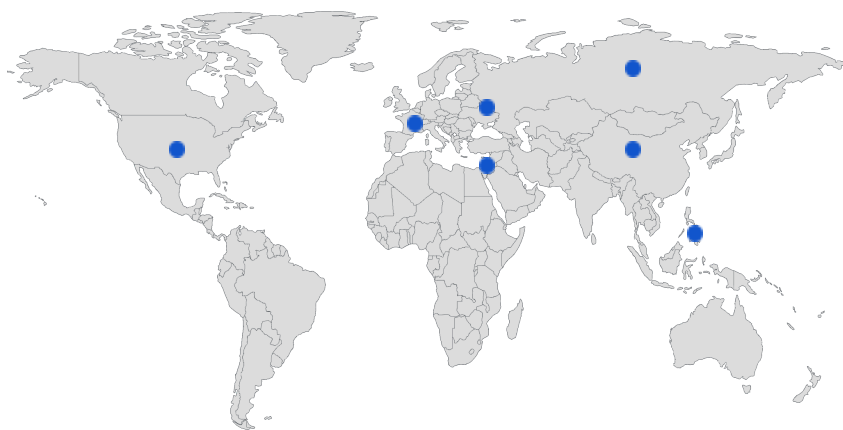


Threat Intel Report: October 21-27, 2024

Countries



Top Tags

ShadyShader

APT28

perftl

APT41

Handala

Executive Summary

Actionable Information:

- **Heightened Focus on Supply Chain Security:** Organizations are increasingly vulnerable to attacks targeting third-party tools and open-source dependencies, necessitating rigorous validation and monitoring practices to prevent breaches from exploited vulnerabilities.
- **Evolving Phishing and Malware Tactics:** Cybercriminals are innovating phishing strategies and malware deployment techniques, emphasizing the need for comprehensive security awareness training and enhanced email filtering systems to safeguard sensitive information.
- **Rising Threats in Politically Sensitive Sectors:** Nation-state actors are intensifying their focus on politically charged environments, indicating a need for proactive risk assessments and defensive measures to protect critical infrastructure and information from potential cyber espionage.

Outlook:

The outlook for cybersecurity suggests an ongoing rise in sophisticated, targeted attacks that exploit both technology vulnerabilities and human behavior, particularly in critical and politically charged sectors. State-sponsored actors will likely continue targeting government entities and companies for espionage and financial gain, while cybercriminals increasingly focus on supply chain vulnerabilities to amplify their reach. Moving forward, organizations must prioritize cloud security, supply chain validation, and threat awareness to preempt potential breaches and secure sensitive information.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 17% [CVE-2023-40044](#)

- In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system

↑ 25% [CVE-2023-3460](#)

- The Ultimate Member WordPress plugin before 2.6.7 does not prevent visitors from creating user accounts with arbitrary capabilities, effectively allowing attackers to create administrator accounts at will.

↑ 51% [CVE-2023-6875](#)

- The POST SMTP Mailer – Email log, Delivery Failure Notifications and Best Mail SMTP for WordPress plugin for WordPress is vulnerable to unauthorized access of data and modification of data due to a type juggling issue on the connect-app REST endpoint, making it possible for unauthenticated attackers to reset the API key used to authenticate to the mailer and view logs, including password reset emails, allowing site takeover.

French Retail Site Targeted in 4.5M RPS DDoS Attack

[+France](#) [+DDoS](#) [+Retail](#)

- A French retail site was hit by a large application-layer DDoS attack this week, reaching 4.5 million requests per second (RPS) in only 9 minutes. Application-layer attacks of this scale can quickly disrupt e-commerce operations, potentially leading to losses in revenue, brand reputation, and customer trust.

Filipino Government Sites Hit by Automated Attacks

[+Government](#) [+Philippines](#) [+Automated Attack](#)

- Several government sites in the Philippines were targeted by automated attacks this week, reaching a collective 35 million requests in one day. These attacks, involving browser impersonation tools and other automated methods, coincided with a powerful tropical storm sweeping through the Philippines. The timing raises the possibility that threat actors exploited the storm's disruption to divert attention from digital defenses, knowing that emergency responses would be focused on the physical crisis, thus decreasing the likelihood of immediate detection and mitigation.

Recent Cyber Threats

One-Click Apple M-Series Crash Exploit Uncovered

[+ShadyShader](#) [+CVE](#)

- A new vulnerability dubbed [ShadyShader](#) has been found to exploit Apple's M-series chips, causing them to crash with a single click. This flaw allows a specially crafted shader program to overwhelm Apple's GPU, causing repeated freezes that ultimately lead to a system crash.

