UNDERSTANDING THE THREATS OF MALICIOUS BROWSER EXTENSIONS

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Yukesh Sitoula

March 27, 2020

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.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

The Internet is one of the most prominent technologies in the world. As of January 2020, almost 4.54 billion people, which covers approximately 59 percent of the global population, were active internet users (Clement, 2020). It has changed the way people live, the way people interact with other people, the way people work, the way people study, the way people play, and many other essential aspects of human life. A web browser is used to access the Internet. Through a web browser, users have access to a wide range of services such as email, banking, shopping, and many others.

Every well-known modern web browser uses browser extensions to extend and modify its functionality. The browser extensions provide many additional features to web browsers such as modifying web pages, accessing sensitive data, and many others. While the user uses the web browser to perform a task such as shopping, the user confidential personal information such as credit card number, username, password, etc. are exposed to the browser (Bauer et al., 2014, p. 184). Since the browser extension has the same level of privilege as the browser, this sensitive personal information can also be accessed through browser extension (Liu et al., 2012, p. 1). Therefore, a browser developer with malicious intent will be able to steal user's sensitive personal information.

The browser extensions are a 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 many attackers. Research studies have shown that several 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 are malicious (Jagpal

et al., 2015, p. 579). These were the extensions that were found by Google. There might have been some malicious browser extensions which were gone unnoticed because it is impossible to have perfect security. Therefore, it is safe to assume that at least 1 in 10 browser extension is malicious.

A malicious browser extension is one of the widespread problems in cybersecurity. These browser extensions harm users and steal users' 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 easy for cybercriminals to publish malicious browser extensions (Stillwagon, 2018). It is hard for users to differentiate safe, legitimate browser extension from the malicious browser extension. Most malicious browser extensions seem genuine at first glance. Non-technical users may not be able to identify malicious browser extensions even after using them for a long time. Furthermore, most browsers allow browser extensions to use many functionalities listed in Table 1 on page 5 and 6, by default allowing malicious browser extensions to perform tasks behind the scene without users' permission (Perekalin, 2018).

Even though the number of malicious browser extensions is increasing, this topic has not received much attention from defense experts. The malicious browser extension problems have received much less attention compared to standard 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, the successful attacks will result in a big reward. Therefore, web users need to understand the consequences of installing a malicious browser extension. This research paper uses the Actor-Network Theory (ANT) framework to analyze the threats of a malicious

browser extension on users' privacy and how web users can minimize the possibility of an attack. Loosely coupled with the STS research paper, the technical project will develop a browser extension for the University of Virginia Library, and use relevant knowledge obtained from the STS research paper to develop a secure browser extension.

USING ACTOR-NETWORK THEORY (ANT) TO UNCOVER INVOLVED FACTORS

This research paper uses the Actor-Network Theory framework to understand the threats of a malicious browser extension in-depth. The ANT framework is different from other technological frameworks in the sense that it emphasizes and considers the presence of all factors, human and nonhuman, in technical studies. The human and nonhuman factors are actors, and the connection between these actors is called the network. This framework is perfect for researching and explaining this STS research topic because the topic contains both, humans actants such as cybercriminals, web users, browser developers, etc., and nonhuman actants such as malicious browser extension, malware, etc. Figure 1 summarizes the actants and the network in the ANT model for analyzing the malicious browser extension.

