ERMES
INTELLIGENT WEB PROTECTION

HIJACKED ON THE WEB

The Growing Threat of
MALICIOUS BROWSER EXTENSIONS

WHITE PAPER

August 2021
Version 3.0

ERMES
Intelligent Web Protection

www.ermes.company

Executive Summary

As enticing as they may be, there are significant risks a ssociated w ith installing extensions on a web browser to enhance functionality. Powerful APIs give web browser extensions complete visibility over a user's navigation. Moreover, in conjunction with expansive APIs, initial requests for user permissions can be easily exploited by cyber criminals that use browser extensions as a tool or pathway to plan a multitude of malicious attack types against unsuspecting individuals and organizations.

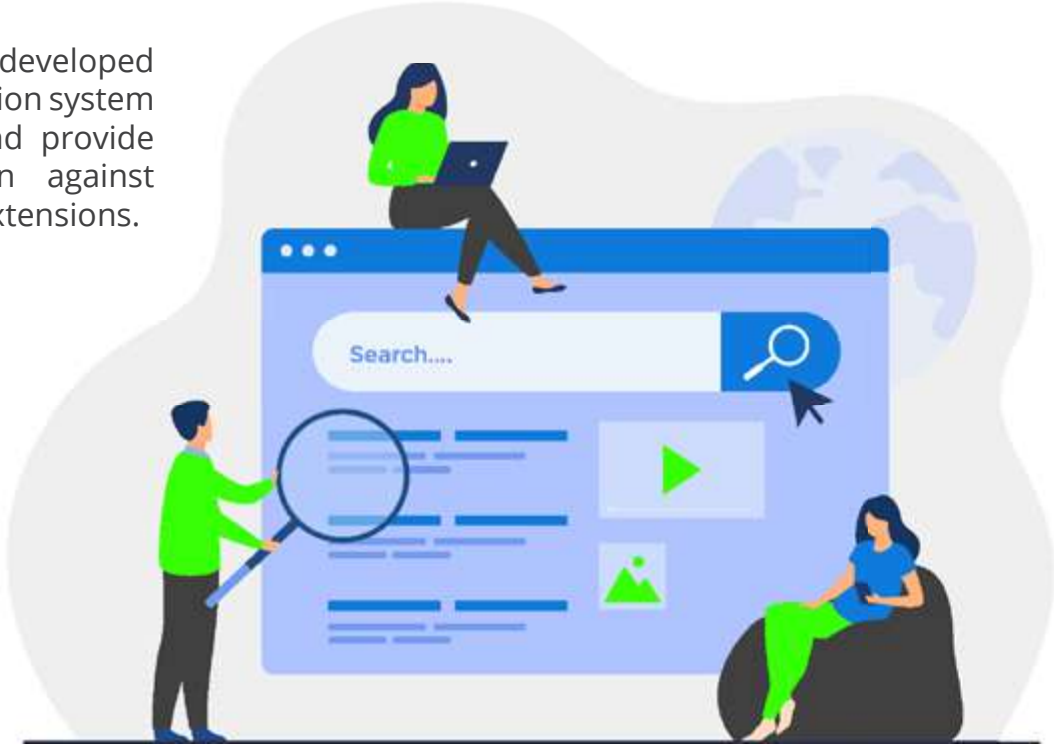
Today, almost anyone can publish browser extensions to an official store. Threat intelligence researchers considered them to be a weak link in the online security chain. Neither Google Chrome, Mozilla Firefox, or Microsoft Edge have come up with an adequate system to effectively vet the authenticity of the people submitting these extensions or the safety of the code. Accordingly, malicious browser extensions are on the rise and triggering millions of attacks worldwide.

Examples of different attack types using malicious browser extensions as their vehicle of delivery include, among others, link hijacking with redirection to malware and adware distribution websites, search results modifications, capturing credential and sensitive information, account takeovers, social media tampering, and opening backdoors to botnets.

Ermes researchers recently discovered a malicious browser extension campaign that was operating across extensions available in the Google Chrome Web Store and Microsoft Edge Add-Ons Store. This campaign—named "SocialDivert"—was composed of extensions that deployed successful attacks resulting in link hijacking.

