Evaluating the Effectiveness of JavaScript Crypto Miner Blocker Browser Extensions

Babak Amin Azad (111740448), Avinash Kumar (111471353)

May 15, 2018

1 INTRODUCTION

JavaScript crypto miners have been around for quite a while. Monero (XMR), the crypto currency mined by these scripts was released in April 2014. As shown in Figure 1.1, the increase in price of Bitcoin was coupled with increase in price of Ethereum and Monero. This jump led to these in browser miners being over emphasized in the media.

2 ANALYSIS OF JAVASCRIPT CRYPTO MINERS

With the rise of JavaScript crypto miners, website administrators started including miner scripts in their websites. The more the user stays on the website, the more Monero mined. "Coinhive review: Embeddable JavaScript Crypto Miner - 3 days in" [1] shows that using JavaScript crypto miners in place of advertisements provides a marginally smaller revenue. The takeaway is that miners can't replace ads, but using both of them or using miners specifically on websites where users spend more time like video sharing or gaming websites can increase the income.

2.1 REPLACING ANNOYING ADVERTISEMENTS WITH ANNOYING MINERS

Many of us use ad blockers to prevent advertisements being shown on websites when we are surfing the web. Use of these blockers brings up many arguments and ethical concerns, since advertisements are usually the source of income for websites, by blocking them the income for