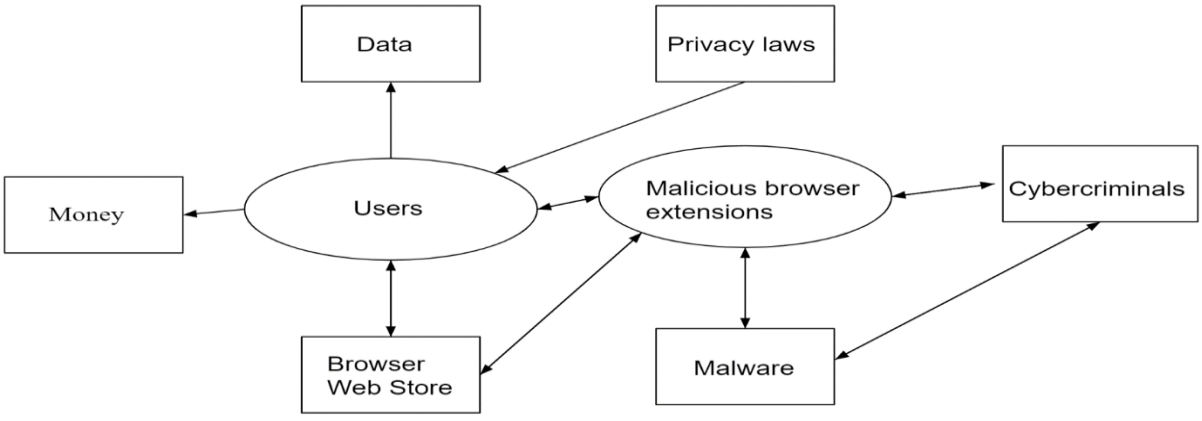

Figure 1: ANT model to analyze the malicious browser extension: This figure is responsible for understanding the actants and networks in the ANT framework (Sitoula, 2019).

As seen in Figure 1, cybercriminals are targeting the user's data and money. The cybercriminals use malicious browser extensions to target the users directly, or they use malware to install malicious browser extensions to attack web users. The malicious browser extensions get into web user's computer through the browser web store or other third-party websites. There are some laws protecting web users from the cybercrimes, but they are not enough to safeguard web users adequately.

RESEARCH QUESTION, MOTIVATIONS, AND METHODS

The specific research question I seek to answer is, "How can the web users protect their privacy given that the popularity of browser extension, as well as the number of a malicious browser extension, is rapidly increasing?" It is essential to answer this question because the cyberattacks are getting more sophisticated every day, and it is harder for average web users to protect their privacy more than ever before. To answer the research question, the following steps are examined:

1. Identify the security vulnerability of two of the most popular web browsers: Google Chrome, and Mozilla Firefox. It will help to explain how malicious browser extensions get inside the browser web store.
2. Explain the importance of privacy and different laws protecting web users' privacy.
3. Explain how some of the popular malicious browser extensions work and the capabilities of their attacks.
4. Provide general countermeasures web users can take to minimize the possibility of attacks via browser extensions.

RESULTS

Security Vulnerabilities of browsers: Google Chrome and Mozilla Firefox

Chrome and Firefox are two of the most popular browser extensions available. It is hard to find any computer which does not have either of these browsers. Table 1 summarizes the capability of the browser extensions that can compromise a user's security and privacy:

Table 1
Capabilities of the Browser Extensions that can Compromise a User's Security and Privacy

	Chrome	Firefox
DOM-based capabilities		
Read webpage's DOM	✓	✓
Edit webpage's DOM	✓	✓
Write to webpage's DOM	✓	✓
Replace webpage's DOM	✓	✓
Iframe-based phishing	✓	✓
JavaScript-based capabilities		
Crash browser	Partial	✓
Use of eval	Partial	Partial
XHR requests	✓	✓
Location data	✓	✓
Keystrokes	✓	✓
Mousestrokes and touchstrokes	✓	✓
Cookie capabilities		
Read cookies	✓	✓
Edit cookies	✓	✓
Delete cookies	✓	✓
Clipboard capabilities		
Read clipboard	✓	✓
Modify clipboard	✓	✓
Bookmark capabilities		
Read bookmarks	✓	✓
Add bookmarks	✓	✓
Edit bookmarks	✓	✓
Delete bookmarks	✓	✓

Browsing history capabilities		
Read history	✓	✓
Write to history	✓	✗
Delete history	✓	✗
File system capabilities		
Directory listing	✗	✓
Read files	✗	✓
Edit files	✗	✓
Delete files	✗	✓
Add new folders	Partial	✓
Add new files	Partial	✓
Execute processes	✗	✓
Extension management capabilities		
Disable extensions	✓	✗
Uninstall extensions	Partial	✓
Other capabilities		
Proxy settings	✓	✓
Browser preference	✗	✓
DDoS	✓	✓
Password manager	✗	✓
XPCOM usage	✗	✓
System library/API usage	✗	✓
Battery drain	✗	✗
Certificate exceptions	✗	✓

Note. Adapted from "Botnet in the browser: Understanding threats caused by malicious browser extensions," by R. Perrotta & F. Hao, 2018, *IEEE Security & Privacy*, 16(4), 66-81.

