

Threat Intel Report: March 24-30, 2025

Countries



Top Tags

AMOS Stealer

GuLoader

Atlantis AIO

SparrowDoor

DeepSeek

Executive Summary

Actionable Information:

- **Insider Threats and Third-Party Vulnerabilities:** The Twitter breach, allegedly caused by an insider, and the Concord Orthopaedics breach involving a third-party vendor highlight the persistent risks associated with internal actors and third-party relationships. Organizations should strengthen their access controls, auditing mechanisms, and vendor management processes.
- **Malware Evolution and Evasion Techniques:** The re-emergence of the AMOS Stealer targeting macOS, and the abuse of Microsoft's code-signing service to distribute malware, reflects a trend where cybercriminals are using more sophisticated and evasive techniques to avoid detection. Enterprises should focus on enhancing endpoint detection and response (EDR) solutions and continuously monitor for unusual behavior.
- **Credential Stuffing and Phishing:** Large-scale attacks leveraging tools like Atlantis AIO for credential stuffing, as well as phishing campaigns using GuLoader, reinforce the importance of robust multi-factor authentication (MFA) and credential management strategies. Organizations must encourage users to adopt strong, unique passwords and implement MFA across critical platforms.
- **Impact on Sensitive Data:** Data breaches in the healthcare, education, and dating app industries—resulting in the exposure of personal, health, and intimate data—highlight the need for stronger data protection practices. Encryption, secure cloud storage, and stringent access controls should be prioritized for organizations handling sensitive user data.

Outlook:

The threat landscape is expected to continue evolving, with attackers increasingly targeting vulnerabilities in cloud-based services and using social engineering tactics to exploit human trust. Insider threats will remain a significant concern, especially in large organizations experiencing layoffs or internal transitions. Furthermore, as sophisticated

malware variants like the AMOS Stealer and SparrowDoor backdoor become more prevalent, organizations will need to invest in advanced detection technologies to combat these evolving threats. Credential stuffing and phishing attacks will continue to exploit weak or reused passwords, underscoring the importance of adopting comprehensive identity and access management solutions. Moving forward, organizations must adopt a proactive approach to cybersecurity, prioritizing not just defense mechanisms but also incident response and recovery plans to mitigate the impact of these ever-present threats.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 265% [CVE-2024-4885](#)

- In WhatsUpGold versions released before 2023.1.3, an unauthenticated Remote Code Execution vulnerability in Progress WhatsUpGold. The WhatsUp.ExportUtilities.Export.GetFileWithoutZip allows execution of commands with iisapppool\ntmconsole privileges.

↑ 245% [CVE-2025-29891](#)

- Bypass/Injection vulnerability in Apache Camel. This issue affects Apache Camel: from 4.10.0 before 4.10.2, from 4.8.0 before 4.8.5, from 3.10.0 before 3.22.4. Users are recommended to upgrade to version 4.10.2 for 4.10.x LTS, 4.8.5 for 4.8.x LTS and 3.22.4 for 3.x releases. This vulnerability is present in Camel's default incoming header filter, that allows an attacker to include Camel specific headers that for some Camel components can alter the behaviours such as the camel-bean component, or the camel-exec component.

↑ 98% [CVE-2024-45195](#)

- Direct Request ('Forced Browsing') vulnerability in Apache OFBiz.

US Site Targeted by 3.7M Request ATO Attack

+US +Food & Beverage +ATO

- A US-based company in the Food & Beverage industry was recently targeted by account takeover attacks, reaching 3.7 million logins in one day. The attacks, which were brute-force based, came from primarily US-based IPs.

Recent Cyber Threats

Mass Compromise of Websites Linked to Gambling

+CMS +China +Gambling

- Over 150,000 websites have fallen victim to a massive compromise through a sophisticated [JavaScript](#) injection campaign. The attack targeted websites using vulnerable content management systems (CMS), injecting malicious scripts that redirected visitors to Chinese gambling platforms. The attackers likely sought to promote illicit gambling operations, capitalizing on the websites' established traffic.

Ukraine Railway Hit by Cyberattack, Ticket System Offline

+Ukraine +Travel

- Ukraine's national railway company, [Ukrzaliznytsia](#), was targeted by a cyberattack that disrupted its online ticketing system, causing significant inconvenience for travelers. The cyberattack led to the unavailability of online services, preventing passengers from booking tickets and accessing important information. Although no group has claimed responsibility, the timing of the attack suggests a deliberate effort to disrupt critical infrastructure amid ongoing geopolitical tensions in the region.

Microsoft Signing Service Abused for Malware Code Signing

+Malware +Code-Signing

- A new threat has emerged where attackers are exploiting [Microsoft's](#) trusted code-signing service to distribute malware. By using legitimate digital certificates to sign their malicious software, the attackers effectively bypass security systems that would normally flag unsigned or suspicious files. The technique gives the malware the appearance of being from a trusted source, making it much more difficult for antivirus programs and other security measures to detect.

