Accessibility, Security, and Privacy: A Comparative Analysis of NVDA and Chrome Addon Ecosystems

Kaushik Dhamodaran

Submitted for the Degree of Master of Science in

Information Security

Department of Computer Science
Royal Holloway University of London
Egham, Surrey TW20 0EX, UK

October 1, 2025

Contents

1 Executive Summary **5**

2 Introduction **6**
2.1 Screen Reader software history 6
2.2 NVDA and Google Chrome Accessibility 7
2.3 Research Questions and Objectives 9

3 Background and Related Work **10**
3.1 Related Work 10

4 Accessibility and Privacy Concerns **11**
4.1 NVDA 11
4.1.1 Installation 11
4.1.2 CodeQL 13
4.1.3 Addon review process 14
4.2 Google Chrome 17
4.2.1 Installation 17
4.2.2 Addon review process 20
4.2.3 Manifest V3 23
4.2.4 VirusTotal 24

5 Experimentation **25**
5.1 Experimental Setup 25
5.1.1 NVDA addon setup 25
5.1.2 Chrome addon setup 27
5.2 Methodology 29
5.2.1 NVDA addon testing 29
5.2.2 Chrome addon testing 30

6 Results **31**
6.1 Addon compatibility 31
6.1.1 NVDA Telegram Archive 31
6.1.2 NVDA Addon Store 33
6.1.3 Chrome Web Store 34
6.2 Network Capture Results 38
6.2.1 NVDA Telegram Archive 38
6.2.2 NVDA Addon Store 38
6.2.3 Chrome Web Store 39
6.3 Other Security and Privacy Issues 40

6.3.1 NVDA Telegram Archive 40
6.3.2 NVDA Addon Store 41
6.3.3 Chrome Web Store 41
6.4 Embedded Virus Scanning 42
6.4.1 NVDA Telegram Archive 42
6.4.2 NVDA Addon Store 44
6.4.3 Chrome Web Store 47

7 Limitations and Future Work **51**

8 Conclusion **52**

9 Appendix **57**
9.1 NVDA Telegram addon results 57
9.2 NVDA Addon Store results 61
9.3 Chrome Web Store results 66
9.4 Wireshark capture data 71

List of Figures

1 Top search result in Google (2024-06-10) 12
2 Other search results (2024-06-10) 13
3 Top Google Chrome download results from Bing (2024-08-10) 18
4 Google Chrome download results continued (2024-08-10) . . . 19
5 Stages of an addon lifecycle, by Google [1] 20
6 Violation process, by Google [1] 22
7 Top search result in Google (2024-06-10) 26
8 Search results in Google continued (2024-06-10) 26
9 Incompatible addon message in NVDA 27
10 Top search results in Google (2024-07-25) 28
11 Top accessibility addons on the Chrome Web Store (2024-07-25) 29
12 Chrome developer tools Network capture of bbc.co.uk (2024-07-25) 31
13 Pie chart showing the percentages of working addons tested from Telegram 32
14 Pie chart showing the percentages of working addons tested from NVDA's addon store 33
15 Percentages of working addons on Google Chrome 35
16 Screenshot of the Dark Reader addon on the Chrome Web Store 36
17 Screenshot of the Access8Math addon on the NVDA Addon Store 37
18 Screenshot of the JSON file containing server locations 39
19 Privacy Policy for CroxyProxy 40
20 NVDA error message failing to open winGlulxe 40
21 VirusTotal first submission 42
22 VirusTotal Script.Ks.Malware.10590 malware in WLmail . . . 43
23 Percentages of URLs flagged by VirusTotal 44
24 VirusTotal Anity-AVL malware detected 45
25 VirusTotal ArcSight Threat Intelligence malware detected . . 45
26 Pie chart showing percentages of addons that have been flagged by VirusTotal 47
27 VirusTotal screenshot of malware signatures found in the RoBox addon 50
28 More information on Google as a security vendor 50

List of Tables

1 A table showing which developers have contributed addons . 16
2 A table showing addons and their related malware 49

1 Executive Summary

There is a very small but important group of people that rely on accessibility aids when using technology in their day-to-day lives. However due to these accessibility technologies only impacting the lives of few rather than many, it is an area that does not see a lot of research, especially in the security and privacy area. People use these technologies to help them with important stuff like online banking, so it is vital that such technologies at least follow baseline standards for privacy and security when a more vulnerable part of the population relies on such a technology for such important needs.

The purpose of this paper is to look at two different accessibility addon ecosystems and compare them and see what aspects of each ecosystem work and which don't and how having a smaller, community driven addon ecosystem such as the one cultivated by NVDA stacks up to a more corporate and huge addon ecosystem works with Chrome addons.

After compiling a list of addons to test from each ecosystem, 50 addons obtained via a Telegram Archive for NVDA, 50 addons obtained from NVDA's official addon store, and 50 addons from the Chrome Web Store, each addon was tested against network analysis using Wireshark and Chrome Developer Tools and malware signature analysis using VirusTotal to check for any privacy and security issues.

While the network analysis only showed all the addons working as intended and any network activity from these addons being specified by the developer, it did not provide any conclusive proof that there is no malicious network activity embedded in the addons tested though malware scans using VirusTotal showed suspicious activity for both ecosystems. While the flags for NVDA's addons may be more likely to be false positives as manual code analysis, only being flagged by one vendor and internet research supporting the claim that they are false positives, it seems unlikely that any of the NVDA addons tested may be malicious. However, the Chrome addons were flagged by more than one vendor, increasing the possibility that there may be malicious code in an addon, and the fact that most addons are closed-source make it impossible to fully verify if an addon is trustworthy or not without being able to see the code.

A key finding in this report is that comparatively, Chrome addons, despite being subject to a more rigorous security process, seemingly have more security and privacy issues than NVDA addons, which could be due to it being more community driven and there being trust amongst developers, organisations and users.

2 Introduction

Technology sees use from people with disabilities, from people to visual impairments to people with motor impairments. In order to navigate computer and web interfaces, people with impairments rely on software such as screen-readers or addons for web browsers to help them read, write and navigate content. A general purpose definition of screen readers is that they are software that typically reads out to users using an automated voice the content that would be displayed on a computer screen to help assist people with sight-related difficulties to navigate and understand the content being displayed on a computer screen [2]. Modern screen readers typically work by reading out text content, but where it encounters images or UI elements (such as text boxes), it will read them out based on (sometimes invisible) alt-text that is assigned to them to let the user know the content of an image or of there is a graphical element that they can interact with [2]. Screen reader capabilities can also be augmented with plugins/addons which are "small pieces of code that could extend screen readers' builtin functionalities or could repair application specific accessibility issues" [3].

2.1 Screen Reader software history

When it comes to assistive technology in general, the origins of screen reader software can be traced back to Deane Blazie who created the Talking Terminal while working at Maryland Computers and is also one of the few sighted people involved in the initial creation of assistive technology. The Talking Terminal was a Hewlett Packard 2621 computer terminal which could read back words typed into it, letter-by-letter and was the first of its kind [4]. One of the most prominent testers of this new technology was a man called Ted Henter who was someone who had lost his sight and would offer suggestions to Blazie and improved the technology where it could read word-by-word instead of letter-by-letter. These early implementations of assistive technologies were slow top read things out but allowed Henter to code on the Terminal without external assistance [4].

As assistive technologies evolved alongside operating systems, both increasing in complexity, and Henter who tested early applications of the Talking Terminal teamed up with Bill Joyce to create JAWS (Job Access With Speech) which not only worked with operating systems such as DOS, but had braille support as well. In addition to being able to read out text, additional features such as a dual cursor was also implemented. Henter describes it as one cursor being the PC cursor and the other "can roam around any-

where on the screen and go places where the PC cursor can not go. Just like a person's eyes can move around on the screen" [5]. This can be likened to modern day computers where there is a text cursor and a mouse cursor that can go around anywhere. While advances in assistive technologies by directing reading text off a terminal made major advances during this time, operating systems were starting to shift to be more visual and with the release of Windows, JAWS was no longer something that people who required assistive technologies to do their job could use anymore as graphical UI was not something that JAWS had the capability of doing at this point.

Up to this point, JAWS would read out text by direct reading it from the computer memory, but the introduction of graphical UI made it difficult to use that same method to read off what was on the screen, so JAWS was remade to work with Windows with a new model called an off-screen model [5] which would take into account graphical elements and is more reminiscent of modern screen reader software.

JAWS is still a popular screen reader in the present day, with the most recent WebAIM survey placing it as the second most popular screen reader in usage with 60.5% of respondents claiming it to be their most commonly used screen reader, slightly behind NVDA with 65.6% of respondents claiming it to be be their most commonly used screen reader [6].

2.2 NVDA and Google Chrome Accessibility

NVDA is a free and open-source screen reader software that was initially developed by Michael Curran and James Teh as a response to the licensing costs of JAWS which "can cost thousands of dollars to purchase and more money to upgrade" [7]. NVDA has overtaken JAWS in recent years in terms of popularity, possibly due to it being free and also has the highest satisfaction rate among its users with a WebAIM survey showing that 97.6% of respondents were very or somewhat satisfied with NVDA as their primary screen reader [6]. However, due to the cost of JAWS it is likely that a large amount of respondents have not been able to use and compare against it which may skew the results positively.

NVDA is coded in Python, along with any addons developed for it and is only available for Windows. It introduced support for eSpeak and Windows OneCore speech synthesizer in order to output the voice for their reader [8]. This allows NVDA to support multiple languages as well as allowing users to use 3rd party voices if they choose and allows for user flexibility, which is a big leap in customisation compared to the early days of JAWS. Due to many using VDA for work, which would include web browsing, NVDA

has official support for work-based applications such as Microsoft Word and the Microsoft Office suite of programs, Email clients such as Outlook and Thunderbird as well as Firefox and Chrome support [8]. This marks a stage in screen reader software with official support for many work-based applications as opposed to a more generic screen reader that works the same way no matter what application is being used. However, accessibility barriers still remain when it comes to web browsing, and while NVDA supports WAI-ARIA [8], which is a specification published by W3C on how to make websites more accessible. there remain a host of web accessibility issues that frustrate users of screen readers as many websites are not built with accessibility in mind [2].

NVDA being open-source means that the code is viewable by anyone and the community can contribute to the code and as such has developed an addon ecosystem where individuals can develop additional addons that integrate with NVDA and can add extra functionality to help improve accessibility for individuals. They can range from checking a user's BMI to tweaking how NVDA reads out LATEX code [9]. These addons are developed in Python, same as NVDA and can have access the same APIs that NVDA uses, such as Microsoft Active Directory to help read out what is being displayed on the screen [8]. However APIs can also be susceptible to attacks add a section about UI Automation, Microsoft Active Accessibility, IAccessible2 and Java Access Bridge attacks

The majority of people that use web browsers nowadays use Google Chrome, owned by Alphabet, With up to 64.72% of internet desktop users using Chrome [10]. This number jumps even higher (80.99%) when considering the fact that browsers such as Microsoft Edge and Opera are built off of Chromium which is the rendering engine that powers chrome and forms the basis of these browsers with many third party browsers using it as its core due to chromium being open-source and backed by Google. Addons on Chrome are defined by Google as being "small software programs that customize the browsing experience" [11]. Browser extensions were introduced in Internet Explorer 4.0 in 1997 and initially only allowed developers to create "Explorer Bars and add entries into the standard context menus" [12]. While limited initially, Chrome introduced an extension API built on HTML, CSS and JavaScript [11] of which other browsers such as Firefox also use today [13]. This has lead to Apple, Microsoft, Google and Mozilla creating a community group called WebExtensions which "seeks to align on a common vision for browser extensions and to work towards future standardization" [14].

2.3 Research Questions and Objectives

This paper's objectives are to test and discuss research and findings that compare two different extension ecosystems, namely NVDA's ecosystem aimed at users who need to use screen-readers and tend to be more specific in their use cases and developed my smaller communities and comparing it to Google Chrome's extension ecosystem which it targeted at all users that browse the internet and have varied purposes and how they interact with Google's systems. Limitations and findings of previous related research papers were used to guide the following research questions.

- RQ1: Which ecosystem has a more secure and private set of addons?
- RQ2: How transparent is each addon ecosystem when it comes to communicating how they work?
- RQ3: How does each organisation (Google and NVDA) design their official addon policy and distribution of addons?

The goal of this project is to compare two different addon ecosystems for people with accessibility needs. Accessibility technologies is not an often researched area and information is sparse, especially when it comes to the security and privacy of these programs as they are intended for minority groups, which can also be vulnerable to any security or privacy issues. By taking a look at these ecosystems, it can be determined which extension ecosystem works better when looking at them in terms of privacy and security as well as testing to see if there is any malicious activity going on with these addons and see if people are already at risk due to malware infecting addons that people rely on to function in their day-to-day lives. Key results from this paper indicate that the smaller and more tight community of NVDA addons is generally more private and secure compared to Chrome's huge addon ecosystem. However, Chrome does show more privacy information related to the addon and asks developers to be more transparent about data collection on their addon homepages, which NVDA does not do. Each organisation has designed an addon approval system that works for the type of community that it serves, with NVDA's policies giving more trust and access to developers than Chrome.

3 Background and Related Work

3.1 Related Work

When it comes to related work in regards to screen reader privacy and security, there is not much research done on screen reader privacy and security and this is not a well-researched area. This could be due in part because its research on software that is used by minority populations. However, screen reader security and privacy is a vital issue as many people rely on it in their day-to-day lives from using it for their jobs to checking bank details online, which involves both inputting and reading out sensitive information which could be compromised if the security and privacy of the screen reader software isn't sufficient enough. However, there has been some research done when it comes to the accessibility of screen readers. These papers are mostly focused on screen readers and web accessibility. Papers written by Lazar et al [7] and Borodin et al [2] focus on what frustrates users of screen reader software when browsing websites, naming issues such as "no alt text for pictures" [7], broken skip-links [2] and poorly designed/unlabeled forms [7], [2], amongst others. However, these two studies were written in 2007 and 2010 with the web and screen reader software having evolved since then.

More recent papers written by Clarke et al. [15] and Kearney-Volpe et. al. [16] look at screen reader accessibility with the modern web, looking at how various implementations of cookie notices affect how users navigate websites [15]. This in turn can also have privacy implications as if users are not able to properly reject cookie notices if they wish to do so, are unable to get the same level of privacy as a sighted person may have as they would be able to visually navigate the cookie notice and reject advertising cookies. One of the papers [3] also echos certain concerns that were also present in the papers written in 2007 and 2010 showing that even over time, web pages are still not being built with accessibility in mind. The study by Clarke et al. [15] shows that out of 46 top UK websites, there were accessibility issues with 22 of the websites.

However, one paper [3] discusses the relationship that users have with screen reader plugins. It goes on to discuss how users rely on plugins to help alleviate issue brought up in the previous research papers as well as both browser and screen reader plugins to help with accessibility concerns. The study also touches upon the privacy and security concerns of plugins being developed and maintained oftentimes by a handful of people, and while they are well known in the community, a handful of participants in the study relied on plugins from unknown developers and that "some of these plugins

are not up to the quality that they get from the reputed developers" [3]. Further discussion is made on the maintenance and distribution of these plugins and how a lot of plugins are found through "google searches" or certain screen readers lack an official addon store with developer policies to help protect users.