Overall, a total of 18 extensions were found in the Edge Add-Ons Store and 16 in the Chrome Web Store. **All together these malicious browser extensions affected over 220,000 users.**

Currently, Ermes has developed a unique early detection system that can identify and provide complete protection against malicious browser extensions.



CONTENTS

Introduction

A browser extension is a small unit of software added to a web browser that controls the way a user might visit a web page or view information emanating from a web service.[1]

Browser extensions generally enhance the capabilities and functionality of major web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge. These extensions can be used for a myriad of beneficial purposes such as blocking ads, password management, tracking tasks, and screen capturing.[2] However, it is also a vulnerable tool that can be readily "hijacked" or rampantly exploited by cunning cyber criminals with malicious intent.

There are significant risks associated with certain browser extensions even though on the surface they appear to be for benign purposes such as providing entertaining content, improving privacy, user experience, or security. Lurking underneath, however, there are vulnerabilities posed by malicious browser extensions that frequently involve the misuse of application programming interfaces (APIs)[3] and user permissions.

Once installed, the available APIs associated with a browser extension can give it complete visibility over a user's navigation of the web. This includes sensitive information such as emails, credentials, and corporate internal web services. A malicious browser extension can actively interfere with user navigation by surreptitiously redirecting to other websites, performing activities on web pages, contacting remote services while intercepting communications and collecting sensitive user data. All of this malicious activity can be done without the user ever noticing that it is happening.

In addition to the dangers posed by APIs, malicious browser extensions must ask for user permissions to perform certain activities through their web browser. However, this request is done only once when the browser extension is first being installed by the user under the pretext of a beneficial purpose. Subsequently, most users then have no visibility on when and how those permissions are exploited by cyber criminals for a future threat or attack.

1. See generally "How Browser Extensions Work," Forbes, April 16, 2019, at https://www.forbes.com/sites/adrianbridgwater/2019/04/16/how-browser-extensions-work/.

2. See generally "Five Types of Browser Extensions Every Professional Should Have," TechRepublic, September 14, 2016, at https://www.techrepublic.com/article/five-types-of-browser-extensions-every-professional-should-have/.

3. An application programming interface (API) is a set of protocols, routines, functions, and/or commands that programmers use to develop software or facilitate interaction between distinct systems. See "Application Programming Interface (API): What Does Application Programming Interface (API) Mean?" Techopedia, June 8, 2017, at https://www.techopedia.com/definition/24407/application-programming-interface-api.

It is possible to introduce malicious behavior in these already installed extensions over time—without the user ever becoming aware—because browser extension updates are done automatically by default. Users are not informed about subsequent updates. Accordingly, version updates could exploit the original permissions granted at installation time for different and malicious purposes than those used in previous versions.[4]

Furthermore, because almost anyone can publish browser extensions to an official store, they are considered a weak link in the online security chain. Neither Google, Mozilla, or Microsoft have come up with an adequate system to vet the authenticity of the people submitting these extensions or the safety of the code.[5]

This white paper will briefly explore some of the specific threats and attacks that can result from the use of malicious browser extensions. Following this there will be an overview of a proprietary analysis conducted by Ermes researchers as it relates to malicious browser extensions published on the Google Chrome Web Store and Microsoft Edge Add-Ons Store. Finally, an effective solution for early detection of malicious browser extension threats will be discussed.

Malicious Browser Extension Campaigns

By themselves, malicious browser extensions are not an attack methodology, but rather a tool or path that makes it possible to implement an array of different attack types using JavaScript. Given the powerful nature of the APIs available through web browser extensions, they can implement many different attack methodologies and campaigns.

