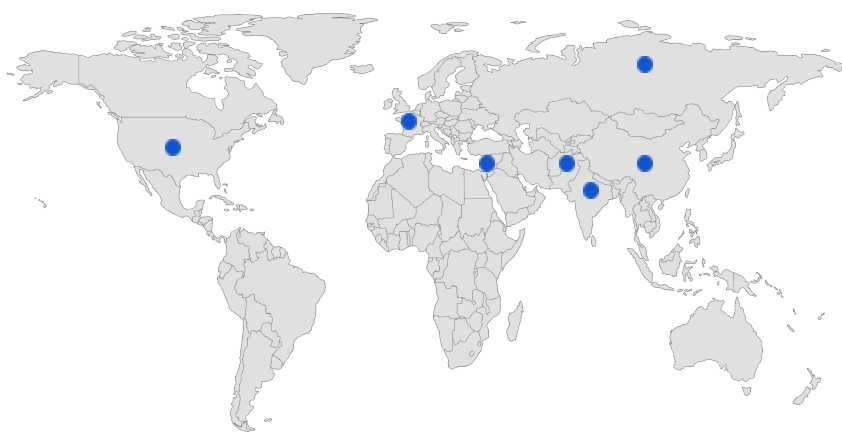


Threat Intel Report: October 9-15, 2023

Countries



Top Tags

Rapid Reset

DarkGate

Athena Agent

AnonGhost

Stayin Alive

Executive Summary

Actionable Information:

- **Software Vulnerabilities:** A rising trend in vulnerabilities across various popular software indicates the need for organizations to prioritize patch management and regular software updates. Ensuring that systems are up-to-date can significantly reduce the risk of potential breaches.
- **Ransomware Evolution:** The continuous evolution and adaptation of ransomware campaigns, highlighted by source code leaks and targeted attacks on specific server types, emphasize the importance of robust backup strategies and employee education.
- **Communication Platforms Under Siege:** The increasing targeting of widely-used communication platforms suggests that businesses should re-evaluate the security of their communication tools, ensuring end-to-end encryption and educating employees about potential threats.
- **Web Manipulation Tactics:** The emergence of tactics like altering error pages and hiding malicious code within legitimate platforms indicates a shift towards more covert attack methods. Organizations should invest in advanced threat detection tools and regularly audit their web assets.

Outlook:

The cyber landscape continues to evolve with attackers leveraging various methods, from exploiting software vulnerabilities to sophisticated malware campaigns. The recent DDoS attacks in the Israel conflict and the Stayin Alive cyber espionage campaign targeting Asian sites underscore the geopolitical nature of some cyber threats. Additionally, high-profile breaches, such as the hack of Facebook's official page and the cyberattack on Air Europa, emphasize the



need for robust cybersecurity measures across all sectors. Organizations should remain vigilant, continuously monitor their digital assets, and invest in proactive cybersecurity measures to mitigate potential threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 6% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

⬆ 24% [CVE-2022-22965](#)

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

⬆ 26% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

Bot attacks on retail sites rising

+Retail +US +France

- Bad bot attacks on retail sites are trending upwards as we go into the holiday season. Since July, automated attacks have risen 14%, and will continue to rise as holiday shopping brings sales, coveted items, and retail traffic. Most attacks are on US-based sites, followed by France.

Chinese computing site hit with almost 1000 GBPS attack

+China +Computing & IT

- A Chinese computing site was targeted this week with network DDoS reaching 913 GBPS. The attack lasted six and a half hours, and was successfully blocked by Imperva's DDoS protection.

Recent Cyber Threats

Recent vulnerabilities in popular applications blocked by Imperva

+CVE

- Several recent [vulnerabilities](#)– in Juniper, Progress, Atlassian, Microsoft, and JetBrains software– are blocked by Imperva. These vulnerabilities affect a wide variety of products, although several are remote code execution bugs.

HelloKitty ransomware source code leaked

+HelloKitty +Ransomware

- The source code for the notorious HelloKitty ransomware has been leaked in an online cybercrime forum. This could potentially lead to an increase in attacks using this ransomware, as more cybercriminals gain access to the code.

Rapid Reset bug blocked by Imperva

+Rapid Reset +DDoS +HTTP2

- A newly discovered DDoS bug, termed "[Rapid Reset](#)," has set a record for its speed and intensity. This bug is blocked by Imperva protection.

Athena Agent malware exploits WinRAR vulnerability

[+Athena Agent](#) [+WinRAR](#) [+Russia](#)

- The [Athena Agent](#) malware is exploiting a vulnerability in the popular WinRAR software. This malware, which was discovered targeting a Russian semiconductor supplier, ultimately attempts to take over compromised systems.

Unpatched WS_FTP servers targeted in ransomware attacks

[+Ransomware](#) [+WS_FTP](#)

- Ransomware attackers are targeting unpatched [WS_FTP](#) servers. These servers, if not updated, are vulnerable to attacks, leading to potential data breaches and ransom demands. Imperva customers are [protected](#) against this vulnerability.

Malware campaign targets corporate communications platforms

[+DarkGate](#) [+Malware](#)

- A new [DarkGate](#) malware campaign is leveraging popular communication platforms like Skype and Microsoft Teams to infiltrate organizations. The campaign ultimately delivers the DarkGate commodity loader malware.

EtherHiding technique conceals malicious Web2 code

[+EtherHiding](#) [+Web2](#)

- A new technique termed "[EtherHiding](#)" has been identified where malicious Web2 code is concealed within Web3 smart contracts. Victims are tricked into downloading fake updates that contain the malicious content.

DDoS attacks leveraged in Israel conflict

[+DDoS](#) [+Israel](#) [+Government](#)

- In the midst of the Israel conflict, attackers are leveraging Distributed Denial of Service (DDoS) to intensify disruptions. Imperva's [analysis](#) reveals a significant spike in DDoS attacks targeting Israeli sites, emphasizing the evolving nature of cyber warfare in geopolitical disputes.

Magecart campaign leverages 404 error pages

[+Magecart](#)

- A new [Magecart](#) campaign has been identified where attackers are altering 404 error pages to inject malicious skimming code. Unsuspecting users visiting these altered error pages risk having their personal and financial information stolen.

Data Breaches

Facebook's official page hacked

[+Facebook](#) [+Pakistan](#)

- [Facebook's](#) official page was briefly hacked, displaying messages in support of former Pakistani Prime Minister Imran Khan. The posts have been removed, and the Facebook page was disabled as the company investigates the incident.

Indian payment company investigating theft of millions of dollars

[+India](#) [+Financial Services](#)

- Indian company [SafeXPay Technology's](#) payment gateway was compromised, leading to a scam where millions of dollars were siphoned off to foreign accounts. The police are investigating the incident.

European airline urges customers to cancel credit cards after cyberattack

[+Travel](#)

- [Air Europa](#) faced a cyberattack that potentially exposed the payment card details of its customers. Customers have been urged to cancel their credit cards after the incident, although the company has not released further details about the attack.

Stayin Alive cyber espionage campaign targets Asian sites

[+Stayin Alive](#) [+China](#) [+Telecommunications](#) [+Government](#)

- A cyber-espionage campaign, linked to China and dubbed "[Stayin Alive](#)," is targeting telecom and government entities in Asia. The campaign has been active since at least 2021.

AnonGhost sends fake nuclear warnings via Israeli missile alert app

[+AnonGhost](#) [+Israel](#)

- Hacker group [AnonGhost](#) sent a fake nuclear attack warning to Israelis through the Red Alert app, accompanied by racist imagery. Researchers claim the group was able to exploit an API vulnerability in the app.

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