Verify Google Chrome Extensions Before you Install Them

by Martin Brinkmann on November 21, 2015 in Google Chrome - Last Update: July 18, 2016 - 8 comments

Google Chrome extensions can extend the functionality of the web browser or make life easier while browsing the Web. While that is the case, they may also be abused by companies to track users across the Internet, display advertisement or download malicious code to the user system.

This article provides you with the means to verify Chrome extensions before you install them. It is important to do so before the extension gets installed in the browser as it may already be too late after installation.

While you can set up a test environment for browser extensions, for instance in a Sandbox and with a network traffic monitor like Wireshark, it may not really be something that most users feel comfortable with.

Part 0: What you should not trust

The Chrome Web Store may appear like a secure location for all your extension needs, but it is not. Google uses automated checks that scan extensions that developers upload to the store. These checks catch some but not all forms of privacy-invasive or outright-malicious functions.

Trend Micro discovered for instance malicious browser extensions in the official Web Store in 2014, and it is not the only company that did so.

A common method used by extensions to pass all security checks is to include a script that will load the malicious payload.

The extension itself does not contain it when submitted to the Chrome web store. Thus, the extension passes the check and is added to the store where all Chrome users can download it.

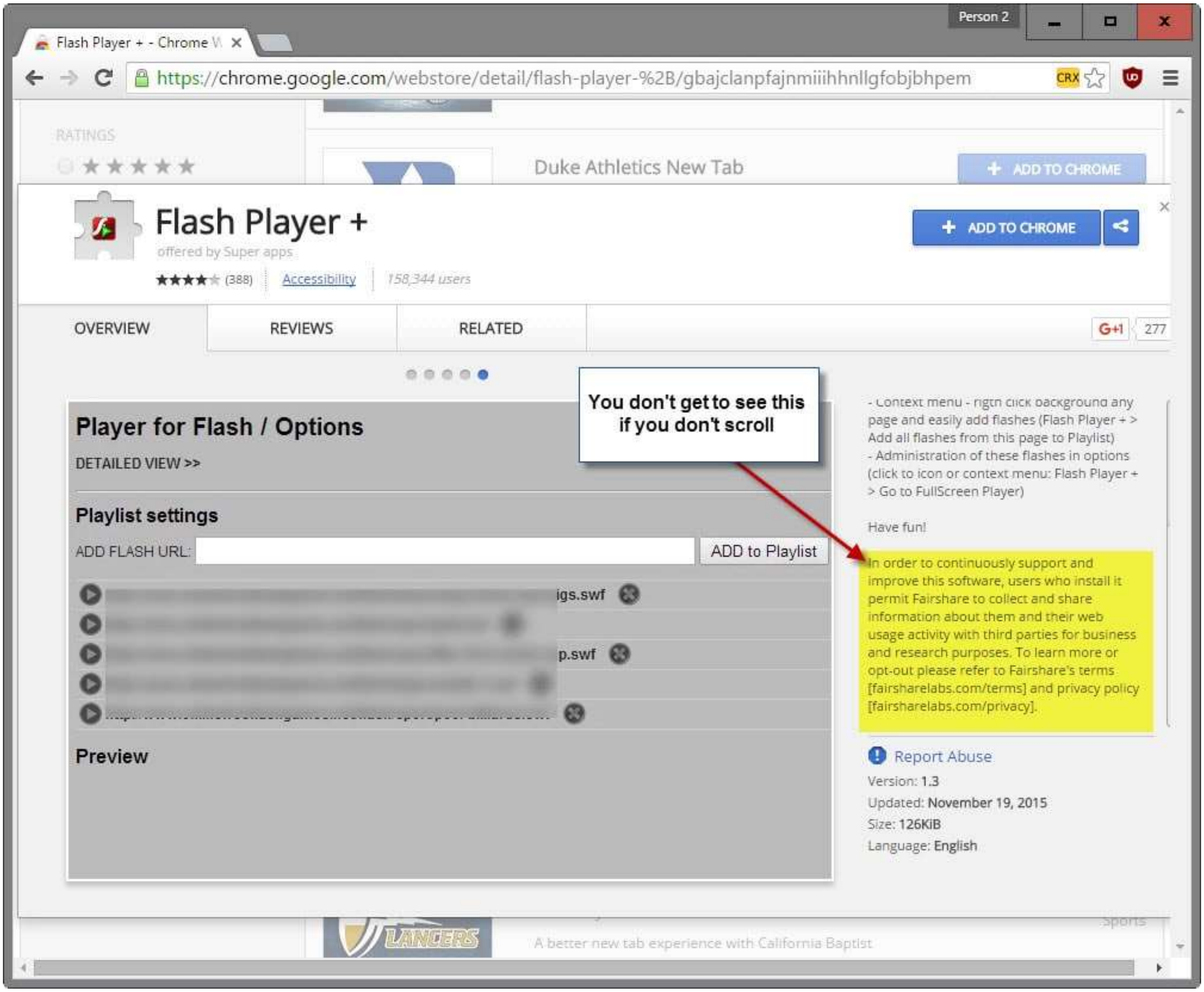
If you are interested in one nasty recent example, check out the malware in the browser article by Maxime Kjear.

