# 

# 

**Cryptojacking**

Cloud Computing

Maurici Abad

Mohamed Chait

Agustín D'Acunto

Meir Mouyal

March 22nd of 2019

Facultat d’Informàtica de Barcelona

Universitat Politècnica de Catalunya

Index

[**1. Introduction**](#_35syjopf1f8p) **2**

[1.1 What is cryptojacking?](#_pidj2o2rpwcf) 2

[1.2 What is the relation to Cloud Computing?](#_c1t5uujwle41) 2

[**2. Context**](#_kib3wkf6ayi2) **3**

[2.1 What are Cryptocurrencies?](#_1vsbfkrzooh1) 3

[**3. Cryptojacking**](#_imyp5k1yw390) **4**

[3.1 File-based cryptojacking](#_bkgx70gvldah) 4

[3.1.1 WannaMine](#_fcewodk6csff) 4

[3.1.2 Smominru](#_4x7ubb4nhlnb) 4

[3.2 Web-based cryptojacking](#_xi22opv6kich) 5

[**4. Impact of cryptojacking**](#_n7bxzo6aoppc) **7**

[4.1 Earnings](#_scvrgrlaulja) 7

[4.2 Consequences for victims](#_o0xiz9lwf4ny) 7

[**5. Detection and mitigation**](#_c66z62h6020n) **8**

[5.1 Detection](#_vude04khm0zh) 8

[5.2 Mitigation](#_12vw8bm643nv) 8

[**6. Future of Cryptojacking**](#_z6nr1ea8bhhs) **9**

[**7. Conclusion**](#_k295hwdwt8y3) **9**

[**8. References**](#_d74xskw5lvqx) **10**

**Presented in class by**

Meir Mouyal

Mohamed Chait

# 1. Introduction

## 1.1 What is cryptojacking?

Cryptojacking is an emerging online threat with the possibility of compromising all kind of devices with an internet connection [1]. It is defined as “*the secret use of your computing device to mine cryptocurrency*”.

Hackers use cryptojacking to steal computing resources from their victims devices. Like most malicious attacks, the motive is profit, but unlike many other types of malware, cryptojacking does not damage the victims device data. Nevertheless, slows the computers performance by stealing CPU resources, which can be annoying for an individual user, and for larger organizations quite expensive due to electricity costs.

Cryptojacking is also known as malicious cryptomining, and its main feature is the ability to remain hidden in the victim’s computer or mobile device while it uses the machine’s resources to mine cryptocurrencies[3].  
Is a relatively new threat, but due to its effectiveness it has become one of the most common cyber threats nowadays. In fact, criminals even seem to prefer cryptojacking to ransomware due to its invisibility and high profits[2].

## 1.2 What is the relation to Cloud Computing?

Cloud Computing is “*the the use of various services, such as software development platforms, servers, storage and software, over the internet*”. Nowadays the whole internet is based on Cloud Computing, especially due to accessibility and hosting purposes [4].

Cloud Computing is fundamental for cryptocurrencies to exist, which are what makes cryptojacking possible through network services, therefore, cryptojacking works by taking advantage of Cloud Computing. This advantage is based on fog computing, which is the usage of small computers to collaborate to fulfill tasks, as cryptojacking does.

Cryptojacking is achieved through Cloud Computing in 2 ways, which will be explained later on with more detail:

1. secretly installing a program in the victim's computer.
2. in-browser cryptojacking, which doesn’t require any program being installed.

# 2. Context

## 2.1 What are Cryptocurrencies?

Cryptocurrencies are forms of digital money that exist solely within the online world, with no actual physical form. Unlike ancient currencies, cryptocurrencies were created as an alternative to traditional money, where there is no government oversight or central regulator. They gained popularity for their innovative design, growth potential and anonymity. The first and most successful cryptocurrency to appear was Bitcoin, which came out in December of 2009.

The words “cryptography” and “currency” combine to make “cryptocurrency”, considering its principles are based of complex mathematical encryption and that it is electronic money. As a result of cryptocurrencies not depending on a government or bank, all cryptocurrencies exist as encrypted decentralized monetary units, freely transferable between network participants.

In order to be trustworthy, cryptocurrency databases uses encryption to control the creation of new coins and verify the transfer of funds. To keep the cryptocurrency active with the creation of new coins, the concept of mining was created. Mining is a method which basically turns computing resources into cryptocurrency coins.

