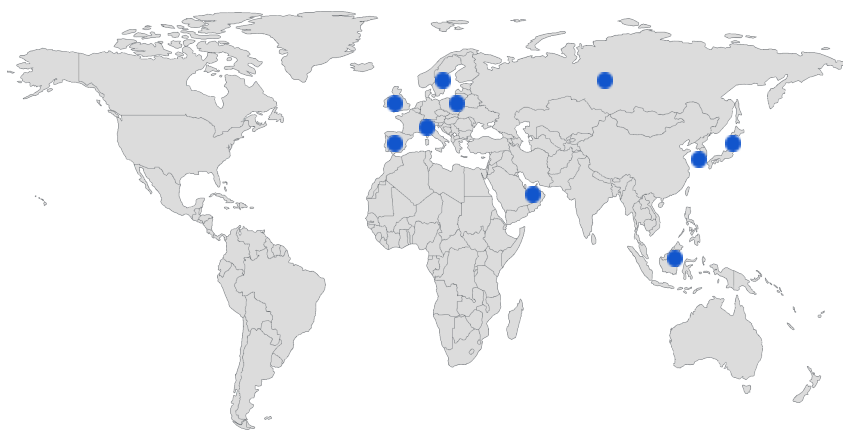


Threat Intel Report: January 15-21, 2024

Countries



Top Tags

NoName

Anonymous Sudan

BigPanzi

LockBit

Midnight Blizzard

Executive Summary

Actionable Information:

- **Ransomware and DDoS attacks:** The NoName ransomware group's activities in Lithuania and Switzerland, along with Anonymous Collective's DDoS attacks in Bahrain, indicate a rising trend in politically motivated cyberattacks targeting government and media entities.
- **Botnet exploitation:** The BigPanzi botnet targeting Android TV boxes and the AndroXgh0st malware forming a botnet to compromise networks highlight the evolving threat landscape in IoT and network security.
- **Vulnerability exploitation:** The discovery of the MyFlaw vulnerability in Opera and TensorFlow's CI/CD pipeline issues underscore the importance of robust security practices in software development and the need for continuous monitoring of software vulnerabilities.
- **Data breaches and credential theft:** The Indonesian election data breach and the massive leak of 71 million passwords across major platforms like Facebook and Coinbase reveal the growing scale of data breaches and the sophistication of credential theft techniques.
- **State-sponsored cyber espionage:** The breach of Microsoft's corporate emails by Russian hackers, identified as Midnight Blizzard, points to the ongoing threat of state-sponsored cyber espionage and the need for heightened security measures in corporate environments.

Outlook:

As we navigate the evolving landscape of cyber threats, it's clear that the challenges facing organizations worldwide are becoming increasingly complex. The trend of cyberattacks driven by political motives, as demonstrated by groups like NoName and Anonymous Collective, is expected to persist, particularly in politically volatile regions. The advancement in

botnet capabilities and the exploitation of software vulnerabilities, such as those found in Opera and TensorFlow, highlight that attackers are constantly refining their methods to find and leverage system weaknesses. The scale of data breaches is on the rise, especially those involving extensive personal data and credentials, posing serious risks to individual privacy and organizational security. In response, organizations must step up their cybersecurity game. This means not only conducting regular system checks for vulnerabilities but also investing in educating employees about cybersecurity risks and deploying cutting-edge security solutions. On top of that, the involvement of state-backed groups in cyber espionage underscores the need for a united front. This calls for stronger collaboration between government bodies and the private sector to bolster our collective cyber defenses and response strategies. In summary, staying ahead in this dynamic cyber environment requires a proactive and collaborative approach to cybersecurity.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 24% [CVE-2023-35078](#)

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

↓ 11% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB.

↓ 24% [CVE-2023-22518](#)

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

Korean gambling site targeted in large DDoS attack

+Korea +Gambling +DDoS

- A Korean gambling site was targeted in a 2M RPS DDoS attack this week, in an almost 10 hour attack coming from 5,000 IP addresses. This site was likely targeted due to the volume of financial transactions in the gambling industry, making it an attractive target for attackers seeking to disrupt operations and potentially extort money.

Japanese business site hit by RCE and SQLi attack

+Japan +Business +RCE +SQLi

- A Japanese business site experienced a two-day attack this week, composed of remote code execution (RCE) and SQL injection (SQLi). Attacks reached a total of over 3.5M requests in two days, coming from just 679 distinct IPs.

Recent Cyber Threats

Bahrain's media outlets targeted by Anonymous Collective

+Bahrain +Anonymous Collective

- The [Anonymous Collective](#) launched a DDoS attack on Bahrain, affecting several media outlets like Akhbar al-Khaleej and Al-Ayam, in retaliation for Bahrain's support of US and UK strikes on Yemen. The attack caused disruptions and "403 Forbidden" errors on the affected websites.

