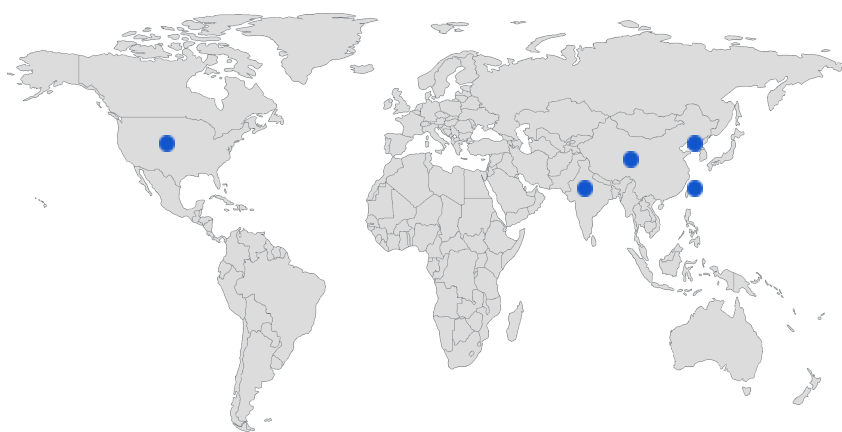


Threat Intel Report: April 22-28, 2024

Countries



Top Tags

AndroxGh0st

Sharp Stealer

APT28

STORM-1849

Cactus

Executive Summary

Actionable Information:

- *Supply Chain and Third-Party Package Risks:* Malicious software packages found in repositories like PyPI and npm, such as discordpy_bypass-1.7 and deceptive npm packages targeting developers, underscore the critical need for rigorous validation and security checks in software supply chains.
- *Infrastructure Vulnerabilities:* The exploitation of server vulnerabilities by Androxgh0st malware and unpatched Qlik Sense servers highlight the urgent necessity for timely application of security patches and comprehensive vulnerability management programs.
- *Information Theft through Common Platforms:* The theft of personal and system information through gaming platforms, and location data from apps like iSharing, reflects an increase in the targeting of consumer data through everyday software applications.
- *Emerging Threats in Data Handling and Privacy:* Demonstrations of EDR systems being weaponized to delete critical data, and massive breaches like the one at Kaiser Permanente, point to the evolving methods by which data integrity and privacy are being compromised.

Outlook:

The recent spate of cyber threats and breaches demonstrates a clear trend towards the exploitation of both technological and human vulnerabilities across diverse digital platforms. From software development kits to everyday consumer apps, attackers are finding innovative ways to infiltrate systems and exfiltrate data. This indicates a pressing need for entities at all levels to enhance their cybersecurity posture by implementing advanced threat detection tools and adopting a more proactive approach to cybersecurity education and awareness. Additionally, as the complexity of



cyberattacks increases, it's crucial for organizations to foster stronger collaborations with cybersecurity experts and institutions to stay ahead of potential threats. As we look ahead, maintaining robust and up-to-date security measures will be key to defending against the sophisticated cyber threats of tomorrow.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

↓ 17% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

↓ 25% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

↓ 1% [CVE-2023-35082](#)

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

German IPs Target a Telecommunications Site

+Telecommunications

- A telecommunications site was targeted by path traversal attacks this week. The site, which attackers are likely intending to use to access customer information, came almost entirely from German-based IPs.

Bots Target US Financial Services Site

+US +Financial Services

- A US financial services site was hit by automated attacks this week, coming from US-based IP addresses, likely in an attempt to scrape customer data off the community portal.

Recent Cyber Threats

Deceptive PyPI Package Unearthed

+PyPI

- Researchers discovered a deceitful PyPI package, [discordpy bypass-1.7](#), designed to exfiltrate sensitive user data, such as credentials and browser information, using advanced persistence techniques and evasion methods to avoid detection. The analysis revealed the malicious package utilized obfuscation and payload encryption to operate undetected, impacting all platforms where PyPI packages can be installed.

Global Server Compromise by Androxgh0st Malware

+AndroxGh0st +US +India +Taiwan +Malware

- Research detected widespread server compromises due to [Androxgh0st](#) malware, affecting over 600 servers in the US, India, and Taiwan. The malware exploited vulnerabilities like CVE-2021-3129 and CVE-2024-1709, deploying web shells that enable remote control and contributing to a growing botnet aimed at credential theft and establishing persistent backdoors.

Sharp Stealer: A New Threat to Gamers and Crypto Wallets

+Sharp Stealer +Crypto +Discord +Telegram

- Introduced as a .NET application targeting gamers and cryptocurrency users, [Sharp Stealer](#) was sold by a Russian-speaking threat actor through a Telegram channel. This infostealer malware was capable of extracting extensive personal and system information, including payment data from platforms like Discord and gaming services, directly transmitting it to the attacker via Telegram.

