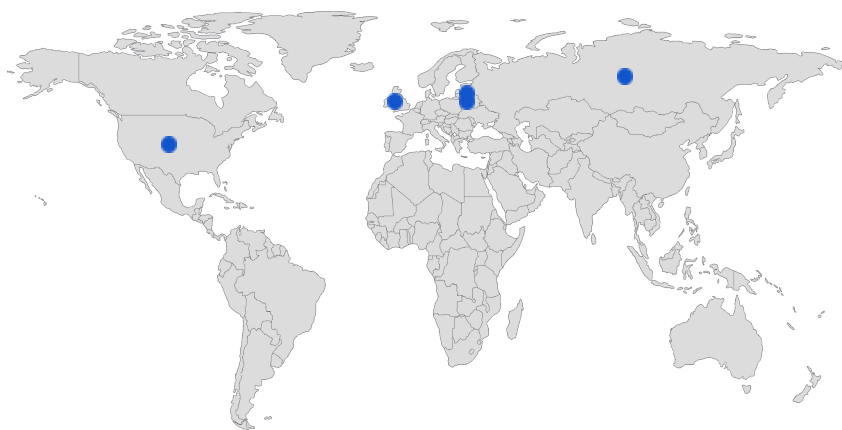


Threat Intel Report: September 2-8, 2024

Countries



Top Tags

HeadMare

GreenCharlie

NPM

DarkCracks

Fog

Executive Summary

Actionable Information:

- **State-Sponsored Attacks on National Infrastructure:** The DDoS attacks targeting Latvian government websites, likely from Russian and Belarusian actors, highlight the ongoing threat of politically motivated cyberattacks. These attacks focus on disrupting national infrastructure and public trust during periods of geopolitical tension.
- **Evolving Phishing and Malvertising Tactics:** Phishing campaigns are becoming more sophisticated, as seen in both the Booking.com and Lowe's incidents. The combination of malvertising and phishing shows how attackers are increasingly blending techniques to steal credentials and sensitive data from both retail employees and consumers.
- **Supply Chain Vulnerabilities:** Multiple incidents, such as the malicious NPM campaign targeting Roblox developers and the fake Palo Alto VPN software, emphasize the growing threat of supply chain attacks. Attackers are leveraging trusted platforms to infiltrate businesses through compromised software, increasing the need for robust vetting and monitoring of third-party software.
- **Increased Ransomware Threats to High-Value Targets:** The new Fog ransomware variant, specifically targeting the financial sector, demonstrates how ransomware actors continue to focus on industries with valuable data. Financial institutions, in particular, are high-risk targets, given the potential for significant financial gain for attackers.

Outlook:

The current cyber threat landscape suggests an escalation in politically motivated attacks on critical infrastructure, alongside a steady increase in sophisticated phishing and supply chain attacks. As ransomware continues to evolve, targeting high-value sectors like finance, organizations must prioritize security measures like zero-trust architectures, regular patch management, and employee education on phishing. Moving forward, businesses must be prepared for a

rise in AI-driven attacks, supply chain compromises, and more persistent ransomware campaigns, all of which pose significant risks to operational integrity and customer trust.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 1702% CVE-2024-4885

- A path traversal vulnerability in JetBrains TeamCity

📈 853% CVE-2024-2879

- A file upload vulnerability in some versions of CRMEB

📈 767% CVE-2024-7593

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

ATO Attacks Target US Business Site

+US +Business +ATO

- A US-based business site was targeted by account takeover this week, with over 1 million brute force attempts coming from automated tools. Attack attempts were widespread, and came from IPs based in over 100 countries, and used compromised credentials for over half of the login attempts.

Uk Entertainment Site Experiences Four-Day Business Logic Attack

+UK +Entertainment +Business Logic

- A UK entertainment site experienced a four-day business logic attack attempt this week, with daily rates averaging 25 million requests. Attacks came from within the UK, as well as Germany, and leveraged automated tools.

Recent Cyber Threats

Latvian Government Sites Hit by DDoS Attacks Amid Tensions

+Latvia +Russia +Belarus

- Several [Latvian](#) government websites were recently targeted in a series of Distributed Denial of Service (DDoS) attacks, with evidence pointing to Russian and Belarusian threat actors. These attacks coincided with political tensions in the region, as hackers aimed to disrupt critical services and public trust. The incident highlights the persistent threat of state-sponsored cyberattacks targeting national infrastructure.

Malvertising Campaign Targets Lowe's Employees with Phishing

+US +Retail +Malvertising

- A sophisticated malvertising campaign has been discovered targeting employees at US home retail chain [Lowe's](#), using fake advertisements to lure victims into clicking malicious links. The attack aimed to steal employee credentials and gain access to sensitive internal systems. This highlights the continued evolution of phishing tactics through malvertising to exploit retail organizations.

Phishing Scam Exploits Booking.com Travelers

+Travel +Phishing

- Travelers using Booking.com have become the target of a widespread [phishing](#) campaign, where attackers impersonate the platform to steal personal and financial information. The phishing emails are designed to resemble

legitimate Booking.com communications, tricking users into providing sensitive data. This scam underscores the need for heightened vigilance among consumers and businesses in the travel sector.

Sextortion Scams Now Include Photos of Victims' Homes

+Sextortion

- A new trend in [sextortion scams](#) has emerged, where attackers are using publicly available information, including photos of victims' homes, to intimidate individuals. The cybercriminals claim to have compromising materials and threaten to release them unless a ransom is paid. This tactic amplifies the psychological pressure on victims, demonstrating how attackers are increasingly leveraging personal data in extortion schemes.

