First Chrome extension with JavaScript Crypto Miner detected

By Martin Brinkmann

Published: 2017-09-19 · Archived: 2026-04-06 01:29:20 UTC

Google's automatic verification system for Chrome extension uploads to the official Chrome Web Store is a wreck; less than a day after the Steam Inventory Helper incident, another Chrome extension was found to abuse user trust by using user systems for crypto currency mining.

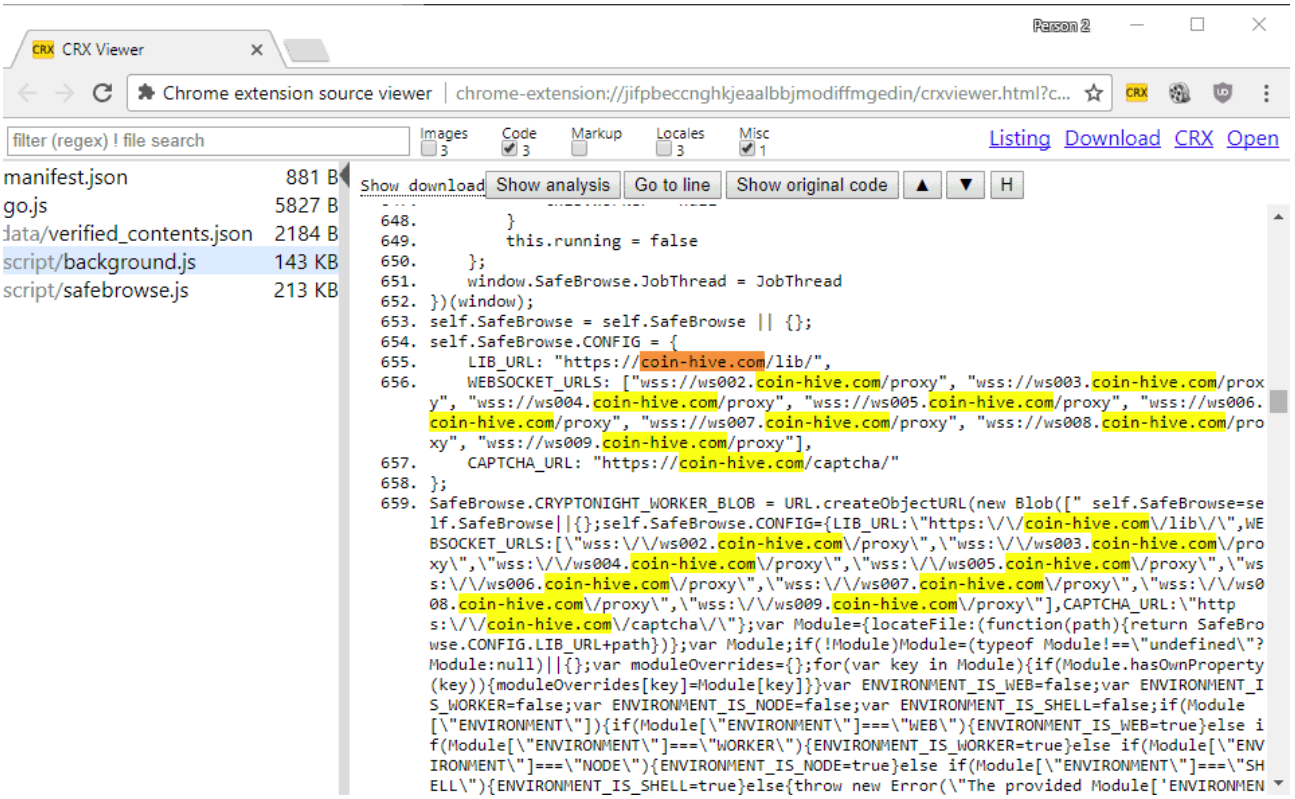
The most recent version of Steam Inventory Helper transfers any page a user visits in Chrome to a third-party server. The free browser extension SafeBrowse on the other hand runs a crypto mining module in the background while it is enabled in the browser and while the browser is open on the system.

SafeBrowse's main purpose is to skip forced intermediary advertising pages from services such as adf.ly or Linkbucks.

The most recent update of the browser extension includes a crypto miner that runs in the browser automatically. It uses the computer's processing power -- CPU -- to mine cryptocurrency.

Chrome users who have installed the browser extension may have noticed that CPU usage is going up whenever Chrome is open. Those with proper firewall protection may have noticed that connections are made to the domain coin-hive.com.

A quick look at the source code of the Chrome extension SafeBrowse confirms that connections are made to the site.



The rise of in-browser crypto mining seems inevitable.Â One of the longest standing torrent indexing sites, The Pirate Bay, was found to run a crypto miner on its website as well this month.

Torrentfreak broke the story, and a quick analysis of the Pirate Bay's code revealed that it too used the JavaScript miner provided by Coin Hive.

Now it is the first Google Chrome extension that mines crypto currency while the extension is installed, and it seems likely that it won't be the only one that will make use of such an option.

While there is nothing wrong with crypto mining in the browser, other than that it is highly ineffective as it relies solely on the processor, it becomes a huge issue if the mining is not user initiated but enforced automatically either on visit or when an extension is installed.

The first anti-mining browser extension was released recently. No Coin is designed to block known mining domains, but it may not work properly if the mining comes from an extension and not from a website.

Anyway, if you have installed SafeBrowse for Chrome, it is probably a good idea to uninstall the browser extension at this point in time.

Google needs to change its stance on the store's verification process for new extensions and extension updates. Mozilla, a much smaller organization, does this a lot better as it has a manual review policy in place for all new and updated Firefox extensions.

Source: https://www.ghacks.net/2017/09/19/first-chrome-extension-with-javascript-crypto-miner-detected/