CRYPTOCURRENCY AND CRYPTOCURRENCY HIJACKING

Student’s name

Name of the University

Date of submission

Cryptocurrency and Cryptocurrency Hijacking

In the current world financial security in organizations, e-commerce and performing a secure transaction over the network has become the most significant issue and concern of all the parties conducting the transaction over the internet. This has caused a lot of insecurity in these organizations and parties involved in transaction form attacks and loss of their good, services offered and money paid or stolen in the process. The emergence of the cryptocurrencies systems has led to more secure and safe transactions performed and reduces the chances of loss of integrity in the systems.

Cryptocurrencies are global decentralized systems designed on a blockchain technology to generate and regulates the use of the digital currency exchanged digitally without any limitation of supply. Blockchain technology keeps cryptocurrencies on track irrespective of if they are being held in a digital wallet or used in the transaction (Hileman & Rauchs 2017).

**How cryptocurrencies systems work**

The cryptocurrencies require an infrastructure that ensures security for the effective running of the system. It has a ledger, where all transactions that are made visible for all the users thus improving integrity and trust among the parties. Ledger provides a list of entries in a database that cannot be changed by any party without satisfying certain conditions. Ledger and the cryptocurrency blockchain are decentralized meaning running without the interference of outside parties (Higbee 2018).

After the purchase is made, the transaction undergoes through a verification process after which is recorded in the history of operations on the blockchain public ledger and the miner is given a reward for their efforts based on the cryptocurrency.

**Cryptocurrency Hijacking**

Cryptocurrency hijacking is a type of an attack that allows websites or hackers to intrude into the system resources of remote computer users where it gains access into a server or a web page to take advantage of the user's resources.

**How to Protect Against Cryptocurrency Hijacking**

Testing

There are tools and methods available to test web browsers to confirm that anti-crypto-jacking tools are working. e.g. cryptojackingtest.com. The use of multiple technologies including browser and gateway solutions can help limit the risk of cryptocurrency attacks.

Antivirus software.

Use of antivirus recognizes and protects a computer against attack and malwares, providing the user with ability to detect and mitigate potentially malwares and intrusion before they cause any damage in the system.

Firewall installation

Firewalls prevents attack by blocking malicious incoming and outgoing traffic before it can get access a computer system and restricting unnecessary communications based on the set of security riles laid. A firewall establishes a barrier between the internal network and external network e.g. the Internet (Apostolaki, Zohar &Vanbever, 2017).

Security of the Browser

Different browsers offer a varying degree of protection when it comes to cryptocurrency protection. Browsers including safari by apple and google chrome have the capabilities of ad-blocking which is limited resulting in blocking few of cryptocurrency miners. This protection is available in other web browsers such as Opera and Mozilla Firefox.

Endpoint Protection

Endpoint Detection tools used to identify and to block crypto-jacking attacks on endpoints through browser scripts. Endpoint detection offers continuous monitoring and response to advanced security threats.

Gateway Protection

Web gateway protection technologies provide site filtering rules that will block cryptocurrency miners at the gateway

High Resource Utilization

Browsers provide resource utilization metrics that can help pinpoint potential cryptocurrency mining activities.

