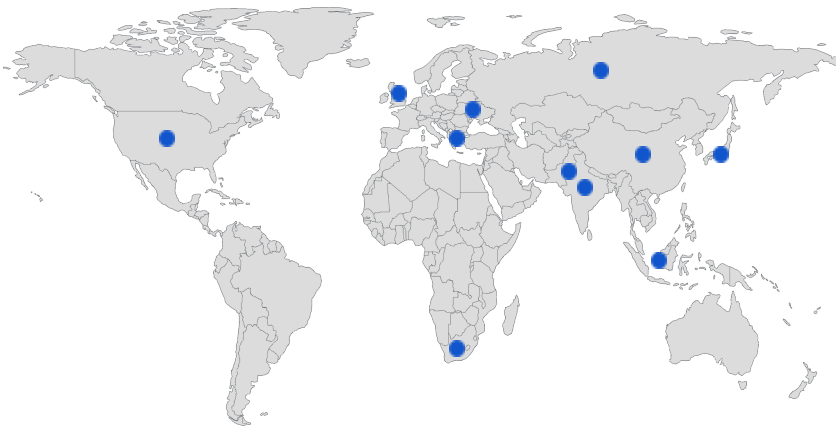


Threat Intel Report: November 4-10, 2024

Countries



Top Tags

Andariel

Ukrainian Cyber Alliance

MirrorFace

APT36

MOVEit

Executive Summary

Actionable Information:

- **Increased sophistication of malware:** Attackers are using more covert and advanced techniques to persist within systems, leveraging zero-day vulnerabilities and more persistent access methods.
- **Targeted exploitation of trusted software:** Exploits are increasingly targeting common platforms, browsers, and developer tools, often bypassing existing security mechanisms.
- **Social engineering and human error:** Many breaches are enabled through phishing, social engineering, and manipulation of user behavior, highlighting the need for stronger awareness training.
- **Geopolitical cyber activity:** State-sponsored cyberattacks are becoming more frequent, targeting high-value geopolitical targets like government entities and critical infrastructure.

Outlook:

As attackers evolve, organizations will face an increasing number of targeted campaigns exploiting both software vulnerabilities and human behavior. The trend toward persistent access methods and decentralized command-and-control systems suggests that traditional security defenses will need to be supplemented with more proactive, behavior-based threat detection systems. Geopolitical cyberattacks are expected to grow, especially in critical infrastructure sectors, requiring enhanced international collaboration and more robust defensive strategies.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 1,011% [CVE-2024-21893](#)

- A server-side request forgery vulnerability in the SAML component of Ivanti Connect Secure, Ivanti Policy Secure, and Ivanti Neurons for ZTA allows an attacker to access certain restricted resources without authentication.

📈 330% [CVE-2023-40044](#)

- In WS_FTP Server, 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.

📈 300% [CVE-2024-8522](#)

- The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query.

Business Logic Attacks Hit Indonesian Government Site

+Indonesia +Government

- An Indonesian government site was targeted by Business Logic attacks this week, reaching 12M requests in one day. Attacks came primarily from bots, primarily using Indonesia-based IPs.

111 GBPS DDoS Attacks Targets Ukrainian Retail Site

+Ukraine +Retail

- A Ukrainian retail site was hit by a network-layer (L3/4) DDoS attack this week, reaching 111 GBPS. The attack, which mainly consisted of UDP floods, lasted 15 minutes.

Recent Cyber Threats

New Version of LightSpy iOS Spyware Targets iPhones with Advanced Features

+LightSpy +Spyware +iOS

- A new version of the iOS spyware [LightSpy](#) has been identified, targeting iPhones with advanced surveillance features and destructive capabilities. Distributed through watering hole attacks, it uses a WebKit exploit to deploy plugins that can capture sensitive data such as Wi-Fi, screenshots, iCloud Keychain, and app information. The spyware also includes modules to delete files, prevent device startup, and generate fake notifications, with signs suggesting a Chinese origin.

JavaScript Drive-By Attacks Exploit Chromium Browsers via Social Engineering

+Drive-By +JavaScript +Social Engineering

- [Chromium](#)-based browsers are able to be exploited via JavaScript drive-by attacks, leveraging social engineering to convince a user to drag and drop malicious files into the browser. Bypassing the Chrome blocklist, which typically blocks read and write access to the /Applications folder on macOS, allows attackers to execute arbitrary code on the victim's machine.

Critical SQL Injection in ZoneMinder Exposes Sensitive Data

+SQLi

- A critical SQL injection vulnerability, [CVE-2024-51482](#), was discovered in ZoneMinder, a popular video surveillance platform. This flaw, rated 9.9 in severity, allows attackers to manipulate SQL queries via an unvalidated parameter, potentially exposing sensitive data or causing system disruption. A proof-of-concept showed that attackers could delete data or initiate denial-of-service attacks. Users are urged to upgrade to version 1.37.65 or later, which addresses the issue by implementing parameterized queries to prevent such exploits.

New Windows Process Injection Technique Allows Malicious Code Execution

+Process Injection

- A new process injection technique exploiting the [Kernel Callback Table](#) within the Process Environment Block (PEB) of Windows systems has been uncovered. This method allows attackers to inject malicious code into legitimate processes, evading detection. By manipulating function pointers in the Kernel Callback Table, adversaries can stealthily redirect execution flows, executing payloads without triggering security alerts. Advanced attackers may even restore the original state after execution to further avoid detection, making this a particularly covert attack method.