The malicious browser extensions, once installed, can easily compromise a user's security and privacy by abusing these over-privileged capabilities. For example: being able to modify a website's DOM allows malicious browser extension to make changes to the display of a website and deceive users into believing something false. "The change of the web page content may be subtle, but when it is combined with social engineering techniques, it can cause significant harm to user security" (Toreini, Shahandashti, Mehrnezhad, & Hao, 2019, p. 801-802). Similar to DOM-based capabilities, JavaScript-based capabilities are also extremely dangerous. Since a huge percentage of Web-based attacks use JavaScript, having JavaScript-

based capabilities allows browser extensions to perform these JavaScript web attacks. The JavaScript-based web attacks through browser extension are dangerous because browser extension has access to every website's users visit so it can attack every website every time users visits. Likewise, cookie capabilities allow browser extension to read, edit, and delete the cookie. The cookies are data files that websites use to "keep track of user movements within site, help [user] resume where [user] left off, remember [user] registered login, theme selection, preferences, and other customization functions" ("All about cookies", n.d.). The malicious browser extension can send cookies to the attacker, and the attacker can use these cookies to login to the users account on the website. Another vulnerable capability that is directly connected to users' privacy is browsing history capabilities. Since the browser allows browser extension to read, write, and delete history, the attacker can use a browser extension to steal users' online activities and compromise users' privacy. There are many other capabilities listed above in Table 1 that attackers can use. Still, these capabilities are rarely used in the web-based attacks, possibly because of improved security against these capabilities or low rewards compared to other capabilities attacks.

Laws protecting user's privacy

Few laws in the United States cover the Internet and the user's privacy. The 1974 Privacy Act arguably is the foundation of it all (NortonLifeLock, n.d.). According to the United States Department of Justice website, the Privacy Act of 1974 "establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies" (United States

Department of Justice, 2020). Additional laws and regulatory agencies affecting/protecting online privacy are outlined below:

1. The Federal Trade Commission Act (FTC) - 1914

   The FTC prohibits unfair practices from companies. It says, "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" (Federal Trade Commission Act, 2006, p. 3). It protects online users by bringing enforcement actions against companies if companies fail to comply with their privacy policies or to protect user's personal information.

2. Electronic Communications Privacy Act of 1986 (ECPA) - 1986

   The ECPA was passed in 1986. The law protects wire, oral, or electronic communication from the interception, use, disclosure, and procurement (Electronic Communications Privacy Act of 1986, 1986).

3. Computer Fraud and Abuse Act (CFAA) - 1986

   The CFAA was enacted in 1986 to address hacking. This law is the first federal computer fraud law. It introduces many computer-related offenses and punishments for those offenses. Some offenses include:

   a. Accessing a computer without authorization or exceeding authorized access and obtaining information
   b. Accessing a computer to defraud and obtain value
   c. Intentionally, recklessly, or negligently causing damage and loss to a protected computer
   d. Trafficking in passwords or similar information

e. Extortion involving computers (Computer Fraud and Abuse Act, 1986).

4. Financial Services Modernization Act (GLBA) - 1999

   The GLBA law was enacted in 1999. This law includes some changes in the financial industry. It requires financial sectors to provide clear disclosures on their privacy policies. It also requires industries to inform their customers if they share the customers' nonpublic information with third parties and affiliates. This law allows customers to disallow such information without their consent.

5. Children's Online Privacy Protection Act (COPPA) – 1998

   The COPPA was first enacted in 1998, which required Internet-connected entities that collect data of children under the age of 13, to comply with the FTC and obtain parental consent before collecting and using information. The COPPA was updated in 2013 to cover the collection of photos, videos, audio recordings, usernames, IP addresses, location data, and unique identification numbers associated with specific devices.