DDoS Attack Targets Russian Independent Media Outlet

[+Russia](#) [+Journalism](#) [+DDoS](#)

- [Novaya Gazeta Europe](#), an independent Russian media outlet, was hit with a significant DDoS attack, temporarily disabling access to its online platform. The attack comes amidst heightened tensions in Russia, likely aiming to

suppress critical reporting on local events. This marks another example of cyber pressure faced by independent media in Russia.

Russian APT Group Targets European Diplomats for Espionage

+APT28 +Russia +Ukraine +Government +Malware

- Russian-linked espionage group [APT28](#) has been observed targeting the Ukrainian military with spear-phishing campaigns. APT28 operates a Telegram channel called Civil Defense, which claims to be a provider of free software programs designed to enable potential conscripts to view and share crowdsourced locations of Ukrainian military recruiters. If someone opens this attachment on Android devices that have Google Play Protect disabled, it deploys an operating system-specific commodity malware along with a decoy mapping application dubbed SUNSPINNER.

New Technique Jailbreaks AI Models

+Deceptive Delight

- Researchers have introduced a novel adversarial technique called [Deceptive Delight](#), designed to jailbreak large language models (LLMs). This approach leverages multi-turn conversations to bypass LLM safety measures by embedding harmful prompts within innocuous interactions, achieving a high success rate in tricking models into generating unsafe content.

Fake ESET Emails Targets Israeli Organizations with Malware

+Israel +Malware +Handala

- Hackers have launched a phishing campaign impersonating cybersecurity firm [ESET](#), targeting organizations in Israel with wiper malware. The phishing emails, falsely claiming to be from ESET, directed recipients to download malicious files under the guise of responding to a state-sponsored attack. ESET stated it was not compromised, noting that the malicious campaign was quickly blocked and involved a partner company in Israel. Security experts suspect links to pro-Palestinian threat actors, specifically Handala.

Critical File Read Vulnerability Found in Vendure E-commerce Platform

+CVE +eCommerce

- A newly discovered vulnerability, [CVE-2024-48914](#), in the Vendure e-commerce platform could allow attackers to read sensitive files remotely, posing a severe risk to affected online stores. This high-severity flaw (CVSS 9.1) makes customer and transaction data vulnerable to theft if exploited. Vendure users are encouraged to update immediately to secure their systems.

Docker API Exploited by Malware to Control Exposed Servers

+API +Malware +perftcl +Cryptomining

- Attackers are exploiting unprotected Docker Remote API endpoints to deploy a new malware strain called [perftcl](#), which hijacks server resources for cryptocurrency mining. The malware affects organizations with insufficiently secured Docker environments, adding another layer to the risks associated with exposed APIs in DevOps setups.

Malicious NPM Packages Targeting Backend Development Tools

+Ethereum +npm

- Researchers have discovered malicious npm packages targeting [Ethereum](#) developers by collecting private keys and enabling unauthorized SSH access to compromised systems. These packages, masked as legitimate dependencies, require developers to initiate certain functions, such as creating new wallets, to activate the backdoor, which then uploads sensitive data to an attacker-controlled domain.

AWS CDK Vulnerability Exposes Accounts to Takeover Risk

+S3 Buckets +Namesquatting +AWS

- A vulnerability in the AWS Cloud Development Kit allows attackers to conduct S3 bucket [namesquatting](#), potentially allowing attackers to gain control over buckets. This issue poses a risk of account takeover if malicious actors identify and exploit these misconfigurations. Users are advised to audit and secure their AWS configurations promptly.

Data Breaches

Chinese APT41 Targets Global Gambling Sector for Profit

[+China](#) [+APT41](#) [+Gambling](#)

- Chinese nation-state hackers from [APT41](#) have been observed launching financially motivated attacks against global gambling entities. Using a mix of social engineering and technical exploits, the group seeks financial gain while compromising sensitive corporate data. This campaign highlights the diverse tactics employed by APT41 to expand their influence.

France's Second-Largest ISP Confirms Data Breach Post-Leak

[+France](#) [+ISP](#)

- [Free](#), the second-largest ISP in France, confirmed a data breach following the online leak of customer information. The breach reportedly exposed personal data and account details, raising privacy concerns for millions of affected customers. The data stolen in the attack is now being auctioned on BreachForums to the highest bidder, with the threat actor claiming that the breach impacts almost a third of France's population.

UnitedHealth Customer Data Leak Affects 100 Million Accounts

[+Healthcare](#) [+US](#)

- A breach of [UnitedHealth's](#) database exposed sensitive data of 100 million customers, marking one of the largest healthcare data breaches in recent years. Compromised information includes medical records and personal details, posing serious privacy risks and potential identity theft. The breach is a stark reminder of the cybersecurity vulnerabilities in the healthcare industry.

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.