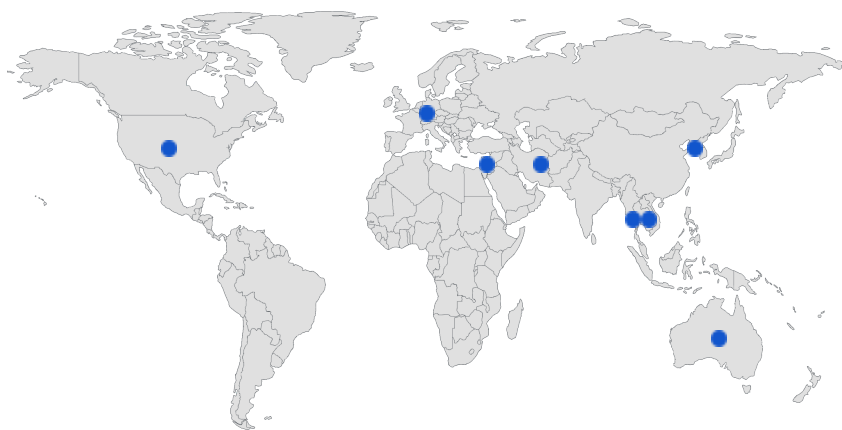


Threat Intel Report: December 4-10, 2023

Countries



Top Tags

ALPHV

APT28

Malek Team

Andariel

Lazarus

Executive Summary

Actionable Information:

- **Ransomware and malware attacks:** A significant trend is the continued prevalence of ransomware and malware attacks, targeting various sectors including education, healthcare, and defense. Notable examples include the Black Suit ransomware attack on DePauw University and the ALPHV ransomware gang's breach of HTC Global Services.
- **Exploitation of vulnerabilities:** Cybercriminals are exploiting vulnerabilities in widely-used systems and protocols. The exploitation of the CVE-2023-23397 Outlook flaw by APT28 and the DICOM standard's security weaknesses leading to patient data exposure are key instances.
- **Targeted phishing campaigns:** Phishing remains a common tactic, with campaigns like the MrAnon Stealer malware targeting users through fake hotel bookings and Android loan apps deceiving users in Southeast Asia, Africa, and Latin America.
- **Data exposures due to misconfigurations:** Several incidents of data exposure due to misconfigurations in cloud services were observed, including the WALA cloud misconfiguration and the Android Barcode to Sheet app's Firebase database leak.
- **State-sponsored cyber espionage:** The Andariel group's theft of South Korean defense data highlights the ongoing threat of state-sponsored cyber espionage.
- **Increased attacks on utility companies:** There has been a noticeable increase in cyberattacks targeting utility companies over the past few weeks, as evidenced by the ransomware attack on the St. Johns River Water Management District in Florida and the Ho Chi Minh City Energy Company. These attacks pose a significant risk to critical infrastructure and public safety.

Outlook:

The current landscape of cyber threats demonstrates a diverse range of attack vectors, with state-sponsored activities, ransomware, and phishing campaigns at the forefront. The exploitation of vulnerabilities in both old and new technologies indicates that attackers are continuously adapting their strategies to exploit any available weakness. The trend of targeting healthcare and educational institutions is particularly concerning due to the sensitive nature of the data involved. Organizations must prioritize robust cybersecurity measures, including regular vulnerability assessments, employee training against phishing, and secure configurations of cloud services. The outlook suggests an increasing need for multi-layered security approaches and collaboration between entities to share threat intelligence and best practices.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 23% [CVE-2022-21371](#)

- a path traversal vulnerability in Oracle WebLogic Server

↓ 24% [CVE-2022-22965](#)

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

↓ 25% [CVE-2023-35078](#)

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

US healthcare site targeted in broad attacks

+US +Healthcare +RCE +XSS +Path Traversal

- A US healthcare site was targeted this week with remote code execution (RCE), cross site scripting (XSS), and path traversal attacks at abnormal levels for the site. Attacks came from 8,800 UK-based IPs.

Low and slow attack targets Thai site

+Thailand +Entertainment

- A Thai entertainment site saw an attempted two-day DDoS attack this week. Although the maximum requests per second (RPS) were relatively low at about 550,000, the attack lasted almost 40 hours in a relatively "low and slow" attack style. Attacking IPs came mostly from the US and Brazil.

Recent Cyber Threats

ScrubCrypt facilitates RedLine Stealer deployment in ATO attacks

+RedLine +ScrubCrypt +Malware

- Researchers have discovered a new build of [ScrubCrypt](#), an obfuscation tool used in account takeover attacks to deploy RedLine Stealer malware. This malware targets end users to compromise accounts by stealing credentials and cryptocurrency wallet information.

