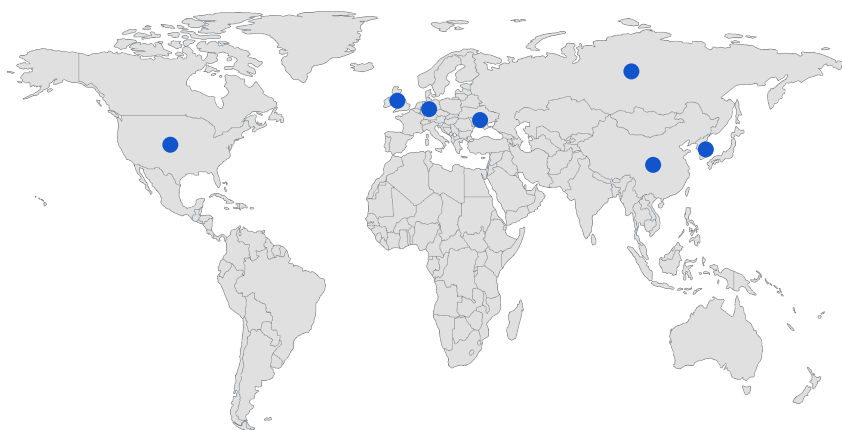


Threat Intel Report: December 16-22, 2024

Countries



Top Tags

Clop

BadBox

Nova

Snake

XLoader

Executive Summary

Actionable Information:

- **Ransomware and Zero-Days:** The Clop ransomware gang continues to exploit zero-day vulnerabilities, targeting Cleo's managed file transfer platforms to steal corporate data. Organizations should prioritize patching known vulnerabilities and improving monitoring for zero-day threats.
- **State-Sponsored Attacks: Russian** state actors are focusing on critical infrastructure in the UK and launching large-scale attacks on Ukrainian state registries, signaling an increase in geopolitical cyber tensions. Enhanced threat intelligence sharing and sector-specific defenses are critical for resilience.
- **Healthcare and Data Breaches:** The healthcare industry faced significant breaches, affecting millions through attacks on Ascension, HealthSource RI, and ConnectOnCall. These incidents highlight the critical need for robust data encryption and real-time monitoring in healthcare systems.
- **Sophisticated Malware Campaigns:** Malware like Nova (a Snake keylogger variant), XLoader, and BadBox demonstrate increasing sophistication in delivery and evasion techniques. Mitigations include deploying advanced endpoint detection and user training to avoid malicious downloads.
- **Platform Exploitation:** Attack vectors such as SharePoint (XLoader malware) and open-source IT software (GLPI vulnerabilities) emphasize the need for strict configuration management and routine security audits.
- **Exploitation of Consumer Channels:** Android spyware apps disguised as health tools on mainstream platforms like the Amazon Appstore underline the importance of app vetting and educating users about malicious applications.

Outlook:

This week underscores a troubling trend of increased targeting of critical infrastructure, healthcare, and widely used platforms. State-sponsored attacks are becoming more aggressive, with a focus on disruption and data theft, particularly

in geopolitical hotspots. Meanwhile, ransomware operators and malware campaigns are leveraging sophisticated evasion tactics and exploiting unpatched systems to maximize impact. Organizations must prioritize a proactive defense strategy by investing in real-time monitoring, advanced threat intelligence, and user education to mitigate risks. As the cyber threat landscape continues to evolve, collaboration across sectors and nations will be critical to combating these growing challenges.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 118% [CVE-2024-50623](#)

- In Cleo Harmony before 5.8.0.21, VLTrader before 5.8.0.21, and LexiCom before 5.8.0.21, there is an unrestricted file upload and download that could lead to remote code execution.

📈 101% [CVE-2024-8963](#)

- Path Traversal in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.

📈 96% [CVE-2023-26009](#)

- Improper Privilege Management vulnerability in favethemes Houzez Login Register allows Privilege Escalation. This issue affects Houzez Login Register: from n/a through 2.6.3.

Korean Sports Betting Site Hit With Almost 3M RPS DDoS Attack

+Korea +US +China +DDoS +Gambling

- A Korean sports betting site was recently targeted by an application-layer DDoS attack reaching 2.7 million requests per second (RPS) in 15 minutes. The attacks came from over 2,000 distinct IP addresses, primarily based in the US and China.

