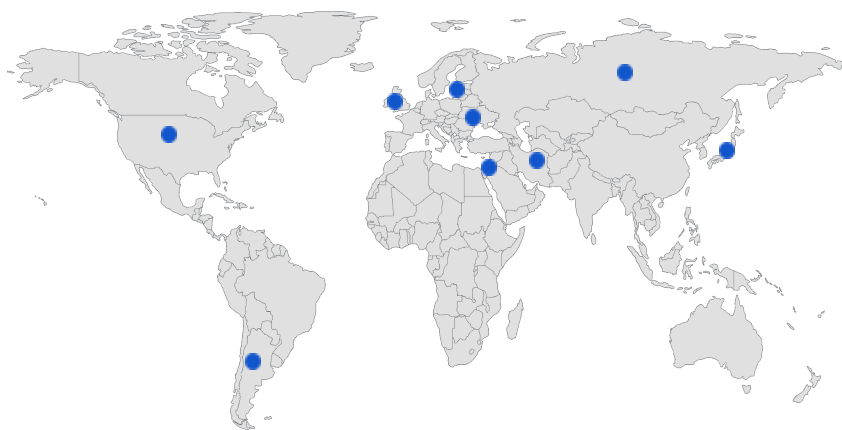


Threat Intel Report: December 11-31, 2023

Countries



Top Tags

LockBit

ALPHV

Killnet

CyberAv3ngers

Rhysida

Executive Summary

Actionable Information:

- **Vulnerability exploits:** Recent cyber threats have heavily exploited vulnerabilities in widely used systems and applications, such as mobile password managers (AutoSpill flaw in Android apps), WordPress plugins, and Microsoft Outlook (zero-click RCE exploit).
- **Ransomware and malware attacks:** The ALPHV ransomware gang's dark web leak site seizure and the discovery of JaskaGO malware targeting Windows and macOS systems highlight the ongoing prevalence of ransomware and sophisticated malware.
- **Data breaches and information theft:** Significant data breaches have occurred in various sectors, including healthcare, real estate, and financial services, with incidents like the DonorView breach and the theft of 1.5 billion real estate records.
- **Cyberwarfare activities:** The Russia-Ukraine conflict continues to manifest in cyberspace, with attacks on utilities, telecommunications, and government entities, indicating a trend of state-sponsored or politically motivated cyberattacks.
- **Emerging techniques:** Novel techniques like SMTP smuggling and Google session hijacking in info-stealing malware demonstrate the evolving tactics of cybercriminals to bypass security measures and gain unauthorized access.

Outlook:

The current landscape of cyber threats is marked by a mix of sophisticated attacks targeting critical vulnerabilities, persistent ransomware threats, and politically motivated cyberwarfare activities. The trend of exploiting existing vulnerabilities in widely used systems and applications is particularly concerning, as it indicates a high potential for widespread impact. The involvement of state-sponsored actors in cyberwarfare activities, especially in the context of



the Russia-Ukraine conflict, underscores the need for heightened vigilance in national security and critical infrastructure sectors. Additionally, the emergence of new techniques like SMTP smuggling and session hijacking points to the evolving sophistication of cybercriminals, necessitating continuous adaptation and enhancement of cybersecurity measures. Overall, the threat landscape calls for proactive and comprehensive strategies to address the diverse and evolving nature of cyber threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 26% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

⬇ 6% [CVE-2023-35078](#)

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

⬇ 4% [CVE-2023-35082](#)

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

Apache OFBiz vulnerability exploited by attackers

+SSRF +US +Financial Services

- On December 26, researchers discovered an authentication bypass vulnerability in [Apache OFBiz](#), tracked as CVE-2023-51467. This bug has a CVSS score of 9.8 and allows attackers to achieve server-side request forgery (SSRF) by bypassing the program's authentication. In less than one day, Imperva observed over 30,000 attempted attacks exploiting CVE-2023-51467. Attackers primarily used automated tools and targeted mainly US-based financial services sites.

Imperva customers are protected against CVE-2023-51467.

Argentinian gambling site targeted in 2M RPS attack

+DDoS +Argentina +Gambling

- An Argentinian gambling site was targeted on December 28 by a DDoS attack reaching over 2M requests per second (RPS). Attacks came from 2000 primarily US-based IP addresses.

Recent Cyber Threats

Vulnerability in mobile password managers exposes user credentials

+AutoSpill +Android

- Researchers discovered a vulnerability, named [AutoSpill](#), in popular mobile password managers that could expose user credentials. The flaw occurs in the autofill functionality of Android apps, where password managers may incorrectly target user login information, potentially exposing credentials to malicious apps. The issue affects several password managers, including 1Password, LastPass, Keeper, and Enpass.