At first, anyone with a computer could mine cryptocurrency, however the complexity of the encrypted problem calculations steadily increased over time, becoming costly in computing power. Therefore, as an incentive for those who sacrifice the time and their computer resources to maintain the network and create new coins, the miner who first solves the encrypted problem receives a reward, usually some amount of new cryptocoin.

Since there existed a way to generate profit, this method became a race for miners. But miners quickly discovered that even high-end computers with powerful processors could not mine profitably enough to cover the costs involved. To remain competitive, miners ramped up to assembling large farms of computers with dedicated hardware for mining cryptocurrencies.

Nevertheless, hackers realized a new opportunity to generate profit, secretly taking advantage of the victim’s computers to mine cryptocurrency, which is known as cryptojacking.

# 3. Cryptojacking

Cryptocurrencies can be mined on personal computers using either file-based miners or browser-based miners.

The primary cryptocurrency mined by these cryptojacking miners is Monero, because the popular one’s Bitcoin requires special equipment that have a lot of processing power to mine. So it’s not viable to mine Bitcoin with regular computers.

## 3.1 File-based cryptojacking

This type of cryptojacking needs to be installed in the machine to start mining cryptocurrencies. Involves downloading and running an executable file.

File-based cryptojacking malware works very much just like regular malware. It’s loaded directly onto a device and runs quietly in the background. This type of cryptojacking is typically used for highly targeted attacks.

The most popular threat of this type of cryptojacking were WannaMine and Smominru.

### 3.1.1 WannaMine

Derives its name from the Wannacry ransomware that infected more than 360.000 computers over the world in 2017 [5]. It used the Eternal Blue exploit for Windows from the NSA.

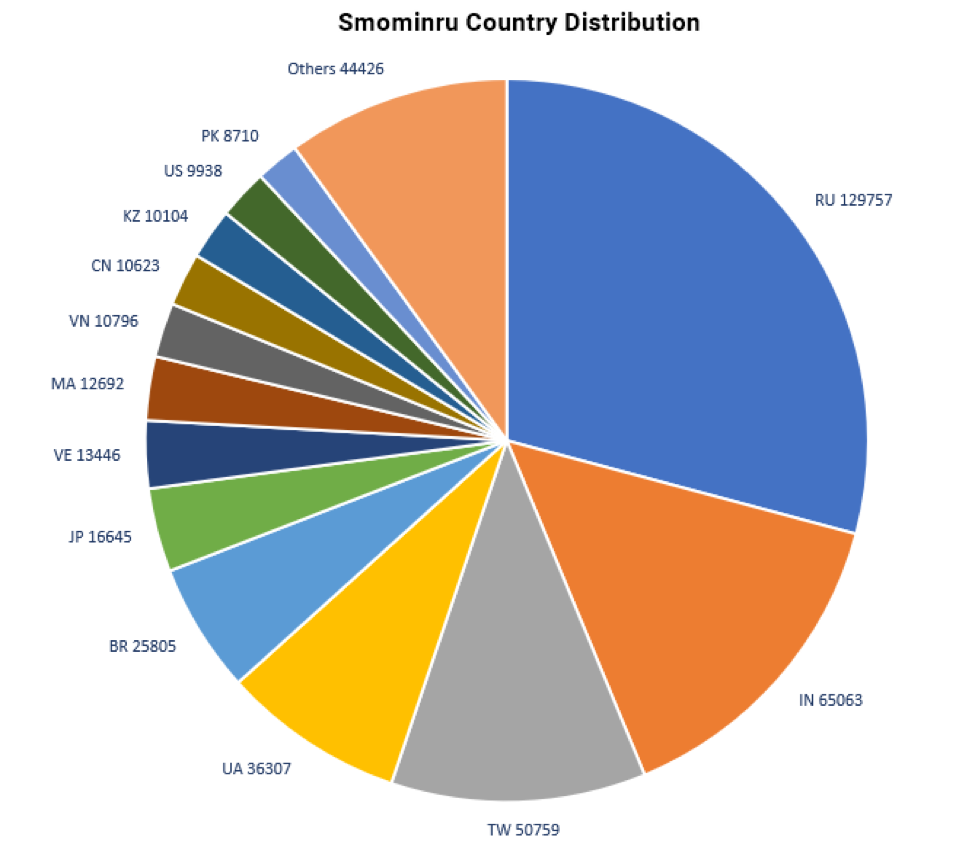
WannaMine was reported in October 2017, it can infect a computer with many techniques, it can use an infected website or mail link, and other malware tactics, such as exploits and credential stealers, to maintain persistence and propagate it to other computers on the network.

