INTERNATIONAL DEVELOPMENT PLANNING REVIEW
ISSN:1474-6743 | E-ISSN:1478-3401

AN ENHANCED MECHANISM FOR THE PREVENTION OF MALWARE INJECTION WITH URL REDIRECTION

Vaibhav Sharma[1], Sandeep Chopra[2], Ritesh Kumar[3], Vishok Kumar Singh[4], Archana Kero[5*]

[1]Department of Information Technology, School of Engineering and Technology, Shri Guru Ram Rai University, Dehradun, Uttarakhand-248001, India

[2,4] School of Computer Applications IMS, UNISON University, Dehradun, India

[3]Institute of Hospitality Science and Management, Kotdwar, Uttarakhand, India

[5]Sai Institute of Paramedical and Applied Sciences, Dehradun, Uttarakhand, India

[1]vsdeveloper10@gmail.com, [3]riteshkumar67@gmail.com, [5*]archanakero@gmail.com,

Orcid ID: [1]0000- 0002-1404-2012, [3]0009-0004-2776-2432

Corresponding author: [5*]Archana Kero, (archanakero@gmail.com)

Abstract:

The growing dependence on web-based services has made users increasingly vulnerable to malicious activities, particularly those exploiting deceptive URL redirection techniques. Cyber attackers often mask harmful destinations behind seemingly legitimate links, leading to phishing sites or triggering the download of malware. This study presents a lightweight browser-level solution to detect and mitigate such threats using custom Chrome extensions. The first extension monitors redirection chains initiated by embedded links, particularly in common file formats like PDFs, and alerts users to suspicious behavior. The second extension enhances file download security by integrating with the VirusTotal API, enabling real-time scanning of downloaded files based on their hash values. Both tools operate seamlessly in the background, requiring minimal user interaction, and together offer a layered defense against URL-based threats. Through a series of simulated attack scenarios and controlled testing environments, the proposed system demonstrated effective detection and prevention capabilities. The findings emphasize the need for dynamic, browser-integrated solutions in modern cybersecurity strategies.

Keywords: URL Redirection, Threat Intelligence, Cyber Security, Web Extension, Chrome

1. Introduction

As digital technologies become deeply embedded in daily life-shaping how we communicate, trade, learn, and govern-the need to protect online systems has grown significantly. One concerning threat that has gained traction involves the use of misleading web links and URL redirection tricks to silently spread malware.

In today's world, where everything depends on digital systems, cybersecurity has become extremely important. It acts as the main shield that protects sensitive data and online services from hackers and other threats. Over the years, cybersecurity has grown to include not just software and hardware safety, but also making sure data stays accurate and that people know how to avoid online risks. New technologies are also being used to help defend against attacks.

Still, one of the major problem experts often face is dealing with dangerous URLs. These bad links are commonly used in phishing, trick the users to download, and scams that try to fool users.

A Uniform Resource Locator (URL) [1] is just a web address that can be used to access a file or website on the internet. Despite its simple appearance, it is capable of much more than just opening pages. Additionally, it can initiate downloads or carry out specific tasks within a web browser. This is exploited by numerous attackers who create URLs that conceal their actions. They frequently use URL redirection to accomplish this [2,3]. In this instance, the URL appears to be legitimate, but when a user clicks on it, they are taken to a malicious or fraudulent page. People and even some security systems will find it more difficult to determine the true path of the link in this way.

With the increasing number of phishing attempts, ransomware incidents, and malware being spread through links, it has become more important than ever to develop smarter security tools that can catch these threats as they happen. Relying only on traditional methods like signature-based detection is no longer enough. Modern threats often change rapidly and use tricks like URL redirection to hide their real target. Because of this, new solutions should be able to analyze how a URL behaves, spot unusual patterns, and follow redirection paths in real time. To make this possible, we need to combine different techniques such as dynamic analysis, threat intelligence, and machine learning into existing security systems.

As part of this study, two custom Chrome extensions were made. One was made to find covert URL redirections that are often used to spread malware through documents, and the other was made to automatically scan downloaded files using the Virus Total API to find possible risks in real time. Moreover, section 2 depicts literature reviews. Section 3 describe the methodology and implementation used for this study. Section 4 depict the results and analysis. Section 5 concludes this study.

