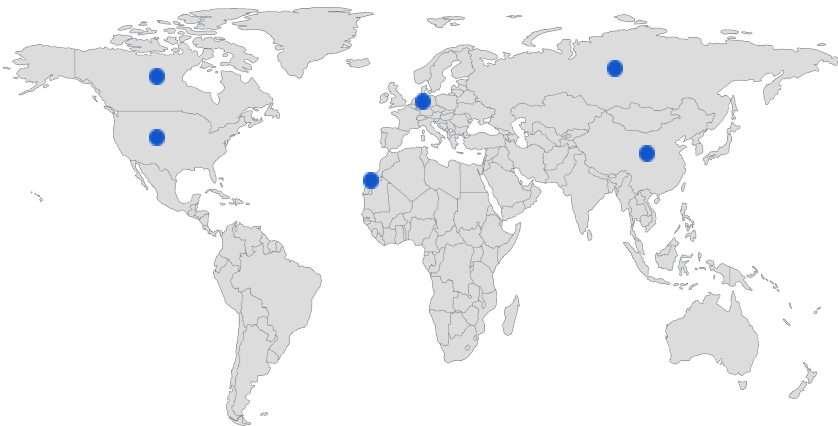


Threat Intel Report: April 8-14, 2024

Countries



Top Tags

Starry Addax

TA547

Rhadamanthys

Muliaka

RansomHub

Executive Summary

Actionable Information:

- *E-commerce Platforms Targeted:* Persistent malware attacks have been identified within Magento's XML templates, revealing vulnerabilities in e-commerce security and the need for heightened monitoring and patch management.
- *AI and Software Development Risks:* Architectural flaws in AI models on Hugging Face and GitHub's manipulated search functions demonstrate increased risks in software development environments, necessitating rigorous code reviews and enhanced security protocols.
- *Sector-Specific Attacks:* Notable targeted attacks include the hospitality industry in Europe and retail businesses in Germany, emphasizing the need for sector-specific security enhancements and training to recognize phishing attempts.
- *IoT and Smart Devices:* Security vulnerabilities in IoT devices like LG Smart TVs highlight ongoing challenges in device security, underscoring the importance of regular updates and patches.
- *Ransomware Evolution:* The emergence of new ransomware groups exploiting leaked codes, like Muliaka using Conti's source code, calls for robust network defenses and backup strategies to mitigate ransomware threats.

Outlook:

The landscape of cyber threats continues to evolve with sophisticated attacks targeting diverse sectors and technologies. The current trends suggest an increased focus on exploiting vulnerabilities in e-commerce, AI technologies, and IoT devices, alongside a resurgence in ransomware activities leveraging previously leaked codes. Going forward, organizations must prioritize comprehensive security measures including regular updates, in-depth training, and the deployment of advanced threat detection and response systems. Enhanced collaboration between



industries and cybersecurity agencies is also crucial to stay ahead of emerging threats and mitigate potential breaches effectively. These measures, combined with vigilant monitoring and rapid incident response strategies, will be vital in protecting sensitive data and maintaining trust in digital platforms.

Threat Activity in Imperva

Top 3 CVEs targeted this week:

Imperva customers are protected against these CVEs.

⬆ 13% [CVE-2023-30185](#)

- A file upload vulnerability in some versions of CRMEB

⬆ 25% [CVE-2024-27199](#)

- A path traversal vulnerability in JetBrains TeamCity

⬇ 1% [CVE-2023-35082](#)

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

Second Largest DDoS Attack This Year Targets China

+DDoS +China

- The second largest DDoS attack of 2024 has targeted a Chinese site, reaching 4.2M requests per second (RPS). The attack, lasting almost five hours, came from about 2,600 distinct IPs, mainly based in China and the US.

US Travel Site Sees Automated Attacks

+US +Travel +Scanning

- A US travel site saw abnormally large automated attacks this week, reaching almost 7M requests over two days. The attacks, which were likely scanning for access points, came exclusively from within the US.

Recent Cyber Threats

Persistent Malware Disguised within Magento's XML

+E-Commerce +Magento

- A new, persistent backdoor has been detected in [Magento's](#) XML layout templates, cleverly used by attackers to inject malware into e-commerce sites. This backdoor enables remote code execution when the checkout cart is accessed, using a manipulated XML code that reinstalls the malware even after manual removals. The threat has led to additional vulnerabilities including a fake Stripe payment skimmer, directly compromising customer payment data.

Generative AI Models Compromised by Architectural Flaws

+AI

- Several critical security vulnerabilities have been identified in generative AI models on [Hugging Face](#), potentially leading to customer data theft. The flaws allow unauthorized execution of code via the AI models, highlighting a significant oversight in the architecture that could be exploited to access and steal personal and sensitive data, posing a serious risk to all users and developers relying on these AI resources.

Widespread Vulnerability in Hotel Self-Service Terminals

+Travel +Germany

- A significant security breach was found in the self-service check-in terminals used across [European hotels](#), particularly in a German Ibis hotel. The vulnerability enables unauthorized individuals to obtain guest room codes without needing sophisticated tools, by simply using a sequence of dashes in the terminal prompt. This flaw exposes guests to potential theft and personal safety risks, and despite remediation efforts, it reflects broader security issues within the hospitality industry's check-in systems.

