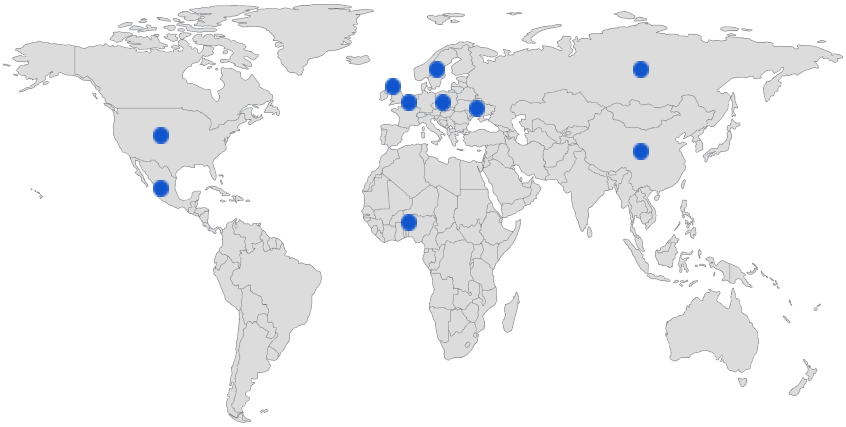
imperva

IMPERVA THREAT RESEARCH

Threat Intel Report: January 22-28, 2024

Countries



Top Tags

- Conti
- Blackwood
- Akira
- Black Basta
- APT29

Executive Summary

Actionable Information:

- *Ransomware and malware trends:* A significant increase in ransomware attacks is visible, notably the Godzilla web shell attacks exploiting Apache ActiveMQ and the emergence of 3AM ransomware linked to Conti and Royal cybercrime gangs. The use of malware in pirated macOS apps and the distribution of NS-STEALER malware via Discord bots highlight the evolving tactics of cybercriminals.
- *Supply chain and API vulnerabilities:* The MavenGate attack method targeting Java and Android applications and the exploitation of the Trello API demonstrate the growing threat to software supply chains and the importance of securing APIs.
- *Critical infrastructure and cloud security:* The attacks on Southern Water by the Black Basta ransomware gang and the Sys:All loophole in Google Kubernetes Engine emphasize the vulnerability of critical infrastructure and cloud environments.
- *Data breaches and leaks:* The historic data leak exposing 26 billion records and the exposure of 1.3 million records from a medical lab database underscore the ongoing risk of data breaches and the need for robust data protection measures.
- *Geopolitical cyber warfare:* The cyberattacks by Ukrainian hackers on Russian scientific research centers and the breach of HP Enterprise by Russian intelligence group APT29 reflect the increasing use of cyber operations in geopolitical conflicts.

Outlook:

The current landscape of cyber threats reveals a diverse range of sophisticated attacks targeting both private and public sectors. Ransomware continues to be a primary threat, with attackers leveraging known vulnerabilities and expanding their tactics to include social media extortion. Supply chain attacks are becoming more intricate, exploiting abandoned software libraries and API vulnerabilities, indicating a need for heightened security in software development and third-party integrations. Critical infrastructure remains a high-value target, with recent attacks underscoring the necessity for enhanced security protocols in these sectors. The vast scale of data breaches highlights the ongoing challenge of protecting sensitive information against unauthorized access. Geopolitically motivated cyberattacks are increasingly prominent, reflecting the cyber domain's role in global conflicts. Organizations must prioritize comprehensive cybersecurity strategies, encompassing robust defense mechanisms, continuous monitoring, and proactive threat intelligence to mitigate these evolving threats.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬇ 35% CVE-2023-30185

- A file upload vulnerability in some versions of CRMEB

⬇ 1% CVE-2023-35078

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

⬇ 3% CVE-2023-35082

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

Polish financial site targeted in short but intense DDoS attack

+Poland +DDoS +Financial Services

- A Polish financial site saw an application-layer DDoS attack this week that reached 1.2M RPS in just seven minutes. The attack came from 7,100 IP addresses, indicating an aggressive and coordinated assault.

US computing site hit with China-based RCE attack

+US +Computing & IT +China +RCE

- A US computing site was targeted in a remote code execution (RCE) attack this week, coming from 2,000 China-based IPs. The nature and scale of this attack suggests a coordinated, targeted effort to disrupt operations or access sensitive data.