Mac users targeted with proxy malware

+MacOS +Trojan

- Cybercriminals are targeting [Mac users](#) with a new proxy trojan malware, which is bundled with pirated macOS software on warez sites. This malware turns infected computers into traffic-forwarding terminals, anonymizing malicious activities. The campaign exploits users' tendency to download pirated software, posing significant risks to their systems.

APT28 exploits Outlook vulnerability to hijack Exchange accounts

+APT28 +Russia

- Microsoft has reported that Russian state-sponsored actor [APT28](#) is actively exploiting the CVE-2023-23397 Outlook flaw to hijack Microsoft Exchange accounts and steal sensitive information. Targeting entities in the US, Europe, and the Middle East, this campaign also exploits other vulnerabilities, posing a significant threat to key organizations.

Open-source library flaw endangers multiple NFT collections

+NFTs

- A vulnerability in a widely-used open-source library impacts the security of pre-built smart contracts, affecting multiple [NFT collections](#), including those on Coinbase. The flaw was disclosed by Web3 development platform Thirdweb, which pushed a remediation but did not reveal specific details. The vulnerability has caused concern among NFT holders and platforms, prompting urgent mitigation measures.

Android loan apps targeting Southeast Asia, Africa, and Latin American users

+Android loan apps +Financial Services

- Researchers have identified a surge in deceptive Android loan apps since early 2023. These apps, disguised as legitimate personal loan services, defraud users with high-interest-rate loans and collect personal and financial information for blackmail. Despite appearing on official platforms like Google Play, these apps, termed [SpyLoan](#), have been primarily targeting users in Southeast Asia, Africa, and Latin America.

Fake lockdown mode on iOS devices

+iOS

- A new post-exploitation tampering [technique](#) can trick users into believing their iOS device is in Lockdown Mode when it's not. This technique, which doesn't exploit a flaw in Lockdown Mode itself, is possible only on compromised or jailbroken iPhones. It highlights the limitations of Lockdown Mode, which doesn't stop malware from operating on an already compromised device.

AWS security token service exploited for cloud account infiltration

+AWS +Cloud data

- Threat actors are exploiting [Amazon Web Services Security Token Service](#) to infiltrate cloud accounts and conduct attacks. By impersonating user identities and roles, they can steal long-term IAM tokens through malware, exposed credentials, or phishing, and create additional IAM users for persistence.

SLAM attack compromises kernel data on modern CPUs

+SLAM +Side-channel attack

- A new side-channel attack called [SLAM](#) targets hardware features in CPUs from Intel, AMD, and Arm. This attack exploits memory features like Linear Address Masking (LAM) to steal sensitive data like root password hashes from kernel memory. SLAM affects future chips with specific criteria and leverages transient execution techniques to exploit Spectre disclosure gadgets.

WordPress addresses critical RCE vulnerability in latest update

+WordPress +RCE

- [WordPress](#) released version 6.4.2 to fix a remote code execution (RCE) vulnerability, potentially allowing attackers to run arbitrary PHP code on websites. This vulnerability, stemming from a Property Oriented Programming (POP) chain in WordPress core 6.4, could be exploited in conjunction with flaws in plugins or themes. Over 800 million sites using WordPress were at risk, prompting urgent updates to mitigate this significant security threat.

MrAnon stealer campaign targets users with bogus hotel bookings

+MrAnon +Germany

- A phishing campaign has been discovered deploying [MrAnon Stealer](#) malware through emails with fake hotel booking details. The emails contain a malicious PDF that downloads a .NET executable file, which then runs a PowerShell script to fetch the final Python-based malware. This malware, designed to steal credentials, system information, browser sessions, and cryptocurrency extensions, primarily targeted users in Germany, indicating a region-specific attack strategy.

HeadCrab malware variant takes over thousands of servers

+HeadCrab +Cryptomining

- The [HeadCrab](#) malware, known for adding infected devices to a botnet for cryptomining and other attacks, has emerged with a new variant. This variant has infected over 1,100 servers, adding to the 1,200 servers already compromised by the first variant. The malware exhibits rootkit-like actions, controlling responses and remaining undetected. It primarily targets Redis servers, using them for cryptomining and potentially other malicious activities.

Data Breaches

WeMystic's open database exposes user data

+Exposed database

- [WeMystic](#), a website focused on astrology and spiritual guidance, inadvertently exposed 34GB of sensitive user data due to an open and passwordless MongoDB database. The exposed data included personal details like names, email addresses, dates of birth, IP addresses, gender, and horoscope signs of over 13.3 million users. This security lapse posed significant risks, as attackers could exploit this data for targeted attacks or other malicious purposes.