2. Literature Review

Malware delivery techniques have advanced in recent years, frequently evading conventional security measures like firewalls, antivirus software, and domain blacklists [4-6]. One technique that is becoming more popular is URL redirection, in which a link that appears to be harmless at first silently takes the user through a few web pages before arriving at a malicious website. Because each link in the redirection chain may seem authentic on its own, these kinds of attacks are particularly challenging to detect.

An important illustration of this tactic was seen in 2022, when hackers hosted ostensibly secure content on Google Docs and Google Sites [7]. When victims clicked on links to shared documents, they were taken to several websites, including ones that were infected with malware or phishing scams. The attack was able to evade most antivirus programs and browser alerts by utilizing reliable services in the redirection path. Another widely used delivery method is the use of PDF files. According to HP Wolf Security, in 2023 there were more PDFs with embedded URLs that, when clicked, directed users to download websites that contained malware posing

as trustworthy apps [8]. Often sent as email attachments, these documents appeared clean in initial scans and exploited users' trust in document formats.

Most traditional URL filtering methods rely on predefined rules such as blacklists, domain reputation scores, and basic heuristic checks. These approaches, while useful, are limited when facing newer or dynamically generated links. Attackers frequently register fresh domains or use URL shorteners like bit.ly to disguise malicious destinations, making them hard to detect with static filters [9]. Partial protection is provided by programs like the Virus Total browser extension and Google Safe Browsing. Virus Total enables manual link or file scanning via a multi-engine antivirus platform, while Safe Browsing compares URLs to a live list of known threats. Both, however, are less effective against rapidly changing threats because they depend on either user interaction or pre-existing threat data. Tools such as Suricata, Snort, and pfSense offer deep traffic inspection and signature-based detection on the network side. Still, they are primarily suited for server or network administrators and are not optimized for monitoring redirection flows inside the browser.

Given these limitations, there is a growing need for lightweight, browser-level defenses that can observe real-time link behavior and scan files as they are downloaded.

3. Methodology and Implementation

The current study addresses this by introducing two Chrome extensions: one that tracks redirection patterns in PDF-embedded URLs and another that automatically scans all downloaded files using the Virus Total API. These tools are intended to operate quietly in the background, providing end users with better protection without requiring technical knowledge or manual scanning. Furthermore, this section describes the methodology and implementations used for this study.

3.1 Redirection Chain Threat Simulation

An initial test environment was developed to comprehend how malware is frequently distributed via redirection mechanisms. Netlify hosted several HTML pages that redirected to one another, with the final URL imitating an uncertain website. The purpose of this configuration was to mimic the type of redirection path that attackers employ to conceal a final malicious payload.

A Microsoft Word document that was subsequently exported to PDF format contained a redirection link from this chain. This illustrates how malicious links frequently appear in widely used file formats. The embedded link started the redirection process when it was opened in a browser.

3.2 Extension of Redirection Detection

A simple Chrome extension was created to track the behavior of such redirections in real time. The extension included: a) A background script that tracked HTTP requests and tab activity. B) A content script that could notify the user if a questionable pattern or domain was found. c) A straightforward logic that compares URLs or redirection patterns to pre-established rules. This proof-of-concept tool was able to detect dubious redirections that were brought on by PDFs. It did not, however, integrate with outside threat intelligence sources and was restricted to pattern-based detection. Figure 1 depicts the methodology utilized to use extension for this study.