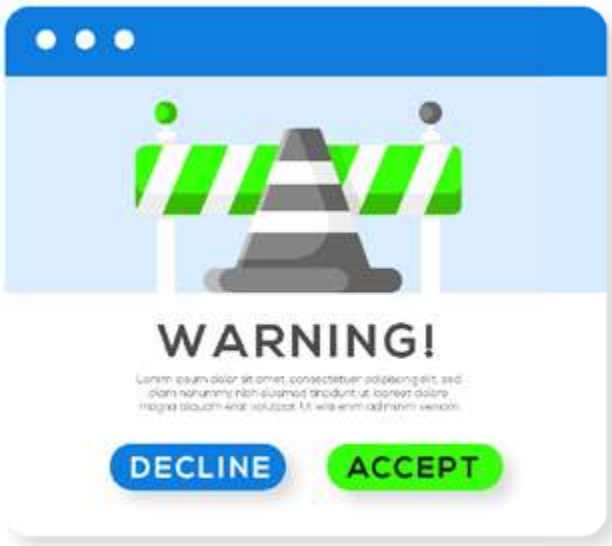
Attacks exploiting browser extensions are very common today and can typically involve millions of users. For example, threat intelligence researchers have identified malware hidden in at least 34 third-party Google Chrome and Microsoft Edge extensions that have affected three million people worldwide.[6]

4. See "You've Changed: Detecting Malicious Browser Extensions Through Their Update Deltas," Association for Computing Machinery (ACM), October 30, 2020, at https://dl.acm.org/doi/10.1145/3372297.3423343. Recently, Google removed a Chrome plugin used by approximately 2 million users after reports that the browser extension had been compromised and installed potentially malicious code and tracking software on user systems. See "Malicious Code Injected Via Google Chrome Extensions Highlights App Risks," Dark Reading, February 8, 2021, at https://www.darkreading.com/application-security/malicious-code-injected-via-google-chrome-extensionhighlights-app-risks.

5. See "Abusive Add-Ons Aren't Just a Chrome and Firefox Problem. Now It's Edge's Turn," ARS Technica, November 20, 2020, at https://arstechnica.com/gadgets/2020/11/fraudulent-add-ons-infiltrate-the-official-microsoft-edgestore/.

6. See "Third Party Browser Extensions for Instagram, Facebook, Vimeo and Others Infected with Malware," Avast, December 16, 2020, at https://press.avast.com/third-party-browser-extensions-from-instagram-facebook-vimeo-and-others-infected-with-malware.

One of the most common attack types involves link hijacking and redirection to malware and adware distribution websites using remote browser command and control.[7] There are also attacks that modify or redirect search engine results[8] and collect sensitive user data such as credentials. Google recently removed 106 Chrome malicious extensions for collecting user keystrokes, clipboard content, and cookies.[9] Moreover, it was reported that the Google Chrome "Sync" feature was abused by threat actors to harvest information from compromised computers using maliciously-crafted Chrome browser extensions.[10]



Malicious browser extension campaigns can be used to takeover user accounts. A recent article in Threat Post reported that a newly uncovered cyberattack was taking control of victims' Gmail accounts by using a customized, malicious Mozilla Firefox browser extension.[11] Also, "adblocking" extensions with more than 300,000 active users were found to be surreptitiously uploading user browsing data and tampering with users' social media accounts.[12] Browser extensions are also becoming backdoors to botnets—networks of private computers infected with malicious software and controlled as a group.[13]

7. Ibid. Users reported that these extensions are manipulating their internet experience and redirecting them to other websites. Anytime a user clicks on a link, the extensions send information about the click to the attacker's control server, which can optionally send a command to redirect the victim from the real link target to a new hijacked URL before later redirecting them to the actual website they wanted to visit. See also "Researchers Discover Two Dozen Malicious Chrome Extensions," Dark Reading, March 22, 2021, at https://beta.darkreading.com/vulnerabilities-threats/researchers-discover-two-dozen-malicious-chromeextensions. This article details how browser extensions are being used to serve up unwanted adds, steal data, and divert users to malicious websites.

8. See "Abusive Add-Ons Aren't Just a Chrome and Firefox Problem. Now It's Edge's Turn," ARS Technica, November 20, 2020, at https://arstechnica.com/gadgets/2020/11/fraudulent-add-ons-infiltrate-the-official-microsoft-edgestore/. This article specifically mentions how browser extensions were redirecting Google searches to oksearch[.]com when Microsoft Edge was being used.

9. See "Google Removes 106 Chrome Extensions for Collecting Sensitive User Data," ZDNet, June 18, 2020, at https://www.zdnet.com/article/google-removes-106-chrome-extensions-for-collecting-sensitive-user-data/.

