

A first look at browser-based cryptojacking

Shayan Eskandari*, Andreas Leoutsarakos*, Troy Mursch†, Jeremy Clark*

*Concordia University, †Bad Packets Report

Abstract—In this paper, we examine the recent trend towards in-browser mining of cryptocurrencies; in particular, the mining of Monero through Coinhive and similar code-bases. In this model, a user visiting a website will download a JavaScript code that executes client-side in her browser, mines a cryptocurrency—typically without her consent or knowledge—and pays out the seigniorage to the website. Websites may consciously employ this as an alternative or to supplement advertisement revenue, may offer premium content in exchange for mining, or may be unwittingly serving the code as a result of a breach (in which case the seigniorage is collected by the attacker). The cryptocurrency Monero is preferred seemingly for its unfriendliness to large-scale ASIC mining that would drive browser-based efforts out of the market, as well as for its purported privacy features. In this paper, we survey this landscape, conduct some measurements to establish its prevalence and profitability, outline an ethical framework for considering whether it should be classified as an attack or business opportunity, and make suggestions for the detection, mitigation and/or prevention of browser-based mining for non-consenting users.

Index Terms—Cryptocurrency; Monero; Coinhive; Mining; Bitcoin; Blockchain; Cryptojacking; Ethics

1. Introduction

Bitcoin [21] emerged almost a decade ago as an open source project, which mushroomed into a cryptocurrency sector collectively capitalized at over \$500 billion USD¹. 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 of Bitcoin, users on their personal computers could effortlessly acquire the currency through mining—a process Bitcoin uses to incentivize nodes to verify transactions as they are recoded in the blockchain. However, a second wave of mining technology saw users augmenting the CPU power of their computers with GPUs. Other groups of people deployed snippets of JavaScript code on websites that recruited their visitor’s CPU power, often unknowingly, to mine for them as part of a bigger mining network (*i.e.*, a mining pool). However, both approaches quickly became infeasible as the computing power required

1. Coinmarketcap - Global Charts - Accessed: 2017-12-14 <https://coinmarketcap.com/>

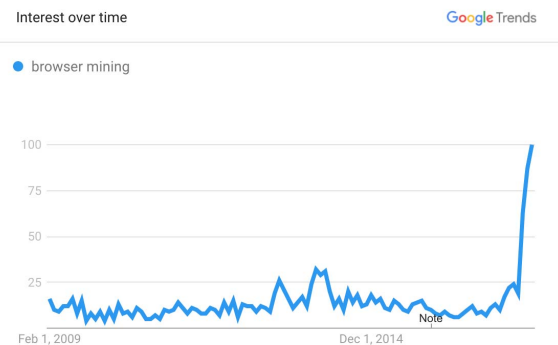


Figure 1. Search interest for “browser mining” over time. Search interest seems to have piqued during price surges, which culminated with Bitcoin crossing \$1000 USD for the first time in December 2013. Soon after Bitcoin’s first major crash searches consistently waned until a recent large spike, which 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.

to mine bitcoins grew exponentially to over 12 petahashes². This was due to the emergence of application-specific integrated circuits (ASICs) and collective mining pools, which continue the third wave of mining to this day [23].

As the years passed and a few key cryptocurrencies emerged as the market leaders, the concept of browser mining largely became forgotten. Today, the most common way for the average person to acquire cryptocurrencies is to purchase them. It came as a surprise to many when stories began to circulate on popular media outlets this year about websites mining cryptocurrencies through browsers again. Figure 1 shows how the searches for “browser mining” have changed since Bitcoin was launched. Websites like The Pirate Bay [10] experimented with browser mining as a way to add a new revenue stream, while others like Showtime.com [40] claimed they had the code injected after they were discovered.

This paper tells the story behind the rejuvenation of browser-based mining. It is centred on *cryptojacking* (also known as *coinjacking* and *drive-by mining*), a term coined to refer to the invisible use of a vulnerable user’s computational resources to mine cryptocurrencies. Technically in-browser mining is a subset of cryptojacking, although most uses

2. Bitcoin hash rate - Accessed: 2017-11-20 <https://blockchain.info/charts/hash-rate>

of the term apply to browser-based mining. In this case, mining happens within the client browser when the user visits the website. We have also seen the term cryptojacking applied to malware that mines cryptocurrencies, or in the situation where malware renders a machine as an unwitting participant in a botnet, and the botnet is rented for the purposes of mining cryptocurrencies (*cf.* [12]). The resource consumption of in-browser cryptojacking can noticeably degrade a computer's performance.

