Pulkit Jain
Professor Ming Chow
Comp116: Introduction to Computer Security
Spring 2018

In-Browser Cryptojacking: An Old Threat in a New Guise

Project: https://github.com/pjain03/spike_detector

Abstract

Cryptocurrencies have become an extremely valuable resource in recent times which has attracted many to try to obtain them in vast quantities. Not surprisingly, this increase in popularity has invited a measure of crime into the fold. The goal of this paper is to describe the state of cryptomining and cryptojacking, how it affects the general public, and discuss a few ways to detect and suppress it when it occurs in one's web browser. Finally, this paper will touch on the legitimacy of in-browser cryptomining as a possible alternative to ads as a source of income for websites.
Keywords: cryptocurrency, bitcoin, cryptojacking, Coinhive, monero, crypto

Introduction

The high rewards that the field of cryptocurrencies currently offers has enticed many to devote a lot of finances, time, and energy into building a cryptocurrency portfolio that is as large and diversified as possible. Some choose to purchase and sell crypto as they would stock or shares, but others instead choose to undertake the task of "cryptomining"[1]. The specifics of how cryptomining works is beyond the scope of this paper but to provide a very brief background, it involves people performing complex computational tasks in return for cryptocurrency. The more one mines, the more crypto one acquires, and the more wealth one amounts. Increased computation power allows a cryptominer to mine more and this has resulted in a race to gather as much hardware (GPU's, ASIC's etc.) as one can to mine as much as possible[2]. It has also unsurprisingly attracted cryptominers to participate in the malicious act of "cryptojacking". As the term implies, cryptojacking refers to the unauthorized use of someone's computer in order to outsource the calculations need to cryptomine.

[1] "Bitcoin Mining", Investopedia. https://www.investopedia.com/terms/b/bitcoin-mining.asp (3/1/2018)
[2] Waters, Alex, "Here comes the Pickaxe Race: Bitcoin Mining Jumps to GPUs" (04/12/2017), Coindesk. https://www.coindesk.com/bitcoin-milestones-alex-waters-mining-cpu-gpu/ (04/05/2018)

To the Community

Cryptojacking manifested itself as a legitimate threat to large-scale businesses earlier this year when attackers wrested control of resources from Tesla[3] and Jenkins[4] to mine cryptocurrency. In terms of sheer cost, cryptomining on business resources (such as AWS servers as in the cases of the previously mentioned companies) can slow servers to a complete halt, cause an immense increase in power consumption (a bitcoin transaction uses as much energy as a house does in a week[5]), and, upon detection, adversely affect a company's trust-relationship with its users[6]. Due to the novelty of this attack, it is still not something businesses are necessarily aware of or taking seriously. The fact that the frequency of these attacks is growing unboundedly makes it a severe security threat[7].

Not only does cryptojacking pose a risk to businesses, but it also affects many unaware end-users. In fact, Symantec, a cybersecurity company, reported that cryptojacking had increased by 8500% over the last quarter of 2017[8], likely due to the increased ease with which it could be done remotely though people's browsers. Coinhive – a JavaScript library packaging all the tools required to perform cryptojacking, has been a key cause of this. It provides the tools necessary for malicious individuals to mine cryptocurrency on someone's device without their permission. Although such a utility – albeit in a reduced and less-powerful format - existed prior to Coinhive in libraries such as Bitcoin Plus[9], in-browser cryptomining using Coinhive has resurfaced in a remarkable manner due to its ease of use, and the availability of cryptocurrencies that can be mined easily in-browser (Monero). The unauthorized cryptomining that both cryptojackers and websites perform increases the end-user's power consumption, causes their processors to overheat and slow-down, and affects the longevity of their devices[10]. As such, to be able to detect and stop cryptojacking would be immensely useful to everyone. This paper will focus on the detection of in-browser cryptojacking to spread awareness amongst the average user.

