

# Threat Intel Report: October 28-November 3, 2024

## Countries



## Top Tags

PSAUX

Jumpy Pisces

PLAY

Cactus

Rhysida

## Executive Summary

### Actionable Information:

- **Ransomware Targeting Broadened Across Platforms:** The increase in ransomware attacks on both traditional and non-traditional platforms, such as MacOS, indicates that threat actors are broadening their focus to exploit previously overlooked vulnerabilities, suggesting a shift in the threat landscape.
- **Increased Threat from Zero-Click Vulnerabilities:** Newly discovered zero-click vulnerabilities allow attackers to compromise systems without user interaction, highlighting a critical need for improved security protocols in software design and deployment.
- **Weaponization of AI Technologies:** The manipulation of AI models to generate malicious code represents a concerning trend in the weaponization of technology for cyberattacks. This raises important considerations for monitoring AI outputs and implementing safeguards against misuse.
- **Persistent Risks from Legacy Software Vulnerabilities:** The prevalence of long-standing vulnerabilities in widely used software underscores the importance of proactive patch management and regular system audits to address outdated or insecure components.
- **Targeting of Sensitive Data in Critical Sectors:** Recent high-profile data breaches affecting sensitive personal data in government and healthcare sectors reveal a trend toward targeting critical infrastructure, emphasizing the need for enhanced security measures and robust incident response plans.

### Outlook:

As cyber threats continue to evolve, the week's incidents highlight a concerning shift towards increasingly sophisticated and varied attack vectors. Ransomware attacks are not only becoming more prevalent across various sectors, including government and healthcare, but are also being executed with new methodologies that bypass traditional defenses. The exploitation of zero-click vulnerabilities and the growing manipulation of AI technologies point to a future where

attackers leverage both human error and technical loopholes more effectively. Organizations must remain vigilant and prioritize the implementation of robust security measures, timely patching of systems, and comprehensive incident response strategies to mitigate these rising threats and safeguard sensitive information.

## Threat Activity in Imperva

### Top CVE Growth This Week:

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

📈 1,808% [CVE-2023-0669](#)

- Fortra GoAnywhere MFT suffers from a pre-authentication command injection vulnerability in the License Response Servlet due to deserializing an arbitrary attacker-controlled object.

📈 282% [CVE-2023-34960](#)

- A command injection vulnerability in the wsConvertPpt component of Chamilo v1.11.\* up to v1.11.18 allows attackers to execute arbitrary commands via a SOAP API call with a crafted PowerPoint name.

📈 47% [CVE-2023-30185](#)

- CRMEB v4.4 to v4.6 was discovered to contain an arbitrary file upload vulnerability via the component \attachment\SystemAttachmentServices.php.

### US Financial Site Targeted by Automated Attacks

**+Financial Services +US +Automated Attacks**

- A US financial site's login portal was targeted by automated attacks this week, reaching 1.6M requests. Attacks came from vulnerability scanners based in the US, including one specifically probing for Shellshock vulnerabilities.

### French Business Site Hit by 1.5M Path Traversal, XSS, and RCE Attacks

**+France +Business +Path Traversal +XSS +RCE**

- A French business site experienced path traversal, cross-site scripting (XSS) and remote code execution (RCE) attacks this week, reaching almost 1.5M requests and coming primarily from France-based automated tools.

## Recent Cyber Threats

### MacOS Malware Strikes with Fake Finder Ransomware

**+Mac +Malware +Ransomware**

- Security researchers recently discovered a MacOS-targeted [ransomware strain](#) pretending to be Finder, Apple's native file manager, which attempts to scare users into paying for data recovery. The malware encrypts data and demands a ransom, a rare approach in the Mac ecosystem where ransomware is less common.

### 22,000 CyberPanel Servers Vulnerable to Critical Zero-Click Exploit

**+RCE +PSAUX +Ransomware**

- A newly discovered zero-click remote code execution (RCE) vulnerability in [CyberPanel](#), a popular web hosting control panel, has left 22,000 servers exposed to potential attacks. The vulnerability allows attackers to gain full access to servers without any interaction from users, posing a severe risk to web hosting companies and administrators globally. The instances are actively targeted by [PSAUX](#) ransomware, leveraging the vulnerability to gain access and encrypt data across affected instances.

### ChatGPT Manipulated Using Hex Encoding

#### +AI +LLM +Hexadecimal

- Security researchers demonstrated a method to manipulate ChatGPT into outputting malicious code by encoding it as [hexadecimal](#), effectively bypassing OpenAI's content filters. Using this approach, they were able to have ChatGPT generate potentially harmful code snippets that evade detection by traditional filtering mechanisms.

