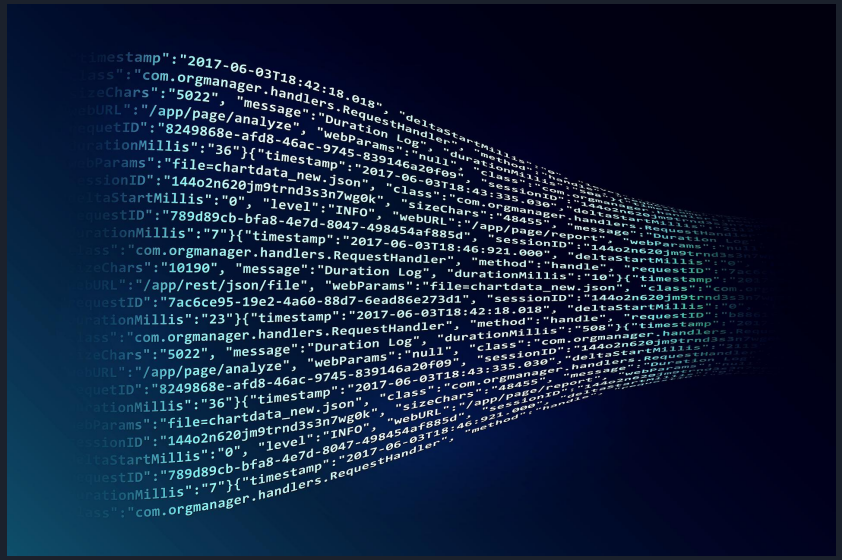
MineSweeper

Drive-by Cryptocurrency Mining and its Defences

Jordan Foss - 45302282
Isaac Flower - 45814945
Jak Blashki - 46415059

Introduction of Cryptomining

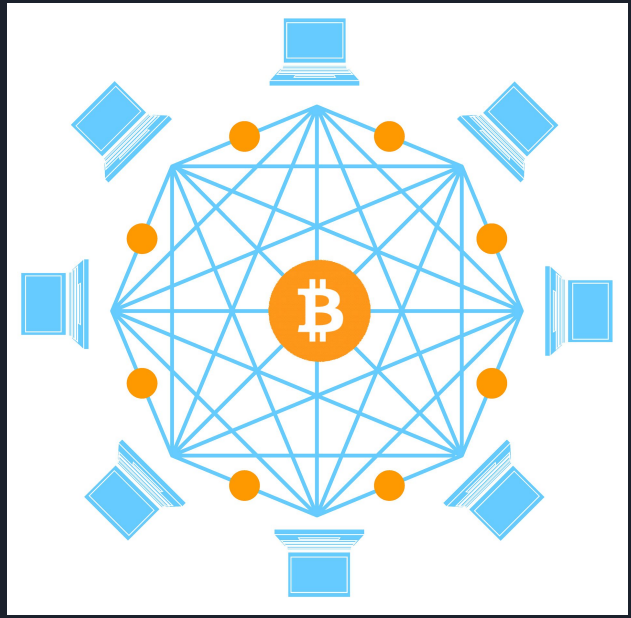
- Blockchain is used to keep track of all the transactions
- Currency is earned by adding blocks to said blockchain
- Adding a block requires the miner to solve a cryptographic puzzle based on the block
- Puzzles provide artificial scarcity to the currency and stop malicious entities
- This form of mining validation is known as Proof-of-Work (PoW)



https://pixabay.com/illustrations/analytics-information-innovation-3088958/

Mining Pools

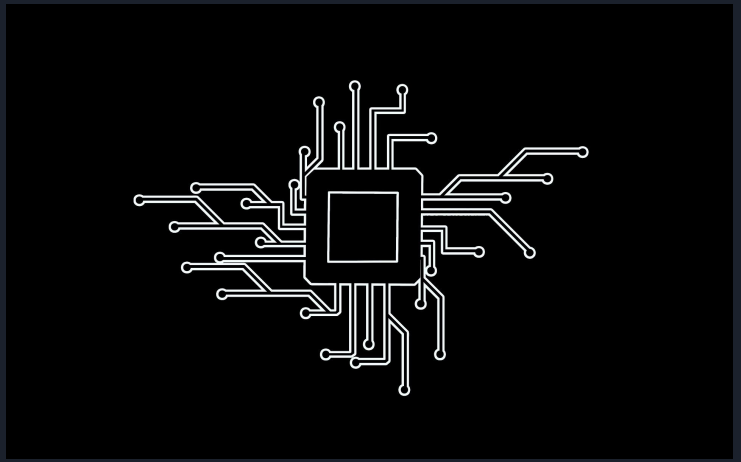
- Miners normally work on puzzles in groups of miners called mining pools
- Rewards are shared in the pool when a puzzle is solved
- Allows for systems with little computation power to help
- Protocol for communication with pool is Stratum
- Stratum allows for any system to easily connect to a mining pool



