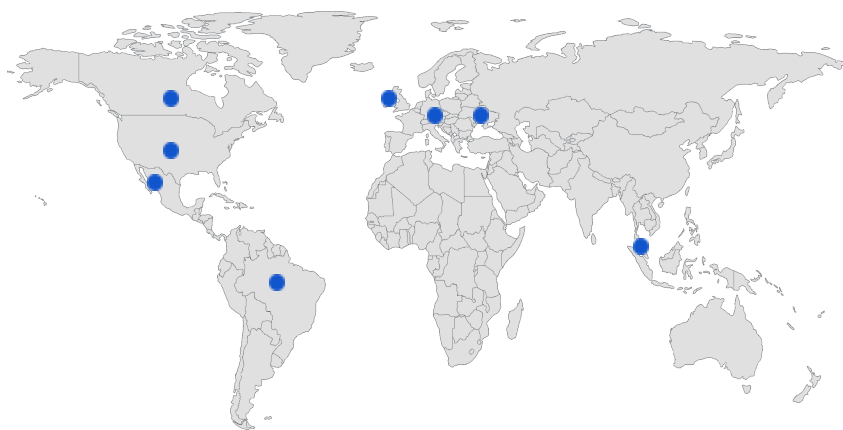


Threat Intel Report: October 30 - November 5, 2023

Countries



Top Tags

Black Basta

AlphV

LockBit

UserSec

Anonymous Sudan

Executive Summary

Actionable Information:

- **Geopolitical cyber tensions:** The cyberattack by the Ukrainian IT Army on a Russian ISP highlights the escalating trend of geopolitically motivated cyberattacks. Organizations, especially those operating in regions with political tensions, should be prepared for potential cyber repercussions and bolster their defenses accordingly.
- **Data protection urgency:** Recent incidents, including the Elektra leak and the breach at the Indian Council of Medical Research, emphasize the global challenge of safeguarding data. Organizations across all sectors should prioritize data protection, conduct regular security audits, and ensure that they have robust mechanisms to detect and respond to breaches.
- **Ransomware on the rise:** The increasing frequency and diversity of ransomware attacks signal a growing threat that organizations cannot afford to ignore. It's imperative for entities to invest in preventive measures, maintain updated backups, and establish clear response protocols for potential ransomware incidents.
- **Software vulnerability exploits:** The discovery of vulnerabilities in widely-used platforms underscores the importance of continuous software updates and security monitoring. Organizations should adopt a proactive approach to software security, ensuring timely patching and educating employees about potential risks.

Outlook:

The cyber landscape continues to evolve with threat actors exploiting both political situations and software vulnerabilities. The diversity of targets, ranging from news sites to public health services, suggests that no sector is immune. Organizations must remain vigilant, prioritize cybersecurity hygiene, and foster a culture of security awareness. The trend of ransomware attacks remains particularly concerning, with attackers becoming more audacious in their

choice of targets and their demands. As software becomes more integrated into daily operations, vulnerabilities in popular platforms can have wide-reaching implications, making regular updates and patches crucial.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↑ 21% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↑ 40% [CVE-2022-22965](#)

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

↑ 203.6% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

US computing site targeted in DDoS attack

+US +Computing & IT

- A US-based computing site experienced a 9-minute application-layer DDoS attack that reached 1.8M RPS. The attack came from 2400 IPs, and points to the increased intensity and volume of application-layer DDoS attacks in the second half of 2023.

Brazilian financial site hit with attempted RCE attacks

+Brazil +Financial Services

- A Brazilian financial site experienced remote code execution attacks this week almost 1200% higher than average. Attacks came almost entirely from Germany, which points to an attacker utilizing proxy services or German infrastructure to conduct these attacks.

Recent Cyber Threats

Ukrainian IT army targets Russian ISP

+Ukraine +Russia +Hactivism +IT Army

- The Ukrainian [IT Army](#), a hactivist group, launched a cyberattack against a Russian internet service provider. The group temporarily disrupted internet service in some Russian-occupied territories.