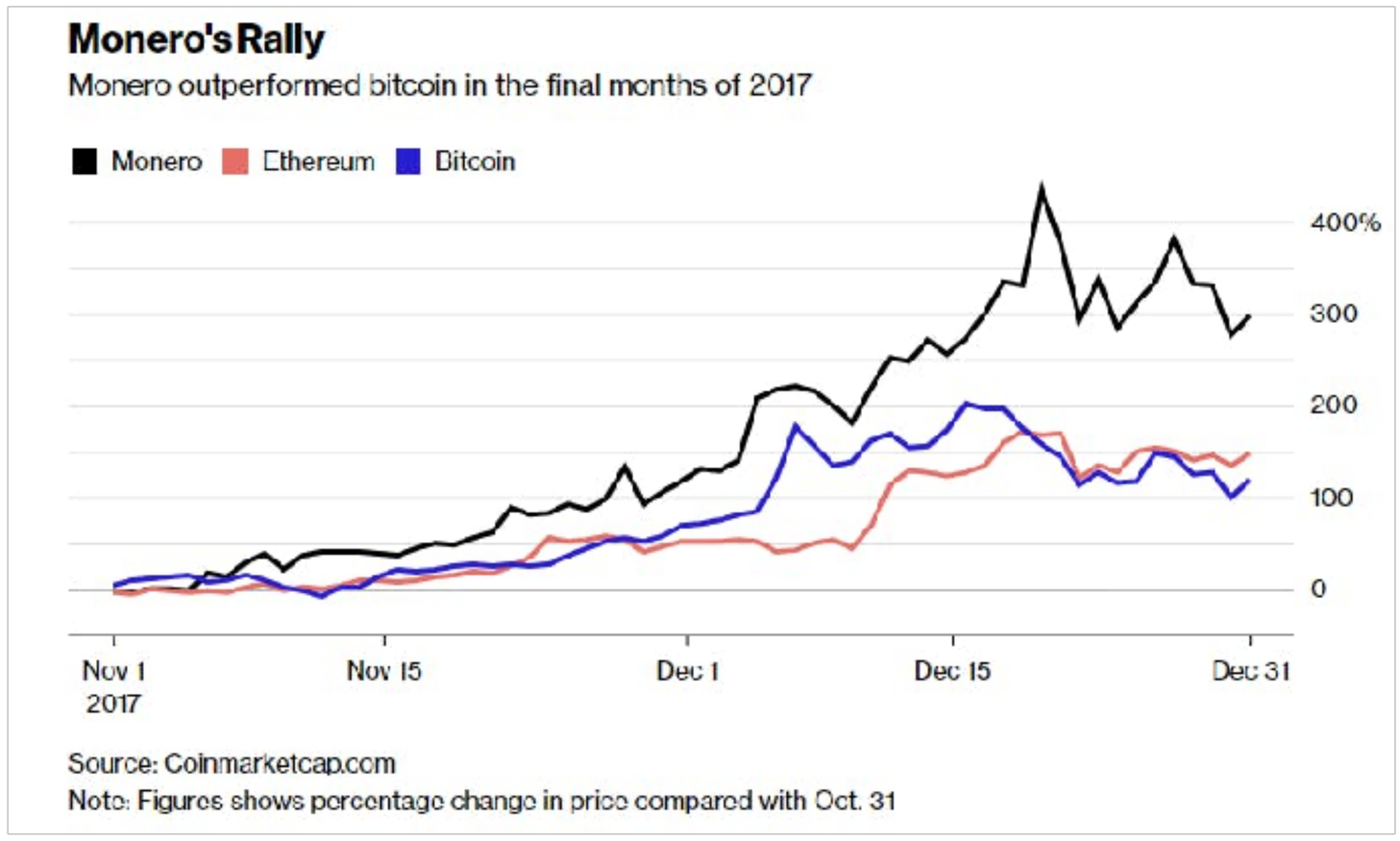

Figure 1.1: Price comparison between Bitcoin, Ethereum and Monero

Table 2.1: List of analysed browser extensions

Firefox	**Chrome**
No Coin (84,524 Users)	No Coin (570,185 Users)
No Miner (28,413 Users)	Miner Block (157,807 Users)
Miner Block (15,557 Users)	CryptoMiner Blocker (5,811 Users)
Mining Blocker (12,187 Users)	

these websites is being limited. On the other hand we see Malwaretisement campaigns abusing ad networks to distribute their malware and compromise users' machines. As websites started including miners in their pages, users started using miner blocker extensions to stop the miners from running. In this study we analysed top miner blocker extensions for Firefox and Google Chrome and report on their effectiveness. List of analysed extensions is available in the Table 2.1):

"No Coin" extension on Google Chrome, has more than half a million installation from Chrome store. In the next step we analyse the source code of these extensions. Turns out the same method of blocking is used in nearly all of them. A set of regex statements that match URLs that the main javascript for known miners are hosted on, one example of this would be:

```
https://coinhive.com/lib/coinhive.min.js
```

and the regex matching this script for different miner blocker extensions is:

