University of Virginia Library Chrome Extension

Understanding the Threats of Malicious Browser Extension

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Yukesh Sitoula

October 31, 2019

Technical Project Team Members
Ryan Kelly, Tho Nguyen, Ben Ormond, Nitesh Parajuli, Ben Spector, & Ashish Upadhyaya

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: Yukesh Sitoula Date: 11/24/2019

Approved: Catherine D. Baritaud Date: 12/2/2019
Catherine D. Baritaud, STS Division, Department of Engineering and Society

Approved: Ahmed Ibrahim Date: 11/26/2019
Ahmed Ibrahim, Department of Computer Science

The Internet was invented few decades ago, and it has already become one of the most prominent technology in the world. As of July 2019, over 4.33 billion people, which covers approximately 56 percent of the global population, actively use Internet (Clement, 2019). The Internet has revolutionized educational sectors by improving the quality of education. It has opened the doorways to a wealth of information, knowledge and educational resources by increasing opportunities for students to learn educational materials in and beyond the classroom ("Internet Access and Education", 2017). That does not mean all the resources and information in the Internet are free-of-cost, but many costly resources are available in the University library for free-to-use for students and staff. The technical project creates a web browser extension for the University of Virginia's library which will notify students and staff about the resources available in the university library so that they do not waste their money for the resources that can be obtained free-of-cost from the University library. Tightly coupled, the Science, Technology, and Society (STS) research topic will focus on understanding the threats of malicious browser extension.

The technical project will be developed in the course of two semesters, the Fall of 2019 and the Spring of 2020. The capstone course will be directed by Professor Ahmed Ibrahim, an assistant professor at the University of Virginia at the Department of Computer Science. During the course of two semesters, the team members will meet with the customer, University of Virginia Library, at Alderman Library bi-weekly and discuss about the project. During these meetings, we, the developer, will show the progress we have made on the extension, and the customers, Robin Ruggaber, Jasmin Perez, and Doug Chestnut, will provide their feedbacks. The STS research project will be conducted independently.

UNIVERSITY OF VIRGINIA LIBRARY CHROME EXTENSION

At the University of Virginia (UVA), a wide range of resources are available to both members of the library system and guests, yet knowledge of these resources is still limited for many. The UVA library system has access to a multitude of physical and online resources including books, movies, and other databases. However, as reported by the University of Virginia Library Statistics Report (2017), the total number of people using the library has reduced from 104,280 in 2010/11 to 72,938 in 2016/17. According to a survey of both graduate and undergraduate students conducted by UVA, around 35-40% only occasionally use physical library materials, and another 33-37% never take advantage of them (Public Report: Qualtrics Survey Software, n.d.). According to Ms. Robin Ruggaber (personal communication, September 18, 2019), Director of Strategic Technology Partnerships & Initiatives at the UVA Library, the main reason behind this problem is that people are not aware that these resources are being offered by the library. Many researchers and casual users alike often seek out some of these same resources through more convenient online methods of access through sites like Amazon, Google Scholar, or Netflix, which are available for free at the library. This means that content consumers often pay a fee for the convenience that is provided to them by accessing material that they unknowingly have access to for free. To solve this problem, our team is developing a Google Chrome browser extension which recommends items from the UVA library system whenever an item is searched that the UVA library may have access to in its system.

The aforementioned resource knowledge deficit is something that has been addressed in the past, and needs to be tackled again. Roughly a decade ago, a browser extension was created that made recommendations of library resources to its users, presenting them with materials that

corresponded to what they were presently viewing online. By automatically querying the plethora of library databases and catalogs for relevant results, the extension worked to better inform its users, saving them both time and, potentially, money in their everyday content searching. This existing extension is regrettably no longer functional or available, prompting the library to request the creation of an updated version, in the form of a Google Chrome browser extension. My teammates and I will be working to implement this updated version over the 2019-2020 academic year, with improved functionality and more features. Bringing back such a service will boost the visibility of lesser-known resources, and once again help individuals within the UVA community to potentially save both time and book-buying money.

