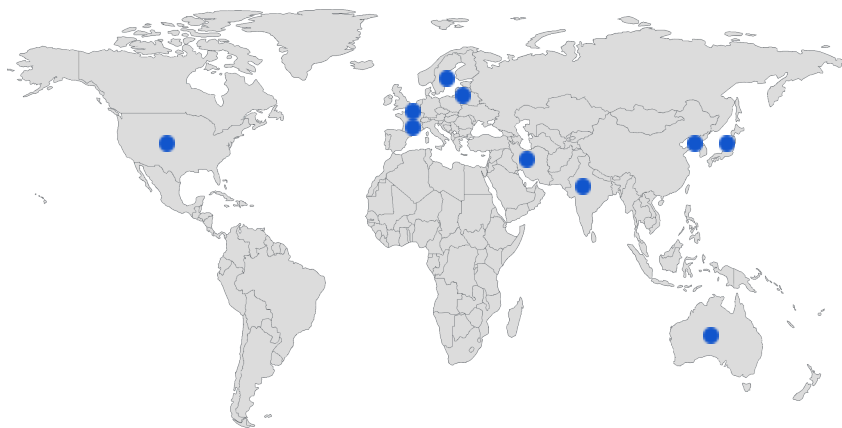


Threat Intel Report: January 1-7, 2024

Countries



Top Tags

BlueNoroff

Irleaks

Cactus

Belarusian Cyber Partisans

IntelBroker

Executive Summary

Actionable Information:

- *Privilege escalation and misconfigurations:* Recent incidents, including the Google Kubernetes Engine exploit and the Google Drive misconfiguration by Ateam, highlight the critical importance of proper configuration and the dangers of privilege escalation in cloud environments.
- *Account takeovers and data breaches:* The misuse of Google OAuth by malware, the Spotify music converter data leak, and the MyEstatePoint app breach underscore the ongoing threat of account takeovers and the need for robust data protection measures.
- *Ransomware and malware threats:* The Cactus ransomware attack on Coop and the discovery of cryptocurrency miners in Python packages indicate the persistent threat of ransomware and malware, particularly targeting financial and technology sectors.
- *Nation-state cyber activities:* The MacOS backdoor linked to North Korean hackers and the Belarusian hacktivists' attack on a state-owned news agency reflect the continued involvement of nation-state actors in cyber espionage and propaganda efforts.
- *Critical infrastructure and government targets:* Cyberattacks on the Australian court system and the French township Pays Fouesnantais demonstrate the vulnerability of government and critical infrastructure to cyberattacks.

Outlook:

The current landscape of cybersecurity is marked by a diverse range of threats, from sophisticated nation-state activities to opportunistic cybercriminal exploits. The trend towards exploiting misconfigurations and privilege escalation



in cloud environments is particularly concerning, as it can lead to significant data breaches and system compromises. Ransomware continues to be a major threat, with attackers targeting both private and public sector entities. The involvement of nation-state actors in cyber operations, particularly targeting media and government infrastructure, is a reminder of the geopolitical dimensions of cybersecurity. Organizations must prioritize robust cybersecurity measures, including regular audits, employee training, and the implementation of strong data protection and access control policies. Heightened vigilance and proactive defense strategies are needed to counter these evolving threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 25% [CVE-2023-35078](#)

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

↓ 21% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB.

↓ 20% [CVE-2023-22518](#)

- An improper authorization vulnerability in Confluence Data Center and Server.

US entertainment site targeted in 2M RPS DDoS attack

+US +Entertainment +DDoS

- A US entertainment site was targeted this week in a DDoS attack that reached almost 2M RPS in less than two hours. The attack came from 42,000 Thailand and Spain-based IPs, and may come from hackers who oppose the group's anti-piracy efforts.

Belgium-based scientific site experiences XSS and RCE attacks

+Belgium +Science +XSS +RCE

- A Belgium-based scientific site experienced cross-site scripting (XSS) and remote code execution (RCE) attacks on January 2, reaching a collective 3.1M requests. Attackers targeted the Index and Webmail parts of the site with attacks which, if not mitigated, could have led to serious breaches of communications or distributed malicious code to users.

Recent Cyber Threats

Exploitation chain uncovered in Google Kubernetes engine

+Privilege Escalation

- A dual privilege escalation chain was discovered in [Google Kubernetes Engine](#) (GKE), stemming from misconfigurations in GKE's FluentBit logging agent and Anthos Service Mesh. Attackers with existing Kubernetes cluster access could escalate privileges, potentially leading to data theft and cluster disruption. Researchers identified this as a sophisticated second-stage cloud attack. Google has since patched these vulnerabilities.

Malware exploits Google OAuth for account hijacking

+Account Takeover

- Several malware families are abusing an undocumented Google [OAuth](#) endpoint, MultiLogin, to restore expired authentication cookies and hijack user accounts. This method allows unauthorized access to Google accounts, even after password resets. Google has taken steps to secure compromised accounts and advised users to follow best practices for account security.

Critical Qualcomm chip flaw enables remote voice call attacks

+Telecommunications

- [Qualcomm](#) disclosed a critical vulnerability in its chipsets, allowing remote attacks via malicious voice calls over LTE networks. Affecting a range of devices, including popular smartphones, this buffer overflow flaw could lead to remote code execution. Qualcomm has provided patches to OEMs, and users are advised to connect only to secure LTE networks.