https://pixabay.com/illustrations/bitcoin-cryptocurrency-money-3012035/

CPUs are Trash

- CPUs are not profitable for mining most currencies
- Monero however uses an algorithm where CPUs are more efficient due to memory requirements
- Drive-by mining exclusively uses the CPU



https://pixabay.com/illustrations/chip-processor-icon-circuit-6399681/

Why Monero?

- During time of publication, Monero used the CryptoNight algorithm
- CryptoNight favours mining done on CPUs, while resisting mining done on ASICs
- Wallet lookup is not possible in Monero, providing more privacy to the users
- Monero aims to be a crypto mineable for any user and tries to be truly decentralized

https://pixabay.com/photos/bitcoin-number-metallic-metal-3090250/

Introduction of Browser Based Mining

- Various services, such as CoinIMP and formerly Coinhive, offer a browser based mining API as an alternative to ads
- Service is not inherently malicious, but is easily abused
- As it uses CPU time, the only profitable coin to mine is Monero, using the CryptoNight algorithm

https://pixabay.com/illustrations/browser-web-www-computer-773215/

Drive-by Mining

- More profit the longer the miner is allowed to run (time on webpage)
- Evasion tactics are used, such as pop-under windows and video streamer, in order to maximise mining time
- Not necessarily the fault of the website owners

https://pixabay.com/illustrations/youtube-earning-subscription-movie-5061859/

Past Defences and Why they are not Reasonable

- Blacklisting URLs is easily evaded with URL randomisation
- CPU load monitoring is easily evaded with CPU throttling
- CPU load monitoring also results in false positives with other CPU intensive tasks, such as games

https://pixabay.com/photos/the-main-processor-bitcoin-intel-3286065/

Introducing MineSweeper

- Checked Alexa's Top 1 Million websites to find examples of drive-by mining
- Used websocket frame log data to identify communication to a mining pool using Stratum
- Detects drive-by mining by identifying the CryptoNight Algorithm via static and dynamic analysis
- Paper found that drive-by mining was earning some attackers $30,000 USD per month

MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense

Radhesh Krishnan Konoth
Vrije Universiteit Amsterdam
r.k.konoth@vu.nl

Emanuele Vineti
Vrije Universiteit Amsterdam
emanuele.vineti@gmail.com

Veelasha Moonsamy
Utrecht University
email@veelasha.org

Martina Lindorfer
TU Wien
martina@iseclab.org

Christopher Kruegel
UC Santa Barbara
chris@cs.ucsb.edu

Herbert Bos
Vrije Universiteit Amsterdam
herbertb@cs.vu.nl

Giovanni Vigna
UC Santa Barbara
vigna@cs.ucsb.edu

ABSTRACT

A wave of alternative coins that can be effectively mined without specialized hardware, and a surge in cryptocurrencies' market value has led to the development of cryptocurrency mining (*cryptomining*) services, such as Coinhive, which can be easily integrated into websites to monetize the computational power of their visitors. While legitimate website operators are exploring these services as an alternative to advertisements, they have also drawn the attention of cybercriminals: *drive-by mining* (also known as *cryptojacking*) is a new web-based attack, in which an infected website secretly executes JavaScript code and/or a WebAssembly module in the user's browser to mine cryptocurrencies without her consent.

In this paper, we perform a comprehensive analysis on Alexa's Top 1 Million websites to shed light on the prevalence and profitability of this attack. We study the websites affected by drive-by mining to understand the techniques being used to evade detection, and the latest web technologies being exploited to efficiently mine cryptocurrency. As a result of our study, which covers 28 Coinhive-like services that are widely being used by drive-by mining websites, we identified 20 active cryptomining campaigns.

Motivated by our findings, we investigate possible countermeasures against this type of attack. We discuss how current blacklisting approaches and heuristics based on CPU usage are insufficient, and present MineSweeper, a novel detection technique that is based on the intrinsic characteristics of cryptomining code, and, thus, is resilient to obfuscation. Our approach could be integrated into browsers to warn users about silent cryptomining when visiting websites that do not ask for their consent.

