Bent Heier Johansen

The effects of cryptojacking

Master's thesis in Informatics
Supervisor: Guttorm Sindre
May 2019

Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Bent Heier Johansen

The effects of cryptojacking

Master's thesis in Informatics
Supervisor: Guttorm Sindre
May 2019

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Acknowledgements

I want to thank my supervisors Guttorm Sindre and Per Håkon Meland for their help and support during the last year. They have both shown a keen interest in the subject matter and have contributed a lot to it. The thesis could not have been done without them.

I also want to give a special thank to Mr. Steve Gibson of the Gibson Research Corporation and his podcast Security now. The show have given me interesting insights into computer security for the last 7 years and the show notes have been a gold mine of information and references for this thesis.

Finally I want to thank Samfundet. I would not be the man I am today without you.

Abstract

Cryptojacking is the exploitation of internet users' bandwidth and processing power to mine cryptocurrencies. In late 2017 and through 2018 cryptojacking emerged as one of the largest online threats, rivaling all other malware. The enablers for this new threat was the rising popularity of Monero, a cryptocurrency that is viable to be mined on consumer grade hardware, the explosive value growth of most popular cryptocurrency and the start of Coinhive, a service that made web browser based cryptomining a viable alternative.

Cryptojacking has seen a decline in 2019 and while it might have been just a short time threat it took the keen interest of a large part of the computer security community. Several nefarious actors are likely to have made quite a profit from it. As of the writing of this thesis it is impossible to know whether cryptojacking will become a serious threat again or not, but the lessons that can be learned from it are interesting none the less.

This thesis seeks to understand how cryptojacking effects the systems and users suffering from it, as well as the viability of cryptojacking as a source of income for those perpetuating it and understanding the main differences between different kinds of cryptojacking attacks. This is done through an investigation of the available literature, controlled experiments and analysis of the profits created by cryptojacking over a prolonged amount of time and analysis of the cost data related to it.

The main findings is that cryptojacking does not significantly harm it's victims and it is relatively easy to protect against. On the other hand the costs and risk associated with performing cryptojacking are quite low. The main costs are the opportunity costs, as there are other ways to abuse compromised systems, and when the cryptocurrency markets are in decline cryptojacking are not as profitable as other ventures.

Table of Contents

List of Tables

List of Figures

Glossary

Cryptocurrency	=	A digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.
Cryptomining, mining	=	Using computational power to solve hashes in order to acquire cryptocurrency.
Cryptojacking	=	The act of mine cryptocurrency without the computers owners knowledge or consent.
ASIC	=	Application-Specific Integrated Circuit, customized for a particular use, rather than intended for general-purpose use.
Side loading	=	Installing an application outside of sanctioned app stores
Blockchain	=	A growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data
Bot	=	A software application that runs automated tasks over the Internet.
Botnet	=	A number of Internet-connected devices, each of which is running one or more bots.
Monero	=	A kind of cryptocurrency
XMR	=	Monero coin
Malware	=	Malicious software
webGL	=	A web based programming language using the GPU
APK	=	Android application package

Chapter 1

Introduction

This thesis seeks to investigate how malicious cryptomining effects users and their systems as well as cost data related to this. A better understanding of the business models within the dark economy can help in understanding the motivation and capabilities of malicious actors, and help predict the likelihood of attacks without having to rely solely on historical data. The main focus will be on browser-based mining and "fly-by" attacks as well as systems infected with a cryptominer, this exploitation of users computer resources without the owner's knowledge and consent is known as cryptojacking.

1.1 Motivation

Cryptocurrencies such as Bitcoin have been around for about a decade, but it has been unfeasible to mine it on consumer hardware for a very long time, and as such gaining illicit control over consumer hardware to mine it have not been lucrative, however with the introduction of alternative cryptocurrencies, nicknamed altcoins, particularly those like Monero[2] that are made specifically to combat the use of ASICs and custom made hardware it has again become feasible to mine using consumer hardware. While it has been possible to mine Bitcoin in the browser for years[3] it has not been profitable in a very long time. The emergence of coinhive.com[4] in 2017 changed this and it became apparent that it could be profitable to mine cryptocurrency in browsers using JavaScript running in browsers on consumer hardware.

Cryptojacking is the latest of a large family of cryptocurrency related crimes, including blatant theft, both digital [5][6][7] and physical [8][9], illegal trading [10], money laundering [11], extortion[12][13], ransomeware[14][15], pyramid schemes[16], scams [17] among others, except for one very important factor. While some kinds of cryptojacking, where one compromises computers and have them mine cryptocurrency[18] browser based cryptojacking has not been tested thoroughly in the courts and there are not necessary any reason to believe that JavaScript running in the browser mining coins will be found to be illegal.

Cryptojacking is a relatively new phoneme that skyrocketed in popularity in late 2017 and early 2018, this can be illustrated by using Google Scholar and custom range. There are no articles from 2015 about cryptojacking, this rises to 5 articles in 2016, 7 in 2017, 127 in 2018 and 44 as of mid May in 2019.

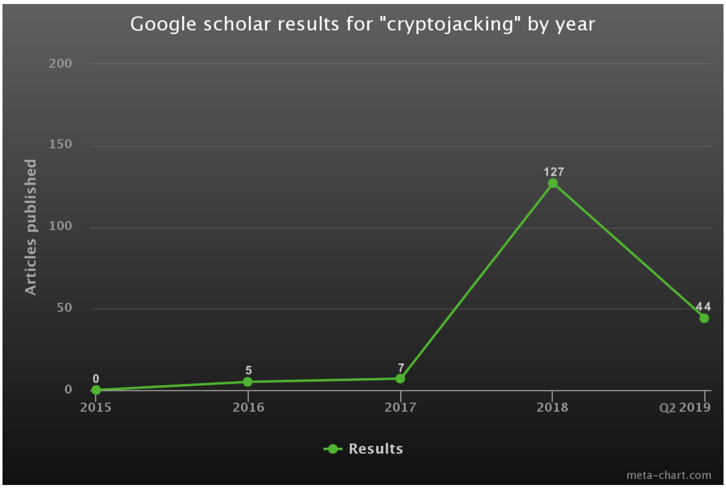


Figure 1.1: Results for "Cryptojacking" by Google Scholar custom search

According to an Europool report from 2018 *the industry is reporting an explosion in the volume of cryptominers (...), such that in the latter part of 2017, it overshadowed almost all other malware threats* and that cryptojacking is likely to increase in volume[19] and according to a Webroot article cryptojacking accounted for 35% of the cyber threats as of September 2018[20]. Cryptojacking is currently uncharted territory as far as the law is concerned and so far law enforcement is not doing much to stop it and according to the Europol report it is still only anecdotaly mentioned in criminal reports and no one have been arrested on the grounds of cryptojacking alone. However a more recent report from Symantec in 2019 finds that cryptojacking have dropped by 52% between January and December 2018 and the trend is further decline[21].

This thesis is written between the August 2018 and June 2019 and the Monero and Cryptojacking landscapes have changed a lot during this year, it is not possible to predict what will happen in the future, but this thesis should be give some insight into what have been learned over the last couple of years in regard to cryptocrime.

1.2 Goals and Research Questions

1. RQ1: What are the new characteristics of cryptomining attacks?
   (a) 1.1 How are cryptomining attacks carried out?
   (b) 1.2: How are the victims affected by cryptomining attacks?
   (c) 1.3: How can cryptomining attacks be prevented?
2. RQ2: How can cryptomining costs data be used to improve threat models?
   (a) 2.1: Which types of cost data are relevant to improve threat models?

1.3 Literature Review

A study of the current research was performed prior to the experiments. The goal of this study is connect the findings with the established research and work that have already been done and to look at which methods have already been used. The sources was mostly found by using *Google Scholar* and *Scopus* with the following search words

- Cryptomining
- Cryptojacking
- Crypto Crime
- Crypto Payment
- Drive-by Infection
- JavaScript Attack

The list of articles relevant to the searches were far to extensive to be fully examined, the list of papers were filtered based on the research questions and date of publication. The latter is due to the very fast changing nature of the cryptojacking, with it only gathering public traction in late 2017 most of the papers dated in the early 2010's were not very relevant.

Chapter 2

Background

According to previous research most browser based mining is done using Coinhive to mine Monero. This chapter will look at these technologies [22].

2.1 Legality

The legality of cryptojacking is still somewhat unclear, but most of the methods used to deliver cryptojacking software are no doubt illegal and could be prosecuted under laws such as U.S. Code § 1030 - Fraud and related activity in connection with computers[23] or the UK's Computer Misuse Act 1990[24]. Browser based cryptojacking is different, it is in essence just another kind of script running in the user's web browser. In the case where the scripts are put on the web site by the owners of the site and ran without the user's explicit consent it is not clear whether or not that is illegal, it is using the visitor's CPU to run a script that generate some tokens, in this case cryptocurrency, that can be exchanged for fiat currency, like US dollar or Euro. This is not all that different from running tracking cookies that gather information that then can be sold to the highest bidder. It is however quite different from advertising, with advertising the user is very much aware of the advertisement scripts being run in their browsers. The legality of browser based cryptomining without user consent is something that must be figured out by legal systems the world over if cryptojackers are to be prosecuted.

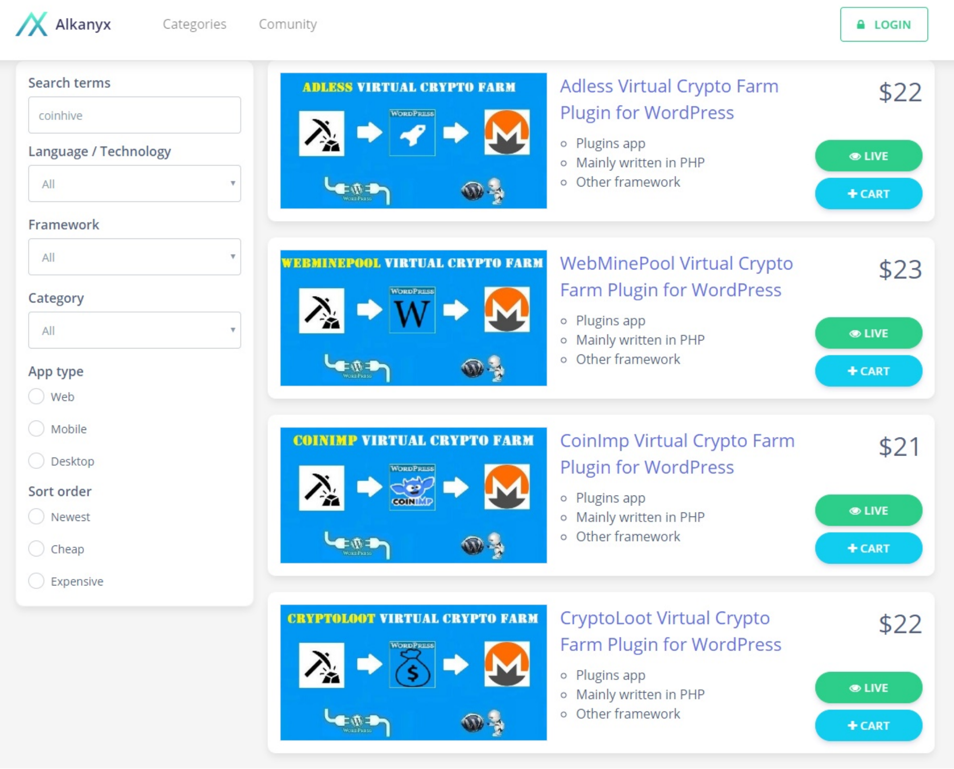
2.2 Types of attacks

There exist several different ways of performing cryptojacking, this thesis will mainly focus on browser based drive-by attacks and infections. Drive-by attacks is characterized by that they do not require any additional actions from the user except visiting a web site. The web site will then run some script to take advantage of an exploit of the visitor's computer to download and execute malicious software. With cryptojacking there is an even more subtle way of doing a drive-by attack. About 95% of all web sites uses

JavaScript[25] and due to it's popularity JavaScript is supported by all major web browsers. JavaScript is a quite powerful scripting language running inside the web browser and uses the computing power of the client, not the server. This allows for a lot of power, including the power to mine cryptocurrency.
While there exist several webminers using webGL and thus utilizing the GPU for mining Bitcoin, these are not very efficient and thus far no webGL miner have been found widely used in the wild mining Monero. There does not seem to be a technical reason why a webGL miner for Monero cannot exist and one will likely be created, if only as a proof of concept.

2.2.1 Website plugins

Instead of using websites directly to mine it is possible to use plugins that are used by websites, such as Wordpress plugins, this way it is possible to reach many more websites with a single attack/compromise. This requires an compromise of the browser extension itself, to be effective the extension have to be quite widely deployed, this means that detection and thus removal is more likely.


Alkanyx
Categories
Comunity
LOGIN
ADLESS VIRTUAL CRYPTO FARM
WEBMINEPOOL VIRTUAL CRYPTO FARM
COINIMP VIRTUAL CRYPTO FARM
CRYPTOLOOT VIRTUAL CRYPTO FARM
LIVE
CART

Search terms
coinhive

Language / Technology
All

Framework
All

Category
All

App type
○ Web
○ Mobile
○ Desktop

Sort order
○ Newest
○ Cheap
○ Expensive

Adless Virtual Crypto Farm Plugin for WordPress — $22
- Plugins app
- Mainly written in PHP
- Other framework

WebMinePool Virtual Crypto Farm Plugin for WordPress — $23
- Plugins app
- Mainly written in PHP
- Other framework

CoinImp Virtual Crypto Farm Plugin for WordPress — $21
- Plugins app
- Mainly written in PHP
- Other framework

CryptoLoot Virtual Crypto Farm Plugin for WordPress — $22
- Plugins app
- Mainly written in PHP
- Other framework

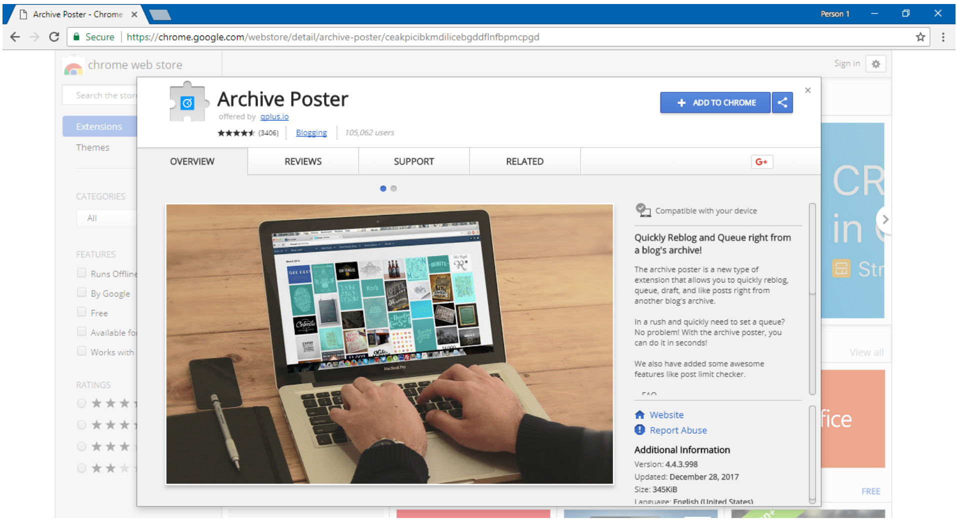
Figure 2.1: Wordpress plugins for several popular cryptojacking sites.

Wordpress has had plugins on it's official plugin page, including several Monero miners using Coinhive [26], some can be seen in fig 2.1. These could be included by legitimate web site owners, but they could also be deployed on compromised sites. To install it on a compromised site will only affect users of that site, so it follows that each attack will have a lesser impact, but discovery and removal is less likely.

2.2.2 Browser extensions

A large part of the modern web experience can be enhanced by browser extensions that work by adding, changing or even removing features to the web browsers, all the major browsers as of 2018 support extensions.

Extensions are yet another vector for attackers. In terms of attacks they are similar to website plugins in that one can reach many users with a singe attack, the main difference lies in that with browser extensions the individual user is attacked and not a single website. One such example is the now defunct Archive Poster seen in fig 2.2.



https://chrome.google.com/webstore/detail/archive-poster/ceakpicibkmdilicebgddflnfbpmcpgd

Archive Poster

offered by qplus.io

★★★★★ (3406) | Blogging | 105,062 users

Compatible with your device

Quickly Reblog and Queue right from a blog's archive!

The archive poster is a new type of extension that allows you to quickly reblog, queue, draft, and like posts right from another blog's archive.

In a rush and quickly need to set a queue? No problem! With the archive poster, you can do it in seconds!

We also have added some awesome features like post limit checker.

Additional Information

Version: 4.4.3.998

Updated: December 28, 2017

Size: 345KiB

Language: English (United States)

Figure 2.2: A plugin for Google's Chrome browser that secretly mines Monero in the background

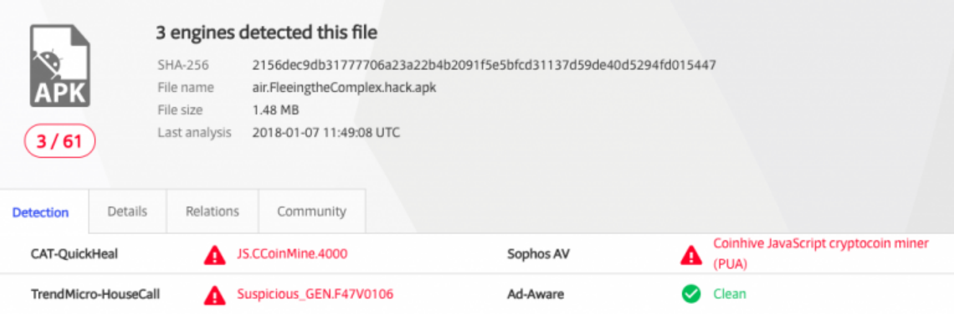
Browser extension attacks can be divided into two main categories, the first is compromising existing extensions and the other is tricking users into installing nefarious extensions, either with or without the user's consent.

2.2.3 Mobile apps

Android apps is a somewhat curious case. They are not really drive-by in the strict sense, but deserves a mention anyway. In Android it is possible to download applications as APK-files from the Internet and install them directly without going through Google's Play Store just like with traditional operative systems. Unlike traditional operative systems the same checks and warnings are lacking in Android, instead there exist a setting to allow side loading, this is off by default in most handsets, but it does not have to be. This

allows for cryptomining apps like HiddenMiner [27] to be installed. Android also have an auto update feature to make sure users are using the latest version of apps, by extension this will allow an app to be updated to include a cryptominer.
It should also be noted that Google have removed all webmining apps from the Google Play Store. Figure 2.3 shows an example of an APK file containing JavaScript cryptominer from Coinhive.

Apple's Ios is less susceptible to these kinds of attack since it is much more locked down, in order to mine natively it requires either a developer account or having the Ios-device jailbroken.
Apple have also made a public statement that they do not allow cryptominers in their App Store.



3 engines detected this file

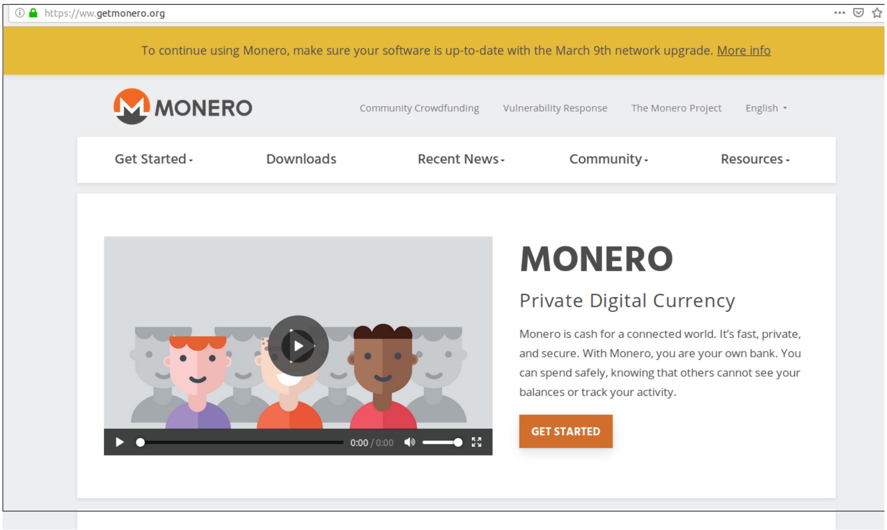
SHA-256	2156dec9db31777706a23a22b4b2091f5e5bfcd31137d59de40d5294fd015447
File name	air.FleeingtheComplex.hack.apk
File size	1.48 MB
Last analysis	2018-01-07 11:49:08 UTC

CAT-QuickHeal	JS.CCoinMine.4000	Sophos AV	Coinhive JavaScript cryptocoin miner (PUA)
TrendMicro-HouseCall	Suspicious_GEN.F47V0106	Ad-Aware	✓ Clean

Figure 2.3: A scan performed on an Android APK by VirusTotal

2.3 Prevention

Luckily for those wanting to avoid cryptojacking many existing techniques can be deployed to prevent cryptojacking[28]. For native miners all the same procedures that prevent other kinds of malware will be effective just the same. Anti-virus program are also catching up and have started detecting cryptominers[29][30][31]. In fact, Windows Defender kept deleting the cryptominer that was downloaded onto the Windows 10 system for this report until a special exception was made for the directory it resides in. For web miners there exist a lot of options as well in the forms of web extensions to some of the most popular browsers such as Mozilla Firefox and Google Chrome, some specialized addons for stopping cryptominers, such as MinerBlock[32] or NoCoin[33] have been created especially for this purpose, but the already established and more general purpose ad-blockers such as Ublock Origin[34] and Ghostery[35] also get the job done as they treat the cryptominer scripts just like advertisement scripts.



To continue using Monero, make sure your software is up-to-date with the March 9th network upgrade. More info

MONERO

Private Digital Currency

Monero is cash for a connected world. It's fast, private, and secure. With Monero, you are your own bank. You can spend safely, knowing that others cannot see your balances or track your activity.

Figure 2.4: Getmonero front page

2.4 Monero

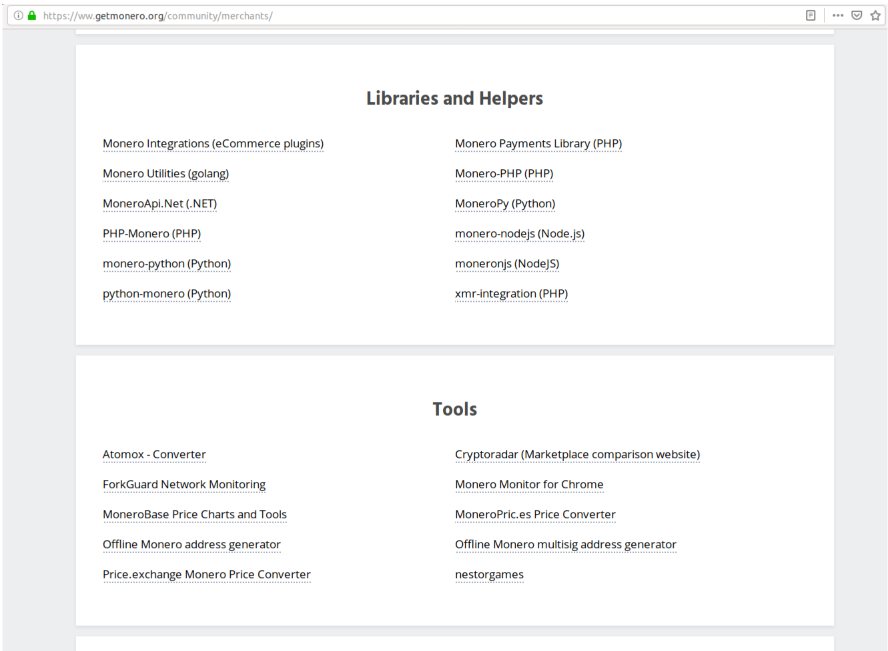
Monero [2] is a form of crypto currency that is often associated with cryptojacking. It uses an algorithm called CryptoNote that offers two features in particular that make it very attractive for the activity[36]:

- It is virtually untraceable and unlinkable.
- It uses a memory-bound function to shrink the gap between consumer grade hardware and special purpose grade hardware.

Monero is a community project and Getmonero (fig 2.4) is the de facto home page for the project. At this page one can get information about how to acquire and spend Monero as well as information about the project as a whole, find resources for Monero and participate in the Monero community.