The benefits that such a browser extension yields to its users are plentiful, not only including the reduction of resource ignorance, but also an easily-expandable platform for future improvements and expansions. The development of an extension for the most popular web browser on the internet that will automatically appear on search will make access to UVA library resources highly convenient ("Browser Market Share", 2019, "Browser Market Share Worldwide", 2019). This convenience will be compounded by the inclusion of login functionality, allowing for automatic authentication of users, yielding immediate digital resource access. By providing access to free resources through member accounts, and some free resources for the public, we would be saving many users the potential cost of paying for a product on a site like Amazon. In all of these manners, our extension would both save users time and the costs of accessing these resources through other methods. The extensions is embedded within the Chrome browser which eliminates the extra steps users have to take, such as traversing through the library website, then searching through the Virgo database and then obtaining the result.

In addition to casual users, academic researchers will benefit greatly from the institution of such a proposed tool. Students and researchers at the University of Virginia sometimes visit the library, only to discover that their desired material was either not available at the library or not in the library system at all. They then have to wait for it to become available or request an interlibrary loan (ILL). With the addition of our Google Chrome extension, a researcher will be able to see the availability of an item at the library through their web browser and potentially request ILL immediately. This will save researchers precious time, meaning they will not have to go to the library to check availability and request ILL.

Lack of knowledge about the university resources and ease of online shopping are two of the most significant factors in the decline of use of the UVA library. The extension we are developing for the library suggests UVA library's books and resources to users while they are searching for books on Amazon, Barnes and Nobles, and Google Scholar. The extension will look over the webpages and look for keywords like ISBN, UPC, and product name, then suggest the relevant resources that are available in the UVA library in an interactive popup bar at the top of the browser containing information of the resources such as title, author, availability and location. Further, we will extend the project to use Machine Learning (ML) and Artificial Intelligence (AI) to suggest the book and train ML/AI based on the user's interaction with the suggestions.

After several client meetings and revision, we have come up with a list of requirements for the extension. These requirements, however, are not final: as we build the product using agile methodology, there is room for additional requirements or improvements coming from clients and test users' feedback.

Gathering system requirements is essential in building a meaningful product. It can easily provide an outline for what goals can be obtained and it can provide the steps needed to take in reaching the goal. Project management tools can be used to list those requirements and it can help manage tasks based on weekly or daily goals. Tools like Jira can aid in this process and it can also help assign different tasks to each team member. Processes like these are made possible because of adding requirements.

Minimum requirements for this project include:

- Searching for a book on Amazon, Barnes and Nobles and Google Scholar results in the extension showing a banner with the book name, author, availability or method of accessing the material and location of the library if available.
- Clicking the extension icon will also show the results of a search from the listed three websites. Also, users can do additional searches in the extension with search results shown below the search bar (in the extension).

Desired requirements:

- Using asynchronous functions to responds fast to users' browsing result.
- Embedding logging in users.

Optional requirements:

- Extending the chrome extension to search in other universities library.
- Using Machine Learning to analyze search history and show customized recommended books.

- Security of the extension to be further solidified, so users do not misuse the extension and cause any harm to the library database.

UNDERSTANDING THE THREATS OF MALICIOUS BROWSER EXTENSION

Every well-known modern web browser uses browser extensions to extend and modify their functionality. The browser extensions provide many additional features to the web browsers such as modifying web pages, accessing sensitive data, and many others. Modern web browsers allow users to download millions of extensions to enhance users' browsing experience. The browser extensions are very popular tool among web users. They are downloaded and used by hundreds of millions of users (Perrotta & Hao, 2018, p. 66). As the popularity of the browser extensions is growing, it has also attracted the attention of attackers. Many research studies have shown that many browser extensions available in the browser extension store are malicious. A survey conducted by Google researchers in 2015 concluded that nearly 10% of the total browser extensions submitted to the Chrome Web Store from January 2012 - 2015 to be malicious (Jagpal et al., 2015, p. 579).