The description is created by the developer of the extension and is therefore not to be trusted without verification.

User comments may highlight problematic extensions, but that is not always the case. Therefore, they are not to be trusted either in this regard without verification.

Last but not least, you should not trust recommendations blindly, or offers to install an extension because it is needed for something or advertised to you.

Part 1: The description



You don't get to see this if you don't scroll

- Context menu - rigth click background any page and easily add flashes (Flash Player + > Add all flashes from this page to Playlist)
- Administration of these flashes in options (click to icon or context menu: Flash Player + > Go to FullScreen Player)

Have fun!

In order to continuously support and improve this software, users who install it permit Fairshare to collect and share information about them and their web usage activity with third parties for business and research purposes. To learn more or opt-out please refer to Fairshare's terms [fairsharelabs.com/terms] and privacy policy [fairsharelabs.com/privacy].

Version: 1.3
Updated: November 19, 2015
Size: 126KiB
Language: English

Many extensions that use analytics, click-tracking, tracking of your browsing history and other tracking forms highlight the fact in the description of the extension.

You may not see this one first glance as Google favors style over substance in the store. The description field is tiny and you often need to scroll to read it all.

Check out the popular Awesome Screenshot extension for instance. Looks legitimate right? Lots of positive reviews, more than 580,000 users.

If you take the time and scroll through the description, you will eventually stumble upon the following passage:

Usage of the Awesome Screenshot browser extension requires granting it permission to capture anonymized click stream data.

Want another example? How about Hover Zoom, an extension with more than 1.2 million users that has been criticized in the past for tracking integration? Scroll down and you find..