Bots Attempt To Gain Unauthorized Access to US Computing Site

+US +Computing +Automated Attack

- A US computing site had a three-day automated attack this week, coming from US-based IP addresses. The attack, which reached almost 5M requests at its peak, targeted login, admin, and account pages in a likely attempt to find and exploit unauthorized access.

Recent Cyber Threats

Clop Ransomware Gang Exploits Cleo Zero-Day Vulnerabilities

+Clop +Ransomware

- The [Clop](#) ransomware group has claimed responsibility for recent data theft attacks exploiting zero-day vulnerabilities in Cleo's managed file transfer platforms. By leveraging flaws tracked as CVE-2024-50623 and CVE-2024-55956, the group breached corporate networks to steal sensitive data.

Germany Disrupts BadBox Malware Operations

+Germany +BadBox +Malware +Android

- Germany's Federal Office for Information Security (BSI) has successfully severed hacker access to approximately 30,000 devices infected with [BadBox](#) malware. The malware, pre-installed on various Android

devices, allowed attackers to remotely control compromised systems. BSI's intervention involved redirecting malicious traffic to secure servers, effectively neutralizing the threat.

GLPI Vulnerabilities Expose Systems to Potential Attacks

+IT +Code Execution

- Multiple critical vulnerabilities have been identified in [GLPI](#), an open-source IT asset management software, potentially allowing attackers to execute arbitrary code and compromise systems. Administrators are urged to apply the latest patches to mitigate these risks.

Nova: Enhanced Snake Keylogger Variant Emerges

+Nova +Snake +Keylogger

- A new variant of the Snake Keylogger, dubbed [Nova](#), has been discovered, featuring advanced techniques to evade detection and enhanced capabilities for data theft. Users are advised to update their security measures to detect and prevent infections.

XLoader Malware Delivered via Sophisticated SharePoint Attack

+Xloader +SharePoint

- The [XLoader](#) malware is being distributed through a complex attack vector involving Microsoft SharePoint, tricking users into downloading malicious files. This method increases the malware's reach, posing significant risks to organizations utilizing SharePoint.

Russian State Actors Target UK Critical Infrastructure

+Russia +UK +Critical Infrastructure

- [Russian state-sponsored cyber actors](#) have launched a campaign targeting the UK's critical infrastructure, including energy and transportation sectors. The attacks aim to disrupt services and gather intelligence, escalating cyber tensions between the nations.

Ukraine's State Registries Hit by Massive Cyberattack

+Ukraine +Russia

- Ukraine's [state registries](#), containing vital citizen information, were temporarily suspended following a significant cyberattack attributed to Russian actors. The disruption is expected to last up to two weeks, impacting administrative services nationwide.

Android Spyware Disguised as Health App Found on Amazon Appstore

+Android +Healthcare +Spyware

- A [malicious Android application](#) posing as a health tool was discovered on the Amazon Appstore, designed to steal sensitive user information. Although removed from the store, users who installed the app are advised to uninstall it and scan their devices for potential threats.

Data Breaches

Massive Health Care Data Breach Threatens Millions

+Healthcare +US

- A significant data breach in the healthcare company [Ascension](#), which operates 140 hospitals and 40 senior care facilities, has compromised the personal information of millions of individuals. The breach exposes sensitive data, including medical records and personal identifiers, posing substantial risks to affected individuals.

Rhode Island's HealthSource RI Faces Data Breach Amid Enrollment

+US +Healthcare

- [HealthSource RI](#), Rhode Island's health coverage exchange, experienced a data breach during its open enrollment period. The incident has raised concerns about the security of personal information for residents seeking health coverage.

Duke Energy Announces Data Breach Affecting Over 8 Million Customers

+Energy +US

- [Duke Energy](#) has reported a data breach potentially impacting more than 8 million customers. The compromised information includes personal and account details, prompting the company to enhance security measures and notify affected individuals.

ConnectOnCall Health Data Breach Puts Over 910,000 Patients at Risk

+Healthcare

- [ConnectOnCall](#), a healthcare communication platform, suffered a data breach affecting over 910,000 patients. The exposed data includes sensitive health information, leading to potential privacy risks for those impacted.

BeyondTrust Reports Breach of Remote Support SaaS Instances

+Cybersecurity +API

- [BeyondTrust](#), a cybersecurity firm specializing in privileged access management, disclosed a breach involving its Remote Support SaaS instances. Threat actors exploited an API key to reset passwords for local application accounts, affecting a limited number of customers.

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.