2. Preliminaries and Related Work

2.1. Browser-based Mining

2.1.1. Early days. The idea of in-browser mining started in the early days of Bitcoin. Bitcoin Plus³ is one example of a discussion on replacing ads with Bitcoin browser miners⁴. It was also argued that browser-based mining provides greater scalability and decentralization as the barrier to entry is lowered to any unmodified computer with an internet connection. Soon after there was a rise in Bitcoin JavaScript miners such as JSMiner (2011)⁵ and MineCrunch (2014)⁶. MineCrunch's visibility was increased by campaigns and the active online presence of its developers. Based on the developer claims, MineCrunch was well optimized for Javascript, but still worked 1.5x slower than native applications for CPU mining (*e.g.*, CPUMiner⁷). Although CPU mining became uncompetitive with GPU and ASIC-based mining, it remained a sandbox for botnet admins to experiment with the thousands of CPUs at their disposal. Botnet mining has been studied in the literature [12], [45], as well as covert mining within enterprises and cloud environments [32].

In addition to unprofitability, browser-based mining faced legal challenges. In May 2015, the New Jersey Attorney General's office reached a settlement with the developers of "Tidbit", a browser-based Bitcoin miner. Terms of the settlement included ceasing operations of Tidbit. Then acting Attorney General John J. Hoffman stated "No website should tap into a person's computer processing power without clearly notifying the person and giving them the chance to opt out." [24].

2.1.2. From one CPU to ASICS and mining pools. The first Bitcoin block mined on a GPU happened on July 18th, 2010 by a user named ArtForz [44], by using a private mining code that he developed himself. It was not until mid-2011 that others started implementing and releasing

3. Bitcoin For the Uninitiated: Now, A Browser-Based Mining Client May 19th, 2011 <https://www.themarysue.com/browser-based-bitcoin-mining/>

4. BitCoin browser mining as a replacement for ads https://www.reddit.com/r/Bitcoin/comments/ieaw/bitcoin_browser_mining_as_a_replacement_for_ads/

5. A JavaScript Bitcoin miner <https://github.com/jwhitehorn/jsMiner>

6. MineCrunch, web(JS) miner with integration feature <https://cryptocurrencytalk.com/topic/24618-minecrunch-web-js-miner-with-integration-feature/>

7. CPU miner for Litecoin and Bitcoin - <https://github.com/pooler/epuminer>

open source GPU-based mining tools. These tools greatly increased mining efficiency due to the hashing power of a GPU and the massive parallelizing possible with multiple GPUs (also known as mining rigs). The move from software to hardware followed shortly after. First, programmable FPGA chips resulting in custom-built circuits specifically for mining⁸. Then by mid-2012, companies started selling ASICs designed specifically for Bitcoin mining. After delay of about a year in delivering ASIC products, Bitcoin mining started transitioning from GPUs to ASICs where it remains today. Consequently, the hashing power of the Bitcoin network increased and the mining difficulty followed. To illustrate the change, consider a desktop PC CPU mining at 10 MH/s: on expectation, it will take 425 years before mining a single block [12].

In parallel to the evolving technology, collective action emerged through the use of mining pools. A mining pool is a collective of individual miners. Participants receive a slice of work for mining the current block on behalf of the pool. If a member of the pool mines the block, the block reward is split amongst the participants of the pool *pro rata* according to their computational effort [26]. As an aside, a very elegant protocol for reporting 'near-solutions' to the pool enables participants to prove, without trust, the level of effort they are contributing to the pool at all times. In general, a mining pools cannot amplify earnings, they only change their shape. An income stream from a pool is a steady trickle, while solo-mining results in sporadic dumps of income. The first Bitcoin block found on a mining pool was on December 16, 2010 that was a beta implementation of a pool operated by a user named *slush*.

2.2. Monero

Launched in April 2014, Monero [18] is a cryptocurrency alternative to Bitcoin. It purportedly offers increased privacy by obfuscating the participants in a transaction, as well as the amounts. This is in contrast to more popular cryptocurrencies like Bitcoin and Ethereum, where a pseudonymous-but-complete transaction graph can be constructed from the public blockchain. Recent research has shown Monero's obfuscation techniques are less effective than originally claimed [17], [14]. Since regulation on exchanging between cryptocurrencies is lighter than exchanging cryptocurrencies for fiat money, and such services are not geographically bound, obtaining Monero for Bitcoin and vice versa is efficient and enables Monero to be used as a short-term medium of exchange for Bitcoin holders. This approach (and Monero's acceptance) is particularly popular on so-called dark web markets; markets that do not ban illicit goods and services.

A second characteristic that distinguishes Monero from Bitcoin is in the mining algorithm it uses. Monero still employs proof-of-work, specifically an algorithm called Cryptonight [6]. However the computational puzzle is designed

8. Custom FPGA Board for Sale! (August 18, 2011) <https://bitcointalk.org/index.php?topic=37904.0>

2014-04-18	Monero Cryptocurrency released.
2017-09-14	Coinhive Miner launched.
2017-09-17	ThePirateBay caught using coinhive [33].
2017-09-21	Adblockers started to block coinhive scripts.
2017-09-24	Showtime caught running coinhive [40].
2017-09-25	Coinhive clones started to appear.
2017-10-13	PolitiFact website compromised [43].
2017-10-16	Coinhive launched authedmine - authorized mining.
2017-11-23	LiveHelpNow Hack incident [15].
2018-01-25	Cryptojacking code found on Youtube ads [16].
2018-02-11	UK Information Commissioner's Office incident [38].