2.4.1 Monero as payment

Monero, like other crypto currencies are touted as alternative payment methods, and to some degree this holds true. The Monero project's own website have an up to date list of merchants they know accept Monero[37]. This includes several exchanges that allow one to trade Monero for other currencies, crypto or otherwise, some casinos and a lot of services that accept donations. However, there are also a many products of a more material art that can by bought with Monero, most of it seem to cater to a tech-savvy crowd, such as VPNs and web hosting, but it is possible to buy jewelry, coffee and even dog training. It must also be assumed that Monero is used in illegal and illegitimate business, but that is beyond the scope of this thesis. Some of the Tools and libraries for integrating Monero into a website can be seen in fig 2.5



https://ww.getmonero.org/community/merchants/

Libraries and Helpers

- Monero Integrations (eCommerce plugins)
- Monero Utilities (golang)
- MoneroApi.Net (.NET)
- PHP-Monero (PHP)
- monero-python (Python)
- python-monero (Python)
- Monero Payments Library (PHP)
- Monero-PHP (PHP)
- MoneroPy (Python)
- monero-nodejs (Node.js)
- moneronjs (NodeJS)
- xmr-integration (PHP)

Tools

- Atomox - Converter
- ForkGuard Network Monitoring
- MoneroBase Price Charts and Tools
- Offline Monero address generator
- Price.exchange Monero Price Converter
- Cryptoradar (Marketplace comparison website)
- Monero Monitor for Chrome
- MoneroPric.es Price Converter
- Offline Monero multisig address generator
- nestorgames

Figure 2.5: Some merchants that accept Monero as payment

2.4.2 CryptoNote

While Bitcoin in theory is anonymous it is in reality trivial to link a person with an account. To keep the integrity of the blockchain all Bitcoin transactions and associated wallets are public. This means that if a person is linked to a wallet it is trivial to find all previous transactions made the same person, assuming a person only have a single wallet and a wallet is only used by a single individual. CryptoNote solves this problem by creating a stealth address associated with every transaction.

In cryptomining everyone that mines is competing to solve the next "block" and get the next payout. Some currencies such as Bitcoin uses primarily raw computing power and can be effectively done in parallel, this is not the case of CryptoNote. CryptoNote and thus Monero requires a relatively large amount of memory (CPU-cache or RAM) and the blocks are dependent on previous blocks. This means that the benefits of using GPUs or ASICs over CPUs are severely diminished compared to Bitcoin. Accordingly average consumer hardware have a decent chance to solve the puzzle and get the payout. This in turn make Monero an attractive currency to mine in browsers using JavaScript.

Ring Signatures

In the traditional public key/private key system a user Alice uses her private key to sign and her public key can be used to verify Alice's signature. This system has proven very efficient, but it is not ideal for keeping users anonymous. The concept of ring signatures fixes this, instead of a single pair of public and private keys a group of keys are used and the public key can only be used to verify that the signer belong to the group and thus provide anonymity of outgoing transactions.

One-time keys

To anonymize incoming transactions CryptoNote create one-time keys for every transaction. This is done using the Diffie-Hellman exchange protocol where the sender can only produce the public part of the key pair and the receiver can only produce the private part, thus making sure only the receiver can release the funds.

Double spending

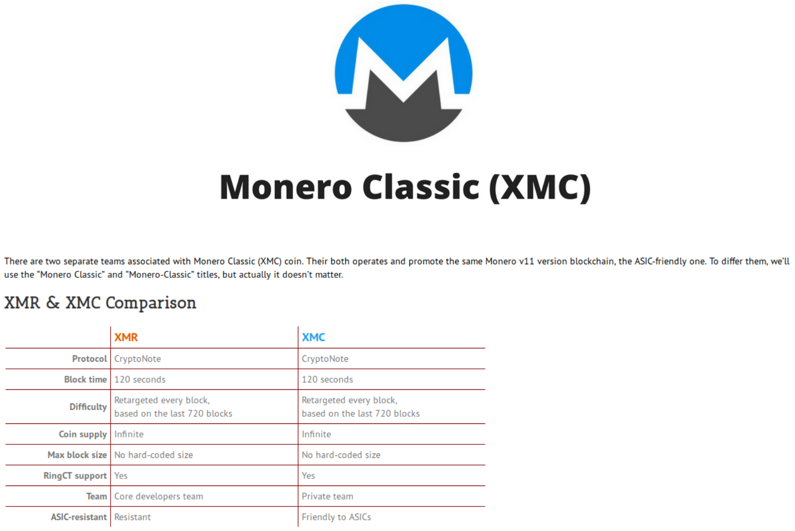
If the transactions was fully anonymous anyone would be able to spend their coins as many times as the liked, this obviously cannot be allowed. This is solved by introducing a key image, a one-way cryptographic function of the secret key. It can be used to link transactions created with the same private key, that is double-spending attempts, while still keeping the sender anonymous.

2.4.3 Hard forks

One of the things that sets Moenro apart from other crypto currencies is it's philosophy towards how mining should be done. Monero started out as a grassroots project and the project have a goal of letting regular people with consumer hardware rather than specialized and optimized hardware have a realistic chance of mine. To this end the Monero project have worked to stifle application specific integrated circuits (ASICs). This have been accomplished by hard forking the Monero project and make changes to the algorithm[38][39]. The many forks have led to other alternative Monero currencies, some of which can be seen in fig 2.6, more are listed on Monero.org.[40]

2.4.4 Bytecoin

Monero is a derivative of Bytecoin and uses much of the same technology. Bytecoin was released into the public in 2014. It's creators had backdated it's release to 2012 and mined about 80% of the supply themselves. When it was discovered the cryptocommunity disowned Bytecoin, but the technology was sound so instead of abandoning it completely it was forked, first to Bytemonero, and later to Monero.



Monero Classic (XMC)

There are two separate teams associated with Monero Classic (XMC) coin. Their both operates and promote the same Monero v11 version blockchain, the ASIC-friendly one. To differ them, we'll use the "Monero Classic" and "Monero-Classic" titles, but actually it doesn't matter.

XMR & XMC Comparison

	XMR	XMC
Protocol	CryptoNote	CryptoNote
Block time	120 seconds	120 seconds
Difficulty	Retargeted every block, based on the last 720 blocks	Retargeted every block, based on the last 720 blocks
Coin supply	Infinite	Infinite
Max block size	No hard-coded size	No hard-coded size
RingCT support	Yes	Yes
Team	Core developers team	Private team
ASIC-resistant	Resistant	Friendly to ASICs

Figure 2.6: Monero Classic

2.5 Coinvalue

Since cryptojacking is achieved by mining cryptocurrency it's viability is inevitably linked to the value of the mined currency. The value of cryptocurrencies is largely unregulated and is for the most part based solely on supply and demand. This, and the fact that cryptocurrencies is a relatively recent concept it has thus far been a very volitional commodity. Fig 2.7 is a chart showing the price trend of Bitcoin, Etherium and Monero in United States Dollars from January 1st 2017 to April 16th 2019.2.7 The main take-away from these is that cryptocurrencies are very volatile and unpredictable. A second take-away is that the currencies seem to mirror each other in price trends. Note that the scale is logarithmic.

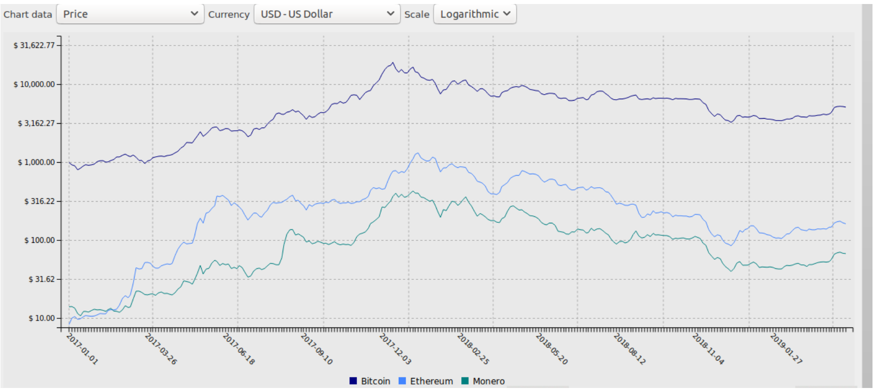


Chart data: Price

Currency: USD - US Dollar

Scale: Logarithmic

Figure 2.7: Bitcoin, Etherium and Monero price trend 2017-01-01 to 2019-04-16 [1]

Chapter 3

Related work

While cryptomining has been around for more than a decade, cryptojacking has not. It was first discovered widely deployed in late 2017 and thus there are not much previous research on the topic. However, what little there is seems to be in agreement. Cryptojacking is different from most other kinds of malware in that the impact is different. In contrast to most other attacks cryptojacking is not concerned by getting information from the victim, neither does it want to interrupt the victims work flow or operations, all it wants are CPU cycles. The longer it can stay hidden and undetected the more CPU cycles it can extract.

Google trends show that interest in browser based cryptomining skyrocketed in late 2017 and early 2018 [41]. This coincides with the start of Coinhive [4]. The main impact of cryptojacking seems to be excess power consumption, especially impacting battery powered devices, and to some extent denial of service [42] [43].

But while the goal of cryptomining is dissimilar to other malware it can be dealt with like most other malware, as it will in most cases infect the machines using the same kind of techniques used by other malware and many well known exploits and features from around the web is used in cryptojacking.

3.1 Crypto currencies and the blockchain

This section will give a brief overview of crypto currencies and the blockchain in general.

3.1.1 Crypto currency as money

The first mainstream cryptocurrency, Bitcoin, was created with the stated goal of create a decentralized global currency[44]. The system implemented as part of the Bitcoin system, and by subsequent cryptocurrencies is the block chain. The traditional method of doing business online is trough a trusted third party, such as VISA, MasterCard or PayPal. The blockchain does away with the need for a trusted intermediary and relies instead on cryptographic proof to maintain the integrity of the system. Cryptocurrencies differ from fiat currencies in another fundamental way: While both fiat and cryptocurrencies lack any intrinsic value fiat currencies are usually backed by a nation state that guaranty that the currency will have at least some value, if for no other reason that the state requires taxes to be paid in the local fiat currency. Cryptocurrencies lack this backing and their value is set solely by the marked, more akin to stocks and bonds. However, that comparison also falls apart due to the fact that stocks and bonds get their value from the companies or products they are linked with.

3.1.2 Crypto currency in crime

Cryptocurrencies have been linked to many kinds of crimes since their inception, this section will look briefly at how cryptocurrencies are used in crime today and in the past.

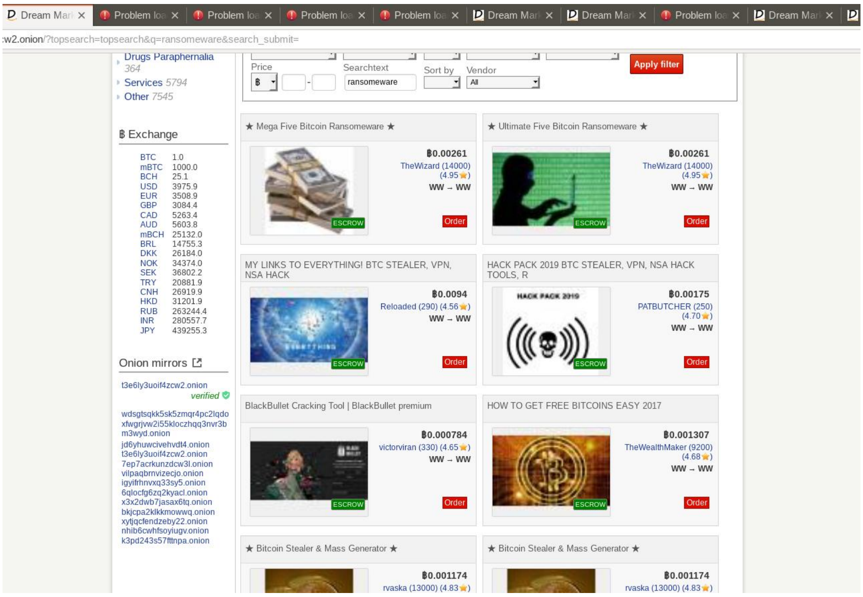
Marketplaces

Crime is by it's very nature a risky activity. Exposure by law enforcement will likely lead to fines or imprisonment. Additionally a criminal record can make it more difficult to get a (legitimate) job. Despite this there exist several online marketplaces that exist primarily to facilitate trade of illegal goods and services. One example of this is the now defunct Silk Road[45] and it's spiritual successor Dream[46]. These sites are only accessible through Tor[47] as a hidden service. Cryptocurrencies provide a method of transferring money that are more anonymous than most, is tax free and does not rely on a central entity to function as a intermediary. One of the interesting aspects of sites like The Silk Road and Dream is that they in many ways functions like legitimate e-commerce sites such as eBay. Both kinds of sites relies on trust [48][49] on the buyers and sellers, and cryptocurrency cannot remove the need for trust, it can only serve to mask the buyers and sellers, it cannot guarantee that the customer get what they pay for and in the lawless market of the dark web trust is even more valuable than on the open web.

These market places are host a whole suite of different services, among them botnets, cryptominers and extortion software.

Ransomeware and extortion

Ransomware is a class of malware that works by encrypting the victims data, thus render it unreadable. Then the attacker will demand a ransom from the victim in order for the files to be decrypted. One of the challenges for the attackers are how to receive the payment without revealing their identity or the transaction being traced or blocked by banks or law enforcement. Over the years criminals have used many different techniques such as short message services to premium numbers, gift vouchers that are then resold, payment services such as PayPal or YandexMoney and prepaid services such as Ukash or Moneypak[50]. All of these services are inferior to cryptocurrencies in terms of tractability and ease of use, from the perspective of the criminals. Bitcoin has been the preferred cryptocurrency of choice for some years, but Bitcoin is by nature



:w2.onion/?topsearch=topsearch&q=ransomeware&search_submit=

Drugs Paraphernalia 364
Services 5794
Other 7545

Price ฿ -
Searchtext ransomeware
Sort by
Vendor All

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	25.1
USD	3975.9
EUR	3508.9
GBP	3084.4
CAD	5263.4
AUD	5603.8
mBCH	25132.0
BRL	14755.3
DKK	26184.0
NOK	34374.0
SEK	36802.2
TRY	20881.9
CNH	26919.9
HKD	31201.9
RUB	263244.4
INR	280557.7
JPY	439255.3

Onion mirrors

t3e6ly3uoif4zcw2.onion
verified

wdsgtsqkk5sk5zmqr4pc2lqdo
xfwgrjvw2i55kloczhqq3nvr3b
m3wyd.onion
jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

★ Mega Five Bitcoin Ransomeware ★
฿0.00261
TheWizard (14000) (4.95★)
WW → WW

★ Ultimate Five Bitcoin Ransomeware ★
฿0.00261
TheWizard (14000) (4.95★)
WW → WW

MY LINKS TO EVERYTHING! BTC STEALER, VPN, NSA HACK
฿0.0094
Reloaded (290) (4.56★)
WW → WW

HACK PACK 2019 BTC STEALER, VPN, NSA HACK TOOLS, R
฿0.00175
PATBUTCHER (250) (4.70★)
WW → WW

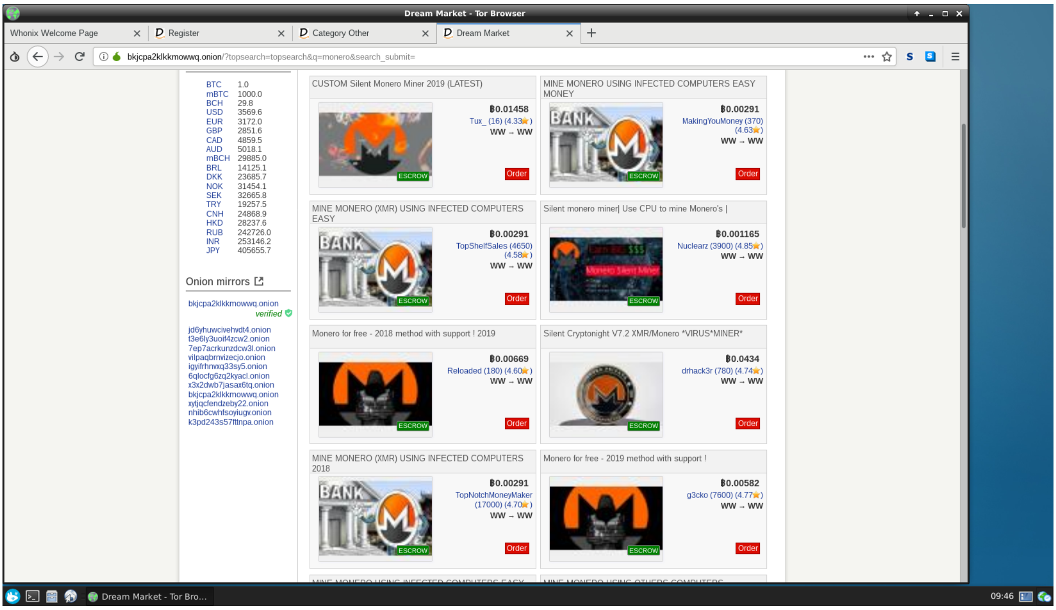
BlackBullet Cracking Tool | BlackBullet premium
฿0.000784
victorviran (330) (4.65★)
WW → WW

HOW TO GET FREE BITCOINS EASY 2017
฿0.001307
TheWealthMaker (9200) (4.68★)
WW → WW

★ Bitcoin Stealer & Mass Generator ★
฿0.001174
rvaska (13000) (4.83★)

★ Bitcoin Stealer & Mass Generator ★
฿0.001174
rvaska (13000) (4.83★)

Figure 3.1: The front page of Dream



bkjcpa2klkkmowwq.onion/?topsearch=topsearch&q=monero&search_submit=

BTC	1.0
mBTC	1000.0
BCH	29.8
USD	3569.6
EUR	3172.0
GBP	2851.6
CAD	4859.5
AUD	5018.1
mBCH	29885.0
BRL	14125.1
DKK	23685.7
NOK	31454.1
SEK	32665.8
TRY	19257.5
CNH	24868.9
HKD	28237.6
RUB	242726.0
INR	253146.2
JPY	405655.7

Onion mirrors

bkjcpa2klkkmowwq.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

CUSTOM Silent Monero Miner 2019 (LATEST)
฿0.01458
Tux_ (16) (4.33★)
WW → WW

MINE MONERO USING INFECTED COMPUTERS EASY MONEY
฿0.00291
MakingYouMoney (370) (4.63★)
WW → WW

MINE MONERO (XMR) USING INFECTED COMPUTERS EASY
฿0.00291
TopShelfSales (4650) (4.58★)
WW → WW

Silent monero miner| Use CPU to mine Monero's |
฿0.001165
Nuclearz (3900) (4.85★)
WW → WW

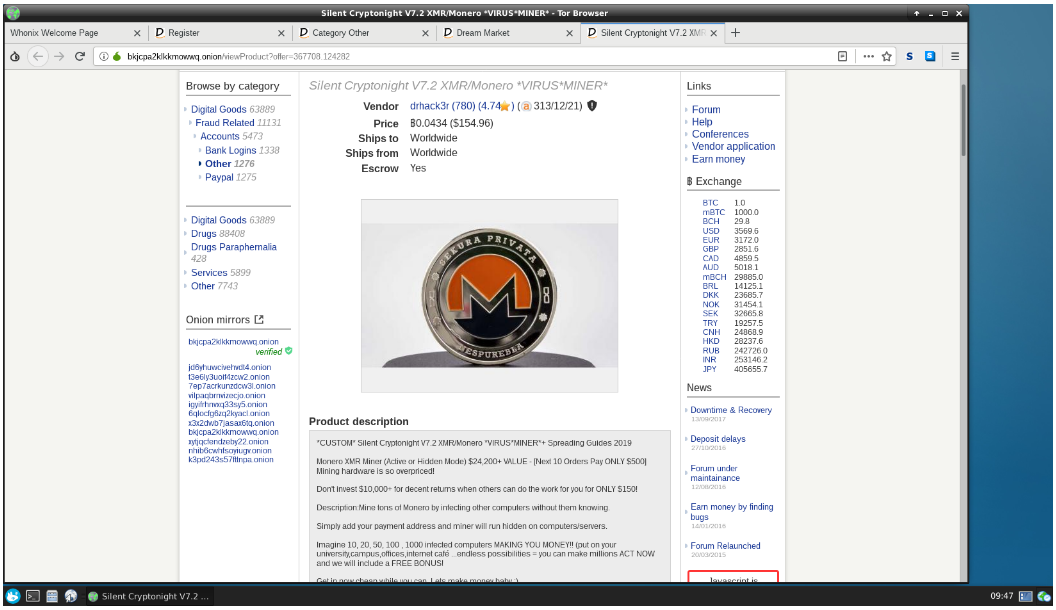
Monero for free - 2018 method with support ! 2019
฿0.00669
Reloaded (180) (4.60★)
WW → WW

Silent Cryptonight V7.2 XMR/Monero *VIRUS*MINER*
฿0.0434
drhack3r (780) (4.74★)
WW → WW

MINE MONERO (XMR) USING INFECTED COMPUTERS 2018
฿0.00291
TopNotchMoneyMaker (17000) (4.70★)
WW → WW

Monero for free - 2019 method with support !
฿0.00582
g3cko (7600) (4.77★)
WW → WW

Figure 3.2: Search results for "Monero" on Dream


Silent Cryptonight V7.2 XMR/Monero *VIRUS*MINER* - Tor Browser
Whonix Welcome Page
Register
Category Other
Dream Market
Silent Cryptonight V7.2 XMR
bkjcpa2klkkmowwq.onion/viewProduct?offer=367708.124282
Silent Cryptonight V7.2 ...
09:47

Browse by category

- Digital Goods 63889
- Fraud Related 11131
- Accounts 5473
- Bank Logins 1338
- **Other** 1276
- Paypal 1275

- Digital Goods 63889
- Drugs 88408
- Drugs Paraphernalia 428
- Services 5899
- Other 7743

Onion mirrors

bkjcpa2klkkmowwq.onion *verified*

jd6yhuwcivehvdt4.onion
t3e6ly3uoif4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbrnvizecjo.onion
igyifrhnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion
nhib6cwhfsoyiugv.onion
k3pd243s57fttnpa.onion

*Silent Cryptonight V7.2 XMR/Monero *VIRUS*MINER**

Vendor	drhack3r (780) (4.74⭐) (ⓐ 313/12/21)
Price	฿0.0434 ($154.96)
Ships to	Worldwide
Ships from	Worldwide
Escrow	Yes

Product description

CUSTOM Silent Cryptonight V7.2 XMR/Monero *VIRUS*MINER*+ Spreading Guides 2019

Monero XMR Miner (Active or Hidden Mode) $24,200+ VALUE - [Next 10 Orders Pay ONLY $500] Mining hardware is so overpriced!

Don't invest $10,000+ for decent returns when others can do the work for you for ONLY $150!

Description:Mine tons of Monero by infecting other computers without them knowing.

Simply add your payment address and miner will run hidden on computers/servers.

Imagine 10, 20, 50, 100 , 1000 infected computers MAKING YOU MONEY!! (put on your university,campus,offices,internet café ...endless possibilities = you can make millions ACT NOW and we will include a FREE BONUS!

Get in now cheap while you can. Lets make money baby :)

Links

- Forum
- Help
- Conferences
- Vendor application
- Earn money

฿ Exchange

BTC	1.0
mBTC	1000.0
BCH	29.8
USD	3569.6
EUR	3172.0
GBP	2851.6
CAD	4859.5
AUD	5018.1
mBCH	29885.0
BRL	14125.1
DKK	23685.7
NOK	31454.1
SEK	32665.8
TRY	19257.5
CNH	24868.9
HKD	28237.6
RUB	242726.0
INR	253146.2
JPY	405655.7

News

- Downtime & Recovery 13/09/2017
- Deposit delays 27/10/2016
- Forum under maintainance 12/08/2016
- Earn money by finding bugs 14/01/2016
- Forum Relaunched 20/03/2015

Javascript is

Figure 3.3: A Monero crypto miner on Dream

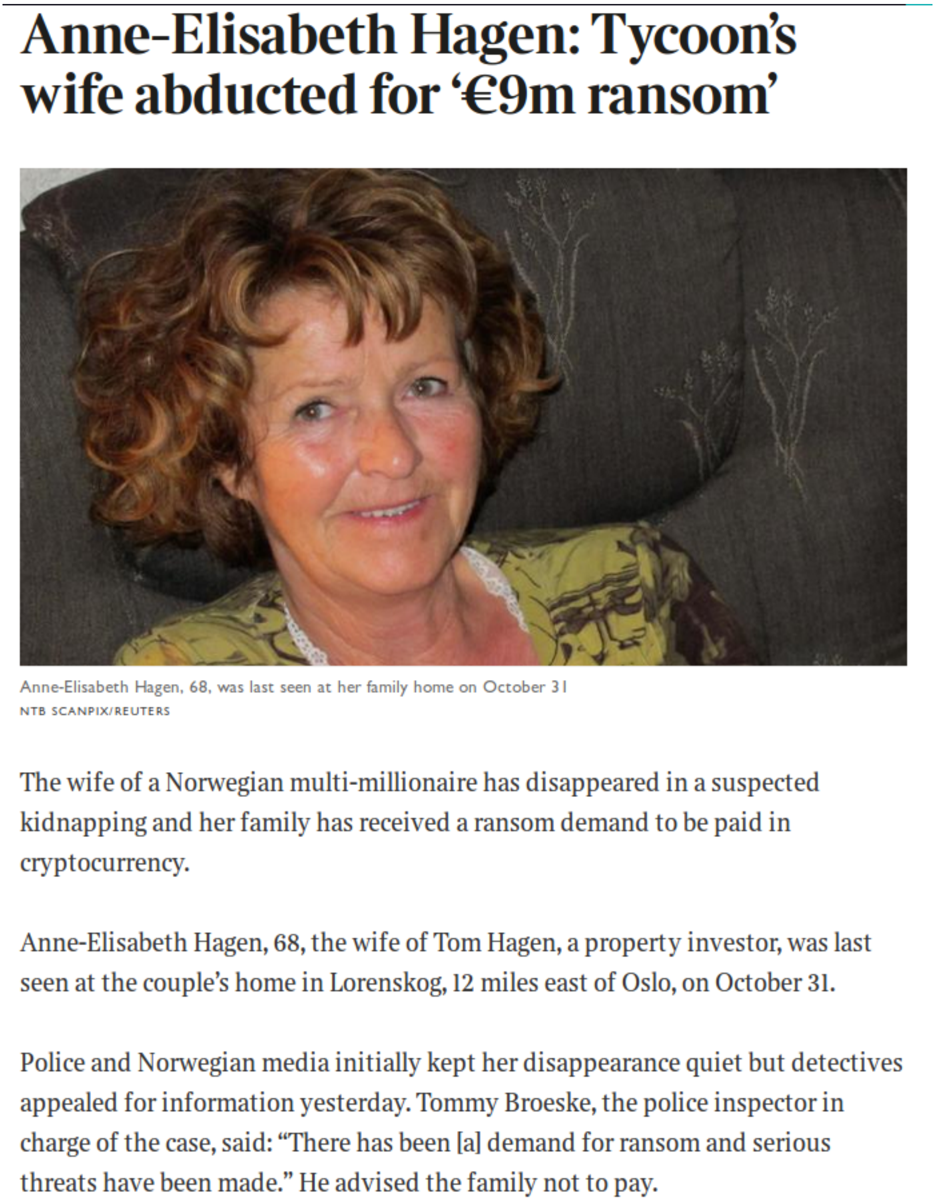
traceable as all the transactions are visible on the public block chain. It is likely that more privacy focused currencies such as Monero will become the more preferred alternative in the future. Recently Monero was demanded as ransom in an abduction case in Norway[51][52].