10. See "Malicious Extension Abuses Chrome Sync to Steal User's Data," Bleeping Computer, February 5, 2021, at https://www.bleepingcomputer.com/news/security/malicious-extension-abuses-chrome-sync-to-steal-usersdata/.

11. See "Malicious Mozilla Firefox Extension Allows Gmail Takeover," Threat Post, February 25, 2021, at https://threatpost.com/malicious-mozilla-firefox-gmail/164263/.

12. See "Adblockers Installed 300,000 Times are Malicious and Should Be Removed Now," ARS Technica, October 20, 2020, at https://arstechnica.com/information-technology/2020/10/popular-chromium-ad-blockers-caughtstealing-user-data-and-accessing-accounts/

13. See "Is Your Browser Extension a Botnet Backdoor?" Krebs on Security, March 1, 2021, at https://krebsonsecurity.com/2021/03/is-your-browser-extension-a-botnet-backdoor/.

Malicious Browser Extension Campaign Discovered By Ermes

Ermes researchers recently discovered a pervasive malicious browser extension campaign by conducting a thorough analysis of extensions published on both the Google Chrome Web Store and Microsoft Edge Add-Ons Store.

This malicious extension campaign which researchers named "SocialDivert" was spreading across both official stores and composed of extensions that deployed successful attacks resulting in link hijacking. Specifically, links were redirecting users to malicious websites instead of the ones they had intended to visit.

The attack implemented by these malicious browser extensions was basically carried out in the following manner:

1. The user clicked on a link in a webpage that was being visited,

2. Then the malicious extension—while listening for click events—intercepted the click and checked the destination Uniform Resource Locator (URL), and

3. If the destination URL contained one of 164 pre-defined strings,[14] the extension replaced it with one redirecting the user to a malicious website.

In most cases observed in this campaign, these malicious extensions targeted victims by enticing them to add social-related functionality to their web browsers. These functionalities specifically included the ability to download videos from Instagram, Facebook, YouTube, Vimeo, and LinkedIn. Moreover, these extensions also provided the ability to view and download Instagram stories as well as music tracks from SoundCloud.

During this research, a total of 18 malicious SocialDivert extensions were found in the Edge Add-Ons Store and 16 in the Chrome Web Store affecting a total of 220,000 users.

14. The set of 164 pre-defined strings were carefully crafted in such a manner to match popular social websites, banking websites, search engines, web email services, and confidential login pages to other websites

The SocialDivert campaign exhibited many characteristics of particular interest when studying its deployment methodology as well as general complexity.

First, each extension was published on the official stores by a purposedly-made developer account—whose only published extension was the malicious one. By doing so, attackers mitigated the risk of easily discovering all malicious extensions once one of them was successfully identified.

Second, all extensions made large use of deeply obfuscated[15] JavaScript code to prevent the recognition of the malicious behavior being exploited.

Third, all involved extensions started performing the attack procedure only a few days from installation by the user. This was likely done to avoid suspicion of anomalous browser behavior as well as to thwart detection from automated systems.

Fourth, these extensions also implemented several techniques to avoid the malicious behavior discovered by researchers. These included avoiding the execution of the attack on Linux machines and on locally hosted webpages.

Fifth, in an attempt to avoid detection, when performing the attack, malicious browser extensions contacted many different hostnames and URLs. Interestingly, some of the content extensions used to carry out the attack were hosted on Amazon Web Services (AWS S3.

Lastly, many extensions were positively reviewed on the official stores—with even some dedicated accounts offering support to reviews that included questions and reported difficulties.

Remarkably, one of the extensions taking part in the SocialDivert campaign was a Manifest V3-ready extension.[16] This updated standard poses many limitations to browser extensions capabilities in an attempt to enhance their security. Ironically, not only was this campaign not affected by Manifest V3's updated restrictions, but also future-proofed one of its extensions by making it adhere to the new standard well in advance of expected deadlines.

15. In software development, obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand. See generally, "Obfuscation (software)," Wikipedia, at https://en.wikipedia.org/wiki/Obfuscation_(software).