TABLE 1. TIMELINE OF MONERO AND IN-BROWSER MINING REPORTS

to be *memory-hard*: it requires the storage of a large set of bytes and then requires frequent reads and writes from this memory. Such puzzles are optimized for CPUs with low-latency memory-on-chip, and not as well suited for circuits like FPGAs and ASICs. CryptoNight requires approximately 2MB per instance, which fits in the L3 cache of modern processors. Over the course of the next few years, these L3 cache sizes should become mainstream and allow more CPUs, and thus users, to participate in Monero's 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, which are used in modern GPUs and considered one of the fastest types of memory, is notably slower than L3 cache [41].

2.3. Coinhive

Monero built on its early success and continued to gain in popularity over the years, which caught the attention of some developers who decided to revisit the idea of browser mining. See Table 1 for a timeline of events. One of the earliest efforts appeared in September 2017 and was called Coinhive [5]. Soon after, a competitor named Crypto-Loot⁹ emerged. Both websites provided APIs¹⁰ to developers for

9. Crypto-Loot - A web Browser Miner — Traffic Miner — CoinHive Alternative <https://crypto-loot.com/>

10. Application Programming Interface

implementing browser mining on their websites that used their visitors' CPU resources to mine Monero. A portion of mined Monero would go back to the API developer, and the rest would be kept by the website. Not long after their early success, several copycats appeared such as Coin-Have and PPoi [7] to take part in the reborn practice. It even inspired a new coin specifically designed for browser mining named JSECoin,¹¹ which has yet to find an audience. These developments took place over the course of a few weeks, which signalled the renewed success of browser mining. However, Coinhive's approach as a legitimate group 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 short-links, which could be used to prevent spam while mining Monero [5].

3. Threat Model

In-browser mining is considered as an abuse unless user's consent is granted. The attack surface to abuse users' browsers through cryptojacking is broad, and there are multiple vectors where various entities can inject mining scripts in the website's codebase. We summarize those here.

3.1. Webmaster initiated

A website administrator can add a mining script to her webpage, with or without informing users. Website owners may do this to monetize their sites, especially when they have been blacklisted or blocked by standard advertising platforms. In one example, a researcher found Coinhive on a large Russian website offering child pornography to users [27]. Revenue estimates, based on the website traffic data available, were roughly \$10,000 a month after converting the value of XMR mined to USD.

3.2. Third-party services

Many websites serve active Javascript from third parties within their own webpages. This could be ads from an ad network, accessibility tools or tracking and analytics services. Third parties with these privileges can inject cryptojacking scripts into the sites that use them, either intentionally or as a result of a breach. The first two incidents, Coinhive was injected into the websites of Movistar¹² and Globovision¹³ using Google Tag Manager¹⁴. Movistar stated that Coinhive was not put on their website by a hacker, but instead was due to "*internal error*" while they were conducting "production tests". No statement was provided

11. JSEcoin's Website Cryptocurrency Mining <https://jsecoin.com/>

12. Movistar is a major telecommunications brand owned by Telefonica, operating in Spain and in many Hispanic American countries <https://www.movistar.com/>

13. Globovision is a 24-hour television news network in Venezuela and Latin America <http://globovision.com/>

14. Google Tag Manager is a tag management system created by Google to manage JavaScript and HTML tags used for tracking and analytics on websites

by Globovision on why the cryptojacking scripts appeared on their site on November 15, 2017 [36]. Another high-profile cryptojacking case involving a Google platform occurred in January 2018 when Trend Micro researchers found advertisements containing Coinhive miner script were shown to YouTube users in Japan, France, Taiwan, Italy, and Spain for nearly a week [16]. Similar to Showtime, YouTube inherently has a high average visit duration as a video streaming site and thus is prime target for cryptojacking operations.

3.3. Browser extensions

Cryptojacking was not limited to websites in 2017. The Chrome extension *Archive Poster* remained on the Chrome Web Store for days while silently cryptojacking an unknown portion of their 100,000+ users. After multiple user reports, followed by multiple news media outlets covering the issue, the extension was removed [11]. Similar cryptojacking extensions has been identified on less popular Mozilla Firefox add-ons as well.

3.4. Breaches

If an attacker is able to breach principle servers, websites, extensions, or the scripting services they use, they can inject cryptojacking scripts that will impact the site's users without the site's knowledge or consent. For example, a researcher found a malicious modification to webchat system LiveHelpNow's SDK; it resulted in unsolicited mining across nearly 1500 websites using their chat support service [15] such as retail store chains Crucial and Everlast websites. In another example, Coinhive was found on the political fact-checking website PolitiFact¹⁵. A compromised JavaScript library was found to be injecting the cryptojacking code. The malicious code remained on the site for at least four hours before it was removed [43]. PolitiFact executive director stated, "Hackers were able to install their script on the fact-checking website after discovering a mis-configured cloud-computing server" [42].