3.2 Drive-by infections

This thesis focuses mainly on the drive-by nature of cryptojacking and this section will look briefly at how drive-by attacks are conducted in the past and present.

Drive-by downloads

A drive-by download is an attack that will download a file onto the victims computer, often automatically upon visiting a web site. The simplest of kinds of attacks require the user to actively click on and launch the downloaded file[53]. Getting the user to open the file is usually done by social engineering, and thus convincing the victim that file is legitimate. The more advanced methods uses unpatched vulnerabilities, often Zero-days to bypass the user entirely. This can be exploited to get a victim to run any kind of software, including cryptominers, but this thesis will only briefly touch on native cryptomining.



Anne-Elisabeth Hagen: Tycoon's wife abducted for '€9m ransom'

Anne-Elisabeth Hagen, 68, was last seen at her family home on October 31

NTB SCANPIX/REUTERS

The wife of a Norwegian multi-millionaire has disappeared in a suspected kidnapping and her family has received a ransom demand to be paid in cryptocurrency.

Anne-Elisabeth Hagen, 68, the wife of Tom Hagen, a property investor, was last seen at the couple's home in Lorenskog, 12 miles east of Oslo, on October 31.

Police and Norwegian media initially kept her disappearance quiet but detectives appealed for information yesterday. Tommy Broeske, the police inspector in charge of the case, said: "There has been [a] demand for ransom and serious threats have been made." He advised the family not to pay.

Figure 3.4: A news article about the Anne-Elisabeth Hagen abduction

Drive-by JavaScript Malware

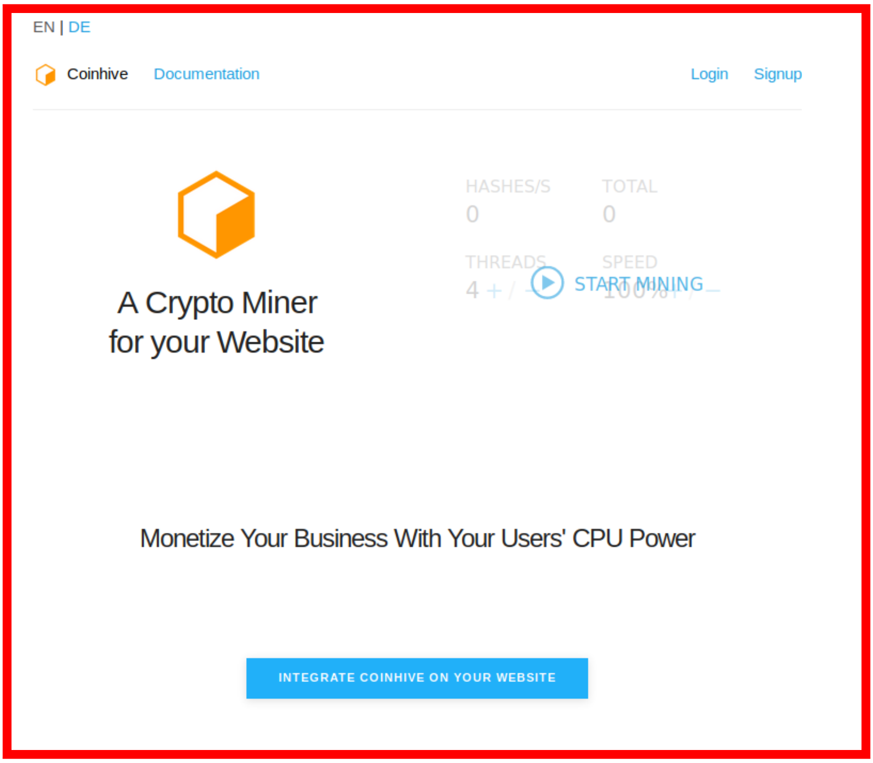
Drive-by script attacks on the other hand does not try to download a malicious payload to the victims system or utilizing flaws or vulnerabilities, instead it works by using legal means within the browser and the HTML-document, often Cross Site Scripting (XSS) or Cross Site Request Forgery (XSRF) are used. JavaScript Malware can be used to track a person, or at least their browser cross sites, called fingerprinting, even when cookies are disabled and execute code with implicit privileges and authentication, such as performing a task that a logged in user could do given that the browser contain a logged in session token or gaining access to a a local intranet that the browser can access. Or more mundanely, JavaScript Malware can be used to simply run some code contained inside the web page, this is done legitimately by most pages to show content, including advertisements, but it can also be used to attack a third party. By executing the attack from a site in JavaScript the connection will actually come from the browser's IP and the browser will function as a proxy, or in the case of an Distributed Denial of Service (DDoS) attack the browsers function as an amplifier[54]. JavaScript have been known to be injected into sites using the advertisement platforms such as Google Tag Manager[41]. In this thesis JavaScript Malware, and in particular the mundane kind are the most relevant kind of attacks, as that is how cryptojacking is performed. It usually leaves no trace on the victims and often they do not know that that they have been exploited.

3.3 Coinhive

An example of flyby cryptojacking is Coinhive [4]. It allowed website owners to deliberately put a Monero [2] cryptominer on their website. It worked by placing a string of JavaScript into the website, as users visits a site with a miner they are given the choice to let it use their CPU to mine Monero. However it has also been injected into compromised sites [55][56]. Coinhive took a 500 EUR for signups, then they took a 30% share of whatever it's users mined. Coinhive also offered a captcha service and short links. They both worked by using proof of work, that is, in order for a user to be verified they have to do some work, they have to spare some CPU cycles to mine Monero for the owner of the capthca or short link.
The services offered by Coinhive was not itself nefarious or illegal, in fact, they advertises themselves as an alternative to advertisement, which is one of the main sources of revenue on the Internet to day. While not the primary objective this thesis will shed some light on whether this could be viable alternative.

Coinhive was quite controversial and have received their share of criticism. Much of this stems from the fact that their initial script did not ask web site visitors for their consent and that it was felt that they did not do enough to prevent their scripts from being used an compromised sites.

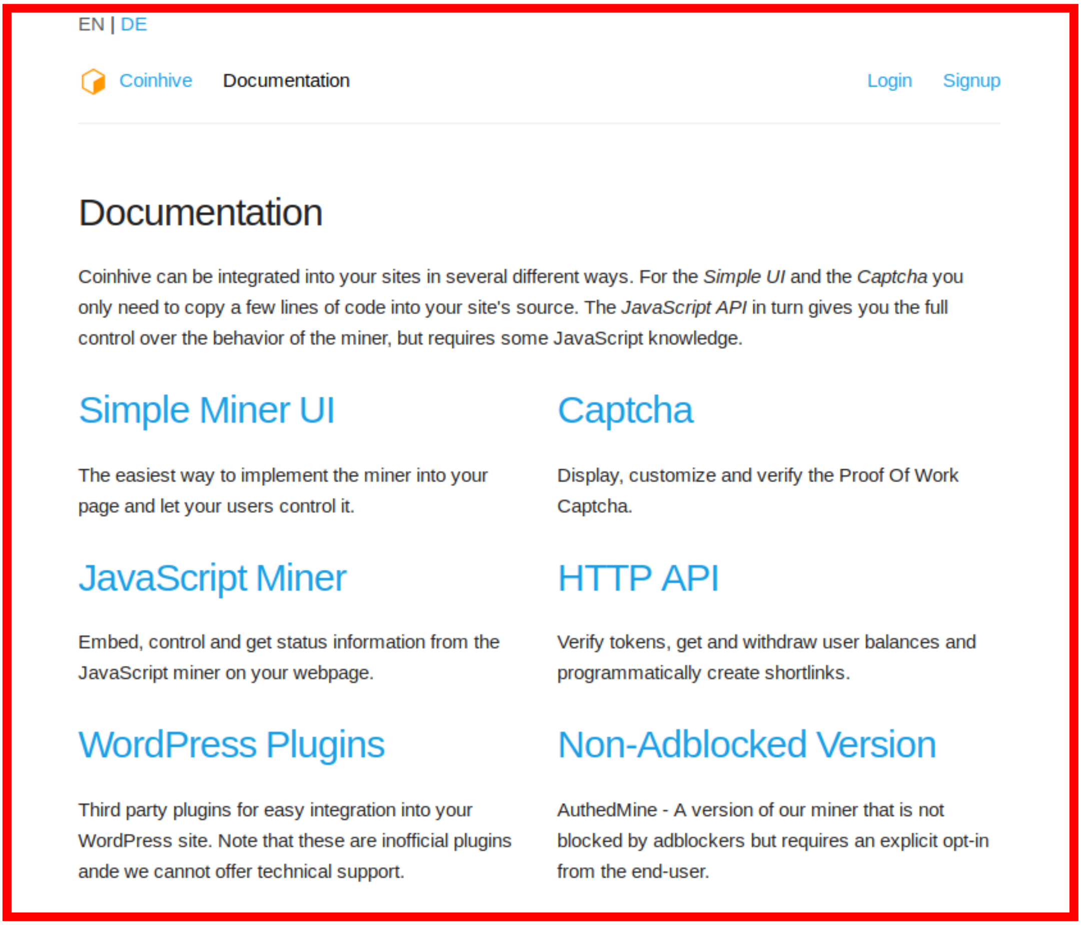
On February 26, 2019 the Coinhive Team posted on their blog that they were shutting down their service as of March 8, 2019. According to the Coinhive Team it was no longer profitable to keep the service operating anymore, citing that Monero have



A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power

Figure 3.5: Coinhive's landing page



EN | DE

Coinhive Documentation Login Signup

Documentation

Coinhive can be integrated into your sites in several different ways. For the *Simple UI* and the *Captcha* you only need to copy a few lines of code into your site's source. The *JavaScript API* in turn gives you the full control over the behavior of the miner, but requires some JavaScript knowledge.

Simple Miner UI

The easiest way to implement the miner into your page and let your users control it.

Captcha

Display, customize and verify the Proof Of Work Captcha.

JavaScript Miner

Embed, control and get status information from the JavaScript miner on your webpage.

HTTP API

Verify tokens, get and withdraw user balances and programmatically create shortlinks.

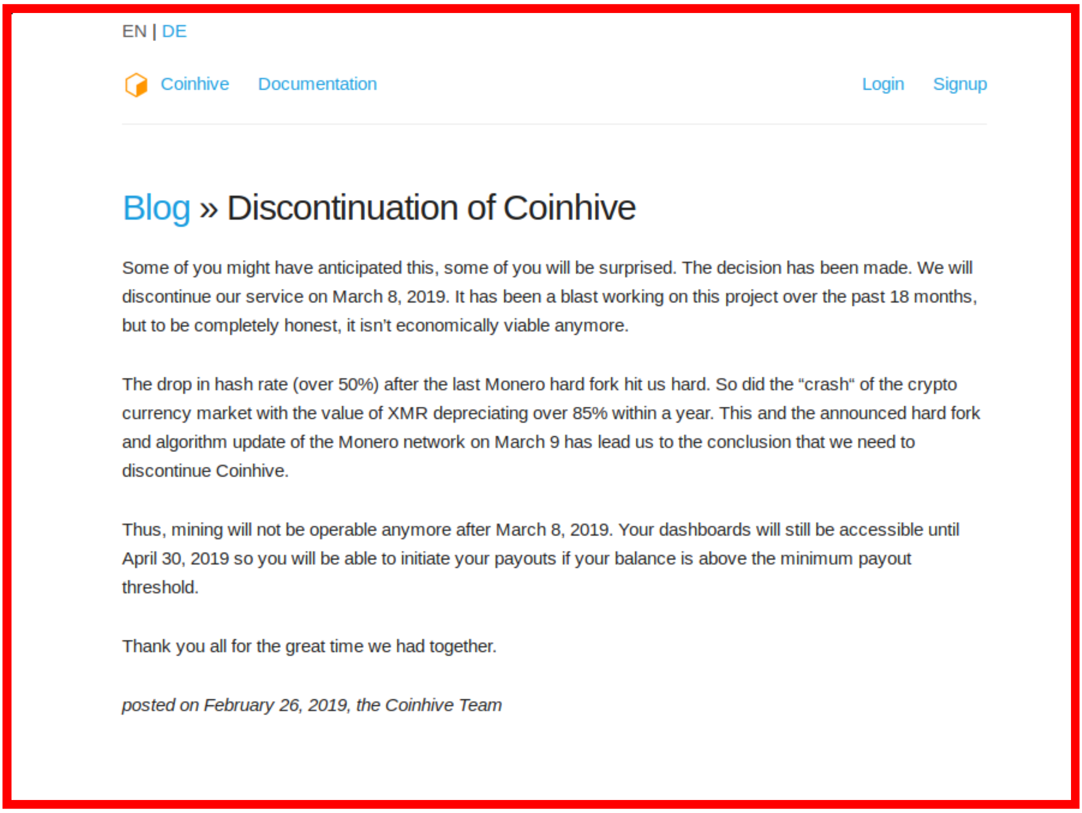
WordPress Plugins

Third party plugins for easy integration into your WordPress site. Note that these are inofficial plugins ande we cannot offer technical support.

Non-Adblocked Version

AuthedMine - A version of our miner that is not blocked by adblockers but requires an explicit opt-in from the end-user.

Figure 3.6: Coinhive's documentation page



Blog » Discontinuation of Coinhive

Some of you might have anticipated this, some of you will be surprised. The decision has been made. We will discontinue our service on March 8, 2019. It has been a blast working on this project over the past 18 months, but to be completely honest, it isn't economically viable anymore.

The drop in hash rate (over 50%) after the last Monero hard fork hit us hard. So did the "crash" of the crypto currency market with the value of XMR depreciating over 85% within a year. This and the announced hard fork and algorithm update of the Monero network on March 9 has lead us to the conclusion that we need to discontinue Coinhive.

Thus, mining will not be operable anymore after March 8, 2019. Your dashboards will still be accessible until April 30, 2019 so you will be able to initiate your payouts if your balance is above the minimum payout threshold.

Thank you all for the great time we had together.

posted on February 26, 2019, the Coinhive Team

Figure 3.7: Coinhive's blog stating that they are going out of business

depreciated more than 85% over the last year and that the hash rate dropped over 50% after the last hard fork[57].

3.3.1 Alternatives

There exists several alternatives to Coinhive that provides more or less the same service, among these are CoinIMP[58] and CryptoLoot[59], both launched in 2017, neither have had much success when compared to Coinhive, but with Coinhive's recent shutdown they might sweep in to take it's place. Another alternative are projects like Deep Miner[60] that decided to open source their entire project after the most recent hard fork.

3.4 The current state

With the rise of cryptojacking there have been done a considerable amount of research into the subject over the last couple of years, this section will summarize some of the findings. Coinhive's scripts accounted for almost 70% of the current cryptojacking

JavaScript on the web in 2018 [61], and while their scripts defaults to use 100% of the victims CPU researchers have found that most sites that used Coinhive's script throttle themselves and uses between 25% [41] and 70% [62] of available CPU power, this is likely to stop the affected computer to stall and to not inconvenience the user. There are however large discrepancies and some sites try to use as many cores as possible, some even try to use more cores than are available on the system.

3.4.1 Profitability

Coinhive touts themselves as an alternative to advertisements and estimates that a site can make a monthly revenue of about 0.3 XMR (approx. 15 USD at 7 March 2019) with 10-20 active users[4]. While this might be true it requires users to keep the website open in their browsers, ads usually only requires to be loaded once to pay out to the website. Some sites, such as large video streaming sites, like YouTube and Pornhub might be able to keep their customers around for a longer time and thus they can be expected to make a much larger profit, several hundreds XMR per day, however the average web site will have a hard time making any profit from web based miners, only making a few dollars per day and even the bit hitters like Pornhub already make more by advertisements at 1 USD per thousands impressions (approx 80,000 USD than they would by using Conihive (approx. 12,000 USD at 1 XMR = 50 USD)[62]. Some research indicate that the profitability of cryptojackers are several orders of magnitude lower than that of traditional web advertisements[61]. This was true even when one XMR sold for over 200 USD.

3.4.2 Cost to the user/victim

The cost imposed on the end user is not insignificant, in fact the average miner requires 1.7 times more RAM, about 60 times more CPU and about 3.4 times as much network traffic when compared to advertisements [61]. If the user have several web sessions open simultaneously this impact could incur significant costs, both in power consumption and bandwidth. The excess bandwidth is especially concerning when considering mobile devices where most end users still have a data cap or pay based on usage.

Chapter 4

Research method

To measure the impact of cryptojacking an experiment was set up. Using the Merriam-Webster definition of an experiment, the experiment is a tent that shall test the following hypothesis[63]. The goal of the experiment was multifaceted, first it was to understand how cryptojacking affected performance of the system used to mine, secondly to measure the power consumption impact of cryptomining, thirdly to get a sense of how profitable it would be to mine Monero on different machines and finally to measure the difference in mining nativly on the machines and mining with JavaScript in a web browser.
Fisher's defines a few important principles of experiments[64]:

- Comparison
  Comparison are used to when independent measurements are not meaningful, for example it is much more useful to compare computer benchmarks to each other than to look at the numbers by themselves. Comparison often uses a scientific control or an established standard as a baseline.

- Randomization
  Randomization is a process where individuals are assigned to different groups. This process remove some of the bias of the observers and the ones conducting the experiment. Randomization also tends to mitigate confounding.

- Statistical Replication
  Statistical Replication means that it must be possible to recreate the experiment. It is important to document all the uncertainty and imperfections in the experiment, so that it is known when the experiment is replicated. An experiment that is peer-reviewed and gives the similar results when it is replicated is strengthen in terms of reliability and validity.

- Blocking
  Blocking means to arrange the units to be experimented on into groups (blocks) that share similar characteristics. Blocking reduces known, but irrelevant sources

of variations between the units, this allows for greater precision when estimating the sources of variation during the study.

- Orthogonality
  Orthogonality concerns the comparisons/contrasts that can be efficiently and legitimately be carried out. These contrasts can be represented by a vectors and sets of orthogonal contrasts are uncorrelated and independently distributed. Since they are independent each orthogonal provides different information to the others. This can be used to reduce the number of variables that must be kept track of.
- Factorial Experiments
  Factorial experiments are experiments that tests several factors at the same time. This kinds of experiments are efficient at evaluating the interactions of several independent variables.

Comparison

The results have to be compared to be useful, while some of the numbers, in particular the power consumption one's are interesting in a vacuum they are much more interesting as a basis for comparison and the hash rate numbers are rather meaningless without comparison. To make the numbers as comparable as possible a common format for collecting and displaying the data is used.

Randomization

The experiment will not use randomization, in fact there are some barriers in place to minimize the randomness of the results. Randomization could have been used if the experiment had been expanded to include more users to test the machines. In that case the subjects could have been given machines with cryptominers running at different configurations and the subjects could have reported how they found the machine and one could have look at how the users subjective experience compared to the mining being performed at the machines.

Statistical Replication

To facilitate statistical replication the experiment are detailed, all hardware, software as well as settings used are heavily documented. This is done to make sure that if anyone wishes to recreate the experiment it should be as easy as possible.

Blocking

In this experiment blocking is used in regard to the computers, blocking the result's from each computer together. Blocking can also be used on the different parameters, that is blocking i.e. single core performance.

Orthogonality

Orthogonality is not used in the experiment at all, it does not fit.

Factorial Experiments

The experiment have some facets of a factorial experiment in the performance tests were both performance and latency is tested. There the machines single core and multicore performance are tested, both when idling and with different amounts of cores mining.

4.1 Hypothesis

The hypothesis assumes that mining, both in the browser and nativly will affect the user negatively, but that the impact of most miners will be relatively minor and in most cases it will not cause significant harm to the system mining or significantly hinder everyday use.

It is expected that there will be a significant overhead when mining in the browser versus natively.
The power consumption is expected to be similar when mining with the same amount of cores, whether in browser or native.
It is expected that there will be some overhead when adding cores, so the increase in mining efficiency is expected to be somewhat less than linear.
CrytoNigth uses chunks of 2 MiB at the time (MiB is defined as 2^{20} bytes. MiB is sometimes used interchangeably with MB, which is defined as 10^6 bytes.), it is therefore expected to see a leveling off when the CPU cache is less than 2 MiB per core that mine and it is also expected that CPU cache size is a very significant factor along with CPU speed.
The performance impact of mining is expected to be significant, both subjectively perceived and objectively measured, however the perceived impact will likely be much more obvious on the lower powered computers than the more powerful ones.

4.2 Data

To test the hypothesis data must be collected. The data gathered will be impacted by several factors. The main factors that contribute are

- Hardware
  The hardware used to mine defines the physical capabilities of the mining rig. Changing hardware will change the hashrate of the miners significantly. Due to it's importance all hardware used in this experiment are heavily documented.

- Software
  The mining software is also of great importance. Different software might yield different results depending on implementation. The hashrate is also taken from the mining software so it has to produce reliable data. To minimize the variance the same mining software, XMR-stak are used on all machines that mined nativly except for the Raspberry Pi, XMR-stak is not compatible with it's ARM processor.

- Web browser
  The web browser used to web mine, much like the native mining software might influence the hash rate. To minimize the variance the the same web browser, Chromium, are used on all systems to web mine.
- Operating System
  The underlying Operating System might have some impact on the mining performance. This experiment however did not have the time to prioritize testing several Operating Systems on the same hardware.
- Other processes
  Other processes uses the CPU and other resources, this will in all likelihood impact the mining operations, to minimize the variance as few processes as possible are running when the mining data are collected.

The variables changed when collecting the data were:

- Cores mining
  The amount of cores mining was changed to see what the impact adding or removing a core had on the mining performance.
- Cores tested
  When running the test software different amounts of cores are checked, this is because it is interesting to look at the single core and multicore performance of the machines used.
- GPU
  It is interesting to look at how mining with a GPU differs from mining with a CPU, unfortunately, only one of the machines in this experiment had a dedicated GPU.
- The websites used to web mine.
  Different web sites could implement web mining different and that could impact the hashrate, since it is fairly quick to test multiple sites, multiple sites are used to measure hashrate.

4.2.1 Measurements

The collected measurements are:

Performance impact measured:
To measure the impact of cryptomining it was measured how many system events that can get run in a certain amount of time and also measures the time the CPU uses from the request is send until the event is completed. This measurement allows for a measurable comparison of how much the CPU is slowed down when mining.

Performance impact perceived:
Perceived performance degradation is by definition subjective so in order to measure

it a 4 point schema was created ranging from zero to three, zero means no perceived impact, one means some perceived impact, two means significant perceived impact and three means that the perceived impact is so large that the computer becomes practically unusable.

Power consumption:
Power consumption is measured by the spot watt usage when running idle and when mining with a different amount of cores. The consumption is measured over a few minutes, this should be enough time to get an estimate to be extrapolated and calculate the average cost of mining Monero.

Mining efficiency:
In order to determine how efficient the machines are at mining Monero the hash rate is used. The hash rate is recorded by the mining software, both the peak and average hash rate is recorded as both are valuable, the peak tells us about what the machine is capable of when the miner have most of the computer's resources for itself, while the average hash rate tells us something about how much is likely to be mined when the computer is used regularly. This test is performed with a varying amount of cores mining, and as thus the overhead of adding more cores and how much the CPU cache memory impacts hash rates can be measured as well.