Malicious browser extensions are one of the widespread problems in cybersecurity. These browser extensions are designed to harm users and steal users' personal data. The Google Chrome Web Store, which is the most popular store for extensions, does not screen extensions before they are published so it is very easy for cybercriminals to publish malicious browser extensions (Stillwagon, 2018). It is extremely hard for users to differentiate safe and legitimate browser extension from malicious browser extension. Most malicious browser extensions seem legitimate at first glance. Most average users, who does not have much technical knowledge, would not be able to identify malicious browser extension even after using it for a long time

because most browsers allow browser extensions to do anything by default allowing malicious browser extensions to perform tasks behind the scene without users' permission (Perekalin, 2018).

Research Methods

Even though the number of malicious browser extension is growing rapidly, this topic has not received much attention. It has received much less attention compared to common web security problems such as SQL injection, XSS, logic flaws, client-side vulnerabilities, drive-by-download, etc. (Shahriar, Weldemariam, Zulkernine, & Lutellier, 2014, p. 66). Since the browser extensions have the same level of privilege as the browser (Guha, Fredrikson, Livshits, & Swamy, 2011, p. 116), the successful attacks will result in big reward. Therefore, it is very important for web users to understand the consequences of installing a malicious browser extension. The objective of this research project is to understand the threats of malicious browser extensions by exploring the "Razy" malware, "Nigelify" browser extension, and malicious advertisement blocking extensions such as "AdBlock" and "uBlock".

A Windows malware named "Razy" uses browser extensions to commit a range of online scams to victims. Razy malware mostly spreads through affiliate networks. When the user downloads and installs software from free-file hosting services such as ZippyShare, Mediafire, MEGA, etc., these kind of softwares tend to sometimes load and install Razy malware (Seals, 2019). Once this malware is installed and executed, it will disable the integrity check for installed browser extensions, blocks the browser from updating, and then install malicious browser extension (Seals, 2019). This malware is only compatible with Google Chrome, Mozilla Firefox and Yandex Browser. It is mostly used for stealing cryptocurrency. It is capable of

looking for cryptocurrency wallets' addresses on websites and replacing the found addresses with the attackers' wallet addresses, substituting images of QR codes that points to wallets, displaying fake messages to the user in the web pages of cryptocurrency exchanges, and spoofing Google and Yandex search results (Vlasova & Bogdanov, 2019). Even though this malware is mostly related to the theft of cryptocurrency, it has potential to commit a range of attacks using malicious browser extension. Therefore, understanding the way this malware works and searching for the countermeasures against this malware will protect web users from being victims of many cybercrimes.

Speaking of malicious browser extension, the 'Nigelify' application is an active malicious browser extension that performs Facebook propagation, YouTube fraud, crypto mining, credentials thefts, and other nefarious actions. Nigelify is abused by the malware "Nigelthorn" to infect the victim's computer. The cybercriminal group behind this operation has been active from March of 2018 and has already infected over 100,000 users in more than 100 countries (Raff & Shapira, 2018). Nigelthorn malware only works on Google Chrome browser so it does not affect users using other browsers. The Nigelify browser extension works through links redirections. As seen in Figure 1, the malware redirects the user to a fake YouTube page which asks user to download malicious browser extension, and if the user install the browser extension, the computer will be a part of botnet. The attacker will have full access to the botnet device. This botnet machine can be used for variety of attacks such as distributed denial-of-service attack (DDoS attack), steal data, send spam, and many more. Therefore, the detail research on these kinds of browser extension, which is dangerous but still available for download from the official browser extension store, is very important to understand the threats of active

malicious browser extension, and protect ourselves from these kinds of "legitimate" browser extension.