CCS CONCEPTS

• **Security and privacy** → **Browser security**; **Malware and its mitigation**; • **Social and professional topics** → *Computer crime*;

KEYWORDS

cryptocurrency; mining; cryptojacking; drive-by attacks; malware

CCS '18, October 15–19, 2018, Toronto, ON, Canada

ACM ISBN 978-1-4503-5693-0/18/10…$15.00
https://doi.org/10.1145/3243734.3243858

ACM Reference Format:
Radhesh Krishnan Konoth, Emanuele Vineti, Veelasha Moonsamy, Martina Lindorfer, Christopher Kruegel, Herbert Bos, and Giovanni Vigna. 2018. MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense. In *CCS '18: 2018 ACM SIGSAC Conference on Computer & Communications Security Oct. 15–19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3243734.3243858

1 INTRODUCTION

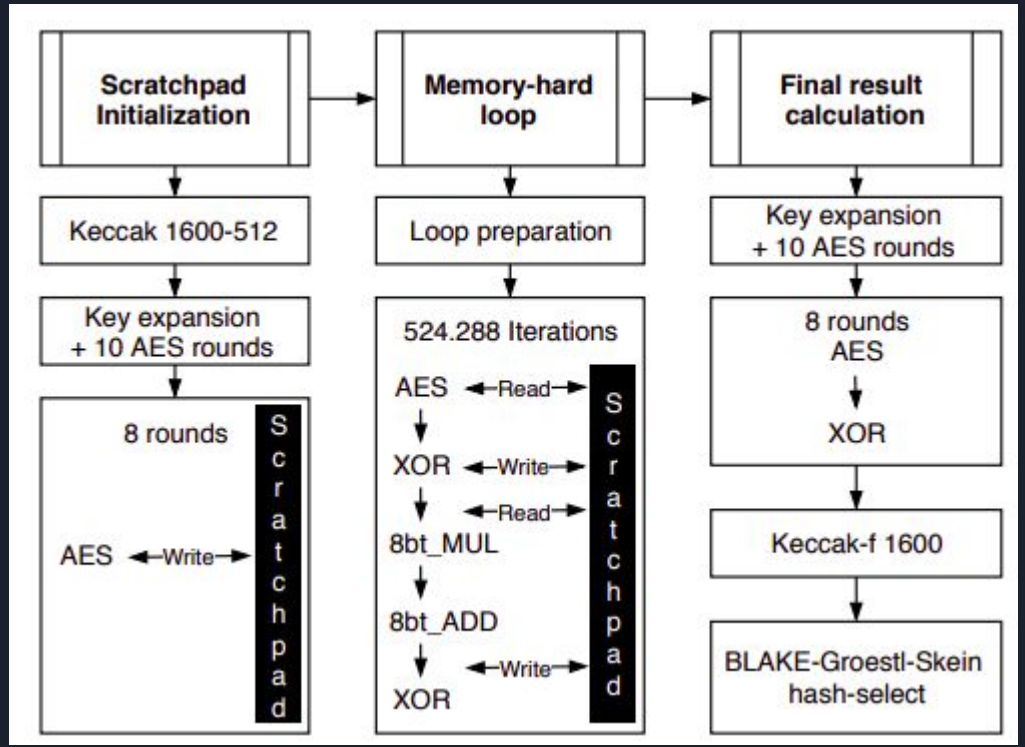
Ever since its introduction in 2009, Bitcoin [47] has attracted the attention of cybercriminals due to the possibility to perform and receive anonymous payments. In addition, the financial reward for using computing power for mining has incentivized criminals to experiment with *silent* cryptocurrency miners (*cryptominers*), which gained popularity among malware authors who were, after all, already in the business of compromising PCs and herding large numbers of them in botnets. However, as Bitcoin mining became too difficult for regular machines, the profits of mining botnets dwindled, and Bitcoin-mining botnets declined: an analysis by McAfee in 2014 suggested that malicious miners are not profitable on PCs and certainly not on mobile devices [37].

Since then, a wave of alternative coins (altcoins) has been introduced: the market now counts over 1,500 cryptocurrencies, out of which more than 600 see an active trade. At the time of writing, they represent over 50% of the cryptocurrency market [24]. Unlike Bitcoin, many of them are still mineable without specialized hardware. Furthermore, miners can organize themselves into *mining pools*, which allow members to distribute mining tasks and share the rewards. These new currencies, and an overall surge in market value across cryptocurrencies at the end of 2017 [26], has renewed interest in cryptominers and led to the proliferation of cryptomining services, such as Coinhive [5], which can easily be integrated into a website to mine on its visitors' devices from within the browser.

