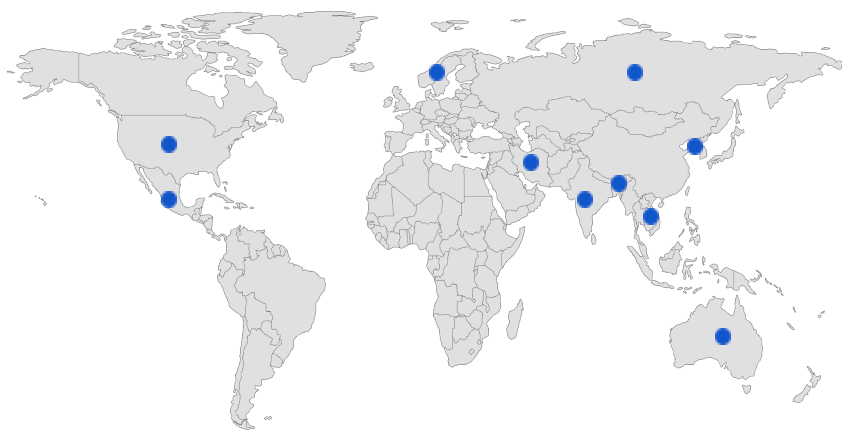


Threat Intel Report: November 13-19, 2023

Countries



Top Tags

ALPHV

SpyAgent

Medusa

Randstorm

Reptar

Executive Summary

Actionable Information:

- *Geopolitical malware:* The BiBi Wiper malware in Israel, attributed to Iranian-backed APT groups, highlights the rising trend of geopolitical cyber warfare. Organizations, especially in the education and technology sectors, need to enhance their defenses against such targeted attacks.
- *Exploitation of misconfigurations:* The Python malware exploiting Docker API misconfigurations for DDoS attacks underlines the critical importance of proper configuration and security hygiene in preventing such exploitations.
- *Targeted social engineering:* Vietnamese hackers targeting Indian marketers using Delphi-powered malware via Facebook ads demonstrate the evolving sophistication of social engineering tactics. Businesses must be vigilant about such targeted campaigns that exploit trusted platforms.
- *Vulnerabilities in common tools:* The SQL injection vulnerability in the WP Fastest Cache plugin and the Reptar CPU vulnerability in Intel systems emphasize the need for regular updates and patch management in both software and hardware components.
- *Cryptocurrency risks:* The Randstorm flaw in cryptocurrency wallets and the massive theft from Poloniex platform highlight the ongoing vulnerabilities in the cryptocurrency sector, necessitating enhanced security measures for wallet protection.

Outlook:

The current threat landscape is increasingly complex and multifaceted, with significant implications for a wide range of sectors. The rise in geopolitical cyberattacks, such as those seen in Israel, indicates a need for heightened awareness and preparedness for state-sponsored cyber activities. The exploitation of software vulnerabilities and misconfigurations, as seen in the Docker API and WordPress plugin incidents, calls for a renewed focus on cybersecurity

fundamentals, including regular updates, patches, and secure configurations. The trend of using social engineering tactics to exploit trusted platforms, as observed in the Vietnamese campaign against Indian marketers, suggests that organizations must invest in advanced threat detection and employee training to counter sophisticated phishing and malware distribution strategies. Finally, the vulnerabilities and attacks in the cryptocurrency domain underscore the need for robust security protocols and awareness among users and platforms dealing with digital assets. As the threat landscape evolves, organizations must adapt their cybersecurity strategies to address these diverse and dynamic challenges.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 12% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

⬇ 56% [CVE-2022-22965](#)

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

⬇ 51% [CVE-2023-35078](#)

- A remote unauthenticated API access vulnerability in Ivanti Endpoint Manager Mobile

US telecom company targeted by RCE

+US +Telecommunications

- On November 18, a US telecommunications company was targeted by remote code execution (RCE) attacks at rates 1,560% above average. Attacks primarily came from Poland and the Netherlands, and probably attempted to steal valuable customer data.

Largest retail DDoS attack reaches almost 2.5M RPS

+Retail +DDoS

- The largest DDoS attack we've seen in the retail industry occurred on November 13, reaching a maximum of 2.4M requests per second (RPS). The attack came from 6,300 distinct IP addresses, and marks a significant warning for the retail industry as we go into the holiday shopping season.

Recent Cyber Threats

Rising threat of BiBi Wiper malware in Israel

+Israel +Iran

- [Israeli computers](#) are increasingly targeted by data-wiping attacks from variants of the BiBi malware family, affecting both Linux and Windows systems. These attacks, attributed to an Iranian-backed APT group, have significantly impacted Israeli organizations, particularly in the education and technology sectors, leading to data destruction and operational disruption.

Python malware exploits Docker API for DDoS attacks

+Python +DDoS

- Attackers are exploiting misconfigurations in publicly exposed [Docker Engine APIs](#) to deploy Python malware, functioning as a DDoS bot agent. This malware, compiled as an ELF executable, targets various systems with different DoS attack methods.

Vietnamese hackers target Indian marketers with Delphi-powered malware

+Vietnam +India +Delphi

- [Vietnamese threat actors](#), known for the Ducktail stealer malware, have launched a new campaign targeting Indian marketers. This campaign aims to hijack Facebook business accounts using Delphi as the programming language. The attackers use sponsored ads on Facebook to spread malicious ads and deploy malware, leading to unauthorized access and financial exploitation of the hijacked accounts.