Another recent example of such incident is a breach in a website plugin called *Browsealoud*¹⁶ led to injection of cryptojacking scripts in some United Kingdom governmental websites such as *Information Commissioner's Office*, *UK NHS services*, *Manchester City Council* and around 4200 other websites [38]. Within the same month, cryptojacking script was seen on *Tesla* and *LA Times* websites through poorly secured cloud configuration [22].

3.5. Man-in-the-middle

A user's web traffic is often routed through intermediaries that may have plaintext access to content. For example, internet service providers or free public wireless routers

15. PolitiFact: Fact-checking US politics <https://politifact.com/>

16. An accessibility tool to read the content aloud in multiple languages <https://www.texthelp.com/en-gb/products/browsealoud/>

can inject cryptojacking scripts into non-HTTPS traffic. Advertisement code injection has been seen in practice before [39] and there have been assertions of similar injections of browser mining scripts at certain Starbucks free Wi-Fi hotspots in Argentina¹⁷.

4. Measurements

4.1. Prevalence of Coinhive and alternatives



Figure 2. The number of instances of the Coinhive miner scripts found using the query in Figure 3 in top one million websites over a three month period beginning with the release of Coinhive in September 2017.

Based on the fact that Coinhive is the dominant website offering in-browser mining (see Figure 4), we first focus on measuring the prevalence of Coinhive scripts deployed on internet sites. We use the censys.io BigQuery dataset [8] for the top million sites indexed by Zmap¹⁸. We simply look for the `coinhive.min.js` script within the body of the website page. The query we use is in Figure 3 and the results over a two month period are provided in Figure 2. These findings are corroborated by another search engine, PublicWWW¹⁹, which indexes the source code of publicly available websites. Using PublicWWW's dataset, over 30,000 websites were found to have the `coinhive.min.js` library [20]. As seen from our data in Figure 2, the adoption of this script was substantial in the first days of its release. However, progress slowed down at the same time as ad-blockers and organizations started to block Coinhive's website. The initial purpose of this service, as claimed by Coinhive, was to replace ads and cover server costs for webmasters. As the service did not require that websites receive user consent before running the miner code, it started to be used maliciously in users' browsers. This type of usage resulted in Coinhive being included in some company's top-10 most wanted malware list [4].

This type of measurement will become less accurate moving forward. Cryptojacking services are evolving to use obfuscated JavaScript and randomized URLs to evade detection²⁰. An example of these methods can be found in

17. <https://twitter.com/imnoah/status/936948776119537665>

18. <https://zmap.io>

19. Search Engine for Source Code <https://publicwww.com/>

20. https://twitter.com/bad_packets/status/940333744035999744

```

1 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 wwbody, p80.http.get.body as plainbody
2 FROM censys-io.domain_public.20171123
3 WHERE STRPOS(p80.http.get.body, coinhive.min.js) > 0 or STRPOS(p80.http_www.get.body, coinhive.min.js) >0

```

Figure 3. A BigQuery SQL query to find websites that embed the Coinhive script using a dataset of the top one million sites from censys.io.

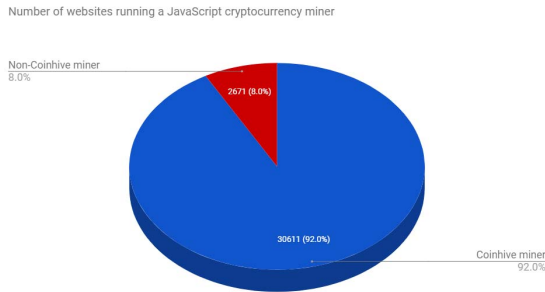


Figure 4. Share of websites using a Javascript cryptocurrency miner, details in Table 2

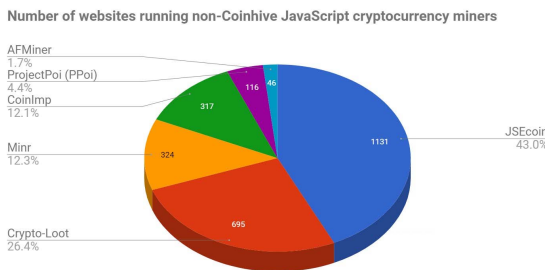


Figure 5. Share of websites using a Coinhive alternative, details in Table 2

the cryptojacking service provider called Minr. In this case, the script is automatically obfuscated for users implementing the code. In addition, the domain names used by Minr frequently change to circumvent blocklists and anti-malware software.

Coinhive has begun to be blocked by enterprises. One example is shown in Figure 7. This blocking seems to have sent Coinhive operators to lesser known alternatives with the same or similar functionality. We used the same methodology on PublicWWW dataset to find the usage of Coinhive and its alternatives on the internet. Table 2 shows the keywords used to identify these services. The result can be found on Figure 4 and Figure 5.

