Scientific and Practical Cyber Security Journal (SPCSJ) 6(2): 1-5 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

A TALE OF BETRAYAL: MALICIOUS BROWSER EXTENSIONS IN THE CONTEXT OF CYBER SECURITY AND PRIVACY

Giulia Melotti Garibaldi, Cyber Security Consultant Master's degree in Law, University of Milano-Bicocca, Italy

ABSTRACT: Browser extensions are popular additions to web browsers meant to enhance the online user experience by providing customizable options to meet the individual needs of users. In the wide variety of extensions available on the market, spanning from ad blockers to password managers, some of these software modules have proven to be a double-edged sword. As a matter of fact, in the past few years we have witnessed an alarming increase of malicious extensions available for download, targeting unaware victims relying on their apparent functional nature while hiding a world of illicit data thefts and sharing practices to the consumers' detriment. In order to examine whether the trade-off of privacy for functionality might still be an ongoing issue, this article follows two different approaches where theory and practice go hand in hand. The first one consists of a technical state-of-the-art analysis of different browser extensions available for download on the Chrome Web Store, while the second comprises a study of the questionable risks posed by those technologies from a privacy perspective. With regards to the latter, the author acknowledges the worldwide reach of browser extensions, while understanding the existence of a vast regulatory landscape around the globe. For the purpose of this paper, the analysis solely focuses on the European privacy framework, consisting of the General Data Protection Regulation (hereafter referred to as the GDPR) and the Directive on Privacy and Electronic Communications (the ePrivacy Directive). The conclusion drawn is that, despite all the efforts to counteract malicious browser extensions, some of them are still perpetrating harm and breaching privacy principles in a way which might not seem evident to users.

KEYWORDS: *cyber; security; browser extensions; protection; privacy.*

INTRODUCTION

A browser extension is a small module added to web browsers with the purpose of giving additional functionality to users in relation to many subjects, including, but not limited to, third party websites, native applications, browser appearance and browser security. Browser extensions can ask for permissions to gain access to specific browser data and control of the browser, while having the ability to send and receive information from arbitrary external servers. In some cases, all browser data, including login credentials, financial and health information, can be accessed and collected by the browser extension, and network requests can be intercepted, modified, or blocked.

In the circumstance that an extension has been granted the ability to interact with requests, it is possible for a malicious browser extension to deceive users for the purpose of phishing by forcing a redirect to a malicious site or attempting to get the user to download and execute malware [25]. Their documented success in tricking users should come as no surprise [26]: browser extensions interface with a broad audience which seems to be anything but wary. According to a survey conducted in 2021, users are confident that developers for both default browsers and browser extensions reliably ensure the safety of user data [27]. Moreover, while a large portion of those trusty users does not read browser extensions' privacy policies [11], others do not take further steps to ensure their privacy and security once those extensions are installed [27].

TECHNICAL METHODOLOGY

The overall purpose of testing was to determine if any browser extensions on the most popular internet browser per market share in Europe, i.e., Chrome [28], violated the European privacy legal framework. The sample examined consisted of twenty randomly selected browser extensions sourced from the Chrome Web Store in May 2022 [5], with all extensions tested on a device running Windows 10 (20H2) operating system using Google Chrome version 101.0.4951.54 . The browser extensions were analysed

manually and then automatically with the assistance of the online tool CRXcavator [7]. The extensions were tested with the aim of enumerating permissions, external communication with remote servers and defined privacy policy in the light of the GDPR [10] and the ePrivacy Directive [9].

RESULTS

It was observed that twenty percent of the browser extensions tested were in breach of the GDPR, as they did not have a defined privacy policy and externally shared collected information from the user without fulfilling the information obligations [18,19]. Moreover, they also had excessive control of the user's browser via permissions to access the chrome.webRequest API [4], allowing for traffic interception, blocking and modification.

It was also noticed that another twenty percent of browser extensions tested did have a defined privacy policy, but was insufficient to meet the requirements under European law due to, for instance, inappropriate legal basis [15], illegitimate re-use of data for secondary processes despite their incompatibility with the pre-defined utilization and retaining data beyond the originally stated purpose and for an indefinite time [14]. Also for the scenario in question, the browser extensions were externally sharing collected information from the users without informing them, while having excessive control of the browser via permissions to access the chrome.webRequest API.