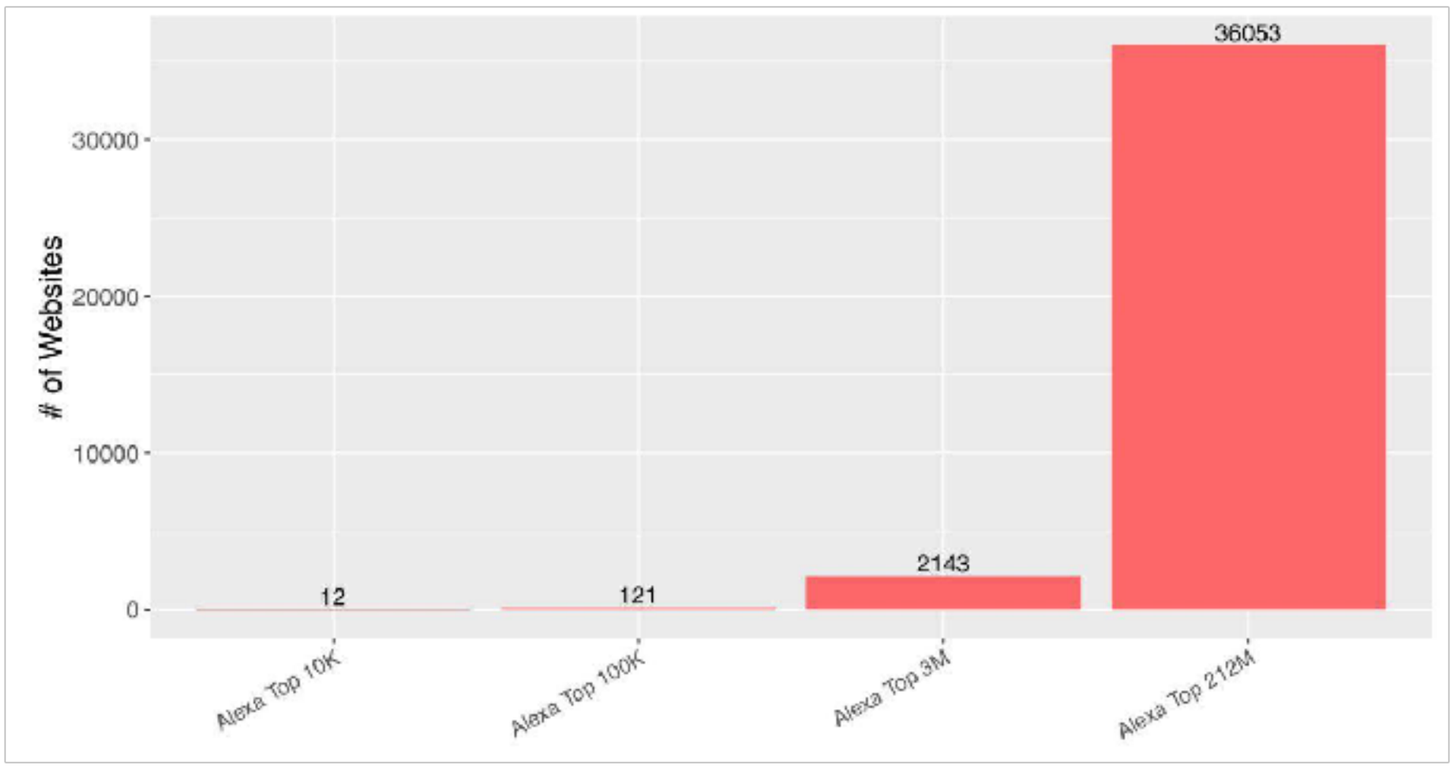

Figure 2.1: Distribution of websites using miner scripts

```
*://*.coinhive.com/*
*://*/*coinhive*.js*
*://coinhive.com/lib*
*://*.coinhive.com/lib/*
*://*/*coinhive.min.js*
```

Existing method in extensions to block miners is by detecting and blocking the main JavaScript library that has to be included in web pages. As you already noticed, by self hosting these scripts one can trivially bypass these blockers. Now let's use PublicWWW to find out how many miners on the web actually include these JavaScript libraries from the provided URLs.

Based on signatures derived from browser extensions, as depicted in Figure 2.1, we found only 12 websites in top 10k Alexa websites, this number grows linearly and reaches 36053 for Top 212M Alexa websites. This would either mean that top Alexa websites do not use miners, or it could mean that they actively try to hide their miners which makes miner blocker extensions useless.

Now let's look at the websites which use miners from another view, for this part of the report, https://fortiguard.com/webfilter, is used to categorize the URLs, since most of these samples are not well known websites, the category won't be present for most of them, but out of those which we could find a category for, this is the top ones:

1. Malicious Websites
2. Business

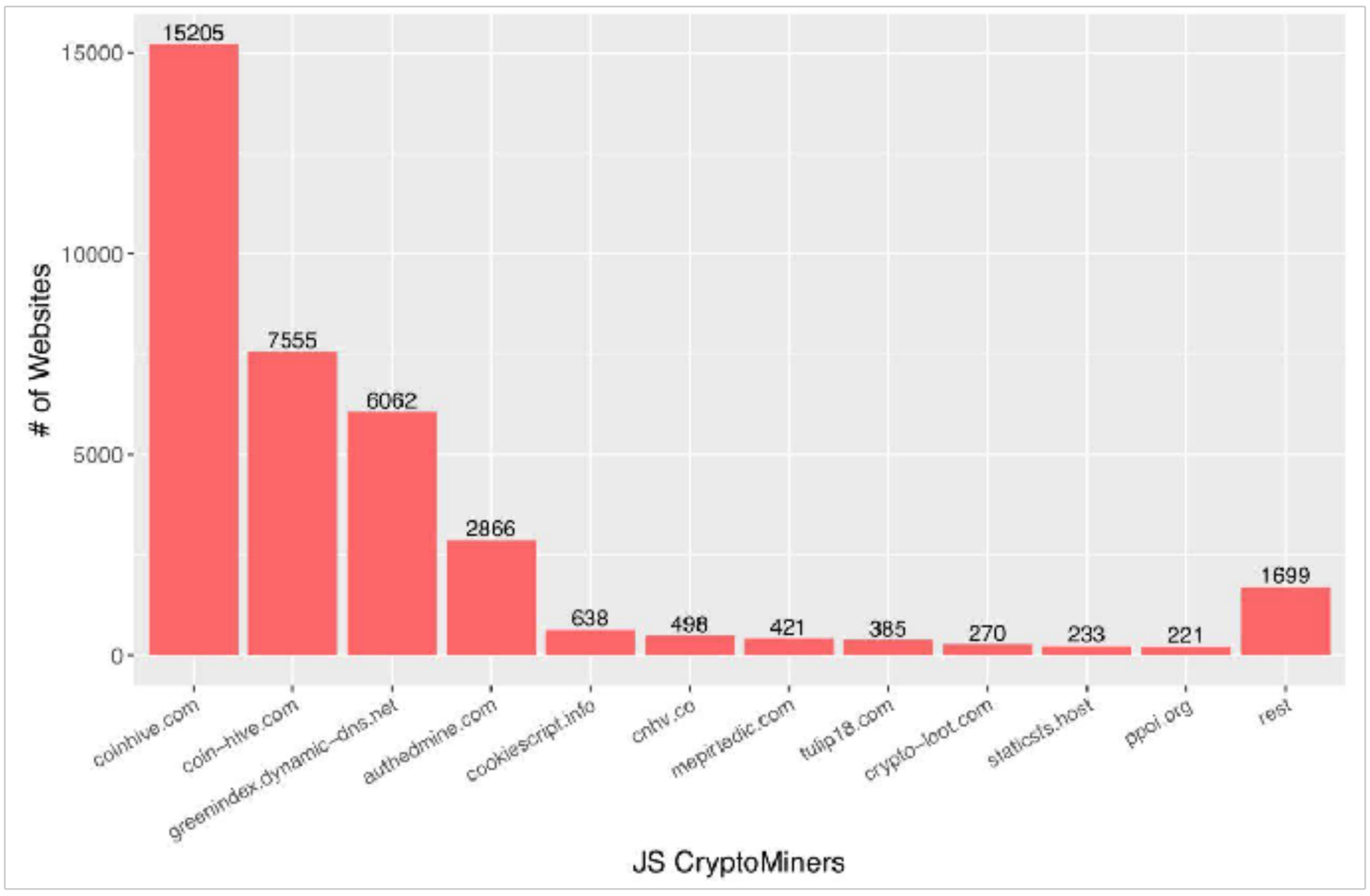

Figure 2.2: Miner script providers and their number of clients on Alexa top 212M

3. Information Technology
4. Pornography
5. Personal Websites and Blogs

Next, we analyze which miners are more popular in Figure 2.2

Figure 2.2 has a couple of interesting findings, first, coinhive and its other domains (coinhive.com, coin-hive.com, cnhv.co) together make up the most popular miners used by websites on the web. Next we have authedmine.com, which also belongs to coinhive, but this service explicitly asks the user for permission to mine on his computer, this is due to the fact that mining without users' concent was deemed as a malicious act and browser extensions started blocking them. To prevent it, coinhive proposed authedmine as a fully "ethical" counterpart of their original service.