Coinhive has also reacted by focusing on adding methods to enforce asking for user consent and legitimizing the use of cryptojacking. It introduced another domain and service called *Authedmine*, which requires user’s consent to start mining in the browser. This service did not get the same attention as the original service, but it did inspire discussions regarding the ethics of such services, which is discussed in Section 6. Using the same methodology, censys.io was

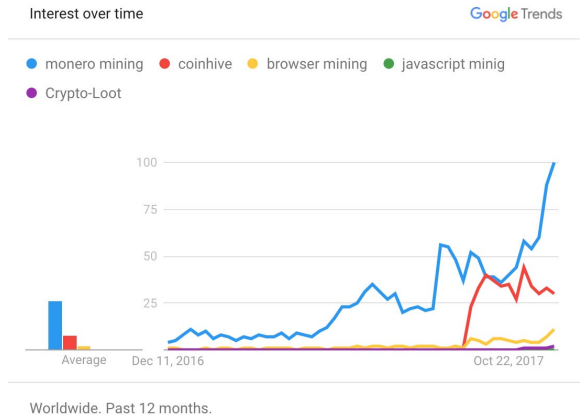


Figure 6. Google Trend over last 12 months: there has been more interest in Coinhive than the broader, related search term “Browser mining”. Comparing to other services offering Monero browser mining API, Coinhive had the advantage of being the first to offer the service.

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
 Server IP: 7
 User name:
 Group name:

Figure 7. Concordia university has categorized the coinhive.com website as malicious and has blocked it.

used to measure the prevalence of AuthedMine and show the results in Figure 8.



Figure 8. Usage of AuthedMine Miner scripts in top one million websites since its introduction

Website	Results	Query Parameter
Coinhive	30611	'coinhive.min.js'
JSEcoin	1131	'load.jsecoin.com'
Crypto-Loot	695	'CryptoLoot.Anonymous'
Minr	324	'minr.pw', 'st.kjli.fi', 'abc.pema.cl', 'metrika.ron.si', 'cdn.rove.cl', 'host.d-ns.ga', 'static.hk.rs', 'hallaert.online', 'cnt.statistic.date', 'cdn.static-cnt.bid'
CoinImp	317	'www.coinimp.com/scripts/min.js', 'www.hashing.win'
ProjectPoi (PPoi)	116	'projectpoi.min'
AFMiner	46	'afminer.com/code/miner.php'
Papoto	42	'papoto.com/lib/papoto.js'

TABLE 2. CRYPTOJACKING DATA WAS GATHERED BY TOTALLING THE NUMBER OF WEBSITES WHICH HAD THE FOLLOWING LIBRARIES IN THEIR SOURCE CODES, INDEXED BY PUBLICWWW BY 12/24/2017. FIGURE 4 AND FIGURE 5 ARE VISUALIZATIONS OF THESE RESULT.

4.2. Client impact

Most cryptojacking scripts discovered were configured to use around 25% of user's CPU, which can be justified as it will be under the threshold of attracting the user's attention, and it could be argued as fair-usage of their hardware. During the first few days, however, there were some reports of 100% CPU usage while visiting websites containing these scripts [34], which can be characterized as malicious. By default, the Coinhive JavaScript library will use all available CPU resources. The user implementing the script must include a throttle value to reduce the client-side CPU usage during mining operations. We show an example in Figure 9.

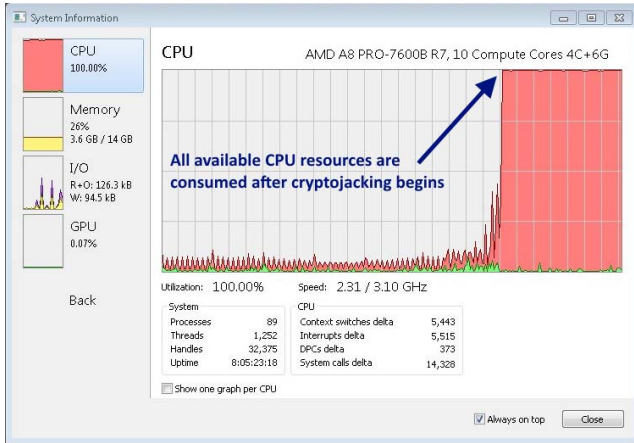


Figure 9. Comparison of CPU usage of browser without and with browser mining enabled.

