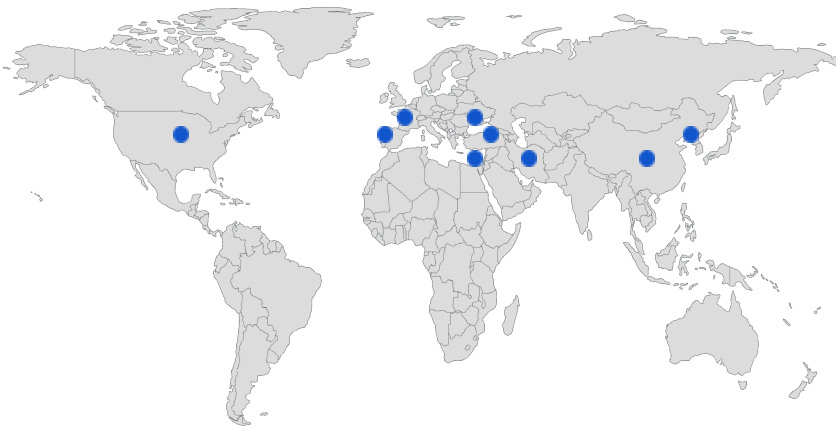


Threat Intel Report: November 11-17, 2024

Countries



Top Tags

Volt Tycoon

WezRat

GuLoader

Strela

TA455

Executive Summary

Actionable Information:

- **State-Sponsored Threats Remain Active:** State-sponsored threat actors from China, Iran, and North Korea remain highly active, employing advanced techniques and targeting various sectors, including telecommunications, aerospace, industrial, and retail.
- **Supply Chain Attacks on the Rise:** Supply chain attacks targeting popular platforms and plugins are on the rise, posing significant risks to a large number of users and organizations.
- **Phishing Campaigns Continue to Prevail:** Phishing campaigns continue to be a prevalent attack vector, with threat actors leveraging social engineering tactics to distribute malware and steal sensitive data.
- **Major Data Breaches Compromise Personal Information:** Major data breaches have compromised personal and financial information of millions of individuals and customers across various industries, including telecommunications, gaming, aerospace, and retail.
- **Resilient Botnets Evade Disruption:** Botnets like Volt Typhoon demonstrate resilience, rapidly rebuilding infrastructure and expanding operations despite disruption attempts.

Outlook:

The cyber threat landscape remains highly dynamic, with threat actors continuously adapting their tactics and expanding their targets. Proactive measures such as implementing robust access controls, data encryption, and incident response plans will be crucial for mitigating risks. Increased international cooperation and information sharing among law enforcement agencies and security researchers will play a vital role in disrupting and deterring these malicious cyber activities. Organizations must prioritize cybersecurity as a strategic imperative, allocating appropriate resources and fostering a culture of security awareness throughout their workforce to address these evolving cyber threats effectively.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 461% [CVE-2023-0669](#)

- A path traversal vulnerability in JetBrains TeamCity

📈 364% CVE-2024-20767

- A file upload vulnerability in some versions of CRMEB

📈 179% CVE-2023-28343

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

Shadow APIs On The Rise

[+Shadow API](#)

- This week, the rate of Shadow APIs—undocumented or forgotten APIs within an organization's environment that operate outside of official monitoring and security measures—rose from 6 to 8%. Although still a small percentage of the total number of APIs, a jump of even 2% shows a massive number of forgotten APIs. These unmaintained APIs create potential vulnerabilities and access points for exploitation.

Recent Cyber Threats

Election-Related Sites Targeted on Election Day

[+US](#) [+Government](#) [+Election](#) [+Business Logic](#)

- On Election Day, [business logic attacks](#) targeting election-related sites were unusually high. These attacks, seen across the US but primarily in Sun Belt swing states, aimed to gather election and voter information, conduct account takeover attacks, and leak data, rising over 100% on November 5.

Massive Credit Card Fraud via Fake E-Commerce Sites

[+eCommerce](#) [+Credit Card Fraud](#)

- Researchers uncovered a [fraud network](#) operating over 4,700 fake e-commerce websites designed to steal credit card information. The websites mimic legitimate online stores to trick customers into entering payment details, which are then harvested by cybercriminals. The scheme facilitates widespread credit card theft from unsuspecting online shoppers.

Critical Vulnerability Affects Really Simple Security WordPress Plugin

[+CVE](#) [+WordPress](#) [+Plugin](#)

- A critical vulnerability has been discovered in the [Really Simple Security](#) plugin for WordPress, a widely used security solution for the popular content management system. The vulnerability could potentially allow remote code execution, enabling threat actors to take control of affected WordPress sites. The vulnerability is scriptable, meaning that it can be turned into a large-scale automated attack, targeting over 4,000,000 vulnerable WordPress sites.