4 Accessibility and Privacy Concerns

When looking at the security and privacy of software, security and privacy issues can stem from user understanding from the installation steps of using software, as discussed in a paper written by Momotaz et al. [3]. For the purposes of testing and evaluation, data from WebAIM [6] shows that the majority of people using screen readers do so on Windows and use Google Chrome to browse the web. As there can be accessibility and privacy concerns during installation, this section will look the installation experience for both NVDA and Google Chrome as well as looking at the addon submission and review process for each ecosystem.

4.1 NVDA

4.1.1 Installation

When it comes to the installation of NVDA, a Google search for "NVDA Download" results with the link to the download page on the NV Access website being the top result, as shown in Figure 1.

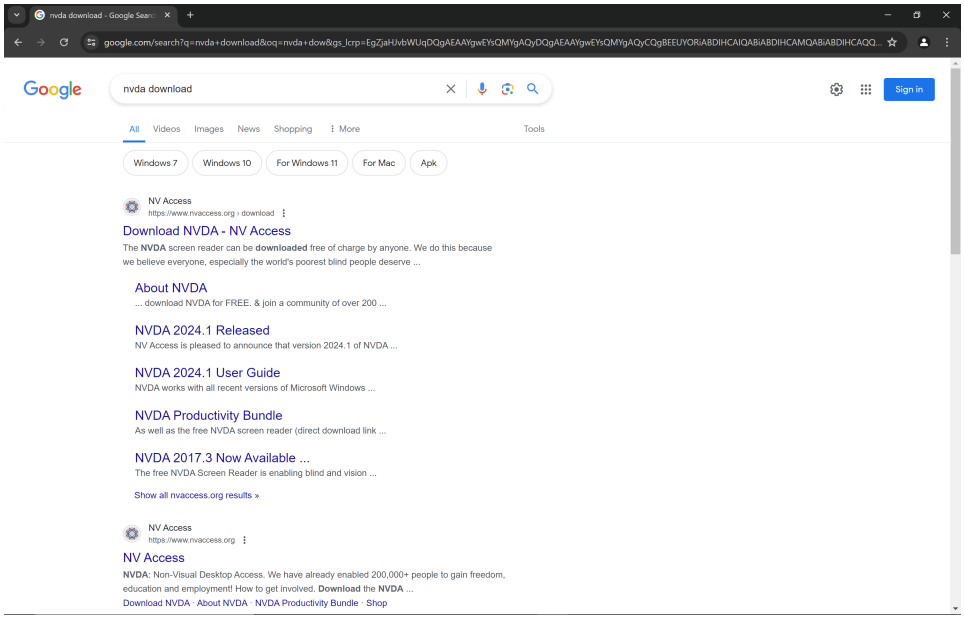

Figure 1: Top search result in Google (2024-06-10)

However, scrolling down reveals download links from websites not associated with NVDA being displayed and the trustability of these websites is unknown, as shown in Figure 2. This can lead to users who are less tech-literate clicking on download links that may contain builds that may be outdated or come with malware as the trustability of these other sites is unknown.

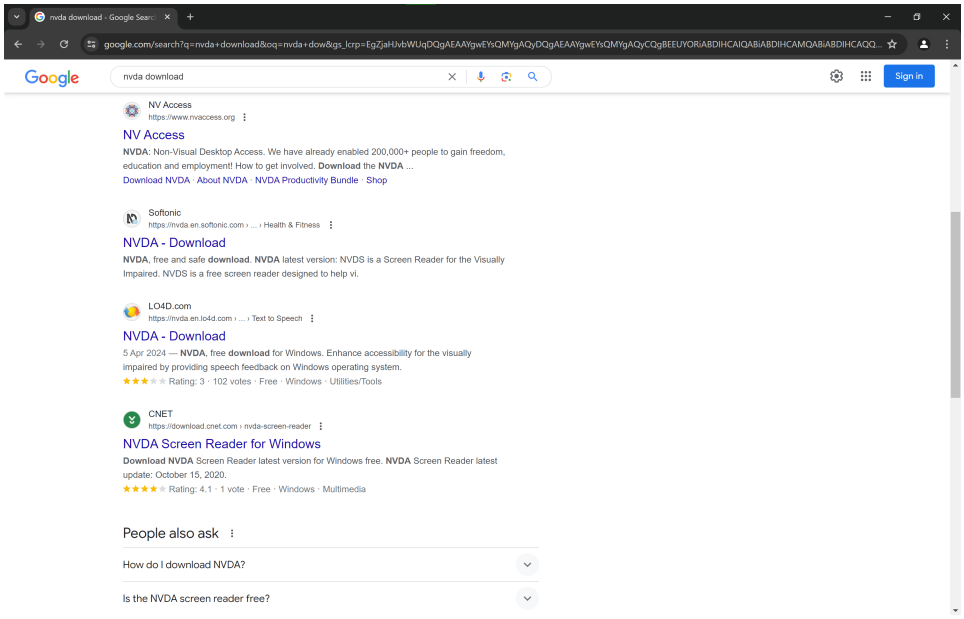

Figure 2: Other search results (2024-06-10)

Once installed, the user is free to use NVDA however they wish and can now choose to install addons either externally or through NVDA's addon store which is built into the program.

4.1.2 CodeQL

NVDA leverages CodeQL for initial security analysis of addons submitted to NVDA's addon store. NVDA claims that it performs automated Python and JavaScript code vulnerability analysis on the GitHub repository being submitted to check for any malicious code [9]. CodeQL is a static vulnerability scanning technology that is developed my Microsoft which can be quite effective, evidenced by research showing that over the "last two years, researchers found over 300 security vulnerabilities through custom CodeQL queries" [17]. However, the paper acknowledges that an issue with static vulnerability analysis tools is "scalability and applicability" [17]. Scalability does not apply much to NVDA addons as they tend to be relatively small in scope and size, typically implementing just one feature per addon. However, applicability can be an issue as "static analysis relies heavily on manual API specifications" [17] and screen reader addons are also niche and specialised software with API specifications quite different from more popular software

addons such as browser addons. NVDA addons not only can interact with browsers, but also computer programs as well, interfacing with Microsoft APIs such as Microsoft Active Accessibility in order to read elements of graphical interfaces [18]. Therefore the effectiveness of CodeQL scanning is dependent on if there exists CodeQL queries to check for vulnerabilities for screen reader specific API. While CodeQL queries are written by both professional and community members, it is also possible for users to write their own queries to better suit their own applications, but as of the writing of this paper, the exact details of how NVDA manages their CodeQL queries is not fully explained on their GitHub and is still in the process of being properly implemented.

4.1.3 Addon review process

If an addon developer is submitting an addon for the first time, an additional measure is put in place where "the submission is blocked pending initial review from NV Access [...] to confirm that the GitHub user has authorisation to submit the addon from the addon maintainers" [9]. This human check for a new publisher adds an extra level of security that automation cannot check for and the source code is checked and if "submitter matches the repository ownership, or the submitter is a core maintainer for the project" then the addon is put through the automated tests before it is merged into the repository. NVDA goes on to specify that "if this is not the case, tag the core maintainer in the submission to confirm they give permission for the submission" [9]. Checking for addon origin author ownership in this method can help prevent a malicious actor submitting an addon that someone else developed (with potential malicious code). Further manual checks are done on the repository "Check for any obvious red flags with the repository i.e. it doesn't look structured as an addon, inappropriate content in the README, author and code only been around for a few days" [9]. However, while this initial step does not check the actual addon code manually for any malicious code, it does look at origin ownership, which is not something that CodeQL or VirusTotal can check for. In addition, NVDA states that "if you submit many addons you may be granted trusted submitter status, which allows you to publish/submit for all addons. It is expected that trusted submitters do not abuse this process. Granting and removing trusted submitter status of publishers will be decided and handled entirely by NV Access." [19], meaning that once a submitter has successfully submitted an addon, they have privileged access to push or delete code from other submitted addons as well, not just their own. In the worst case, this

could lead to developers tampering and adding malicious code into addons that other people have created. A way of avoiding this is keeping track of the Git log to make sure developers haven't been pushing changes to addons other than their own, as there are 63 developers that have submitted addons, as shown in Table 1. Publishers that have developed more than one addon in the store are named, while publishers that have only submitted only one addon are all grouped under "other" indicating that there are 37 publishers that have only developed one addon.

Publisher	Number of addons contributed
abdel792	3
ahmed samy	2
Angel Alcántar	4
Carter Temm	2
Cary-rowen	5
ChrisDuffley	2
Cyrille Bougot	3
Gozaltech	4
huaiyinfeilong	3
hxebolax	2
Ibrahim Hamadeh	3
Javi Dominguez	7
jmdaweb	5
josephsl	3
kefaslungu	2
Luke Davis	5
Marlon Sousa	3
mesteranas	4
Nael Sayegh	3
NVDACN	4
nvdaes	16
Pierre-Louis Renaud	3
Rainer Brell	3
Rui Fontes	17
Ruslan Dolovaniuk	3
Tony Malykh	5
Other	37

Table 1: A table showing which developers have contributed addons

From the table it can be seen that a total of 13 individual publishers are responsible for developing and maintaining 54% of the addons in the official NVDA addon store. Publishers such as nvdaes account for 16 addons and while the publisher name looks like it is officially affiliated to NVDA, looking at the publisher's GitHub page (https://github.com/nvdaes) it seems to belong to just an individual that's highly involved in the addon community, particularity for Spanish-speaking users. While so far, no malicious content has been found from this publisher and they are trusted within the community, new users to the addon ecosystem may confuse the publisher name for being an official Spanish developer from NVDA as their name is used in the publisher name.

But as paper [3] suggested, many people also tend to do a google search to find addons. Like for installation, the official community addons website is the first result. However, the more a user scrolls, the more dubious the results become. Some results for unofficial addons are not indexed by Google and can be found in Telegram chats, so the trustability of the addons are not verified by the community.

4.2 Google Chrome

4.2.1 Installation

To install Google Chrome on a computer using a default Windows installation, users have to go through whatever browser comes bundled on the operating system, which in this case is Microsoft Edge. Results of a search containing keywords "chrome download" on the default search engine, Bing, on Microsoft Edge.

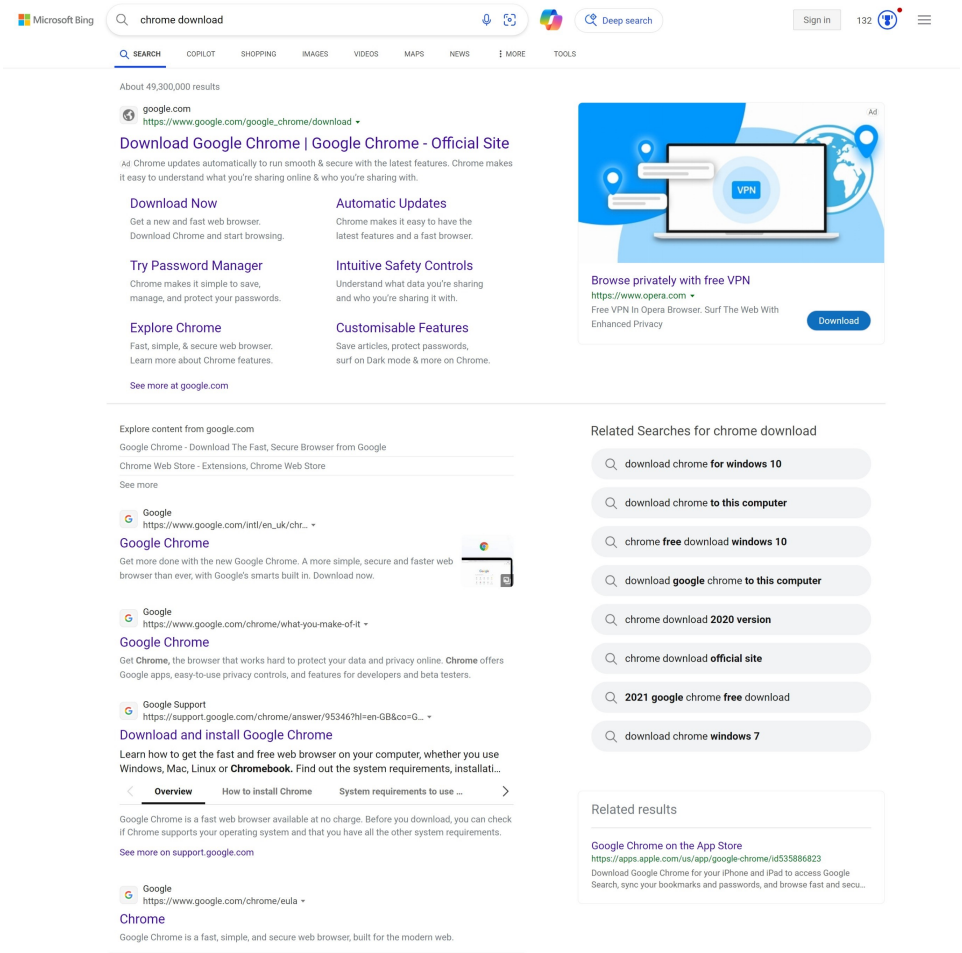

Figure 3: Top Google Chrome download results from Bing (2024-08-10)

Most of the top results are links to official Google sites, so even if they do not directly link to official downloads, they lead to support webpages which direct the user to the official download site.

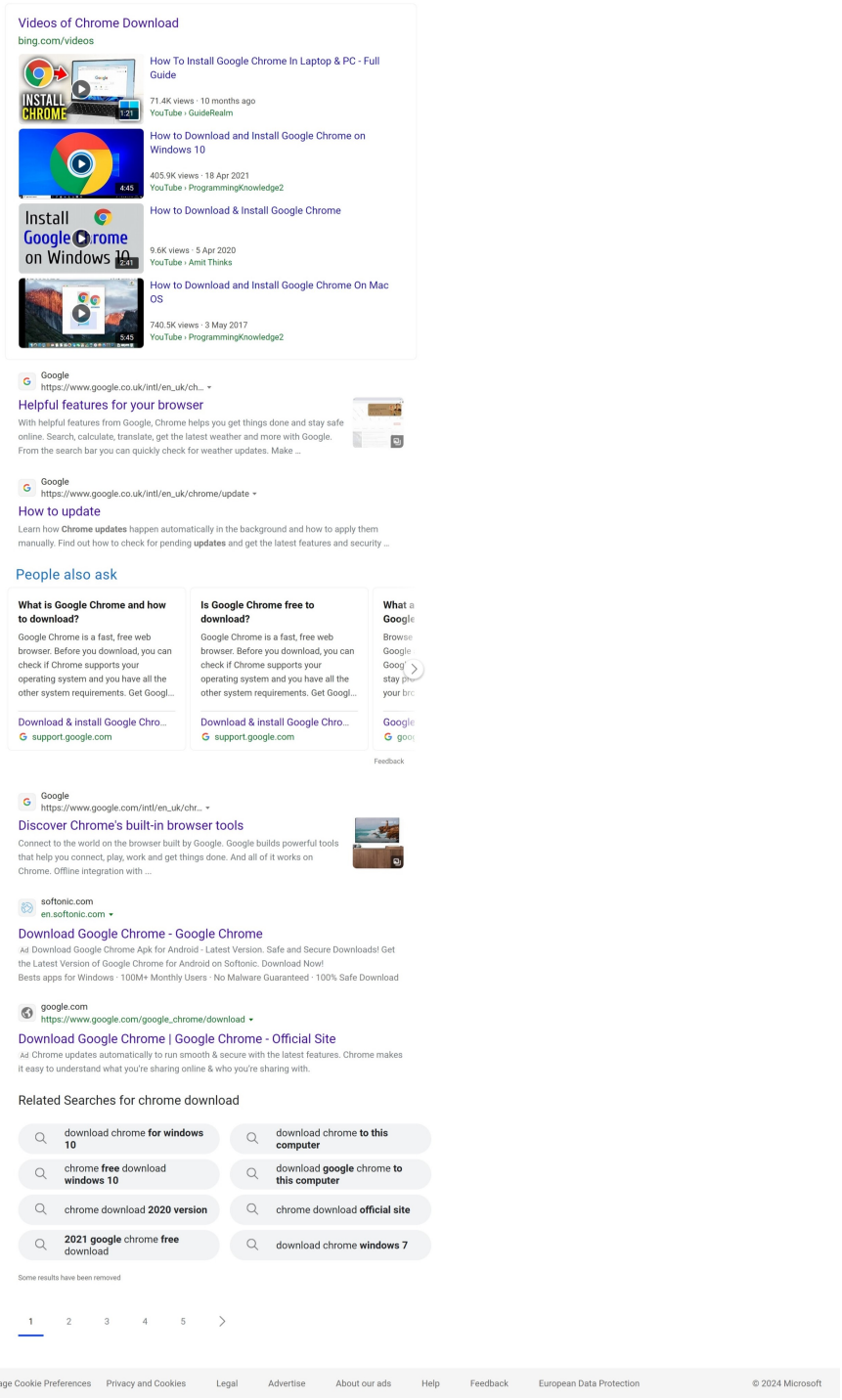

Figure 4: Google Chrome download results continued (2024-08-10)

Figure 4 shows continued search results on the first page of Bing, showcasing YouTube videos that show installation guides on how to download Chrome followed by more Google support pages. However, there is one link to a download on Softonic and is the only website result not associated with Google. As such, it is less likely for a user to download an official installation of Google Chrome compared to NVDA's search results.

