Concordia University

Information Security

INSE6630 - Bitcoin and Blockchain Technology

Case of hijacking user's CPU - Monero Javascript Miner

Authors:
Shayan Eskandari
Andreas Leoutsarakos

Supervisor:
Jeremy Clark

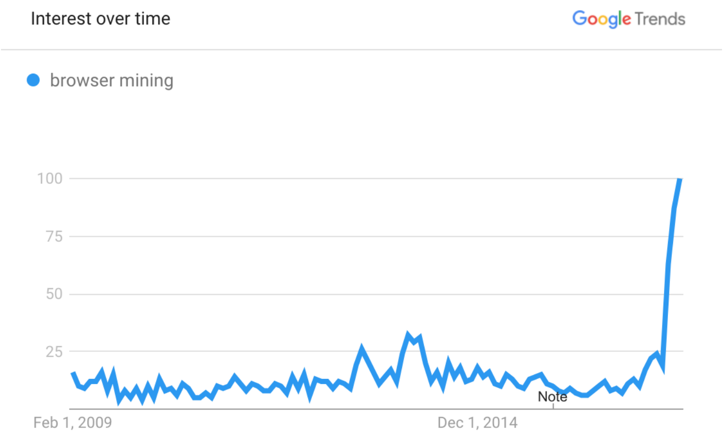
December 8, 2017

1 abstract

Browser mining is the process of running code in a web browser for the purpose of mining a cryptocurrency by performing CPU calculations. In the early days of Bitcoin, which is the most popular cryptocurrency today, this method of mining gained popularity before quickly being phased out due to the exponential increase in its mining difficulty. However, the recent emergence of egalitarian proof-of-work cryptocurrencies, such as Monero, revived the practice of browser mining by making it viable once again. Implementations of browser mining have resulted in unethical usage of such technology that infringes on user‘s rights and unsolicitedly uses their resources. The implications and real-world consequences of browser mining are explored in this paper.

2 Introduction

Bitcoin (13) emerged less than a decade ago as an open source project, which mushroomed to an industry worth more than 250 billion dollars as of this report‘s writing (6), which is made up of many different cryptocurrencies. Consequently, every day people new to the concept of cryptocurrencies look for a quick and simple way to acquire some crypto wealth. In the early days many decided to speed up the process of mining for themselves by combining CPUs and GPUs to work together. Other groups of people deployed snippets of JavaScript code on websites that recruited their visitors’ CPU power, often unknowingly, to mine for them as part of a bigger mining network (a.k.a botnet). However, both approaches quickly became infeasible as the computing power required to mine bitcoins grew exponentially to over 12 petahashes/s (3), and lead to the emergence of application-specific integrated circuits (ASICs) and collective mining pools to continue the mining race. As the years passed and a few key cryptocurrencies emerged as the market leaders, the concept of in-browser crypto-mining largely became forgotten. Today, the most common way for the average person to acquire cryptocurrencies is to purchase them. Unusually, stories began to circulate on popular media outlets this year of websites mining cryptocurrencies through browsers again. And even more intriguingly, high profile websites were now involved, and the practice seemed to be growing at a quick pace.



Search interest for “browser minin” over time

The graph above shows how the searches for “browser mining” have changed since Bitcoin was launched. Search interest seems to have piqued during price surges, which culminated with Bitcoin crossing $1000 USD. Soon after Bitcoin‘s first major crash, searches consistently waned until a recent large spike that is more than 4 times the lifetime average. The waning period before the recent surge could be attributed to the advent of ASIC usage for Bitcoin mining, and the surge is likely due to the revival of browser mining for non-Bitcoin currencies that have gained a sizeable market capitalization. As a result, websites like Showtime.com (18), and ThePirateBay.org (11) have been experimenting with in-browser mining as a way to add a new revenue stream.

3 Egalitarian Proof-of-Work

One of the reasons for the resurgence of this type of mining is the recent rise in price and popularity of the cryptocurrency Monero (12). Launched in April 2014, Monero focuses on privacy by obfuscating the participants and amounts in transactions. This is in contrast to more popular cryptocurrencies like Bitcoin and Ethereum where transactions can be traced back through the entire blockchain. In fact, Monero gained some fame for its ability to anonymize bitcoins by converting them into Monero, transacting them privately, and then converting them back to bitcoins. This has made Monero popular on black market websites where illicit goods can be purchased without having transactions traced back to buyers.

