5 super fast ways to stop digging virtual money on web browser

When mining Cryptocurrency becomes popular, website owners use Cryptocurrency mining scripts to use the visitor's CPU power to make a profit. So this article will introduce you to some methods of preventing cryptocurrency exploitation in web browsers.

Cryptocurrency is a digital or virtual currency that uses encryption for security. Because they are anonymous and decentralized, many people can use them for payment that the government cannot follow. When mining Cryptocurrency becomes popular, website owners use Cryptocurrency mining scripts to use the visitor's CPU power to make a profit. So this article will show you some methods to prevent exploiting virtual currency in web browser.

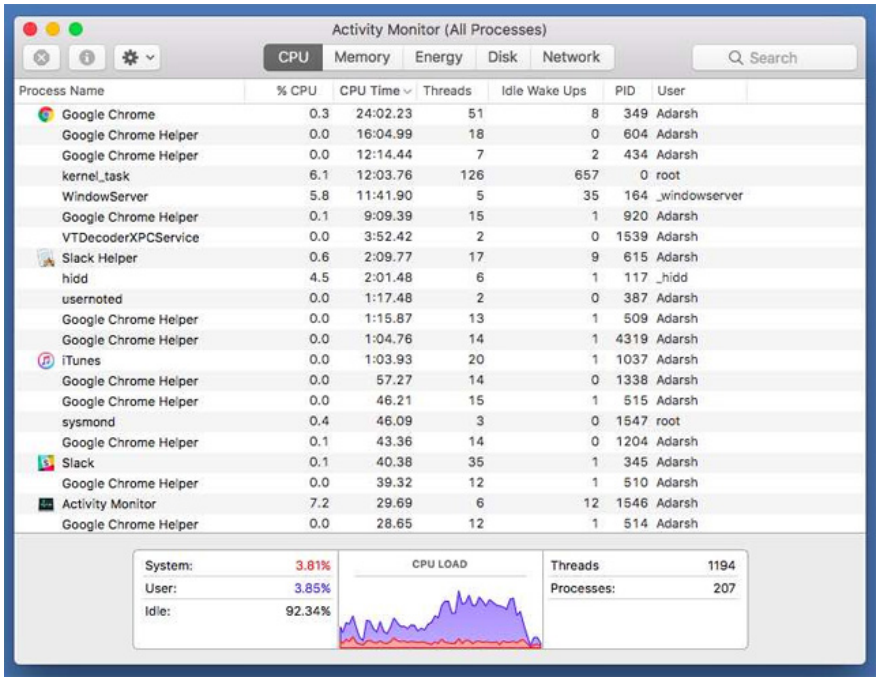
Blocking virtual money in web browser

1. How to detect computers is secretly exploiting cryptocurrency
2. How to prevent cryptocurrency exploitation in the web browser
    1. 1. Use No Coin extension for Chrome web browser
    2. 2. Use the minerBlock extension for Chrome web browser
    3. 3. Block domain names from exploiting virtual money in the host file
    4. 4. Block domain names in ad blockers
    5. 5. Use NoScripts for Firefox

How to detect computers is secretly exploiting virtual money

In addition to some ransomware, malware digging bitcoin is growing progressively. In the case of criminals using your web browser to dig money for cryptocurrency, you can completely find out easily.