---

[3] Redlock CSI Team, "Lessons from the Cryptojacking Attack on Tesla" (02/20/2018), Redlock. https://blog.redlock.io/cryptojacking-tesla (03/02/2018)

[4] Check Point Research Team. "Jenkins Miner: One of the Biggest Mining Operations Ever Discovered" (02/15/2018), Check Point Research. https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/ (05/06/2018)

[5] Malmo, Christopher. "One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week" (01/11/2017), Motherboard. https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change (05/06/2018)

[6] Ashford, Warwick. "Businesses Need to take Cryptojacking Seriously" (March 2018), ComputerWeekly. https://www.computerweekly.com/feature/Businesses-need-to-take-cryptojacking-seriously (05/06/2018)

[7] Shaikh, Rafia. "Cryptojacking Has Become One of the Top 10 Biggest Threats – 55% of Businesses Affected" (01/16/2018), WCCFTech.https://wccftech.com/cryptojacking-top-10-biggest-threats/ (05/06/2018)

[8] Georgiev, Georgi. "Cryptojacking Up 8500% Last Year: Stay Protected!" (03/28/2018), Bitcoinist. http://bitcoinist.com/cryptojacking-8500-last-year-stay-protected/ (03/29/2018)

[9] Ibid

[10] Dascalescu, Ana. "What is Cryptojacking and How to Avoid this Attack" (02/22/2018), Heimdal Security.https://heimdalsecurity.com/blog/cryptojacking-monero-malware/#cryptojacking (03/29/2018)

In-Browser Mining

1. Bitcoin

A lot of people believe Bitcoin and the concept of cryptocurrencies to be synonymous and with good reason; it has been one of the most volatile and hence profitable cryptocurrencies in the market, and currently holds the largest well-known market cap for cryptocurrencies[11] which has brought it immense popularity. But there are a lot more cryptocurrencies out there than just Bitcoin.

Due to technical reasons beyond the scope of this paper, Bitcoin mining moved from being viable over CPUs to GPUs and now to ASICs (specifically designed to mine Bitcoin). As such, Bitcoin is not a cryptocurrency that can be mined in browser (profitably) anymore. Even if it could be mined from a browser profitably, Bitcoin has considerable privacy issues that provide adequate barriers to anyone looking to use it as a currency for illegal purposes, for example a major issue (which has had a few "messy workarounds") is that any end of a transaction risks exposure of the complete sum of money owned by either party[12].

2. Monero

In sharp contrast to Bitcoin, Monero was developed specifically to be able to be mined through multiple different computational resources at once. Compared to Bitcoin, it is relatively new, however it still has a considerable market cap, is monitored by law-enforcement to a much lesser degree, and has a much greater emphasis on privacy. These reasons have motivated criminals have moved their transactions over to Monero[13]. A popular example of this is that the operator(s) of the immensely infamous WannaCry worm moved their ransom payments from Bitcoin to Monero for added untraceability[14].

In addition to this, it is extremely easy to mine Monero through the popular tool Coinhive, which is available as a JavaScript library, and can be embedded into a website[15]. Initially created as an alternate source of revenue for businesses whereby websites could mine cryptocurrency on their users' CPU, it has become a dangerous cryptojacking tool because it doesn't make user permission, and CPU throttling compulsory. To Coinhive's credit, it maintains that it is firmly an alternate source of revenue (discussed further in this paper), but because the above restrictions are unenforced, there is no way to stop malicious people from abusing this tool. Moreover, it is available as a script that can be run easily, thus any website that is

---

[11] "Top 100 Cryptocurrencies by Market Capitalization", CoinMarketCap. https://coinmarketcap.com/ (03/01/2018)
[12] "The Merits of Monero: Why Monero vs Bitcoin", Monero.how. https://www.monero.how/why-monero-vs-bitcoin (03/06/2018)
[13] Leyden, John. "Crooks opt for Monero as crypto of choice to launder ill-gotten gains" (03/16/2018), The Register. https://www.theregister.co.uk/2018/03/16/cyber_crime_economics/ (03/06/2018)
[14] Gallagher, Sean. "Researchers say WannaCry operator moved bitcoins to "untraceable" Monero" (08/04/2017), ArsTechnica. https://arstechnica.com/gadgets/2017/08/researchers-say-wannacry-operator-moved-bitcoins-to-untraceable-monero/ (03/29/2018)
[15] Javascript Miner, Coinhive. https://Coinhive.com/documentation/miner (03/12/2018)

susceptible to XSS attacks (vulnerability 7 on OWASP's top 10[16]) could be made part of a larger pool of websites that mine for a malicious attacker.