Crypto Drainers Invade Thousands of WordPress Sites

+Crypto +WordPress

- Hackers have compromised nearly 2,000 [WordPress](#) sites to install crypto drainers, tricking visitors with fake NFT offers and cryptocurrency discounts. The attacks exploit vulnerable sites to display malicious pop-ups, coaxing users to connect their crypto wallets, which then enables the drainers to siphon off funds. Initially focused on using these sites for brute-forcing other sites' admin passwords, attackers have pivoted to monetizing their access through crypto scams, significantly raising the risks for visitors of these compromised sites.

Critical Security Loopholes in LG Smart TVs

+Entertainment

- Researchers have discovered critical security vulnerabilities in various [LG Smart TV](#) models that run on webOS versions 4 through 7. These vulnerabilities allow attackers to bypass authentication protocols, escalate privileges, and execute arbitrary commands. The issues, which were disclosed responsibly to LG and have since been patched, highlight ongoing security challenges in IoT devices and the need for regular updates and patches.

Starry Addax Targets Sahrawi Activists with Advanced Malware

+Starry Addax +Phishing +Android +FlexStarling +Sahrawi Arab Democratic Republic

- [Starry Addax](#), a new cyber threat actor, has been actively targeting human rights defenders linked to the Sahrawi Arab Democratic Republic in North Africa. The group uses sophisticated phishing schemes to deliver malware through malicious Android apps that impersonate legitimate applications. This malware, known as FlexStarling, enables extensive access to compromised devices, including sensitive data exfiltration. Starry Addax's focused attacks on activists demonstrate a high level of sophistication and pose a significant threat to privacy and security in the region.

Manipulating GitHub Search to Spread Malware

+Malware +GitHub

- Cybercriminals have developed a new technique to exploit [GitHub's](#) search functionality by creating repositories that appear legitimate but contain malware. These repositories are enhanced with fake stars and frequent updates to rank high in search results, misleading developers into downloading harmful code. This supply chain attack targets developers by embedding malicious code within project files, which execute automatically upon building the projects, posing serious threats to software integrity and security.

Rhadamanthys Malware Campaign Targets Germany

+TA547 +Germany +Retail +Rhadamanthys

- [TA547](#), a known threat actor, has launched a targeted campaign against German organizations using the Rhadamanthys malware. This operation involves sending phishing emails that impersonate the German retail giant Metro and include a password-protected ZIP file containing malicious LNK files. These files, when executed, deploy PowerShell scripts to load Rhadamanthys directly into memory, bypassing disk-based detection mechanisms. This marks the first known instance of TA547 using LLM-generated scripts for sophisticated cyberattacks.

Zero-Day in Telegram Desktop Exploited to Launch Python Scripts

+Telegram +Python

- A zero-day vulnerability in [Telegram's](#) Windows application was discovered, which allowed attackers to launch Python scripts on users' devices without triggering security warnings. The exploit was facilitated by a typo in Telegram's source code, misidentifying Python file extensions, thereby bypassing Telegram's internal security

checks. Although initially disputed by Telegram, the issue was confirmed and patched via a server-side fix. This vulnerability underscores the risks associated with file handling security in widely used messaging applications.

Data Breaches

Muliaka Ransomware Operation Exploits Conti Leak

+Muliaka +Russia +Ransomware +Conti

- A new ransomware group named [Muliaka](#) has emerged, targeting Russian businesses by leveraging the leaked source code from the notorious Conti ransomware group. The Muliaka ransomware disrupts businesses by encrypting critical data and demanding ransom payments. Their method involves disguising the ransomware as legitimate corporate antivirus software, thereby gaining unfettered access to corporate networks. The group's activities underscore the persistent threat of ransomware and the dangers of source code leaks in enhancing cybercriminal capabilities.

Massive Security Breach Compromises 576,000 Roku Accounts

+Credential Stuffing

- [Roku](#) has disclosed a breach impacting 576,000 accounts where hackers made unauthorized purchases using stored payment methods. The breach was discovered during investigations into a smaller, earlier incident. It was executed via credential stuffing, using previously breached credentials. Roku has reset passwords for affected accounts and enabled two-factor authentication universally as remedial measures.

Giant Tiger's Data Breach Exposes 2.8 Million Customer Records

+Canada +Retail

- The Canadian retailer [Giant Tiger](#) has suffered a data breach resulting in the exposure of 2.8 million customer records, including email addresses, names, and physical addresses. The breach, attributed to a compromised third-party vendor, did not involve payment information or passwords. The leaked data includes extensive customer interaction data with the store, increasing the risk of phishing attacks. Customers are advised to remain vigilant for suspicious communications.

Sisense Data Breach Prompts CISA Investigation

+Analytics +Critical Infrastructure

- [Sisense](#), a major data analytics firm, experienced a significant data breach, prompting an investigation by CISA due to the potential impact on critical infrastructure sectors. The breach involved unauthorized access to customer data including email passwords and SSL certificates, reportedly through compromised GitLab repository credentials. This extensive breach has led to stolen terabytes of data, raising severe concerns about the security of Sisense's data handling and the broader implications for its global customer base.

RansomHub Leaks Stolen Change Healthcare Patient Data

+Healthcare +RansomHub +ALPHV

- An extortion gang known as RansomHub has leaked sensitive patient records from [Change Healthcare](#), impacting millions. This incident marks the second ransom demand targeting the company, with the stolen data including patient billing and medical information. The breach is linked to a ransomware attack facilitated by ALPHV, a ransomware gang, which complicates the situation with internal disputes among cybercriminals over ransom payments. Change Healthcare is coordinating with law enforcement to manage the breach, which has led to multiple extortion attempts.

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