For cybercriminals, these services provide a low-effort way to monetize websites as part of *drive-by mining* (or *cryptojacking*) attacks: they either compromise webservers (through exploits [15, 39, 50, 62, 65], or taking advantage of misconfigurations [49]) and install JavaScript-based miners, distribute their miners through advertisements (including Google's DoubleClick on YouTube [28] and the AOL advertising platform [41]), or compromise third-party libraries [71] included in numerous websites. Attackers also have come up with creative tactics to conceal their attack, for example

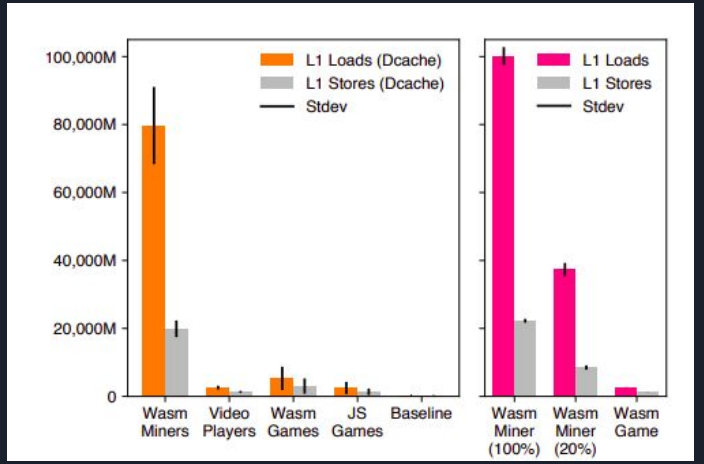
How CryptoNight Algorithm Works and How Minesweeper can Detect it

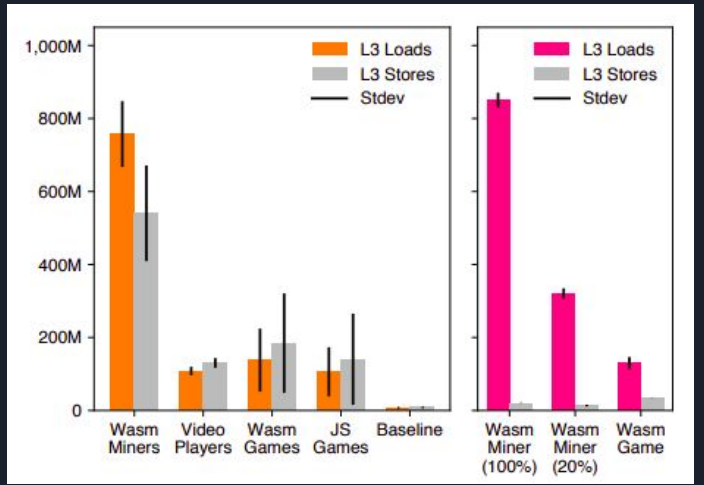
- CryptoNight uses five cryptographic primitives
- MineSweeper identifies whether any of these primitives are present in the Wasm module by means of fingerprinting.
- CryptoNight must use all of these primitives in order to compute a correct hash
- MineSweeper can also detect payload implementation split across modules.



How CPU Data Caches Work and how Minesweeper can Monitor Them

- CPUs have some amount of internal memory stored in the L1, L2 and L3 caches
- CryptoNight requires about 2 MB of fast memory per instance for efficient mining
- 2 MB doesn't fit in L1 or L2 cache, but does fit in L3
- ASICs and GPUs don't have the memory speeds required
- Graphs show that WASM miners take significantly more stores than other browser based CPU applications





Results from Paper on the Effectiveness of MineSweeper

- Successfully detected all mining websites that were found
- No false positives or false negatives
- Performed significantly better than past protection of CoinBlockerList and Dr. Mine
- MineSweeper could be avoided by heavily throttling CPU usage and code obfuscation, however this would result in less profits to the point where it is not worth the effort
- Miners were checked for on 3 random pages with a 4 second wait time, so paper may have missed some sites

https://pixabay.com/vectors/speedometer-speed-automobile-icon-1970476/

Future areas of Study

- Detection on mobile devices should be investigated
- asm.js payloads should be investigated
- Knowledge from MineSweeper could be applied to other forms of crypto-jacking, i.e infected routers

https://pixabay.com/illustrations/smartphone-app-news-web-internet-1184883/

Developments Since The Paper

- Coinhive has shut down due to Monero changing it's algorithm from Cryptonight to RandomX and a significant drop in the value of Monero
- Some services are still open, such as CoinImp, however drive-by mining is significantly less popular today
- Lack of popularity is due to its poor profit margins

https://pixabay.com/vectors/chart-arrow-businessman-stock-6164414/

Any Questions?

Thank you for listening