4.2.2 Addon review process

Chrome addons are published on the Chrome Web Store, which is Google's official addon marketplace. To submit an addon, Google requires developers to have a specific Chrome developer account where addons are submitted. There, the developer has to pay a one time registration fee ($5) and then can setup their developer profile [1]. When compared to NVDA, anyone can make a GitHub account for free. Both accounts can be anonymous as neither requires a user to store their payment credentials, addresses or real name on their account unless they specifically add a payment method to their account [1]. Google has provided a diagram illustrating the stages of an addon lifecycle [1], which is shown in figure 5

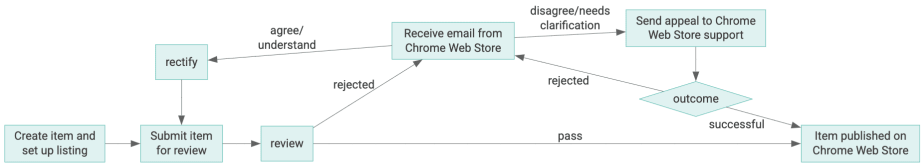

Figure 5: Stages of an addon lifecycle, by Google [1]

Broadly, this follows a similar system as NVDA's where addons are submitted for review to the organisation in which if it passes, it is listed on their storefront, otherwise it is rejected and can either be rectified or appealed. However, NVDA requires a new review application to be made each time the addon is submitted for review. Both organisations use a mix of automation and manual systems in their review process, with NVDA specifying that manual approval is needed for first-time addon submitters to be added to their approved addons submitters list [19]. However, Google specifies that "All submissions go through the same review system, regardless of the tenure of the developer or number of active users" [1], however developers can gain "trusted submitter status" [19] by submitting many addons

and being in good standing, and allows developers to publish/submit for all addons. While this gives power to the developers in NVDA's community, which is based on trust, as NVDA notes, it is expected that those with the role do not abuse it by pushing malicious addons or removing existing ones. While this does allow for a considerable attack vector, NVDA still manually reviews role access as well as there so far being no reported incidents in terms of role abuse. In opposition, Google treats each developer the same way with extra clauses for special cases such as "new developers, new extensions, dangerous permission requests, significant code changes" which "may cause the reviewer to examine an extension more closely" [1]. With Google following a model that trusts its community of developers less for the tradeoff of more security. Google's addon ecosystem is not only much larger than NVDA's, making it harder to manually and fully review each addon, but Google has also run into security and privacy issues with addons already published on the Chrome Web Store, with security researchers in 2020 finding malicious addons and removing them from the Chrome Web Store [20]. Due to NVDA's smaller community, manual review of addons is more feasible and high developer trust allows the company to give dedicated developers more freedom within their ecosystem.

To publish an addon on the Chrome Web Store, a developer needs to submit a addon for review through their developer account, after which it enters the review process. If a violation is found, Google deals with it in the process detailed in figure 6.

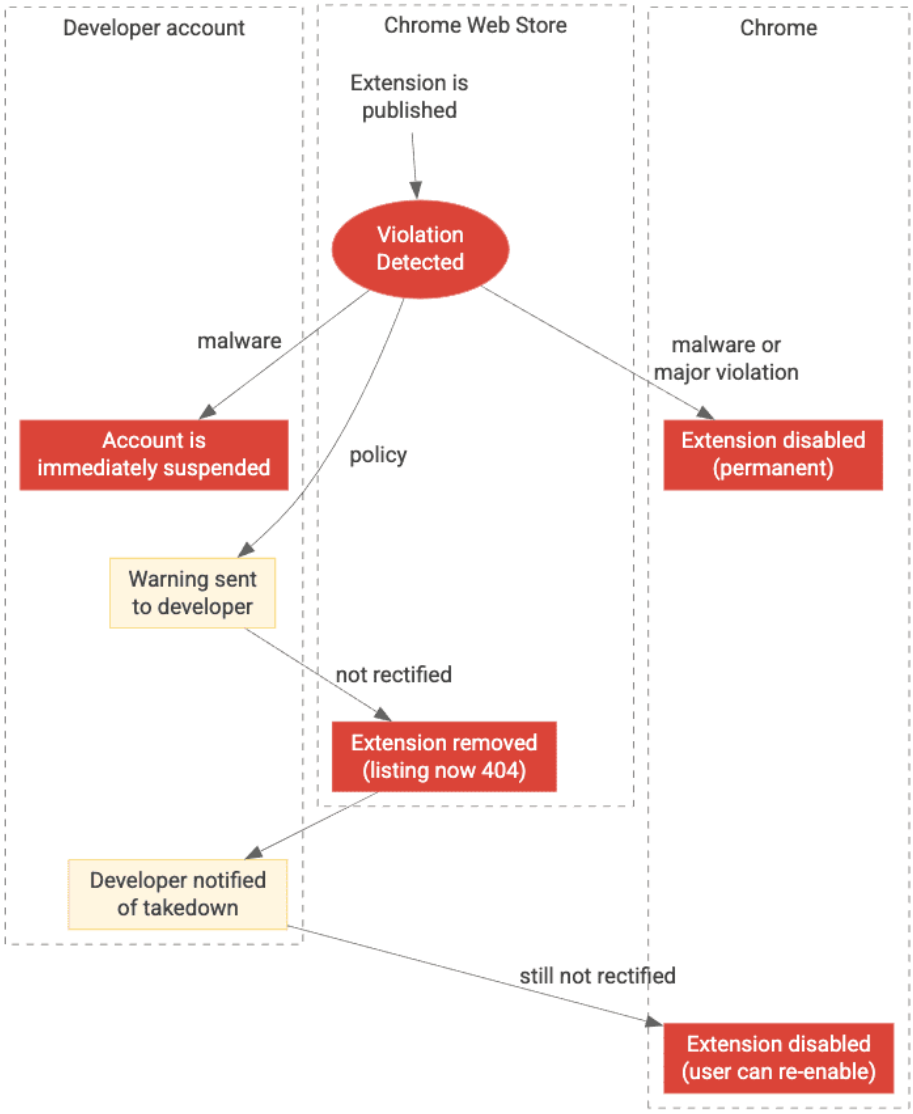

Figure 6: Violation process, by Google [1]

The diagram shows that if a violation is detected, depending on the severity, Google will either suspend the developer's account and/or disable the extension permanently. This can prevent repeated malicious addon submission from a single developer, however it is not specified on what level the account is suspended on. If it is a simple account ban, truly dedicated

malicious actors can simply pay the $5 and make a new developer account and submit another malicious addon. NVDA does not give details on what can happen after an addon is rejected other than if "the [automated] checks fail, a comment should be added to the issue outlining the failure. To address the issues, resubmit the issue form" [19], meaning that malicious actors can keep resubmitting addons until they gain approval, or game the system by submitting valid addons to gain trusted submitter status and then push malicious code to the store. As all of this is done through GitHub with open-source code, it can be easy to roll back and catch malicious actions by reviewing Git logs, but they would have to be checked frequently and once malicious changes are pushed, the changes could affect a large portion of the userbase before it is fixed.

4.2.3 Manifest V3

Manifest V3 is a set of standards which at the time of writing this paper, is a new set of standards governing addons which affects how extensions (including privacy enhancing extensions such as uBlock Origin which blocks ads and trackers) interact with with the browser. This is currently being rolled out by Google and most chromium-based browsers are implementing these new standards. Google states that it helps improve performance [21] however, is refuted by a research paper which "found no evidence that privacy-focused browser extensions substantially negatively affect performance, neither for Google Chrome nor Mozilla Firefox, contradicting Google's claim that the functionality these extensions rely on is a performance concern that justifies severely restricting privacy-focused extensions, and limiting users' choice" [22]. When it comes to research papers on this subject there, only two papers were found while doing research in this area about Manifest V3 when looking with search engines such as Google Scholar with only one of them being available for viewing without a subscription. However, the paper that was available talks about Manifest V3 in a more positive light presenting the fact that by limiting how extensions can interact with the browser, "Manifest V3 produces a relative reduction in detectability, growing from 4% to 10% as extensions become more popular" [23]. While research has not been conducted on whether or not reducing fingerprinting but restricting the functionality of privacy enhancing extensions will improve the privacy of users, many developers do not agree with the changes that Google wants to push to extensions stating it will hamper the extension ecosystem as certain extensions will become far more limited in what they can do and take away user control from the browser [21].

In comparison, there have been no reports so far of NVDA restricting addon functionality in order to retain performance, privacy and security. However, until very recently (May 8th, 2024) [9] NVDA lacked a privacy and security policy for addons included in their addon store. This could be in part due to NVDA being a smaller company than Google and as such they may not have the resources that Google does. One of the papers [3] mentions how community focused NVDA is with many addon developers having strong relationships with the community as a whole, so this communal trust may also be a reason as to it taking so long for NVDA to put an official review process and policies in places due to a lack of need to do so and a lack of any public security and privacy incidents when it comes to the privacy and security of their addons.

4.2.4 VirusTotal

VirusTotal is a website that allows users to upload links or files to check for any malicious code or files. It is a static antivirus scanner that works by collecting malware signatures from designated security vendors [24] to check for malicious code within files. However, there are issues that come with an automated process for addons as static automated processes can be bypassed by developers with true malicious intent. Hashes of uploaded files are checked against databases of various companies for malware signatures, and while VirusTotal has real-time updates for these databases [24], signature-based malware detection does not always catch malware signatures or can also catch false positives.

One issue that can occur with using VirusTotal for malware detection is that "malware developers often leverage [VirusTotal] during development to check if their samples are detected and, if so, revise them until they become fully undetected" [25]. Malicious actors wanting to bypass NVDA's automated system of checking against VirusTotal scans can be circumvented by malicious actors themselves tweaking their code and checking against their own VirusTotal scans before GitHub submission can easily use this method to sidestep this security measure. In addition, it "is possible that a malicious sample is fully undetected when first submitted to VT, but a later report classifies it as malicious" [25]. NVDA's GitHub mentions that VirusTotal scanning occurs when an addon is submitted to be added to their addon store, however, it does not mention whether they receive periodic updates from VirusTotal if a scan gets reclassified later as being malicious or not, so in this way, a malicious actor can submit an addon to the store which initially passes but then can get reclassified by VirusTotal later and

NVDA may not get notified of a potentially malicious extension.

5 Experimentation

5.1 Experimental Setup

Experiments took place between 1st June-1st August 2024 and was conducted on a laptop running Windows 10 with a screen size of 13.5 inches and a resolution of 3240 x 2160. Only programs that are active are NVDA, Chrome, and Wireshark. Only one addon is enabled in each test to avoid any conflicts.

5.1.1 NVDA addon setup

The official addon store can be found in the tools menu in the NVDA application. Within the application, a total of 153 addons can be found. NVDA has an automated security review process detailed on their README on their GitHub [26]. However, similar to the installation of the NVDA program, when searching for addons in Google, only the first search result is for the official community addons website, and the rest are unofficial addon collections, as seen in figures 7 and 8. The other website links all contain NVDA in the name, making them seem more official than they may possibly be and only the community addons that have been submitted to their GitHub have been tested by NVDA, with the rest being untested addons that anyone can download and use.

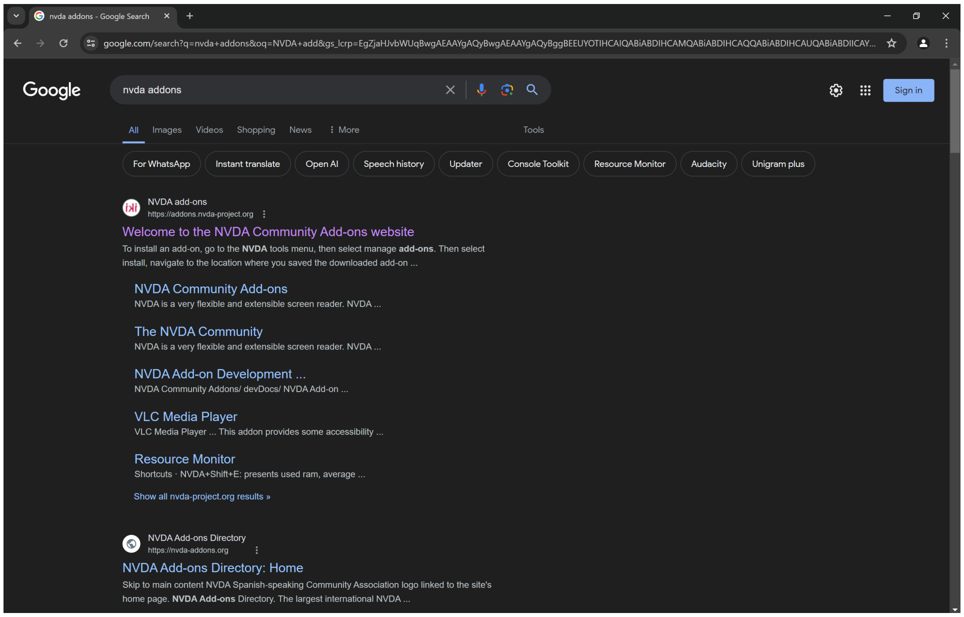

Figure 7: Top search result in Google (2024-06-10)

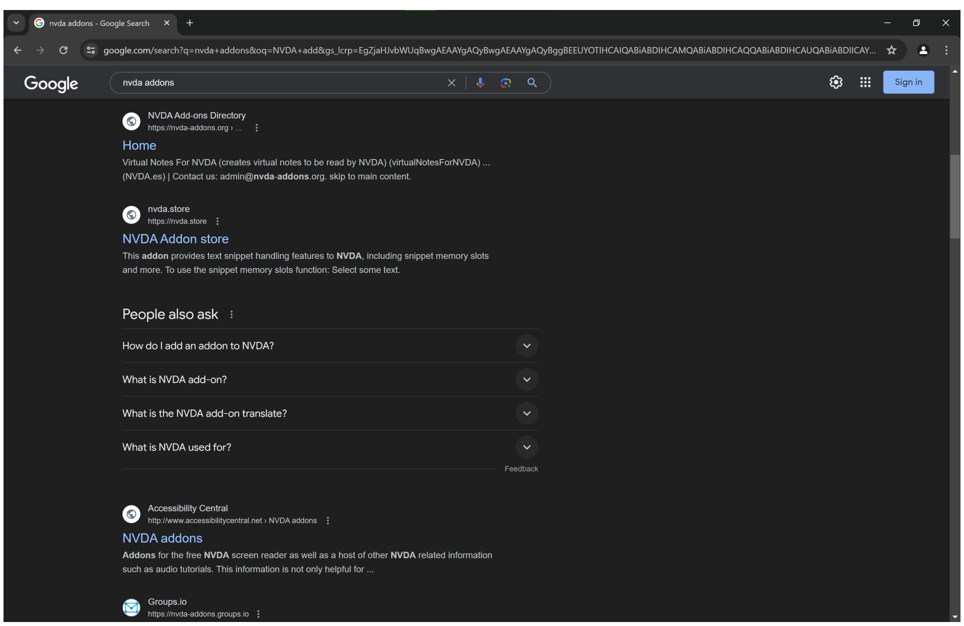

Figure 8: Search results in Google continued (2024-06-10)

There also exists methods of obtaining addons that do not show up on Google search results such as Telegram archives, one such group chat having up to 1.2K members in them which is a high number considering the niche use-cases some of these addons can have. These archives also can contain older versions of addons that are no longer maintained or may have critical security flaws and users have no way of knowing this information. However, installing addons on NVDA come with a warning message shown in figure 9.

