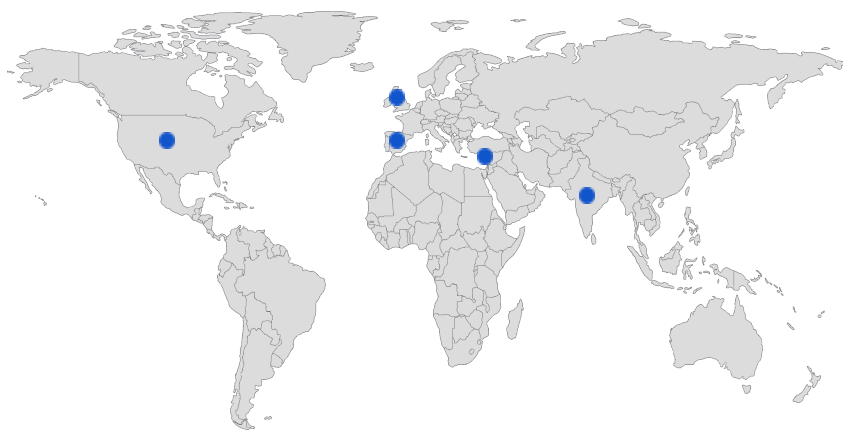


Threat Intel Report: November 18-24, 2024

Countries



Top Tags

Lumma

K-47

NgIOweb

needrestart

Akira

Executive Summary

Actionable Information:

- **AI and Infostealer Malware:** Cybercriminals are exploiting fake AI video generation tools to distribute Lumma infostealer malware, targeting both Windows and macOS users. This highlights a growing trend of leveraging popular themes (like AI tools) for malicious activity.
- **Critical Vulnerabilities:** There are several active vulnerabilities being exploited, including those in Citrix Virtual Apps, Ubuntu, and mySCADA systems. These flaws expose systems to remote code execution and unauthorized access, emphasizing the ongoing risk from outdated or misconfigured systems.
- **Targeted Attacks on Key Industries:** The food & beverage, financial services, and healthcare sectors were prime targets this week. Starbucks faced a ransomware attack disrupting payroll, while over 8,100 financial institutions were impacted by a breach in Finastra.
- **Increased Ransomware Aggression:** Groups like Akira and NgIOweb are ramping up operations, with Akira leaking the largest number of victim data so far and the NgIOweb botnet fueling credential-stuffing attacks.

Outlook:

The overall outlook continues to show a heightened focus on exploiting vulnerabilities in critical infrastructure and widely-used software, particularly in the remote access and healthcare sectors. Threat actors are becoming increasingly sophisticated in using popular themes and technologies (e.g., AI) to bait victims into malicious activities. While many of these incidents are still under investigation, the rapid exploitation of vulnerabilities in systems like Citrix and Ubuntu suggests that attackers are capitalizing on delayed patching and weak security practices. In the ransomware sector, aggressiveness is on the rise, and organizations must prepare for more frequent, larger-scale data breaches and financial fraud.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 52,857% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.

↑ 3,224% [CVE-2023-28770](#)

- The sensitive information exposure vulnerability in the CGI "Export_Log" and the binary "zcmd" in Zyxel DX5401-B0 firmware could allow a remote unauthenticated attacker to read the system files and to retrieve the password of the supervisor from the encrypted file.

↑ 1,200% [CVE-2024-51568](#)

- CyberPanel allows Command Injection via `completePath` in the `ProcessUtilities.outputExecutioner()` sink. There is `/filemanager/upload` (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.

Recent Cyber Threats

Fake AI Video Generators Infect Windows and macOS with InfoStealer

+Lumma +Infostealer

- Cybercriminals are distributing info stealers disguised as [fake AI video generator tools](#), targeting both Windows and macOS users. These malicious applications claim to offer advanced video creation capabilities but instead install Lumma info stealer malware on victims' devices. The malware collects sensitive data, including login credentials, cryptocurrency wallets, and other personal information, and transmits it to threat actors.

Citrix Virtual Apps and Desktops Vulnerabilities Actively Exploited

+CVE +Citrix

- Two vulnerabilities in [Citrix's](#) "Virtual Apps and Desktops" remote access solution, CVE-2024-8068 and CVE-2024-8069, are actively being exploited in the wild, allowing threat actors to execute arbitrary code on vulnerable systems. These vulnerabilities arise from multiple factors, including an exposed and misconfigured Microsoft Message Queuing (MSMQ) instance coupled with the utilization of the insecure `BinaryFormatter` class within the Citrix software stack.

