

Threat Intel Report: April 7-13, 2025

Countries



Top Tags

Ubuntu

NeptuneRAT

JabaROOT

RansomHouse

Satanic

Executive Summary

Actionable Information:

- **Targeting Vulnerabilities in Popular Software:** The release of a PoC for CVE-2025-3155, which targets a flaw in Yelp on Ubuntu systems, highlights the continued exploitation of vulnerabilities in widely-used applications. This week, the theme of targeting software flaws extends to other platforms like VSCode and NPM, emphasizing the need for rigorous patch management and secure development practices.
- **Cryptomining and Remote Access Attacks:** Cryptomining continues to be a significant concern, with malicious VSCode extensions and NPM packages exploiting legitimate tools to infect systems. Similarly, Neptune RAT demonstrates the growing sophistication of remote access malware, which is capable of both stealing sensitive data and causing physical destruction on compromised systems.
- **Cyberattacks on Critical Industries:** Cyberattacks on telecommunications, education, and financial services industries are intensifying. South African telecom provider Cell C and Western Sydney University were both breached, while Australian superannuation funds also faced credential stuffing attacks. These incidents show that no sector is immune from attacks targeting sensitive data, financial information, and personal details.
- **Third-Party and Supply Chain Risks:** The breach of Magento via third-party integrations underscores the growing risks posed by the supply chain. The hacker "Satanic" exploited third-party access to leak CRM data, showing how vulnerable e-commerce platforms are to these types of attacks, which can lead to widespread phishing and impersonation scams.

Outlook:

The overall outlook indicates a continued trend of cybercriminals targeting vulnerabilities in both widely-used platforms and critical infrastructure sectors. As attackers become more sophisticated, leveraging legitimate tools like VSCode extensions and third-party integrations, organizations will need to strengthen their defenses against remote access

malware and ensure that their software supply chains are secure. The rise of targeted attacks on financial services, telecommunications, and education sectors signals a greater need for industry-specific cybersecurity measures. The impact of these attacks will likely prompt increased regulation and scrutiny, particularly in sectors that handle sensitive financial and personal data, such as superannuation funds and social security agencies. Moving forward, organizations must prioritize patch management, multi-factor authentication, and enhanced threat detection to mitigate the growing range of cyber risks.

Threat Activity in Imperva

Top CVE Growth This Week:

Imperva customers are protected against these CVEs.

📈 9,830% [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.

📈 215% [CVE-2024-51568](#)

- CyberPanel (aka Cyber Panel) before 2.3.5 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.

📈 188% [CVE-2025-2748](#)

- The Kentico Xperience application does not fully validate or filter files uploaded via the multiple-file upload functionality, which allows for stored XSS. This issue affects Kentico Xperience through 13.0.178.

US Retail Site Hit By 7M Request ATO Attack

+US +Retail +ATO

- A United States-based retail site was targeted by an account takeover attack last week, reaching 7 million requests in one day. The attack, which came from over 200,000 distinct IPs, utilized brute-force techniques to hammer the site.

1.3M RPS DDoS Attack Targets Mexican Education Site

+Mexico +Education +DDoS

- A Mexican education site was attacked by an application-layer (L7) DDoS attack reaching 1.3 million requests per second (RPS). Coming from 7,500 IPs with an average risk score of 53%, the attack lasted just 9 minutes.

Recent Cyber Threats

Yelp Flaw Exposes SSH Keys on Ubuntu Systems

+CVE +Ubuntu

- A newly released Proof of Concept (PoC) for [CVE-2025-3155](#) targets a flaw in Yelp, the GNOME user help application that comes pre-installed on Ubuntu desktop, potentially exposing SSH keys on Ubuntu systems.

The vulnerability could allow attackers to gain access to systems that are running the affected software, posing a serious risk to organizations that use Ubuntu.

Malicious VSCode Extensions Infect Windows with Cryptominers

[+VSCode](#) [+Crypto](#)

- Malicious extensions in [Visual Studio Code \(VSCode\)](#) are being used to infect Windows systems with cryptominers. These extensions are often disguised as legitimate development tools, and once installed, they mine cryptocurrency on infected machines, consuming system resources and reducing performance.

Neptune RAT Targets Windows with Destructive Capabilities

[+NeptuneRAT](#) [+Windows](#)

- [Neptune RAT](#), a highly destructive malware targeting Windows systems, is being distributed via malicious email attachments and exploit kits. Once executed, it allows remote attackers to control the compromised system, exfiltrate data, and even destroy files, posing a significant risk to enterprises and individual users alike.

Malicious NPM Campaign Targets Crypto Wallets

[+NPM](#) [+Crypto](#)

- A malicious [NPM](#) package campaign is targeting popular crypto wallets like Atomic and Exodus. The campaign masquerades as a PDF-to-Office conversion tool but contains malicious code that replaces the wallet's destination address with one controlled by the attackers, leading to potential crypto theft. The use of legitimate NPM packages for such attacks highlights the growing risks in software supply chains.

Data Breaches

Morocco Investigates Major Data Breach Allegedly by Algerian Hackers

[+Morocco](#) [+Algeria](#) [+JabaROOT](#) [+Government](#) [+Hacktivism](#)

- [Morocco's](#) national social security agency is investigating a cyberattack that resulted in the leak of sensitive personal data reportedly belonging to millions of citizens. Although not officially attributed yet, an Algerian hacktivist group known as JabaROOT has claimed responsibility. The National Social Security Fund of Morocco confirmed that hackers bypassed its security systems and leaked some of the agency's data. The breach is believed to have affected both Moroccan and foreign entities, including European firms operating locally.

South African Telecom Provider Cell C Confirms Data Leak

[+South Africa](#) [+RansomHouse](#)

- [Cell C](#), a South African telecommunications company serving 7.7 million subscribers, confirmed a data breach following a cyberattack in 2024. The hacker group RansomHouse claimed to have obtained 2 TB of the organization's data, which included personal and sensitive information such as full names, contact details, ID numbers, banking information, driver's license numbers, medical records, and passport details. The company is working with international cybersecurity experts and relevant authorities to address the incident.

Western Sydney University Discloses Security Breaches

[+Australia](#) [+Education](#)

- [Western Sydney University](#) announced two security incidents that exposed personal information belonging to members of its community. The first incident involved unauthorized access to demographic, enrollment, and progression information for approximately 10,000 current and former students via the university's single sign-on system between January and February 2025. The second incident concerned the discovery of personal information on a dark web forum, believed to have been posted in November 2024 and accessed between August and October of the same year. Investigations into both incidents are ongoing.

Australian Superannuation Funds Targeted in Cyberattack

[+Australia](#) [+Financial Services](#)

- Several [Australian superannuation funds](#), including AustralianSuper, Australian Retirement Trust, Hostplus, and Rest, were targeted in a coordinated cyberattack. Hackers employed credential stuffing techniques, using previously stolen credentials to gain unauthorized access to members' accounts. AustralianSuper confirmed that four members lost a total of \$500,000, with funds transferred via unauthorized transactions. The breach has prompted increased scrutiny of digital security in the superannuation sector.

Hackers Claim Magento Breach via Third-Party, Leak CRM Data

[+eCommerce](#) [+CRM](#) [+Satanic](#)

- A hacker using the alias "Satanic" claimed responsibility for a data breach involving [Magento](#), an open-source e-commerce platform. The breach, which occurred on April 9, 2025, was facilitated through a third-party integration, leading to the theft of CRM data from over 700,000 users. The leaked data, published on Breach Forums, includes emails, phone numbers, and company information from major firms, posing risks for phishing and B2B impersonation scams.

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.