More importantly, Monero differs in the way its currency is mined by employing a proof-of-work that is egalitarian by design. This is achieved by using the proof-of-work algorithm named CryptoNight (7), which makes its puzzle resistant to ASICs and fast memory-on-chip devices with low latency. While many cryptocurrencies use a similar type of proof-of-work, Monero was one of the earliest to adopt and popularize it.

Bitcoin uses SHA-256 for its hash-based proof-of-work algorithm, which is a CPU-bound function. This allows miners to use ASIC devices to increase their calculation speeds, which greatly surpasses an ordinary computer in hashes per unit of money. CryptoNote, which is an evolution of Bitcoin that acts as the application layer protocol to power several cryptocurrencies such as Monero, chose CryptoNight for its proof-of-work. CryptoNight uses a memory-bound function, which relies on a situation where the time taken to complete a given computational problem is decided primarily by the amount of memory required to hold data. This limits the ability for pipelining, which is also known as instruction-level parallelism.

Satoshi Nakamoto's original philosophy and intention for Bitcoin was "one-CPU-one-vote" (13), which CryptoNight attempts to enforce. In CryptoNight, users vote for the right order of transactions and honest money supply distribution with their CPU power, so the more CPU cores they have the more voting power they acquire. Since CPUs are relatively affordable and accessible, it follows that most users will have approximately equal voting rights. Then by relying on random access to a slow memory and emphasizing latency dependence, it is ensured that proof-of-work is largely controlled by CPUs instead of GPUs and ASICs. This is done by having every new block depend on the previous block's solution, which must be kept in memory. This algorithm requires approximately 2MB per instance, which fits in the L3 cache per core of modern processors. Over the course of the next few years, these modern processor L3 cache sizes should become mainstream and allow more CPUs, and thus users, to vote in the Monero ecosystem. It has also been shown that ASICs cannot handle more than 1MB of internal memory, which is less than the size of memory required to calculate a new block. GPUs are also at a disadvantage since GDDR5 memory, for example, is notably slower than L3 cache (19).

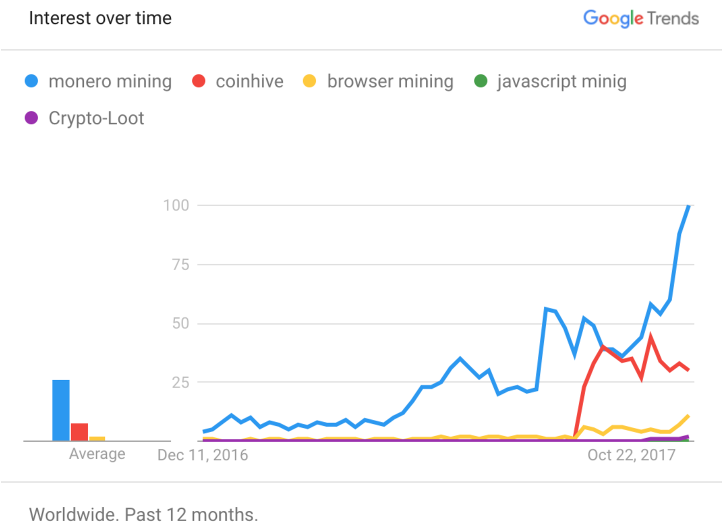
4 Browser Mining

The concept of browser mining can be described as accessing the CPU processing power through the JavaScript programming language on a web browser instead of a standalone application. This allows for more scalability as there is no need to install any software on a computer, and instead the script can combine multiple CPUs to execute the same task while running in the the browser with an internet connection. In the early days of cryptocurrency mining, there was a rise of Bitcoin JavaScript miners such as JSMiner[1](2011) and MineCrunch[2](2014). Minecrunch had a bigger campaign and more online presence from their developers. Based on what the developer claimed, the JavaScript miner was optimised and worked 1.5x slower than native CPUMiner[3], which was an application to mine on CPUs. However, as the hashing power of the Bitcoin network increased the mining difficulty similarly increased, and Bitcoin CPU mining was no longer profitable. As a result, the developers stopped maintaining the codebase of such miners.