Starbucks Supplier Ransomware Attack Disrupts Employee Tracking System

+Food & Beverage +US

- A ransomware attack on one of [Starbucks'](#) software suppliers has disrupted operations. The breach has caused delays in processing payroll, directly impacting employees' payments. Starbucks is working with the supplier to restore functionality and mitigate the effects on its workforce, while details about the attacker remain undisclosed.

APT Group K-47 Uses Hajj Lures Against Palestinian Targets

+K-47 +Palestine

- An advanced persistent threat (APT) group tracked as [K-47](#) has been observed using Hajj-themed lures in a campaign targeting Palestinian individuals and organizations. The attacks employ malicious Microsoft Office documents to initiate the compromise. K-47, also known as Mysterious Elephant, is a politically-motivated threat actor that has a history of targeting entities across the Middle East and North Africa region.

NgIOWeb Botnet Commandeers Residential Devices for Credential Stuffing Attacks

+NglOweb +NSOCKS +Credential Stuffing +Botnet

- Researchers have uncovered a large-scale botnet named [NglOweb](#) that leverages thousands of compromised residential routers and internet-connected devices to fuel DDoS attacks. The botnet is designed to be resilient, with its operations orchestrated through a decentralized infrastructure spanning tens of thousands of machines globally. NglOweb-compromised devices are sold as proxy servers for NSOCKS, which has been used in credential-stuffing attacks.

Decades-Old Vulnerabilities in Ubuntu Could Give Attackers Root Privileges

+Ubuntu +needrestart +Code Execution

- Multiple decade-old security vulnerabilities have been disclosed in the [needrestart](#) package installed by default in Ubuntu Server that could allow a local attacker to gain root privileges without requiring user interaction. Successful exploitation could allow a local attacker to set specially crafted environment variables for PYTHONPATH or RUBYLIB, that could result in the execution of arbitrary code pointing to the threat actor's environment when needrestart is run.

Google's OSS-Fuzz Discovers Critical Vulnerabilities in Open-Source Projects

+Vulnerability Scanning +AI

- Google's AI-powered [OSS-Fuzz](#) vulnerability scanner has identified 26 security vulnerabilities in open-source projects since its launch. The tool, which added the ability to leverage LLMs in 2023, has improved its ability to detect flaws and streamline debugging processes. Vulnerabilities were found in widely used libraries and applications, including OpenSSL and SQLite.

Critical Vulnerabilities Expose mySCADA Systems to Remote Hacking

+ICS +SCADA +CVE

- The recent vulnerabilities found in [mySCADA's myPRO HMI/SCADA](#) product could allow remote, unauthenticated attackers to gain full control of the affected systems. The flaws, which include OS command injection, improper authentication, and path traversal issues, were patched by mySCADA in November 2024. Exploiting these vulnerabilities could lead to complete system compromise, with several internet-exposed mySCADA systems potentially at risk. However, CISA reports no known exploitation yet.

Data Breaches

UK Prison Layouts Leaked on Dark Web

+UK +Government +Dark Web

- Confidential prison layouts for [UK prison systems](#), which include key security features like cameras and sensors, have been found on dark web sites. The leaked documents, which affect England and Wales, are most likely linked to gangs using drones to deliver illicit shipments or break members out of prison.

Dark Web Breach Puts Global Financial Institutions at Risk

+Financial Services

- A breach targeting [Finastra](#) threatens over 8,100 global banks and financial institutions that work with the company, potentially exposing financial records and transaction details. The breach's scale highlights the severe impact on the financial sector, including fraud, identity theft, and operational risks.

French Hospital Data Breach Exposes 750,000 Patients' Records

+France +Healthcare

- A data breach at a major [French hospital network](#) has exposed the medical records of 750,000 patients, including sensitive health and personal details. The hacker, known as nears, claims to have accessed over 1.5M records across the French hospital system after gaining access to an online patient record system using breached credentials.

Akira Ransomware Gang Unleashes Record Data Leak

+Akira +Ransomware

- The [Akira](#) ransomware group, a ransomware-as-a-service gang, has published a record number of new victims to its darknet leak site in a single day, with 35 published and more on the way. This is their largest dump yet, and may signal their newfound aggressiveness in the cybercrime world.

HDFC Life Investigates Customer Data Breach

+India +Financial Services +Insurance

- [HDFC Life](#), a prominent Indian life insurance company, confirmed a data breach exposing customer information and has initiated an internal investigation. Reports suggest compromised data—7.24 TB, including six million claims records—includes policyholder names, contact details, and sensitive insurance information.

Andrew Tate's "The Real World" Platform Suffers Hack

+Education +Hacktivism

- Hackers targeted Andrew Tate's online education platform [The Real World](#), exposing user data including email addresses and payment details, as well as defacing the site with fake images of Tate. The breach, impacting a wide user base, has drawn attention due to the platform's controversial figurehead and the possible misuse of leaked information.

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.