Recent Cyber Threats

Critical flaw in Apache ActiveMQ leads to Godzilla web shell attacks

+Godzilla +Ransomware +Crypto

- Cybersecurity researchers have identified a significant increase in attacks exploiting a patched flaw in Apache ActiveMQ, leading to the deployment of the Godzilla web shell on compromised hosts. This vulnerability, CVE-2023-46604, has been used by various adversaries to install ransomware, rootkits, cryptocurrency miners,

and DDoS botnets. The web shell allows attackers to execute arbitrary shell commands and control the host, posing a severe threat to users of Apache ActiveMQ.

3AM ransomware linked to Conti and Royal cybercrime gangs

+Conti +3AM

- Security researchers have discovered connections between the newly emerged 3AM ransomware operation and notorious groups like the Conti syndicate and the Royal ransomware gang. 3AM, known for its unique extortion tactics involving social media, is believed to be connected to the Royal ransomware group, a rebrand of former Conti members. The group's tactics, infrastructure, and communication channels show significant overlap with those of the Conti syndicate.

GoAnywhere MFT Authentication Bypass

+CVE +Authentication Bypass

- A vulnerability in GoAnywhere MFT (CVE-2024-0204) allows an unauthenticated attacker to create an administrative user. The exploit involves bypassing security filters using path traversal techniques, enabling the creation of an administrative user. The vulnerability highlights the importance of securing APIs and endpoints in web applications.

Imperva customers are protected against this vulnerability.

MavenGate attack hijacks Java and Android via abandoned libraries

+Java +MavenGate +Supply Chain

- A new software supply chain attack method, MavenGate, targets abandoned but still used libraries in Java and Android applications. Attackers can hijack projects through domain name purchases, making it challenging to detect such attacks. This method allows attackers to inject malicious code into applications and compromise the build process, affecting a wide range of Maven-based technologies.

NS-STEALER malware exploits Discord bots for data exfiltration

+NS-STEALER +Stealer Malware

- NS-STEALER, a sophisticated Java-based information stealer, uses Discord bots to exfiltrate sensitive data from compromised hosts. Distributed via ZIP archives disguised as cracked software, it steals screenshots, cookies, credentials, and more from over two dozen web browsers, along with system information and session data from platforms like Discord and Steam. The malware's advanced functions and cost-effective exfiltration method via Discord make it a significant threat.

Sys:All loophole in Google Kubernetes Engine allows unauthorized access

+Cloud Security

- A critical loophole in Google Kubernetes Engine, known as Sys:All, was found to allow any Google account holder to potentially access and control GKE clusters. Over a thousand vulnerable clusters were discovered, exposing sensitive data like JWT tokens, GCP API keys, and private keys. A notable case involved a publicly traded company where this misconfiguration led to extensive unauthorized access, highlighting the need for stringent cloud security protocols.

Over 5,300 GitLab servers at risk of zero-click account takeover

+Zero-Click Attack +CVE

- More than 5,300 internet-exposed GitLab instances are vulnerable to a critical zero-click account takeover flaw, CVE-2023-7028. This flaw allows attackers to send password reset emails to an attacker-controlled email address, enabling account takeover. While it doesn't bypass two-factor authentication, it poses a significant risk to accounts without this extra security. Most vulnerable servers are in the United States, Germany, and Russia, and the flaw can lead to supply chain attacks and proprietary code disclosure.

Imperva customers are protected against this vulnerability.

Pirated macOS apps distribute backdoor malware

+macOS +Backdoor Malware

- Researchers have identified a campaign distributing backdoor malware through pirated macOS applications hosted on Chinese websites. The malware, resembling the ZuRu malware, is embedded in applications like Navicat Premium and Microsoft Remote Desktop, and can download and execute multiple payloads, compromising the machine.

China-backed hackers use software updates to plant NSPX30 spyware

+China +Blackwood +Spyware

- A China-aligned threat actor, Blackwood, has been conducting adversary-in-the-middle attacks to hijack legitimate software updates and deliver the NSPX30 implant. This sophisticated spyware, targeting Chinese and Japanese companies, is deployed via updates of software like Tencent QQ and WPS Office. NSPX30 can harvest system information, record keystrokes, and take screenshots.

Critical Jenkins vulnerability allows remote code execution

+RCE +CVE

- Jenkins, a popular CI/CD automation software, patched a critical vulnerability (CVE-2024-23897) that could lead to remote code execution. The flaw, an arbitrary file read vulnerability, was exploitable through Jenkins' built-in command line interface. Attackers could read files on the Jenkins controller, potentially leading to various attacks, including remote code execution.

Imperva customers are protected against this vulnerability.

Malicious ads target Chinese users seeking restricted messaging apps

+China +RAT

- Chinese-speaking users searching for restricted messaging apps like Telegram and LINE are being targeted by malicious ads. These ads, created using compromised Google advertiser accounts, lead users to download Remote Administration Trojans (RATs) instead of the legitimate apps, potentially for data collection and spying purposes.