4.3. Profitability

Coinhive developers estimate a monthly revenue of about 0.3 XMR (about \$101 USD) for a website with 10-20 active miners [5]. We sought to validate this estimation with

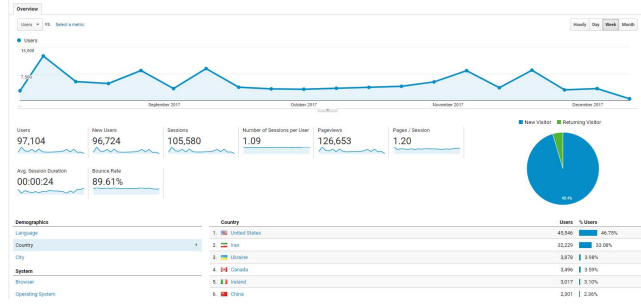


Figure 10. Google Analytics dashboard showing the number of visitors to a domain parking service of 11 000 domains.

a real world data set provided to us²¹. One of the biggest Coinhive campaign operators is a domain parking service. It runs Coinhive on over 11 000 parked websites. While visits to parked domains are considerably shorter than an average website, the data spans a period of three months and gives some insight into the profitability of cryptojacking. During the experimental period of about 3 months, they accumulated 105 580 user sessions for an average of 24 seconds per session. For the period examined, the revenue was 0.02417 XMR (Monero's currency) which at the time of writing is valued at \$7.69 USD. Further detail is provide in Figures 10 and 11. While an A/B test was not setup to determine how much traditional web advertising would have brought in, freely available web calculator tools suggest we might expect an order or two of magnitude greater for comparable traffic.

5. Mitigations

We discuss the ethics of cryptojacking in the next section, but in the case of cryptojacking without user consent, it seems natural to us to presuppose users want to be protected. Protection might take a few forms, which we outline here.

5.1. Obtaining consent

Cryptojacking tools might attempt to legitimize the practice by first obtaining user consent on a service provider level. An example of this is the Authedmine service from Coinhive discussed previously. Malicious sites might also opt for a service like Authedmine if it is whitelisted on its users' networks and then attempt to circumvent the consent process. For example, consent that requires a click from the user has been shown in some circumstances to be vulnerable to clickjacking attacks [28].

While cryptojacking is nowhere near the prevalence of tracking cookies, eventually it might grow into a regulatory issue where governmental bodies could use legislative approaches to obtain consent, similar to the provisions many

21. In collaboration and with thanks to Faraz Fallahi <https://github.com/ffaraz>

HASHES/S: 0
 TOTAL HASHES: 171.17 M
 TOTAL PAID: 0 XMR
 PENDING PAYMENTS: 0.02417 XMR
current payout 0.0009178 XMR per 1M hashes
 (difficulty: 44.937G, block reward: 5.89 XMR, payout: 70%, updated: Dec 11, 2017 - 21:03:09 - FAQ)

Sites

Name	Hashes/s	Total Hashes	Total XMR	Miner
Your Site	0	171 165 184	0.02417040 <small>xmr</small>	open

Hashes/s (One Hour Average)



Figure 11. Coinhive dashboard showing the earnings of a domain parking service that runs Coinhive on 11 000 domains. Over the course of about 3 months, the operator earned 0.02417 XMR (currently \$7.69 USD).

countries now use for cookies (including honouring the ‘do not track’ HTTP header and obtaining click-based consent).

5.2. Browser-level mitigation

Browser developers have begun discussion of intervening in cryptojacking²². Potential mitigations include: throttling clientside scripting, warning users when clientside scripting consumes excessive resources, and blocking the sources of known cryptojacking scripts. Determining appropriate for thresholds for client-side processing that are high enough to allow legitimate applications and low enough to deter cryptojacking is an open research problem, as would be the wording of any notifications to the user that would lead the user to make an informed decision about allowing or not allowing resource consumption (cf. SSL/TLS warnings [31], [30], [1]). Browsers such as Opera, have taken a stance against cryptojacking scripts and blocked them via their “NoCoin” blacklist [25]. It is too early to determine the effectiveness of using a blacklist to block such activities.

It is worth noting that some browsers might actually take the exact opposite approach and promote (consensual) in-browser mining, as it enables a form of monetizing websites independent of both (1) ad networks and the user tracking that accompanies the current ad model, and (2) users maintaining some form of credits or currencies for making micropayment to websites they use (e.g., Brave Browser²³). Browser mining has been shown to not be as efficient as

22. ‘Please consider intervention for high cpu usage js’ <https://bugs.chromium.org/p/chromium/issues/detail?id=766068>

23. <https://brave.com>

native mining applications today. Therefore, optimizations on how browsers pass system calls to the operating system can be made, or there can even be browsers designed specifically to support efficient browser mining.

6. Discussion

While cryptojacking might be relatively new, it fits the pattern of various other technologies deployed on the web that raise ethical questions. In thinking about it, we distinguish a few cases: (1) the use of cryptojacking on a breached website, (2) the use of cryptojacking by the website owner with an attempt at obtaining user consent, and (3) the use of cryptojacking by the website owner without obtaining user consent. We would argue that (1) is clearly unethical; invariant to one’s views on the ethics of hacking, we cannot see a justification for a breach that profits the adversary without any external benefits to anyone else.