On this list we also see crypto-loot, which is a new player in this game, they provide 80% of the mining income to website administrators compared to 70% revenue share for admins using coinhive. "rest" category is the sum of samples with presence on less than 200 websites on Alexa top 212M websites.

On this list, we see greenindex.dynamic-dns.net which looks to be a non-miner website. Our first guess was that someone hosted a miner script on their website. After doing some research, we get to their website which looks benign. They host https://greenindex.dynamic-dns.net/jqueryeasyui.js which is a version of deepMiner [2], which is a self hosted cryptominer. Various blogs point out that this miner is used in a malicious way, as in being injected into compromised websites. deepMiner has a feature to limit the amount of its CPU utilizations, and in some of the compromised websites with this specific miner URL in them, this value was set to 0.5, preventing full cpu utilization by the script as referenced by "The Growing Trend of Coin Miner JavaScript Infection" [3].

Another benign looking domain is cookiescript.info. They advertise themselves as:
The most popular free solution to US and European Cookie Laws:
"*European and American laws require that digital publishers give visitors to their sites and apps information about their use of cookies and other forms of local storage. These laws also require that consent be obtained. A breach of these regulations can result in a fine of up to $500,000.*"
As it turns out, these guys have been abusing their script that users would include in their website to mine cryptocurrencies. The two following URLs are examples of mining scripts present on this domain:

```
http://cdn.cookiescript.info/libs/cookieconsent.5.min.js
https://cdn.cookiescript.info/libs/cookiescript.min.js
```

The author of "CookieScript.info mining Monero on your website?! It's true" [4], claims that cookiescript moderators have been contacted and no response was received as of the writing.

2.2 Analyzing the miner scripts

We extracted the list of URLs that host JavaScript miner scripts. They can be used in a future research but for now, we tested their reachability. Following are some samples of URLs with invalid SSL certificates, Figure 2.3 is one example of such cases:

```
https://staticsfs.host/js/EQHAwxADAgAUxAGS
https://gtg02.bestsecurepractice.com/meri.js
```

These samples were using let's encrypt, they might have forgotten to setup auto renew script to renew certificates, but the outcome of this is that websites that include these JavaScript files won't be able to mine because browsers will not fetch scripts hosted in websites with invalid SSL certificates. This was also reported recently on twitter by *@bad_packets*, a malicious actor managed to break into a government website, but due to invalid SSL certificate of the website hosting his miner, he failed to mine crypto currency.