4.3 Limitations

There are some obvious limitations in this experiment. The main is the relative small sample size with only 6 devices, all running different Operating Systems and hardware configurations, in particular only one of the PCs had a dedicated graphics card.
None of the computers will be running the same Operating System, this is by design to ensure that several Operating System are tested in the given time frame, but it does limit the experiment as the different Operating Systems might affect mining performance differently.
Additionally it is difficult to account for other running processes, to counter this, the base line, called idle, was set before mining was started, and the difference in resources used by the machine between idle and mining was recorded as well.

Chapter 5

Specification

Two laptop computers, two desktop computers, one Raspberry Pi and one smart phone running different OSes and hardware configurations was set up to get some data on how cryptomining impacted them. The computers are described in Implementation. Four of them was set up to mine nativly and five was set up to mine using the web browser.

This experiment was set up to shed light on several aspects of mining Monero. It could show how Monero scales with CPU clock speed and cores used. It also gives a reasonable estimate on how much overhead is created when mining in a browser using JavaScript versus mining nativly on the hardware.

Monero's CryptoNote mining algorithm uses memory blocks of 2MiB at the time, meaning that in theory each CPU or GPU thread running CryptoNote will be most efficient if they can get 2MiB of cached memory for themselves. There are also some overhead to be expected when running multiple threads on the same system, thus the effectiveness of each consecutive thread should be somewhat diminished. Web browsers do have access to the CPU cache, but it is not clear how well they utilizes it when mining compared to native C programs, this experiment should shed some light on that aspect as well. It is also expected that the browser based mining will be less efficient than the native mining due to the overhead produced by running JavaScript in the web browser as opposed to running native C code directly in the OS.

Another thing to note is that most of the systems tested, and indeed most modern system offers CPUs with multiple modes, so called turbo modes, that increases the clock speed if the CPU is running bellow it's thermal design power. Running multiple cores will create more heat, it is therefore reasonable to expect that the CPU will clock down, thus producing less heat if multiple cores are being run.

5.1 Mining Rigs

To get a better idea of how cryptomining works it has been tested on several computers, both as a native installation and running in a web browser. The testing has been conducted both under Linux Ubuntu, Linux Raspbian, Chrome OS, Windows 10, Android and Mac OS. The goal is to better understand how Monero and CryptoNigth performs under different hardware setups, how efficient web mining is in comparison to native mining and how much power is consumed when mining using different configurations. For a full description of the hardware for each computer see Appendix Hardware. A summary follows.

Name	*CPU*	*GPU*	*OS*	*Native mining*	*HW cost*
NUC7i5BNK	i5 @ 2.30GHz	N/A	Ubuntu 18.04	Yes	5000 NOK
Macbook	i5 @ 2.60GHz	Intel Iris 5100	macOS High Sierra	Yes	4000 NOK
Chromebook	Celleron @2.16GHz	N/A	Chrome OS	No	2000 NOK
Tower PC	i7 @ 3.40GHz	Nvida GeForce GTX 760	Windows 10	Yes	4000 NOK
Sony H4113	Cortex-A53 @ 2.2GHz	Qualcomm Adreno 508	Android 8.0	No	2000 NOK
Raspberry pi 2B	Cortex-A7 @ 900MHz	N/A	Raspbian 8 Jessie	Yes	200 NOK

Table 5.1: The devices used in this experiment

Figure 5.1: Devices used to mine. Upper left: Chromebook, lower left: NUC, middle left: Tower, upper middle right: Macbook, lower middle right: Raspberry Pi, right: Phone.

The HW cost column in fig 5.1 is an approximation of the prices adjusted for the devices lifetime. The Tower and Macbook was acquired in 2014, the Rpi was acquired in 2016 and the rest was all acquired in 2018. The HW cost assumes a write off of 20% year over year to reflect the fact that computer hardware loses value over time.

The NUC7i5BNK, henceforth NUC, is a tiny computer running Linux Ubuntu 18.04, it has a two core, four thread, i5 CPU that run at about 2.3 GHz with a turbo mode at 3.4 GHz and have 4MiB CPU cache memory. It was released in Q1 2017 and is relatively low powered. It was chosen as a stand in for average low-to-medium powered computer.

The Macbook is a mid 2014 13” laptop running MacOS High Sierra, it has a dual core, four thread, CPU running at about 2.6 GHz with a turbo mode at 3.1 GHz and have 3 MiB CPU cache memory and no discrete graphics. It was chosen to represent laptops.

The Chrombook is a low powered ASUS laptop running Chrome OS with developer access, it has a 2.16 GHz dual core CPU without hyper threading and 1 MiB of L2 cache. It was chosen as a machine to represent several application machines that does not have true access to the hardware. It was only used to test web based mining.

The tower PC, henceforth Tower, is a custom made desktop PC build in early 2014 with a four core, eight thread, i7 CPU running at 3.40 GHz, with turbo up to 3.90 GHz and 8 MiB of L3 cache, and a discrete Nvidia GTX 760 graphics card making it the most powerful PC in the experiment. It runs Windows 10.

The Sony H4113, henceforth Phone, is an android smart phone with root. It is included to investigate how mining affects a phone compared to a PC. It has only been tested with browser based mining. It has two ARM CPUs, both dual core, four thread, one running at 2.2 GHz and one running at 1.8 GHz.

The Raspberry pi B 2, henceforth Rpi, with a 900 Mz ARM Cortex-A7 CPU with 256 kb of L2 cache was the least powerful device used it this experiment. It is used as a stand in for IoT devices, although it should be noted that it is likely that the Rpi has a more powerful CPU than many IoT-devices. It has only been used to test native mining.

5.2 Native Mining

This section only covers the NUC, Macbook, Tower and Rpi as the Chromebook and Phone did not perform native mining. For the native tests a miner called XMR-stak[65] was used. It runs naively as a Command Line Interface (CLI) program on x86 versions of Linux, Windows and MacOS and runs on both CPU and GPU. It was thus a fine candidate to use for testing the three major OSes. Due to it being a CLI-application it also lend itself very well to automation and being controlled remotely, i.e. over SSH. XMR-stak also provide a small web server that gives one the ability to monitor the mining in a web browser. XMR-stak does not run on ARM devices, and as thus it could not be used on the Rpi, instead another program, cpuminer-multi[66] was used instead.

To get easy access to data a mining pool was used[67]. A mining pool works by connecting many miners together and pool their resources, then when a block is solved every member of the pool get a share of the coinage based on the amount of work they contributed. In this way a mining pool can provide a steady and predictable income as opposed to the random nature of solo mining. For this experiment that also means that the random nature of cryptomining can be somewhat removed, thus providing more reliable data that can be better used to predict the profitability of mining. The pool chosen was supportxmr.com, it provides an easy to use interface and does not require an account, in order to view one's stats all that is required is the wallet address. Supportxmr.com provides a dashboard that shows mining stats for the last 24 hours, the total amount of hashes solved for the wallet address, the total amount of XMR the wallet is due and how much has been payed to the wallet. The total hashes and total due/paid was one of the reasons for choosing supportxmr.com because it allows to extrapolate how many hashes that are required to mine one coin of XMR without actually having to mine a whole coin.

The NUC, Macbook and Tower used for testing had a web browser, either Chrome or Firefox, running it the background, this was intentional as it is unlikely that a compromised system would be powered on, but not having any programs running for extended periods of time. However they only had a few static web pages open and was idling at about 2-6% CPU usage before mining was initiated. The NUC, Macbook and Rpi also had an SSH[68] server running and the native miners was ran within a Tmux[69] for easy remote access. While mining the machines were looked, the screen(s) turned off and left alone for a few hours for each run.

XMR-stak keeps track of the average hashes per second for the last 10 seconds, 60 seconds, 15 minutes and the highest recorded since the program was started, cpuminer-multi prints the current result to the screen every few seconds. The NUC, Macbook and Rpi was accessed via SSH several times during the run time and the current 15 minute average was recorded. The Tower was not accessible remotely and so the hashrates there was recorded locally, that does mean that fewer records was recorded for the Tower and the average there is thus less reliable. Supportxmr.com also gives an average of how much each machine have mined, but this hashrate fluctuates much more than the one provided by xmr-stak and the average hashrate reported by supportxmr.com are larger than the maximum reported by xmr-stak. Why this is has not been investigated, but the hashrate numbers provided by supportxmr.com have been disregarded in favor of those provided by xmr-stak.

XMR-stak allows the user to specify how many threads one want to be mining and if one want to use a GPU if applicable. The CPU threads are specified in a file called cpu.txt, and the GPU is specified in a file called nvidia.txt or amd.txt depending on the brand of GPU used. [See appendix y for examples of the configuration files.] For this experiment the configuration files were created on each system by the xmr-stak client upon first run, pools.txt, config.txt, amd.txt and nvidia.txt was never touched while cpu.txt was only changed to use a different amount of cores/threads on each consecutive run. For the Tower, it was ran with the –noCPU and –noNVIDIA for testing only GPU mining and only CPU mining respectively. The Rpi was only ran with cpuminer-multi's default configuration running all four cores.

5.3 Webminer

To test the effectiveness of mining in a web browser several websites was used, including coinhive.com[4], coinwebmining.com[70] and minero.cc [71]. Coinwebmining was used to gather most of the hard data as it provided the best interface, but all the web miners gave approximately the same results for the same setup. All machines was tested using Google Chrome, although Mozilla Firefox had almost identical results when tested. Coinwebmining.com was used to generate the numbers used it the results for the NUC, Macbook and Tower. This is because it conveniently displays the max hashrate unlike the other alternatives, one drawback of this is that it only gives the hashrate as a whole number, while minero.cc and coinhive.com gives the hashrate with one decimal, but for these machines hashrate is large enough that the decimal is insignificant and it changed too fast to record properly. On the Chromebook and Phone however the hashrate was only in the single digits and did not fluctuate nearly as much, so here coinhive.com was used to determine the rates.

To get the averages every machine ran either coinwebminig.com or coinhive.com for 5 minutes (300 seconds) for each configuration of cores, i.e., 5 minutes mining with 1 core, then 5 minutes using 2 cores and so on, they always mined at 100%. The average hashrate was then calculated and recorded, this time is somewhat short, but the hashrate was very steady when using the webminers so it was deemed unnecessary to prolong the experiment.

5.4 Power consumption and benchmarks

Part of the experiment was finding how power consumption and how the user experience is affected by the mining process. In order to test for the power consumption several different techniques had to be employed. For the machines that connect directly to a power outlet, that is the NUC, Tower and Rpi, a simple hardware power recorder was placed between the machine and the power outlet and the consumption was read directly. For the other devices this did not work due to them having a battery and thus they gave very inaccurate readings and software that read the battery and calculates the power consummation was used. For the Chromebook a build-in utility was used, it can be accessed by typing chrome://power into the URL-bar in the Chrombooks browser. For the Macbook a third party utility called iStats Menu[72]. For the phone it was more difficult and to get a reading, Android Studio and Battery Historian[73] was used. The power usage was recorded for all devices for all mining configurations, including idling.

To test the user experience two different approaches was used, one objective and one subjective. The objective method was to run sysbench[74] on the supported systems. Sysbench was chosen because it is open source, free, lightweight, can be customized and can be made to run on all but one of the tested platforms. It runs natively on Ubuntu, MacOS and Raspbian, on Windows it can be run in the Linux subsystem for Windows[75] and on the Chromebook it can be made to run natively when in developer mode. On Android no comparable benchmarking tool to sysbench was found and thus no benchmark data have been collected for the phone. Due to time constraints only about one forth of the possible configurations were benchmarked. The benchmarks collected when having coinhive.com running in the browser on all platforms.

For the subjective testing a scale of annoyance was used. It ranges from 0 - not annoyed at all to 4 - the machine is practically unusable. The machines were tested doing some common tasks such as surfing the web, reading the news, streaming HD-video on sites such as YouTube and HBO Nordic, some office work with Libre Office and playing games, the games tested were Sid Meier's Civilization V and Blizzard's Warcraft 3, Blizzard's Heartstone, Wizards of the Cost's Magic the Gathering Arena and Bandai Namco's Dragonball Xenoverse 2.

Chapter 6

Mining results

6.1 Power consumption and hashes comparison

Here follows a comparison made to see the power draw versus hash rate using different computers, varying the amounts of threads used to mine and native versus browser based mining. On the laptops and the phone battery drain is also measured.

To get an accurate number each rig ran for at least 1 hour at each configuration with native mining and for at least 10 minutes with the web-app, although most configurations was ran for longer. The web-apps gave a real time update and had far less variance than the native mining.

Explanation of the table:

Machine is the machine mining, here NUC in the NUC7i5BNK, Mac is the Macbook pro 13" 2014, Chrome is the Asus Chromebook, Rpi is the Raspberry Pi 2B, Phone is the Sony H4113 and Tower is the custom build desktop PC.

H/s (highest) is the highest recorded hashes per second in XMR-stak and coinhive.com while H/s (avg. aprx.) is an approximated average value. Both values was recorded in order to get a better perspective, the average value is more telling of the efficiency than the peak, but it is much harder to determine. XMR-stak only keeps record of the last 15 minutes of hashes and the highest amount of hashes per second since it was started. The highest value is thus very easy to record while the average is just an approximation made by taking screenshots every 15-minutes for an extended period of time. It should however also be noted that the machines were usually being used for other tasks some of the time they were mining and this will in all likelihood have impacted the results somewhat. The highest hashes per second might therefore be a more reliable number to use for strictly comparing one setup to another. Especially on the laptop it was difficult to get a good reading as they seem to throttle the mining to reduce power consumption when the screen is on.

Power drain is measured in different ways on the different devices, for the two desktop computers (NUC and Tower) a simple hardware power recorder was put between the computer's electrical cord and the power outlet in the wall. For the Mac a software program called iStats Menus [72] was used. On the Chromebook the build in tool chrome://power was used and for the phone an app called AccuBattery Pro was used, the app shows the current power usage an the screen, but in mAh, not in Watts. Due to this the phone's power consumption cannot be compared directly to the other devices. The consumption numbers for the phone fluctuated a lot so an approximated average was used.

Type of mining denotes what kind of mining was performed, Native mining is mining with XMR-stak, native + GPU denotes that the GPU was used in tandem with the CPU in XMR-stak. Web is mining using a web browser and mining through Coinhive.com and Minero.cc.

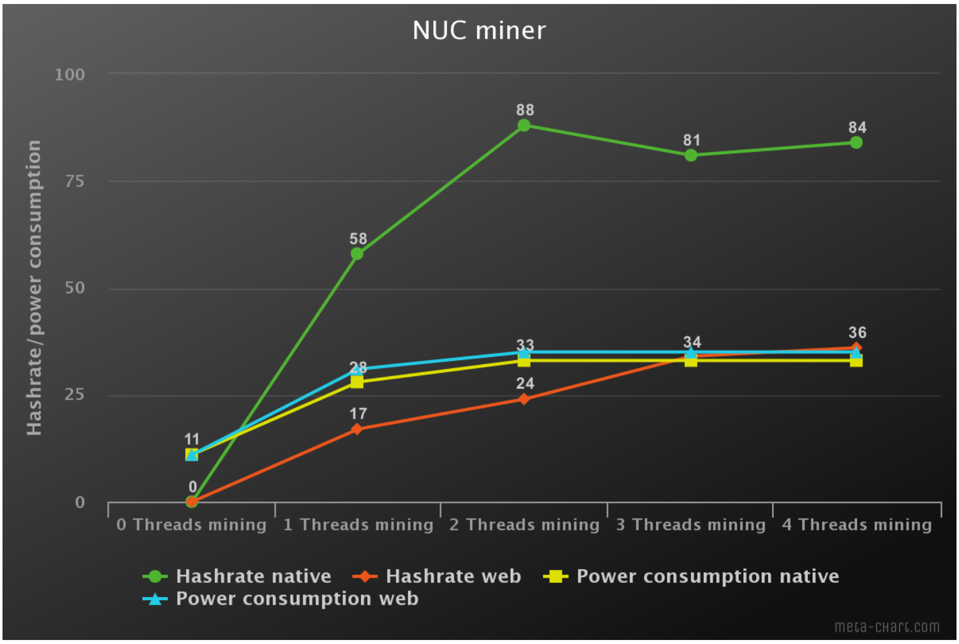


Figure 6.1: Hashrate and power consumption of the NUC

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain (avg)*	*Type of mining*
NUC	0	0	0	10-12 W	None
NUC	1	58.1	50.0	23-34 W	Native
NUC	2	87.7	81.0	29-36 W	Native
NUC	3	81.4	79.0	28-36 W	Native
NUC	4	84.4	81.5	29-34 W	Native
NUC	1	17.0	15.0	25-37 W	Web
NUC	2	24.0	22.3	34-37 W	Web
NUC	3	34.0	28.9	34-37 W	Web
NUC	4	36.0	31.3	34-37 W	Web

Table 6.1: Hashrate and power consumption of the NUC

The NUC have 4 MiB of L3 cache and fig 6.1 shows that when mining natively it peaks at 2 cores as expected, and decreases somewhat when adding more cores, while when web mining adding more cores seems to work well to increase the hashrate, although the 4th core does not add much. The power consumption is very similar between native and web mining, at about three times the power consumption when idling, interestingly adding more cores to mine does not increase the power consumption by a whole lot.

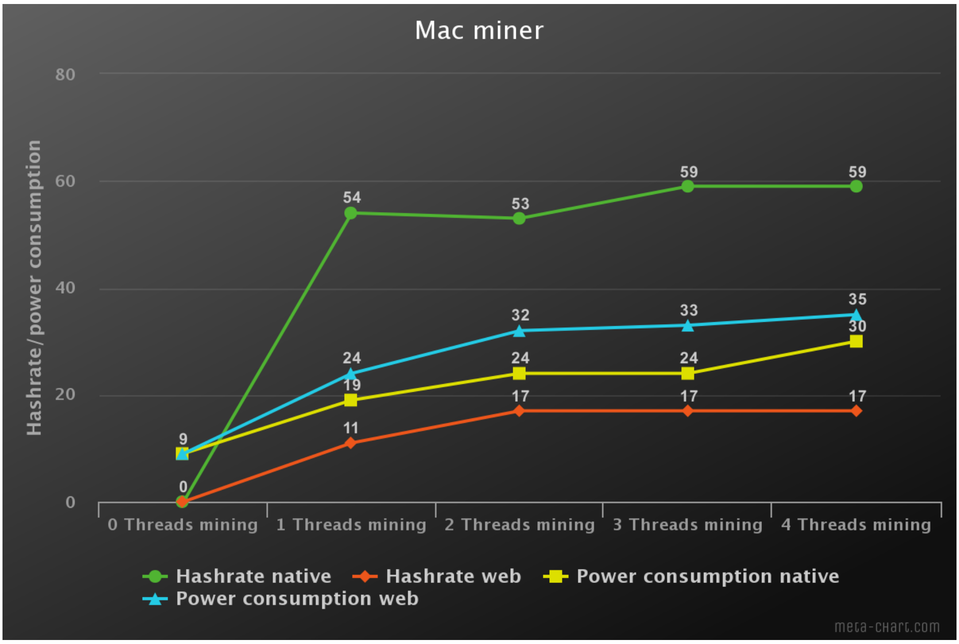


Figure 6.2: Hashrate and power consumption of the Mac

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain (avg)*	*Type of mining*
Mac	0	0	0	6-12 W	None
Mac	1	53.9	44.0	18-21 W	Native
Mac	2	52.6	44.5	23-25 W	Native
Mac	3	58.7	49.0	23-26 W	Native
Mac	4	58.6	50.0	28-31 W	Native
Mac	1	11.0	10.0	22-26 W	Web
Mac	2	17.1	15.0	31-33 W	Web
Mac	3	17.1	15.5	33-34 W	Web
Mac	4	17.1	16.0	33-36 W	Web

Table 6.2: Hashrate and power consumption of the Mac

The Mac have 3 MiB of L3 cache and the stats can be seen in fig 6.2. While it does not peek at 1 core when mining natively, adding a second core does not affect the hashrate beyond the margin of error and adding the third core adds less than a 10% increase and the fourth core does not add anything at all. When web mining it flattens at two cores and the third and fourth cores does add a tiny amount to the average amount mined, but the maximum is completely flat. The power consumption increases similarly to the NUC, but notably the native miners draws significantly less energy than the web miner.

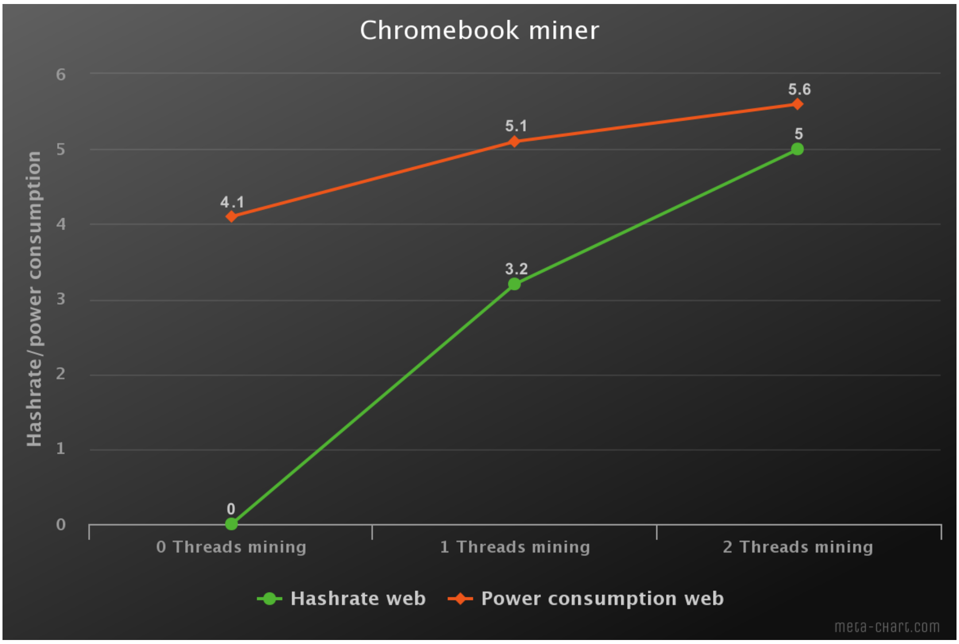


Figure 6.3: Hashrate and power consumption of the Chromebook

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain (avg)*	*Type of mining*
Chrome	0	0	0	3.7-4.5 W	None
Chrome	1	3.2	3.0	4.7-5.5 W	Web
Chrome	2	5.0	4.0	5.3-5.9 W	Web

Table 6.3: Hashrate and power consumption of the Chromebook

The Chromebook only have 1 MiB of L3 cache and with only two cores it does not mine very efficently, but the power consumption is also quite low as can be seen in fig 6.3

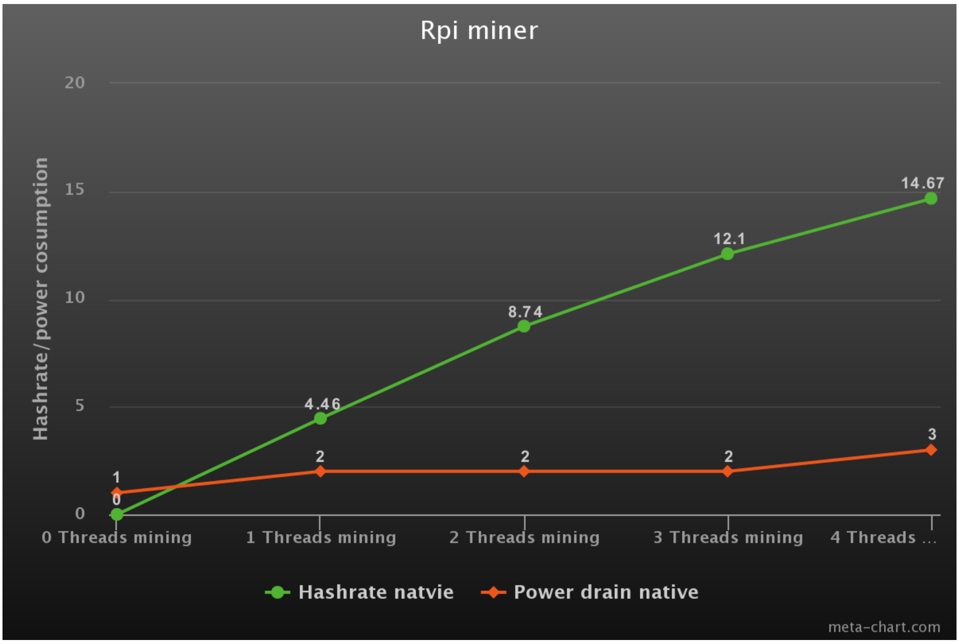


Figure 6.4: Hashrate and power consumption of the Raspberry Pi

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain* (avg)	*Type of mining*
Rpi	0	0	0	1 W	Native
Rpi	1	4.64	4.63	2 W	Native
Rpi	2	8.74	8.64	2 W	Native
Rpi	3	12.1	11.69	2 W	Native
Rpi	4	14.67	14.17	3 W	Native

Table 6.4: Hashrate and power consumption of the Raspberry Pi

The Raspberry pi does only have 256 kiB of cache memory so it scales almost linearly when adding cores for mining. The power consumption is very low even when maxing out the CPU for mining.