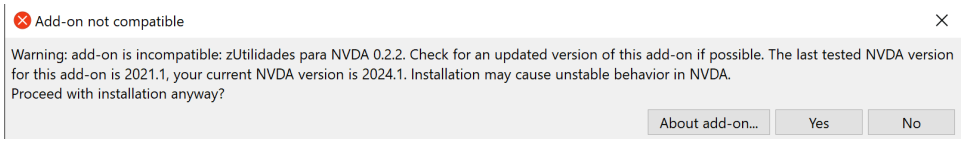

Figure 9: Incompatible addon message in NVDA

This can help dissuade users from installing outdated addons with potential security flaws, however some users may require to use the features of an outdated addon and may choose to install it. After installation of the addon, experiment testing can begin.

5.1.2 Chrome addon setup

Similar to how addons were found in NVDA, a Google search was performed to find Chrome addons, the results of which are detailed in Figure 10.

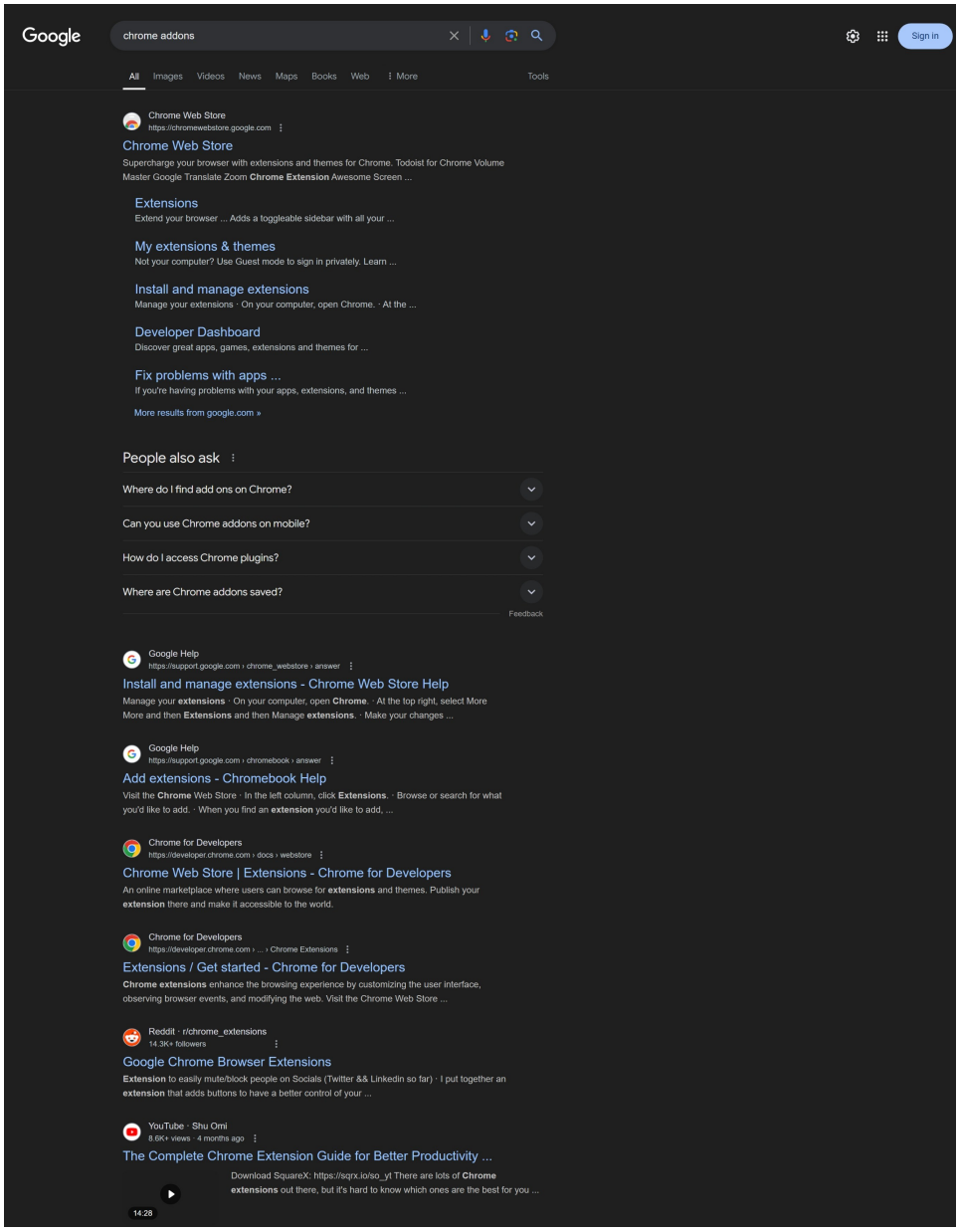

Figure 10: Top search results in Google (2024-07-25)

As opposed to NVDA's search results, the majority of results here relate to official results leading the user to one of many Google pages relating to addons. The first 5 results are all Google resources, and while only the first

main result takes the user to the addon store, the last two results (a dedicated subreddit for Chrome addons and a YouTube video about Chrome's addon ecosystem) are good resources for users who may be confused as well. Here, search results lead to less shady websites and more towards sites that are helpful to the user. From here, addons from the "accessibility" section of the Chrome Web store (shown in Figure 11) were chosen to be tested as addons from that category are helpful to people who need assistive technologies to browse webpages. These addons are sorted by most relevant as this displays addons with the most users as opposed to addons with the highest rating which may not have as many users. Doing so gives a better idea of what addons are commonly used by people with accessibility needs.

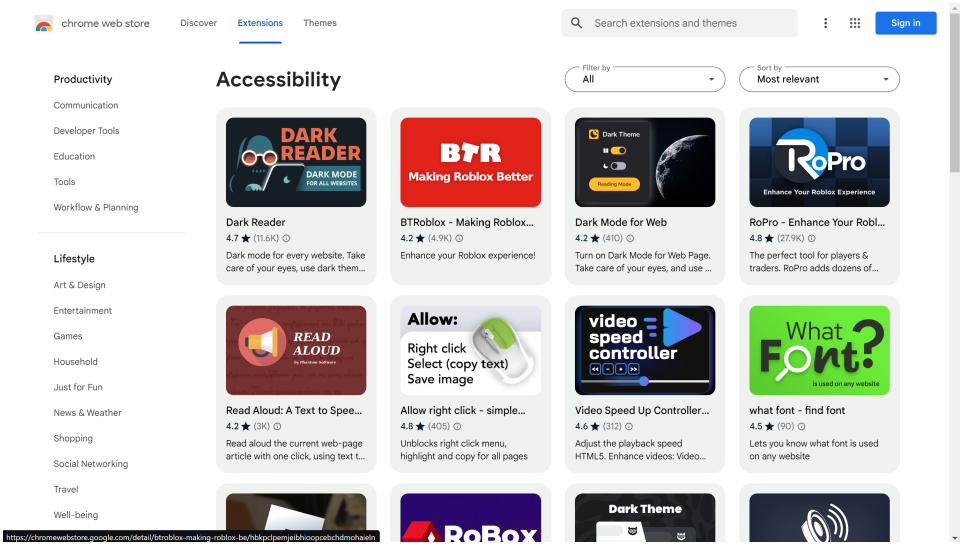

Figure 11: Top accessibility addons on the Chrome Web Store (2024-07-25)

5.2 Methodology

5.2.1 NVDA addon testing

To begin, each addon file is put through VirusTotal prior to network analysis to see if any malware can be detected through static automated malware analysis. Afterwards, the addon is installed on NVDA and NVDA is restarted. While NVDA is restarting, the Wireshark capture begins. Once NVDA has completed restarting, the addon's features will be interacted with for a duration of 90 seconds. If the addon's features do not require interaction with a web browser, an offline application such as Notepad is used to

limit the amount of network traffic. If a web browser is required, google.com is the website that is visited first to check for addon interactivity. For more specialised addons (ex. require latex) an appropriate website (such as Overleaf) is opened up in Google Chrome to test the functionality. After two minutes, the Wireshark capture is saved and the process is repeated two more times before the entire process is repeated again with another addon.

Addons tested either come from a Telegram archive [27] of NVDA addons or NVDA's official addon store built into the NVDA application. Where each addon comes from is specified. The Telegram archive was chosen to also be included in these tests because it contains many addons not found in NVDA's addon store. This is done in part due to the popularity of this archive, having 1.3K users as a part of it. But it also contains addons designed in other languages such as French, Russian, and Chinese whereas the addons in the NVDA store tend to skew towards being English-language addons. In addition, as many addons are not included in NVDA's store it would likely give a better overview of the types of addons some users may install as some useful addons are no longer maintained/updated but still can have some use. A total of 50 addons from the Telegram archive and a total of 50 addons from NVDA's addon store were selected.

5.2.2 Chrome addon testing

Like with NVDA, each addon file is put through VirusTotal prior to network analysis to check for embedded malware. Afterwards to test the addon, bbc.co.uk is opened up and Chrome's developer tools panel is opened up to perform network analysis. An example of a clean network capture of bbc.co.uk is shown in Figure 12.

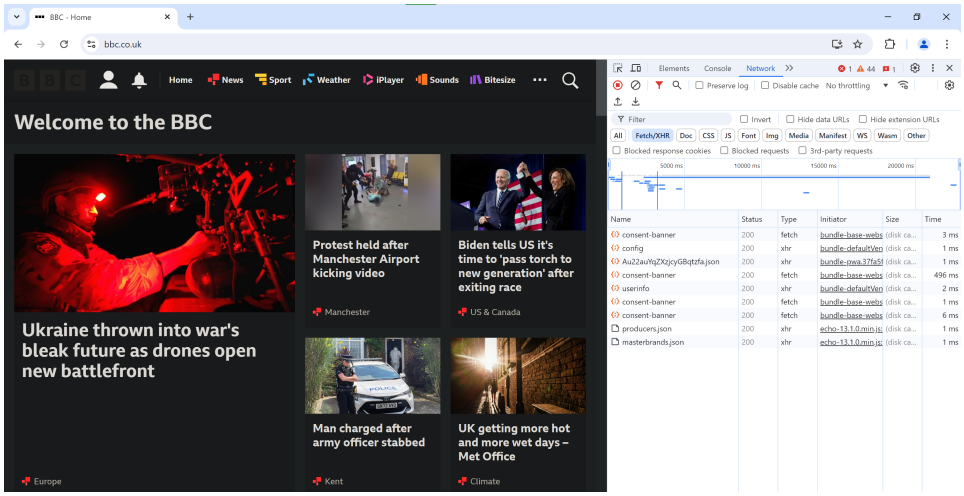

Figure 12: Chrome developer tools Network capture of bbc.co.uk (2024-07-25)

Chrome developer tools is used here instead of Wireshark as it gives more specific information on network activity such as telemetry coming specifically from an addon rather than website network activity mixing with addon network activity.

6 Results

6.1 Addon compatibility

6.1.1 NVDA Telegram Archive

As seen in Figure 13, out of the 50 telegram addons tested, only 14 addons worked as intended. A further 6 addons were unclear as to whether they worked or not and the majority of addons (30 addons), didn't work as intended. This is due to the addons coming from a Telegram group archive [27] where the last update was in 2021.

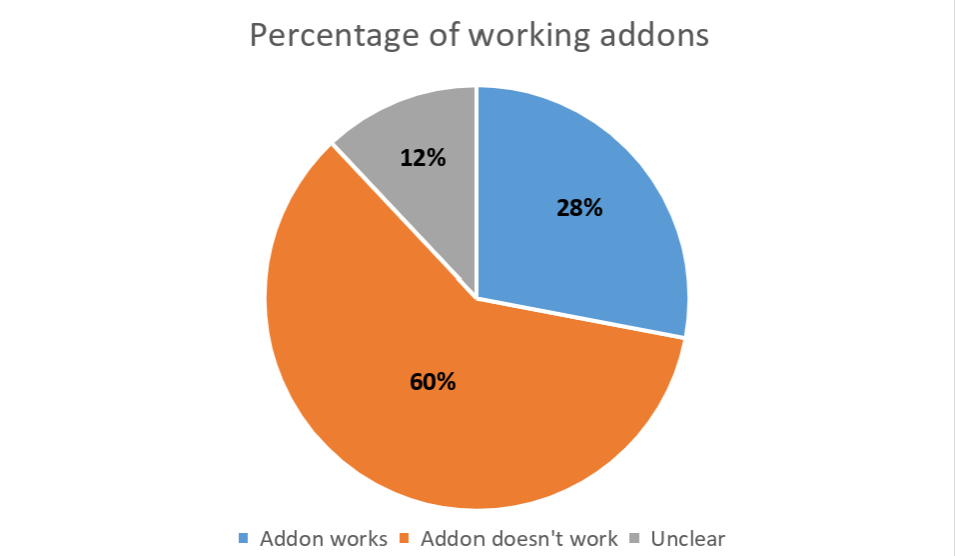

Figure 13: Pie chart showing the percentages of working addons tested from Telegram

These addons were being tested using the most recent version of NVDA and therefore are considered outdated by the application with NVDA throwing an error message stating that the addons have only been tested with older versions of NVDA. Addons uploaded to the group chat also have multiple versions, but for testing only the most recently uploaded version was tested. While the number of addons in this archive is greater than the number of the addons in NVDA's addon store with the Telegram archive containing 2.47k files compared to NVDA's 153 addons. A majority of the files on the archive are just previous versions of the same addon. This serves as a good archiving purpose as users have the choice to use or rollback to previous versions of an addon if for some reason they require functionality that only works in an older version. Installing an external addon from this archive in the NVDA application causes NVDA to throw the message found in Figure 9. The version differences may be a large reason as to why a lot of these addons do not work as intended. However, a few of them do and while addon usage numbers on NVDA are not public information, there can exist some people who rely on these older addons that may not be actively developed or solely get their addons from 3rd party archives such as this Telegram group chat. In addition, users who installed these addons back in 2021 when these were published to the Telegram group chat may still have them active, even

if it may not work anymore, creating an attack vector for malware developers who could potentially exploit the security flaws of an addon that is no longer being maintained. However, the archive serves as a way for users to obtain functionality from addons that are no longer supported.