Lastly, the remaining sixty percent of tested browser extensions met the requirements of the EU privacy legal framework, including compliant privacy policies referring to, *inter alia*, the collected data, the purpose of collection and correct legal basis, third party data sharing, security measures, individual rights and cross-border transfers outside of the EU/EEA, with specific reference to safeguards for third countries not providing adequate protection [18,19].

Concluding, sixty percent of the inspected browser extensions fulfill the requirements, while forty percent do not only neglect the considered data protection framework, but also collect personal identifiable data to an extent which cannot be assessed due to lack of information from the developers' side. Whether data is collected following the least intrusive approach or not is left to the imagination.

DISCUSSION

The sample in analysis is not large enough to draw any firm conclusions from the research conducted, as this paper primarily exists with the aim of raising awareness and stimulating more research and debate on the topic. There is a possibility that, although the European privacy legal framework requirements are not met by certain extensions tested, their security and privacy posture could be greater than what immediately visible to the author conducting this research. All things considered, the presence of forty percent potential non-compliant browser extensions appears to be a significant number that cannot be ignored: according to this study, critical data safety pitfalls take place on a common basis, with extensions spying on users and stealing their information for unknown purposes without them being aware thereof. This unlawful and unrestraint access to data also seems capable of deceiving Chrome's revision processes [2]. Hence, the small test carried out in this paper could not only serve as a wake-up call for cybersecurity practices, but also for privacy compliance. In an intangible borderless yet impacting world such as the Internet, technologies like browser extensions might attempt to escape the application of provisions and principles to which they are indeed subject to, and the interconnection between cybersecurity and privacy could turn out to be the winning cocktail to duly grant the security and rights of data subjects. Instead of considering them separately, it is of pivotal importance that privacy becomes the beating heart of technology when designing and engineering valuable and efficient products.

Starting off with the GDPR, the latter finds its application regardless of where organizations are established in the world, as long as the processing of data for the offering of goods or services or to monitor individuals is carried out by European-based organizations or relates to individuals in the European Union [12]. Therefore, not only can browser extensions not shield themselves by invoking the place where they are established, but they cannot rely on the nature of the processed data either, as the GDPR leaves the door open to a wide definition of personal identifiable information [13]. Unless disaggregated and anonymized [23], kinds such dynamic IP addresses and logged HTTP requests, for instance, are sufficient elements to directly or indirectly identify an individual, leading to the creation of an extensive user profile entailing patterns where even highly sensitive information could be exposed [6, 24]. The processing of personal data is not, however, forbidden per se under the GDPR, as long as it is happening in a lawful, fair and transparent manner [14]. The cost for respecting those principles is less hefty than what might be expected: for forty percent of the extensions analysed, having a compliant privacy policy to disclose data practices upfront could be the right starting point.

While notices' format might have different nuances, their content should invariably correspond to the requirements as outlined in the GDPR. Google Chrome also provides guidelines to help developers in drafting notices to be published on the extension download page [3]. Privacy policies should unequivocally document the collected data and the ways in which such personal information is intended to be used by the controller according to the business objectives, including its disclosure to third-parties [18,19]. The processing of data needs to be justified with a legal basis [15]: where the GDPR provides for six different bases to choose from, picking the right one for a lawful data processing appears to be a sweet spot for many developers, either because they fail to demonstrate that the processing of personal data is indispensable to achieve the stated purposes (i.e., such collection of data is not justified, and therefore violating the privacy-by-default principle) [21], or because they choose to rely on the wrong one. The Chrome guidelines set a strict requirement to request consent when browser extensions simultaneously meet two conditions: they collect personal or sensitive data, and the processing of such data is not "closely related" to its functionality [3]. At the very same time, some browser extensions rely on legitimate interest even when collecting those types of data, justifying the latter by assessing their own business interests against those relating to their consumers and declaring the former as overriding. The prevailing confusion on the topic is however no wonder when no clear rules and *consensus* regarding browser extensions have been defined. While the GDPR requests consent when the processing of behavioural data or preferences might reveal individual sensitive attributes [17] or when data is inferred as the result of probabilistic assumption and constructed profiles can be used for automated decision-making [20], the ePrivacy Directive would require it in the event of access to or storing information on the user's terminal [8]. As a matter of fact, by looking at the current regulatory framework and ongoing legal debate, it is undisputed that consent is the required legal basis for similar technologies to cookies such as device fingerprinting [1]. Even though no clear-cut reference to browser extensions has been made, in this author's opinion browser extensions with access to powerful APIs such as the chrome.webRequest API are able to fingerprint devices by several sources such as user behaviour and analysis of overall network traffic, where such actions are executed covertly without the acknowledgment of the end user. The technical method of device fingerprinting by browser extensions would likely not fall under the exemptions defined in Article 5(3) ePrivacy Directive, and therefore users' consent cannot be avoided.