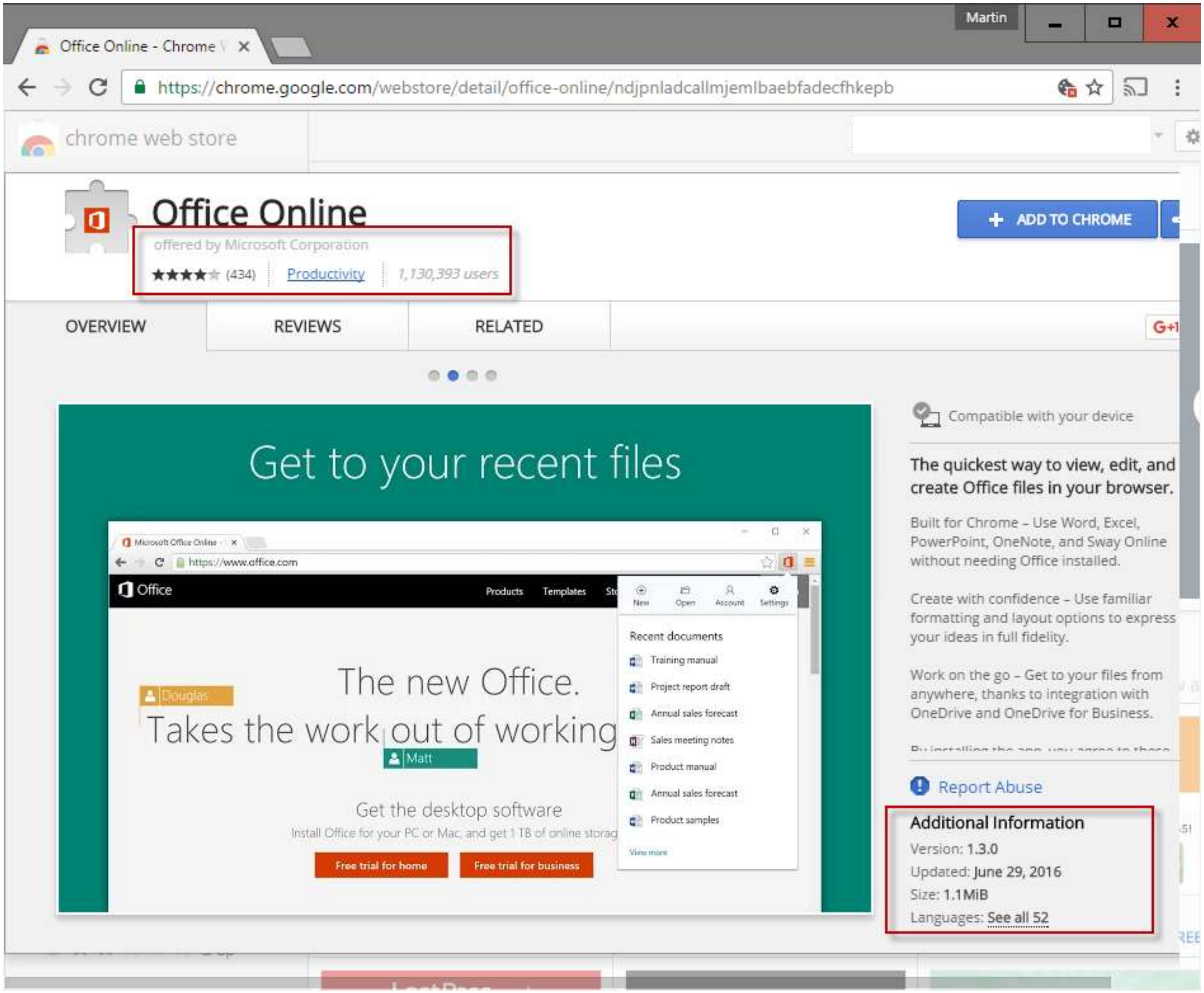
Hover Zoom requires that extension users grant Hover Zoom permission to collect browsing activity to be used internally and shared with third parties all for use on an anonymous and aggregated basis for research purposes

Flash Player+ is another extension that highlights in its description that it records data and shares that data with third-parties.

In order to continuously support and improve this software, users who install it permit Fairshare to collect and share information about them and their web usage activity with third parties for business and research purposes

A quick way to find these extensions is to search for phrases used in those descriptions. A search for opt-out for instance reveals many of them in the search results (next to legitimate extensions). Many use the same description which means that a search for "to collect and share information about them" will reveal extensions that use this kind of tracking for instance.

Part 2: Direct information



Office Online

offered by Microsoft Corporation

★★★★☆ (434) | Productivity | 1,130,393 users

Compatible with your device

The quickest way to view, edit, and create Office files in your browser.

Built for Chrome – Use Word, Excel, PowerPoint, OneNote, and Sway Online without needing Office installed.

Create with confidence – Use familiar formatting and layout options to express your ideas in full fidelity.

Work on the go – Get to your files from anywhere, thanks to integration with OneDrive and OneDrive for Business.