AllaKore RAT targets Mexican banks and cryptocurrency platforms

+Mexico +AllaKore RAT +Financial Services

- A financially motivated threat actor is targeting Mexican banks and cryptocurrency platforms with a modified version of AllaKore RAT. The campaign uses lures related to the Mexican Social Security Institute and targets large companies, indicating the threat actor's base in Latin America. The RAT is capable of stealing banking credentials and conducting financial fraud.

Monobank faces unprecedented DDoS attack in Ukraine

+Ukraine +DDoS +Financial Services

- Monobank, Ukraine's largest mobile-only bank, experienced a massive DDoS attack with 580 million service requests, following a similar attack the previous day. The CEO did not specify the attackers but noted past threats linked to Russian hackers. This attack is part of a broader pattern of cyber warfare in the ongoing conflict between Russia and Ukraine, with critical infrastructure being targeted.

Data Breaches

Tietoevry suffers Akira ransomware attack, impacting Swedish services

+Akira +Sweden +Computing & IT

- Finnish IT services provider Tietoevry experienced an Akira ransomware attack, affecting cloud hosting customers in one of its Swedish data centers. The attack led to outages for multiple Swedish businesses and government services. Tietoevry is working on restoring infrastructure and services, but the full extent of the attack's impact is still being assessed.

Cyberattack disrupts services at three English councils

+UK +Government

- Three English councils - Canterbury, Dover, and Thanet - faced a cyberattack, leading to the shutdown of multiple online services. The councils, which outsource IT and HR services to Civica, are investigating the incident's impact. Civica denied the attack originated from their systems, but the connection suggests a potential supply chain attack.

Historic data leak exposes 26 billion records

+Data Leak

- Cybersecurity researchers discovered the largest data leak ever, containing 26 billion records from multiple previous breaches. The 12 terabytes of data include sensitive information from companies like Tencent QQ, Weibo, MySpace, and LinkedIn. The leak poses significant risks for identity theft, phishing schemes, and targeted cyberattacks.

Black Basta ransomware gang targets UK water utility Southern Water

+Black Basta +Infrastructure +UK

- The Black Basta ransomware gang claimed to have hacked Southern Water, a major UK water utility. The group threatened to leak 750 gigabytes of sensitive data, including personal documents and corporate information. The exact ransom demand is unknown, but the attack highlights the increasing threat of ransomware to critical infrastructure.

Trello API exploited to link email addresses to millions of accounts

+API Abuse

- An exposed Trello API was abused to link private email addresses to over 15 million Trello accounts, creating data profiles containing both public and private information. The data, sold on a hacking forum, included emails, usernames, full names, and other account info. Trello has since secured the API, but the leak raises concerns about targeted phishing campaigns using the exposed information.

Ukrainian hackers target Russian scientific research center

+Ukraine +Russia +Government +BO Team

- Pro-Ukraine hackers reportedly breached Russia's State Research Center on Space Hydrometeorology, "Planeta," destroying its database and valuable equipment. The attack, claimed by the hacker group BO Team, reportedly led to the loss of 280 servers, two petabytes of data, and paralyzed the work of supercomputers. The impact of the attack on Russia's scientific capabilities is significant, but independent verification of the claims is not available.

HP hacked by Russian intelligence group APT29

+Computing & IT +Russia +APT29

- Hewlett Packard Enterprise reported a cyberattack by the Russian state-sponsored group APT29, which infiltrated HPE's cloud email environment and exfiltrated mailbox data. The attack, which began in May 2023, went undetected for over six months. APT29, linked to Russia's Foreign Intelligence Service, has been involved in high-profile hacks, including the 2016 DNC breach and the 2020 SolarWinds compromise.

Medical lab database exposes 1.3 million records including COVID test info

+Healthcare +Netherlands

- An unsecured database belonging to a Netherlands-based medical laboratory exposed 1.3 million records on the internet. The database, linked to Coronalab.eu, contained COVID test results, personal identifiable information, appointment details, and QR codes. The exposure raises concerns about potential phishing campaigns and the misuse of sensitive health data.

Pegasus spyware targets journalists in Togo

+Pegasus +Togo +Journalism

- Multiple journalists in Togo were targeted by the Pegasus spyware, reportedly used by the Togolese government until 2021. The spyware, developed by NSO Group, allows access to and extraction of data from mobile devices. At least 23 spyware intrusions were reported on the phone of Loïc Lawson, a Togolese journalist, with other journalists also targeted. Pegasus has been used globally to monitor journalists and politicians.

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.