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.User('SITE_KEY', 'john-doe');
    miner.start();
</script>
```

Figure 1: From the documentation of Coinhive's website - how easy it is to set up a miner as injectable script tags

3. Others

Due to the rapid rise values of most cryptocurrency, there are a lot of options for what can mine – a popular one being Ethereum (the cryptocurrency with the 2nd largest market cap). But the issue with the most popular cryptocurrencies is that most of the mining that could have been done has been done and any future profitable mining requires costly dedicated machinery. The one's that aren't as popular yet might not be worth mining. Monero however provides the perfect medium between the two.

As for alternative mining software – there are a few worth mentioning such as Coinhive Captcha and Coinhave. We will focus on Coinhive since it dominates the market by far. In a 2018 study, 1 in 7000 websites (voluntarily or involuntarily) were found to be mining cryptocurrency with Coinhive being the most popular tool (93.82%) that was used[17].

Defenses: Detection and Blocking

Traditional techniques to block undesirable content on the internet, such as those used by ad-blockers whereby a blacklist of cryptomining software/websites is maintained and verified against, are useful in blocking cryptomining. As such, they should be utilized by all users. In fact, AdBlock Plus, a popular ad blocker, was upgraded to include blocking such unauthorized mining[18]. NoCoin, another popular extension, maintained a more extensive blacklist of cryptomining scripts and CDNs, and has been hailed as a very popular option to negate unauthorized, in-browser cryptomining[19]. However, as these tools grew in complexity, so did the cryptojackers. Recently, these criminals have come up with proxy networks to deliver the

[16] "Top 10 2017", OWASP. https://www.owasp.org/index.php/Top_10-2017_Top_10 (03/29/2018)
[17] Terlato, Peter. "How many websites mine cryptocurrency?" (04/06/2018), Finder. https://www.finder.com/how-many-websites-mine-cryptocurrency (03/06/2018)
[18] Williams, Ben. "Kicking out Cryptojack" (09/21/2017), AdBlock Plus. https://adblockplus.org/blog/kicking-out-cryptojack (04/06/2018)
[19] Verma, Adarsh. "6 Easy Ways To Block Cryptocurrency Mining In Your Web Browser" (02/07/2018) , Fossbytes. https://fossbytes.com/block-cryptocurrency-mining-in-browser/ (05/06/2018)

same content (Coinhive miners etc.) which cannot be detected by ordinary techniques and saves them the fee they must pay to Coinhive[20].

MinerBlock is another browser extension that maintains blacklists much like its other discussed counterparts, but in addition to it, monitors the scripts used by websites for behavior similar to traditional cryptomining/Coinhive[21]. This serves to not only deter those proxy networks, but also inlined JavaScript in websites. However, if there is anything we have learnt as a community from the behavior of malicious cybercrime, it is that there will always be new ways for attackers to adapt to our defensive measures. Therefore, when cryptojackers find another way to mine cryptocurrencies in-browser, it will resurface. As such, the only foolproof way to defend an individual user's resources is as follows:

1. Keep updated versions of the aforementioned browser extensions.
2. Monitor CPU usage/computer performance and if the root of it lies in the browser, be wary of cryptojacking [**see project linked at top of document**].

Conclusion

Seeing as cryptojacking has been growing at a frightening rate, it is important that the security community, big corporations, and casual users be aware of the threat that it poses. Furthermore, it is important that users be aware of the resources at their disposal, and of the reasons and thought behind it all. As such, it is important to consider Coinhive's purported purpose: it aims to be an alternative source of income for websites. As long as websites can mine using Coinhive without unboundedly charging their users' CPUs (as PirateBay did very infamously[22]) it might help websites supplement their revenue, improve user experiences on the internet by reducing the number of ads, all without choking up their users' resources. However, by placing the onus of this in the hands of the implementers without necessitating user permission or consideration (in the form of throttled mining), Coinhive has created a tool that can be used to wreak massive amounts of havoc which must be defended against. If, however, we are able to stop the websites that choke up resources and allow websites that do not to continue to perform minor cryptomining, we might be able to safely reach an optimal user experience on the web