Additional Information

Version: 1.3.0
Updated: June 29, 2016
Size: 1.1MiB
Languages: See all 52

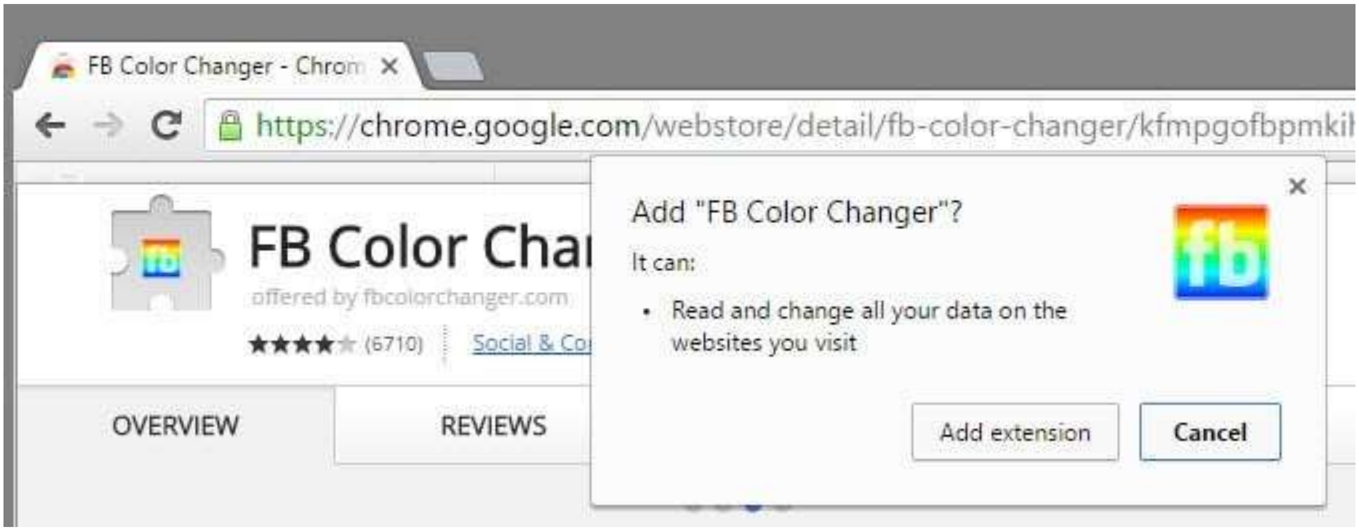
The following information are displayed on the extensions' profile page on the Chrome Web Store:

The company or individual that created it / offers it.
An aggregate rating, and the number of users who rated it.
The total number of users.
The last updated date.
The version.
The information give you clues but they are not sufficient to judge an extension. Many can be faked or inflated artificially for instance.

Google fails to provide a link to all extensions of a company or individual, and there is no option to get validation.

While you may use the search to find other extensions by a company or individual, there is no guarantee that the results list them all.

Part 3: Permissions


FB Color Changer - Chrom
https://chrome.google.com/webstore/detail/fb-color-changer/kfmpgofbpmkil
FB Color Char
offered by fbcolorchanger.com
★★★★☆ (6710)
Social & Co
OVERVIEW
REVIEWS
fb
Add extension
Cancel

Add "FB Color Changer"?

It can:

- Read and change all your data on the websites you visit

It is usually not possible to determine if an extension is legitimate, tracking you or outright malicious based on the permissions that it requests alone.

There are indicators however of that. For instance, if an extension that improves Facebook requests to "read and change all your data on the websites you visit", you may come to the conclusion that you better not install the extension based on that. Since it should only work on Facebook, there is no need to give it far-reaching permissions to see and manipulate data on all sites.

This is just an indicator however but if you use common-sense, you may be able to avoid installing problematic extensions. Usually, there is an alternative available that offers similar functionality but without the wide-reaching permission requests.

You may want to check these permissions for all installed extensions as well. Load chrome://extensions/ and click on the details link underneath each extension. This display all permission requests of that extension again as a popup in the browser.

Part 4: The Privacy Policy

Provided that the extension links to a Privacy Policy page, you may find information in it that reveal whether users are tracked by it or not. This won't work obliviously for outright malicious extensions.