Volt Typhoon Malware Botnet Rebuilds After Disruption

[+Volt Typhoon](#) [+China](#)

- Chinese-sponsored threat actor [Volt Typhoon](#), capable of launching DDoS attacks and distributing other malware payloads, has rebuilt its infrastructure following an FBI attempt to disrupt its operations. Despite law enforcement

actions, the botnet's operators have expanded their network and continue recruiting new victims to spread the KV-Botnet malware.

Iranian Hackers Target Companies with Wezrat Malware

[+Iran](#) [+WezRat](#) [+Malware](#) [+Cotton Sandstorm](#) [+Israel](#)

- Hacking group Cotton Sandstorm, with ties to Iran, has been deploying a new strain of malware called [WezRat](#) to conduct cyberespionage operations against Israeli companies. The malware is designed to exfiltrate sensitive data and maintain persistence on compromised systems.

Critical WordPress Theme Flaw Affects Thousands of Sites

[+CVE](#) [+WordPress](#)

- A critical vulnerability ([CVE-2024-10470](#)) has been discovered in the popular WPLMS Learning Management System WordPress theme, potentially exposing thousands of websites to attacks. The flaw, with a CVSS score of 9.8, could allow remote code execution, enabling threat actors to take control of affected sites.

Europe's Industrial Sector Targeted by Guloader Malware Campaigns

[+Guloader](#) [+Industrial](#)

- Cybercriminals have been conducting spear-phishing campaigns distributing the [Guloader](#) malware, primarily targeting industrial organizations across Europe. The attacks aim to deliver additional payloads, potentially leading to ransomware infections or data theft.

North Korean Hackers Use Flutter Apps to Bypass macOS Security

[+North Korea](#) [+macOS](#)

- Cybersecurity researchers have discovered that North Korean state-sponsored hackers are creating malicious applications using the [Flutter](#) framework to bypass security measures on macOS systems. These malicious Flutter apps are designed to evade macOS's strict code-signing requirements, allowing the deployment of malware on targeted machines.

Strela Malware Spreads Through Malicious Invoice Emails

[+Strela](#) [+Infostealer](#) [+Germany](#) [+Spain](#) [+Ukraine](#) [+Hive0145](#)

- The Strela infostealer malware is being distributed through a widespread phishing campaign from threat actor [Hive0145](#) that uses fake invoice emails as lures. Once installed, the malware can exfiltrate sensitive data, including credentials, from compromised systems, primarily based in Germany, Spain, and Ukraine.

Vulnerabilities in OVR Platform Expose Businesses to Attacks

[+Business](#) [+IoT](#)

- Ten vulnerabilities have been discovered in the [OvrC](#) platform, a popular online service used by businesses for remote IoT management. These vulnerabilities could potentially allow threat actors to access sensitive data, including customer information and financial records stored on the platform.

Iranian Hackers Target Aerospace Job Seekers in "Dream Job" Campaign

[+Iran](#) [+TA455](#) [+Dream Job](#) [+Aerospace](#)

- [TA455](#)—a hacking group linked to Iran—has been conducting a phishing campaign dubbed "Dream Job" to target job seekers and gather intelligence. The campaign involves sending fake job offers and luring victims into downloading malicious documents or providing sensitive information, primarily targeting the aerospace industry.

Data Breaches

T-Mobile Hit by Massive Chinese Cyberattack

[+Telecommunications](#) [+China](#)

- [T-Mobile](#), one of the largest telecommunications companies in the United States, has been the target of a massive cyberattack carried out by state-sponsored hackers from China. The breach reportedly allowed the Chinese actors to access data from T-Mobile's networks and systems, potentially compromising sensitive customer and operational information— although it's currently unknown what may have been taken..

Turkey Fines Twitch Over Data Breach Incident

+Turkey +Gaming

- Turkish authorities have fined [Twitch](#), the popular live streaming platform owned by Amazon, 2 million lira (approximately \$104,000) following a data breach incident. The fine was imposed due to Twitch's failure to implement adequate security measures to protect user data, resulting in the exposure of personal information belonging to Turkish users.

Satellite Company Maxar Confirms Employee Data Breach

+Aerospace

- [Maxar Technologies](#), a major satellite company operating in the aerospace and defense sectors, has confirmed that a cybersecurity incident resulted in unauthorized access to personal data belonging to its employees. The company is currently investigating the breach and taking necessary steps to mitigate potential risks and notify affected individuals.

Massive Data Breach Exposes 57 Million Retail Customer Records

+Retail

- A massive data breach has reportedly exposed the personal information of over [57 million customers](#) from various retail companies, including Hot Topic and Boxed Lunch. The breached data is believed to include sensitive details such as names, addresses, email addresses, and phone numbers, raising significant privacy and security concerns for the affected individuals and businesses.

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.