How-To Geek

News

These 5 Popular Chrome Extensions Are Malware: Delete Them Now

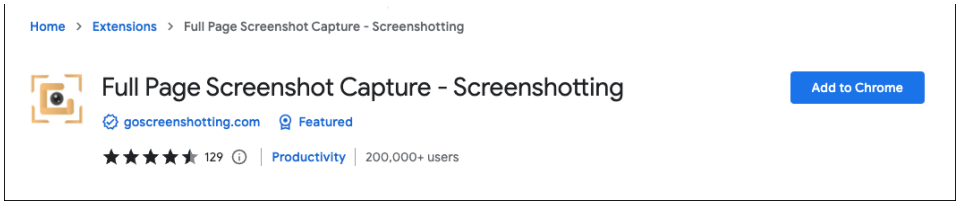
CORBIN DAVENPORT @corbindavenport
AUG 30, 2022, 4:22 PM EDT | 1 MIN READ

Google Chrome extensions can super-charge your browsing experience with more features, but there have been many malicious extensions over the years. Five more bad extensions have been discovered, thanks to a recent security report.

McAfee published a report on Monday detailing five malicious browser extensions available on the Chrome Web Store, including two “Netflix Party” extensions, “FlipShope — Price Tracker Extension,” “Full Page Screenshot Capture — Screenshotting,” and “AutoBuy Flash Sales.” Each of them had more than 20,000

downloads, with over 1,400,000 downloads combined.

> **Note:** This article is based on the research performed by . We have not examined the individual extensions and verified McAfee's claims ourselves.



One of the malicious extensions, which is also featured by Google.

Each extension listens for page changes in the browser, and each time the user navigates to a new page, the extension sends the page URL to a remote server to check if affiliate revenue code can be injected. Many sites (including *How-To Geek*) include affiliate code in links to shopping websites, which sometimes provides them with a small cut of revenue. However, most of the offending extensions are not related to buying items at all, and they are injecting the code for *all* possible pages. McAfee also found evidence that some of the extensions wait 15 days after they are installed to start injecting affiliate code, presumably to avoid initial detection.

RELATED
Browser Extensions Are a Privacy Nightmare: Stop Using So Many of Them

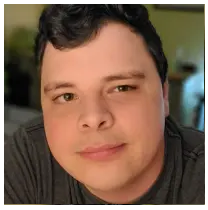
Google has been working to crack down on malicious extensions with the new Manifest V3 standard. Compared to the older Manifest V2 technology (which at least one of the extensions is using), Manifest V3 gives people more control over what pages extensions can access. Manifest V3 also blocks remotely hosted code, which would prevent some (but not all) of the behavior reported by McAfee.

The most popular Netflix Party extension, which had over 800,000 users, has since been removed from the Chrome Web Store. The

rest of them are still live, and “Full Page Screenshot Capture” still has a “Featured” label on the Store. If you have any of them installed, be sure to remove them. *How-To Geek* has reached out to Google for comment, and we will update this article when (or if) we get a response.

Source:

Via: Bleeping Computer



CORBIN DAVENPORT

Corbin Davenport is the News Editor at How-To Geek, an independent software developer, and a podcaster. He previously worked at Android Police, PC Gamer, and XDA Developers. **READ FULL BIO »**