As Monero became more popular, it caught the attention of some independent developers who decided to revisit the idea of browser mining. One of the earliest efforts appeared in September 2017 called Coinhive (5), and soon after a competitor named Crypto-Loot[4] emerged. Both were startups that provided an API to websites to implement that would mine their visitors‘ CPU resources to mine Monero. A portion of monero would go back to the startup, and the rest would be kept by the website. Not long after their early success, several copycats appeared such as Coin-Have and PPoi (8). It even inspired a new coin specifically desiged for browser mining named JSECoin. These developments took place over a few short weeks, which signaled the renwed success of browser mining. However, Coinhive‘s approach as a legitimate startup set it apart from its peers and established itself as the leader in the space. They also launched separate services such as proof-of-work CAPTCHAs and shortlinks, which could be used to prevent spam while mining Monero (5).

5 State of affairs

In order to find out how browser mining is changing internet use, the approach taken was to find measurements of the impact. One is to see what is the search interest over time for such services.



Google Trend - Search interest over last 12 months

It seems there has been more interest in Coinhive, even more than the terms such as B̀rowser mining. Comparing to other services offering Monero browser mining API, Coinhive had the advantage of being the first to offer the service, hence more interest at the time of writing. There has not been enough data and evidence of usage for

[1] A JavaScript Bitcoin miner https://github.com/jwhitehorn/jsMiner

[2] Minecrunch, web(JS) miner with integration featurehttps://cryptocurrencytalk.com/topic/24618-minecrunch-web-js-miner-with-integration-feature/

[3] CPU miner for Litecoin and Bitcoin - https://github.com/pooler/cpuminer

[4] Crypto-Loot - A web Browser Miner — Traffic Miner — CoinHive Alternative https://crypto-loot.com/

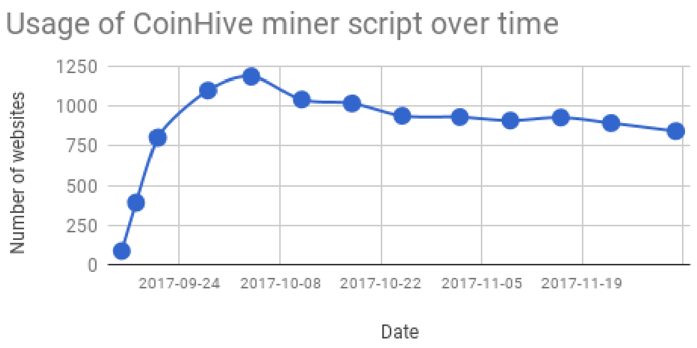
other services to analyze, thus the focus of this paper is on the impact of Coinhive scripts on internet.

Next step was to see how many websites are jumping on Coinhive train using Internet scanners such as Zmap[5]. More interestingly is to see how the trend of this usage was, for this purpose historical data is required.

Listing 1 BigQuery SQL query to find websites using coinhive miner script

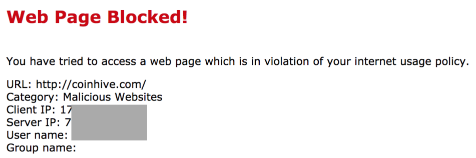
```
SELECT domain, tags, p80.http_www.get.headers.content_language, p80.↩
    http_www.get.headers.server, p80.http.get.headers.x_powered_by, p80.↩
    http.get.title , p80.http_www.get.body as wwwbody, p80.http.get.body ↩
    as plainbody
FROM `censys-io.domain_public.20171123`
WHERE STRPOS(p80.http.get.body, 'coinhive.min.js') >0 or STRPOS(p80.↩
    http_www.get.body, 'coinhive.min.js') >0)
```

Using censys.io Bigquery dataset (9), it is feasible to query for such trends. The method used to gather these data is simply looking for the ‘coinhive.min.js‘ script within the body of the website page, which could be circumvented if the website owner uses a custom version of this script (e.g. renamed hosted file).