The second case, cryptojacking after gaining user consent, is controversial primarily because it is unclear if users understand what they are consenting to, what they receive in return (some examples might include the elimination of ads, premium features, paywalled content, or higher definition video streams), and whether it is a fair exchange. To understand the zeitgeist, consider a recent poll conducted by Bleeping Computer that found: “many users said they are OK with websites mining Monero in the background if they don’t see ads anymore” [3]. Coinhive released AuthedMine in recognition of the importance to many of user consent. ThePirateBay.org [2] ran cryptojacking scripts while users searched for torrent files without notice in their Privacy Policy, nor any 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 following statement, “Do you want ads or do you want to give away a few of your CPU cycles every time you visit the site?” [34]. While the admins admitted to their testing of browser mining, their notice came after it was discovered and they ultimately removed the code. In both auction-based and keyword-based online advertisement, the advertiser pays the advertisement publisher to distribute the advertisement and the advertisement publisher pays a portion of the revenues to the website owner whom the advertisement was shown on her website [13]. However with in-browser mining as a replacement monetization strategy, a more direct compensation is established with less intermediaries which could benefit users and sites alike.

The potential harm to users of cryptojacking is higher energy bills, along with accelerated device degradation, slower system performance, and a poor web experience [29], [33]. While consent may be obtained from the user, it is unclear if the user’s mental model of how they are paying can be made clear to them. On the other hand, the privacy disclosures users make in the traditional advertising model are also intangible; it is doubtful users understand what they are consenting to when they, for example, consent through a banner [9] to the use of tracking cookies; and many websites waste computational resources without consequence through

buggy scripting and unnecessary libraries. In short, the ethics are not clear-cut and should be debated.

One webservice prone to cryptojacking is video streaming—the longer a user is engaged on a website, the more income can be earned through browser mining. Showtime.com [35] and UFC.com [37] are two popular streaming sites that were asserted by researchers to have deployed Coinhive. Showtime has declined to comment on how or why Coinhive was implemented on their website. Speculation has been raised that it was injected via a third-party analytic tool, New Relic, due to Coinhive being found inside the New Relic code block within showtime’s website source code. However a New Relic representative denied these claims in a statement to The Register, “It appears [Coinhive scripts] were added to the website by [Showtime’s] developers.” [35]. In a statement released by the UFC, they denied the presence of the code stating, “[they] did not find any reference to the mentioned Coinhive JavaScript [code]”²⁴.

The third case is the use of cryptojacking without user consent. Moor, in “What is Computer Ethics?” [19] introduces the concept of an *invisible factor* for invisible computer operations in society. Based on his definitions, we would classify cryptojacking that does not gain user consent as *invisible abuse*: the intentional use of the invisible operations of a computer to engage in unethical conduct. Here the cryptojacker is earning money from unaware users that are being charged on their electricity bill. As discussed before, we already have court cases against such activities [24] and regulations for activities such as online user tracking [9], which indicates the need to start discussions and regulation on in-browser mining to fill in this policy vacuum as well.