6.1.2 NVDA Addon Store

On the other side, when testing compatibility of addons from NVDA's official addon store, 42 out of 50 addons (84%) were compatible, as seen in Figure 14.

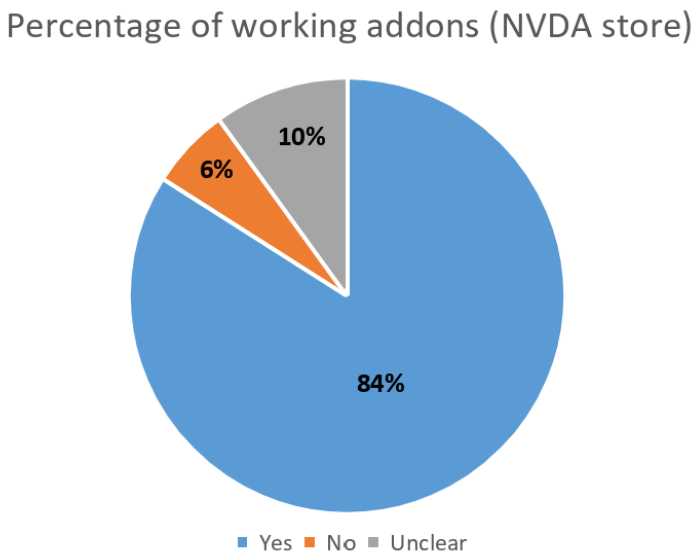

Figure 14: Pie chart showing the percentages of working addons tested from NVDA's addon store

Only three addons (Autoclip, baiduTranslation and AVC) did not work during testing, however it is possible that builds were simply just broken during testing or the addons were not being activated correctly due to errors during testing. A further 5 addons it was unclear if they were working or not due to some addons not having or having unclear instructions for use on their GitHub (edico, AiSound5, androidStudio, Banking4W, ime_expressive). As such, functionality for this addons is unclear, though in the case of baiduTranslation, it was sending API calls to its translation api (api.fanyi.baidu.com), so it can be seen that some parts of the addon were functioning. In general, all addons installed from NVDA's store were

compatible with the current version of NVDA, with most of them working as intended. One thing to note with addons installed from NVDA's store is that all of the addons had links to their GitHub repositories, unlike the majority of Telegram addons where only 15 out of 50 addons (30%) had links to GitHub repositories meaning the majority of addons on the Telegram group chat may have been closed sourced addons as there is no easily accessible GitHub link associated with each addon. To publish an addon in the NVDA store, developers need to

- Maintain or obtain authorisation to publish addon from GitHub repository maintainers
- Register the addon by creating an issue on GitHub and fill out the relevant details (Download URL, Source URL, Publisher, Channel, Licence name)

after which the addon will be pending manual approval before it is published on the NVDA store.

6.1.3 Chrome Web Store

As seen in Figure 15. The Chrome Web Store has the highest amount of addons that function as intended with only 2 out of the 50 addons tested not working as intended. There are no addons that are uncertain if they work or not, unlike tests with some NVDA addons. In general it was more clear if addons worked or not possibly due to each addon having a store page on the Chrome Web Store which details functionality through images and descriptions. One of the main reasons compatibility tests would show up as unclear for certain NVDA addons is because they either did not have a GitHub page linked which would detail functionality or a description of addon features failed to show up in NVDA when installing certain addons, making it more difficult to determine addon functionality and how to activate it.

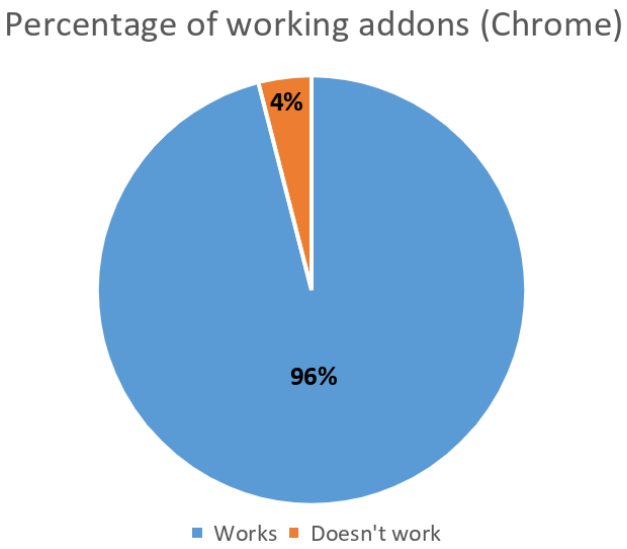

Figure 15: Percentages of working addons on Google Chrome

In addition, all addons have unique UI associated with them where users can access extra functionality and information, and while the use cases for such UI for a screen-reader application such as NVDA may vary a lot and may not be as necessary, addons having their own associated page with standardised information on usage may be more beneficial to newer users of NVDA. Figure 16 and Figure 17 show information displayed to the user on addon installation pages in Chrome and NVDA respectively.

Figure 16: Screenshot of the Dark Reader addon on the Chrome Web Store

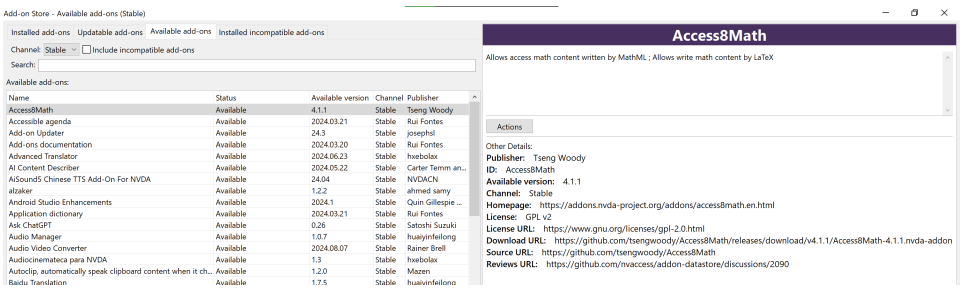

Figure 17: Screenshot of the Access8Math addon on the NVDA Addon Store

As seen in the above figures, the Chrome Web Store typically has more information about the addon than NVDA's store. This is due in part to Google enforcing developers to fill out a lot of listing information to publish an addon on their web store [1]. This information includes

- Graphical assets: A store icon image, at least one screenshot, a link to a YouTube video showcasing features of the addon and a promo tile image
- Localisation information such as descriptions and screenshots if the addon is localised
- Privacy information: permissions requested, remote code execution (which will be removed with Google's full rollout of Manifest V3), data use practices and a privacy policy
- Monetisation: Declare any in-app purchases, store visibility, geographic distribution

As one paper [3] writes, NVDA's addon ecosystem is a lot more community-driven than Chrome's, which could lead to larger trust between addon developers, organisations and users as there is a trust established within the community. In addition, none of the addons on NVDA's store are monetised nor do they seem to harvest any private data, and as such are not required to display information such as privacy disclaimers as seen in Figure 16 like in Chrome's Web Store.

6.2 Network Capture Results

6.2.1 NVDA Telegram Archive

Out of the 50 tested addons, the majority of addons showed normal network activity indicating that they were not contacting any external domains. Only 2 addons showed any network activity. Addons such as YandexTranslate have to contact an API for it to work and in such cases only the API (in this case translate.yandex.ru) is contacted in the generation of an API key and translation functionality. Weather_Plus is also another addon that contacted an external API (veloroutes.org) to determine user location to get weather data.

One addon (volume_on_startup) was not able to be properly tested via Wireshark analysis due to it being an addon that is activated when Windows starts up with NVDA, and as such, Wireshark cannot capture packets before startup. Therefore passive Wireshark analysis was one on this addon wherein the addon was active, but its features could not be triggered actively. However, Wireshark analysis shows no malicious activity while the addon is active in the background. Ventrilo is an addon that was also analysed using passive analysis as it only works with an older version of the Ventrilo client (used for messaging) which is unavailable to download, so Wireshark analysis was done passively.

Two more addons (winGlulxe and USA-V) were not able to be analysed using Wireshark due to installation errors preventing NVDA from running the addon and thus being able to run analysis on these addons.

6.2.2 NVDA Addon Store

Like with the results of the Telegram Archive, out of the 50 tested addons, the majority of addons showed no discernible network activity. The only addons showing network activity were baiduTranslation, crypto_info and CurrencyConverter. Just like with the results in the Telegram Archive, these addons contact a specified API to carry out their functionality

- baiduTranslation contacts api.fanyi.baidu.com for the translation API
- crypto_info contacts api.coincap.io for getting current cryptocurrency rates
- CurrencyConverter contacts google.com to submit a search query to get current conversion rates

One thing to note that occurs when testing for both Telegram addons and NVDA addon store addons is that NVDA contacts its own domain www.nvaccess.org, which while not confirmed officially on the NVDA GitHub, most likely may be NVDA contacting its own domain to check for application updates.

6.2.3 Chrome Web Store

Very similarly to previous tests, out of the 50 addons tested, only 3 addons showed any network activity. RoPro - Enhance Your Roblox Experience contacted https://ropro.io/api/getServerLocations.php?placeid=286090429, Night shift mode contacted palette-picker.css and CroxyProxy contacted https://www.google-analytics.com/g/collect?_cpo=1 &v=2&en=page_view&tid=G-0WD9HNFY6Z&cid=1722782209.447132652& dh=www.bbc.co.uk&ul=en-GB&dt=BBC+-.

As shown in Figure 18, the RoPro addon contacts its own domain (https://ropro.io/api/getServerLocations.php?placeid=286090429) to get a JSON file and insert a list of server locations for a game on Roblox. This is a feature that is outlined by RoPro's store description and it serves no malicious purpose.

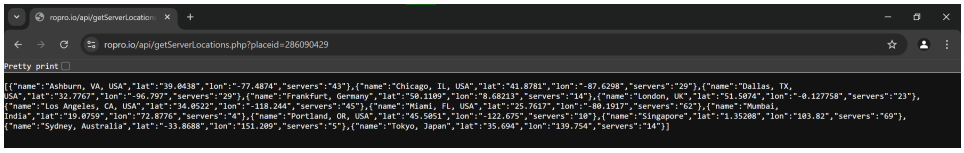

Figure 18: Screenshot of the JSON file containing server locations

As for Night Shift Mode, it is uncertain why palette-picker.css shows up in the network capture, the palette picker css file is injected into the webpage itself and users can click a coloured box at the top of the webpage to give the webpage a tint in any colour the user wishes. This is part of the described functionality of the addon and serves no malicious purpose, however it is uncertain why the css file is being fetched over the network instead of being loaded locally.

CroxyProxy seems to send back some Google Analytics data as it contacts Google's analytics domain and the URL seems to send back what website is currently being viewed. While the privacy policy, shown in Figure 19, on the addon store page states that they may "use third-party web statistics services to collect and analyze general visitors' behaviour in order

to improve the service performance" [28], which could potentially include Google Analytics, although it is not specified.

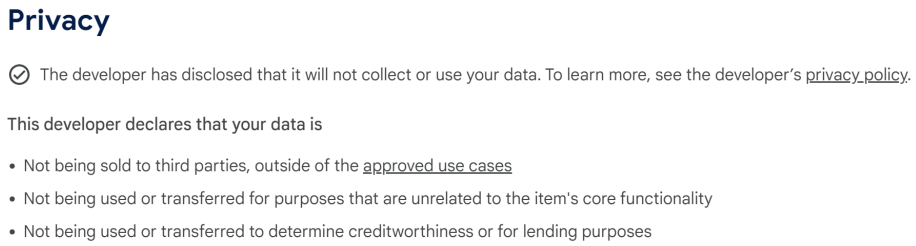

Figure 19: Privacy Policy for CroxyProxy

6.3 Other Security and Privacy Issues

6.3.1 NVDA Telegram Archive

One addon (winGlulxe) was not able to work with NVDA at all, it is unknown what the purpose of this addon is or what it does as when trying to install it, NVDA gives the error message shown in Figure 20. It is possible that this addon could only be installed on older versions of NVDA, but considering that every other addon can be installed regardless of if they work or not, this could just be a corrupt addon file that does not work. The VirusTotal scan for this addon came out clean, indicating that there are no known malware signatures within the addon files either.

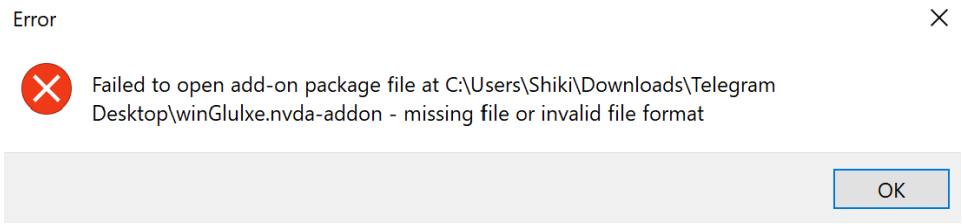

Figure 20: NVDA error message failing to open winGlulxe

USA-V was another addon that also had installation errors, with NVDA having installed the addon with no errors, but it not showing up in the "installed addons" list in NVDA. It is uncertain is there was some kind of error in the installation process preventing the addon from showing up or if the addon was installed but didn't display properly. Multiple reinstalls yielded the same results.

For 5 out of the 50 addons tested (YYPatch, wintenApps, Weather_Plus, virtualCopy, unmute), upon installation of the addon, Windows file explorer threw an error stating "Error:The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application". This error is difficult to consistently reproduce, sometimes appearing upon installation and sometimes appearing during addon usage. The Wireshark captures show no sign of any telemetry being sent for these addons, so it is likely that the addons were unstable due to them being outdated causing NVDA to behave erratically.

6.3.2 NVDA Addon Store

There are some addons which are clearly contacting external websites but their API/website calls do not seem to show up in Wireshark capture analysis, or if it does, it is showing up as encrypted traffic. Addons such as TranslateAdvanced and audiocinemateca are both addons that both state they contact external websites and the addons themselves work as intended, so the API calls not showing up in the Wireshark capture may be due to experimenter error as other addons show their API calls clearly on Wireshark.

The emoticons addon displayed a "Error: The system detected an overrun of a stack-based buffer in this application. This overrun could potentially allow a malicious user to gain control of this application" message, however as stated before, this error is difficult to reproduce and it us unclear what the true cause of this error may be as both Network and VirusTotal analysis for this addon came back as clean so the possibility of this addon purposefully trying to do something malicious may be low.

6.3.3 Chrome Web Store

The only thing to note for other security/privacy concerns for Chrome addons is that 5 of the 50 addons had an extra note on their store pages stating "This extension may soon no longer be supported because it doesn't follow best practices for Chrome extensions" which relates to Manifest V3 and Chrome implementing tighter security measures on addons, limiting what they can do such as phasing out Remote Code Execution for Chrome addons. These addons may contain functionality not supported in Manifest V3 and as such they have this message displayed on their store page. Addons that display this message are

- Substital: Add subtitles to videos and movies

- Darkness - Beautiful Dark Themes
- CroxyProxy Free Web Proxy contacted
- Midnight Lizard
- Scrollbar Customizer

6.4 Embedded Virus Scanning

6.4.1 NVDA Telegram Archive

Addon files obtained were submitted to VirusTotal to check for any Malware signatures. However, as older versions of addons from a Telegram archive were being tested, all of the submissions were being submitted to VirusTotal for scanning for the first time, as seen in Figure 21.

