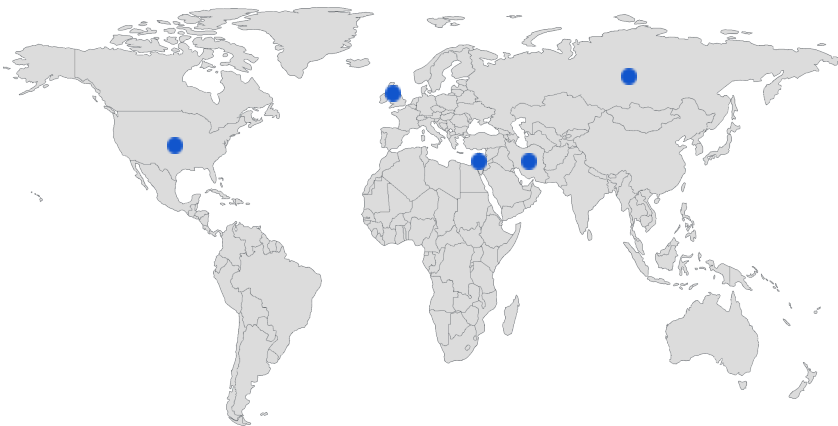


# Threat Intel Report: April 1-7, 2024

## Countries



## Top Tags

DinoDaSRAT

JSOutProx

Rhysida

Black Shadow

INC

## Executive Summary

### Actionable Information:

- **Supply Chain and Software Dependencies:** The XZ Utils backdoor incident underscores the risks associated with software supply chains and dependencies, necessitating thorough security evaluations of third-party components.
- **Ransomware Resurgence:** The Sexi ransomware targeting VMware ESXi servers and the incidents involving MarineMax and Leicester City Council indicate a continuing trend of ransomware attacks on both private sector and government entities, emphasizing the importance of robust backup and disaster recovery strategies.
- **Targeted Espionage and Malware Campaigns:** The DinoDaSRAT malware targeting Linux servers and the JSOutProx malware distributed via phishing campaigns targeting financial institutions illustrate the ongoing threat of targeted espionage and the need for heightened vigilance and defense mechanisms against sophisticated cyber threats.
- **Data Breaches and Leaks:** The incidents involving Europol, Atraf, and PandaBuy, among others, highlight the persistent risk of data breaches and leaks, necessitating stringent data protection measures and rapid incident response capabilities.

### Outlook:

The landscape of cyber threats continues to evolve, with adversaries exploiting a broad spectrum of vulnerabilities and employing sophisticated tactics to target organizations across various sectors. The recent incidents underscore the critical importance of maintaining up-to-date security measures, including regular software updates, comprehensive vulnerability assessments, and robust cybersecurity frameworks to protect against both opportunistic and targeted attacks. Additionally, the resurgence of ransomware and the exploitation of supply chain vulnerabilities highlight the need for organizations to enhance their resilience through improved backup solutions, incident response planning, and



cybersecurity awareness training. Looking ahead, organizations must remain vigilant and proactive in their cybersecurity efforts, adapting to the ever-changing threat landscape to safeguard their assets and data against potential cyber threats.

---

## Threat Activity in Imperva

### Top 3 CVEs targeted this week:

**Imperva customers are protected against these CVEs.**

⬆ 21% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

⬆ 279% [CVE-2023-38205](#)

- An improper access control vulnerability in Adobe ColdFusion

⬇ 11% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

### Attackers Leverage Adobe Vulnerability for the First Large Attack of 2024

**+US +Telecommunications**

- This week, a US telecommunications company was targeted in attack attempts leveraging the Adobe ColdFusion vulnerability [CVE-2023-38205](#). Attacks came mostly from tools written in the Go programming language, and represent the first large attack attempt we've seen with this CVE so far this year.

### Car Auction Site Targeted by DDoS

**+DDoS +US +Automotive**

- A US car auction site was hit by attempted application-layer DDoS this week, reaching 1.6M requests per second (RPS). The attack came from over 11,000 distinct IP addresses, and lasted only about 20 minutes.

---

## Recent Cyber Threats

### Linux Distributions Compromised by XZ Backdoor

**+XZ Utils**

- A supply chain attack has compromised major Linux distributions through a backdoor in the [XZ Utils](#) data compression library. The malicious code was introduced in version 5.6.0 of XZ Utils, affecting distributions like Fedora, openSUSE, Kali Linux, and Arch Linux. The backdoor, tracked as CVE-2024-3094 with a CVSS score of 10/10, allows unauthenticated remote access, posing a severe security risk.

### Single Connection HTTP/2 DoS Vulnerability Endangers Web Servers

**+HTTP/2 +CONTINUATION Flood +DoS**

- A set of vulnerabilities in the HTTP/2 protocol, termed [CONTINUATION Flood](#), can cause denial of service (DoS) attacks, leading to web server crashes with just a single TCP connection. These vulnerabilities affect various HTTP/2 implementations, potentially resulting in out-of-memory conditions or CPU resource exhaustion. The attack leverages the inherent functionality of the HTTP/2 protocol, making it particularly challenging to detect and mitigate without affecting normal traffic.

## DinoDaSRAT Targets Linux Servers in Espionage Effort

[+Linux](#) [+DinoDaSRAT](#) [+Malware](#)

- The [DinoDaSRAT](#) malware campaign is specifically targeting Linux servers for espionage purposes. This sophisticated malware enables attackers to execute commands and exfiltrate data from compromised servers. The campaign's focus on Linux servers highlights the need for heightened security measures in protecting against espionage-oriented threats.