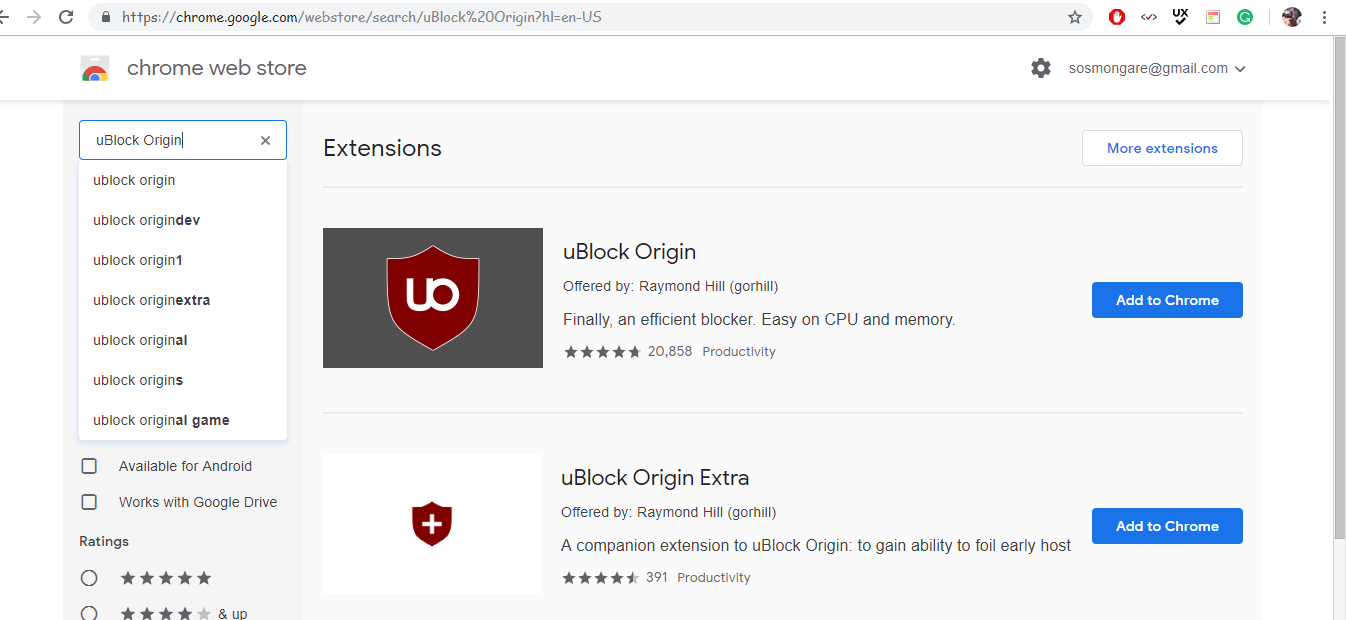
**The browser that provides the best way to block crypto jacking attack**

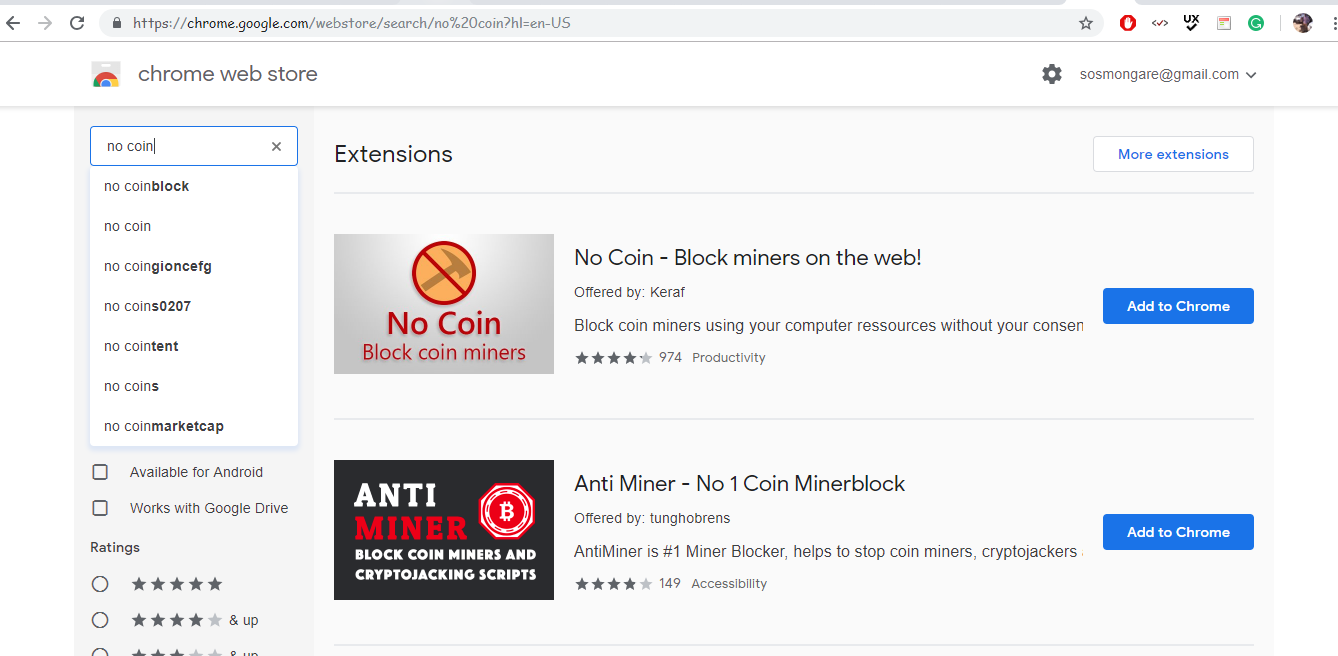
Opera offers the best prevention measures to crypto-jacking attack to its users by protecting them from unwanted crypto-mining activities. The protection measures proposed will be achieved by the browser providing no clues while browsing on your device hence ends up not exposing the device to mining. A single webpage visited by a user can take up to 5 hours of battery time if tab open. The opera browser has a feature that protects smartphones devices used from attacker mine cryptocurrencies details of the users like bitcoin.