7. Acknowledgements

J. Clark thanks NSERC and FRQNT for partial funding of this research.

References

- [1] M. E. Acer, E. Stark, A. P. Felt, S. Fahl, R. Bhargava, B. Dev, M. Braithwaite, R. Sleevi, and P. Tabriz. Where the wild warnings are: Root causes of chrome https certificate errors. In *CCS, CCS '17*, pages 1407–1420, New York, NY, USA, 2017. ACM.
- [2] BBC. Websites hacked to mint crypto-cash. <http://www.bbc.com/news/technology-41518351>, 2017.
- [3] BleepingComputer. The internet is rife 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.
- [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] Cryptonote. Cryptonote technology. <https://cryptonote.org/inside.php#equal-proof-of-work>, 2017. Accessed: 2017-11-20.
- [7] DeepDotWeb. Coinhive hacked and launches new opt-in service. <https://www.deepdotweb.com/2017/11/11/coinhive-hacked-launches-new-opt-service/>, 2017.
- [8] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. A search engine backed by Internet-wide scanning. In *ACM CCS*, Oct. 2015.
- [9] European-Commission. Cookies. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm, 2011. Accessed: 2017-12-08.
- [10] 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.
- [11] Fortune. Popular google chrome extension caught mining cryptocurrency on thousands of computers. <http://fortune.com/2018/01/02/google-chrome-extension-cryptocurrency-mining-monero/>, 2017. Accessed: 2018-01-20.
- [12] D. Y. Huang, H. Dharmdasani, S. Meiklejohn, V. Dave, C. Grier, D. McCoy, S. Savage, N. Weaver, A. C. Snoeren, and K. Levchenko. Bitcoin: Monetizing stolen cycles. In *NDSS*, 2014.
- [13] M. King, J. Atkins, and M. Schwarz. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *The American economic review*, 97(1):242–259, 2007.
- [14] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of moneros blockchain. In *European Symposium on Research in Computer Security*, pages 153–173. Springer, 2017.
- [15] LiveHelpNow. Security incident nov 23rd, 2017. <https://blog.livehelpnow.net/security-incident-nov-23rd-2017/>, 2017. Accessed: 2017-12-14.
- [16] T. Micro. Malvertising campaign abuses googles doubleclick to deliver cryptocurrency miners. <https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/>, 2018. Accessed: 2018-01-31.
- [17] A. Miller, M. Moeser, K. Lee, and A. Narayanan. An Empirical Analysis of Linkability in the Monero Blockchain. Technical report, arXiv, 2017.
- [18] Monero. MONERO private digital currency. <https://getmonero.org/>, 2014. Accessed: 2017-11-20.
- [19] J. H. Moor. What is computer ethics? *Metaphilosophy*, 16(4):266–275, 1985.
- [20] T. Mursch. Cryptojacking malware coinhive found on 30,000+ websites. <https://badpackets.net/cryptojacking-malware-coinhive-found-on-30000-websites/>, 2017. Accessed: 2018-01-20.
- [21] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.
- [22] NakedSecurity. Unsecured aws led to cryptojacking attack on la times. <https://nakedsecurity.sophos.com/2018/02/27/unsecured-aws-led-to-cryptojacking-attack-on-la-times/>, 2018. Accessed: 2018-02-28.
- [23] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.
- [24] N. J. D. of Consumer Affairs. New jersey division of consumer affairs obtains settlement with developer of bitcoin-mining software found to have accessed new jersey computers without users knowledge or consent. <http://nj.gov/oag/newsreleases15/pr20150526b.html>, 2015. Accessed: 2018-01-20.
- [25] Opera. New year, new browser. opera 50 introduces anti-bitcoin mining tool. <http://blogs.opera.com/desktop/2018/01/opera-50-introduces-anti-bitcoin-mining-tool/>, 2018. Accessed: 2018-01-20.
- [26] M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*, 2011.
- [27] S. Ruwhof. Massive child porn site is hiding in plain sight, and the owners behind it. <https://sijmen.ruwhof.net/weblog/1782-massive-child-porn-site-is-hiding-in-plain-sight-and-the-owners-behind-it>, 2017. Accessed: 2018-01-20.
- [28] G. Rydstedt, E. Bursztein, D. Boneh, and C. Jackson. Busting frame busting: a study of clickjacking vulnerabilities at popular sites. In *IEEE SSP*, volume 2, 2010.
- [29] D. Sillars. The performance impact of cryptocurrency mining on the web. <https://discuss.httarchive.org/t/the-performance-impact-of-cryptocurrency-mining-on-the-web/1126>, 2017. Accessed: 2017-12-20.
- [30] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in

24. https://twitter.com/bad_packets/status/928044219222048769

usable security lab studies: Lessons learned from replicating a study on SSL warnings. In *SOUPS*, 2011.

- [31] J. Sunshine, S. Egelman, H. Almuhiemedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *USENIX Security*, 2009.
- [32] R. Tahir, M. Huzaifa, A. Das, M. Ahmad, C. Gunter, F. Zaffar, M. Caesar, and N. Borisov. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. In *RAID*, 2017.
- [33] 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.
- [34] ThePirateBay. The galaxy's most resilient bittorrent site. <https://thepiratebay.org/blog/242>, 2017. Accessed: 2017-11-20.
- [35] TheRegister. Cbs's showtime caught mining crypto-coins in viewers' web browsers. https://www.theregister.co.uk/2017/09/25/showtime_hit_with_coinmining_script/, 2017. Accessed: 2018-01-20.
- [36] TheRegister. Crypto-jackers enlist google tag manager to smuggle alt-coin miners. https://www.theregister.co.uk/2017/11/22/cryptojackers_google_tag_manager_coin_hive/, 2017. Accessed: 2018-01-20.
- [37] 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.
- [38] TheRegister. Uk ico, uscourts.gov... thousands of websites hijacked by hidden crypto-mining code after popular plugin pwned. https://www.theregister.co.uk/2018/02/11/browsealoud_compromised_coinhive/, 2018. Accessed: 2018-02-28.
- [39] 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.
- [40] 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.
- [41] N. van Saberhagen. Cryptonote v 2. 0. <https://bytecoin.org/old/whitepaper.pdf>, 2013.
- [42] WallStreetJournal. Your computer may be making bitcoin for hackers. <https://www.wsj.com/articles/hackers-latest-move-using-your-computer-to-mine-bitcoin-1509102002>, 2017. Accessed: 2018-01-20.
- [43] Washingtonpost. Hackers have turned politifact's website into a trap for your pc. <https://www.washingtonpost.com/news/the-switch/wp/2017/10/13/hackers-have-turned-politifacts-website-into-a-trap-for-your-pc>, 2017. Accessed: 2018-01-20.
- [44] V. Wikipedia. Important milestones of the bitcoin project. <https://en.bitcoin.it/wiki/Category:History>, 2009. Accessed: 2018-01-18.
- [45] J. Wyke. The zeroaccess botnet: Mining and fraud for massive financial gain. *Sophos Technical Paper*, 2012.