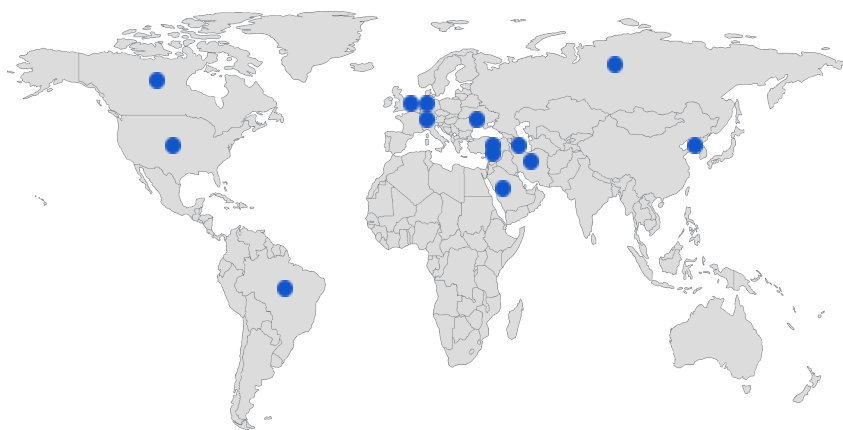


Threat Intel Report: January 8-14, 2024

Countries



Top Tags

UTA0178

Blackjack

NoName

Rhysida

BlackCat

Executive Summary

Actionable Information:

- *Exploitation of public platforms:* The use of YouTube channels to distribute Lumma Stealer malware signifies a trend where threat actors exploit popular public platforms to spread malware. This approach capitalizes on the trust and high traffic of these platforms.
- *Vulnerabilities in commonly used devices and software:* The discovery of vulnerabilities in Kyocera printers and Bosch Rexroth pneumatic wrenches highlights the ongoing risk in widely used devices and software. These vulnerabilities can lead to significant operational disruptions and security breaches in organizations.
- *Targeted malware campaigns:* The active deployment of Pikabot malware by Water Curupira and the exploitation of Ivanti VPN zero-day vulnerabilities by UTA0178 indicate a rise in targeted malware campaigns aimed at specific industries or technologies.
- *Data breaches and leaks:* Significant data breaches, such as the exposure of sensitive user data by Bit24.cash and the data leak affecting the Brazilian population, underscore the persistent threat of data breaches and the need for robust data protection measures.

Outlook:

The current cyber threat landscape is characterized by a mix of sophisticated targeted attacks and widespread vulnerabilities in commonly used systems. The trend of exploiting public platforms for malware distribution is particularly concerning, as it can lead to widespread infections among unsuspecting users. Additionally, the discovery of critical vulnerabilities in widely used devices and software underscores the importance of regular security updates and vulnerability management. The rise in targeted malware campaigns suggests that threat actors are becoming more

selective and strategic in their attacks, focusing on high-value targets or specific industries. Finally, the ongoing incidents of data breaches and leaks highlight the critical need for enhanced data protection measures and cybersecurity awareness among organizations and individuals. Looking ahead, we can expect continued evolution in attack methodologies, with an increased focus on exploiting emerging technologies and targeting specific sectors for maximum impact.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↑ 271% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB.

↑ 216% [CVE-2023-35078](#)

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

↑ 102% [CVE-2023-35082](#)

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

Largest DDoS attack of 2024 so far targets Korean gambling site

+South Korea +Gambling +DDoS

- A Korean gambling site was targeted this week in the largest DDoS attack of the year so far. The attack reached almost 2.4M RPS, and came from 11K IPs.

Azerbaijani financial site targeted in path traversal and XSS attacks

+Azerbaijan +Financial Services +Path Traversal +XSS +Germany

- An Azerbaijani financial services site experienced a targeted path traversal and cross-site scripting (XSS) attack this week, coming from only 19 German IPs. This is the first time we've seen this site targeted in the last year.

Recent Cyber Threats

YouTube channels compromised to spread Lumma Stealer malware

+Lumma Stealer

- Researchers have discovered a threat group using YouTube channels to distribute a [Lumma Stealer](#) variant. The attackers uploaded videos featuring cracked applications, embedding malicious URLs leading to a .NET loader that fetches Lumma Stealer. This malware targets sensitive information like user credentials and browser data. The global presence of Lumma Stealer's command-and-control servers indicates a widespread impact.