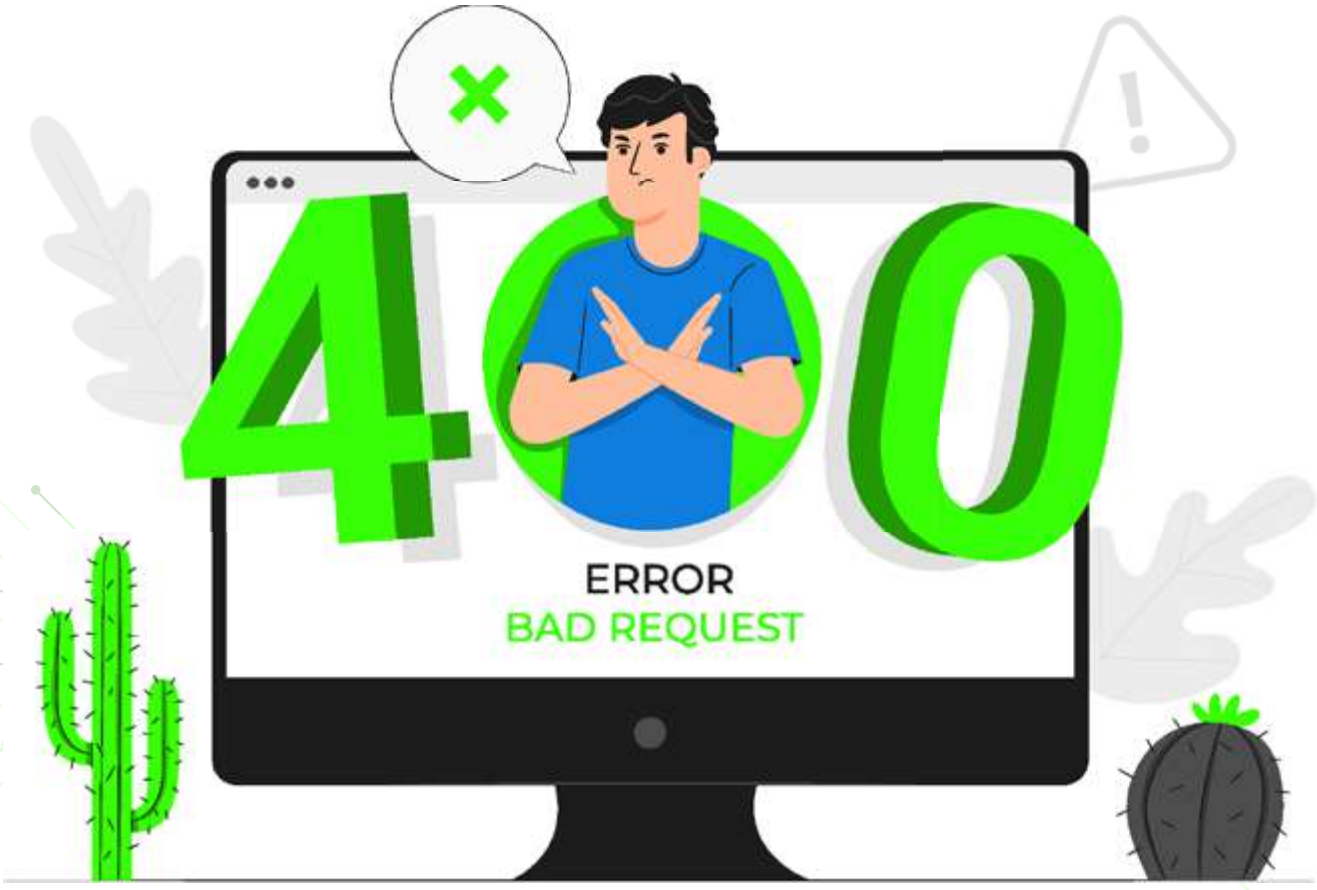
16. Manifest V3 is a new standard for web extensions intended to replace the current Manifest V2 scheduled to commence the first half of 2022 on Google Chrome (other browser vendors have not given estimated deployment dates yet for this standard).

All of these malicious extensions—taking into account some minor to more significant differences—exhibited very similar behavior to those first identified by Czech researchers at CZ.NIC in November 2020, and then further analyzed by the Avast Threat Intelligence team to discover the whole campaign behind them—which they ultimately called "CacheFlow." Interestingly, some of the extensions Ermes detected in this new campaign were already public and available on both the Chrome and Edge extensions stores during that same period. This suggests that previous studies might have missed them.