Even though these law tries to protect web users from many types of attacks, these laws are not enough to protect web users' privacy and reduce online attacks. It is tough to prosecute cybercriminals. There are some reasons for it. The first reason is that most of the time, cybercriminals are located outside of the country, outside of legal jurisdiction of the court, so even having enough legal evidence, identity, and location of the cybercriminal might not be enough to arrest the person. The second reason is that most cybercrimes are not reported. It is because most people do not know where and how to report internet crime, and even if they do, rarely anything comes out of it because it is hard to get bulletproof evidence of cybercrime (Grimes, 2016). There is also a problem with the lawmakers. Most lawmakers are not tech-savvy, and they do not understand what kinds of technical laws are needed and how much

restrictions need to be put in technical fields. The technical field is changing rapidly, but the laws are not able to keep up with it. Therefore, web users have to learn to become safe from the web attacks by themselves because the laws and government are not able to protect or defend them.

Popular malicious browser extensions

There are many malicious browser extensions in the browser web store. As mentioned earlier, approximately 10% of the Chrome Web Store browser extensions are malicious. This research paper explores Nigelify browser extension, malicious advertisement blocking extensions such as AdBlock and uBlock, and Razy malware that use browser extensions to exploit, to understand the threats of a malicious browser extension.

Many browser extensions are malicious, and when found, are removed from the browser web store. But some browser extensions have not been removed from the browser web store even after researchers discovered them conducting malicious acts. Nigelify browser extension is one of them. The Nigelify browser extension is an active browser extension that performs Facebook propagation, YouTube fraud, crypto mining, credential 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 since March of 2018 and has already infected over 100,000 users in more than 100 countries (Raff & Shapira, 2018). Nigelthorn malware only works on the Google Chrome browser, so it does not affect those using other browsers. The Nigelify browser extension works through links redirections. Figure 2 will help to understand this extension's infection process better. As seen in Figure 2, the malware redirects the user to a fake YouTube page, which asks the user to download the malicious browser extension. If the user installs the browser extension, the computer will be a part of a botnet. The

attacker will have full access to the botnet device. This botnet machine can be used for a variety of attacks such as distributed denial-of-service attacks (DDoS attacks), stealing data, sending spam, etc.

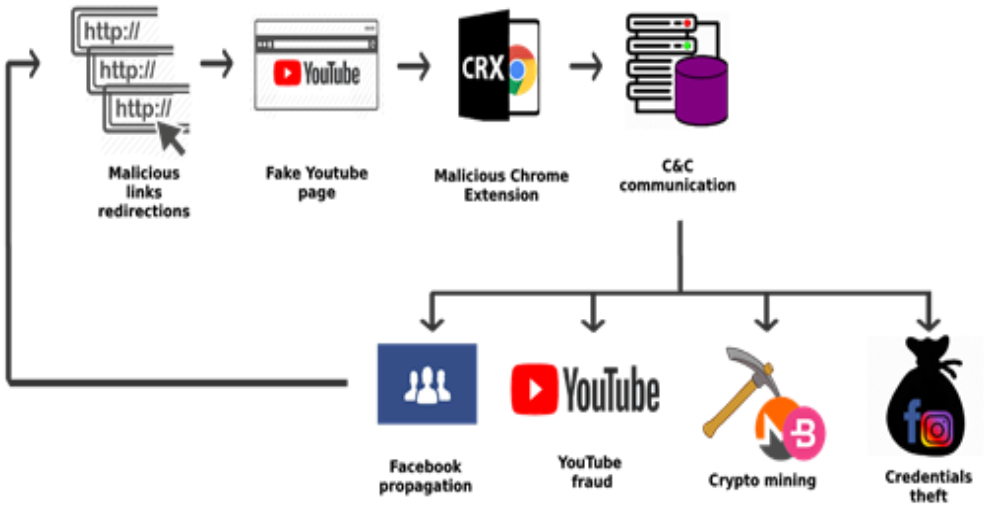

Figure 2: Nigelify infection process: This figure shows how the Nigelify infection process works. (Raff & Shapira, 2018)