CRON#TRAP Phishing Campaign Deploys Backdoored Linux VM for Persistent Access

+CRON#TRAP

- A new phishing campaign, [CRON#TRAP](#), has been discovered that infects Windows systems by deploying a backdoored Linux virtual machine (VM). The attackers send phishing emails disguised as a survey, which, when opened, install a Linux VM using a ZIP archive that contains a backdoor. The VM is loaded with QEMU, a legitimate tool, allowing it to bypass security checks and establish a persistent command-and-control (C2) connection through secure channels. This method enables the attackers to maintain undetected access to corporate networks, even after system reboots.

Malware Campaign Uses Typosquatted npm Packages to Target Ethereum Smart Contracts

+Typosquatting +npm +Crypto

- A malware campaign targeting npm developers uses typosquatted packages to deploy malicious JavaScript, which retrieves binaries from [Ethereum](#) smart contracts for further exploitation. These binaries establish persistence and exfiltrate data from compromised machines. The use of Ethereum smart contracts for command-and-control (C2) infrastructure makes the campaign harder to disrupt, as the decentralized nature of blockchain allows attackers to update server addresses without detection.

North Korean Keylogger Malware Targets U.S. Organizations with Obfuscation

+Andariel +North Korea +US

- A new keylogger attributed to North Korean group [Andariel](#) has been detected targeting U.S. organizations. The malware logs keystrokes and mouse activity, storing the data in an encrypted archive, while using obfuscation techniques like junk code to hinder analysis. Additionally, it installs persistent hooks for keyboard and mouse input, modifies system registry settings, and stores logs in a password-protected file.

GodFather Malware Expands to 500+ Banking and Crypto Apps

+GodFather +Financial Services +Crypto +UK +US +Japan +Greece

- The [GodFather](#) malware has expanded its attack scope to over 500 banking and cryptocurrency apps, using advanced techniques like native code implementation to avoid detection. It distributes through phishing sites and leverages Android's Accessibility service to steal user credentials by loading fake login pages for targeted apps. Initially focused on regions like the UK and US, it now targets users in countries including Japan and Greece. The malware's increasing sophistication and global reach make it a significant threat to mobile security.

Pro-Ukraine Cyberattack Disrupts Parking Services in Russian City of Tver

+Ukraine +Russia +Ukrainian Cyber Alliance

- A suspected pro-Ukraine cyberattack disrupted parking services in the Russian city of Tver, with the [Ukrainian Cyber Alliance](#) claiming responsibility. The group alleged that it took down the city's administrative network, wiping out data and rendering systems like email and parking payment services inoperable. Local authorities initially attributed the issue to a "technical failure" but later confirmed system outages.

MirrorFace Group Targets EU Diplomats Using World Expo Bait

+MirrorFace +Japan +China +APT10

- The China-aligned [MirrorFace](#) hacking group is targeting EU diplomats using the upcoming 2025 World Expo as bait in their spear-phishing campaigns. The attackers sent a malicious ZIP archive masquerading as Expo-related content, which deployed backdoor malware (ANEL and NOOPDOOR) on the victim's system. This marks MirrorFace's first attack against European targets, although their primary focus remains Japan and related events. The group is part of the APT10 umbrella, known for its cyber espionage operations.

APT36 Refines Tools for New Cyber Espionage Attacks Against India

+APT36 +Pakistan +India +ElizaRAT

- [APT36](#), a Pakistan-based cyber espionage group, has significantly refined its toolset to launch new attacks against Indian targets. This refined campaign includes the deployment of an updated version of their "ElizaRAT" malware, a remote access trojan designed for espionage. The group has been targeting high-profile Indian organizations for over a decade, with a focus on information gathering.

Data Breaches

Amazon Confirms Employee Data Breach from MOVEit Attack, 2.8M Records Exposed

+MOVEit +Name3L3ss

- Amazon confirmed a breach of employee data following the [MOVEit](#) attacks in May 2023, where a third-party vendor's systems were compromised. The leaked data, published by the hacker group Nam3L3ss, included over 2.8 million Amazon employee records, such as names, contact details, and building locations, but no sensitive information like Social Security numbers.

Card Skimming Attack Exposes Sensitive Payment Data of 200,000 SelectBlinds Customers

+Card Skimming

- A data breach affecting around 200,000 [SelectBlinds](#) customers was disclosed, stemming from a card skimming attack. The breach involved malicious code on the company's online payment pages, allowing attackers to intercept and steal sensitive payment information.

Alleged Hacker Arrested for Data Breaches at Ticketmaster, AT&T, and More

+Arrest +Hacker

- Authorities have [arrested](#) an alleged hacker behind dozens of data breaches affecting companies including Ticketmaster and AT&T. The hacker is accused of gaining unauthorized access to millions of customers' personal data, which they allegedly used for fraudulent purposes. These incidents have led to lawsuits and class action claims, with affected consumers seeking compensation for identity theft risks and other damages.

Standard Bank Data Breach Exposes Sensitive Client Information through Third-Party Supplier

+South Africa

- [Standard Bank](#) in South Africa experienced a significant data breach, exposing sensitive client data. The breach, caused by a third-party supplier, has led to the leak of customer names, ID numbers, and other private 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.