Hacktivist Group HeadMare Leverages WinRAR Exploit

+HeadMare +WinRAR +Russia +Belarus

- The hacktivist group [HeadMare](#) has been exploiting a vulnerability in WinRAR to launch attacks against targets in Russia and Belarus. By using this flaw, the group aims to disrupt operations and expose sensitive information. The incident demonstrates the continued use of well-known software vulnerabilities in hacktivist campaigns and the need for timely patch management.

GreenCharlie Campaign Targets U.S. Political Infrastructure

+GreenCharlie +US +Government

- The [GreenCharlie](#) group has been linked to a sophisticated infrastructure designed to target U.S. political campaigns. Using a combination of spear-phishing and malicious infrastructure, the group aims to influence political processes and gain access to sensitive data. This activity highlights the growing threat of Advanced Persistent Threat (APT) actors in the lead-up to major elections.

Fake Palo Alto GlobalProtect Used to Backdoor Enterprises

+Backdoor +Business

- A malicious campaign has been discovered in which cybercriminals are distributing a fake version of Palo Alto's [GlobalProtect VPN](#) client to compromise enterprise systems in the Middle East. The backdoored software allows attackers to gain persistent access to networks, facilitating data theft and espionage. This incident highlights the dangers of supply chain attacks and the need for organizations to verify the integrity of software downloads.

Roblox Developers Targeted by Malicious NPM Campaign

+Gaming +NPM +Supply Chain

- A new malicious campaign has been identified targeting Roblox developers through the NPM package manager. The attackers inject malicious code into widely used NPM packages, potentially allowing them to steal sensitive data or deploy additional malware. This attack highlights the increasing focus on supply chain attacks in the gaming industry, particularly against developers using popular tools.

SQL Injection Vulnerability Bypasses TSA Security Checks

+US +Transportation +SQLi

- Researchers have discovered a critical [SQL injection vulnerability](#) in the software used at some U.S. airports for TSA security checks. This flaw allows attackers to bypass authentication and potentially manipulate sensitive data, raising significant concerns about the integrity of airport security systems. The vulnerability highlights the importance of securing backend systems in critical infrastructure.

DarkCracks Malware Framework Targets GLPI and WordPress Sites

+DarkCracks +Malware

- [DarkCracks](#), a newly identified stealthy malware framework, is exploiting vulnerabilities in GLPI and WordPress platforms. The malware is designed to evade detection while compromising servers, allowing attackers to install additional payloads or take control of infected systems. This attack highlights the persistent threat of malware frameworks targeting popular web platforms.

Fog Ransomware Focuses on Financial Sector

+Fog +Ransomware +Financial Services

- A new ransomware variant, known as [Fog](#), has been identified targeting the financial sector. This ransomware encrypts critical financial data and demands large sums for decryption. With its focus on financial institutions, Fog represents a growing trend in ransomware attacks seeking to disrupt high-value targets for maximum financial gain.

Apache Fixes Critical Remote Code Execution Vulnerability in OFBiz

+RCE +CVE

- Apache has issued a patch for a critical remote code execution vulnerability in its [OFBiz](#) framework, tracked as CVE-2024-45195. This flaw allows attackers to execute arbitrary commands on affected systems, putting enterprises using OFBiz for business automation at risk of system compromise. Organizations are advised to apply the patch immediately to prevent exploitation of this serious vulnerability.

Data Breaches

Penpie DeFi Protocol Targeted, Millions Stolen in Ethereum

+Crypto +Financial Services

- The decentralized finance protocol [Penpie](#) has suffered a significant cyberattack, resulting in the theft of millions of dollars in Ethereum. The hackers exploited vulnerabilities in the smart contract governing the protocol, allowing them to drain funds from user accounts. This incident underscores the persistent risks associated with DeFi platforms and highlights the need for robust security in decentralized financial systems.

Payment Gateway Data Breach Exposes 17 Million Credit Card Holders

+Financial Services

- A major data breach at a payment gateway provider has exposed the sensitive financial details of [17 million credit card owners](#) worldwide. The stolen data includes credit card numbers, names, and expiration dates, putting millions of customers at risk of fraud and identity theft. This breach highlights the vulnerability of payment systems to cyberattacks and the importance of enhanced security in financial infrastructure.

Nearly 1 Million Medicare Enrollees Affected by Data Breach

+US +Healthcare

- A data breach has compromised the personal information of nearly 1 million [Medicare](#) enrollees. The breach involved unauthorized access to Medicare systems, exposing sensitive data such as Social Security numbers and healthcare records. This incident raises concerns about the security of healthcare information and the potential for identity theft among vulnerable populations.

Disneyland and Disney Cruise Guests' Data Leaked in Major Breach

+US +Entertainment

- A recent data breach at [Disney](#) has exposed the personal information of Disneyland and Disney Cruise Line guests and crew members. The leaked data includes names, addresses, and passport information, potentially affecting millions of individuals. This breach raises questions about data protection practices in the entertainment and hospitality sectors, especially for high-profile companies like Disney.

Avis Car Rental Customers Impacted by Data Breach

+Transportation +Travel

- [Avis](#) car rental has confirmed a data breach that affected a significant number of its customers. The exposed data includes customer names, driver's license numbers, and payment details. This breach highlights the increasing frequency of cyberattacks targeting the transportation sector and the need for stronger security measures to protect customer data.



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.