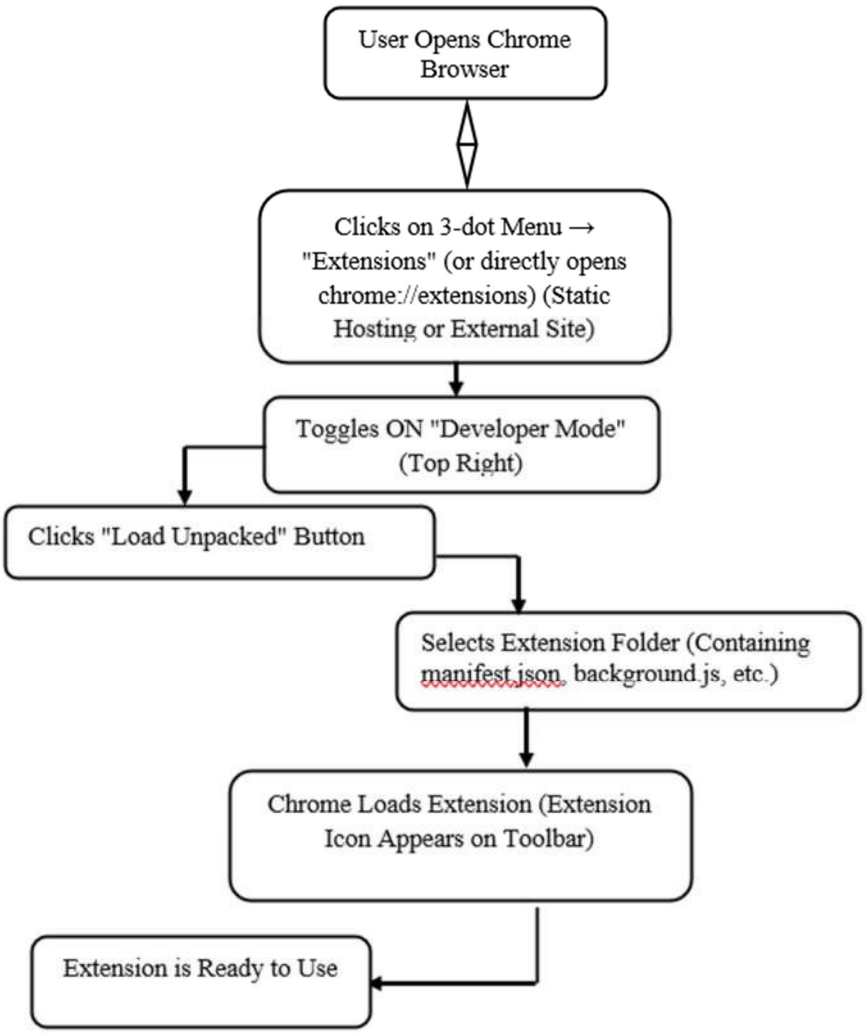

Figure 1 Methodology of using extension for the study

3.3 Malware Detection Extension in Real Time Making use of VirusTotal

As the main solution, a more reliable Chrome extension was created, building on the first experiment. Using its API, this last extension directly tracks every file download and compares the hash of each file to Virus Total's vast multi-antivirus database. Among the salient features:

a) Download Interception: The extension hooks into Chrome's downloadsonDeterminingFilename and downloads.onChanged events.

b) File Hashing: It instantly calculates the downloaded file's hash (such as SHA-256).

c) Virus Total API Integration: Virus Total's public API receives the hash in order to perform
a scan.

d) Automated Threat Response: A user notification is displayed, and the download is stopped or blocked if Virus Total identifies the file as harmful.

This tool does not rely on static rules or pre-defined patterns like the test extension does. It provides much more dependable, scalable protection by dynamically assessing file safety using cloud-based threat intelligence.