EDR Systems Weaponized to Delete Critical Data Remotely

+BlackHat +EDR

- At [Black Hat Asia](#), researchers demonstrated how EDR systems from Microsoft Defender and Kaspersky could be manipulated to remotely delete files, including entire databases. By embedding malware signatures into legitimate files, these files were falsely flagged as malicious and deleted, highlighting a significant vulnerability that could potentially affect global infrastructure services if exploited.

Russian APT28's "GooseEgg" Hacking Campaign

+APT28 +GooseEgg

- Microsoft reported on a sophisticated, long-running credential theft campaign orchestrated by Russia's APT28, dubbed [GooseEgg](#). Utilizing advanced phishing techniques and malware, this campaign targeted a wide range of sectors, aiming to gather extensive organizational and governmental credentials, potentially leading to broad-scale espionage or data manipulation.

Massive Keystroke Leakage in Chinese Keyboard Apps

+China +Keystroke Leakage

- Research recently revealed that popular [cloud-based pinyin keyboard apps](#) from companies like Baidu, Tencent, and others had severe security flaws that could expose user keystrokes during transmission. Nearly a billion users were potentially affected by these flaws, which ranged from poor encryption to the transmission of keystrokes over unencrypted channels, posing significant privacy risks to users

iSharing App Flaws Expose Millions of Users' Locations

+Location Sharing

- The popular [iSharing](#) location-sharing app, which boasts 35 million users, was found to contain critical security flaws that exposed users' precise locations, names, profile photos, and login credentials, which allowed unauthorized access to any user's coordinates.

ArcaneDoor Exploits Cisco Firewalls for Government Espionage

+STORM-1849 +Line Dancer +Line Runner

- Researchers revealed that state-backed hackers, identified as [STORM-1849](#), have been exploiting zero-day vulnerabilities in Cisco ASA and FTD firewalls since November 2023. These vulnerabilities allowed for the deployment of sophisticated malware tools, Line Dancer and Line Runner, to perform espionage activities targeting government networks globally.

SEO Poisoning Used to Spread Malware

+Black Hat +SEO Poisoning +Malware

- Threat actors are using [Black Hat SEO](#) techniques to manipulate search engine results, directing users to malicious sites that appear legitimate. These sites, hosted on reputable platforms, deploy malware through obfuscated JavaScript and multi-layered zip files. Once interacted with, these files execute payloads that steal sensitive information and perform other malicious activities like keystroke logging and clipboard monitoring.

Deceptive npm Packages Lure Developers with Malware

+North Korea +DEV#POPPER

- North Korean hackers are targeting software developers with malicious npm packages as part of a social engineering campaign dubbed [DEV#POPPER](#). The attackers pose as employers and during fake job interviews, encourage developers to download npm packages containing malware, including the BeaverTail and InvisibleFerret backdoors, leading to system compromise and data theft.

Thousands of Qlik Sense Servers at Risk from Cactus Ransomware

+Cactus

- Despite patches released by Qlik for three critical vulnerabilities (CVE-2023-41266, CVE-2023-41265, CVE-2023-48365) in their Sense servers, over 3,143 servers remain unpatched and vulnerable to [Cactus ransomware attacks](#). These vulnerabilities allow remote attackers to execute arbitrary code on affected systems, posing a severe security risk to numerous global organizations.

Data Breaches

Massive Privacy Breach: Discord User Messages for Sale

+Discord

- A privacy invasion has occurred with the sale of [four billion private Discord messages](#) on Spy.pet, a clear web scraping site. This data was collected from over 14,201 servers involving 627 million users. The nature of the breach suggests a security loophole in Discord's interaction with bots or third-party apps. This breach exposes a broad range of personal information, potentially including private conversations, financial details, and media, putting numerous users at risk of fraud and identity theft.

Class Action Lawsuit Hits Billion-Dollar Bank After Data Breach

+Financial Services

- [SouthState Bank](#), a major US bank with over \$45 billion in assets, faces a class action lawsuit following a data breach in February 2024 that exposed customers' names, Social Security numbers, and financial account information. The breach has reportedly been used by hackers for identity theft, prompting legal actions accusing the bank of negligent security practices and failure to provide timely and accurate breach notifications.

Kaiser Permanente Reports Major Health Data Breach

+Healthcare

- [Kaiser Permanente](#) has reported a significant data breach affecting 13.4 million members, marking the largest health-related breach disclosed this year. The breach involved unauthorized sharing of patient data, including medical information, with advertisers such as Microsoft and Google. Kaiser Permanente is taking steps to notify affected individuals and has reported the incident to the relevant authorities, highlighting the ongoing challenges of protecting patient information in the digital age.

Two Million Americans Compromised in Debt Collector Breach

+Financial Services

- [Financial Business and Consumer Solutions](#) (FBCS), a major US debt collection agency, has reported a data breach affecting approximately 1.955 million individuals. Hackers accessed sensitive personal information, including Social Security numbers, birth dates, and driver's license numbers, during a 12-day intrusion in February. This breach raises significant concerns about the potential for identity theft and fraud, as well as the overall security measures taken by financial institutions handling sensitive consumer data.

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