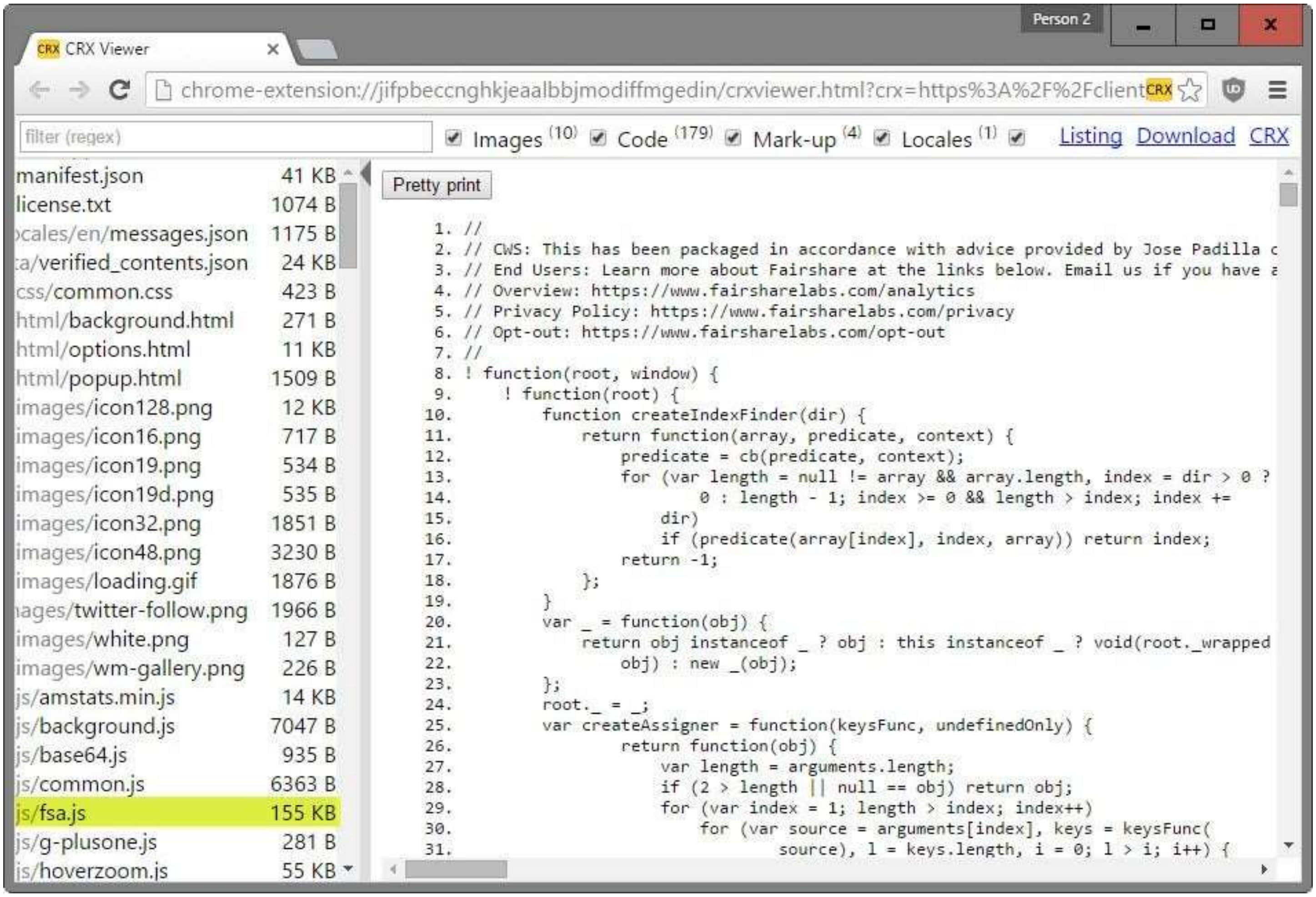
For example, if you check out the Fairshare Privacy Policy linked from extensions such as Hover Zoom, you find the following passage in it:

The Company may use browser cookies, web and DOM storage data, Adobe Flash cookies, pixels, beacons, and other tracking and data collection technologies, which may include an anonymous unique identifier.