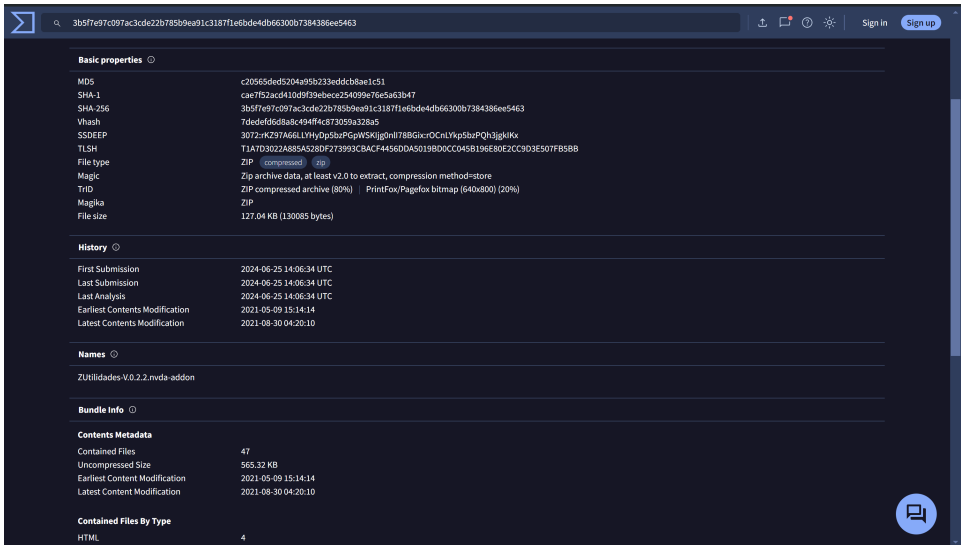

Figure 21: VirusTotal first submission

Out of the 50 tested addons, WlanReporter, WLmail and WindowsMail are the three addons that VirusTotal detected malware signatures from. The result of the analysis the WLmail addon is shown in Figure 22.

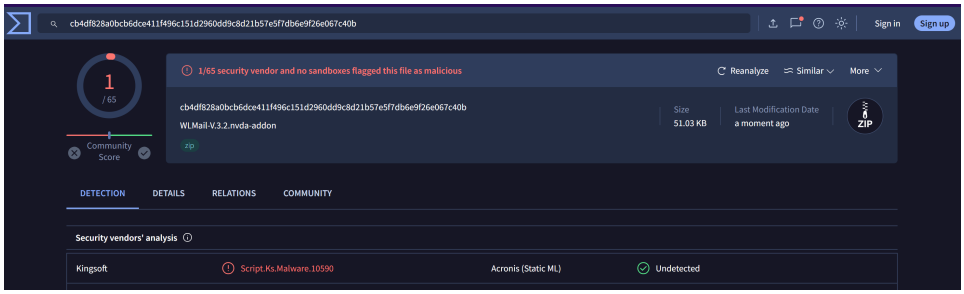

Figure 22: VirusTotal Script.Ks.Malware.10590 malware in WLmail

All three addons that were flagged by VirusTotal were shown having the same malware signature, Script.Ks.Malware.10590. However, Google searches do not net any detailed results on what this specific malware could possibly be, with the closest relation being Script.Ks.Malware.3866. GitHub user sillyfire raised this issue when scanning for a different program called v2rayN but later marked it as a bug, possibly indicating that this was due to it being a false positive [29]. In addition, it was only detected by one of the 65 security vendors on VirusTotal. The malware was not detected by Windows Defender, so it is unknown if a malicious script was run on the machine upon activation of the addon. Furthermore, the WMail addon has no linked source code, so source code analysis cannot be done to see if any scripts are embedded in the code. However, WlanReporter does have a GitHub link, and submitting the most recent GitHub code for analysis on VirusTotal flags no Malware, even by Kingsoft, the vendor that flagged the version for testing found no malware on the most recent version. This could mean that there was a bug in the version being tested that was later fixed, or the malware is better hidden from static code analysis tools. Looking at the python code of the addon on GitHub [30], it does not seem as though it is triggering any malicious scripts as all the addon does is interface with Windows to check the WiFi/LAN connection status and notify the user about it, the only changes from the version tested (2021) and the current version (2023) is changes on how error checking is done, so it could be possible that these error checks are what have been causing the malware vendor to flag the addon as having a malicious script. Another possible explanation could be that the addon may have been complied from an untrustworthy source and then put in the Telegram group chat as there is no indication that the addon was built from source.

In addition, it is worth noting that four out of the 50 addons had previously been submitted to VirusTotal for malware analysis. VLC and vir-

tualRevision were both submitted on 2021-07-30, possibly by the addon developers or user(s) who wanted to check it for malware before installing. However, unmute and virtualCopy were submitted on 2023-12-07 and 2024-06-29 respectively, with virtualCopy being a very recent submission which could indicate that there are users still using outdated addons from this Telegram archive and checking for any malware before using it.

6.4.2 NVDA Addon Store

For malware scanning of the official addons, both a GitHub repository and file analysis were conducted for each of the 50 addons tested. The GitHub URL was fed to VirusTotal as well as the most recent release of each addon was downloaded from GitHub and uploaded to VirusTotal. Testing using this method gave different results as VirusTotal didn't flag any of the files for each addon tested. However, 82% of GitHub links submitted to VirusTotal were flagged as either suspicious or having malware, as seen in Figure 23.

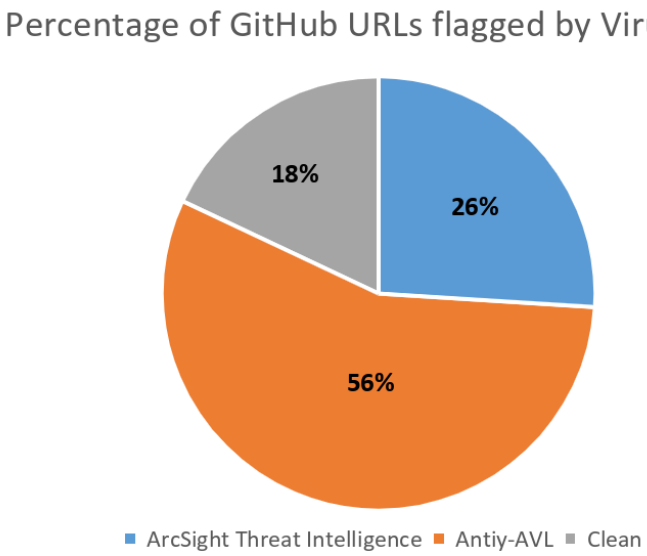

Figure 23: Percentages of URLs flagged by VirusTotal

56% of links were flagged by the security vendor, Anity-AVL as being malicious with no specific malware signature to point to a root cause, as seen in Figure 24.

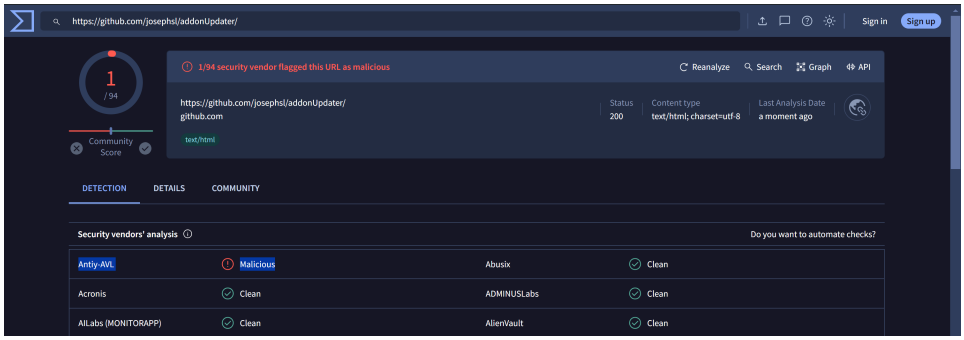

Figure 24: VirusTotal Anity-AVL malware detected

Some webpages were also flagged by ArcSight Threat Intelligence as shown in Figure 25.

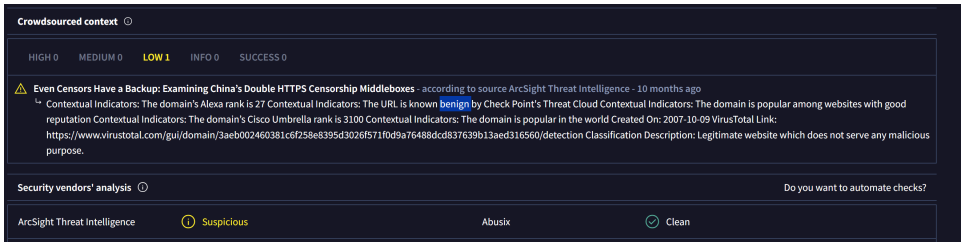

Figure 25: VirusTotal ArcSight Threat Intelligence malware detected

What is different about this flag is that VirusTotal classifies it as a low threat and it has extra "crowdsourced context" However, like with the flags shown when testing the Telegram addons, these could also be false positives as the actual addon files scanned by VirusTotal were all clean with the Wireshark captures also showing no signs of suspicious network activity. However something to note is that while sites were either flagged by ArcSight Threat Intelligence or Anity-AVL, no site was ever flagged by both at the same time. The crowdsourced states several contextual indicators reformatted below for the sake of clarity:

1. Contextual Indicators: The domain's Alexa rank is 27
2. Contextual Indicators: The URL is known benign by Check Point's Threat Cloud
3. Contextual Indicators: The domain is popular among websites with good reputation

4. Contextual Indicators: The domain's Cisco Umbrella rank is 3100
5. Contextual Indicators: The domain is popular in the world
6. Classification Description: Legitimate website which does not serve any malicious purpose

The first contextual indicator refers to the popularity of GitHub as a whole (not just the specific addon repository), ranking number 27 out of the list of most visited websites as rated by Amazon Alexa. The service shut down on May 1st, 2022. However an archive of the webpage the day it shut down shows that the 27th ranked website globally is twitter.com and not GitHub, so the information from VirusTotal may be outdated in that regard. VirusTotal doesn't display when the contextual indicator was added and where it gets its information from, but as the Alexa domain ranking list shut down in 2022, any information regarding sit ranks are not based on up-to-date information. However, the fourth contextual indicator ranks github.com as being 3100 under Cisco's classification system which "contains our most queried domains based on passive DNS usage" [31]. It is still active, unlike Alexa's rankings so it can be seen as more reliable. However issues with contextual indicators 1, 4 and 5 is that site rankings based on popularity do little to prove or disprove any security claims other than an assumption that popular sites are "more secure" as there is still a possibility that hackers can hack into a well-known website and distribute malware through it. The classification description however, does state that from the crowdsourced context that github.com is a legitimate website which does not serve any malicious purpose but it also doesn't mean that malicious content can't be found on the website even if the website itself does not serve a malicious purpose as there have been reports of GitHub repositories serving malware to users despite them still being open source with one research article [32] showing that over 100,000 infected repositories were found on GitHub. So even if a website isn't malicious, malicious content can still be placed on the website. However, just because VirusTotal reports certain links has potentially having malware, these are not supported by Wireshark and file analysis.

The second contextual indicator is a flag from Check Point's Threat Cloud system which supposedly uses AI to catch malware with a "99.8%" accuracy [33]. If these claims are to be believed, then a total of 13 addons have malware signatures somewhere on the GitHub repository. However, no specifics are given apart from the statement that the URL is "known benign". It is unclear if it is referring to the domain as a whole or if it is in relation to the specific repository. If it referred to the domain as a whole

then it can be assumed that this malware signature should show up for every addon URL submitted, however it only shows for a subset of addons which could indicate the presence of malware on these specific GitHub pages even though no malicious activity was detected using both Wireshark and file analysis. Once again it is possible that this may be a false positive but without more information as to what triggered this malware flag it is difficult to formulate definite conclusions.

6.4.3 Chrome Web Store

As shown in Figure 26, out of the 50 addons tested, 11 were flagged by VirusTotal by multiple vendors as potentially containing malware.

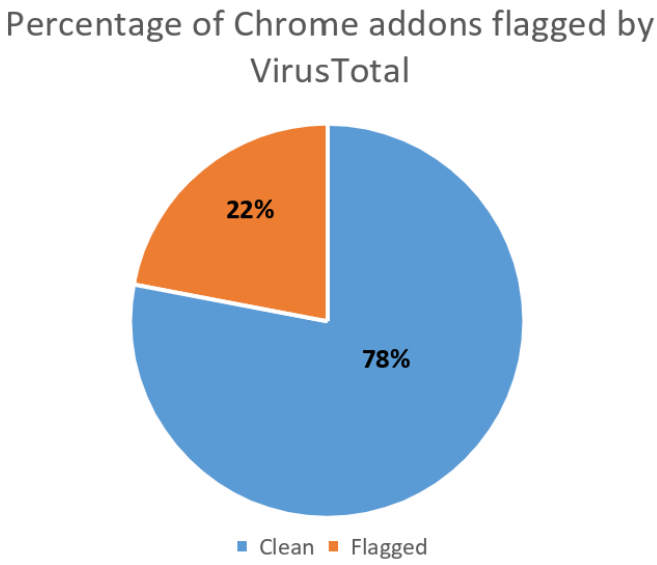

Figure 26: Pie chart showing percentages of addons that have been flagged by VirusTotal

The addons that were flagged by VirusTotal as well as their signatures are detailed in Table 2.

Allow right click allegedly contains a type of Trojan, and information relating to this particular signature could only be found on one site [34], which states that it could

- Download and install other malware.

- Use your computer for click fraud.
- Record your keystrokes and the sites you visit.
- Send information about your PC, including usernames and browsing history, to a remote malicious hacker.
- Give remote access to your PC.
- Advertising banners are injected with the web pages that you are visiting.
- Use your computer to mine cryptocurrencies.

However, as network analysis did not yield any supporting evidence, and the code is closed-source it is difficult to ascertain for sure if this malware is genuine or if its just a false positive.

what font - find font is an addon which according to VirusTotal vendors contains adware which could potentially do the following [35]

- Advertising banners are injected with the web pages that you are visiting.
- Random web page text is turned into hyperlinks.
- Browser popups appear which recommend fake updates or other software.
- Other unwanted adware programs might get installed without the user's knowledge.
- Changing the web browser's default home page
- Changing the browser's search provider and built-in search box

Through observation, no extra adware was being visibly injected into websites visited, so this could mean that it is a false positive or the adware being injected is more subtle or that the malware is not working as intended. More in-depth tests would be required to gather more evidence to prove this.