DePauw University hit by ransomware

+Education +US +Black Suit

- [DePauw University](#) in Indiana suffered a data breach and ransomware attack, compromising personal information of students. Detected on October 31, the university worked with law enforcement and cybersecurity experts to investigate the incident. The Black Suit ransomware gang claimed responsibility, alleging to have stolen 214 GB of data. The attack disrupted campus internet services and is part of a growing trend of ransomware attacks targeting educational institutions.

Exposed Hugging Face API tokens pose threat to major tech projects

+API +AI

- Over 1,500 API tokens from major tech companies like Meta, Microsoft, and Google were found exposed on [Hugging Face](#), an open-source data science and machine learning platform. This exposure could have led to supply chain attacks, data theft, or model poisoning, affecting major AI and ML projects. The companies have since revoked the tokens and secured their repositories, but the incident highlights the importance of securing API tokens in AI and ML supply chains.

ALPHV ransomware targets Vietnam energy organization

+ALPHV +Energy +Vietnam

- The ALPHV ransomware group reportedly targeted [Ho Chi Minh City Energy Company](#), a subsidiary of Vietnam Electricity, leading to a significant data breach. The group threatened to report the incident to the Vietnam Department of Energy, with 84 samples of the breached data posted on the dark web.

WALA cloud misconfiguration exposes pet owners' data

+Australia +Pets

- The [Worldwide Australian Labradoodle Association](#) (WALA) experienced a data leak due to a cloud server misconfiguration, exposing over 56,000 documents and 25GB of sensitive data. This breach included personal information of pet owners, dog microchip numbers, and medical details. The exposed data poses risks such as pet theft, insurance fraud, and identity theft.

Iran-linked hackers allegedly leak Israeli hospital data

+Israel +Iran +Healthcare +Malek Team

- Malek Team, a hacker group allegedly linked to Iran, claimed responsibility for leaking thousands of medical records from [Ziv Medical Center](#) in Israel. The leaked data reportedly includes personal and medical information of patients, including Israeli soldiers.

Florida water agency targeted in ransomware attack

+US +Water

- The [St. Johns River Water Management District](#) in Florida confirmed a cyberattack following a ransomware gang's claim of the incident. This attack coincides with warnings from U.S. cybersecurity agencies about foreign attacks on water utilities.

HTC Global Services confirms cyberattack following data leak

+Computing and IT +ALPHV

- [HTC Global Services](#), an IT services and business consulting company, confirmed a cyberattack after the ALPHV ransomware gang leaked data online. The breach potentially involved sensitive information, including passports and confidential documents. The attack, possibly linked to the Citrix Bleed vulnerability, highlights the ongoing threat ransomware poses to global enterprises and the importance of robust cybersecurity defenses.

North Korean hackers steal South Korean defense data

+Andariel +Lazarus +North Korea +South Korea +Defense

- The Seoul Metropolitan Police Agency accused the North Korean hacker group Andariel of stealing 1.2TB of sensitive defense data from [South Korean defense companies](#). The data included information on advanced anti-aircraft weapons. Andariel, believed to be a subgroup of the Lazarus Group, also extorted about \$357,000 in bitcoin from various companies.

East River Medical Imaging informs patients of SSN-affecting data leak

+Healthcare +US

- [East River Medical Imaging](#) (ERMI) reported a data breach affecting over 605,000 patients. The breach involved unauthorized access to sensitive patient information, including names, Social Security numbers, contact information, insurance details, and medical data. ERMI began sending out data breach notification letters to affected individuals, advising them to be vigilant against potential fraud or identity theft.

US DoD contractor hit by cyberattack

+Defense +US +Hunters International

- [Austal USA](#), a shipbuilding company and contractor for the U.S. Department of Defense and Homeland Security, confirmed a cyberattack after the Hunters International ransomware group leaked data online. The leaked data included compliance documents, recruiting information, finance details, certifications, and engineering data.

Millions of patient records exposed due to DICOM security flaws

+Healthcare

- Researchers found that thousands of servers are exposing the medical records and personal health information of millions of patients due to security weaknesses in the [DICOM](#) (Digital Imaging and Communications in Medicine) standard. Over 3,800 servers in more than 110 countries are leaking patient data, including names, genders, addresses, phone numbers, and in some cases, Social Security numbers. The exposed data totals over 43 million health records, with the majority of exposed servers located in the United States.

Android barcode scanner app leaks user passwords

+Android

- The Android app [Barcode to Sheet](#), with over 100,000 Google Play downloads, was found to be leaking sensitive user information due to an open Firebase database. The exposed data, totaling over 368MB, included enterprise data stored in plaintext and user passwords in the MD5 hash format. The leak poses risks of phishing, credential stuffing, and identity theft, as the data could be exploited by threat actors for malicious purposes.

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