Since it was discovered in October 2017, WannaMine has infected more than 75,000 devices[6].

### 3.1.2 Smominru

The Smominru miner botnet turns infected machines into miners of the cryptocurrency Monero, according to research carried out by cybersecurity firm Proofpoint [7].It used the same exploit as Wannacry and WannaMine, the EthernalBlue exploit created by the NSA and leaked by a group of hackers called Shadow Brockers.

It apparently began operating in May of 2017 and has made its owners more than $3.5 millions since it was established. The botnet is resilient and has remained despite major efforts to take it down. Proofpoint said the botnet includes more than 526,000 infected Windows hosts or nodes, most of which are believed to be servers. In terms of the global distribution of said nodes, the highest instances are in Russia, India and Taiwan as we can see in the figure 1.



*Figure 1, Smominru Country distribution*

## 

## 3.2 Web-based cryptojacking

In-browser mining (or cryptojacking) is a hidden mining strategy that has become very popular in recent times. When a user visits a webpage, a mining code starts running in the background, and it continues while you are in the site.

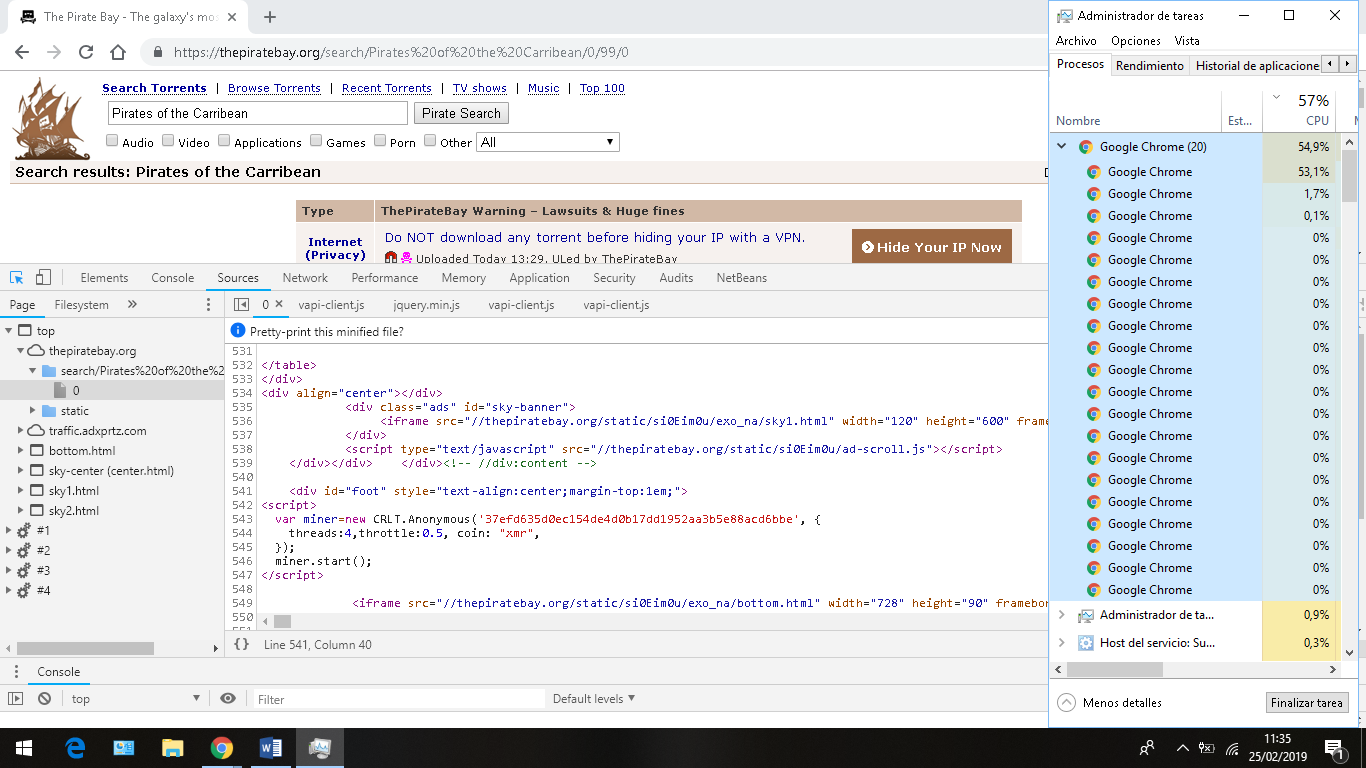
Several companies produce and support technological solutions for building mining scripts into a website with a Javascript API that can be easily integrated. The website owners can use this as an alternative of the ads.