SQL injection vulnerability in WP fastest cache plugin

+WordPress

- Over 600,000 WordPress sites are at risk due to an SQL injection vulnerability in the [WP Fastest Cache](#) plugin. This vulnerability allows unauthenticated attackers to access the site's database, potentially exposing sensitive user data, account passwords, and configuration settings. Users are urged to update to the latest version of the plugin to mitigate this high-severity security risk.

Intel's Reptar CPU vulnerability exposed

+Reptar +CVE

- A new vulnerability named [Reptar](#) has been discovered in Intel's desktop and server systems, impacting both performance and security. This flaw, present in Intel's CPUs, could potentially allow attackers to gain unauthorized access or disrupt system operations. The impact of this vulnerability is significant due to the widespread use of Intel CPUs in various computing environments.

Randstorm flaw endangers cryptocurrency wallets

+Randstorm +Cryptocurrency

- The [Randstorm](#) flaw, a vulnerability in cryptocurrency wallets, poses a significant risk to users. This flaw could potentially allow attackers to access private keys and steal funds from these wallets.

Google Workspace includes plaintext vulnerability

+CVE

- A security vulnerability in [Google Workspace](#) was discovered, allowing attackers to access and read data in plaintext. This weakness in Google's system could lead to significant data breaches and privacy concerns for users and organizations relying on Google Workspace for their operations.

ALPHV ransomware exploits Google ads

+ALPHV +Ransomware

- The notorious ALPHV ransomware gang has been using Google Ads to distribute [Nitrogen](#) malware, targeting corporations and public entities. This new tactic involves luring business professionals to attacker-controlled websites, where they unknowingly download Nitrogen malware, leading to ransomware infections.

Exploitable vulnerabilities discovered in several AI/ML tools

+AI +ML

- Over a dozen exploitable vulnerabilities have been found in [AI/ML tools](#), including H2O-3, MLflow, and Ray. These vulnerabilities expose AI/ML models to risks such as system takeover and sensitive information theft, potentially impacting the entire AI/ML supply chain.

Data Breaches

Poloniex platform hit by major theft

+Cryptocurrency

- Hackers stole millions from the [Poloniex](#) cryptocurrency platform by exploiting a vulnerability in the withdrawal process. The attackers created fake accounts, deposited small amounts, and then withdrew large sums, leading to significant financial losses.

Ransomware disrupts Ohio city services

+US +Government

- A ransomware attack in [Huber Heights, Ohio](#), significantly impacted multiple city divisions, including Zoning, Engineering, Tax, Finance, Utilities, Human Resources, and Economic Development. Public safety services remained unaffected, but the attack caused disruptions in city operations and services.

Ethereum function exploited for massive theft

+Cryptocurrency

- Malicious actors abused Ethereum's '[Create2](#)' function to bypass wallet security alerts and poison cryptocurrency addresses. This led to the theft of \$60 million from 99,000 victims over six months, with losses for some individuals reaching up to \$1.6 million.

Australian logistics firm suffers disruptive cyberattack

+Australia +Logistics

- A cyberattack on [DP World Australia](#), a major logistics firm, severely disrupted freight movement in several large Australian ports. The attack caused significant delays, with about 30,000 shipping containers, including time-sensitive goods, stranded and unable to move.

Denmark's largest cyberattack targets energy sector

+Denmark +Russia +Energy

- Hackers, potentially linked to the Russian GRU, launched a coordinated cyberattack on [Danish critical infrastructure](#), targeting 22 companies in the energy sector. The attackers exploited zero-day vulnerabilities in Zyxel firewalls, leading to significant security breaches and operational disruptions.

Truepill pharmacy data breach exposes millions of records

+Healthcare

- [Truepill](#), a mail-order pharmacy, experienced a data breach affecting nearly 2.4 million people. The breach, discovered in July 2022, exposed sensitive patient information, including names, email addresses, phone numbers, and prescription details.

Mexican casino oversight compromises gambler data

+Gambling +Mexico

- [Strendus](#), a prominent Mexican casino, inadvertently exposed the personal data of thousands of its online gamblers for at least two weeks due to a misconfigured Elasticsearch server. The exposed data included names, emails, and betting details.

SpyAgent malware targets South Korean smartphone users

+Spy Agent +South Korea

- A new [SpyAgent](#) campaign in South Korea has infected over 200 devices since early October. Distributed through phishing sites promoting rogue applications, the malware collects contact information and text messages, sending them to a server controlled by the attackers.

Vietnam Post Corporation data leak exposes sensitive information

+Vietnam +Government

- [Vietnam Post Corporation](#), a government-owned postal service, inadvertently exposed 1.2TB of data, including security logs and employee email addresses. The data was accessible for at least 87 days, and could have been exploited by malicious actors.

Toyota hit by Medusa ransomware attack

+Medusa +Automotive

- [Toyota Financial Services](#) in Europe and Africa was targeted in a cyberattack by the Medusa ransomware gang, who claimed to have stolen data and demanded an \$8 million ransom. Toyota acknowledged the attack, stating that it had taken systems offline and was working with law enforcement.

Bangladesh's database leak exposes sensitive personal data

+Bangladesh +Government

- The [National Telecommunication Monitoring Centre](#) in Bangladesh inadvertently exposed a vast database containing extensive personal information to the open web. The leaked data included names, professions, blood groups, parents' names, phone numbers, call durations, vehicle registrations, passport details, and fingerprint photos. The database was unsecured for months and recently attacked by hackers, who claimed to have stolen the information.

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