### Cross-Barking Attack Puts Opera Browser Users at Risk

#### +Opera +Cross-Barking +API

- Researchers uncovered a new privacy vulnerability called the [Cross-Barking attack](#), which exploits hidden APIs in the Opera browser to track users across websites. This flaw enables malicious sites to bypass typical security restrictions and access sensitive browsing data from other tabs, putting user privacy at risk. The vulnerability, rooted in Opera's implementation of secret APIs, affects millions of users and raises questions about the security of lesser-known browser features.

### North Korean APT Group Deploys PLAY Ransomware in Targeted Attacks

#### +Jumpy Pisces +Andariel +North Korea +PLAY +Ransomware

- Researchers have linked North Korea's APT group [Jumpy Pisces](#) aka Andariel to recent ransomware attacks using the PLAY ransomware variant, marking a shift toward financially motivated cybercrime. The group targeted organizations across sectors, including critical infrastructure, to extort ransoms through data encryption and theft. This activity shows North Korean threat actors expanding their tactics to include ransomware, with potentially severe consequences for victims in various industries.

### 18-Year-Old Vulnerability in X.Org Server Puts Linux Systems at Risk

#### +Linux +CVE

- An 18-year-old memory corruption vulnerability ([CVE-2024-9632](#)) in the X.Org Server has been disclosed, affecting numerous Linux distributions. This flaw can allow attackers to escalate privileges, potentially gaining root access on unpatched systems. The vulnerability underscores long-standing security gaps in legacy code, emphasizing the importance of timely patches to protect Linux environments from exploitation.

### FakeCall Android Malware Redirects Banking Calls to Scammers

#### +FakeCall +Malware +Android +Financial Services

- The [FakeCall](#) Android malware has evolved to intercept and redirect calls to bank customer service lines, tricking victims into speaking directly with attackers posing as bank representatives. By impersonating official bank support, the attackers extract sensitive information, leading to financial fraud and identity theft. This new capability heightens risks for mobile banking users, who are advised to verify banking communications and avoid installing unverified apps.

### qBittorrent Patches 14-Year-Old Vulnerability Exposing Users to MITM Attacks

#### +qBittorrent +MITM

- A recently patched flaw in [qBittorrent](#) exposed users to potential man-in-the-middle (MITM) attacks for 14 years, allowing attackers to intercept and manipulate traffic. Since 2010, qBittorrent accepted any certificate, including forged and illegitimate ones, enabling attackers in a man-in-the-middle position to modify network traffic. The vulnerability, affecting both encrypted and unencrypted connections, left users vulnerable to data theft and malware injection.

---

## Data Breaches

### HACLA Confirms Data Breach by Cactus Ransomware Gang

#### +Government +US +Cactus +Ransomware

- The Housing Authority of the City of Los Angeles ([HACLA](#)) has confirmed a data breach involving the Cactus ransomware group, which has allegedly stolen 900GB of information. The breach reportedly includes personal

information, backups, financial documents, and internal communications. HACL A was previously targeted by LockBit in 2022, and the data was published online after they refused to pay the ransom.

## Hackers Claim to Sell Access to Nokia's Internal Data for \$20,000

**+Telecommunications +IntelBroker**

- Notorious hacker IntelBroker has announced they possess access to [Nokia's](#) internal data, offering it for sale on the dark web for \$20,000. The actor claims to have acquired sensitive information, including SSH keys, source code, RSA keys, Bitbucket logins, SMTP accounts, webhooks, and hardcoded credentials. The data allegedly comes from a third-party contractor linked to Nokia's internal tools development.

## Landmark Data Breach Affects 800,000 Insurance Customers

**+Insurance**

- [Landmark Health](#) has disclosed a significant data breach impacting approximately 800,000 insurance customers, where sensitive personal information– including names, birth dates, Social Security numbers, and insurance policy information–was compromised.

## Columbus Ransomware Attack Exposes Data of 500,000 Individuals

**+Government +US +Rhysida**

- A ransomware attack on the city of [Columbus, Ohio](#), has exposed the personal information of approximately 500,000 individuals, including Social Security numbers and driver's license information. The attack was carried out by the Rhysida ransomware group, which claims to have stolen 6.5 TB of sensitive data. After failed negotiations, the group has posted 3.1 TB of the data on its leak site.

---

## 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.