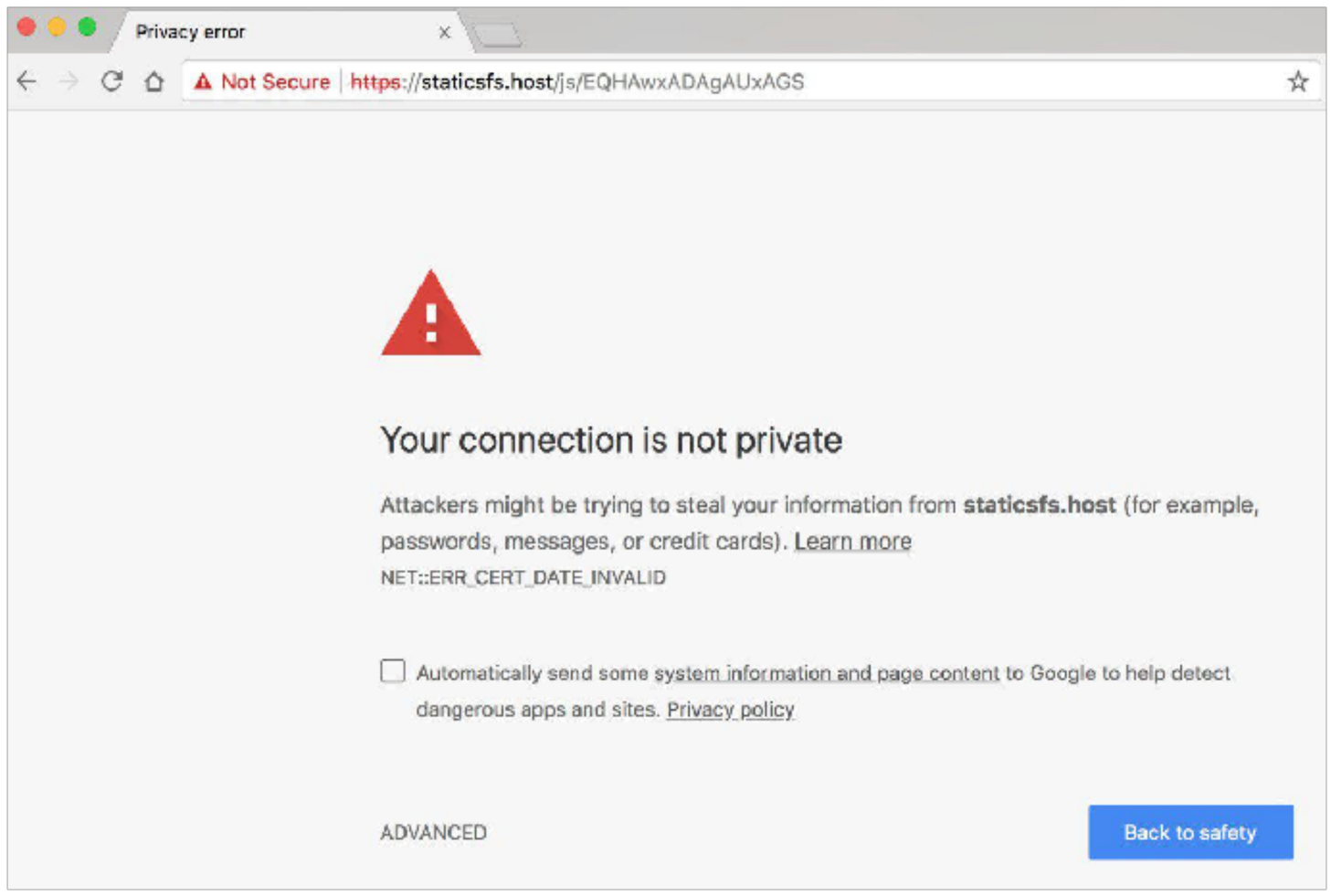

Figure 2.3: Example of miner script being hosted with invalid certificate

2.3 Malicious Miners

Now the question arises, are these the true number of websites using crypto miners? Or are there many other self hosted and malicious miners that obfuscate themselves and their URLs to stay hidden? To answer this question we can refer to "Unauthorized Coin Mining in the Browser" [5], where the author from Palo Alto Networks uses their own dataset of passive DNS and logs from their devices, shows that they observe roughly the same number of malicious infected websites by miner campaigns as we observed by using signatures used in miner blocked browser extensions.

3 Technical & implementation details

Browser extensions as ground truth source of data We reverse engineered top crypto miner blocker extensions and got the list of the miners signatures. This list was then refined to remove the duplicates and non-exiting miners. Analyzed extensions are available at https://github.com/silverfoxy/JSCryptoMinerStudy/tree/master/JSCryptoBlockerAddons.

3.1 Choice of datasource

Common Crawl We started with the idea of crawling top alexa sites (1M) on our won to fetch the page source and run our analysis on top of them. We decided to use Common Crawl datasource as our input http://commoncrawl.org/the-data/, which could provide us with periodic

crawls and stored data of web pages of our need. We downloaded top 10k Alexa pages from there and ran our analysis code to look for the miners. Our approach was to find all possible exitence of miner scripts, hence instead fo looking for just the mining script provider, we looked for all the possible regexes which could be a possible miner. We had the task of matching about 1,000 regexes with 10,000 pages. Using a single computer to run this task turned out to be very time consuming as one regex unfolds to many strings and even Python's standard regex libraries took too much time to yield results.

We modified our code to just look for the miner URLs, in place of all the regexes to bring down the run time. With Alexa top 10,000 pages, we did not find enough results to draw out some relevant conclusions. As we later supported this observation by PublicWWW, only 12 miners could be found on this subset of websites using signatures from browser extensions.

