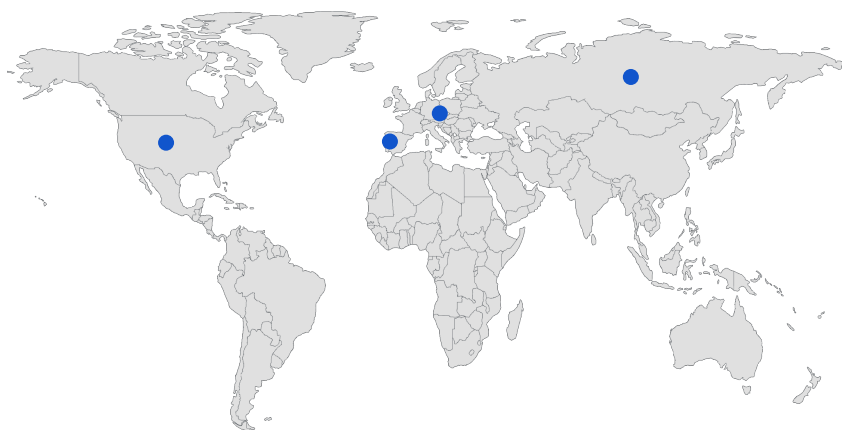


Threat Intel Report: May 5-11, 2025

Countries



Top Tags

Lampion

ClickFix

SmokeLoader

Qilin

LockBit

Executive Summary

Actionable Information:

- **Legacy Systems Still Pose Critical Risk:** Attackers exploited outdated technologies including a zero-click DoS vulnerability in Windows Deployment Services and legacy authentication in Microsoft Entra ID. These flaws allowed for remote denial-of-service and MFA bypass, emphasizing the urgent need to phase out deprecated infrastructure and protocols.
- **Input Validation Gaps Enable RCE and Injection:** Regex and HTML input validation flaws were exploited to achieve remote code execution and arbitrary HTML injection in web applications and Microsoft Bookings. These incidents show that trusting client-side validation remains a significant security pitfall.
- **Malware Delivery Becomes More Sophisticated and Cross-Platform:** Attackers weaponized PDF invoices to deliver Java-based remote access trojans across Windows, Linux, and macOS. At the same time, the Agenda ransomware group added loaders like SmokeLoader and NETXLOADER for stealthier, in-memory execution—bypassing traditional defenses.
- **Ransomware Operations Expand—and Get Exposed:** Qilin disrupted government operations at a Tennessee sheriff's office, while LockBit suffered a rare breach revealing internal negotiation logs. These events highlight both the continued threat ransomware poses and the growing counter-efforts aimed at undermining ransomware groups.
- **Targeted Malware Campaigns Exploit Regional Weaknesses:** Lampion malware actors launched a phishing campaign against Portuguese government and financial organizations using ClickFix-themed lures. These region-specific attacks demonstrate how cybercriminals tailor campaigns to maximize success based on local context.

- **Third-Party Vendors Remain a Soft Underbelly:** Over 430,000 patients were affected by a healthcare data breach at Ascension tied to a third-party vendor. Similarly, a breach at Insight Partners exposed sensitive investor and employee data via social engineering, reinforcing that vendor and partner security is just as important as internal controls.

Outlook:

This week's activity reflects a threat landscape marked by the continued exploitation of legacy technology, input validation oversights, and third-party weaknesses. Threat actors are refining cross-platform malware delivery methods and enhancing ransomware capabilities, while also facing increased scrutiny—evidenced by the leak of LockBit's internal operations. Defenders should prioritize deprecating vulnerable systems, hardening validation logic, tightening vendor access, and investing in behavior-based detection tools to counter stealthy and evasive threats. As the ecosystem becomes more complex and attackers more adaptive, proactive risk management and visibility across the supply chain will be critical.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

↑ 3,120% [CVE-2024-2879](#)

- The LayerSlider plugin for WordPress is vulnerable to SQL Injection via the `ls_get_popup_markup` action in versions 7.9.11 and 7.10.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

↑ 2,165% [CVE-2025-30208](#)

- Vite, a provider of frontend development tooling, has a vulnerability in versions prior to 6.2.3, 6.1.2, 6.0.12, 5.4.15, and 4.5.10. `@fs`` denies access to files outside of Vite serving allow list. Adding `?raw??`` or `?import&raw??`` to the URL bypasses this limitation and returns the file content if it exists. This bypass exists because trailing separators such as ``` are removed in several places, but are not accounted for in query string regexes. The contents of arbitrary files can be returned to the browser.

↑ 472% [CVE-2024-20767](#)

- ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files.

Scalping Attacks Target Release Of Trading Cards

+Gaming +Business Logic

- A gaming retail site was targeted by business logic attacks recently, coinciding with the release of well-hyped preorders for an expansion pack for a popular trading card game. The site was targeted by scraping and scalping attacks attempting to purchase and resell the cards.