**How to Use Browser Functionality to Block Crypto Jacking Attack**

Anti-crypto-mining extensions

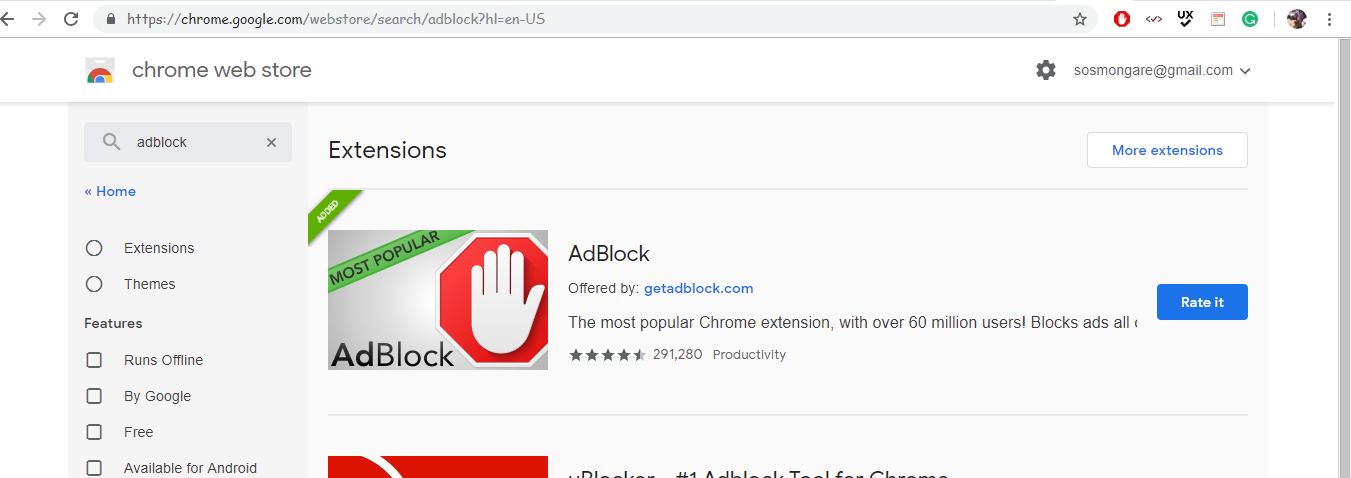
There are many extensions available in various platforms, and they include the following; No Coin for Google Chrome or Firefox, and Miner-Block for Chrome which attempts to block all connections that match with that of a known crypto-jackers. Ad-blockers may be constructed to block all known and newly recognized crypto-jacking domain names (Sigler 2018).