Usage of CoinHive Miner scripts in top 1million websites over time

As seen in the chart above, the adaptation of this script was massive in the first days of release. However the progress slowed down as Adblockers and organizations started to block Coinhive website. The initial purpose of this service as claimed by Coinhive website, is to replace ads and cover server costs for the webmasters. Although as the service did not require user consent, it started to be used as a malicious activity on user‘ s browsers and Coinhive was included in the top 10 most wanted malwares after some famous randomwares (4).



Web Page Blocked!

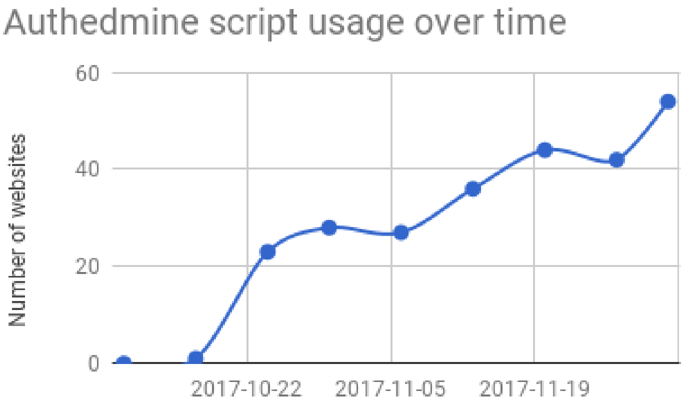
You have tried to access a web page which is in violation of your internet usage policy.

URL: http://coinhive.com/
Category: Malicious Websites
Client IP: 17[redacted]
Server IP: 7
User name:
Group name:

Concordia University blocked page for coinhive.com

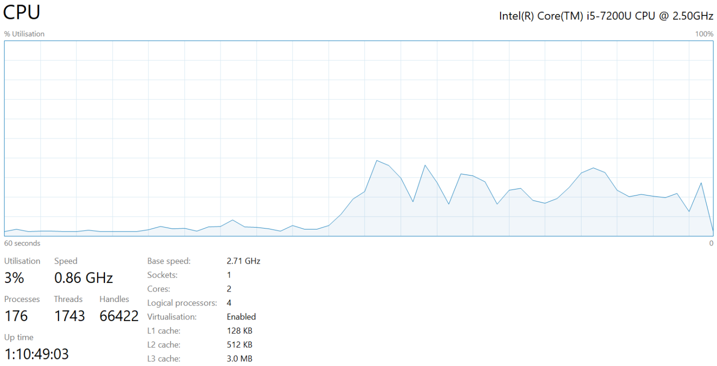
This helped the copycats to gain some market attention, but also pushed Coinhive developers to think of other methods which are more focused on user consent and bypassing blockage for running such scripts. Coinhive introduced another domain and service called “Authedmine” , which requires user‘s consent to start mining on the browser. This service did not get the same attention as the original service. Although this brought up the discussion about ethics of such services, which is covered in Discussion section of this paper.

[5] https://zmap.io



Usage of AuthedMine Miner scripts in top 1million websites over time

Except the first few days of launch, most of these scripts are defaulted to use around 25% of user‘s CPU, which can be justified as to be under threshold of user‘s attention or to fairly use their hardware. The first few days, there has been reports of 100% of CPU usage when visiting websites containing these script (15). ** MAYBE A BIT MORE ON CPU USAGE **



Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz

Utilisation 3%
Speed 0.86 GHz
Processes 176
Threads 1743
Handles 66422
Up time 1:10:49:03

Base speed: 2.71 GHz
Sockets: 1
Cores: 2
Logical processors: 4
Virtualisation: Enabled
L1 cache: 128 KB
L2 cache: 512 KB
L3 cache: 3.0 MB