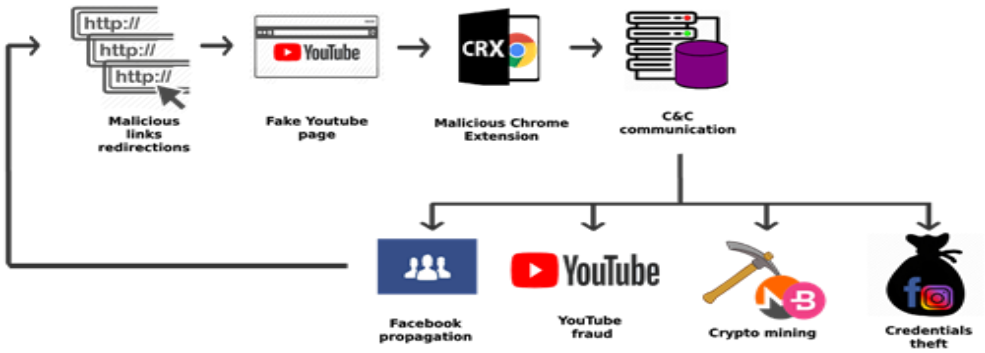

Figure 1: Nigelify infection process: This figure shows how Nigelify infection process works. (Raff & Shapira, 2018)

Even though most malicious browser extension like Nigelify, works with malware to perform the attack, some browser extension like 'AdBlock' and 'uBlock' work on their own. AdBlock and uBlock are malicious browser extension that were caught in ad fraud scheme. These browser extensions "impersonate legitimate extensions but instead engage in cookie stuffing to defraud affiliate marketing programs, a researcher has found" (Montalbano, 2019). Google immediately removed these two malicious browser extensions from Chrome Web Store after they were found. Since these two browser extensions defrauded the users, Google can follow the money trail and find the mastermind behind this ad fraud scheme. Google can prosecute the cybercriminal/s behind this scheme once found. In 2014, the eBay found Brain Dunning, a former eBay affiliate marketer, on a $35 million cookie-stuffing scam. He was prosecuted and sentenced to 15 months in federal prison (Montalbano, 2019).

'AdBlock' and 'uBlock' might not be the only malicious browser performing ad fraud scheme. In 2017, Google found some malicious browser extensions that were spoofing AdBlock

Plus and removed them. The ad fraud browser extension appears in the browser extension store every once in a while. Therefore, this research paper will thoroughly investigate the malicious browser extension performing ad fraud scheme, and provide precaution against these malicious browser extensions.

STS Framework

In order to understand the threats of malicious browser extension, this research paper will use Actor-Network Theory (ANT) framework. The ANT framework is different from other technological framework in a sense that it emphasizes and considers the presence of all factors, human and nonhuman, in the technological studies. The human and nonhuman factors are regarded as actors and the connections between these actors are called the network. This framework is perfect for researching this STS topic in-depth because it contains both, humans actants such as cybercriminals, users, etc., and nonhuman actants such as malicious browser extensions, malwares etc., that causes cybercrimes.