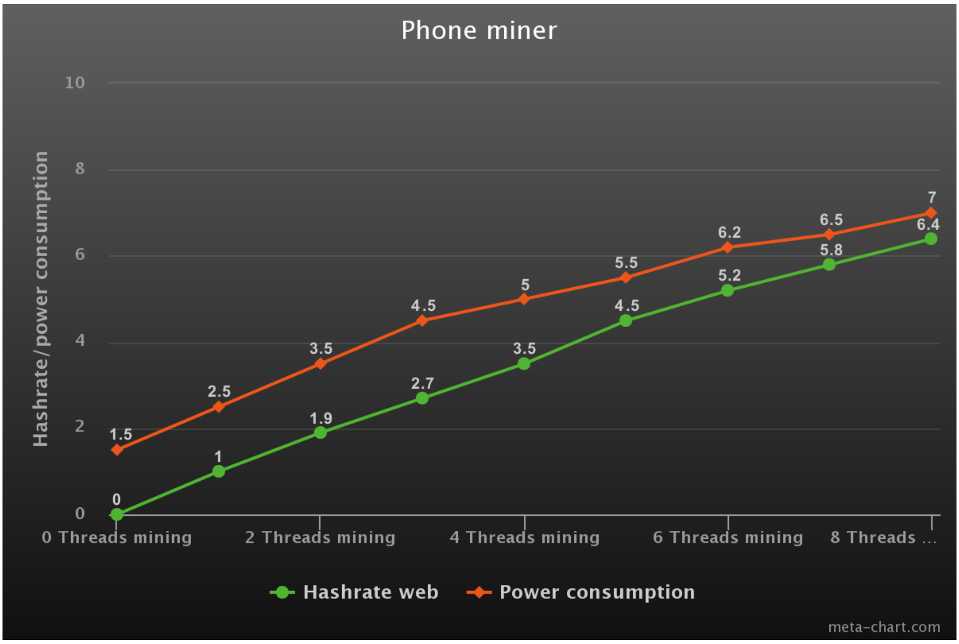


Figure 6.5: Hashrate and power consumption of the phone

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain (avg)*	*Type of mining*
Phone	0	0	0	150 mA	None
Phone	1	1	0.92	250 mA	Web
Phone	2	1.9	1.83	350 mA	Web
Phone	3	2.7	2.68	450 mA	Web
Phone	4	3.5	3.48	500 mA	Web
Phone	5	4.5	4.19	550 mA	Web
Phone	6	5.2	5.03	620 mA	Web
Phone	7	5.8	5.76	650 mA	Web
Phone	8	6.4	6.31	700 mA	Web

Table 6.5: Hashrate and power consumption of the phone

As can be seen in fig 6.5 the phone scales almost perfectly linearly, both in regard to hashrate and power consumption. Due to some technical difficulties the Phone's power consumption was measured in mA rather Watts. To get numbers that can be compared with the other devices more directly one can assume a voltage of 3.7 V for the battery and using Watt = Volt x Ampere.

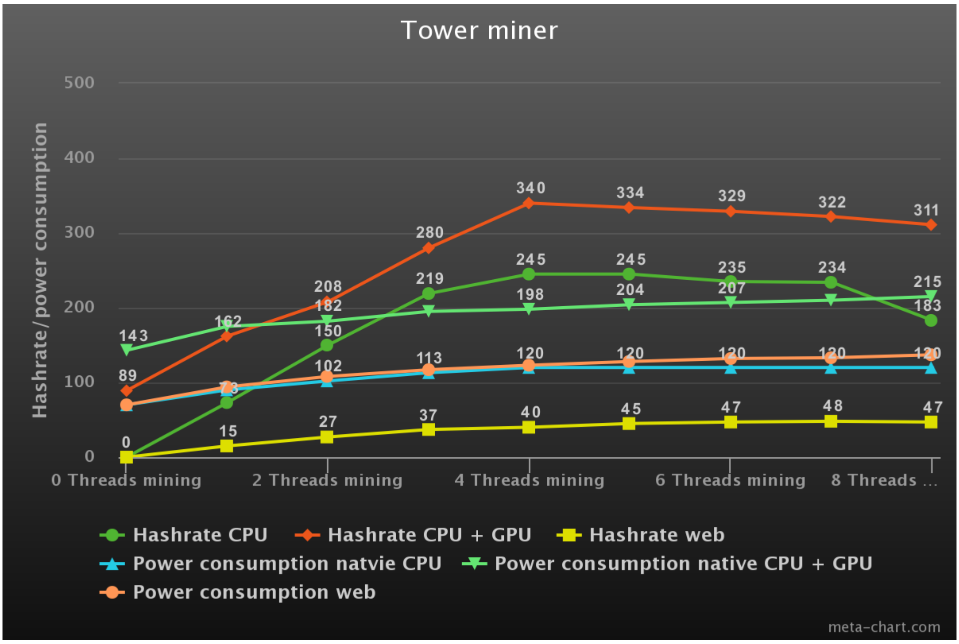


Figure 6.6: Hashrate and power consumption of the Tower

Machine	*Threads mining*	*H/s (highest)*	*H/s (avg. aprx.)*	*Power drain (avg)*	*Type of mining*
Tower	0	0	0	68-72 W	None
Tower	1	72.7	70.5	89-92 W	Native
Tower	2	150.4	148.5	102-103 W	Native
Tower	3	218.7	215.5	110-116 W	Native
Tower	4	244.7	232.5	118-123 W	Native
Tower	5	244.6	230.5	119-122 W	Native
Tower	6	234.6	217.5	119-122 W	Native
Tower	7	233.9	220.5	119-122 W	Native
Tower	8	182.9	170.0	119-122 W	Native
Tower	0	89.2	89.2	142-145 W	Just GPU
Tower	1	161.7	155.5	170-180 W	Native + GPU
Tower	2	208.2	205.5	175-190 W	Native + GPU
Tower	3	279.8	270.0	185-205 W	Native + GPU
Tower	4	340.2	330.0	188-209 W	Native + GPU
Tower	5	334.0	300.0	196-212 W	Native + GPU
Tower	6	329.2	310.0	197-218 W	Native + GPU
Tower	7	322.1	300.0	202-218 W	Native + GPU
Tower	8	311.0	290.0	204-226 W	Native + GPU
Tower	1	14.6	14.0	92-96 W	Web
Tower	2	27.4	26.5	106-110 W	Web
Tower	3	36.9	35.0	110-123 W	Web
Tower	4	40.3	39.0	118-128 W	Web
Tower	5	44.5	44.5	123-133 W	Web
Tower	6	46.5	43.5	129-136 W	Web
Tower	7	48.2	47.0	129-137 W	Web
Tower	8	47.2	46.5	135-139 W	Web

Table 6.6: Hashrate and power consumption of the Tower

As can be seen in fig 6.6 the Tower gives the most amount of data out of the different devices, this is due to it having more cores and a dedicated GPU that can be used for mining. The first thing to notice is that the power drain when mining is almost the exact same whether mining native or web, but when using the GPU the power consumption goes up significantly. The next thing to notice is that the hashrate peaks four cores when native mining, GPU or no GPU, and when adding more cores the hashrate drops noticeably, especially adding the eight core reduces the hashrate by a large margin. This is not true for web mining, there the rate goes up and even adding the eight core does not impact the hashrate hardly at all.

6.2 Benchmarks

To get data on the impact cryptomining has on computer performance sysbench was used both while the machines was idling and while mining.

```
sysbench --test=cpu --max-requests=200000 --max-time=10 --num-threads=1 run
```

Sysbench works by running a large amount of math problems by the CPU to test how many events it can process in a given time. The results vary depending on the time, requests and threads running. Since the numbers are only interesting in relation to each other the max-request and max-time parameters were constant at 200000 and 10 respectively while the number of threads varied tested. Since both the amount of threads tested and the number of threads mining were varying only singel core, dual core, quad core, and in the case of the tower hexa core and and octa core performance was tested to save time. In addition, only the three most powerful machines were tested. It was difficult to find free, easy to use and configure performance software that works cross platform and secondly to save time as this process is quite time consuming. However, the results from this test is quite conclusive and are likely transferable to other devices.

Machine	*Threads mining*	*Threads tested*	*Avg latency (ms)*	*Events*
NUC	0	1	0.83	11978
NUC	2	1	1.20	8320
NUC	4	1	1.53	6546
NUC	0	2	0.86	23182
NUC	2	2	1.34	14859
NUC	4	2	1.88	10603
NUC	0	4	1.13	35433
NUC	2	4	2.51	15917
NUC	4	4	2.43	16449
Machine	*Threads mining*	*Threads tested*	*Avg latency (ms)*	*Events*
Mac	0	1	1.32	7580
Mac	2	1	1.95	5105
Mac	4	1	2.04	4893
Mac	0	2	1.37	14594
Mac	2	2	1.77	11274
Mac	4	2	2.60	7667
Mac	0	4	1.78	22371
Mac	2	4	2.77	14412
Mac	4	4	3.41	11703
Machine	*Threads mining*	*Threads tested*	*Avg latency (ms)*	*Events*
Tower	0	1	0.86	11596
Tower	2	1	0.90	11022
Tower	4	1	1.07	9346
Tower	6	1	1.06	9382
Tower	8	1	1.60	6227
Tower	0	2	0.86	23167
Tower	2	2	0.94	21224
Tower	4	2	1.06	18827
Tower	6	2	1.10	18091
Tower	8	2	1.53	13037
Tower	0	4	0.90	44506
Tower	2	4	0.97	41275
Tower	4	4	1.20	36785
Tower	6	4	1.29	30912
Tower	8	4	1.81	22017
Tower	0	6	1.05	63137
Tower	2	6	1.01	59277
Tower	4	6	1.22	51104
Tower	6	6	1.59	37519
Tower	8	6	2.47	24202
Tower	0	8	1.16	79603
Tower	2	8	1.12	71052
Tower	4	8	1.27	60050
Tower	6	8	1.82	43794
Tower	8	8	2.54	31394

Table 6.7: Sysbench results.

Figures 6.7, 6.8 and 6.9 show that when mining at full speed the performance of all three machines drop to about half and the latency increases dramatically. It is worth noting that testbench uses as much resources as possible, much like the crypto miners. When using less demanding software the performance and latency impact might not be as severe.

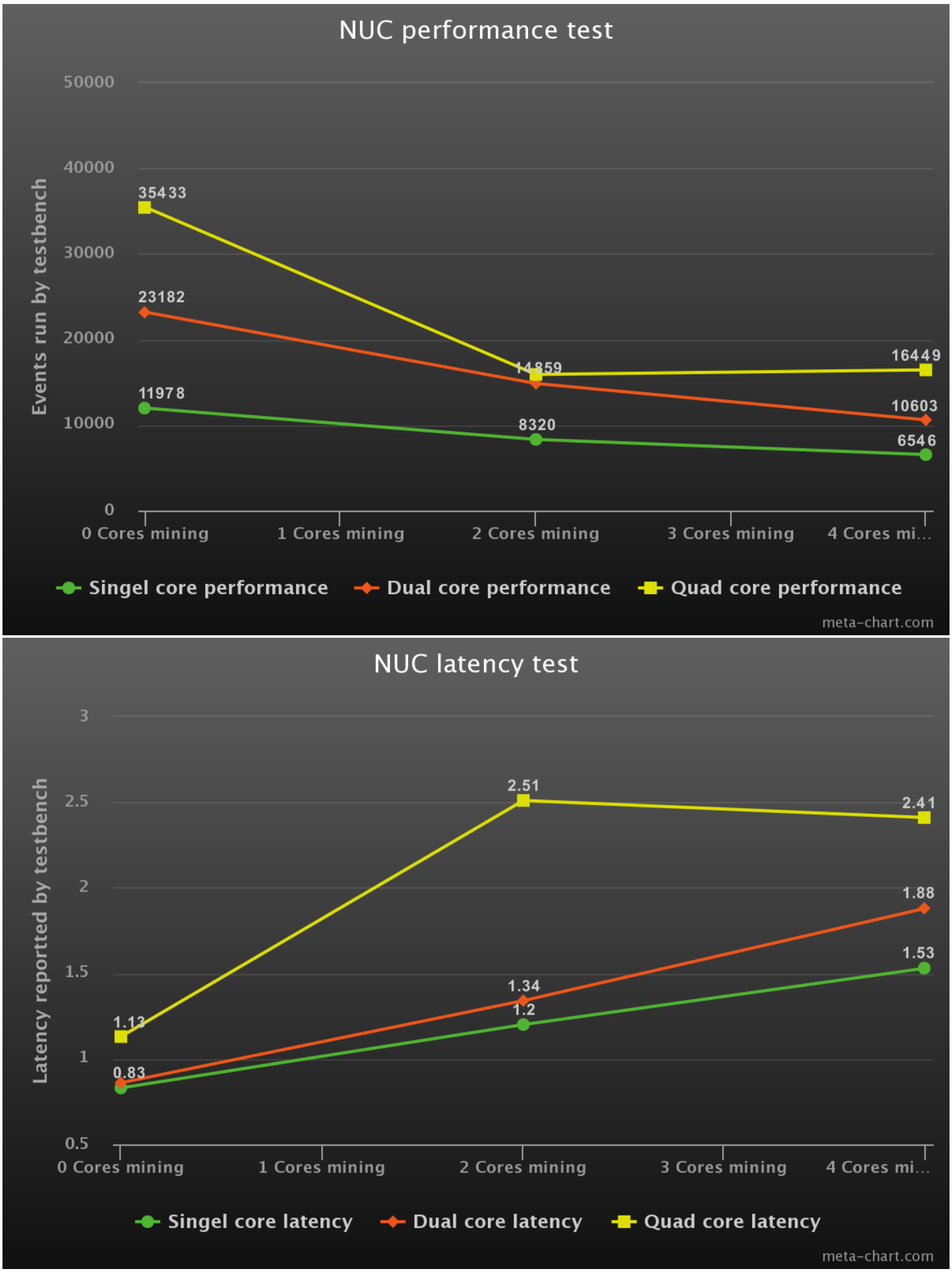


Figure 6.7: Performance and latency tests for the NUC while mining

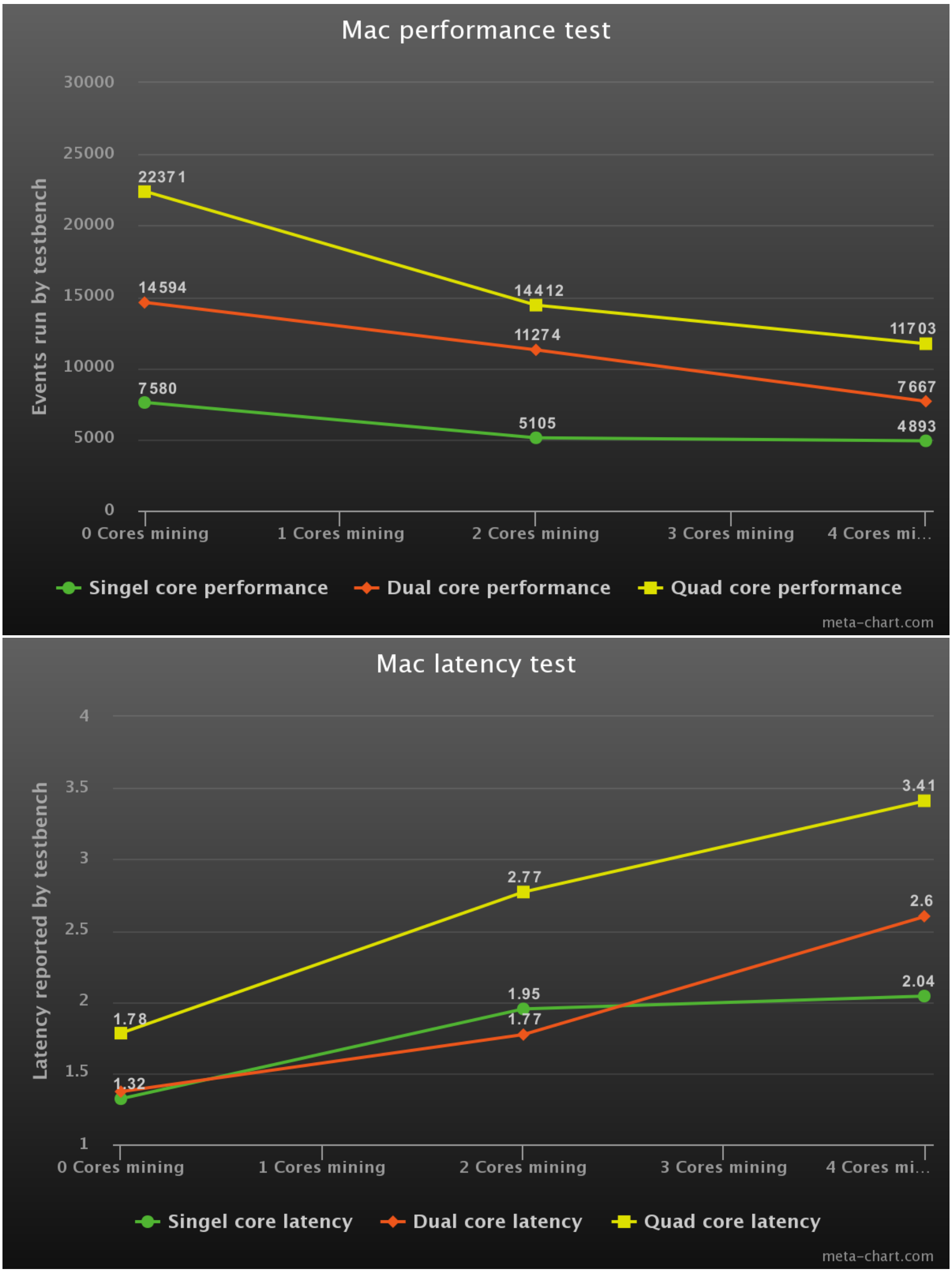


Figure 6.8: Performance and latency tests for the Macbook while mining

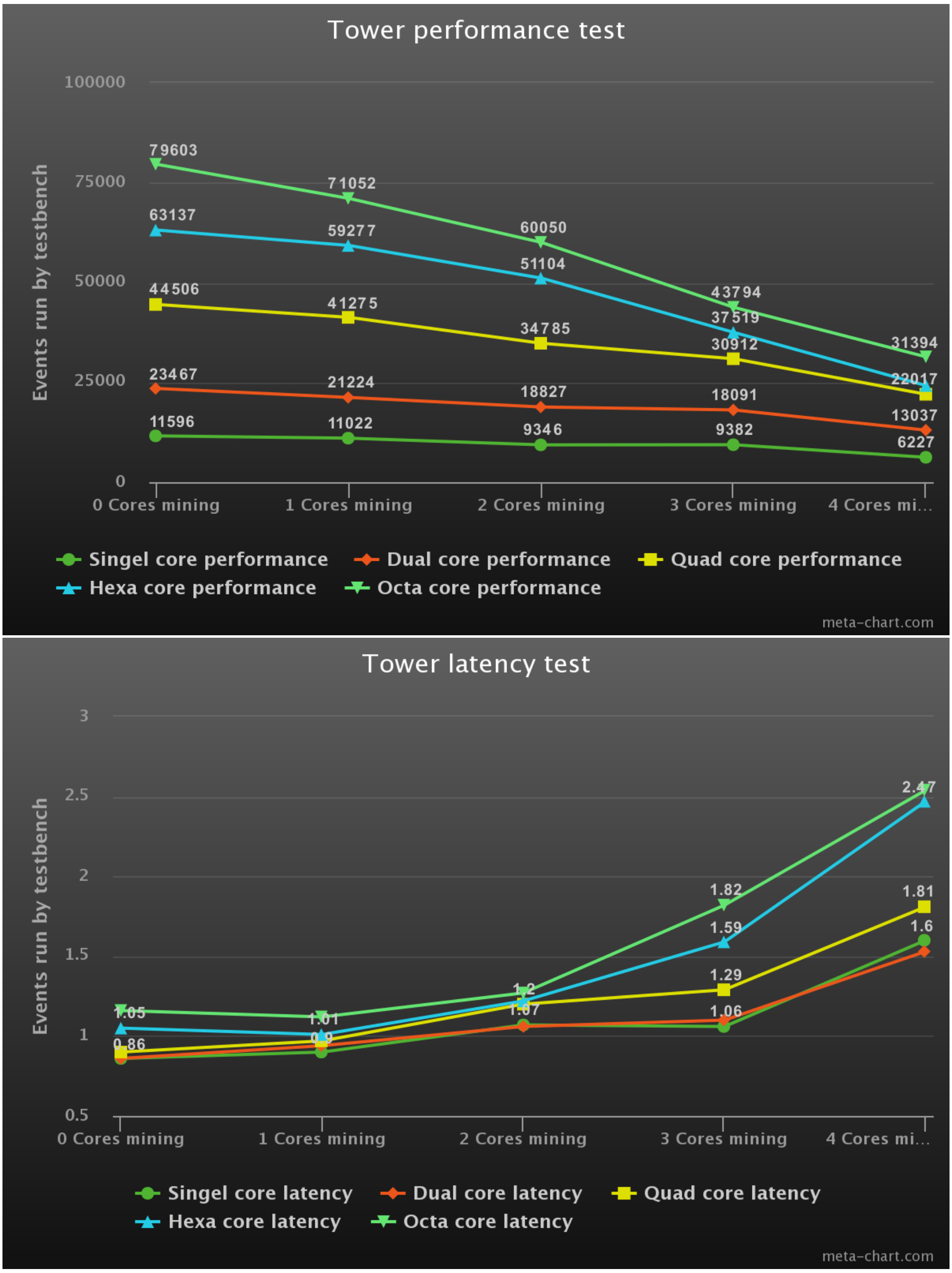


Figure 6.9: Performance and latency tests for the Tower while mining

6.3 Subjective experiences

While benchmarks are very useful for getting an objective view on the power consumption and CPU consumption they does not necessarily tell the whole story. If the user is not very bothered by cryptominers using their CPUs they are less likely to do anything about it, it might even not be considered a problem. This section covers what are mostly subjective experiences when using a computer that mines Monero at high rates. Since all the computers have different hardware the tests have been tailored to test the performance of the devices while mining when used in a way deemed appropriately for the given device.
Table 6.8 gives an overview over the devices, the Phone have been omitted from the table since no true multitasking could be done on it while mining.
The scores are all given by the author, who also owns the devices, the results are thus highly subjective and not very reliable, but it still gives an indication of how mining might impact the perceived performance of cryptojacked systems.

Machine	*CPU Cores mining*	*Annoyance level*
Tower	<5	0
Tower	5,6	1
Tower	7	2
Tower	8	3
Tower GPU	0	4
Macbook	<3	0
Macbook	3	1
Macbook	4	3
NUC	<3	0
NUC	3	1
NUC	4	3
Chromebook	0	1
Chromebook	1	2
Chromebook	2	2
Rpi	0	2
Rpi	1,2	3
Rpi	3,4	4

Table 6.8: Annoyance level when mining, 0 means no annoyance, 4 is virtually unusable.

6.3.1 Tower, Mac and NUC

The Tower's performance was tested while mining both using xmr-stak natively and while mining using coinwebmining.com in Google Chrome. The Tower was tested while performing several different tasks including steaming HD video from Youtube and NRK, doing web browsing, opening and editing some documents in Libre Office and playing some games, including Warcraft 3 (real-time Strategy), MTG Arena (turn based card game), Hearthstone (turn based card game), Dragonball Xenoverse 2 (real-time fighting game) and Sid Meier's Civilization 5 (turn-based strategy). The games were played one at the time, but all other tasks were tested both one at the time and in combination with other tasks, for example HD-video were streamed while playing a game. When mining using the GPU in XMR-stak, even when using no CPU cores to mine, the graphical I/O were severely impacted, to the point of making the whole computer unusable for anything else. However, when running as many as 7 out of 8 CPU threads the impact was negligible when simultaneously streaming HD-video and playing games. When running all 8 threads the impact was noticeable, but the computer was still fully usable. Even so, the increased latency was only significantly noticeable when performing context switches, such as loading new maps in a game, starting a new video on Youtube, open new documents for editing and switching between different websites rapidly. When staying within a single application, document or map for a long time the perceived performance hit was much less noticeable.

The NUC and Macbook was tested in much the same way, but with fewer games, for the NUC only Sid Meier's Civilization V was tested and on the Macbook only Sid Meier's Civilization V and Heartstone was tested. The results were similar, both computers were slower than the Tower even with no mining, but the reduced performance was only really noticeable when using all cores for mining, and even so both computers could be used for the tasks. Latency in load times and context switching was even more noticeable on these devices.