[20] Cimpanu, Catalin. "In-Browser Cryptojacking Is Getting Harder to Detect" (03/27/2018), Bleeping Computer. https://www.bleepingcomputer.com/news/security/in-browser-cryptojacking-is-getting-harder-to-detect/ (03/29/2018)

[21] MinerBlock Project on Github. https://github.com/xd4rker/MinerBlock (03/30/2018)

[22] Kumar, Mohit. "The Pirate Bay Caught Running Browser-Based Cryptocurrency Miner" (09/18/2017), The Hacker News. https://thehackernews.com/2017/09/pirate-bay-cryptocurrency-mining.html (05/06/2018)

References

1. "Bitcoin Mining", Investopedia. https://www.investopedia.com/terms/b/bitcoin-mining.asp (3/1/2018)
2. "The Merits of Monero: Why Monero vs Bitcoin", Monero.how. https://www.monero.how/why-monero-vs-bitcoin (03/06/2018)
3. "Top 10 2017", OWASP. https://www.owasp.org/index.php/Top_10-2017_Top_10 (03/29/2018)
4. "Top 100 Cryptocurrencies by Market Capitalization", CoinMarketCap. https://coinmarketcap.com/ (03/01/2018)
5. Ashford, Warwick. "Businesses Need to take Cryptojacking Seriously" (March 2018), ComputerWeekly. https://www.computerweekly.com/feature/Businesses-need-to-take-cryptojacking-seriously (05/06/2018)
6. Check Point Research Team. "Jenkins Miner: One of the Biggest Mining Operations Ever Discovered" (02/15/2018), Check Point Research. https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/ (05/06/2018)
7. Cimpanu, Catalin. "In-Browser Cryptojacking Is Getting Harder to Detect" (03/27/2018), Bleeping Computer. https://www.bleepingcomputer.com/news/security/in-browser-cryptojacking-is-getting-harder-to-detect/ (03/29/2018)
8. Dascalescu, Ana. "What is Cryptojacking and How to Avoid this Attack" (02/22/2018), Heimdal Security.https://heimdalsecurity.com/blog/cryptojacking-monero-malware/#cryptojacking (03/29/2018)
9. Gallagher, Sean. "Researchers say WannaCry operator moved bitcoins to "untraceable" Monero" (08/04/2017), ArsTechnica. https://arstechnica.com/gadgets/2017/08/researchers-say-wannacry-operator-moved-bitcoins-to-untraceable-monero/ (03/29/2018)
10. Georgiev, Georgi. "Cryptojacking Up 8500% Last Year: Stay Protected!" (03/28/2018), Bitcoinist. http://bitcoinist.com/cryptojacking-8500-last-year-stay-protected/ (03/29/2018)
11. Javascript Miner, Coinhive. https://Coinhive.com/documentation/miner (03/12/2018)
12. Kumar, Mohit. "The Pirate Bay Caught Running Browser-Based Cryptocurrency Miner" (09/18/2017), The Hacker News. https://thehackernews.com/2017/09/pirate-bay-cryptocurrency-mining.html (05/06/2018)
13. Leyden, John. "Crooks opt for Monero as crypto of choice to launder ill-gotten gains" (03/16/2018), The Register. https://www.theregister.co.uk/2018/03/16/cyber_crime_economics/ (03/06/2018)
14. Malmo, Christopher. "One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week" (01/11/2017), Motherboard. https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change (05/06/2018)
15. MinerBlock Project on Github. https://github.com/xd4rker/MinerBlock (03/30/2018)
16. Redlock CSI Team, "Lessons from the Cryptojacking Attack on Tesla" (02/20/2018), Redlock. https://blog.redlock.io/cryptojacking-tesla (03/02/2018)
17. Shaikh, Rafia. "Cryptojacking Has Become One of the Top 10 Biggest Threats – 55% of Businesses Affected" (01/16/2018), WCCFTech.https://wccftech.com/cryptojacking-top-10-biggest-threats/ (05/06/2018)
18. Terlato, Peter. "How many websites mine cryptocurrency?" (04/06/2018), Finder. https://www.finder.com/how-many-websites-mine-cryptocurrency (03/06/2018)
19. Verma, Adarsh. "6 Easy Ways To Block Cryptocurrency Mining In Your Web Browser" (02/07/2018) , Fossbytes. https://fossbytes.com/block-cryptocurrency-mining-in-browser/ (05/06/2018)
20. Waters, Alex, "Here comes the Pickaxe Race: Bitcoin Mining Jumps to GPUs" (04/12/2017), Coindesk. https://www.coindesk.com/bitcoin-milestones-alex-waters-mining-cpu-gpu/ (04/05/2018)
21. Williams, Ben. "Kicking out Cryptojack" (09/21/2017), AdBlock Plus. https://adblockplus.org/blog/kicking-out-cryptojack (04/06/2018)