Critical bug in WordPress backup plugin endangers 50K sites

+WordPress

- A critical vulnerability in the WordPress plugin [Backup Migration](#), installed on over 90,000 sites, could allow attackers to execute remote code and fully compromise vulnerable websites. The bug, tracked as CVE-2023-6553, affects plugin versions up to 1.3.6. Despite the availability of a patched version, nearly 50,000 WordPress sites using vulnerable versions remain at risk. The flaw allows unauthenticated attackers to execute arbitrary commands on the server.

NKAbuse malware exploits NKN blockchain for DDoS attacks

+NKAbuse +DDoS +IoT

- [NKAbuse](#), a new multi-platform threat, uses the NKN (New Kind of Network) protocol for data exchange between peers, functioning as a potent implant with both flooder and backdoor capabilities. This malware targets Linux systems, including IoT devices, primarily in Colombia, Mexico, and Vietnam. It exploits a critical security flaw in Apache Struts to breach systems and has different versions to support various CPU architectures.

Zero-click in Outlook discovered

+Microsoft

- Researchers discovered two new Windows vulnerabilities, CVE-2023-35384 and CVE-2023-36710, that can be chained for a [zero-click RCE exploit](#) in Microsoft Outlook. The exploit requires no user interaction and was found while investigating a previous Outlook mitigation bypass. Microsoft has addressed these issues, but the custom sound notification feature in Outlook continues to pose risks.

SMTP smuggling technique bypasses email security

+SMTP

- A novel [SMTP smuggling technique](#) allows attackers to bypass DMARC and other email protections, enabling targeted phishing attacks from legitimate sources. The technique exploits zero-day flaws in messaging servers from Microsoft, GMX, and Cisco, affecting millions of SMTP servers. Microsoft and GMX have patched their systems, while Cisco's vulnerability remains unaddressed.

Iran's fuel supply disrupted by major cyberattack

+Iran +Predatory Sparrow

- Iran experienced a major cyberattack targeting its fuel supply system, causing nearly 70% of gas stations across the country to shut down. The group [Predatory Sparrow](#) claimed responsibility, stating the attack was controlled and measures were taken to limit potential damage to emergency services. The attack is part of ongoing cyber conflicts involving Iranian infrastructure.

JaskaGo malware targets both Windows and Mac

+JaskaGo

- AT&T Alien Labs discovered [JaskaGO](#), a sophisticated malware strain targeting both Windows and macOS. Crafted in the Go programming language, JaskaGO has low detection rates by traditional antivirus solutions. It is equipped with extensive commands from its C&C server and can persist in infected systems, posing a high risk of data compromise, including browser credentials and cryptocurrency wallet details.

Law enforcement seizes ALPHV leak site

+ALPHV

- An international coalition of law enforcement agencies, including the FBI, seized the dark web leak site of the notorious [ALPHV](#) ransomware gang. The operation involved agencies from the UK, Denmark, Germany, Spain, and Australia. The FBI also released a decryption tool, helping over 500 victims restore their systems and preventing ransom payments totaling approximately \$68 million.

Info-stealing malware now capable of Google session hijacking

+Authentication +Session Hijacking

- Multiple malware-as-a-service info stealers, including Lumma Stealer, now have the capability to [manipulate authentication tokens](#), allowing persistent access to a victim's Google account even after password resets. This exploit targets the OAuth 2.0 security protocol and has been adopted by various malware groups, posing a severe threat to Google-connected accounts and services.

Russia/Ukraine:

+Russia +Ukraine +Killnet +Blackjack +Telecommunications +Financial Services +Utilities

Russian water utility cyberattack impacts 6000 systems

- [Rosvodokanal](#), a Russian water utility firm, was reportedly attacked by the Ukrainian hacker group Blackjack, impacting over 6,000 computer systems and erasing more than 50 terabytes of data. The attack, which could be seen as retaliation for a previous cyberattack on Ukraine's Kyivstar, involved the deletion of backup files, correspondence, and internal documents.

Ukrainian telecommunications company targeted in cyberattack

- Ukrainian telecom operator [Kyivstar](#) was hit by a cyberattack that disrupted internet access and mobile communications. The attack coincided with Ukrainian President Volodymyr Zelenskyy's visit to Washington. Kyivstar, with over 24.3 million mobile subscribers, reported no compromise of personal data. The attack's attribution is uncertain, with suggestions of Russian state hackers and claims by the hacktivist group KillNet.

Ukrainian intelligence claims hack on Russia's tax service

- Ukraine's defense intelligence directorate (GUR) claimed responsibility for a cyberattack on Russia's [federal tax service](#) (FNS), infecting thousands of servers with malware and destroying databases and backups. The attack reportedly paralyzed internet connections between FNS's central office and regional branches. This operation follows GUR's previous cyberattack on Russia's civil aviation agency, Rosaviatsia.