1. 6 best Bitcoin digging software for Windows, Mac, Linux



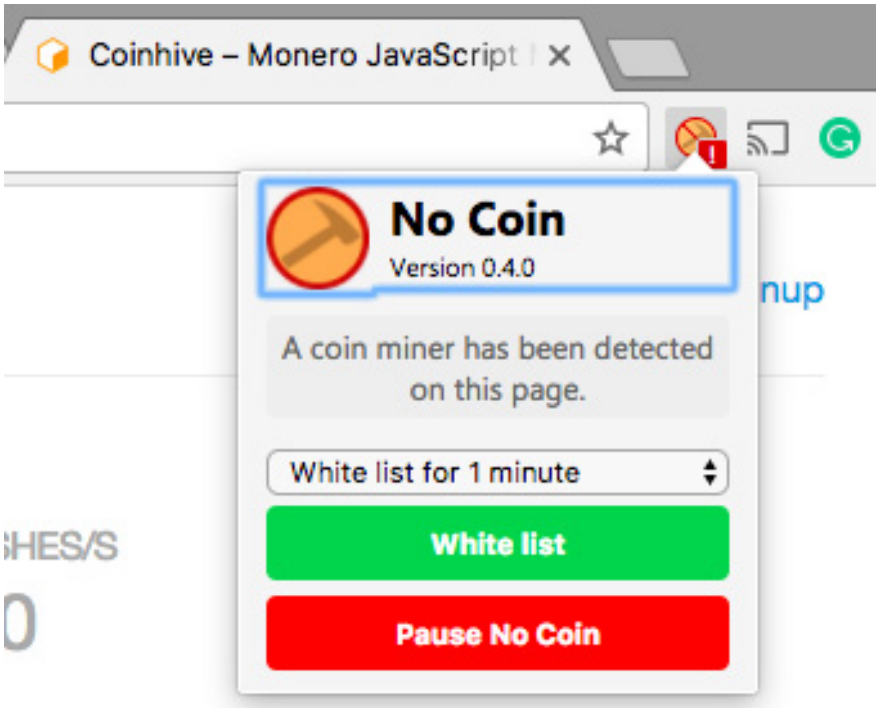
Pirate Bay users have discovered operators due to a sudden increase in CPU usage when accessing the site. You can also use the same technique to see a particular site 'stealing' the processor and making money.

How to prevent cryptocurrency exploitation in the web browser

Most websites with titles like TPB are using a new service called Coin Hive to exploit. There are simple ways to block such activities.

1. Use No Coin extension for Chrome web browser

Installing Chrome extension is the simplest method to prevent exploiting virtual currency in web browser. No Coin is a free solution. This open source extension is a reliable and secure way to control how websites are interacting with web browsers.

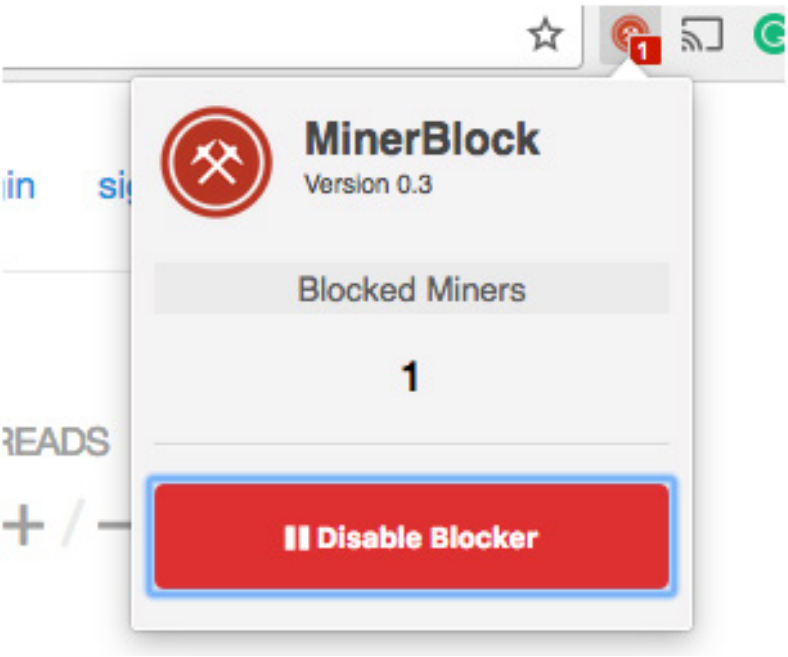


Once you access a website, No Coin will detect and display if any cryptocurrency mining activity is taking place. The user will see a red icon as shown in the illustration. Although this extension blocks any such activity, it also allows users to whitelist sites for a period of time.