Lifestyle Site Targeted By ATO

+ATO +US +Lifestyle

- A US lifestyle site was attacked by account takeover last week, reaching 9 million risky logins in one day. The site allows users to sign up for rewards accounts to earn cash rewards and prizes, and attackers attempted to steal these rewards en masse via brute force.

Recent Cyber Threats

Zero-Click DoS Flaw in Windows Deployment Services Exposes Enterprise Networks

+DoS +Zero-Click

- A critical vulnerability in Microsoft's [Windows Deployment Services](#) (WDS) allows attackers to remotely exhaust server memory by sending malicious UDP packets, leading to system crashes without any user interaction. This "zero-click" flaw poses significant risks to organizations relying on WDS for network-based OS deployments, especially if the service is exposed to the public internet.

Regex Filter Oversight Enables Remote Code Execution

+Regex +RVE

- A security researcher exploited a flaw where a web application's backend trusted frontend [regex validation](#) without revalidating inputs server-side. By sending specially crafted requests using alternative HTTP methods like PUT, the researcher achieved remote code execution, highlighting the dangers of relying solely on client-side input validation.

Lampion Malware Targets Portuguese Organizations via ClickFix Lures

+Lampion +Portugal +ClickFix

- The [Lampion](#) malware group launched a targeted campaign against Portuguese entities, using "ClickFix" lures to distribute their banking information-stealing malware. The campaign primarily affected government, finance, and transportation sectors, emphasizing the group's focus on sensitive financial data.

Agenda Ransomware Group Enhances Arsenal with SmokeLoader and NETXLOADER

+Agenda +SmokeLoader +NETXLOADER

- The [Agenda](#) ransomware group has incorporated SmokeLoader and a new loader named NETXLOADER into their attack toolkit. This enhancement allows them to deploy ransomware more effectively, with NETXLOADER facilitating in-memory execution and evasion of traditional security measures.

Microsoft Bookings Vulnerability Allows Unauthorized Meeting Modifications

+HTML +Injection

- A vulnerability in [Microsoft Bookings](#) permits attackers to inject arbitrary HTML content into meeting invitations and confirmations. Exploiting insufficient input validation, attackers can embed malicious links or scripts, leading to phishing attacks and potential information leakage through manipulated calendar events.

Weaponized PDF Invoices Deliver Cross-Platform Remote Access Trojans

+Trojan +RAT +Phishing

- A sophisticated phishing campaign uses malicious PDF invoices to distribute Java-based [remote access trojans](#) across Windows, Linux, and macOS systems. The attack chain involves social engineering tactics, geolocation filtering, and the use of legitimate services like Dropbox and Ngrok to evade detection, ultimately granting attackers full control over compromised devices.

Data Breaches

Ransomware Disrupts Tennessee Sheriff's Office Operations

+Qilin +US +Government

- The [Qilin](#) ransomware group claimed responsibility for an April 14, 2025, cyberattack on the Hamilton County Sheriff's Office in Chattanooga, Tennessee. The attack disrupted IT systems for over two weeks, affecting services like the website, warrant search, and tip line. While the sheriff's office did not pay the \$300,000 ransom, it incurred \$48,000 in recovery costs. The extent of data compromise remains unclear.

Insight Partners Confirms Breach Exposing Investor Data

+Business

- [Insight Partners](#), a prominent venture capital firm, disclosed a data breach resulting from a sophisticated social engineering attack on January 16, 2025. The breach exposed sensitive information, including fund details, investor data, banking and tax information, and personal details of current and former employees. The firm is notifying affected parties and has involved law enforcement in the investigation.

LockBit Ransomware Gang's Internal Data Leaked

+LockBit +SQL +Russia +Czechia

- The [LockBit](#) ransomware group—associated with Russia—suffered a significant breach when their dark web affiliate panels were defaced, displaying a message "Don't do crime CRIME IS BAD xoxo from Prague." The attackers leaked a MySQL database containing negotiation chats, victim lists, and operational details, exposing the group's internal workings. The identity of the hackers remains unknown.

Microsoft Entra ID Legacy Login Exploited in Cloud Breaches

+MFA

- Attackers exploited a flaw in [Microsoft Entra ID's](#) legacy authentication protocol (BAV2ROPC) to bypass Multi-Factor Authentication (MFA) and gain unauthorized access to admin accounts across various sectors. The campaign, active between March 18 and April 7, 2025, highlights the risks associated with outdated authentication methods in cloud environments.

Ascension Healthcare Data Breach Affects Over 430,000 Patients

+US +Healthcare

- [Ascension](#), a major U.S. healthcare provider, reported that over 430,000 patients were affected by a data breach stemming from a third-party vendor compromise. Exposed data includes personal and health information such as names, contact details, Social Security numbers, medical record numbers, and insurance information. The breach underscores the vulnerabilities in healthcare supply chains.

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.