## Malware Distribution via YouTube and Video Game Cracks

[+Malware](#) [+Cracks](#)

- Threat actors are leveraging [YouTube and video game cracks](#) to distribute malware, exploiting the popularity of these platforms to trick users into downloading malicious software. This method of malware distribution underscores the importance of caution when downloading files from unverified sources, as cybercriminals continue to find innovative ways to exploit digital platforms for malicious purposes.

## E-Commerce Platforms Targeted by Magento Shoplift Malware

[+Magento Shoplift](#) [+WordPress](#) [+E-Commerce](#)

- The [Magento Shoplift](#) malware campaign is targeting e-commerce platforms running on both Magento and WordPress CMS, aiming to compromise websites for financial gain. This malware exploits vulnerabilities to steal sensitive data, underscoring the critical need for e-commerce sites to maintain up-to-date security practices and software versions to protect against such threats.

## New Sexi Ransomware Hits Hosting Firms' VMware ESXi Servers

[+Sexi](#)

- Hosting firms are facing attacks from the new Sexi ransomware targeting [VMware ESXi](#) servers, leading to significant disruptions and data encryption. This ransomware campaign highlights the ongoing threat of ransomware to critical infrastructure and the importance of robust security measures to prevent such attacks.

## Million WordPress Sites at Risk Due to LayerSlider Plugin Flaw

[+WordPress](#)

- A critical unauthenticated SQL injection vulnerability in the [LayerSlider](#) WordPress plugin, affecting over one million sites, has been discovered. The flaw, identified as [CVE-2024-2879](#) with a CVSS score of 9.8, could allow attackers to extract sensitive data, including password hashes, leading to potential site takeovers.

## Visa Alerts on JSOutProx Malware Targeting Financial Institutions

[+JSOutProx](#) [+Trojan](#) [+Financial Services](#)

- Visa has issued a warning about a new phishing campaign distributing the [JSOutProx malware](#), targeting financial institutions and their customers in various regions including South and Southeast Asia, the Middle East, and Africa. JSOutProx, a remote access trojan, enables attackers to execute commands, download payloads, and capture screenshots, among other malicious activities.

---

## Data Breaches

### Sensitive Europol Files Vanish in Security Breach

[+Europol](#)

- Highly sensitive files, including personal information of top Europol executives, [mysteriously disappeared](#) from a secure storage room at Europol's headquarters in The Hague. The breach, discovered last summer, has led to an ongoing investigation. The missing documents raise significant security and privacy concerns, given Europol's critical role in law enforcement across Europe. The incident also highlights potential internal vulnerabilities within the organization.

## MarineMax Yacht Retailer Suffers Data Breach

**+Retail +Rhysida**

- [MarineMax](#), a leading yacht retailer, disclosed a data breach following a cyberattack in March, revealing that personal data of customers and employees was stolen. The Rhysida ransomware gang claimed responsibility, demanding a ransom of 15 BTC (over \$1 million) for the stolen data, which includes financial documents and personal identification. MarineMax has not confirmed payment of the ransom.

## PandaBuy Shopping Platform Compromised, Affecting 1.3 Million Users

**+E-Commerce**

- Over 1.3 million users of the [PandaBuy](#) online shopping platform were affected by a data leak after threat actors exploited critical vulnerabilities. The leaked data includes personal and order information. PandaBuy has not officially acknowledged the breach, and there are reports of attempts to censor discussions on social media platforms. Users are advised to change their passwords and watch for scam attempts.

## OWASP Foundation Reports Member Data Breach

**+OWASP +Misconfiguration**

- The [OWASP Foundation](#) disclosed a data breach affecting members who joined between 2006 and 2014 due to a misconfigured old Wiki web server. Exposed resumes contained personal information, including contact details and employment history. The Foundation has taken steps to secure the data and has removed the information from the internet, advising affected members to be cautious of unsolicited communications.

## Massive Data Leak Hits Israeli LGBTQ Dating App Atraf

**+Israel +Iran +Russia +Adult +Black Shadow**

- The Israeli LGBTQ dating app [Atraf](#) experienced a significant data breach, with personal information of approximately 669,672 users leaked. Initially targeted by the Iranian group Black Shadow, the breach was later claimed by a Russian forum user, exposing sensitive data including names, contact details, sexual orientation, and even payment card data. Users are urged to change their passwords and remain vigilant against potential phishing attempts.

## Ransomware Attack Prompts Missouri County to Declare Emergency

**+US +Government**

- [Jackson County, Missouri](#) declared a state of emergency following a suspected ransomware attack that rendered key IT systems inoperable. The attack disrupted services such as tax payments and marriage license issuance, coinciding with a special election day. Despite the challenges, election offices remained operational. This incident adds Jackson County to the growing list of municipal governments targeted by ransomware, underscoring the persistent threat to local administrations.

## Leicester City Council Targeted by INC Ransomware Group

**+UK +Government +INC**

- The INC ransomware group has claimed responsibility for a cyber incident at [Leicester City Council](#), alleging the theft of 3 TB of data. The council experienced a significant system shutdown on March 7, affecting various public services. While recovery efforts have restored most services, the council has refrained from commenting on the data's compromise due to ongoing criminal investigations. This attack highlights the increasing threat of ransomware to local governments and the potential for sensitive data exposure.

---

## 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

[imperva.com](https://imperva.com)