6.3.2 Phone and Chromebook

These less powerful machines were just tested with web mining. The phone does not support multitasking in the same way as the other machines does, only allowing a maximum of two application to be running active on the screen at the time, and a web browser running the web miner must be open and active in order for the miner to perform any work. Most resource intensive applications however does not work in split screen mode and thus could not be running at the same time as the web miner. In trying to emulate some real multitasking on the phone Chrome was running in split screen with different games and Youtube streaming. When possible Spotify was running in the background playing music. Even so there was no perceived performance impact on the phone at all. Ideally a site with web mining that also had more than just text and a few embedded videos should have been tested, but none were found.

For the Chormebook, it does allow more true multitasking and thus it is possible to get a more true sense of real multitasking. A web miner was set up running at 100% using both cores. To test the perceived performance impact full HD Youtube videos was played and documents in Overleaf and Google Docs. While the Chromebook is slow in comparison to the other machines tested from the start there did not seem to be any added performance impact from the web miner.

6.3.3 Raspberry Pi

The Pi was not tested doing much other than running a web browser in the GUI, it was very slow even with no mining and the mining made it virtually unusable.

6.4 Limitations

When mining in web browser only Google's Chrome browser was tested, this was due to it's availability on all platforms tested and it's general popularity, it is not known how other web browsers might have affected the mining results.
The software used to mine, both XMR-stak natively and the websites using the coinhive.js JavaScript. The software reports the hash rates themselves, and lacking the sufficient time and expertise to investigate the source code those numbers have been trusted on face value. Other implementations of the cryptominers might yield different results.
All of the subjective experiences are drawn from someone very familiar with the hardware and that are aware of how the machines are set up to mine, this might cause some bias.

Chapter 7

Cost analysis

7.1 Cost to victim

Mining cryptocurrency is a CPU intensive venture, many cryptominers will make an effort not to visibly effect the performance of the other programs running on the system, however they will also make an effort to make the system run at high speed in order to maximize the cryptocurrency mined. Most modern CPUs have the ability to clock down when they are idle, this can significantly reduce the power usage. Cryptominers will keep the CPUs running at high speed at all time thus expending significantly more energy than usual.

Most miners try not to interfere with the host computers other activities too much, but not every miner does. Some miners will try to get as much CPU time as possible, even at the risk of discovery, this may render the CPU too busy to perform it's other tasks efficiently and could lead to prolonged load times and system downtime. For example, in the health care industry most machines are low powered compared to even consumer hardware in terms of processor power, and a cryptojacker might be enough to cause malfunction[76].

Then there's the cost of the electricity needed to compute the hashes.
This cost can be estimated by using the electricity needed to mine a single coin. The cost will vary as more people are mining, as of September 2018 the hashrate is at around 600 Mh/s and the amount paid per block is about 3.88 XMR. The Monero network is set to reward about 720 blocks every day. Note that this work was done before the most hard fork at March 9 2019 and the calculations were made in September 2018. This is also only an example, the cost will vary depending on the hardware used, the price of electricity among other things.
After running 223,680,786 hashes about 0.0125 XMR had been generated by mining for the mining pool supportxmr.com, a mining pool was used because it allows for easily to observe progress without having to actually mine an entire XMR coin and it gives

average numbers over a sample size of several thousands of miners.
Thus we can extrapolate and multiply by 80, that give's us 1 XMR = 17,894,462,880, or about 18 billion, hashes, on normal form 1.8×10^{10}.
This system runs at about 30 watts under load and averages 90 hashes per second over a long period of time.
The average price for electricity in Norway is about 1.1 NOK (0.10 EUR) per kWh.
To normalize the numbers: 1 watt of electricity gives about 3 hashes/second, 1.8×10^{10} hashes/second require 6×10^6 kilowatts of power.
6×10^6 kW / 3600 seconds = 1667 kWh for one coin of Monero. In monetary terms, the electricity to mine a single coin of Monero on a non-optimized system will cost about 1800 NOK or about 180 EUR, as of November 2018 the exchange rate is 1 XMR = 97 EUR. However, the system draws about 10 watts when idling, which means the added cost is in the 20 extra watts being used to mine, thus the price to mine one XMR is in reality 120 EUR in electricity, this is still a loss for the miner if the miner were to mine on their own hardware.
There are about 720 hours in a month, spending an additional 20 Watts for entire month is thus an extra expenditure of 1.440 kWh or about 1.5 NOK per month for a low powered system, using a much more potent system of say 500 W we get 360 kWh, or about 400 NOK. For low powered systems the extra cost is negligible, but for powerful machines the cost is quite significant.
This is all excluding the cost of worn out components. When constantly mining the computer's components will wear out faster. This cost is next to impossible to calculate and will vary a lot from device to device, but it is a very real cost.

7.1.1 Cost to business

Businesses have other concerns than end users. For one thing they tend to have many more machines that are interconnected. Should some computers be infected it can be spread through the network. Having unauthorized software running is always a risk for a business, but cryptojacking might not have the same impact as other malware. If the cryptojacker are configured to not be too intrusive the CPU cycles it steals might not impact the productivity, although a cryptojacker might also cripple computer it infects causing loss of productivity and increased demand on IT staff. Having IT removing cryptojackers from the company computers can be a costly affair and as with most other malware should be stopped by properly configured security. Luckily cryptojackers does not require any special means of protection as discussed in Chapter 3.

Another concern to businesses are web based miners, if it get's known that a company hosts cryptojackers on their websites it could cause a major impact to their reputation. If they are hacked and a script is inserted their security could be brought to question and if they are inserting it on purpose without telling their users their credibility could be severely damaged. One example of damaged reputation is The Pirate Bay, a web site known for hosting torrents for pirated software. The site tested a cryptominer in September 2017, it was configured to use between 60% and 80% of the visitor's CPU, the experiment was lasted only for 24 hours, having upset many of it's users[77]. The Pirate Bay decided to implement a new cryptominer in July 2018, but this time the miner was throttled, unlike the first try i 2017[78].

7.1.2 Cost to society

The societal impact of this cryptomining is not insignificant either. The excess energy used to mine cryptocurrency impacts both the environment and the local power companies as the increased power consumption inevitably will cause an increase in the price of electricity. If computers get worn out faster by the strain put on them by mining they will be replaced, this have a negative impact on the environment as well as the users that have to pay for new hardware. The combined loss of productivity and downtime caused by slowed down computers could be huge if a large portion of the population is spending resources mining cryptocurrency. Another factor to consider on a societal scale is that cryptojacking is a way to make money for criminals and even if most consumers are only slightly impacted this money could be used to fund other criminal activity such as terrorism and money laundering[79].

7.2 Cost to attacker

There are also costs to performing the attacks, this section cover some of the costs. It is extremely difficult to estimate the actual cost of developing and distributing malware as there are several factors that cannot accurately be accounted for, if at all. This section will try to summarize some of the costs related to cryptojacking, but will not be conclusive.

7.2.1 Cost of development

The developers are the one making the software. The are many different components to the cryptojackers. Among these are the cryptomining software, the delivery platforms and the infection vectors and the packaging of all these factors into a single product.
The cryptomining software exists regardless of cryptojackers, after all cryptomining itself is perfectly legal in most jurisdictions, thus the job of the developers of cryptojacking is to weaponize it. This includes making it run stealthily and undetected by the user, perhaps include an auto update facility. To get a sense of what it would cost to develop the software one can assume that one line of code costs $15 USD. DeepMiner's source code is freely available and thus it constitutes a good example[60]. It consists of about 1000 lines of code excluding the cryptography, the cryptography adds about 5000 additional lines, most of which are public domain. That means deepMiner would have cost about $15.000 USD to develop after the cryptography was done. The cryptography itself costs five times as much at about $75.000 USD.

The delivery platforms are the ways the cryptojacking software is delivered. For web miners this includes the websites such as cryptoloot.com and the scripts that are to be injected into the sites. For native running cryptojacking software it will also often include malicious websites or modify well known software to mine cryptocurrency in addition to it's other functions or make entirely now versions of software that trick unsuspecting users into installing a cryptominer.

Infection vectors are the way the software get installed. This is usually software exploits that can be used to get into the victims computers. These exploits tend to be generally very useful for all kinds of infectious malware, not just cryptojacking and ca be bought on the dark web.

Cost of maintenance

Once created the malware must be maintained and updated just as any other software. Most software get updated and changed over the course of it's lifetime, but for malware this process is even more important than for legitimate software. Malware usually takes advantage of some flaw or oversight in legitimate software to get itself into the computer it infects and most modern software are updated regularly to patch these vulnerabilities. Even if malware get installed by the user just the same as a legitimate program, anti virus programs get updated and the entire underlying Operating system could change in a way to thwart the malicious program.
The web based miners must also be maintained, the web is ever changing, new standards are developed and web browsers are becoming more powerful tools every year.

Cost of acquisition

Instead of creating the software oneself it is possible to buy off the shelf cryptojacking software on the dark web. Buy using the prices from Dream 3.1, 3.2 3.3 these seem to cost only about 150 USD although the prices and exact offering varies from vendor to vendor and product offering to product offering. Buy acquiring software on the dark web there are some additional costs, such as the higher risk of being scammed with little to no recourse and the risk of getting caught by law enforcement.

7.2.2 Cost of distribution

Distribution refers to how, where and to whom the software is spread. This includes getting the miners onto the victims machines, infecting web sites etc.
Often, the people distributing cryptojacking are not the same people that wrote the software. This is the whole business idea behind Coinhive and it's affiliates. In that case some of the cost is to buy the software. There are also the cost of implementing the software and make sure it does not break any of the sites other functionality. For those infecting others with cryptojacking there are the cost associated with getting the victims to install the software, whether that is through social engineering, or by accessing the computers through a software exploit or even by getting physical access to the victim machines. Some of these costs might be better measured in terms of time rather than money spent.

7.2.3 Opportunity cost and risk

The most important cost to develop cryptojacking software, or indeed most software, is the opportunity cost. Opportunity cost refers to the cost of doing one thing rather than another. Every hour, every dollar and every bit of effort put into making malware could be used to do something else. According to CareerExplorer an average programmer in the United States make about $55.000 US a year. If one assumes that malware developers does not have any other income then they need to make at least $55.000 US a year just to make up for lost income.

However, the cost of creating cryptojacking software is in large part mitigated by the fact that the cryptomining software are legitimate and benign, and are created independently by other parties. Binaries are distributed freely and often the official implementation is open source code. The attack vectors are also for the most part developed independent of cryptojackers and can be used for other kinds of attack. Then there is the question of whether or not cryptojacking is the most efficient way of exploiting a computer, server or web site once it has been compromised.

For those implementing cryptojacking on their own web sites the opportunity cost can be to remove ads, or losing the trust of it's users.

Risk is another important factor. Risk can be calculated by this equation

$$risk = probability \times impact$$

Probability is the likelihood of getting caught, given as a number between 0 and 1, and cost is the cost of getting caught, given in an appropriate measurement.

Web based cryptojacking are not illegal and no one has been convicted for cryptojacking alone and it has a low priority among law enforcement[19]. Thus the cost, or impact, of getting caught putting a miner script on a site by it's owner is close to zero in terms of fines or jail time, but it could be considerable in terms of reputations. Infections are illegal and getting caught can lead prison and fines, but for the most part the chance of getting caught are quite low if one make use of proxies, social engineering and untraceable cryptocurrency. Thus the risk of doing cryptojacking is approaching zero, on both fronts.

Chapter 8

Discussion

8.1 Comparing the devices for mining efficiency

In this section comparisons between the different mining machines will be made based on the data gathered in Chapter 6 and 7.

8.1.1 How mining scale with hardware

One aspect that is noteworthy is how the hardware configurations changes the hashrate of the machines mining Monero (XMR). By looking at the ratio between the single core hashrate and the CPU a pattern appears.

Machine	*CPU clock max*	*Single core hashrate*	*Ratio*
NUC	3.4 GHz	58	17.1
Mac	3.1 GHz	54	17.4
Tower	3.9 GHz	73	18.7
Rpi	0.9 GHz	4.6	5.1

Table 8.1: Comparing single core hashrate for native mining.

For the native miners on the NUC, Mac and Tower the hashrate scale with the CPU clock speed at about the same rate. The Rpi has a much lower ratio, this is likely due to it having less than 2 MiB CPU cache. In fact the CPU cache factor is very noticeable across the board. Looking at fig 6.1 one can see that the NUC peaks at two cores mining, and in fig 6.6 the tower peaks at four cores mining. This is in line with them having 4 MiB and 8 MiB of cache memory respectably. The Mac have 3 MiB of cache and it shows as well. The hashrate is unchanged when adding a second core, and when adding a third it only increase by about 10%. In contrast the NUC have a 50% when adding the second core and the Tower have a 60% increase in hashrate when going from two to four cores mining.

Machine	*CPU clock max*	*Single core hashrate*	*Ratio*
NUC	3.4 GHz	17.0	5.0
Mac	3.1 GHz	11.0	3.5
Tower	3.9 GHz	14.6	3.7
Chromebook	2.16 GHz	3.2	1.5
Phone	2.2 GHz	1.0	0.45

Table 8.2: Comparing single core hashrate for web mining.

The web miners does not seem to scale the same way. While the Tower and Mac have about the same ratio the NUC have a significantly better ratio for single core hashrate. The Chromebook and Phone was expected to have lower hashrates as they both have less than 2 MiB of cache, but the Phone provides less than one third the hashrate than that of the Chromebook. Another interesting finding is that the web miners does not lower the efficiency when adding cores beyond the 2 MiB limit, with all machines having higher hashrate with every added core except the eight core for the Tower. However, the fourth core for the NUC, the third and fourth core for the Mac and the fifth to seventh core for the Tower does not increase the hashrate at nearly the same rate as the ones preceding it.

8.1.2 Power consumption and time spent per XMR

One of the main costs of cryptomining is the electricity spent to power the CPUs. A comparison between the different machines used in this thesis follows.

By using the most power efficient configuration from each machine it is possible to compare the different machines in terms of power efficiency.

Machine	*Hashrate*	*Power consumption*	*H/Wh*
NUC	87.7	32 W	9866
Mac	53.9	24 W	8085
Tower CPU	244.7	120 W	7341
Tower CPU + GPU	340.2	198 W	6185
Rpi	12.2	2 W	21960

Table 8.3: Hashrate and power consumption comparison native miners.

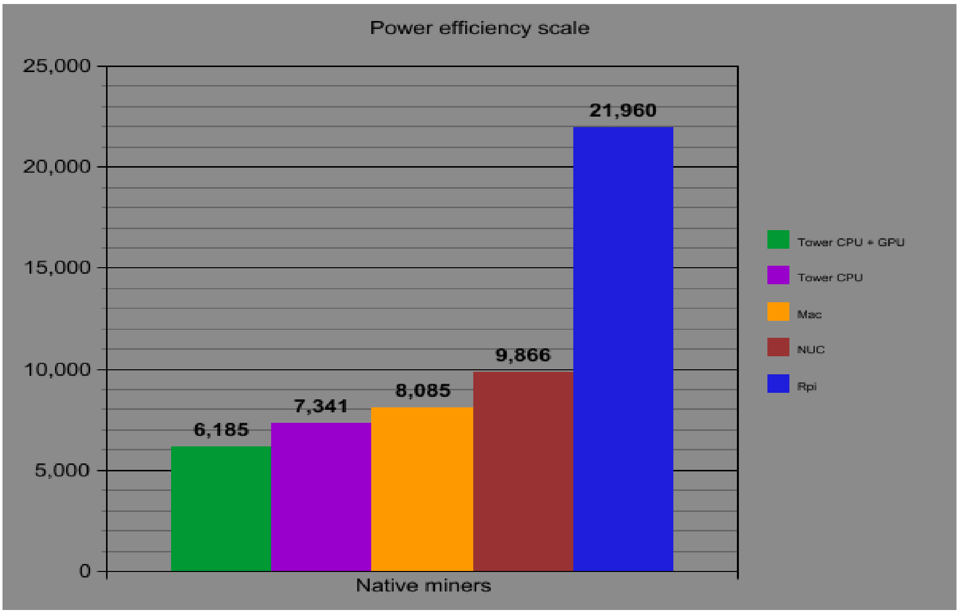


Figure 8.1: The efficiency in terms of electricity used to mine Monero on the different devices with a native miner. Higher is better.

For native miners the Raspberry Pi seems to be the clear winner, and the Tower performs the worst, adding the GPU makes the Tower perform even worse.

Machine	*Hashrate*	*Power consumption*	*H/Wh*
NUC	36.0	36 W	3600
Mac	17.1	32 W	1924
Chromebook	5.0	5.6 W	3214
Phone	6.4	2.6 W*	8862
Tower	47.2	134 W	1268

Table 8.4: Hashrate and power consumption comparison web miners.

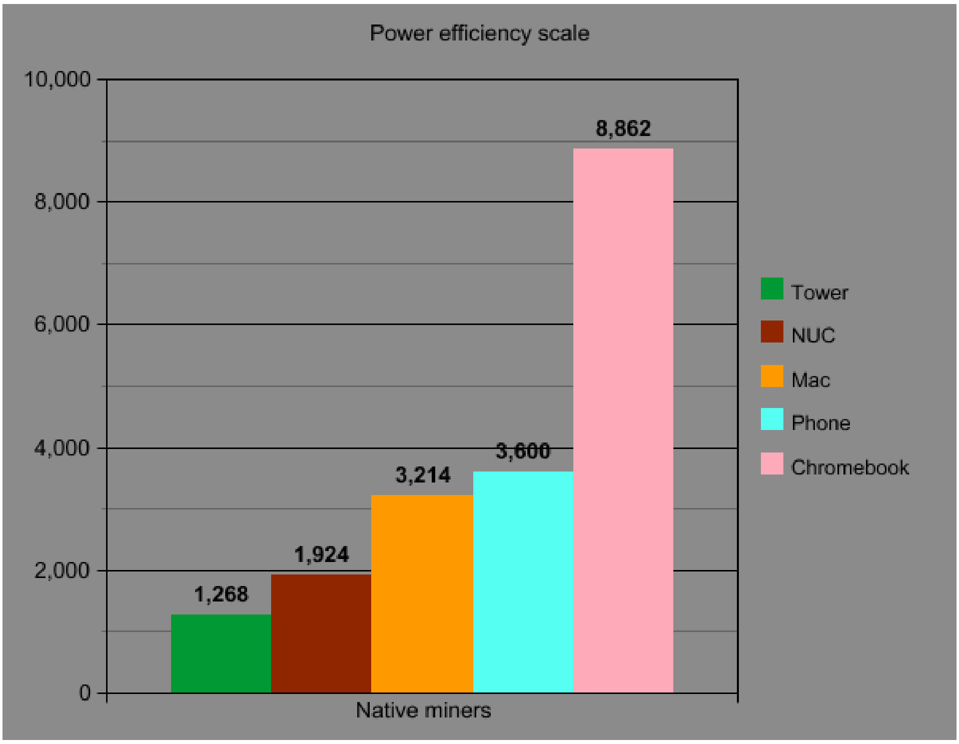


Figure 8.2: The efficiency in terms of electricity used to mine Monero on the different devices in a web browser. Higher is better.

The web the results are similar, the Tower is doing the worst in terms of power efficiency while the Phone is doing the best. It must be noted however that the power usage for the Phone was measured in mA spent, not in Watt and the Watt values was derived using an assumed Voltage of 3.7 V and $Watt = Volt \times Ampere$.

Another important aspects of cryptomining is how long it takes to accumulate the currency, this section will compare the different devices in terms of time efficiency while mining. Unlike the previous section this section will use the configurations that gives the highest hashrate for each device. In chapter 7 it was calculated that it requires about 18 billion hashes to mine one XMR, this number is also used in this comparison. However, these numbers are subject to the ever changing nature of Monero mining, the Monero network are trying to only pays out once per 2 minutes and regulates the mining difficulty of the network to accommodate this goal, thus the more participants in the network the more hashes are required to acquire one XMR. Additionally the payouts decreases in size and this too will increase the amount of hashes necessary to acquire one XMR. Even so these numbers are sufficient to make comparison between the devices and are gives some indication of how long a miner must run to yield results in late 2018.

Miner	*Hashrate*	*Time to mine one XMR*
NUC	87.7	6.5 Years
Mac	58.7	9.9 Years
Tower CPU	244.7	2.3 Years
Tower CPU + GPU	340.2	1.7 Years
Rpi	14.67	38.9 Years

Table 8.5: Years to mine one XMR for native miners. Lower is better.

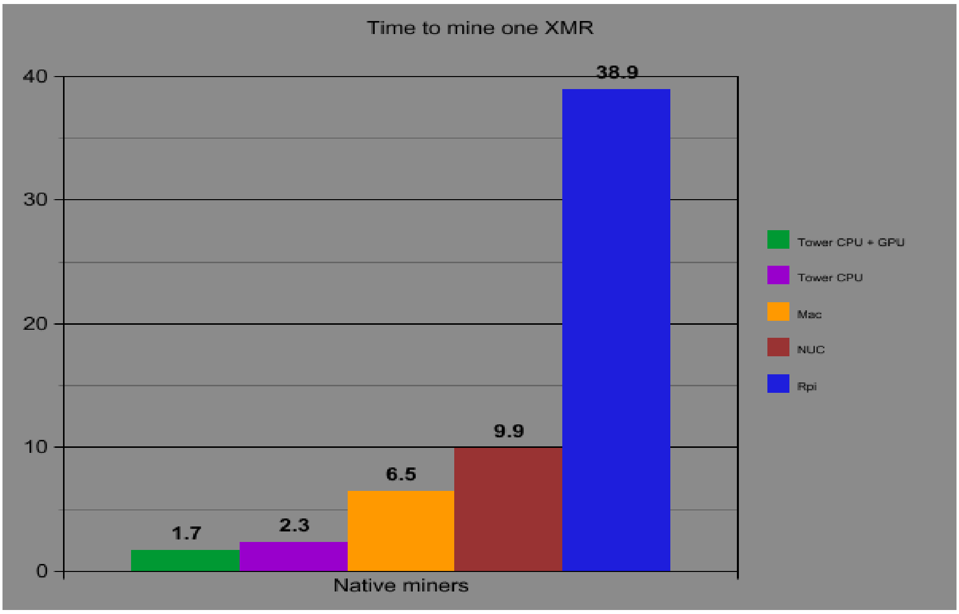


Figure 8.3: Years to mine one XMR for native miners. Lower is better.

As can be seen in table 8.5 and fig 8.3 it would take several years to mine a single XMR even when running on high end devices so to have any reasonable chance of getting the payout it is necessary to use multiple machines, legitimate miners do this through mining pools, but botnets can achieve the same thing through cryptojacking.

Miner	*Hashrate*	*Time to mine one XMR*
NUC	36.0	15.9 Years
Mac	17.1	33.4 Years
Chromebook	5.0	114.2 Years
Phone	6.4	89.1 Years
Tower	48.2	11.8 Years

Table 8.6: Years to mine one XMR for web miners. Lower is better.

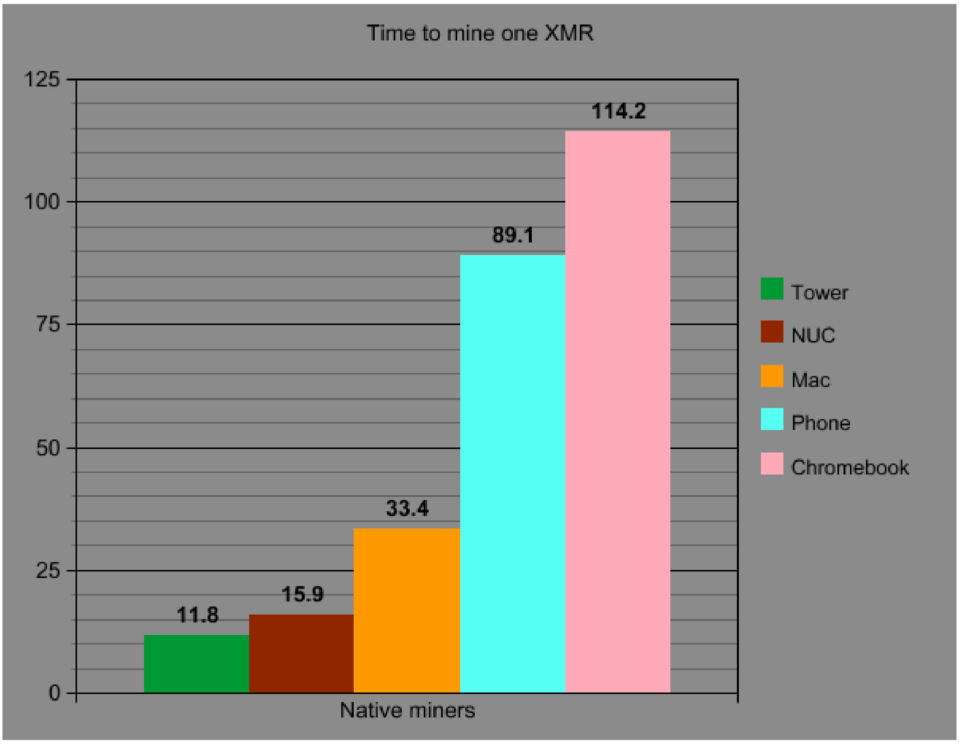


Figure 8.4: Years to mine one XMR for web miners. Lower is better.