Kyocera printers vulnerable to path traversal attacks

+Path Traversal

- Researchers have disclosed a path traversal vulnerability in [Kyocera's](#) Device Manager, used for managing large printer fleets. The flaw, tracked as CVE-2023-50916, allows attackers to change the local path for backup databases, potentially leading to compromised Active Directory credentials. Kyocera has released a patch for this vulnerability, which requires network access to exploit.

Security flaws in Bosch Rexroth pneumatic wrenches

+Manufacturing

- Vulnerabilities have been found in [Bosch Rexroth's](#) pneumatic torque wrenches, commonly used in automotive production lines. These flaws could allow ransomware implantation or unauthorized alteration of tightening programs, impacting operational performance and safety. Bosch Rexroth is working on a patch, highlighting the potential risks in interconnected manufacturing processes.

Critical vulnerability in Cacti network monitoring tool

+SQLi

- A high-severity blind SQL injection vulnerability, CVE-2023-51448, was discovered in [Cacti](#), a network monitoring tool used by telecoms and web hosting providers. This vulnerability could lead to information disclosure and potentially remote code execution.

Imperva customers are protected against this vulnerability.

Pikabot malware campaign by Water Curupira

+Pikabot +Water Curupira

- The threat actor Water Curupira, known for using Black Basta ransomware, has been actively deploying [Pikabot](#), a loader malware similar to Qakbot, in spam campaigns throughout 2023. Pikabot is used for phishing, enabling unauthorized remote access, and executing arbitrary commands, posing significant risks to targeted systems.

Ivanti VPN zero-day exploits threaten network security

+Ivanti +UTA0178

- Two critical zero-day vulnerabilities, CVE-2023-46805 and CVE-2024-21887, in [Ivanti Connect Secure VPN](#) are being actively exploited, allowing attackers to bypass two-factor authentication and execute malicious code. Attributed to the threat actor UTA0178, suspected to be a Chinese nation-state actor, these vulnerabilities pose a significant threat to networks using Ivanti VPN.

FBot hacking tool targets cloud services

+Python +FBot

- A new Python-based hacking tool, [FBot](#), has been discovered targeting web servers, cloud services, and SaaS platforms like AWS, Microsoft 365, and PayPal. Developed for credential harvesting and account hijacking, FBot is distinct from other cloud hacking tools but shares similarities with Legion. It's actively used for hijacking cloud services and harvesting credentials, with features for AWS and Sendgrid API key generation, reverse IP scanning, PayPal account validation, and more.

Critical vulnerabilities in POST SMTP mailer plugin endanger WordPress sites

+WordPress +XSS

- Over 150,000 [WordPress](#) sites are at risk due to two vulnerabilities in the POST SMTP Mailer plugin. The first, CVE-2023-6875, is a critical authorization bypass flaw, and the second, CVE-2023-7027, is a cross-site scripting issue. These vulnerabilities can allow attackers to take complete control of a site, access sensitive information, and potentially plant backdoors or redirect users to malicious sites. A patch has been released in version 2.8.8 of the plugin.

Imperva customers are protected against these vulnerabilities.

GitLab releases urgent patch for critical account takeover vulnerability

+GitLab +ATO

- [GitLab](#) has issued security updates for a critical vulnerability, CVE-2023-7028, which allows account takeover without user interaction. This flaw, rated 10.0 in severity, stems from a bug in the email verification process and affects various versions of GitLab Community Edition and Enterprise Edition. Users are advised to upgrade to the patched versions and enable two-factor authentication.

Imperva customers are protected against this vulnerability.

Data Breaches

Iranian crypto exchange exposes sensitive user data

+Iran +Crypto

- Iranian crypto exchange [Bit24.cash](#) inadvertently exposed sensitive data of nearly 230,000 users. The leak occurred due to a misconfigured MinIO instance, granting access to S3 buckets containing KYC data. Exposed data includes passports, IDs, credit cards, and written consents. The issue has since been secured, but the impact of this exposure on Iranian citizens remains significant.

Cyberattack disrupts Memorial University's operations

+Canada +Education

- The [Memorial University of Newfoundland](#) suffered a cyberattack in late December, leading to the postponement of the semester start at one campus. The attack affected IT systems, causing disruptions in online services and delaying the winter semester's commencement. The university is working to restore systems and has informed law enforcement, but the extent of data compromise is still under investigation.