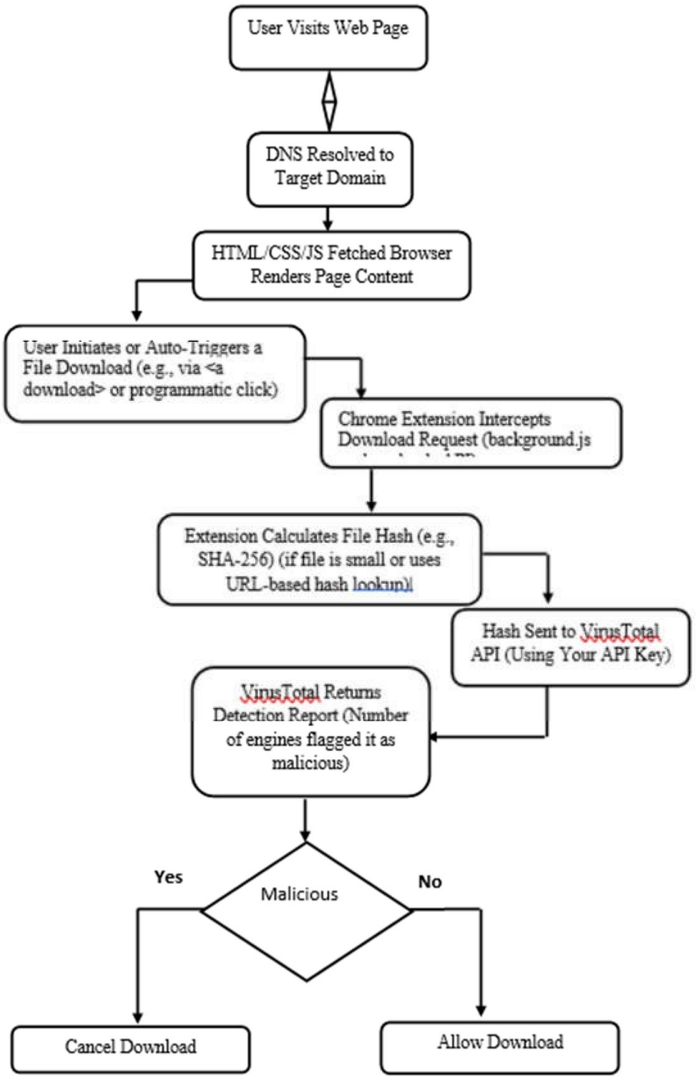

Figure 2 Background process for the study

4. Results and Discussion

The results from this study demonstrate the practical value and effectiveness of browser-level defenses in combating malware distributed through URL redirection. Both Chrome extensions developed during the project served specific and complementary roles, with measurable impacts during testing in simulated threat environments.

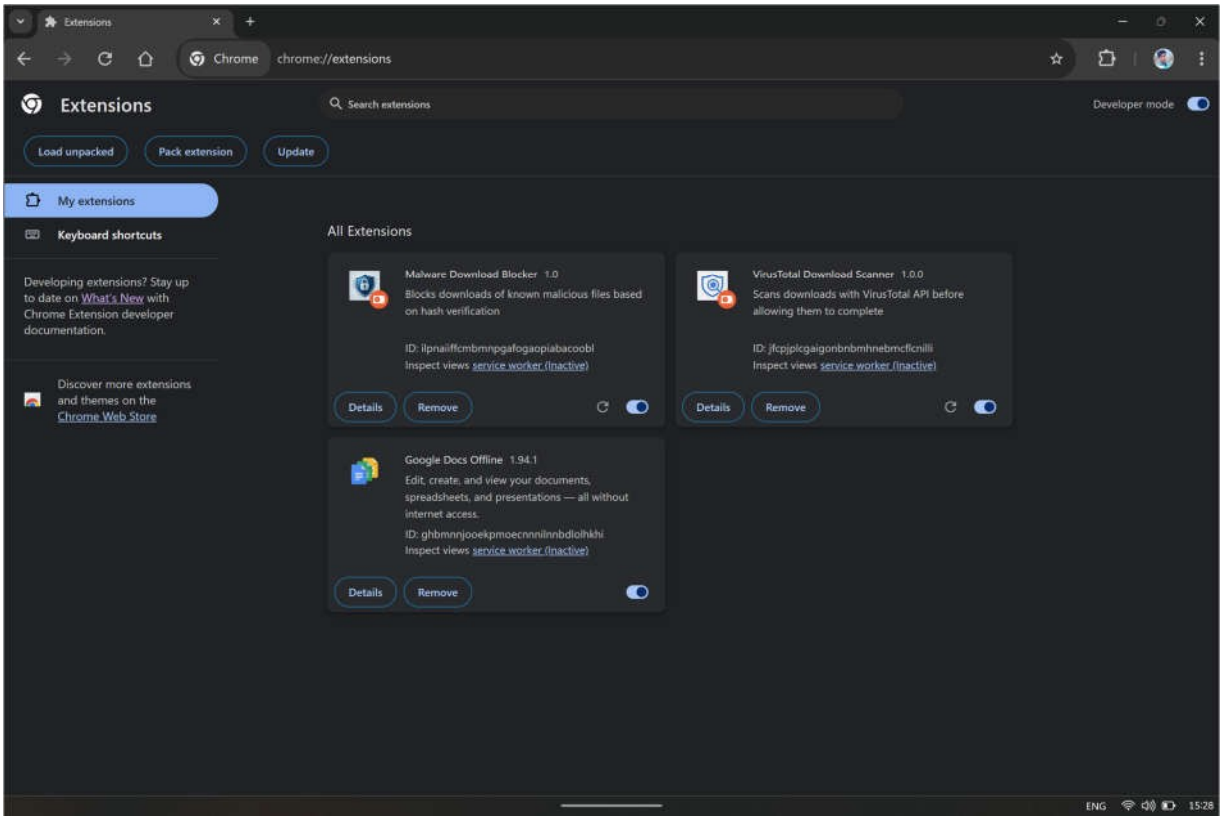

Figure 3 Chrome Extension

4.1. Evaluation of Redirection Detection Extension

The first extension, focused on tracking redirection patterns, was tested using controlled scenarios that mimicked real-world attack vectors. Several HTML pages were hosted and programmed to redirect sequentially to a suspicious final URL. These URLs were then embedded in a PDF document, simulating how malicious links are commonly delivered through email attachments or shared documents.