PUBLICWWW We decided to go ahead with larger number of sites and we came across https://publicwww.com/, a source code search engine. Apart from listing results and providing facility to download pages, it also exposes some APIs to fetch the result in csv format. We developed code to work with those APIs to get the data. And top of it we developed additional code to fetch relevant details for our analysis and plotting.

3.2 IMPLEMENTATION DETAILS

THE CODE is hosted on github (https://github.com/silverfoxy/JSCryptoMinerStudy). The repository has additional data and scripts which we used in former stages of the project, due to the nature of our study which included lots of data gathering, cleaning and analysis, we developed Python and Bash scripts to help us through different stages. The main code lies in the directory *pubwww*.

3.2.1 USAGE

python crawlpubwww.py: fetches following data:

- **pages** : for each miner, list of pages contaning that miner and total number of such pages, displayed as summary src of pubwww displaying the results summary of miner search, count + list
- **csvs** : csvs(url, rank, script_src) of the list of sites containing the particular miner
- **script** : csvs(url, rank, script_src_found) of miners using JS mining
- **wss** : csvs(url, rank, wss_src_found) of miners using web sockets for mining

python miner_counter.py: crawls through the fetched pages and reports the summary of a particula miner in total results

3.2.2 Crawled Data

All the crawled data lies in the following directories:

- **pubwww/data**
- **pubwww/pages**
- **pubwww/script**
- **pubwww/wss**
- **pubwww/csvs**

4 Conclusion

To study the effectiveness of available miner blocker browser extensions, we extracted the signatures used by these extensions, all observed extensions try to statically find URLs that are known to host JavaScript libraries used by these miners. Their database of signatures contain a high amount of false positive and dead links, as we were able to reduce aggregated list of 1000 signatures to 100 valid and live URLs actively hosting miner scripts.

We also show that at best, these extensions are able to detect half of known miners and website moderators can trivially bypass these extensions by self hosting and obfuscating their mining scripts. Hence, a more concrete and dynamic approach is required to detect and block JavaScript crypto miners on the web.

5 Future work

Our framework of data gathering can be run periodically to gather and compare the results to understand the usage pattern of JavaScript based crypto miners on the websites, by having access to enough computation resource, we can run our analysis over monthly crawls of Common Crawl dataset and correlate between zero-day vulnerabilities on famous websites e.g., Wordpress, Drupal, etc. and their effect on rise of number of websites that have miner scripts in them, we can also add the feature to track API keys for miners and track malicious campaigns abusing bugs to inject their own miner scripts into target websites and earn money from websites' visitors. Based on the primary information from the current study, we may crawl the specific sites where we saw the presence of miners, and derive some conclusion about, how effectively browsers work with or without blocking them. The fact that current approach used by miner blocker extensions isn't effective also points at a new area of research and future work, trying to detect miners while being URL and file agnostic, maybe behavioral analysis can be applied to scripts and find anomalies and malicious high CPU usage and put a limit on the amount of resource JavaScript files can use.

References

[1] Coinhive review: Embeddable JavaScript Crypto Miner - 3 days in, 2017. https://medium.com/@MaxenceCornet/coinhive-review-embeddable-javascript-crypto-miner-806f7024cde8.

[2] deepMiner, 2018. https://github.com/deepwn/deepMiner.

[3] The Growing Trend of Coin Miner JavaScript Infection, 2018. https://www.fortinet.com/blog/threat-research/the-growing-trend-of-coin-miner-javascript-infection.html.

[4] CookieScript.info mining Monero on your website?! ItâĂŹs true, 2018. https://www.caveconsulting.com/2018/03/23/cookiescript-info-mining-monero-on-your-website-its-true/.

[5] Unauthorized Coin Mining in the Browser, 2018. https://www.paloaltonetworks.com/resources/blogs/unit42-unauthorized-coin-mining-browser.html.