Cryptocurrency miners hidden in Python packages

+Python

- Three malicious [Python](#) packages were found in the PyPI repository, deploying cryptocurrency miners on Linux devices. These packages, linked to a previous campaign, were downloaded 431 times before removal. The malware ensures persistence and stealthy operation on infected devices.

MacOS backdoor linked to North Korean hackers

+North Korea +Backdoor +BlueNoroff

- Researchers discovered a new macOS backdoor, [SpectralBlur](#), linked to North Korean malware families. Capable of various malicious activities, SpectralBlur shares similarities with KANDYKORN and is part of the Lazarus sub-group BlueNoroff's campaign. This discovery highlights the increasing focus of North Korean actors on macOS targets, especially in the cryptocurrency and blockchain sectors.

Apache RocketMQ servers under siege

+Technology

- Security researchers have observed hundreds of IP addresses scanning and attempting to exploit [Apache RocketMQ](#) servers, vulnerable to two critical remote command execution flaws. The vulnerabilities, which remained active after an initial patch, allow attackers to execute commands remotely. Apache has released updated patches, and users are urged to upgrade their systems.

Data Breaches

Massive data leak event “Leaksmas” on dark web

+Dark Web

- Security experts reported a significant data leak event, dubbed [Leaksmas](#), on the Dark Web on Christmas Eve. Over 50 million records containing personal information from consumers worldwide were leaked. The data breaches affected a wide range of countries, leading to potential account takeovers, identity theft, and financial fraud. The leaks were shared freely among cybercriminals as a form of mutual gratitude, posing a global threat.

Spotify music converter exposes user data

+Music

- [TuneFab](#), a platform used for converting copyrighted music from streaming services like Spotify, exposed over 151 million records including users' IP addresses, emails, and device info due to a misconfiguration in MongoDB. The data was publicly accessible for about 24 hours before the issue was fixed. This exposure could assist threat actors in enriching data from previous leaks, posing a risk to users' privacy.

Swedish grocery retailer targeted in Cactus ransomware attack

+Cactus +Sweden +Food & Beverages

- The [Cactus](#) ransomware group claimed to have hacked Coop, one of Sweden's largest retail and grocery providers, and threatened to disclose over 21 thousand directories of personal information. Cactus ransomware is known for using encryption to protect its binary and employs various legitimate tools for remote access and post-exploitation activities.

Game developer exposes almost one million records in Google Drive misconfiguration

+Gaming +Japan

- [Ateam](#), a Japanese game developer, exposed sensitive information of nearly one million people due to a Google Drive misconfiguration. The exposed data included full names, email addresses, phone numbers, and device identification numbers. The issue, which lasted for over six years, highlights the risks associated with cloud storage misconfigurations and the importance of securing cloud services.

Australian court hacked, hearing records potentially accessed

+Australia +Government

- [Court Services Victoria](#) (CSV) in Australia experienced a cybersecurity incident, potentially compromising recordings of hearings, including cases in the Supreme Court of Victoria. The incident led to unauthorized access to CSV systems, disrupting audio-visual in-court technology. Some recordings may involve people with protected identities, raising concerns about privacy and legal implications.

Major data breach at Iranian food delivery service SnappFood

+Iran +Food & Beverages +Irleaks

- [SnappFood](#), a leading Iranian online food delivery service, suffered a significant data breach. A hacker group known as Irleaks claimed responsibility, stating they stole over 3TB of data, including personal information of 20 million customers, vendor records, payment details, and more. SnappFood acknowledged the breach and reportedly reached an agreement with the hackers to prevent the sale or leakage of the data.

Belarusian hacktivists target state-owned news agency

+Belarusian Cyber Partisans +Belarus +Government +News

- Belarusian hacktivists, known as the [Belarusian Cyber Partisans](#), claimed responsibility for shutting down BelTA, the country's leading state-owned media outlet. They alleged to have wiped the main website servers, backups, and internal network, in retaliation against President Alexander Lukashenko's propaganda campaign. The attack is part of a broader movement against government restrictions on freedom of speech and the press.

Cross Switch exposes millions of user details

+Financial Services +IntelBroker

- [Cross Switch](#), an online payment gateway management company, experienced a data breach by a threat actor named IntelBroker. The breach compromised the personal information of 3.6 million users, including names, emails, phone numbers, banking information, and more.

Cyberattack disrupts services in French township

+France +Government

- [Pays Fouesnantais](#), a coastal township in Brittany, France, faced a large-scale cyberattack that disrupted all of its community services. The mayor confirmed that the township's IT services were rendered inoperable, except for the passport and national identity card service. The attack is part of a series of cyber incidents affecting French organizations.

Property search app exposes user passwords

+India +Real Estate

- The [MyEstatePoint Property Search](#) app, developed by NJ Technologies in India, leaked data of nearly half a million users, including names and plain-text passwords. The breach occurred due to a publicly accessible MongoDB server. The app, popular in the Indian market, has over half a million downloads on Google Play. The exposed data poses risks of unauthorized access and identity theft.

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