Fig 8.3 mirrors fig 8.1 and fig 8.6 mirrors fig 8.2 quite a lot, there are some discrepancies, but the trend is that more power efficient machines are the least efficient in terms of hashrate.

By looking at the numbers it becomes quite clear that it is not efficient to mine using a low number of devices, the opportunity cost of waiting several years, or more than a hundred years in the case of the Chromebook is just way too high, multiple devices is absolutely necessary to mine at any reasonable rate. For criminals this means that there might be more profitable ways to use compromised devices, such as encrypting the data and applying ransomware, have the device participating in denial of service attacks or just have it lay dormant until some use for it can be found.

A curios note is that the Rpi, the most power efficient devices for mining is working at about 1/23 the time efficiency of the Tower, at about 1/20 of the hardware price, one could thus make an argument to get a bunch of Rpis to mine Monero rather than buying a single powerful system.

8.2 The rise and fall of Coinhive

Cryptojacking by browser as a phenomenon is highly linked with the rise of Coinhive. The script provided by Coinhive made it trivial to set up a site to mine Monero on the web by using website visitors' CPUs. There are several things one can learn by looking at Coinhive's short history, this section will look into some of it.

To get some insight into the economy of cryptomining one can look at the historical usage of Coinhive. According to previous research Coinhive was responsible for at least 75% of browser based miners, the same report also found that 10 user accounts are responsible for 80% all short links[22]. This means that only a handful of people were reaping the vast majority of the profits. While it is impossible to know exactly what those profit were, both because of the hard to track nature of cryptomining and because it is not known if or when the Monero were exchanged for fiat currency, but some research suggest that Coinhive's script mined around $250.000 US a month at its height[80].

Coinhive's creators claimed that it was created as an alternative to online advertisements and asked their customers to disclose that the script was running a cryptominer, but most of their customers did not disclose that the script was running, and after Coinhive released their second iteration of the script called Authedmine that required user consent, less than 4% of sites that ran the script was using the new version, the vast majority choosing to keep using the older version that did not require explicit consent[81]. It is not unlikely that Coinhive made money by letting their script be run on compromised web sites and servers. This might have been a contributing factor to them allowing for their first iteration of the script to be continued to function and mine even after Authedmine was released.

Another aspect that is worth giving some thought is that when Coinhive shut down they only gave their users a little more than two month to get their assets off their site. This could mean that Coinhive was part of an exit scam where the Coinhive owners now control all the XMR not claimed, and if it is not an exit scam it is still an important lesson for anyone doing this kind of business, the service shut down fast and unexpectedly, some users might not even have made their initial 500 EUR back when Coinhive shut down their servers.

The reasons stated for why Coinhive and cryptojacking in general has fallen out of favor is the Monero hard fork of March 2019 and the general fall in cryptocurrency valuation in 2018-2019, buth the security industry should not be overlooked in their efforts to stop the miners. The industry worked fast and efficiently to stop the illicit cryptomining and several cryptojacking specific browser addons were created and existing addons for blocking, among other things, advertisements and tracking were updated to also block cryptojacking. Microsoft configured their Windows Defender antivirus software to remove cryptominers that are not allowed explicitly. Google and Apple both took action and removed all miner apps from their app stores. And while cryptojacking is not likely to disappear from the Internet this should be seen as a victory for the industry.

8.3 Impact of cryptojacking

Cryptojacking has had an impact on the web, but not to the extent once feared. This section will cover the impact of cryptojacking for end users, broader society and to criminals and law enforcement.

The infected end users might not notice anything and their machine might be quite usable even after a compromise. As discussed earlier the most efficient way to mine Monero on many systems is to not use the entire CPU, but rather use only so much that the entire CPU cache are used, but not more, users that have systems more powerful than they need might thus never notice anything at all, even the extra power consumption is unlikely to worry the end users as the extra cost minuscule.
Browser based cryptojacking might be more noticeable since they do not use the CPU cache in the same way as native miners and become more efficient the more cores used regardless of the CPU cache size, and due to the lower hashrate of web miners the operators might not throttle as much as necessary in order to make more money.
Businesses and larger organizations will likely have much the same experience, cryptojackers are a nuisance, but for the most part not harmful. This creates misaligned incentives where the process of getting rid of the cryptojacking software might just not be worth it to those responsible for maintaining the computer systems, IT in an organization or the end user themselves in a private setting. The harm done by cryptojacking is usually fully reversible and the culprits are hard to track down. This means that law enforcement are unlikely to prioritize resources to investigate. businesses and private individuals, assuming they have the technical knowledge, might not deem it a worthwhile effort to track down the intruders themselves either.

For criminals wanting to make a profit this means that the risk of running cryptojacking schemes is quite low, web based cryptojacking isn't even illegal as of the writing of this thesis. Even so the decline in cryptojacking attacks in 2018 and 2019 seem to indicate that the low risk isn't worth the effort or opportunity cost. Considering how very old malware such as Code Red[82] and Nimda[83] still exists on the Internet, almost like background radiation and that cryptojacking does make it's propagators some amount of money it is unlikely that cryptojacking will disappear completely, and should the cryptocurrency markets resurge it is likely that cryptojacking will follow suit.

8.4 Threats to validity

This section will cover some of the threats to validity of the results produced in the experiments.

- All the machines used in this experiment are quite clean in that they did not have very much software running besides the miners except for the controlled experiments were performance and subjective impact was tested, this is not normal for cryptojacked systems. Many users have several programs running at the same time, this will impact the results, likely given lower hashrates.
- There are an uncountable variations of computer hardware and this experiment only tested six different variations.
- This experiment only had one computer in each class, so there no control group for each of the devices, only a single GPU and a single phone were used in the entire experiment.
- The machines are from different years and manufacturers so it is somewhat difficult to compare and contrast them.
- The experimenter did not have much prior knowledge of very computing intensive software such as modern games and video rendering software, this might have had an impact on the subjective results.
- No blind tests were performed, all participants that tested the devices knew exactly what software the computer was running, this might bias the results.

8.5 Further work

While cryptojacking might not have been the threat that it was thought to be in the middle of 2018 there are still research that can be done on the subject. More tests can be performed on a larger array of devices to determine how to most efficiently mine cryptocurrency. There are also work that can be done to better determine the exact causes of why cryptojacking did not become the next big threat and under what circumstances it might make a comeback. In that vein there are work that can be done to make an economic model to better understand the circumstances under which cryptojacking becomes viable.

The legality question is still at large and it would be helpful to have set a legal precedence before another cryptojacking or another similar threat emerges. There are also work that can be done to track down the perpetrators of cryptojacking. On the flip side the idea of using CPU power in the form of cryptomining as an alternative to advertisements on the web is intriguing and is something that should be investigated further. If it can become a viable alternative to advertisements and tracking it opens up a whole now world of possibilities for online companies.

The costs aspect is touched upon in this thesis, but there are much that can be expanded upon, the actual costs are hard to determine and might require a whole project to itself. Apart from the purely monetary costs the costs in terms of reputation caused by cryptomining on web sites without obtaining consent and the environmental costs caused by the electricity expended on mining cryptocurrency.

Chapter 9

Conclusion

There are two main types of cryptojacking, browser based miners and native miners, of these the native miners are far more efficient, but require a program to be installed on the users computer while the browser based are mostly harmless JavaScript that terminates as soon as the web page is closed. Browser based cryptojacking was a huge trend among nefarious individuals and groups in 2018. It's ease of use, low impact on end users and hard to track nature lead the security industry, Europol among others to predict that cryptojacking would be the largest security threat, surpassing all other malware. This did not come to pass, the cryptocurrency marked collapsed, the security industry did a terrific job at creating counter measures and the Monero project decided to hard fork their currency. This combined effort have driven the profitability down to the point were the biggest actor, Coinhive shut down their business.

Most victims of cryptojacking are merely inconvenienced by it and not significantly harmed. Cryptojackers want to steal CPU cycles and to this end it is in their best interest to keep the victims content enough that they continue to use their machines, or at least leave them turned on.

Prevention of cryptojacking turned out not to be all that difficult, web extensions were quickly created and existing extensions that block advertisements and tracking were updated to also block cryptojacking.

The cost data gathered in this thesis can be used to better determine at what point criminals will change their methods of operation. For as long as cryptojacking was somewhat profitable there was a relatively large marked for it, but as soon as the cryptocurrencies fell in value cryptojacking fell out of favor and criminals reverted back to other, more profitable methods. Cryptojacking has a very low risk, both in terms of getting caught and in terms of punishment if gotten caught, and is relatively easy to carry out. Despite this it still fell out of favor with the decline in Monero's value. This facts can be used to improve existing thereat models.

Bibliography

[1] Cryptocurrency chart. https://www.cryptocurrencychart.com/. Last accessed: 2019-05-24.

[2] Monero.com. https://monero.org/. Last accessed: 2019-05-24.

[3] David Yanofsky Ritchie S. King, Sam Williams. By reading this article, you're mining bitcoins. https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/, 2013. Last accessed: 2019-05-24.

[4] Coinhive.com. https://coinhive.com/. Last accessed: 2019-04-08. The site is no longer online. an archive can be found at https://web.archive.org/web/20190429000729/https://coinhive.com/.

[5] Trendmicro. Hacker infects node.js package to steal from bitcoin wallets. https://www.trendmicro.com/vinfo/se/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets, 2018. Last accessed: 2019-05-24.

[6] Kate Rooney. $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html, 2018. Last accessed: 2019-05-22.

[7] Ruben Kimmelman. Hackers steal $59 million in cryptocurrency from japanese exchange. https://www.npr.org/2018/09/20/650079273/hackers-steal-59-million-in-cryptocurrency-from-japanese-exchange, 2018. Last accessed: 2019-05-23.

[8] Natahniel Popper. Bitcoin thieves threaten real violence for virtual currencies. *Ny York Times*, 2018. Last accessed: 2019-05-23.

[9] Turkish police detain gang who stole bitcoins worth $2.83m. https://www.dailysabah.com/investigations/2017/11/15/turkish-

police-detain-gang-who-stole-bitcoins-worth-283m, 2017. Last accessed: 2019-05-23.

[10] Cynthia Kim Dahee Kim. South korea says no plans to ban cryptocurrency exchanges, uncovers $600 million illegal trades. https://www.reuters.com/article/us-southkorea-bitcoin/south-korea-says-no-plans-to-ban-cryptocurrency-exchanges-uncovers-600-million-illegal-trades-idUSKBN1FK09J, 2018. Last accessed: 2019-05-24.

[11] Mark Emem. How mexican cartels use chinese crypto brokers to launder drug money. https://www.ccn.com/how-mexican-cartels-use-chinese-crypto-brokers-to-launder-drug-money/, 2018. Last accessed: 2019-05-24.

[12] Digital Desh staff. Over 3,000 luas users may have had records compromised in cyber attack. https://www.irishexaminer.com/breakingnews/ireland/luas-being-held-to-ransom-after-website-hacked-895306.html, 2019. Last accessed: 2019-05-24.

[13] John. Alert: Spike in bitcoin extortion. https://ciphertrace.com/alert-spike-in-bitcoin-extortion/, 2018. Last accessed: 2019-05-24.

[14] F-secure. Crypto-ransomware. https://www.f-secure.com/en/web/labs_global/crypto-ransomware. Last accessed: 2019-05-24.

[15] Sara Tilly. Cryptolocker prevention – how to secure your server environment. https://blog.syskit.com/cryptolocker-prevention, 2017. Last accessed: 2019-05-24.

[16] Nick Chong. *Etherium world news*, 2018. Last accessed: 2019-05-24.

[17] AFP. South korean swaps bitcoins for 2 mln euros in fake notes. *New Strait Times*, 2018.

[18] Marie Huillet. *Cointelegraph*, 2018. Last accessed: 2019-05-24.

[19] Europol. Internet organised crime threat assessment (iocta) 2018. 2018.

[20] Perma CC. *Webroot*, 2018. Last accessed: 2019-05-24.

[21] Symantec. Internet security threat report. https://www.symantec.com/en/sg/security-center/threat-report, 2019. Last accessed: 2019-05-24.

[22] Konrad Wolsing Oliver Hohlfeld Jan Rüth, Torsten Zimmermann. Digging into browser-based crypto mining. *Chair of Communication and Distributed Systems, RWTH Aachen University*, 2018. Last accessed: 2019-05-24.

[23] 18 u.s. code §1030. fraud and related activity in connection with computers. https://www.law.cornell.edu/uscode/text/18/1030. Last accessed: 2019-05-24.

[24] Computer misuse act 1990. https://www.legislation.gov.uk/ukpga/1990/18/contents. Last accessed: 2019-05-24.

[25] Historical trends in the usage of client-side programming languages for websites. https://w3techs.com/technologies/history_overview/client_side_language/all. Last accessed: 2019-05-24.

[26] Wordpress plugins search result for ’mining’. https://wordpress.org/plugins/tags/mining/. Last accessed: 2019-05-24.

[27] Lorin Wu. Monero-mining hiddenminer android malware can potentially cause device failure. *TrendMicro*. Last accessed: 2019-05-24.

[28] Karl Sigler. Crypto-jacking: how cyber-criminals are exploiting the crypto-currency boom. *SpiderLabs at Trustware*, pages 12–14, 2018.

[29] Madeleine Dean. 5 best cryptojacking blockers to use on your windows pc, 2018. Windows report.

[30] Martin Hron. Protect yourself from cryptojacking. *Avast blog*, 2018.

[31] Alexandru Frigioiu. Crypto miners: the rise of a malware empire. *Avaria blog*, 2018.

[32] Minerblock’s github page. https://github.com/xd4rker/MinerBlock. Last accessed: 2019-05-24.

[33] Nocoin’s github page. https://github.com/keraf/NoCoin. Last accessed: 2019-05-24.

[34] Ublock’s github page. https://github.com/gorhill/uBlock. Last accessed: 2019-05-24.

[35] Ghostery.com. https://www.ghostery.com/. Last accessed: 2019-05-24.

[36] Nicolas van Saberhagen. Cryptonote v 2.0. https://cryptonote.org/whitepaper.pdf, 2013. Last accessed: 2019-05-24.

[37] Monero merchants & services. http://ww.getmonero.org/community/merchants/. Last accessed: 2019-05-24.

[38] Trustnodes. A fork, an algo change, a 51% attack, and monero still 85% controlled by asics. https://www.trustnodes.com/2019/02/09/a-fork-an-algo-change-a-51-attack-and-monero-still-85-controlled-by-asics, 2019. Last accessed: 2019-05-24.

[39] Nick Choung. Monero to hard fork blockchain in march to stifle xmr asic miners. https://blockonomi.com/monero-hard-fork-xmr-asic-miners/, 2019. Last accessed: 2019-05-24.

[40] Monero forks and hard forks. https://monero.org/forks/. Last accessed: 2019-05-24.

[41] Troy Mursch Jeremy Clark Shayan Eskandari, Andreas Leoutsarakos. A first look at browser-based cryptojacking. *2018 IEEE European Symposium on Security and Privacy Workshops*, 2018. Last accessed: 2019-05-24.

[42] Tracey Caldwell. The miners strike – addressing the cryptocurrency threat to enterprise networks. *Computer Fraud and Security, Issue 5*, pages 8–14, 2018.

[43] Aziz Mohaisen Muhammad Saad, Aminollah Khormali. End-to-end analysis of in-browser cryptojacking. *arXiv:1809.02152v1*, 2018. Last accessed: 2019-05-24.

[44] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin.org*, 2008.

[45] Amrutha Gayathri. From marijuana to lsd, now illegal drugs delivered on your doorstep. *International Business Times*, 2011.

[46] Darknetmarkets.com. Last accessed: 2019-05-24.

[47] Tor faq. `https://www.torproject.org/docs/faq`. Last accessed: 2019-05-24.

[48] Josh Boyd. In community we trust: Online security communication at ebay. *Journal of Computer-Mediated Communication*, 2006.

[49] Matteo Di Cristofaro Nuria Lorenzo-Dus. ‘i know this whole market is based on the trust you put in me and i don’t take that lightly’: Trust, community and discourse in crypto-drug markets. *Sage Journals*, 2018.

[50] Domhnall Carlin Philip OḰane, Sakir Sezer. Evolution of ransomware. *IET Journals*, 2017.

[51] Tom Byermoen Gordon Andersen Ådne Husby Sandnes Hanna Haug Røset Kari Spets Morten S. Hopperstad, Bjørnar Tommelstad. Forsvinningssaken i lørenskog: Her kan budskapet til familien ligge. *VG*, 2019.

[52] Charles Bremner. Anne-elisabeth hagen: Tycoon’s wife abducted for ‘eur9m ransom’. *The Times*, 2019.

[53] Giovanni Vigna Marco Cova, Christopher Kruegel. Detection and analysis of drive-by-download attacks and malicious javascript code. *AMC Digital Libary*, 2010. Last accessed: 2019-05-24.

[54] Martin Johns. On javascript malware and related threats. *J Comput Virol*, 2008. Last accessed: 2019-05-24.

[55] Joseph Cox. Creators of in-browser cryptocurrency miner ’coinhive’ say their reputation couldn’t be much worse. `https://motherboard.vice.com/en_us/article/vbpbz4/creators-of-in-browser-cryptocurrency-miner-coinhive-say-their-reputation-couldnt-be-much-worse`, 2018. Last accessed: 2019-05-24.

[56] Helen Partz. Coinhive code found on 300+ websites worldwide in recent cryptojacking campaign. `https://cointelegraph.com/news/coinhive-code-found-on-300-websites-worldwide-in-recent-cryptojacking-campaign`, 2018. Last accessed: 2019-05-24.

[57] The Coinhive Team. Discontinuation of coinhive. `https://coinhive.com/blog/en/discontinuation-of-coinhive`, 2019. Last accessed: 2019-05-24.

[58] Coinimp. `https://www.coinimp.com/`. Last accessed: 2019-05-24.

[59] Cryptoloot. `https://crypto-loot.com/`. Last accessed: 2019-05-24.

[60] Deep miner. `https://github.com/deepwn/deepMiner`. Last accessed: 2019-05-24.

[61] Evangelos P. Markatos Panagiotis Papadopoulos, Panagiotis Ilia. Truth in web mining: Measuring the profitability and cost of cryptominers as a web monetization model. *arXiv:1806.01994v1*, 2018. Last accessed: 2019-05-24.

[62] Martin Johns Konrad Rieck Marius Mucsh, Christian Wressnegger. Web-based cryptojacking in the wild. *Computer Science Report, Technische Universitat Braunschweig*, 2018. Last accessed: 2019-05-24.

[63] experiment. `https://www.merriam-webster.com/dictionary/experiment`. Last accessed: 2019-05-24.

[64] Sir Ronald Aylmer Fisher. *The Design of Experiments(9th ed.)*. Macmillan, 1971[1935].

[65] Xmr-stak's github page. `https://github.com/fireice-uk/xmr-stak`. Last accessed: 2019-05-24.

[66] Cpuminer-multi's github page. `https://github.com/tpruvot/cpuminer-multi`. Last accessed: 2019-05-24.

[67] Supportxmr.com. `https://www.supportxmr.com/`. Last accessed: 2019-05-24.

[68] Openssh.com. `https://www.openssh.com/`. Last accessed: 2019-05-24.

[69] Tmux's github page. `https://github.com/tmux/tmux/wiki`. Last accessed: 2019-05-24.

[70] Coinwebmining.com. `https://coinwebmining.com/browser-miner/monero`. Last accessed: 2019-05-24.

[71] Minero.cc. `https://minero.cc/`. Last accessed: 2019-05-24.

[72] istat menus' app store page. `https://itunes.apple.com/us/app/istat-menus/id1319778037?mt=12`. Last accessed: 2019-05-24.

[73] Analyze power use with battery historian. https://developer.android.com/topic/performance/power/battery-historian. Last accessed: 2019-05-24.

[74] Sysbench's github page. https://github.com/akopytov/sysbench. Last accessed: 2019-05-24.

[75] Mike Harsh. Run bash on ubuntu for windows. *Microsoft blog*. Last accessed: 2019-05-24.

[76] Reda Chouffani. Cryptojacking emerging as a new threat to healthcare. https://searchhealthit.techtarget.com/tip/Cryptojacking-emerging-as-a-new-threat-to-healthcare, Last accessed: 2019-05-20.

[77] CSO Ms. Smith. The pirate bay hijacked users' cpu power to secretly mine cryptocurrency monero. https://www.csoonline.com/article/3225512/the-pirate-bay-hijacked-users-cpu-power-to-secretly-mine-cryptocurrency-monero.html. Last accessed: 2019-05-19.

[78] Elizabeth Gail. The pirate bay is crypto mining once again. https://coincentral.com/the-pirate-bay-is-crypto-mining-once-again/. Last accessed 2019-05-19.

[79] Kane Pepi. Bitcoin used to fund terrorism: New york woman pleads guilty. https://blockonomi.com/bitcoin-fund-terrorism/. Last accessed 2019-05-21.

[80] Ian Tozer. Coinhive in-browser software is 'mining' $250k per month, research finds. https://bitcoinist.com/internet-users-making-other-people-over-250k-per-month-cryptocurrency-profit/. Last accessed 2019-05-21.

[81] A Little Sunshine. Posts tagged: Authedmine. https://krebsonsecurity.com/tag/authedmine/. Last accessed 2019-05-21.

[82] Microsoft. Analysis: ida 'code red' worm. Last accessed 2019-05-23.

[83] F-secure. Net-worm:w32/nimda. https://www.f-secure.com/v-descs/nimda.shtml. Last accessed 2019-05-23.