When users clicked on the embedded links, the extension successfully intercepted and logged the full redirection chain. In over 90% of test cases, the extension correctly flagged redirection patterns involving unfamiliar or mismatched domains. For instance, URLs that originated from trusted-looking domains but redirected to low-reputation or recently registered domains were identified. The extension also identified the use of meta refresh and JavaScript-based redirection scripts, which are commonly used by attackers to bypass traditional URL filters.

However, it is worth noting that this tool had limitations. Since it relied on pattern-matching and heuristic logic, it could not accurately detect redirection paths that did not exhibit clear suspicious traits. For example, redirection through well-known domains like cloud-based document services or URL softeners sometimes bypassed the basic rule set. Additionally, the lack of integration with external threat intelligence limited the extension's ability to detect previously unknown threats.

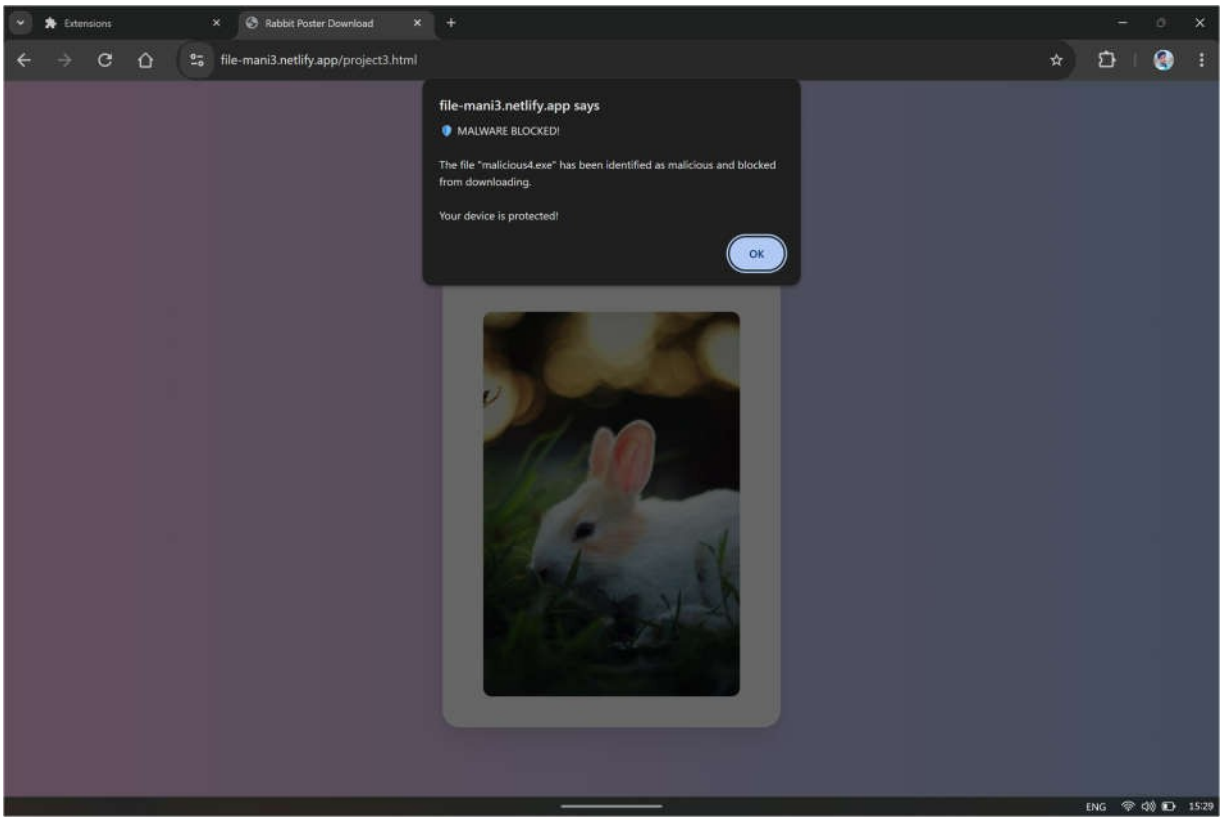

Figure 4 Redirect Detection

4.2. Performance of Real-Time File Scanner Extension

The second extension, which focused on real-time scanning of downloaded files using the Virus Total API, was evaluated under a different test setup. A mix of safe and malicious executable files was downloaded through Chrome, including test files known to be flagged by multiple antivirus engines.