All things considered, compliance is more than a mere piece of paper. Notices might collect consent by users actively agreeing to a clear and unmistakeable request on the product's front-end interface through consent dialogs, disclose international data transfer, refer to the use of accurate data and grant data access rights [16, 18, 19], and that might still not be enough. In fact, browser extensions should effectively observe what they promise to their consumers, implementing data sharing practices which do not only live up to legal standards, but also to users' expectations. Even when authorized, the collection of large datasets for analytics personalization and profiling by an extension to increase productivity, for instance, can hardly be justified in the users' eyes.

CONCLUSION

While multiple browser extensions are still lagging behind in aligning their products to the European privacy requirements, these technologies could unleash much more potential than what they are currently doing by not being compliant. When adopting a consumer-centric view, transparently disclosing data practices to individuals, and refraining from intrusive tracking, profiling and data exfiltration, developers could demonstrate they are far away from merely serving their economic interests while caring for individual rights. Not only for the Data Protection Authorities, which have been particularly attentive and prone to fine for failure in fulfilment of information obligations and legal basis for the processing of data over the past years [22]: this change would also be an act of responsibility towards consumers, who would be capable of understanding to what extent browser extensions operate, while being empowered to make informed and autonomous choices regarding their own rights. If it is true that technology cannot be avoided, a conscious and ethical use of it could make the real difference.

REFERENCES

1. *Article 29 Working Party on Device Fingerprinting.* 2014. Article 29 Data Protection Working Party. "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting". WP 224. https://www.dataprotection.ro/servlet/ViewDocument?id=1089

2. Chrome Developers. "Publish your extension". Accessed April 26, 2022. https://developer.chrome.com/docs/webstore/publish/

3. Chrome Developers. 2016, updated 2021. "Updated Privacy Policy & Secure Handling Requirements". Accessed April 28, 2022. https://developer.chrome.com/docs/webstore/user_data/

4. Chrome.webRequest API. Accessed April 27, 2022 https://developer.chrome.com/docs/extensions/reference/webRequest/

5. Chrome Web Store. Accessed May 3, 2022. https://chrome.google.com/webstore/category/extensions

6. *Court of Justice of the EU* (CJEU). 2016. Breyer, Case C-582/14, at para. 49 https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=40417

7. *EU Directive on Privacy and Electronic Communications* (ePrivacy Directive). 2002. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

8. *EU General Data Protection Regulation* (GDPR). 2016. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)". OJ 2016 L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj

9. Eurostat. 2022. "How do EU citizens manage their personal data online?". Accessed May 3, 2022. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20220127-1

10. Georgescu, Elena. 2021. "Have You Ever Installed a Malicious Chrome Extension?". Heimdal Security. Accessed April 25, 2022.

https://heimdalsecurity.com/blog/malicious-chrome-extension/

11. Jadali, Sam. 2019. "DataSpii: The catastrophic data leak via browser extensions". SecurityWithSam.com. Accessed April 27, 2022. https://securitywithsam.com/

12. Kariryaa, Ankit, Gianluca Savino, Carolin Stellmacher, Johannes Schöning. 2021. "Understanding Users' Knowledge about the Privacy and Security of Browser Extensions". *Proceedings of the Seventeenth Symposium on Usable Privacy and Security* (9-10 August 2021). Accessed April 26, 2022. https://www.researchgate.net/profile/Johannes-Schoening/publication/356892773_Understanding_Users%27_Knowledge_about_the_Privacy_and_Security_of_Browser_Extensions/links/61b1b4ec4d7ff64f05372925/Understanding-Users-Knowledge-about-the-Privacy-and-Security-of-Browser-Extensions.pdf?origin=publication_detail

13. Vailshery, Lionel Sujay. 2022. "Market share held by the leading internet browsers in Europe from 2009 to 2021". Statista. Accessed May 3, 2022. https://www.statista.com/statistics/269881/market-share-held-by-internet-browsers-in-europe/