Appendix Hardware

Name: NUC7i5BNK
Referd to as: NUC

CPU frq range	CPU cache size	GPU	RAM speed & size	SSD/HDD
2.20 - 3.40 GHz	4 MiB	Intel® Iris® Plus Graphics 640	8GiB of 2400MHz DDR3L	124 GB M.2 SSD

Output from lscpu:

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list: 0-3
Thread(s) per core:  2
Core(s) per socket:  2
Socket(s):             1
NUMA node(s):          1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 142
Model name:            Intel(R) Core(TM) i5-7260U CPU @ 2.20GHz
Stepping:              9
CPU MHz:               812.337
CPU max MHz:           3400,0000
CPU min MHz:           400,0000
BogoMIPS:              4416.00
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              4096K
NUMA node0 CPU(s):   0-3
```

Output from lshw:

```
beldum
    description: Desktop Computer
    product: NUC7i5BNK
    vendor: Intel Corporation
    version: J31159-311
    serial: G6BN83000289
    width: 64 bits
    capabilities: smbios-3.1 dmi-3.1 smp vsyscall32
    configuration: boot=normal chassis=desktop family=Intel NUC uuid=55E446F4-43DA-4F76-1D94-94C691A1
771E
  *-core
       description: Motherboard
       product: NUC7i5BNB
       vendor: Intel Corporation
       physical id: 0
       version: J31144-310
       serial: GEBN828008S4
       slot: Default string
     *-firmware
          description: BIOS
          vendor: Intel Corp.
          physical id: 0
          version: BNKBL357.86A.0068.2018.0824.1125
          date: 08/24/2018
          size: 64KiB
          capacity: 8128KiB
          capabilities: pci upgrade shadowing cdboot bootselect socketedrom edd int13floppy1200
int13
floppy720 int13floppy2880 int5printscreen int14serial int17printer acpi usb biosbootspecification
uef
i
     *-memory
          description: System Memory
          physical id: 28
          slot: System board or motherboard
          size: 8GiB
        *-bank:0
             description: [empty]
             physical id: 0
             slot: ChannelA-DIMM0
        *-bank:1
             description: SODIMM DDR4 Synchronous Unbuffered (Unregistered) 2400 MHz (0,4
ns)
             product: CT8G4SFS824A.C8FDD1
             vendor: 859B
             physical id: 1
             serial: E128B123
             slot: ChannelB-DIMM0
             size: 8GiB
             width: 64 bits
             clock: 2400MHz (0.4ns)
     *-cache:0
          description: L1 cache
          physical id: 2c
          slot: L1 Cache
          size: 128KiB
          capacity: 128KiB
```

Name: MacBook Pro (Retina, 13-inch, Mid 2014)
Referd to as: Mac

CPU frq range	CPU cache size	GPU	RAM speed & size	SSD/HDD
2.60 - 3.10 GHz	3 MiB	IRIS 5100	8GB of 1600MHz DDR3L	256 GB SSD

Output from lscpu:

```
Architecture:         x86_64
CPU op-mode(s):       32-bit, 64-bit
Byte Order:           Little Endian
CPU(s):               4
On-line CPU(s) list: 0-3
Thread(s) per core:  2
Core(s) per socket:  2
Socket(s):            1
NUMA node(s):         1
Vendor ID:            GenuineIntel
CPU family:           6
Model:                69
Model name:           Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz
Stepping:             1
CPU MHz:              1420.082
CPU max MHz:          3100.0000
CPU min MHz:          800.0000
BogoMIPS:             5200.05
Virtualization:       VT-x
L1d cache:            32K
L1i cache:            32K
L2 cache:             256K
L3 cache:             3072K
NUMA node0 CPU(s):    0-3
```

Sample output from lshw:

```
bent-usbuntu
    description: Notebook
    product: MacBookPro11,1 (System SKU#)
    vendor: Apple Inc.
    version: 1.0
    serial: C02NT7VBG3QJ
    width: 64 bits
    capabilities: smbios-2.4 dmi-2.4 smp vsyscall32
    configuration: boot=normal chassis=notebook family=Mac sku=System SKU# uuid=2160ED34-9842-BD59-816B-D926
A723BBBB
  *-core
       description: Motherboard
       product: Mac-189A3D4F975D5FFC
       vendor: Apple Inc.
       physical id: 0
       version: MacBookPro11,1
       serial: C02448302F6G3LG1Y
       slot: Part Component
     *-cpu
          description: CPU
          product: Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz
          vendor: Intel Corp.
          physical id: 0
          bus info: cpu@0
          version: Intel(R) Core(TM) i5-4278U CPU @ 2.60GHz
          serial: To Be Filled By O.E.M.
          slot: U3E1
          size: 1919MHz
          capacity: 3100MHz
          width: 64 bits
          clock: 25MHz
        *-cache:0
             description: L1 cache
             physical id: 2
             size: 64KiB
             capacity: 64KiB
             capabilities: asynchronous internal write-back instruction
             configuration: level=1
        *-cache:1
             description: L2 cache
             physical id: 3
             size: 512KiB
             capacity: 512KiB
             capabilities: asynchronous internal write-back unified
             configuration: level=2
        *-cache:2
             description: L3 cache
             physical id: 4
             size: 3MiB
             capacity: 3MiB
             capabilities: asynchronous internal write-back unified
             configuration: level=3
     *-cache
          description: L1 cache
          physical id: 1
          size: 64KiB
          capacity: 64KiB
          capabilities: asynchronous internal write-back data
          configuration: level=1
     *-memory
          description: System Memory
          physical id: 5
          slot: System board or motherboard
          size: 8GiB
        *-bank:0
             description: SODIMM DDR3 Synchronous 1600 MHz (0,6 ns)
             product: 8KTF51264HZ-1G6E1
             vendor: Micron Technology
             physical id: 0
             serial: 0x00000000
             slot: DIMM0
             size: 4GiB
             clock: 1600MHz (0.6ns)
        *-bank:1
             description: SODIMM DDR3 Synchronous 1600 MHz (0,6 ns)
             product: 8KTF51264HZ-1G6E1
             vendor: Micron Technology
             physical id: 1
             serial: 0x00000000
             slot: DIMM0
             size: 4GiB
             clock: 1600MHz (0.6ns)
```

The lshw output for the Macbook was very extensive and very useful, so most of it was omitted and only the relevant parts was kept.

Name: Acer Chromebook CB3-131 11,6" HD
Referd to as: Chromebook

CPU frq range	CPU cache size	GPU	RAM speed & size	SSD/HDD
2.16 - 3.10 GHz	1 MiB	Intel® HD Graphics for Intel Atom® Processor	2GB of 1600MHz DDR3L	16 GB SSD

Output from lscpu:

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                2
On-line CPU(s) list:   0,1
Thread(s) per core:    1
Core(s) per socket:    2
Socket(s):             1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 55
Model name:            Intel(R) Celeron(R) CPU  N2840  @ 2.16GHz
Stepping:              8
CPU MHz:               1405.401
CPU max MHz:           2582.3000
CPU min MHz:           499.8000
BogoMIPS:              4326.40
L1d cache:             24K
L1i cache:             32K
L2 cache:              1024K
```

Output from lshw:

```
localhost
    description: Desktop Computer
    product: Gnawty
    vendor: GOOGLE
    version: 1.0
    serial: 123456789
    width: 4294967295 bits
    capabilities: smbios-2.7 dmi-2.7 smp vsyscall32
    configuration: boot=normal chassis=desktop
  *-core
       description: Motherboard
       physical id: 0
     *-firmware
          description: BIOS
          vendor: coreboot
          physical id: 0
          version: Google_Gnawty.5216.239.156
          date: 12/03/2017
          size: 1MiB
          capacity: 8128KiB
          capabilities: pci pcmcia upgrade bootselect acpi
     *-cpu:0 DISABLED
          description: CPU [empty]
          vendor: GenuineIntel
          physical id: 3
          version: Intel(R) Celeron(R) CPU  N2840  @ 2.16GHz
          configuration: cores=16
     *-memory
          description: System memory
          physical id: 1
          size: 1916MiB
     *-cpu:1
          product: Intel(R) Celeron(R) CPU  N2840  @ 2.16GHz
          vendor: Intel Corp.
                    physical id: 2
          bus info: cpu@0
          size: 2582MHz
          capacity: 2582MHz
          width: 64 bits
          capabilities: fpu fpu_exception wp vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse
     *-pci
          description: Host bridge
          product: Atom Processor Z36xxx/Z37xxx Series SoC Transaction Register
          vendor: Intel Corporation
          physical id: 100
          bus info: pci@0000:00:00.0
          version: 0e
          width: 32 bits
          clock: 33MHz
          configuration: driver=iosf_mbi_pci
          resources: irq:0
        *-display
             description: VGA compatible controller
             product: Atom Processor Z36xxx/Z37xxx Series Graphics & Display
             vendor: Intel Corporation
             physical id: 2
             bus info: pci@0000:00:02.0
             version: 0e
             width: 32 bits
             clock: 33MHz
             capabilities: pm msi vga_controller bus_master cap_list rom
             configuration: driver=i915 latency=0
             resources: irq:262 memory:d0000000-d03fffff memory:c0000000-cfffffff ioport:1000(size=8)
        *-usb
             description: USB controller
                         product: Atom Processor Z36xxx/Z37xxx Series USB xHCI
             vendor: Intel Corporation
             physical id: 14
             bus info: pci@0000:00:14.0
             version: 0e
             width: 64 bits
             clock: 33MHz
             capabilities: pm msi xhci bus_master cap_list
             configuration: driver=xhci_hcd latency=0
             resources: irq:263 memory:d0900000-d090ffff
           *-usbhost:0
                product: xHCI Host Controller
                vendor: Linux 4.4.164-15546-gd8c7defc947f xhci-hcd
                physical id: 0
                bus info: usb@2
                logical name: usb2
                version: 4.04
                capabilities: usb-3.00
                configuration: driver=hub slots=1 speed=5000Mbit/s
           *-usbhost:1
                product: xHCI Host Controller
                vendor: Linux 4.4.164-15546-gd8c7defc947f xhci-hcd
                physical id: 1
                bus info: usb@1
                logical name: usb1
                version: 4.04
                capabilities: usb-2.00
                configuration: driver=hub slots=6 speed=480Mbit/s
              *-usb:0
                   description: Video
                   product: HD WebCam
                   vendor: HD WebCam
                   physical id: 3
                   bus info: usb@1:3
                                      version: 0.03
                   serial: NC2141103Q64200922LM03
                   capabilities: usb-2.00
                   configuration: driver=uvcvideo maxpower=500mA speed=480Mbit/s
              *-usb:1
                   description: Bluetooth wireless interface
                   vendor: Intel Corp.
                   physical id: 4
                   bus info: usb@1:4
                   version: 0.01
                   capabilities: bluetooth usb-2.00
                   configuration: driver=btusb maxpower=100mA speed=12Mbit/s
        *-generic UNCLAIMED
             description: Encryption controller
             product: Atom Processor Z36xxx/Z37xxx Series Trusted Execution Engine
             vendor: Intel Corporation
             physical id: 1a
             bus info: pci@0000:00:1a.0
             version: 0e
             width: 32 bits
             clock: 33MHz
             capabilities: pm msi cap_list
             configuration: latency=0
             resources: memory:d0600000-d06fffff memory:d0700000-d07fffff
        *-multimedia
             description: Audio device
             product: Atom Processor Z36xxx/Z37xxx Series High Definition Audio Controller
             vendor: Intel Corporation
             physical id: 1b
             bus info: pci@0000:00:1b.0
             version: 0e
             width: 64 bits
             clock: 33MHz
             capabilities: pm msi bus_master cap_list
                          configuration: driver=snd_hda_intel latency=0
             resources: irq:265 memory:d0914000-d0917fff
        *-pci
             description: PCI bridge
             product: Atom Processor E3800 Series PCI Express Root Port 1
             vendor: Intel Corporation
             physical id: 1c
             bus info: pci@0000:00:1c.0
             version: 0e
             width: 32 bits
             clock: 33MHz
             capabilities: pci pciexpress msi pm normal_decode bus_master cap_list
             configuration: driver=pcieport
             resources: irq:261 memory:d0800000-d08fffff
           *-network
                description: Wireless interface
                product: Wireless 7260
                vendor: Intel Corporation
                physical id: 0
                bus info: pci@0000:01:00.0
                logical name: wlan0
                version: bb
                serial: f0:42:1c:8c:4c:04
                width: 64 bits
                clock: 33MHz
                capabilities: pm msi pciexpress bus_master cap_list ethernet physical wireless
                configuration: broadcast=yes driver=iwlwifi driverversion=4.4.164-15546-gd8c7defc947f firmware=17.bfb58538.0 ip=192.168.1.8 late
                resources: irq:264 memory:d0800000-d0801fff
        *-isa
             description: ISA bridge
             product: Atom Processor Z36xxx/Z37xxx Series Power Control Unit
             vendor: Intel Corporation
             physical id: 1f
                          bus info: pci@0000:00:1f.0
             version: 0e
             width: 32 bits
             clock: 33MHz
             capabilities: isa bus_master cap_list
             configuration: driver=lpc_ich latency=0
             resources: irq:0
```

Name: Sony H4113
Referd to as: Phone

CPU frq range	CPU cache size	GPU	RAM speed & size	SSD/HDD
1.8-2.20 GHz	1 MiB		3 GiB of 1333MHz LPDDR4	32 GB SSD

Output from lscpu

```
Architecture:        aarch64
Byte Order:          Little Endian
CPU(s):              8
On-line CPU(s) list: 0-7
Thread(s) per core:  1
Core(s) per socket:  4
Socket(s):           2
Vendor ID:           Qualcomm
Model:               4
Model name:          Kryo V2
Stepping:            0xa
CPU max MHz:         2208.0000
CPU min MHz:         614.4000
BogoMIPS:            38.40
L1d cache:           32K
L1i cache:           32K
L2 cache:            1024K
```

Neither lshw, hwinfo or dumpsys gave any usable results on the Phone so this section is omitted for it.

Name: Self build PC
Refereed to as: Tower

CPU frq range	CPU cache size	GPU	RAM speed & size	SSD/HDD
3.40 - 3.90 GHz	8 MiB	NVIDIA GeForce CTX 760	16GB of 1600MHz DDR3L	112 GB SSD and 2 TB HDD

Output from lscpu:

```
Architecture:           x86_64
CPU op-mode(s):         32-bit, 64-bit
Byte Order:             Little Endian
CPU(s):                 8
On-line CPU(s) list:    0-7
Thread(s) per core:     2
Core(s) per socket:     4
Socket(s):              1
Vendor ID:              GenuineIntel
CPU family:             6
Model:                  60
Stepping:               3
CPU MHz:                3401.000
BogoMIPS:               6802.00
Virtualization:         VT-x
```

Output from hwinfo:

```
metang
    description: Computer
    width: 64 bits
  *-core
       description: Motherboard
       physical id: 0
     *-memory
          description: System memory
          physical id: 0
          size: 15GiB
     *-cpu
          product: Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz
          vendor: Intel Corp.
          physical id: 1
          bus info: cpu@0
          width: 64 bits
          capabilities: fpu fpu_exception wp vme de pse tsc msr
pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts
acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp
x86-64 pni pclmulqdq dtes64 monitor ds_cpl vmx smx est tm2 ssse3
fma cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_t
aes xsave osxsave avx f16c rdrand cpufreq
  *-network:0 DISABLED
       description: Ethernet interface
       physical id: 1
       logical name: eth0
       serial: 44:8a:5b:21:40:80
       capabilities: ethernet physical
       configuration: ip=169.254.190.195
  *-network:1 DISABLED
       description: Ethernet interface
       physical id: 2
       logical name: eth1
       serial: 00:ff:66:86:4a:34
       capabilities: ethernet physical
       configuration: ip=169.254.217.108
  *-network:2
       description: Ethernet interface
       physical id: 3
       logical name: eth5
       serial: 00:50:b6:d2:26:7d
       capabilities: ethernet physical
       configuration: broadcast=yes ip=192.168.1.10 multicast=yes
```

Due to the tower running Windows hwinfo was used instead of lshw.

Appendix Config

Windows main XMR-stak config file:

```
// generated by xmr-stak/2.6.0/871371622/master/win/nvidia-amd-cpu/20

/*
 * Network timeouts.
 * Because of the way this client is written it doesn’t need to constantly talk (keep-alive) to the server to make
 * sure it is there. We detect a buggy / overloaded server by the call timeout. The default values will be ok for
 * nearly all cases. If they aren’t the pool has most likely overload issues. Low call timeout values are preferable -
 * long timeouts mean that we waste hashes on potentially stale jobs. Connection report will tell you how long the
 * server usually takes to process our calls.
 *
 * call_timeout - How long should we wait for a response from the server before we assume it is dead and drop the connection.
 * retry_time - How long should we wait before another connection attempt.
 *               Both values are in seconds.
 * giveup_limit - Limit how many times we try to reconnect to the pool. Zero means no limit. Note that stak miners
 *               don’t mine while the connection is lost, so your computer’s power usage goes down to idle.
 */
"call_timeout" : 10,
"retry_time" : 30,
"giveup_limit" : 0,

/*
 * Output control.
 * Since most people are used to miners printing all the time, that’s what we do by default too. This is suboptimal
 * really, since you cannot see errors under pages and pages of text and performance stats. Given that we have internal
 * performance monitors, there is very little reason to spew out pages of text instead of concise reports.
 * Press ’h’ (hashrate), ’r’ (results) or ’c’ (connection) to print reports.
 *
 * verbose_level - 0 - Don’t print anything.
 *                 1 - Print intro, connection event, disconnect event
 *                 2 - All of level 1, and new job (block) event if the difficulty is different from the last job
 *                 3 - All of level 1, and new job (block) event in all cases, result submission event.
 *                 4 - All of level 3, and automatic hashrate report printing
 *
 * print_motd    - Display messages from your pool operator in the hashrate result.
 */
"verbose_level" : 3,
"print_motd" : true,

/*
 * Automatic hashrate report
 *
 * h_print_time - How often, in seconds, should we print a hashrate report if verbose_level is set to 4.
 *               This option has no effect if verbose_level is not 4.
 */
"h_print_time" : 60,

/*
 * Manual hardware AES override
 *
 * Some VMs don’t report AES capability correctly. You can set this value to true to enforce hardware AES or
 * to false to force disable AES or null to let the miner decide if AES is used.
 *
 * WARNING: setting this to true on a CPU that doesn’t support hardware AES will crash the miner.
 */
"aes_override" : null,

/*
 * LARGE PAGE SUPPORT
 * Large pages need a properly set up OS. It can be difficult if you are not used to systems administration,
 * but the performance results are worth the trouble - you will get around 20% boost. Slow memory mode is
 * meant as a backup, you won’t get stellar results there. If you are running into trouble, especially
 * on Windows, please read the common issues in the README and FAQ.
 *
 * By default we will try to allocate large pages. This means you need to "Run As Administrator" on Windows.
 * You need to edit your system’s group policies to enable locking large pages. Here are the steps from MSDN
 *
 * 1. On the Start menu, click Run. In the Open box, type gpedit.msc.
 * 2. On the Local Group Policy Editor console, expand Computer Configuration, and then expand Windows Settings.
 * 3. Expand Security Settings, and then expand Local Policies.
 * 4. Select the User Rights Assignment folder.
 * 5. The policies will be displayed in the details pane.
 * 6. In the pane, double-click Lock pages in memory.
 * 7. In the Local Security Setting - Lock pages in memory dialog box, click Add User or Group.
 * 8. In the Select Users, Service Accounts, or Groups dialog box, add an account that you will run the miner on
 * 9. Reboot for change to take effect.
 *
 * Windows also tends to fragment memory a lot. If you are running on a system with 4-8GB of RAM you might need
 * to switch off all the auto-start applications and reboot to have a large enough chunk of contiguous memory.
 *
 *
 * use_slow_memory defines our behaviour with regards to large pages. There are three possible options here:
 * always  - Don’t even try to use large pages. Always use slow memory.
 * warn    - We will try to use large pages, but fall back to slow memory if that fails.
 * never   - If we fail to allocate large pages we will print an error and exit.
 */
"use_slow_memory" : "warn",

/*
 * TLS Settings
 * If you need real security, make sure tls_secure_algo is enabled (otherwise MITM attack can downgrade encryption
 * to trivially breakable stuff like DES and MD5), and verify the server’s fingerprint through a trusted channel.
 *
 * tls_secure_algo - Use only secure algorithms. This will make us quit with an error if we can’t negotiate a secure algo.
 */
"tls_secure_algo" : true,

/*
 * Daemon mode
 *
 * If you are running the process in the background and you don’t need the keyboard reports, set this to true.
 * This should solve the hashrate problems on some emulated terminals.
 */
"daemon_mode" : false,

/*
 * Output file
 *
 * output_file  - This option will log all output to a file.
 *
 */
"output_file" : "",

/*
 * Built-in web server
 * I like checking my hashrate on my phone. Don’t you?
 * Keep in mind that you will need to set up port forwarding on your router if you want to access it from
 * outside of your home network. Ports lower than 1024 on Linux systems will require root.
 *
 * httpd_port - Port we should listen on. Default, 0, will switch off the server.
 */
"httpd_port" : 8080,

/*
 * HTTP Authentication
 *
 * This allows you to set a password to keep people on the Internet from snooping on your hashrate.
 * Keep in mind that this is based on HTTP Digest, which is based on MD5. To a determined attacker
 * who is able to read your traffic it is as easy to break a bog door latch.
 *
 * http_login - Login. Empty login disables authentication.
 * http_pass  - Password.
 */
"http_login" : "",
"http_pass" : "",

/*
 * prefer_ipv4 - IPv6 preference. If the host is available on both IPv4 and IPv6 net, which one should be choose?
 *               This setting will only be needed in 2020’s. No need to worry about it now.
 */
"prefer_ipv4" : true,
```

Windows CPU config file:

```
// generated by xmr-stak/2.6.0/871371622/master/win/nvidia-amd-cpu/20

/*
 * Thread configuration for each thread. Make sure it matches the number above.
 * low_power_mode - This can either be a boolean (true or false), or a number between 1 to 5. When set to true,
 *                  this mode will double the cache usage, and double the single thread performance. It will
 *                  consume much less power (as less cores are working), but will max out at around 80-85% of
 *                  the maximum performance. When set to a number N greater than 1, this mode will increase the
 *                  cache usage and single thread performance by N times.
 *
 * no_prefetch    - Some systems can gain up to extra 5% here, but sometimes it will have no difference or make
 *                  things slower.
 *
 * asm            - Allow to switch to a assembler version of cryptonight_v8; allowed value [auto, off, intel_avx, amd_avx]
 *                    - auto: xmr-stak will automatically detect the asm type (default)
 *                    - off: disable the usage of optimized assembler
 *                    - intel_avx: supports Intel cpus with avx instructions e.g. Xeon v2, Core i7/i5/i3 3xxx, Pentium G2xxx, Celeron G1xxx
 *                    - amd_avx: supports AMD cpus with avx instructions e.g. AMD Ryzen 1xxx and 2xxx series
 *
 * affine_to_cpu  - This can be either false (no affinity), or the CPU core number. Note that on hyperthreading
 *                  systems it is better to assign threads to physical cores. On Windows this usually means selecting
 *                  even or odd numbered cpu numbers. For Linux it will be usually the lower CPU numbers, so for a 4
 *                  physical core CPU you should select cpu numbers 0-3.
 *
 * On the first run the miner will look at your system and suggest a basic configuration that will work,
 * you can try to tweak it from there to get the best performance.
 *
 * A filled out configuration should look like this:
 * "cpu_threads_conf" :
 * [
 *      { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 0 },
 *      { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 1 },
 * ],
 * If you do not wish to mine with your CPU(s) then use:
 * "cpu_threads_conf" :
 * null,
 */

"cpu_threads_conf" :
[
    { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 0 },
    { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 1 },
    { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 2 },
    { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 4 },
    { "low_power_mode" : false, "no_prefetch" : true, "asm" : "auto", "affine_to_cpu" : 6 },

],
```

Windows GPU config file:

```
// generated by xmr-stak/2.6.0/871371622/master/win/nvidia-amd-cpu/20

/*
 * GPU configuration. You should play around with threads and blocks as the fastest settings will vary.
 * index         - GPU index number usually starts from 0.
 * threads       - Number of GPU threads (nothing to do with CPU threads).
 * blocks        - Number of GPU blocks (nothing to do with CPU threads).
 * bfactor       - Enables running the Cryptonight kernel in smaller pieces.
 *                 Increase if you want to reduce GPU lag. Recommended setting on GUI systems - 8
 * bsleep        - Insert a delay of X microseconds between kernel launches.
 *                 Increase if you want to reduce GPU lag. Recommended setting on GUI systems - 100
 * affine_to_cpu - This will affine the thread to a CPU. This can make a GPU miner play along nicer with a CPU miner.
 * sync_mode     - method used to synchronize the device
 *                 documentation: http://docs.nvidia.com/cuda/cuda-runtime-api/group__CUDART__DEVICE.html#group__CUDART__DEVICE_1g69e73c7dda3fc0
 *                 0 = cudaDeviceScheduleAuto
 *                 1 = cudaDeviceScheduleSpin - create a high load on one cpu thread per gpu
 *                 2 = cudaDeviceScheduleYield
 *                 3 = cudaDeviceScheduleBlockingSync (default)
 * mem_mode      - select the memory access pattern (this option has only a meaning for cryptonight_v8 and monero)
 *                 0 = 64bit memory loads
 *                 1 = 256bit memory loads
 *
 * On the first run the miner will look at your system and suggest a basic configuration that will work,
 * you can try to tweak it from there to get the best performance.
 *
 * A filled out configuration should look like this:
 * "gpu_threads_conf" :
 * [
 *     { "index" : 0, "threads" : 17, "blocks" : 60, "bfactor" : 0, "bsleep" :  0,
 *       "affine_to_cpu" : false, "sync_mode" : 3, "mem_mode" : 1
 *     },
 * ],
 * If you do not wish to mine with your nVidia GPU(s) then use:
 * "gpu_threads_conf" :
 * null,
 */

"gpu_threads_conf" :
[
  // gpu: GeForce GTX 760 architecture: 30
  //      memory: 1673/2048 MiB
  //      smx: 6
  { "index" : 0,
    "threads" : 16, "blocks" : 18,
    "bfactor" : 8, "bsleep" :  25,
    "affine_to_cpu" : false, "sync_mode" : 3,
    "mem_mode" : 1,
  },

],
```

Windows pools config file:

```
// generated by xmr-stak/2.6.0/871371622/master/win/nvidia-amd-cpu/20

/*
 * pool_address    - Pool address should be in the form "pool.supportxmr.com:3333". Only stratum pools are supported.
 * wallet_address  - Your wallet, or pool login.
 * rig_id          - Rig identifier for pool-side statistics (needs pool support).
 * pool_password   - Can be empty in most cases or "x".
 * use_nicehash    - Limit the nonce to 3 bytes as required by nicehash.
 * use_tls         - This option will make us connect using Transport Layer Security.
 * tls_fingerprint - Server's SHA256 fingerprint. If this string is non-empty then we will check the server's cert against it.
 * pool_weight     - Pool weight is a number telling the miner how important the pool is. Miner will mine mostly at the pool
 *                   with the highest weight, unless the pool fails. Weight must be an integer larger than 0.
 *
 * We feature pools up to 1MH/s. For a more complete list see M5M400's pool list at www.moneropools.com
 */

"pool_list" :
[
{"pool_address" : "pool.supportxmr.com:3333", "wallet_address" : "", "rig_id" : "Metagross", "pool_password" : "", "use_nicehash" : false, "use_
],

/*
 * Currency to mine. Supported values:
 *
 *    aeon7 (use this for Aeon's new PoW)
 *    bbscoin (automatic switch with block version 3 to cryptonight_v7)
 *    bittube (uses cryptonight_bittube2 algorithm)
 *    graft
 *    haven (automatic switch with block version 3 to cryptonight_haven)
 *    intense
 *    masari
 *    monero (use this to support Monero's Oct 2018 fork)
 *    qrl - Quantum Resistant Ledger
 *    ryo
 *    turtlecoin
 *
 * Native algorithms which not depends on any block versions:
 *
 *    # 1MiB scratchpad memory
 *    cryptonight_lite
 *    cryptonight_lite_v7
 *    cryptonight_lite_v7_xor (algorithm used by ipbc)
 *    # 2MiB scratchpad memory
 *    cryptonight
 *    cryptonight_v7
 *    cryptonight_v8
 *    # 4MiB scratchpad memory
 *    cryptonight_bittube2
 *    cryptonight_haven
 *    cryptonight_heavy
 */

"currency" : "monero",
```