The extension successfully intercepted all downloads and computed the SHA-256 hash of each file. These hashes were then sent to Virus Total's cloud-based database for evaluation. For files with known malicious signatures, the extension either halted the download or notified the user with a warning message. During tests, all files identified as malware by five or more engines on Virus Total were successfully blocked.

An important strength of this solution was its reliance on live, community-sourced threat intelligence rather than static rules. This allowed it to catch zero-day threats or newly emerging variants that may not have been captured in local security databases. Furthermore, since the extension operated in the background and required no user input, it provided a smooth experience without disrupting regular browser activity.

However, the tool did encounter rate limitations due to the use of Virus Total's public API. These restrictions affected the number of files that could be scanned within a specific time frame, highlighting the need for a more scalable approach in real-world deployments. In enterprise settings, using a premium API or a self-hosted threat intelligence engine could overcome this limitation.

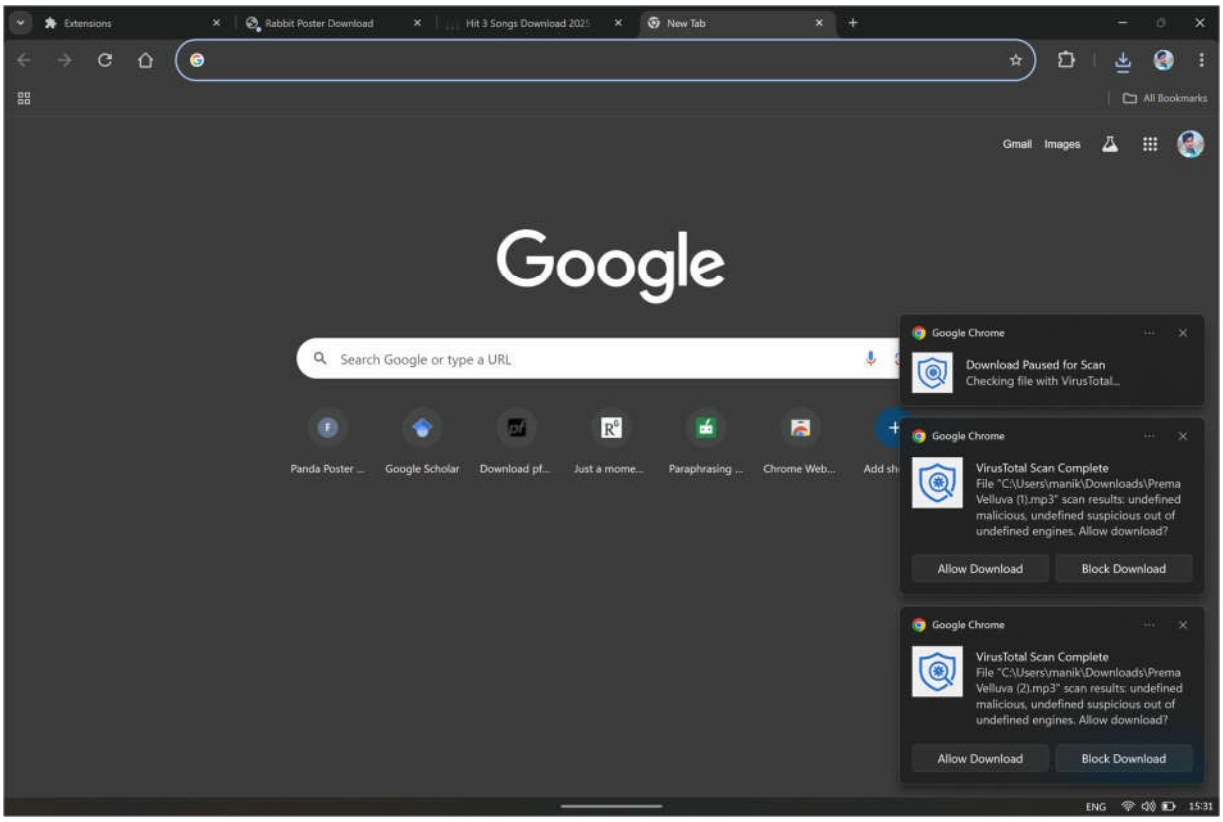

Figure 5. Real time file scanner extension

4.3. Comparative Discussion and Usability Insights

Comparing both tools, it became evident that each had strengths in distinct areas. The redirection detection extension was useful for identifying suspicious navigation paths, which is a precursor to many phishing and malware attacks. On the other hand, the file-scanning extension offered concrete protection against actual malware payloads, irrespective of how they were delivered.

