the importance of proper data handling and server configurations. Organizations, regardless of their industry, should prioritize cybersecurity awareness training, ensuring that employees are equipped to recognize and respond to potential threats. The continuous collaboration between industries and cybersecurity firms will be crucial in staying ahead of emerging threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 1% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↑ 13% [CVE-2022-22965](#)

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

↑ 5% [CVE-2023-35082](#)

- An authentication bypass vulnerability in Ivanti

US computing site targeted in 600 GBPS DDoS attack

+US +Computing & IT

- A US-based computing site was targeted this week by a network-layer DDoS attack reaching almost 600 GBPS. The attack lasted two days, and came from over 1800 distinct IP addresses.

Australian education site hit with path traversal attacks

+Australia +Education

- An Australian education site was targeted this week by path traversal attacks reaching 3M attack attempts. The attacks came mainly from 141 primarily Germany-based IP addresses.

Recent Cyber Threats

Israeli entities targeted by OilRig campaigns

+Israel +OilRig

- Israeli organizations have become the latest targets of the "Outer Space" and "Juicy Mix" campaigns orchestrated by the [OilRig](#) threat group. These cyber-espionage campaigns are leveraging sophisticated techniques to infiltrate and exfiltrate sensitive data.

Ukrainian military targeted in drone-based phishing campaign

+Ukraine +Government

- The [Ukrainian military](#) has been subjected to a targeted phishing campaign leveraging drone manuals. The fake manuals are used as lures, eventually delivering a Go-based toolkit known as Merlin.

Russian flight booking system targeted in Ukrainian hacktivist attack

+Russia +Travel +DDoS +IT Army

- A prominent [flight booking system](#) in Russia experienced a disruptive DDoS attack. The attack caused significant service interruptions in Russian airports lasting over an hour. The attack was claimed by Ukrainian hacktivist group IT Army.

Xenomorph malware targets US financial sector

+US +Financial Services +Xenomorph

- [Xenomorph](#) malware, an Android banking trojan, has resurfaced in a new campaign targeting US banks. This evolved strain is more sophisticated, aiming to compromise banking credentials and siphon funds.

GPU side-channel attack threatens user data

+GPU Side-Channel

- A new [GPU side-channel attack](#) technique has been identified, allowing attackers to steal data from nearly all modern GPUs. This method exploits the GPU's processing capabilities to steal pixels from a site open at the same time as the malicious one, enabling the theft of personal data like usernames.

Emerging ZenRat threat to Windows users

+Windows +ZenRat +Malware

- A new malware strain, dubbed [ZenRat](#), is specifically targeting Windows users. Although the exact distribution process remains unknown, the deployed malware is designed to steal sensitive information.

Snatch ransomware group reveals visitor IPs

+Snatch +Ransomware

- The [Snatch](#) ransomware group's darknet site exposes its Server Status page, which includes information about visitor IP addresses. This data shows that the majority of repeat visitors are coming from Russia.

Data Breaches

Data breach at National Student Clearinghouse affects 890 schools

+Education

- The [National Student Clearinghouse](#) has suffered a data breach impacting 890 educational institutions. The breach was caused by the widespread MOVEit vulnerability.

BBTok trojan targets Latin American banks

+Latin America +Financial Services +BBTok

- New versions of the [BBTok](#) banking trojan have been discovered targeting over 40 banks in Latin America. The trojan is designed to steal banking credentials, posing a significant threat to financial institutions in the region.

Hong Kong consumer watchdog faces cyberattack

+Hong Kong

- A cyberattack against [Hong Kong's Consumer Council](#) has put the personal data of over 25K residents at risk. The potentially stolen data includes credit card information, resumes, and birth dates.

Sony faces ransomware attack from new group

+Gaming +Ransomed.vc

- [Sony](#) has become the latest victim of a ransomware attack from a new hacker outfit known as Ransomed.vc, who have only been active since the beginning of September. The breach allegedly stole over 6K files, including log files and HTML and Java data.

Ransomware attack forces Kuwait to isolate systems

+Kuwait +Government +Rhysida

- In response to a ransomware attack on its Finance Ministry, [Kuwait](#) has taken the precautionary measure of isolating its critical systems. The hack has been claimed by the Rhysida ransomware gang.

MoveIt hack exposes newborn child registry data

+Canada +MOVEit +Healthcare +CIOP

- A decade's worth of [Canadian](#) newborn child registry data has been stolen in a mass hack targeting the MOVEit platform. The breach has exposed the data of over 3.4M people who sought pregnancy and newborn care between

2010 and 2023. Although the CIOp ransomware gang has conducted the mass MOVEit attacks, it has not yet added BORN Ontario to its victim list.

Canadian airline suffers data leak

+Canada +Travel

- [Flair Airlines](#), a Canadian carrier, left credentials to sensitive databases open for at least seven months. The leak was due to publicly exposed environment files hosted on the company's website.

Johnson Controls hit by ransomware

+Manufacturing

- Building automation giant, [Johnson Controls](#), has been targeted by a ransomware attack after initially being breached in one of its Asia offices. The breach has disrupted operations, and many of the company's subsidiary sites are displaying technical outage pages.

WBSC server misconfiguration exposes thousands of passports

+Sports

- A misconfigured server belonging to the [World Baseball Softball Confederation](#) (WBSC) has leaked thousands of passport details. A misconfigured AWS bucket belonging to the group exposed a repository of almost 50K files, including almost 5K passport copies.

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
 By Fax: 888-611-7282	