Roblox with extras! - RoBox is an addon that contains malware flagged by 4 security vendors, as shown in Figure 27

Addon name	Malware signature(s)
Allow right click - simple copy	Trojan.Win32.Tibia.DYZ
what font - find font	Adware.OpenTab/JS!1.F122 (CLASSIC)
Roblox with extras! - RoBox	Trojan.JS.Chromex, Adware.OpenTab/JS!1.F122 (CLASSIC), JS/Chromex.Agent.BZ, Google: Detected
Adblock all advertisement - No Ads extension	Adware.AdInject/JS!1.F11C (CLASSIC)
Floating Video Player	JS/Adware.Chromex.Agent.Y
Free privacy connection - VPN guru	JS/Adware.Chromex.Agent.AA
Cleaner - history & cache clean	JS/Chromex.Agent.A Potentially Unwanted, Adware.OpenTab/JS!1.F122 (CLASSIC)
Sound Booster	JS/Chromex.Agent.BZ, Google: Detected, Trojan.JS.Chromex, Adware.OpenTab/JS!1.F122 (CLASSIC)
CroxyProxy Free Web Proxy	Not-a-virus:HEUR:AdWare.Script.ExtRedirect.gen
Midnight Lizard	Malware.U.GenericMC.cc
Sweet VPN	JS/Adware.Chromex.Agent.AA

Table 2: A table showing addons and their related malware

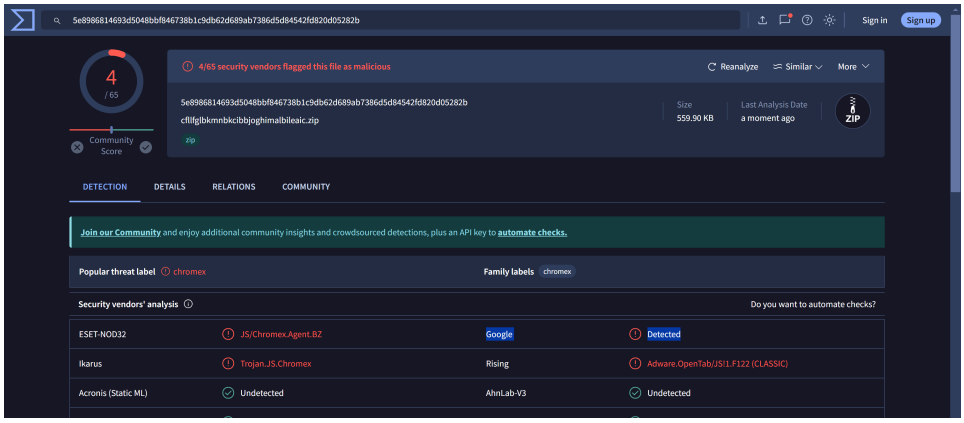

Figure 27: VirusTotal screenshot of malware signatures found in the RoBox addon

One thing to note is that one of the security vendors that flagged this extension as potentially having malware is google themselves. However when the information panel is opened, it provides the information found in Figure 28

Figure 28: More information on Google as a security vendor

It states that the "company decides the particular settings with which the engine should run in [VirusTotal's] platform" which leads back to how Google conducts their addon review process as they have stated that they perform a mix of manual and automated analysis, so if Google is using the same algorithms to detect malware signatures, then their automated analysis should have picked up this signature. However, as VirusTotal points out, the company is responsible for the parameters that work on VirusTotal, so Google themselves could be running a more accurate and up-to-date version of their virus scanning model with the VirusTotal version being behind. On the other hand, multiple security vendors, and not just Google have flagged this addon as potentially malicious, which lends more evidence to the addon

having potential malware. If this malware is picked up by Google's automated systems, then according to Figure 6, Google should have suspended the account or disabled the extension. Once again, it is possible that this is another false positive showing up with multiple security vendors, but it is hard to verify without more testing. One thing of concern is that this is an addon targeted at children as they are the primary userbase for Roblox, so an addon containing adware and/or malware in software targeted towards children is illegal in some regions.

The rest of the addons also all contain various types of adware/malware, with security evaluations for those also being the same as the ones described above as it is hard to properly see if the addon is malicious without being able to perform a manual code analysis due to the majority of addons being closed-source compared to NVDA where all addons on their official addon store were open-source and therefore the code was easy to verify if it had any malicious code in it. In addition, while the exact malware signatures for addons may differ, it is also difficult to find information about specific malware signatures as they are not posted online. Without more in-depth tests for these addons, it is difficult to tell whether these are all just false positives or if there is truly malware embedded in these addons as the network captures do not show anything out of the ordinary for any of these addons.

7 Limitations and Future Work

One of the major limitations of this study is the amount of testing that could have been done in both addon ecosystems. Only 50 Telegram addons + 50 NVDA addon store addons + 50 Chrome addons were able to be tested in ecosystems with hundreds of addons. This leads to having a comparatively small sample size which may not be representative of these ecosystems as a whole. As there is not much research done in this field, it is hard to determine which addons are used the most by NVDA users as it is not public information, and testing out the most popular addons may give a better representation of the addon ecosystem than testing addons alphabetically.

In addition, static code analysis of addons was limited due to time constraints and resources. Most of the chrome addons do not have publicly viewable code, so any further analysis would have to be done in partnership with addon developers to determine any potential security/privacy threats.

One more limiting factor is the tools used for malware analysis such as VirusTotal. There exists AI-based malware scanning tools with more

dynamic malware analysis which could be helpful in trying to weed out false positives as if there are similar matches showing up with static signature based detection and AI based dynamic detection, then there may be stronger evidence to support the fact that some addons may have malware embedded in them.

Another limitation is that not much information can be found on the specific malware signatures flagged by various vendors on VirusTotal, so contacting the vendors and seeing if they're willing to share more information on these malware signatures could have given more definitive evidence on if these are false positives or not.

Further future work could include testing a larger sample size of addons to get a better and more cohesive view of these addon ecosystems. This could then be extended to more platforms, such as accessibility ecosystems found on MacOS. Further usability and accessibility tests could also be performed to compare strengths and weaknesses in each addon system by actual users with disabilities which would help in addon accessibility evaluations. More in depth malware analysis and testing could also be beneficial to prove or disprove malware information found in this paper as findings may only indicate false positives. Case studies on accessibility ecosystems could also be conducted to work together with organisations involved to find deeper insights on any security and privacy issues.

8 Conclusion

In conclusion, NVDA's addon ecosystem relies more on developer trust and a smaller community to function as it does and with most addons (whether official or unofficially obtained) being open-source, it is easier to detect malicious intent. While Chrome tries to provide security by locking down their addon ecosystem which may me more feasible at the scale that they are working at, though the results from the VirusTotal scans show that many addons are still very suspicious despite Google trying to lock down the ecosystem even more and addons going through Google's review process.

References

[1] Google, "Chrome web store — extensions," Chrome for Developers, 2024. [Online]. Available: https://developer.chrome.com/docs/webstore

[2] J. Lazar, A. Allen, J. Kleinman, and C. Malarkey, "What frustrates screen reader users on the web: A study of 100 blind users," *International Journal of Human-Computer Interaction*, vol. 22, pp. 247–269, 05 2007. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/10447310709336964

[3] F. Momotaz, M. T. Islam, M. Ehtesham-Ul-Haque, and S. M. Billah, "Understanding screen readers' plugins," *ScholarSphere (Penn State Libraries)*, 10 2021. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3441852.3471205

[4] T. Candela, "Part 1 of 5," The American Foundation for the Blind, 04 2005. [Online]. Available: https://www.afb.org/blindness-and-low-vision/using-technology/interviews-technology-pioneers/deane-blazie/part-1-5

[5] ——, "Ted henter," The American Foundation for the Blind, 04 2004. [Online]. Available: https://www.afb.org/blindness-and-low-vision/using-technology/interviews-technology-pioneers/ted-henter

[6] WebAIM, "Webaim: Screen reader user survey 10 results," webaim.org, 02 2024. [Online]. Available: https://webaim.org/projects/screenreadersurvey10/#primary

[7] E. Cussen, "A screen reader for everyone: why the world needs nvda," Media Access Australia, 03 2012. [Online]. Available: https://mediaaccess.org.au/latest_news/general/a-screen-reader-for-everyone-why-the-world-needs-nvda

[8] NVDA, "What's new in nvda," NV Access, 07 2024. [Online]. Available: https://www.nvaccess.org/files/nvda/releases/2019.1.1/nvda_2019.1.1_changes.html

[9] ——, "nvaccess/addon-datastore/docs/dev/submissionreview.md," GitHub, 05 2024. [Online]. Available: https://github.com/nvaccess/addon-datastore/blob/master/docs/dev/submissionReview.md#approving-an-author-to-submit-to-a-particular-add-on-id-for-the-first-time

[10] StatCounter, "Desktop browser market share worldwide — statcounter global stats," StatCounter Global Stats, 06 2024. [Online]. Available: https://gs.statcounter.com/browser-market-share/desktop/worldwide

[11] Google, "What are extensions? — manifest v2," Chrome for Developers, 02 2013. [Online]. Available: https://developer.chrome.com/docs/extensions/mv2/overview#:~:text=Extensions%20are%20small%20software%20programs

[12] Microsoft, "About browser extensions (internet explorer)," learn.microsoft.com, 08 2017. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/aa753620(v=vs.85)

[13] J. Villalobos, "Upcoming changes in compatibility features – mozilla add-ons community blog," Mozilla Add-ons Community Blog, 08 2017. [Online]. Available: https://blog.mozilla.org/addons/2017/08/10/upcoming-changes-compatibility/

[14] W. Team, "Webextensions community group," W3.org, 04 2023. [Online]. Available: https://www.w3.org/community/webextensions/

[15] J. M. Clarke, M. Mehrnezhad, and E. Toreini, "Invisible, unreadable, and inaudible cookie notices: An evaluation of cookie notices for users with visual impairments," *ACM transactions on accessible computing*, vol. 17, pp. 1–39, 03 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3641281

[16] C. Kearney-Volpe and A. Hurst, "Accessible web development," *ACM Transactions on Accessible Computing*, vol. 14, pp. 1–32, 07 2021. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3458024

[17] A. Khare, S. Dutta, Z. Li, A. Solko-Breslin, R. Alur, and M. Naik, "Understanding the effectiveness of large language models in detecting security vulnerabilities," 06 2024. [Online]. Available: https://arxiv.org/pdf/2311.16169

[18] K. Bridge, hickeys, and msatranjr, "How active accessibility works," Microsoft, 01 2024. [Online]. Available: https://learn.microsoft.com/en-us/windows/win32/winauto/how-active-accessibility-works

[19] NVDA, "addon-datastore/docs/submitters/submissionguide.md at master · nvaccess/addon-datastore," GitHub, 04 2024. [On-

line]. Available: https://github.com/nvaccess/addon-datastore/blob/master/docs/submitters/submissionGuide.md#approval-process

[20] J. Kaya and J. Rickerd, "Security researchers partner with chrome to take down browser extension fraud network affecting millions of users." Cisco Duo, 02 2020. [Online]. Available: https://duo.com/labs/research/crxcavator-malvertising-2020

[21] D. Barnett, "Chrome users beware: Manifest v3 is deceitful and threatening," Electronic Frontier Foundation, 12 2021. [Online]. Available: https://www.eff.org/deeplinks/2021/12/chrome-users-beware-manifest-v3-deceitful-and-threatening

[22] K. Borgolte and N. Feamster, "Understanding the performance costs and benefits of privacy-focused browser extensions," *Proceedings of The Web Conference 2020*, 04 2020. [Online]. Available: https://doi.org/10.1145/3366423.3380292

[23] E. Athanasopoulos and B. Mennink, *Information Security*. Springer Science+Business Media, 11 2023. [Online]. Available: https://doi.org/10.1007/978-3-031-49187-0

[24] VirusTotal, "How it works," VirusTotal, 12 2023. [Online]. Available: https://docs.virustotal.com/docs/how-it-works

[25] K. Van Liebergen, J. Caballero, P. Kotzias, and C. Gates, "A deep dive into virustotal: Characterizing and clustering a massive file feed," 10 2022. [Online]. Available: https://arxiv.org/pdf/2210.15973

[26] NVDA, "nvaccess/addon-datastore," GitHub, 06 2024. [Online]. Available: https://github.com/nvaccess/addon-datastore

[27] "Archive nvda-addon," Telegram, 12 2021. [Online]. Available: https://t.me/s/nvda_addon

[28] CroxyProxy, "Privacy policy — croxyproxy," Croxyproxy.com, 2024. [Online]. Available: https://www.croxyproxy.com/privacy

[29] sillyfire, "Security concerns with v2rayn-with-core," GitHub, 03 2024. [Online]. Available: https://github.com/2dust/v2rayN/issues/4832

[30] kvark128, "Wlanreporter/addon/globalplugins/wlanreporter/wlanapi.py at master · kvark128/wlanreporter," GitHub, 03 2023. [Online]. Available: https://github.com/kvark128/WlanReporter/blob/master/addon/globalPlugins/WlanReporter/wlanapi.py

[31] CISCO, "Cisco popularity list," s3-us-west-1.amazonaws.com, 2016. [Online]. Available: https://s3-us-west-1.amazonaws.com/umbrella-static/index.html

[32] M. Giladi and G. David, "Over 100,000 infected repos found on github," Apiiro, 02 2024. [Online]. Available: https://apiiro.com/blog/malicious-code-campaign-github-repo-confusion-attack/

[33] C. Point, "Threatcloud ai," Check Point Software. [Online]. Available: https://www.checkpoint.com/ai/threatcloud/

[34] S. Pilici, "Remove trojan:win32/tibia.gcx!mtb trojan [virus removal]," malwaretips, 02 2023. [Online]. Available: https://malwaretips.com/blogs/remove-trojanwin32-tibia-gcxmtb-trojan/

[35] ——, "How to remove adware.agent adware (virus removal guide)," malwaretips, 10 2017. [Online]. Available: https://malwaretips.com/blogs/remove-adware-agent/