These technologies may be used to collect and store information about your use of the Services, including without limitation, web pages, features and content you have accessed, search queries you have run, referral URL information, links you have clicked on, and advertisements you have seen.

This data is used for business purposes such as providing more relevant ads and content, and market research

Part 5: The source code


Person 2
CRX CRX Viewer ×
chrome-extension://jifpbeccnghkjeaalbbjmodiffmgedin/crxviewer.html?crx=https%3A%2F%2Fclient
filter (regex)
☑ Images (10) ☑ Code (179) ☑ Mark-up (4) ☑ Locales (1) ☑
Listing Download CRX
Pretty print

manifest.json	41 KB
license.txt	1074 B
ocales/en/messages.json	1175 B
a/verified_contents.json	24 KB
css/common.css	423 B
html/background.html	271 B
html/options.html	11 KB
html/popup.html	1509 B
images/icon128.png	12 KB
images/icon16.png	717 B
images/icon19.png	534 B
images/icon19d.png	535 B
images/icon32.png	1851 B
images/icon48.png	3230 B
images/loading.gif	1876 B
ages/twitter-follow.png	1966 B
images/white.png	127 B
images/wm-gallery.png	226 B
js/amstats.min.js	14 KB
js/background.js	7047 B
js/base64.js	935 B
js/common.js	6363 B
js/fsa.js	155 KB
js/g-plusone.js	281 B
js/hoverzoom.js	55 KB

```
//
// CWS: This has been packaged in accordance with advice provided by Jose Padilla c
// End Users: Learn more about Fairshare at the links below. Email us if you have a
// Overview: https://www.fairsharelabs.com/analytics
// Privacy Policy: https://www.fairsharelabs.com/privacy
// Opt-out: https://www.fairsharelabs.com/opt-out
//
! function(root, window) {
    ! function(root) {
        function createIndexFinder(dir) {
            return function(array, predicate, context) {
                predicate = cb(predicate, context);
                for (var length = null != array && array.length, index = dir > 0 ?
                        0 : length - 1; index >= 0 && length > index; index +=
                    dir)
                    if (predicate(array[index], index, array)) return index;
                return -1;
            };
        }
        var _ = function(obj) {
            return obj instanceof _ ? obj : this instanceof _ ? void(root._wrapped
                obj) : new _(obj);
        };
        root._ = _;
        var createAssigner = function(keysFunc, undefinedOnly) {
                return function(obj) {
                    var length = arguments.length;
                    if (2 > length || null == obj) return obj;
                    for (var index = 1; length > index; index++)
                        for (var source = arguments[index], keys = keysFunc(
                                source), l = keys.length, i = 0; l > i; i++) {
```

Going through the source code may be the best option that you have to find out if an extension is tracking you or malicious.

This may not be as technical as it sounds and it is often possible to determine that with rudimentary HTML and JavaScript skills.

First thing you need is an extension that enables you to grab the source code of an extension without installing it. Chrome extension source viewer is an open source extension for Chrome that helps you with that.

An alternative to that is to run Chrome in a sandboxed environment, install extensions in it to gain access to their files.

If you use the extension source viewer, you may click on the crx icon in the address bar on Chrome's Web Store to download the extension as a zip file or view its source right away in the browser.

You may ignore all .css and image files right away. Files that you should take a closer look at have the .js or .json extension usually.

You may check the manifest.json file first and check the content_security_policy value to see a list of domains there but that is usually not enough.

Some extensions use obvious names for tracking files, ads for instance so that you may want to start there.

You may not be able to tell if you don't know JavaScript however if that is not the case.

Now You: Do you run Chrome extensions? Have you verified them before installation?

Summary

Article Name

Verify Google Chrome extensions before you install them

Description

Find out how to verify Chrome extensions to make sure they don't track you or are malicious before installing them.

Author

Martin Brinkmann

Publisher

Ghacks Technology News

Logo

ghacks.net

We need your help

Advertising revenue is falling fast across the Internet, and independently-run sites like Ghacks are hit hardest by it. The advertising model in its current form is coming to an end, and we have to find other ways to continue operating this site.