Block Domains with Ad Blocker

This extension is used to block adverts that can also help the parties not to access the domains names and sites due to the factors including, domains that are suspicious to spy the users CPU power and data. This extension will give the user the capability to block ads.

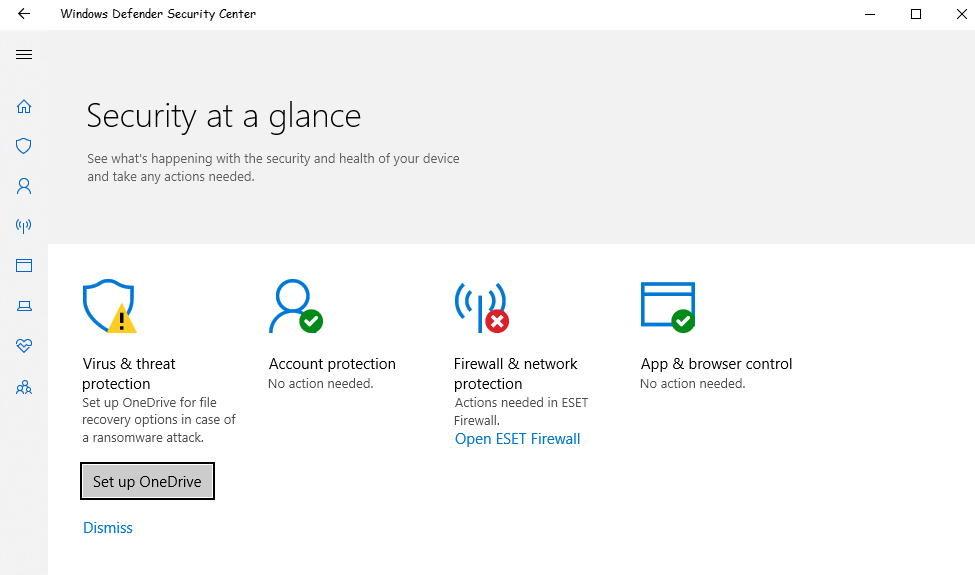


Use ad-filters on the web browser

This ad-filter uses script blocking extensions on the website to neutralize JavaScript they include; script-safe for Chrome and Firefox which warns you before scripts to run, and No-Script for Mozilla. Note that disabling JavaScript can cripple the functionality of many websites, so use these tools with caution.

Monitoring devices, networks, and resources

Monitoring should check out that there are no anonymous increments in the hardware activity and protocols to make sure that they are in place to isolate any error encountered by the devices or processes that are notorious. Example is use of antivirus like esset, avast or Windows Defender.



Using cloud-based web browsers

These run off sites and remote in the cloud rather than locally, with centralized, managed and supervised security measures that are superior to those that can be provided by the user interacting with the system or organizations that use the system to perform their interaction and day to day activities.

Corporate security awareness training

Corporate security includes informing all the parties involved aware of the warning signs and messages that indicate a crypto-jacking attack as well as knowledge of website and unwanted. Extensions for web browsers that should not be accessed to guard against two-divided attacks that exploit web browsers and attempt to get users to allow the installation of malware in the system.

Reference List

Apostolaki, M., Zohar, A. and Vanbever, L., 2017, May. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 375-392). IEEE.

Hileman, G. and Rauchs, M., 2017. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance*, *33*.

Higbee, A., 2018. The role of crypto-currency in cybercrime. *Computer Fraud & Security*, *2018*(7), pp.13-15.

Sigler, K., 2018. Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *Computer Fraud & Security*, *2018*(9), pp.12-14.