Moreover, websites often conduct cryptocurrency mining without explicit user content.

The best-known mining solution provider is CoinHive. Besides them, there's Crypto-Loot, JSEcoin, Coin Have, PPoi (works with Chinese websites), and several others[8].

In April 2018, Hong et al. [9], conducted a study on the Alexa top 100k websites searching for website that used mining scripts to get revenue.They found 868 infected websites with mining scripts. They found that the popular website ThePirateBay was using the Coinhive scripts.They calculated the revenue of this site with the visitors per month (211.47M) and the average duration (326s) of the users in the site. Finally, they found that the PirateBay gets 1095$ per month using this scripts.

In the next figure we can see a real example of cryptojacking. It was using the 50% of the CPU to mine while i was in ThePirateBay website cryptocurrencies. The Javascript code specifies the id of the website, the throttle (0.5) , threads(4) and coin (Monero) that is mining.



*Figure 1,ThePirateBay website mining cryptocurrency.*

# 4. Impact of cryptojacking

## 4.1 Earnings

From the 2 ways of achieving cryptojacking, the most effective way hackers can generate profit is through file-based mining.

While file-based mining is harder to accomplish, it ensures a much higher income. This is due to that every second that the victim is using its computer it benefits the hacker, since he can keep taking advantage of his computational power.

Instead browser-based mining is much easier to perform, but since it only takes advantage of the time the victim is visiting the cryptojacking website, the revenue is quite smaller than when applying file-based mining.

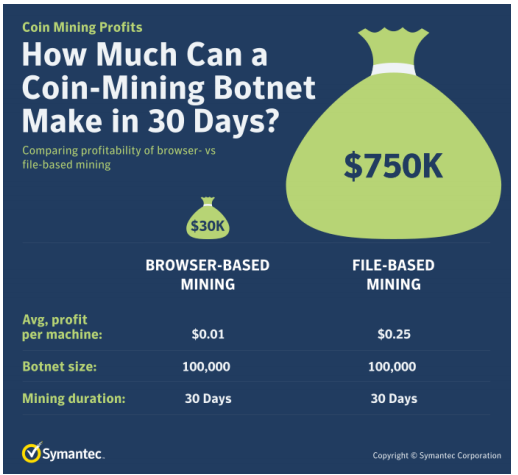


Figure 1, Profitability of browser-based vs file-based

## 4.2 Consequences for victims

As mentioned before, unlike ransomware, if you are a victim of cryptojacking, you may not notice. Cryptojacking’s main objective is to remain hidden from the victim.

Suffering this attacks means working with less computing resources due to that they are already being used to mine cryptocurrencies, therefore consuming extra CPU and battery life, slowing down your computer and increasing your electricity bills.

Some users might think that is better to suffer from cryptojacking than ransomware, but working with a slow computer can get really irritating, and also for big companies with lots of machinery the electricity cost can escalate quickly.

# 5. Detection and mitigation

## 5.1 Detection

Since Cryptojacking is made to remain hidden, sometimes it can get hard to detect. Even if it rises the CPU usage in the victim’s computer, depending on how subtle the attack is done, there might be left some trace.

Possible symptoms in the victim’s device:

* High processor usage on the victim’s device.
* Slow response times.
* Overheating.

Having any of these symptoms doesn’t guarantee your device is being cryptojacked, there are plenty other reasons as streaming online or downloading lots of data that would make your device to manifest these three indicators.

## 5.2 Mitigation

To this day there is no anti-cryptomining software that can ensure blocking all cryptojacking threats, specially once the device is already infected.