CPU usage with authedmine off at beginning and on after

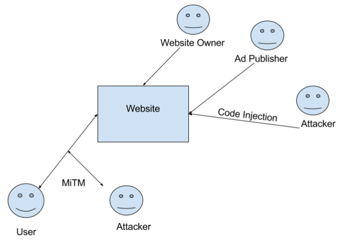
6 Discussion

The opinion of the authors of this report maintain that users should be given the option to enable the miner code in their browser with some benefit to their experience on the website. An example of a benefit could be the removal of advertisements. Recent polls, such as the one conducted by Bleeping Computer, which found that, “many users said they are OK with websites mining Monero in the background if they don‘t see ads anymore” (2). Another example would be granting access to premium features of the website such as journal articles behind a paywall, or streaming in high-definition. The website could also allow the user to participate in mining rewards by allocating a large portion of their CPU resources to the activity of mining, which would benefit both parties. By notifying the user of the potential of this activity, and allowing them to make a choice to participate, the website maintains trust in their relationship with the user while also benefiting from a new source of revenue. By foregoing disclaiming this new activity that can have harmful effects, the website will only gain a new revenue stream for a short time while sacrificing their reputation. Coinhive‘s recent response to the market‘s negative reaction by releasing AuthedMine, which enforces user consent before enabling of any mining JavaScript code, justifies this rationale. However, before this could develop into a sustainable model, the security implications and user impact should be addressed.

6.1 Security

Attack surface to abuse user‘s browsers is broad. If the browsers do not block such scripts, there are different actors which can abuse this functionality for their own profit without user consent.

- **Website Owner:** As discussed before, the website administrator can add the script to the webpage without informing users
- **Ad Publisher:** Similar to the claimed Showtime case (18) the advertisement publisher can inject miner script to any website they have ad space in, instead of showing ads (more on this in User Impact section).
- **Hacked Website:** An attacker can hack the website and inject the miner code to the website
- **Man-in-the-middle attack:** Any internet service provider or free public wireless can inject the script to all the plain text traffic that goes through their routers. Ad injection has been seen in the wild (17) but no reports of miner scripts being injected as of the time of the writing.



Attack vectors to inject miner scripts in webpages

6.2 User Impact

Most in-browser crypto-minings are running without the consent, nor knowledge, of the users involved. The websites that have been found running JavaScript code for the purpose of mining usually employed Coinhive‘s API. One such website, for example, ThePirateBay.org (1), which ran the JavaScript code when users searched for torrent files. Perhaps unsurprisingly, there was no notice in their Privacy Policy nor visible warning on any part of the website that informed their users of this activity. This resulted in a backlash against the website, which responded with the follow statement, “Do you want ads or do you want to give away a few of your CPU cycles every time you visit the site?” (15). While they admitted to their testing of browser mining, their notice came after the fact and resulted in the removal of the JavaScript code altogether. This is in contrast to the banners users are presented with upon the first visit to a website that warns them of the website‘s policy on cookies, which is now enforced through EU laws (10). It’s now widely known that these cookies can be used to track users across the internet, so cookie banners can act as a reminder and allow the user to make better informed decisions regarding their browsing habits. Without any type of disclaimer for users, websites admins have been commandeering their users‘ CPU resources for their business and personal gain. This results in higher energy bills for the user, along with accelerated device degradation, and slower system performance (14).
A second example of a popular website deploying Coinhive’s API is Showtime.com (14), which is a popular cable channel that also streams their TV shows online. It then came as no surprise when UFC.com was accused of using this very same code on the night

of one of their most popular events (16). Both Showtime and UFC defended their actions by claiming that the miner was unknowingly activated through an ad injection. Whether this claim is true or not, the recent trend of streaming websites deploying Coinhive‘s API could be due to the high costs of providing streaming. While ads can be used to offset some of the costs, it would be of interest to some to at least experiment with the idea of recruiting their users to mine Monero, which can later be sold for cash.
We also see the potential for this new form of revenue generation to compete with advertisements and reduce how many ads a user sees on a given website, and perhaps one day even replace them. This is because the malware that is associated with advertisements is still a growing concern, and the public‘s dislike of advertisements will persist and never wane. Also, as cryptocurrencies continue to grow in market capitalization and use cases, their inevitable mainstream use will push the profitability of egalitarian proof-of-work cryptocurrencies such as Monero well into the future. Many blogs have discussed this potential, such as the CEO of OTAMate Technology Ltd, Carl Whalley, who discussed the potential of browser mining one day replacing ads (20).

7 Future Work

Similar to regulations for cookies and user tracking, there is a need to regulate such scripts, mainly to notify user about existence of these scripts on the webpages they visit. Also there is the need to standardize this model, such that to answer some of these questions: If every website uses a browser miner and user has many tabs open, how are user‘s CPU shared between them? How the behaviour of these scripts changes based on the device they are running on? If device is on power saving mode, how that affects the execution?