NoName ransomware group targets Lithuania, Switzerland

+NoName +Lithuania +Switzerland +Government

- The [NoName](#) ransomware group attacked several Lithuanian organizations, including insurance companies and the Lithuanian Roads Association. The cyberattack led to the inaccessibility of websites and was linked to Lithuania's support for Ukraine in the Russia-Ukraine conflict.
- Switzerland also faced DDoS attacks by the pro-Russian group [NoName](#) on government websites, believed to be in retaliation for Ukrainian President Zelensky's visit to Davos. The attacks caused temporary disruptions but did not impact the main government portal.

Anonymous Sudan claims cyberattack on London Internet Exchange

+Anonymous Sudan +UK

- [Anonymous Sudan](#), affiliated with Russia, claimed responsibility for a cyberattack on the London Internet Exchange (LINX) in response to UK's air strikes on Yemen. The authenticity of the claim is uncertain as LINX's website remained operational, raising questions about the impact of the attack.

Opera browser's MyFlow vulnerability exposed

+Opera

- A critical security flaw, named [MyFlow](#), was discovered in the Opera web browser for Windows and macOS, allowing attackers to execute any file on the operating system. This vulnerability exploited the My Flow feature, which syncs messages and files between mobile and desktop devices. The flaw was addressed in updates after disclosure.

Phemedrone stealer exploits Windows Defender bypass

+Stealer Malware

- The [Phemedrone Stealer](#) malware campaign exploited CVE-2023-36025, a Windows Defender SmartScreen Bypass vulnerability, to steal data from web browsers, cryptocurrency wallets, and messaging apps. The malware was distributed via cloud-hosted malicious URLs and used advanced techniques for defense evasion.

BigPanzi botnet targets Android TV boxes

+BigPanzi +Botnet

- The [BigPanzi](#) cybercrime syndicate has infected around 170,000 Android TV and eCos set-top boxes since 2015, creating a large-scale botnet. The malware, introduced through firmware updates or backdoored apps, is used for illegal media streaming, traffic proxying, DDoS attacks, and OTT content provision.

TensorFlow CI/CD pipeline vulnerability exposes supply chains

+Supply Chain +GitHub +PyPi

- Misconfigurations in [TensorFlow's](#) CI/CD pipeline could have allowed attackers to compromise TensorFlow releases on GitHub and PyPi. The vulnerabilities could enable malicious uploads to GitHub, remote code execution, and theft of a GitHub Personal Access Token.

PostgreSQL databases targeted by extortion bot

+Extortion Bot +SQL

- A [malicious bot](#) is autonomously wiping out publicly exposed PostgreSQL and MySQL databases with weak passwords, leaving ransom notes that falsely claim data backup. The bot, which has netted over \$3,000 from victims, only saves the first 20 rows of each table, making full data recovery impossible for those who pay.

CISA advisory on Androxgh0st malware threat

+AndroxGh0st +Botnet

- The FBI and CISA released a joint advisory on the [Androxgh0st](#) malware, which establishes a botnet to identify and compromise vulnerable networks. The malware targets .env files containing credentials and supports functions like SMTP abuse, scanning, exploiting exposed credentials, and web shell deployment.

Data Breaches

Indonesian election data breach raises concerns

+Indonesia +Government

- [Indonesia](#) faces a significant cybersecurity threat with the leak of 6.8 million voter records from the 2017 Jakarta gubernatorial election and a massive database containing 252 million entries, including passport details. The data, offered for sale at \$74,000, poses risks for information warfare in the upcoming 2024 presidential election.

LockBit ransomware group targets Tura Scandinavia AB

+LockBit +Sweden

- [Tura Scandinavia AB](#), a Swedish company, was allegedly targeted by the LockBit ransomware group. The group claimed to have exploited vulnerabilities in the company's network, lacking basic security measures, and is now selling access to the corporate network.

Spanish municipality faces €10 million ransomware demand

+Spain

- Calvià, a municipality in [Spain](#), was hit by a ransomware attack with criminals demanding approximately €10 million. The mayor refused to pay the ransom, aligning with Spain's commitment against paying ransoms. The attack led to the suspension of administrative services until the end of January.

Massive leak of 71 million passwords affects major platforms

+Stolen Credentials

- A [data dump](#) containing 71 million unique credentials for platforms like Facebook, Roblox, eBay, and Yahoo was discovered, with 25 million passwords never seen before. The data, likely obtained from malware and credential stuffing, poses a significant threat to user account security on these platforms.

Russian hackers breach Microsoft corporate emails

+Midnight Blizzard +Russia

- Russian state-sponsored hackers, known as [Midnight Blizzard](#), breached Microsoft's systems and stole corporate emails over a month-long period. The attack, initiated through a password spray attack, compromised accounts in Microsoft's leadership, cybersecurity, and legal departments.

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