Elektra leak leads to cryptojacking surge

+Cryptojacking

- A data leak from the [Elektra](#) project has resulted in an increase in cryptojacking attacks. Threat actors are exploiting the leaked data to target vulnerable systems for unauthorized cryptocurrency mining.

Gatwick Airport faces cyberattack

+UK +Travel +UserSec

- [Gatwick Airport](#) in the UK became the target of a cyberattack, marking it as the second major UK airport to be hit in recent times. The attack group UserSec has claimed responsibility for this attack, which is likely DDoS.

AP News site suffers DDoS attack

+News +Anonymous Sudan

- The [AP News](#) website experienced a DDoS attack, causing temporary outages. Anonymous Sudan has claimed responsibility for this attack, although that is unconfirmed.

DDoS attack hits Singapore's public health services

+DDoS +Singapore

- [Singapore's public health services](#) were disrupted by a DDoS attack. The attack affected several online services, but no data breach was reported, and the attacker is unknown.

Wikipedia pages exploited for Slack redirection attacks

+Wiki-Slack

- Attackers have found a way to use modified Wikipedia pages to launch redirection attacks on Slack users, in an attack known as [Wiki-Slack](#). By manipulating links, they can redirect users to malicious sites.

Atlassian Confluence vulnerability threatens data loss

+CVE

- Atlassian recently announced a vulnerability in its [Confluence](#) Data Center and Server products. This is a critical vulnerability, allowing attackers to bypass the authentication mechanism to potentially gain unauthorized access to sensitive information and systems, and comes just weeks after CVE-2023-22515, a previous vulnerability in the same Confluence products.

Imperva customers are protected against these vulnerabilities.

Apple's Find My network exploited for keylogging

+Keylogging

- Researchers discovered a flaw in Apple's [Find My](#) network that can be abused to steal keylogged passwords. The vulnerability allows attackers to send and receive data using the network, potentially compromising user data.

Data Breaches

Largest Indian data breach to date exposes 815M records

+India +Healthcare

- A significant data leak was traced back to samples from the [Indian Council of Medical Research](#) (ICMR). The exposed data contained sensitive COVID-19 test data for over 815M Indian citizens.

LastPass breach compromises crypto wallets

+Crypto

- A hacker known as "zachxbt" exploited a vulnerability in [LastPass](#), leading to the theft of millions of cryptocurrency wallets. Users are advised to change their passwords and enable multi-factor authentication.

BlackBasta compromises Canadian library

+BlackBasta +Government +Canada

- The [Toronto Public Library's](#) systems were compromised by the BlackBasta ransomware, leading to outages. The library is taking measures to mitigate the impact and recover from the attack.

US defense officials' emails stolen in MoveIT hacks

+US +Government +MoveIT

- A breach in the [MoveIT](#) platform resulted in unauthorized access to emails of over 630,000 US defense officials. The extent of the information accessed is being assessed.

Ransomware attack shuts down German municipalities

+Government +Germany

- A massive ransomware attack affected various services across [Germany](#). An unknown attacker accessed a municipal IT provider, and 70 municipalities shut down online services to prevent the ransomware from spreading.

AlphV targets clinical software provider

+AlphV +Healthcare +Technology

- [Advarra](#), a clinical trial software provider, became a victim of the AlphV ransomware after the gang used a SIM-swapping attack on an executive. The company is working on restoring affected systems and has alerted its clients about potential disruptions.

Lockbit strikes major Mexican airport

+Mexico +Travel +LockBit

- The [Querétaro Intercontinental Airport](#) in Mexico was targeted by a cyberattack. The LockBit ransomware gang has claimed responsibility for the attack, and has threatened to leak data.

Hilb faces data leak incident

+Financial Services

- Financial services company [Hilb](#) has suffered a data leak exposing the personal information of over 81,000 people. The company believes criminals accessed employee emails to steal the data in early 2023.

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