Data Breaches

Graphic footage broadcast in UAE TV hack

+UAE +News

- A group of hackers targeted a [UAE television service](#), replacing broadcasts with graphic footage from the Israel-Hamas conflict. The hackers interrupted European live channels, including BBC News, with a message followed by a fake news broadcast showing alleged Israeli military atrocities. The attack, targeting an unnamed local set-top box provider, affected numerous UAE citizens and is under investigation.

Non-profit donations exposed in DonorView breach

+Healthcare +Financial Services

- Nearly a million records containing personal information of donors to non-profits were exposed in an online database owned by [DonorView](#). Security researcher Jeremiah Fowler discovered the breach, which included sensitive data like names, addresses, and medical conditions of children. The breach's duration is unknown, and DonorView, used by major charities, has yet to respond.

Idaho National Laboratory targeted by SiegedSec

+Government +US +SiegedSec

- The [Idaho National Laboratory](#) reported a cyberattack that compromised the data of over 45,000 individuals, including employees and their families. The attack, attributed to the hacktivist group SiegedSec, accessed sensitive information stored in an off-site data center. The breach is under federal investigation, and victims are being offered identity protection services.

Genetic testing company hit by major data theft

+Estonia +Healthcare

- [Asper Biogene](#), an Estonian genetic testing company, reported a data leak affecting about 10,000 people. The breach, involving personal and health data, is under criminal investigation. The data includes genetic testing results, and affected healthcare providers are notifying individuals. The company faced a financial demand after the attack.

Xfinity discloses data breach affecting 35M people

+Telecommunications +US

- [Xfinity](#) reported a data breach affecting over 35 million people. The breach, linked to a Citrix server vulnerability, exposed customer-sensitive information. Xfinity has asked users to reset passwords and is investigating the full impact of the incident.

1.5 billion real estate records leaked, including celebrity data

+Real Estate +US

- An unprotected database from [Real Estate Wealth Network](#) exposed 1.5 billion records, including real estate ownership data of celebrities like Elon Musk and Donald Trump. Discovered by cybersecurity researcher Jeremiah Fowler, the 1.16 TB database contained sensitive information such as property owners, sellers, investors, and internal user logging data. The exposure raises concerns about privacy and security risks for both celebrities and common homeowners.

Dark web carding marketplace leaks millions of credit card details

+Carding +Financial Services +BidenCash

- [BidenCash](#), a notorious dark web carding marketplace, leaked over 1.6 million valid payment card details, including debit and credit card information. The leak, which did not include cardholders' names or emails, poses a significant risk of financial fraud and identity theft. The exposed data, consisting of card numbers, expiry dates, and CVV numbers, could be exploited for unauthorized transactions.

LockBit targets accounting firm, German hospital

+LockBit +UK +Financial Services +Germany +Healthcare

- The [LockBit](#) ransomware group claimed responsibility for hacking the Xeinadin accountancy firm, threatening to release 1.5 terabytes of stolen customer data. The compromised data includes internal databases, customer financials, passports, account balances, and legal information. The group set a deadline for Xeinadin to contact them, failing which they plan to publish the data.
- https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/?&web_view=true
- The Katholische Hospitalvereinigung Ostwestfalen (KHO) in Germany confirmed disruptions at three hospitals due to a LockBit ransomware attack. The attack encrypted data and impacted critical hospital systems, leading to the unavailability of emergency care. Investigations are ongoing to determine the extent of the damage and whether patient data was stolen.

Rhysida ransomware group attacks Japanese hospital

+Rhysida +Japan +Healthcare

- The [Rhysida](#) ransomware group claimed to have hacked Abdali Hospital in Jordan, threatening to auction off sensitive data for 10 BTC. The group published images of stolen documents, including ID cards and contracts, as proof of the hack. The ransomware operators plan to sell the stolen data to a single buyer and release it publicly if not sold.

ALPHV group targets Fidelity subsidiary

+ALPHV +Financial Services

- [LoanCare](#), a subsidiary of Fidelity National Financial, reported a data breach affecting 1.3 million people. The breach, resulting from a cyberattack in November, exposed names, addresses, Social Security numbers, and loan numbers. Victims are being offered identity protection services, and the incident is linked to the AlphV ransomware gang.

IEC data breach claimed by CyberAv3ngers

+Israel +Iran +CyberAv3ngers +Utilities

- The hacker group [CyberAv3ngers](#) claimed to possess 1TB of data from Israel's electricity infrastructures, allegedly from an IEC data breach. The group is selling the data for 5 BTC and has posted proof of concept details online. The authenticity of these claims is yet to be verified, and the IEC has not issued an official statement.



Patients targeted with extortion emails after data breach

+US +Healthcare

- Patients of [INTEGRIS Health](#) in Oklahoma received extortion emails following a cyberattack on the healthcare network. The emails demanded payment to prevent the sale of stolen personal data, including Social Security numbers and medical information. The attack confirms the theft of patient data, and INTEGRIS Health has warned recipients against responding to these emails.

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