Even though most malicious browser extensions like Nigelify works with malware to perform the attack, some browser extensions like "AdBlock" and "uBlock" worked on their own. AdBlock and uBlock were malicious browser extensions that were caught in an ad fraud scheme. Browser extensions like this "impersonate legitimate extensions but instead engage in cookie stuffing to defraud affiliate marketing programs" (Montalbano, 2019). Google immediately removed these two malicious browser extensions from Chrome Web Store after Google found them conducting malicious acts. AdBlock and uBlock might not be the only malicious browser extensions 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 web store every once in a while, so it is important for web users to only download and install browser extensions that are published by a verified legitimate company.

Most of the time, malicious browser extensions are downloaded by the web users without the knowledge of them being malicious. Other times, computer software might download malicious browser extensions without the user's knowledge. One of the malwares that installs malicious browser extension to a web user's computer is Razy malware. It uses browser extensions to commit a range of online scams to victims, and mostly spreads through affiliate networks. When the user downloads and installs software from free-file hosting services such as ZippyShare, Mediafire, MEGA, etc., these kinds of software sometimes tend to load and install Razy malware (Seals, 2019). Once this malware is installed and executed, it will disable the integrity check for installed browser extensions, block the browser from updating, and then install a malicious browser extension (Seals, 2019). This malware is only compatible with Google Chrome, Mozilla Firefox, and Yandex Browser. Cybercriminals mostly use this malware to steal cryptocurrency. Still, it is more than capable of looking for cryptocurrency wallets' addresses on websites and replacing the found addresses with the attacker' wallet addresses, substituting images of QR codes that point 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 the potential to commit a range of attacks using a malicious browser extension.

Countermeasures against malicious browser extensions

To protect the web users from the malicious browser extensions, it is important for both the web users and the browser developer to understand the countermeasures against the malicious browser extensions. The web users and the browser developer both have to do their

part of work to maximize the protection. Here are some practical countermeasures that the web users and browser developers can perform:

1. *Countermeasures for web users*

   There are multiple countermeasures that web users can take to minimize the damage from browser-extension based attacks.

   a. Do not download too many browser extensions. It will increase the chances of having malicious browser extensions, so narrow down the number to just a few useful ones.
   b. Do not download the browser extension from third party websites. Even though 1 in 10 browser extension is malicious in the browser web store, it is still much less dangerous than downloading from third party websites.
   c. Read and understand the permissions the browser extensions ask requires the web users to provide. Web users need to give just the right permissions so that the browser extension will not be able to do anything inappropriate.
   d. Install antivirus for the browser. It will detect and neutralize the most malicious code that is present in browser extensions.
   e. Download computer software from official websites. It reduces the chances of downloading malware like Razy malware.

2. *Countermeasures for browser*

   Similar to the countermeasures taken by many web users, the browser developer can also include few features in the browser that detects malicious behavior. Here are some countermeasures that browser developers might find useful:

a. Detecting the spying behavior if the browser extension follows some sort of patterns. For example: when the browser extension steals social media access tokens when the user sign-in to the social media site (Aggarwal et al., 2018, p. 57).
b. Informing users if the browser extension uses and transmits data. This countermeasure will allow the web users to know what and how the browser extension is using the user's data.
c. Only granting permissions that are required for the browser extension to work. Many of the browser extension security threats come from browsers giving extra permissions to extensions components that are more than necessary for the extensions to work (Liu et al., 2012, p. 9).
d. Identifying sensitive information in the web pages, and classifying and protecting them based on their importance. For example, finding the password element and categorizing it as highly confidential information and make it so that only content scripts that have high-level permission access this input element (Liu et al., 2012, p. 9).

Since there are many browser security vulnerabilities, there are also many threats to web users. This paper only provides a few essential countermeasures that will reduce the most used browser extension-based attacks. But it is still vital for the browser developers and browser extension developers to understand the scope of their work and protect web users from any obvious security threats.