The SocialDivert campaign discovered by Ermes did not affect the Mozilla Firefox AddOns Store. This is likely because extensions containing obfuscated code are not allowed to be published in that store since mid-2019.

It should be noted that all browser extensions taking part in the SocialDivert campaign were immediately identified by Ermes' products as malicious just as soon as the Ermes research team certified their malevolent behavior. Accordingly, Ermes' customers were informed of these threats even before Google and Microsoft proceeded with their removal of these malicious extensions from their stores.

Finally, Ermes researchers continuously and actively look for new malicious extension campaigns in order to detect and protect customers from potential threats and attacks.



Ermes Solution for Early Detection of Malicious Browser Extensions

Ermes addresses malicious browser extensions by analyzing every single browser extension installed on a customer device.

The first check performed by the Ermes system is to determine whether the extensions being analyzed are already known or have been previously identified as malicious. To that end, Ermes also actively searches for malicious extensions on the web to immediately warn customers when a match is found in its dynamic database of extensions that have been red-flagged for known risks or malicious qualities.

The second check—specifically targeting downloaded browser extensions that have not already been identified as malicious—involves a much deeper dive by the Ermes solution. During this process, Ermes analyzes and scrutinizes the extension's source code, known dependencies, vulnerabilities, permissions, and other security and privacy information. This is done for each and every extension installed by a customer that is not already a known threat.

By doing so, this allows Ermes to determine if extensions downloaded to a customer device are able to execute remote code or collect and expose sensitive information. Following the Ermes proprietary analysis, the results delivered to customers will assign a risk label appropriate to each extension downloaded by a customer. These labels (in order of risk propensity) are "none," "low," "medium," "high," or "critical."

As part of the Ermes early detection solution, customers can thoroughly inspect the assigned risk label given to any downloaded browser extension including the technical motivations behind the scoring and classification. This allows customers to have an in-depth view and complete control over all browser extensions—with their associated capabilities and potential risks—so they can make intelligent decisions about whether it is justified to remove a browser extension from a device because it may pose a threat.

To illustrate the above solution, all extensions taking part in the SocialDivert campaign were already assigned a "high" security risk by the automated labelling system even before the subsequent discovery of their malicious nature by researchers. This same methodology has already allowed Ermes researchers to expeditiously and accurately detect:

- **Over 400 malicious Chrome extensions**
- **Over 45,000 high-risk Chrome extensions**
- **Over 36,000 medium-risk Chrome extension**
- **Over 200 malicious Firefox extensions**
- **Over 6,000 high-risk Firefox extensions**
- **Over 7,900 medium-risk Firefox extensions**

Conclusion

Through both external and internal research, Ermes has concluded that malicious browser extensions are a serious and growing threat on the Internet. They are an attack path routinely being exploited by cyber criminals to deploy a multitude of different attack types against individuals and organizations. These malicious extensions basically provide the "digital vehicle" for being hijacked on the information superhighway.

To best serve its customers and organizations that wish to protect against these growing threats and attacks that occur via web browsers, Ermes has developed an early detection system for malicious browser extensions. We have a unique system that can completely protect against them.

For a demonstration of this system's capabilities or to learn more about our proprietary solution that reviews every single browser extension for a potential threat at lightning speed, please contact us at **info@ermes.company**.

ABOUT

Ermes–Intelligent Web Protection protects companies and employees from contemporary threats that users encounter while surfing the web through the use of artificial intelligence (AI) and deep-learning. As a leading innovator in web security and data protection, we specialize in modern cyber threats that elude traditional security systems including growing attacks that result from the exploitation of malicious web browser extensions.

Our early detection software makes it possible to identify and label the risk associated with every browser extension downloaded to a user device. The Ermes solution is capable of matching known threats and analyzing every extension's source code, dependencies, vulnerabilities, permissions, and other security and privacy information so organizations can completely protect themselves against all malicious extensions.

We look forward to working with you so we can demonstrate the security benefits that our proprietary solutions can provide to your organization.

CONTACT

Ermes Cyber Security S.R.L.
Corso Bernardino Telesio 29,
10146 Torino, Italy

info@ermes.company

www.ermes.company