AMOS Stealer Reloaded Targets macOS with Data Theft

+AMOS Stealer +Malware +MacOS

- The [AMOS Stealer](#) malware, which has been a notorious tool for stealing sensitive data, has recently been updated to target macOS devices, posing a significant threat to Apple users. This newly reloaded version of the stealer has been designed to operate undetected, bypassing traditional security measures such as antivirus software. By targeting macOS, which is generally considered more secure than other operating systems, the malware is able to harvest user credentials, browsing history, and other sensitive information without being flagged. Its undetectable nature makes it a particularly dangerous threat, as it can remain in the system for extended periods while quietly exfiltrating valuable data.

Phishing Email Scam Distributes GuLoader Malware

+GuLoader +Malware

- Cybercriminals are using phishing emails masquerading as communications from an international shipping company to deliver GuLoader malware, a type of malicious software used to gain access to victims' systems. The emails, which appear legitimate to unsuspecting recipients, contain a malicious attachment or link that, once opened, triggers the installation of GuLoader. Once inside the victim's system, the malware gives attackers control over the machine, allowing them to steal sensitive data or use the system for further attacks.

Credential Stuffing Attacks Target 140+ Platforms

+Atlantis AIO +Credential Stuffing

- Hackers are leveraging the [Atlantis AIO](#) tool to carry out large-scale credential stuffing attacks across more than 140 online platforms, including e-commerce sites and social media networks. This attack technique involves using previously leaked username and password combinations to gain unauthorized access to user accounts. Since many people reuse the same credentials across multiple platforms, attackers are able to target a wide range of sites using a single set of data.

New SparrowDoor Backdoor Discovered in U.S. and Mexico

+SparrowDoor +United States +Mexico

- A new variant of the [SparrowDoor](#) backdoor has been discovered in ongoing attacks targeting organizations in the United States and Mexico. The backdoor provides persistent access to the affected systems, allowing cybercriminals to maintain control even after initial breaches are detected. This version of SparrowDoor is particularly dangerous because it is highly evasive, often going unnoticed by traditional detection methods.

Malware Delivered via Fake Sponsored Ads Targeting DeepSeek Users

+Malware +DeepSeek

- Cybercriminals are using fake sponsored Google ads to deliver malware to users of the [DeepSeek](#) search engine. These ads appear as legitimate, sponsored listings on the search engine results page but actually lead to malicious websites that infect users' systems with harmful software. The malware can then exfiltrate sensitive information, install additional malicious tools, or compromise the victim's system for further attacks.

Data Breaches

Twitter Faces Massive Data Leak Allegedly Due to Insider Action

+Social Media

- A significant data breach has exposed the profiles of approximately 2.8 billion [Twitter \(X\)](#) users. The leak, attributed to a disgruntled employee during a period of mass layoffs, was discovered on Breach Forums. The compromised data includes user IDs, screen names, account creation dates, profile descriptions, URLs, location and time zone settings, display names, and follower counts from both 2021 and 2025. This incident represents one of the largest social media data leaks in history, raising concerns about insider threats and data security within major tech companies.

Oracle Cloud Breach Potentially Exposes Millions of Customer Records

+Cloud

- [Oracle](#) is under investigation for a potential data breach affecting its cloud services. A hacker claims to have stolen 6 million records, including user credentials, potentially impacting over 140,000 customers. The breach allegedly exploited a vulnerability in Oracle Access Manager (CVE-2021-35587), which had remained unpatched since 2014.

Concord Orthopaedics Reports Data Breach via Third-Party Vendor

+Healthcare

- [Concord Orthopaedics](#) notified over 67,000 individuals about a data breach involving a third-party vendor's software used for patient registration and check-ins. The compromised data includes names, driver's licenses, Social Security numbers, and health insurance information. Investigations revealed no breach of Concord Orthopaedics' internal systems or electronic health records.

Data Breach Affects Thousands of Alaskan Students and School Staff

+Education +US

- A data breach in [PowerSchool](#), a widely used student information system, has impacted several Alaskan school districts, including Juneau, Lower Kuskokwim, Nome Public Schools, and Bering Strait School District. The exposed data encompasses names, contact information, Social Security numbers, medical histories, and other personal details, with some records dating back over 20 years.

Major Dating App Data Breach Exposes 1.5 Million Private User Images

+Dating Apps +Cloud

- Five dating apps developed by [M.A.D Mobile](#) suffered a significant data breach, exposing over 1.5 million private and explicit user images. The unprotected cloud storage buckets containing these images were accessible without password protection for months before remediation. The exposed data includes profile pictures, direct messages, and verification photos, posing risks of blackmail and extortion for affected users.

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.