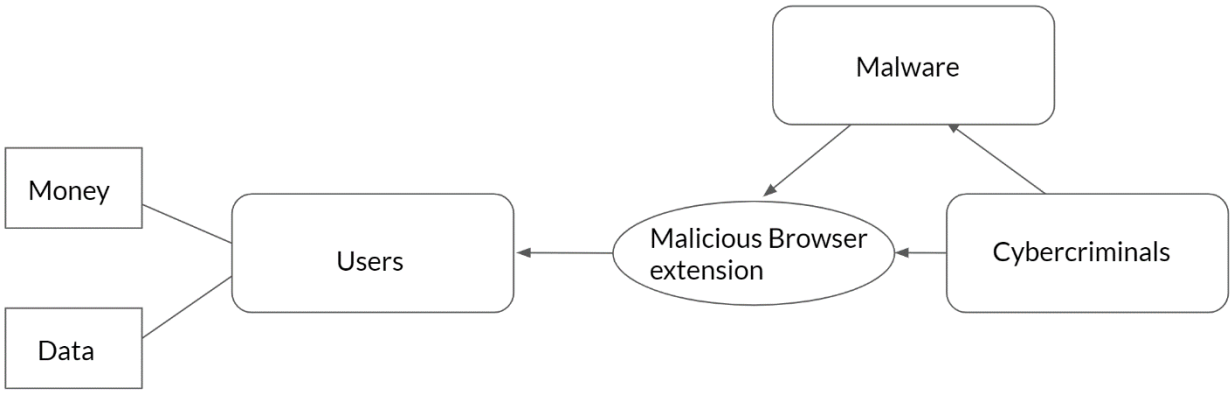

Figure 2: ANT model for analyzing Razy malware: This figure is responsible for understanding the actants and network in ANT framework for Razy malware study (Sitoula, 2019).

This research paper will use ANT framework to research Razy malware, Nigelify browser extensions and ad-blocking extensions, in-depth. In the Razy malware study, as seen in Figure 2, the actors are cybercriminals, malware, malicious browser extensions, and users. The cybercriminals target the users to obtain cryptocurrency and/or Google and Yandex search results. The malicious browser extension is the means for cybercriminals to perform the attack on users, and in order to install malicious browser extension, the cybercriminals uses Razy malware. Similar to Razy malware study, the actors in Nigelify browser extension study and the relation between these actors is same. As seen in Figure 3, the only difference is that Nigelify browser extension installs other malicious browser extension to perform different attacks. The actors in the ad-blocking extensions study are cybercriminals, malicious browser extension, and users. It is similar to the previous two cases, but this study does not have malware. The intention of each actors is same on all of these three research studies.

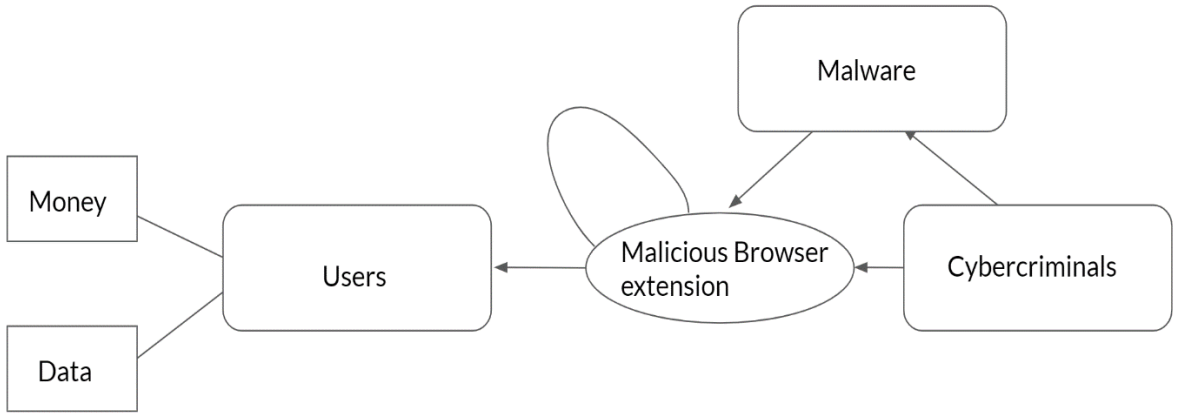

Figure 3: ANT model for analyzing Nigelify browser extension: This figure is responsible for understanding the actants and network in ANT framework for Nigelify browser extension study (Sitoula, 2019).

Expected outcomes and paper type

This research paper will focus on understanding the threats of malicious browser extension and providing web users with precautions. The purpose of this paper is to show the consequences of installing malicious browser extension. This paper is also expected to make readers check their installed browser extensions and make sure the extensions are not compromising their personal data. The research paper will be a scholarly article.