Download : No Coin

2. Use the minerBlock extension for Chrome web browser

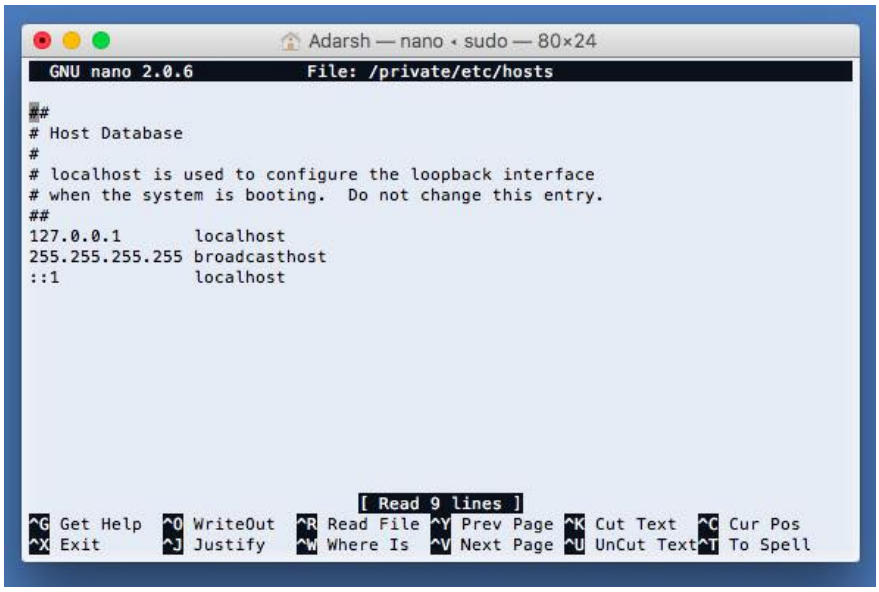
Like No Coin, the minerBlock extension is another open source tool that users can use to block cryptocurrency exploitation in web browsers. This extension lists a few popular cryptocurrency digging domains on the list. Below is a minerBlock notification when visiting the Coin Hive website:



Download : mimerBlock

3. Block domain names from exploiting virtual money in the host file

This is a manual way to block specific domains that users suspect are harmful. Because of blocking such domains, your browser will not be able to connect to these domains. We can edit the host file and redirect it to 0.0.0.0.



In Linux, users only need to open the host file by running the following command and adding 0.0.0.0 coin-hive.com at the end of the document:

sudo nano / etc / hosts

In Linux, run the following command:

sudo nano / private / etc / hosts

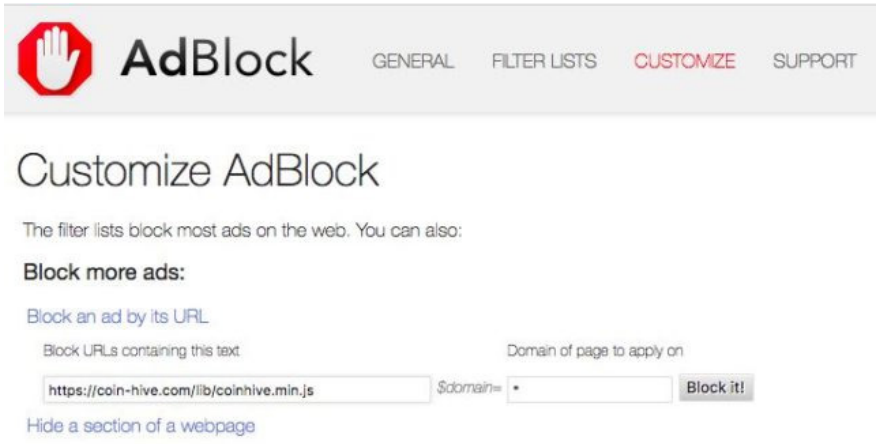
For Windows, navigate to *C: WindowsSystem32driversetc* and edit the host document to add 0.0.0.0 coin-hive.com at the end.

Note: this change will block exploitation scripts hosted by coin-hive.com. In the case of other exploit script domains, users can add them to the end of the line.

4. Block domain names in ad blockers

Ad blocking extensions like AdBlock can prevent exploiting money from cryptocurrency. Depending on the web browser, users may find relevant settings to block specific domains. For example, in Chrome, navigate to the extension list and find AdBlock. There, access **Customize > Block an ad by its URL** , then add the following text to the text box:

https://coin-hive.com/lib/coinhive.min.js



5. Use NoScripts for Firefox

For Firefox web browsers, users can use JavaScript blocking extensions like NoScript. Before using it to block exploitation of cryptocurrency in the web browser, please note that it is quite powerful and can break down many websites because it disables all scripts running on the pages.

Download : NoScript

You finished reading the article "**5 super fast ways to stop digging virtual money on web browser**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.