Better security design is required to narrow down the attack surface, such as using SSL/TLS or tokenizing the requests to make sure websites get user‘s consent before running these scripts.

Surveys with larger sample sizes and diversity is required to gauge users acceptance. These surveys should answer how much cpu power users are willing to volunteer, and if battery impact would change the outcome.

As mentioned previously, browser mining is not as efficient as native mining applications. There can be optimization on how browsers pass system calls to the operating system, or there can be browsers designed specifically to support efficient browser mining.

This new model of monetizing websites can be a paradigm shift in how advertisement giants monopolize the internet traffic. This could lead to re-democratizing the online advertisement ecosystem to make it more fair for small players.

References

1. BBC. Websites hacked to mint crypto-cash. http://www.bbc.com/news/technology-41518351, 2017.
2. BleepingComputer. The internet is ride with in-browser miners and it is getting worse each day. https://www.bleepingcomputer.com/news/security/the-internet-is-rife-with-in-browser-miners-and-its-getting-worse-each-day/, 2012. Accessed: 2017-12-08.
3. Blockchain.info. Bitcoin hash rate. https://blockchain.info/charts/hash-rate, 2017. Accessed: 2017-11-20.
4. CheckPointResearchTeam. October's most wanted malware: Cryptocurrency mining presents new threat. https://blog.checkpoint.com/2017/11/13/octobers-wanted-malware-cryptocurrency-mining-presents-new-threat/, 2017.
5. Coinhive. Coinhive monetize your business with your users cpu power. https://coinhive.com/, 2017. Accessed: 2017-11-20.
6. Coinmarketcap. Global charts. https://coinmarketcap.com/, 2017. Accessed: 2017-11-20.
7. Cryptonote. Cryptonote technology. https://cryptonote.org/inside.php#equal-proof-of-work, 2017. Accessed: 2017-11-20.
8. DeepDotWeb. Coinhive hacked and launches new opt-in service. https://www.deepdotweb.com/2017/11/11/coinhive-hacked-launches-new-opt-service/, 2017.
9. Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by Internet-wide scanning. In *Proceedings of the 22nd ACM Conference on Computer and Communications Security*, Oct. 2015.
10. European-Commission. Cookies. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm, 2011. Accessed: 2017-12-08.
11. ExtremeTech. Browser-based mining malware found on pirate bay, others. https://www.extremetech.com/internet/255971-browser-based-cryptocurrency-malware-appears-online-pirate-bay, 2017. Accessed: 2017-11-20.
12. Monero. MONERO private digital currency. https://getmonero.org/, 2014. Accessed: 2017-11-20.
13. S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
14. TheGuardian. Ads dont work so websites are using your electricity to pay the bills. https://www.theguardian.com/technology/2017/sep/27/pirate-bay-showtime-ads-websites-electricity-pay-bills-cryptocurrency-bitcoin, 2017. Accessed: 2017-11-20.
15. ThePirateBay. The galaxys most resilient bittorrent site. https://thepiratebay.org/blog/242, 2017. Accessed: 2017-11-20.
16. TheRegister. Lets get ready to grumble! ufc secretly choke slams browsers with monero miners. https://www.theregister.co.uk/2017/11/07/ufc_coin_hive/, 2017.
17. TheVerge. Hotel caught injecting advertising into webpages on complimentary wi-fi network. https://www.theverge.com/2012/4/7/2931600/hotel-caught-injecting-advertising-into-web-pages-on-complimentary-wi, 2012. Accessed: 2017-12-08.

18. TheVerge. Showtime websites secretly mined user cpu for cryptocurrency. https://www.theverge.com/2017/9/26/16367620/showtime-cpu-cryptocurrency-monero-coinhive, 2017. Accessed: 2017-11-20.
19. N. van Saberhagen. Cryptonote v 2. 0. https://bytecoin.org/old/whitepaper.pdf, 2013.
20. C. Whalley. Could cryptocurrency kill online advertising? https://www.linkedin.com/pulse/could-cryptocurrency-kill-online-advertising-carl-whalley/, 2012. Accessed: 2017-12-08.