WORKS CITED

Browser Market Share (2019, September). Retrieved from https://www.netmarketshare.com/browser-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2C%22group%22%3A%22browser%22%2C%22sort%22%3A%7B%22share%22%3A-1%7D%2C%22id%22%3A%22browsersDesktop%22%2C%22dateInterval%22%3A%22Monthly%22%2C%22dateStart%22%3A%222018-10%22%2C%22dateEnd%22%3A%222019-09%22%2C%22segments%22%3A%22-1000%22%7D

Browser Market Share Worldwide - September 2019 (2019, September). Retrieved from https://gs.statcounter.com/browser-market-share

Clement, J. (2019, September 17). Worldwide digital population as of July 2019. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Guha, A., Fredrikson, M., Livshits, B., & Swamy, N. (2011). Verified Security for Browser Extensions. *2011 IEEE Symposium on Security and Privacy*. doi: 10.1109/sp.2011.36

Internet Access and Education: Key considerations for policy makers. (2017, November 20). In *Internet Society*. Retrieved from https://www.internetsociety.org/resources/doc/2017/internet-access-and-education/

Jagpal, N., Dingle, E., Gravel, J. P., Mavrommatis, P., Provos, N., Rajab, M. A., & Thomas, K. (2015, August). Trends and lessons from three years fighting malicious extensions. *24th USENIX Security Symposium.*

Montalbano, E. (2019, September 24). Malicious ad blockers for chrome caught in ad fraud scheme. *Threat post*. Retrieved from https://threatpost.com/malicious-ad-blockers-for-chrome-caught-in-ad-fraud-scheme/148591/

Perekalin, A. (2018, January 30). Why you should be careful with browser extensions. *Kaspersky daily*. Retrieved from https://www.kaspersky.com/blog/browser-extensions-security/20886/

Perrotta, R., & Hao, F. (2018, July 1). Botnet in the browser: Understanding threats caused by malicious browser extensions. *IEEE Security & Privacy*, 16(4), 66–81. doi: 10.1109/msp.2018.3111249

Public Report: Qualtrics Survey Software. (n.d.). Retrieved from https://virginia.az1.qualtrics.com/results/public/dmlyZ2luaWEtVVJfYmpZTkNLMXR0

M0hsaEl4LTVhY2NhZTI1OTIxMmY2MDAxMmRmYmZlOQ==#/pages/Page_1468e8d9-7db6-4432-9bf3-d4769bd1a958

Raff, A., & Shapira, Y. (2018, May 10). Nigelthorn malware abuses chrome extensions to cryptomine and steal data [Blog post]. *Radware*. Retrieved from https://blog.radware.com/security/2018/05/nigelthorn-malware-abuses-chrome-extensions/

Seals, T. (2019, January 25). Razy malware attacks browser extensions to steal cryptocurrency. *Threat post.* Retrieved from https://threatpost.com/razy-browser-extensions-theft/141181/

Shahriar, H., Weldemariam, K., Zulkernine, M., & Lutellier, T. (2014). Effective detection of vulnerable and malicious browser extensions. *Computers & Security*, 47, 66–84. doi: 10.1016/j.cose.2014.06.005

Sitoula, Y. (2019). *ANT model for analyzing Razy malware* [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia, Charlottesville, VA.

Sitoula, Y. (2019). *ANT model for analyzing Razy malware* [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia, Charlottesville, VA.

Stillwagon, A. (2018, August 21). Malicious browser extensions: What you should know. *Medium*. Retrieved from https://medium.com/redmorph/malicious-browser-extensions-what-you-should-know-cb7ecb477dbc

Vlasova, V., & Bogdanov, V. (2019, January 24). Razy in search of cryptocurrency. *Securelist*. Retrieved from https://securelist.com/razy-in-search-of-cryptocurrency/89485/