In conclusion, this research paper introduced the security vulnerabilities of Google Chrome and Mozilla Firefox while bringing attention to privacy laws protecting user's privacy,

popular malicious browser extensions, and countermeasures to protect from browser-extension based attack. The paper used the Actor-Network Theory framework to clearly explain the threats of malicious browser extension on user's privacy. Hopefully, readers will be more cautious while downloading malicious browser extensions, and other computer software, in future.

WORKS CITED

Aggarwal, A., Viswanath, B., Zhang, L., Kumar, S., Shah, A., & Kumaraguru, P. (2018). I spy with my little eye: Analysis and detection of spying browser extensions. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 47-61.

All about cookies. (n.d.). Retrieved from https://www.allaboutcookies.org/cookies/

Bauer, L., Cai, S., Jia, L., Passaro, T., & Tian, Y. (2014). Analyzing the dangers posed by Chrome extensions. *2014 IEEE Conference on Communications and Network Security*, 184-192.

Clement, J. (2020, February 3). Global digital population as of January 2020. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986). Retrieved from https://www.law.cornell.edu/uscode/text/18/1030#

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523 (1986). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006). Retrieved from https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf

Grimes, R. A. (2016, December 6). Why it's so hard to prosecute cyber criminals. *CSO*. Retrieved from https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

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

Liu, L., Zhang, X., Yan, G., & Chen, S. (2012). Chrome extensions: Threats analysis and countermeasures. *NDSS*, 1-16.

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/

NortonLifeLock employee. (n.d.) What are some of the laws regarding internet and data security? Retrieved from https://us.norton.com/internetsecurity-privacy-laws-regarding-internet-data-security.html

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

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/

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

Toreini, E., Shahandashti, S. F., Mehrnezhad, M., & Hao, F. (2019, June 11). DOMtegrity: Ensuring web page integrity against malicious browser extensions. *International Journal of Information Security*, 18, 801-814. DOI: 10.1007/s10207-109-00442-1.

United States Department of Justice. (2020, January 15). Privacy Act of 1974. Retrieved from https://www.justice.gov/opcl/privacy-act-1974

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

BIBLIOGRAPHY

Aggarwal, A., Viswanath, B., Zhang, L., Kumar, S., Shah, A., & Kumaraguru, P. (2018). I spy with my little eye: Analysis and detection of spying browser extensions. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 47-61.

All about cookies. (n.d.). Retrieved from https://www.allaboutcookies.org/cookies/

Bauer, L., Cai, S., Jia, L., Passaro, T., & Tian, Y. (2014). Analyzing the dangers posed by Chrome extensions. *2014 IEEE Conference on Communications and Network Security*, 184-192.

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

Clement, J. (2020, February 3). Global digital population as of January 2020. Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986). Retrieved from https://www.law.cornell.edu/uscode/text/18/1030#

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523 (1986). Retrieved from https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (2006). Retrieved from https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf

Grimes, R. A. (2016, December 6). Why it's so hard to prosecute cyber criminals. *CSO*. Retrieved from https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html

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 these years fighting malicious extensions. *24th USENIX Security Symposium*.

Liu, L., Zhang, X., Yan, G., & Chen, S. (2012). Chrome extensions: Threats analysis and countermeasures. *NDSS*, 1-16.

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/

NortonLifeLock employee. (n.d.) What are some of the laws regarding internet and data security? Retrieved from https://us.norton.com/internetsecurity-privacy-laws-regarding-internet-data-security.html

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/dmlyZ2luaWEtVVJfYmpZTkNLMXR0M0hsaEl4LTVhY2NhZTI1OTIxMmY2MDAxMmRmYmZlOQ==#/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

Toreini, E., Shahandashti, S. F., Mehrnezhad, M., & Hao, F. (2019, June 11). DOMtegrity: Ensuring web page integrity against malicious browser extensions. *International Journal of Information Security*, 18, 801-814. DOI: 10.1007/s10207-109-00442-1.

United States Department of Justice. (2020, January 15). Privacy Act of 1974. Retrieved from https://www.justice.gov/opcl/privacy-act-1974

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