Mortgage lender hit by cyberattack affecting payment services

+Financial Services +US

- U.S. mortgage lender [loanDepot](#) experienced a cyberattack that forced the company to take its IT systems offline, disrupting online loan payments. The attack's nature is not yet confirmed but is suspected to be ransomware. loanDepot, servicing loans over \$140 billion, is working with law enforcement and forensics experts. Customers are advised to be vigilant for potential phishing attacks and identity theft.

Sea Turtle espionage campaign targets Dutch telecom and IT providers

+Türkiye +Netherlands +Sea Turtle +Telecommunications & IT

- A Türkiye-linked threat actor, [Sea Turtle](#), has launched a cyber espionage campaign against Dutch telecom, IT service providers, and Kurdish websites. The campaign aims to collect politically sensitive information, leveraging supply chain and island-hopping attacks. Sea Turtle, active since 2017, is known for DNS hijacking and has recently used SnappyTCP for attacks. Organizations are advised to strengthen their cybersecurity measures in response.

Cyber attack disrupts Beirut International Airport

+Lebanon +Travel

- [Beirut International Airport](#) in Lebanon experienced a cyber attack targeting its flight information display system. The attack displayed a politically charged message on airport screens, criticizing Hezbollah and Iran. Additionally, the baggage handling system was disrupted, requiring manual baggage inspections. The attack's origins are currently unknown, and no group has claimed responsibility.

NoName ransomware targets Ukrainian government websites

+Ukraine +Russia +NoName +Hacktivism +Government

- The NoName ransomware group allegedly targeted multiple [Ukrainian government websites](#), including Accordbank, Zaporizhzhya Titanium-Magnesium Plant, and various State Tax Service departments. While some sites remained operational, others displayed error messages, indicating potential disruptions. This attack is part of ongoing cyber conflicts related to the Russia-Ukraine war, with NoName ransomware previously targeting Finnish government websites.

Swiss Air Force data leaked following cyberattack on US security firm

+Switzerland +US +BlackCat +Government

- Sensitive documents from the [Swiss Air Force](#) were leaked on the dark web following a cyberattack on Ultra Intelligence & Communications, a US security provider. The breach, attributed to the BlackCat ransomware group, compromised around 30 gigabytes of documents, including contracts and communication details. The Swiss Federal Department of Defence confirmed the incident, stating that operational systems were not affected.

Ransomware attack on World Council of Churches

+Rhysida +Religion

- The [World Council of Churches](#) and the Lutheran World Federation suffered a ransomware attack during the Christmas season. The Rhysida ransomware gang claimed responsibility for the attack on the Lutheran World Federation, which is linked to the incident at the World Council of Churches. The attack compromised data and disrupted operations, with the Rhysida gang demanding a ransom in Bitcoin for the stolen information.

Pro-Ukraine hackers target Russian internet provider

+Ukraine +Russia +Blackjack +Telecommunications +Government

- The pro-Ukrainian hacker group Blackjack claimed responsibility for breaching Moscow internet provider [M9com](#), in retaliation for a Russian cyberattack on Ukraine's largest telecom company, Kyivstar. The attack was reportedly carried out in cooperation with Ukraine's security forces (SBU). Details are limited, but screenshots of the hacked systems were shared by the group. The extent of the breach and the SBU's involvement remain unconfirmed.

Massive data leak exposes Brazilian population

+Brazil

- A publicly accessible Elasticsearch instance exposed the private data of hundreds of millions of [Brazilian citizens](#). The leaked data included full names, dates of birth, sex, and individual taxpayer numbers (CPF). With more than 223 million records leaked, the entire Brazilian population could be affected. The data's misuse could lead to identity theft, fraud, and targeted cybercrimes, posing severe risks to the individuals involved.

Halara investigates data breach affecting almost 1M customers

+Retail

- Athleisure clothing brand [Halara](#) is probing a data breach after a hacker leaked data for nearly 950,000 customers on a hacking forum. The leaked data includes names, phone numbers, and addresses. The breach was allegedly caused by exploiting a bug in Halara's website API. Customers are advised to be vigilant for smishing attacks and other fraudulent activities using their stolen data.

Saudi Foreign Affairs ministry suffers data breach

+Saudi Arabia +Government

- The [Ministry of Foreign Affairs for the Kingdom of Saudi Arabia](#) reportedly experienced a significant data breach, exposing personal information of over 1.4 million employees. The breach details were posted on a dark web forum, including ID, names, contact numbers, emails, and job titles. The ministry has not yet confirmed the breach, and the website remains operational. This incident is part of a recent trend of cyberattacks targeting Arabian countries.

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