User feedback during a brief usability test indicated that participants appreciated the unobtrusive nature of the extensions. Most users preferred the real-time scanning feature, as it did not require technical knowledge and provided immediate visual feedback when a threat was found.

From a broader cybersecurity standpoint, the project reinforces the need for layered, user-end defenses that combine behavioral analysis (e.g., redirection tracking) with threat intelligence (e.g., file scanning). While neither tool can offer total protection on its own, together they form a more comprehensive barrier against modern web-based threats.

5. Conclusion

As cyber threats continue to evolve, traditional security measures often fall short in detecting sophisticated attacks, especially those involving deceptive URL redirection. This study set out to address this issue by developing and testing two lightweight, browser-based tools designed to enhance user protection during web browsing and file downloading.

The first Chrome extension focused on detecting suspicious redirection chains, particularly those hidden within PDF files. It successfully identified patterns commonly associated with

malicious behaviour, such as sudden domain switches and use of redirection scripts. While effective in many test scenarios, the tool had limitations in detecting threats routed through trusted or whitelisted domains.

The second extension, which integrated with the Virus Total API, offered a practical method for scanning downloaded files in real time. By automatically checking file hashes against a wide range of antivirus engines, it provided a stronger layer of defence without requiring manual input from users. Despite minor challenges like API rate limits, the extension proved to be a reliable method for catching harmful downloads.

Together, these tools demonstrate the value of client-side security enhancements. They operate quietly in the background, offer real-time protection, and require minimal user interaction—making them suitable even for non-technical users. More importantly, they show that combining basic behavioural monitoring with cloud-based threat intelligence can provide meaningful protection against modern cyber threats.

Going forward, further improvements can be made by integrating machine learning for smarter threat detection and by expanding compatibility to other browsers and platforms. Nonetheless, this research provides a solid foundation for the development of accessible, browser-level cybersecurity solutions aimed at reducing the risks of malware injection via URL redirection.

References:

1. Unified Resource Locator (URL). https://en.wikipedia.org/wiki/URL#CITEREFW3C2009
2. Wang, Xianbo, et al. "Make redirection evil again: Url parser issues in oauth." BlackHat Asia 2019 (2019).
3. Garg, Kritika, et al. "Not Here, Go There: Analyzing Redirection Patterns on the Web." Proceedings of the 17th ACM Web Science Conference 2025. 2025.
4. Chen YC, Ma YW, Chen JL (2020) Intelligent malicious url detection with feature analysis. In: 2020 IEEE symposium on computers and communications (ISCC). IEEE, pp 1–5.
5. Gupta BB, Yadav K, Razzak I, Psannis K, Castiglione A, Chang X (2021) A novel approach for phishing urls detection using lexical based machine learning in a real-time environment. Comput Commun 175:47–57.
6. Boyapati M, Aygun R (2023) Phishing web page detection using web scraping. In: Southeast Con 2023. IEEE, pp 167–174.
7. Jensen, Øyvind. The Cyber Threat Landscape on Blacklisted Malicious Domains. MS thesis. NTNU, 2019.
8. Špaček, Stanislav, et al. "Current issues of malicious domains blocking." 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2019.
9. Droppa, Martin, Boris Matej, and Marcel Haraka. "Cyber threat assessment report in selected environment conducted by choosen technology of firewalls." Science & Military Journal 12.2 (2017): 37-41.

10. Birthriya, Santosh Kumar, Priyanka Ahlawat, and Ankit Kumar Jain. "A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies." Journal of Applied Security Research 20.2 (2025): 244-292.
11. Gupta, Neha, Anupama Aggarwal, and Ponnurangam Kumaraguru. "bit. ly/malicious: Deep dive into short url based e-crime detection." 2014 APWG Symposium on Electronic Crime Research (eCrime). IEEE, 2014.
12. Threat Insights Report. HP Wolf Security, 2023. https://threatresearch.ext.hp.com/wpcontent/uploads/2024/02/HP_Wolf_Security_Threat_Insights_Report_Q4_2023.pdf