9 Appendix

9.1 NVDA Telegram addon results

Addon ID	Publisher	Version	Wireshark result	VirusTotal result	Compatible?	Addon works?	GitHub link?
zUtilidades-para-NVDA	ruifontes	0.2.2	Clean	Clean	No	Yes	Yes
zRadio	hxebolax	0.5.3	Clean	Clean	No	No	Yes
zPod	hxebolax	0.1.5	Clean	Clean	No	No	Yes
zoom Enhancements	Mohammad Suliman	1.1.1	Clean	Clean	No	No	No
zararadio	Marcos Antonio de Oliveira	1.0	Clean	Clean	No	No	No
YYPatch		1.0.2	Clean	Clean	No	No	No
youtube_subtitle_reader		beta5	Clean	Clean	No	Yes	No
YoutubePlay	Dalison	1.5	Clean	Clean	No	No	Yes
YandexTranslate	alekssamos	2021.19.14	translate.yandex.ru	Clean	No	No	Yes
WorldVoice	Tseng Woody	2.2	Clean	Clean	No	No	Yes
wordNav	Tony Malykh	1.4	Clean	Clean	No	Yes	Yes
wordAccess Enhancement	paulber19	3.0	Clean	Clean	No	No	No
wlmail	Daniel Poiraud	3.2	Clean	Script.Ks.Malware.10590	No	No	No
WlanReporter	Kvark	2021.07.28	Clean	Script.Ks.Malware.10590	No	Yes	Yes

virtualCopy	Tyler Spivey	1.0	Clean	Clean	No	No	No
winWizard	Oriol Gomez	5.0.3	Clean	Clean	No	Yes	Yes
wintenApps	Joseph Lee	21.09	Clean	Clean	No	No	No
winMag	Cyrille Bougot	1.1	Clean	Clean	No	Yes	Yes
winGlulxe	NA	NA	NA	Clean	NA	NA	NA
winExplore	Daniel Poiraud	4.5.2	Clean	Clean	No	Unclear	No
WindowsMail	Daniel Poiraud	3.2	Clean	Script.Ks. Malware.10590	No	Unclear	No
Windows Frotz	Nick Stockton	1.2	Clean	Clean	No	NA	No
Winboard	Javi Dominguez	dev-2018 1021.1353	Clean	Clean	No	NA	No
WiFiFileSender	Eugene Poplavsky	1.6	Clean	Clean	No	NA	No
whiteNoise	Alberto Zanella	0.1	Clean	Clean	No	No	No
WhatsApp-desktop	Gerardo Kessler	2.2134 .10	Clean	Clean	No	No	Yes
webAccess	Frédéric Brugnot	2021. 06.01	Clean	Clean	No	Unclear	No
WeatherWatcher Live	Doug Lee	1.0	Clean	Clean	No	Unclear	No
Weather_Plus	Adriano Barbieri	8.5	veloroutes .org	Clean	No	Yes	No
VSCode	André-Abush Clause	20. 05.04 :341d 96a	Clean	Clean	No	No	No
volume_on_startup		beta2	Clear (passive analysis)	Clean	No	NA	No
VolumeManager	Danstiv	0.1	Clean	Clean	No	Yes	No
volumeAdjustment	Oleksandr Gryshchenko	1.3.2	Clean	Clean	No	No	Yes

voiceover-sounds	Tiflogroop	1.2	Clean	Clean	No	Unclear	No
voice over by technology and news	technology and news	1.0	Clean	Clean	No	Yes	No
VLC	Javi Dominguez	2.12	Clean	Clean	No	Yes	No
VLCAccess Enhancement	PaulBer19	2.6	Clean	Clean	No	No	No
visualStudio	mohammad suliman	1.0	Clean	Clean	No	No	No
virtualRevision	Rui Batista	21.06	Clean	Clean	No	No	No
virtualCopy	Tyler Spivey	1.0	Clean	Clean	No	No	No
Ventrilo	Ruslan, Beqa Gozalishvili	1.0	Clean	Clean	No	No	No
VAC	Doug Lee	2021.1.1	Clean	Clean	No	No	No
userParams	Unknown	1.0	Clean	Clean	No	Yes	No
USA-V	NA	NA	NA	Clean	NA	NA	NA
updateChannel	Jose Manuel Delicado	1.0	Clean	Clean	No	Yes	Yes
Unspoken	Camlorn	0.6	Clean	Clean	No	No	No
unmute	Oleksandr Gryshchenko	1.5.5	Clean	Clean	No	No	Yes
unigram	Gerardo Kessler	0.5	Clean	Clean	No	Yes	Yes
unicornNVDA	Babbage B.V.	4.21.1	Clean	Clean	No	Unclear	No
unicodeBraille Input	Mesar Hameed	3.2	Clean	Clean	No	Yes	No

Additional notes:

- YYPatch: Windows threw an error message about a stack-based buffer
- wintenApps: Windows threw an error message about a stack-based buffer
- winGlulxe: Error: Failed to open add-on package file
- Windows Frotz: Not fully testable due to not having a number pad on keyboard
- Winboard: Winboard is not a program that is downloadable anymore. Trying to download from the official site (http://hgm.nubati.net/) gives an SQL error
- WiFiFileSender: Unclear what file sender application this addon works with as there is no GitHub link nor addon description in NVDA
- webAccess: Unclear what the decription "Web application modules support for modern or complex web sites." entails
- WeatherWatcherLive: Not sure how to use the addon based on the slim description "Makes NVDA work better with treeview controls."
- Weather_Plus: Windows threw an error message about a stack-based buffer
- volume_on_startup: Not properly testable via wireshark as activation occurs on computer startup
- voiceover-sounds: "swoosh" noises heard when minimising and maximising windows. Unsure if it is the intended effect of addon
- virtualCopy: Windows threw an error message about a stack-based buffer
- Ventrilo: Only works with older Ventrilo client which is unavilable now
- userParams: Author name is blank
- USA-V: Addon completes indtallation but does not show up in "installed addons" list
- unmute: Windows threw an error message about a stack-based buffer
- unicornNVDA: Unsure what the addon does specifically

9.2 NVDA Addon Store results

Addon ID	**Publisher**	**Version**	**Wireshark result**	**VirusTotal result (file)**	**VirusTotal result (Git-Hub)**	**Compatible?**	**Addon works?**	**Git-Hub link?**
Access8Math	Tseng Woody	4.1.1	Clean	Clean	Clean	Yes	Yes	Yes
agenda	Rui Fontes	2024.-03.21	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
addonUpdater	josephsl	24.2.4	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
addonsHelp	Rui Fontes	2024.-03.20	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
TranslateAdvanced	hxebolax	2024.-06.23	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
AIContentDescriber	Carter Temm	2024.-05.22	Clean	Clean	Clean	Yes	Yes	Yes
AiSound5	NVDACN	24.04	Clean	Clean	Antiy-AVL	Yes	Unclear	Yes
alzaker	ahmed samy	1.2.2	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
androidStudio	Quin Gillespie	2024.1	Clean	Clean	Clean	Yes	Unclear	Yes
applicationDictionary	Rui Fontes	2024.-03.21	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes

nvdaChatGPT	Satoshi Suzuki	2022.1	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
audioManager	huaiyinfeilong	1.0.7	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
AVC	Rainer Brell	2024.-06.24	Clean	Clean	Antiy-AVL	Yes	No	Yes
audiocinemateca	hxebolax	1.3	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
Autoclip	Mazen	1.2.0	Clean	Clean	Antiy-AVL	Yes	No	Yes
baiduTranslation	huaiyinfeilong	1.7.5	api.fanyi.baidu.com	Clean	Clean	Yes	No	Yes
Banking4W	Rainer Brell	2024.-03.20	Clean	Clean	Clean	Yes	Unclear	Yes
BasicYoutubeDownloader	Bora FIRLANGEÇ	2.0.2	Clean	Clean	Clean	Yes	Yes	Yes
BMI	Edilberto Fonseca	2024.-04.15	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
calibre	Javi Dominguez	2024.-1.1	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
charInfo	Cyrille Bougot	3.1	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
ime_expressive	NVDACN	2024.-3.21	Clean	Clean	Antiy-AVL	Yes	Unclear	Yes
clipContentsDesigner	nvdaes	37.0.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
clipboardEnhancement	Cary-rowen	2.9.0	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
clipspeak	Rui Fontes	2024.-03.21	Clean	Clean	Clean	Yes	Yes	Yes

clock	Zvonimir stanecic	25.05.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
commandHelper	Javi Dominguez	2024.-1.1	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
consoleToolkit	Tony Malykh	1.4	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
controlUsage-Assistant	nvdaes	2024-0623.-0.0	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
wordCount	Rui Fontes	2024.-03.24	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
contador	Marco Leija	2.0.2	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
crypto_info	alekssamos	2024.-02.18	api.coin-cap.io	Clean	Antiy-AVL	Yes	Yes	Yes
CurrencyConverter	mesteranas	1.0	goog-le.com	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
cursorLocator	nvdaes	14.0.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
customBrowse-Mode	nvdaes	1.0.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
customNotifi-cations	nvdaes	7.0.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes

dayOfTheWeek	abdel792	2024-0507.-0.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
decimal2fraction	tech	1.2	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
dictionaries	Rui Fontes	2024.-03.21	Clean	Clean	Clean	Yes	Yes	Yes
directLink	Fawaz Abdul Rahman	2.2	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
dropbox	Rui Fontes	2024.-03.21	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
dual_voice	Mahmood-Taghavi	5.3	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
easyTableNavigator	Corentin Bacqué-Cazenave	2.5	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
easyNavigation	Javi Dominguez	2024.-1.0	Clean	Clean	ArcSight Threat Intelligence	Yes	Yes	Yes
eclipseEnhance	albzan	2024.1	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
edico	Alberto Zanella	1.3	Clean	Clean	Antiy-AVL	Yes	Unclear	Yes
emoticons	nvdaes	29.0.0	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
eMule	nvdaes	17.0.0	Clean	Clean	Antiy-AVL	Yes	Yes	Yes
enhanced-Annotations	nvdaes	16.0.0	Clean	Clean	Clean	Yes	Yes	Yes
Enhanced-Dictionaries	Marlon Sousa	1.5.0	Clean	Clean	Antiy-AVL	Yes	Yes	Yes

Additional notes:

- AiSound5: Unsure on how to activate addon with no information provided on GitHub
- alzaker: Works partially
- androidStudio: Github doesn't state how to use addon
- Banking4W: Unable to properly test due to vague github instructions
- BMI: Addon dialogue box doesn't display properly
- ime_expressive: Unable to properly test due to full addon functionality only working in full chinese environments
- edico: Github instructions unlcear on how to use addon
- emoticons: Windows threw an error message about a stack-based buffer

9.3 Chrome Web Store results

Addon name	**Publisher**	**Version**	**VirusTotal result**	**Chrome dev tools result**	**Privacy Policy**	**Compatible?**	**Addon works?**	**GitHub link?**
Dark Reader	Dark Reader Ltd	4.9.88	Clean	Clean	FDC	Yes	Yes	Yes
BTRoblox	None	3.6.4	Clean	Clean	FDC	Yes	Yes	Yes
Read Aloud: A Text to Speech Voice Reader	Business	2.11.0	Clean	Clean	FDC	Yes	Yes	No
Dark Mode for Web	Wayne Price	1.0.7	Clean	Clean	FDC	Yes	Yes	No
RoPro - Enhance Your Roblox Experience	RoPro Software Corporation	1.5.-10.2	Clean	https://ropro.io/api-/getServer-Locations.php?placeid=286090-429, https://ropro.io/-api/getServer-Locations.-php?placeid-=286090429	FDC	Yes	Yes	No
Allow right click - simple copy	Allow copy-&select	1.0.5	Trojan.-Win32.-Tibia.-DYZ	Clean	FDC	Yes	Yes	No
Video Speed Up Controller for Chrome	Video tools	1.5	Clean	Clean	FDC	Yes	Yes	No
Adblock all advertisement - No Ads extension	NoAds application	1.6.11	Adware.AdInject/-JS!1.F11C (CLASSIC)	Clean	FDC	Yes	Yes	No

Copyfish Free OCR Software	a9t9 software GmbH	6.0.9	Clean	Clean	FDC	Yes	Yes	No
VPN-free.pro - Free Unlimited VPN	rormibrge	3	Clean	Clean	FDC	Yes	Yes	No
Floating Video Player	Sylvia Stair	1.4.16	JS/Adware.-Chromex.-Agent.Y	Clean	FDC	Yes	Yes	No
Speed Dial [FVD] - New Tab Page, 3D, Sync...	Apptitude LLC	81.7.9	Clean	Clean	Web history, Website content	Yes	Yes	No
Super-Copy, Allow Right Click and Copy	SuperCopy	0.1.14	Clean	Clean	FDC	Yes	Yes	No
WAVE Evaluation Tool	Utah State University	3.2.5.3	Clean	Clean	FDC	Yes	Yes	No
Free privacy connection - VPN guru	henriksumkates	0.8	JS/Adware.-Chromex.-Agent.AA	Clean	FDC	Yes	Yes	No
RoGold - Level Up Roblox	RoGold	1.6.3	Clean	Clean	FDC	Yes	Yes	No
Postlight Reader	Postlight	11	Clean	Clean	FDC	Yes	Yes	No
Location Guard	Kostas Chatzikokolakis	2.5.0	Clean	Clean	FDC	Yes	Yes	No
Flash Player that Works!	Flash Emulator	0.0.3	Clean	Clean	FDC	Yes	No	No
Reader Mode	Reader Mode	1.5.0	Clean	Clean	FDC	Yes	Yes	No
Dark Mode - Night Eye	Promotino Ltd.	5.2.1	Clean	Clean	FDC	Yes	Yes	No

Substital: Add subtitles to videos and movies	None	2.7.0	Clean	Clean	FDC	Yes	Yes	No
Use Immersive Reader on Websites	cws-extension-publishers	1.201	Clean	Clean	FDC	Yes	Yes	No
Night shift mode	None	1.0.9	Clean	palette-picker.css	FDC	Yes	Yes	No
Free VPN	CMO Ltd	2.6.10	Clean	Clean	FDC	Yes	Yes	No
I don't care about cookies	Gen Digital Inc	3.5.1	Clean	Clean	FDC	Yes	Yes	No
Cleaner - history & cache clean	Smart extension	1.1.31	JS/Chromex-.Agent.A Potentially Unwanted, Adware.Open-ab/JS!1.F122 (CLASSIC)	Clean	FDC	Yes	Yes	No
Sound Booster	Sound Master	1.0.2	JS/Chromex-.Agent.BZ, Google: Detected, Trojan.JS-.Chromex, Adware.OpenTab/JS!1-.F122 (CLASSIC)	Clean	FDC	Yes	Yes	No
Charcoal: Dark Mode for Messenger	Andrew Millman	1.5.0	Clean	Clean	FDC	Yes	Yes	No
Dark Mode Chrome	None	1.0.47	Clean	Clean	FDC	Yes	Yes	No
Ads Blocker	None	7.1.6	Clean	Clean	FDC	Yes	Yes	No
RoSeal - Augmented Roblox Experience	None	1.3.44	Clean	Clean	FDC	Yes	Yes	No

History Shortcut	None	1.0.12	Clean	Clean	FDC	Yes	Yes	No
Darkness - Beautiful Dark Themes	Lifehack Labs LLC	3.0.0	Clean	Clean	FDC	Yes	No	No
Call Timer for Meet	Walter Radduso	3.0.1	Clean	Clean	FDC	Yes	Yes	No
AudioPick	None	0.3.10	Clean	Clean	FDC	Yes	Yes	Yes
Text Zoom: Reading Mode	Balaj Zain	1.1.4	Clean	Clean	FDC	Yes	Yes	No
CroxyProxy Free Web Proxy	None	0.99-.26.1	Not-a-virus:HEUR-:AdWare.Script.Ext-Redirect.gen	**	FDC	Yes	Yes	No
Helperbird: Accessibility & Productivity App	Helperbird	2024.7-.22	Clean	Clean	FDC	Yes	Yes	No
Dark Mode Google Docs	DarkMode	4.9.53	Clean	Clean	FDC	Yes	Yes	No
Midnight Lizard	None	10.7.0	Malware.U-.Generic-MC.cc	Clean	FDC	Yes	Yes	Yes
Sweet VPN	VPN Developer	1.1.4	JS/Adware-.Chromex-.Agent.AA	Clean	FDC	Yes	Yes	No
Dark Mode - Dark Reader for Chrome	None	1.0.3	Clean	Clean	FDC	Yes	Yes	No
Scrollbar Customizer	play.ka2n	1.3.3	Clean	Clean	FDC	Yes	Yes	No

Additional notes:

- *FDC Stands for "Functional Data Collection" to indicate that the only data collected is that needed only for addon functionality. This is due the store page for these addons stating that data is "Not being sold to third parties, outside of the approved use cases, not being used or transferred for purposes that are unrelated to the item's core functionality and not being used or transferred to determine creditworthiness or for lending purposes"
- ** https://www.google-analytics.com/g/collect?__cpo=1 &v=2&en=page_view&tid=G-0WD9HNFY6Z&cid=1722782209.447132652& dh=www.bbc.co.uk&ul=en-GB&dt=BBC+-.

9.4 Wireshark capture data

https://github.com/KashiDashi/MSc-Project-Wireshark-Captures