As with all other malware precautions, it’s much better to install security before you become a victim, therefore is highly important installing security software such as Norton Security or Malwarebytes to help prevent an attack[10].

In addition, is still recommended to have installed ad-blocking and anti-cryptomining extensions on web browsers such as *NoCoin* or *minerBlock* for extra layers of protection.

Even with all these layers of protection, the user should always be well informed about the topic and be sure to stay cautious of phishing emails, suspicious links and unknown attachments.

# 6. Future of Cryptojacking

The longevity of this activity very much depends on the future value of these cryptocurrencies.

The most used mining scripts is for Monero cryptocurrency.

In the last year, the price of Monero [XMR] has dropped. Monero was having a rough time over the last one month with allegations against Monero being used by criminals for money laundering and ransom. However, according to LongForecast, that is a forecasting agency which is specialized to predict the financial market, predicts that Monero might be in the range of $554-$638 in April 2020 [11]. In consequence, this will increase the cryptojacking to get revenue.

Another factor, is the creation of laws that outright bans the use of cryptocurrency.

“The Future of Digital Currency” was recently discussed by the House Financial Service Committee in the U.S. Congress, with one of the participants -Representative Brad Sherman- suggesting that “We should prohibit U.S. persons from buying or mining cryptocurrencies.”

Moreover, countries as China and India, have implemented laws cracking down on cryptocurrency trading.

# 7. Conclusion

In conclusion in this work , we introduced the problem of the cryptojacking and explained the emerging growth of this problem.

Then we explained the two types of cryptojacking, the file-based and the web-based. We explained the revenue and the impact in the users and enterprise machines of the two types of cryptojacking. We analyzed the detection and mitigation.

Finally we pointed out the future of this problem and the factors that can make spark the use of cryptojacking to obtain benefits.

# 

# 8. References

[1]Li, Ray, et al. “What Is Cryptojacking?” *Hacker Bits*, 25 Jan. 2018, hackerbits.com/programming/what-is-cryptojacking/.

[2]“Curated Directory of Cryptocurrency Resources.” *Cryptominded*, cryptominded.com/.

[3] “What Is Cryptojacking? How It Works and How to Help Prevent It.” *Norton Family Premier*, us.norton.com/internetsecurity-malware-what-is-cryptojacking.html.

[4]“What Is Cloud Computing? - Definition from Techopedia.” *Techopedia.com*, www.techopedia.com/definition/2/cloud-computing.

[5] A.m. “WannaCry Sigue Vivo: Casi 75.000 Usuarios En Todo Han Sido Infectados Por El Popular «Ransomware».” *Abc*, ABC.es, 23 Nov. 2018, www.abc.es/tecnologia/redes/abci-wannacry-sigue-vivo-casi-75000-usuarios-todo-sido-infectados-popular-ransomware-201811221644\_noticia.html.

[6]Symantec Community. “New Security Response Whitepaper: Cryptojacking: A Modern Cash Cow.” *Intelligent Systems Monitoring*, intelligentsystemsmonitoring.com/community/symantec-community/new-security-response-whitepaper-cryptojacking-a-modern-cash-cow/.

[7]“Smominru Monero Mining Botnet Making Millions for Operators.” *Proofpoint*, 27 Jan. 2019, www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators.

[8]“The State of Cryptojacking.” *The State of Cryptojacking*, crypto.adguard.com/.

[9] G. Hong, Z. Yang, S. Yang, L. Zhang, Y. Nan, Z. Zhang, M. Yang, Y. Zhang, Z. Qian, and H. Duan, “How You Get Shot in the Back: A Systematical Study about Cryptojacking in the Real World,” CCS ’18 (ACM Conf. Comput. Commun. Secur., p. 13, 2018.

[10]“Cryptojacking Definition – What Is It, and How Can You Prevent It?” *Malwarebytes*, www.malwarebytes.com/cryptojacking/.

[11] CoinSwitch. “Monero Price Prediction 2019 | XMR Price May Touch 500 USD In 2019.” *What Is Neblio - An Ultimate Guide on NEBL Crypto*, CoinSwitch, 4 Mar. 2019, coinswitch.co/news/monero-price-prediction-2019-xmr-price-may-touch-500-usd-in-2019.