October 2017

A look into the global ‘drive-by cryptocurrency mining’ phenomenon

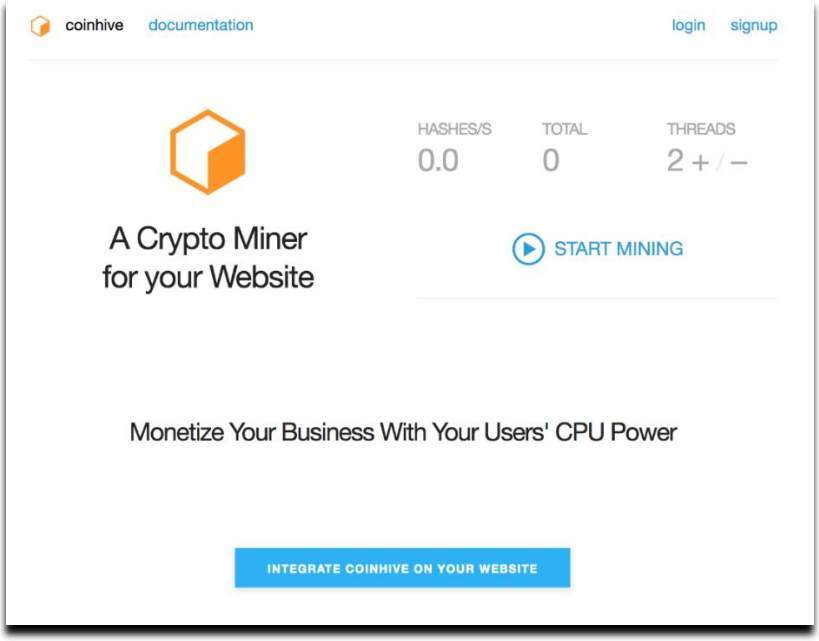
Jérôme Segura
Lead Malware Intelligence Analyst

Introduction

Contrary to traditional money, cryptocurrencies are not issued by a central bank or authority. Instead, this digital asset can be produced by "mining," a process that involves solving complex mathematical and cryptographic algorithms. Bitcoin is one of the most famous cryptocurrencies, but now requires exceptional computational power to be mined.

Cryptocurrencies were bound to trigger the interest of criminals and it wasn't long before coin mining malware made an appearance and addressed the scalability and resource-intensive process by enrolling as many bots as possible for the common effort.

Several other cryptocurrencies continued to come out, including Monero (XMR), which unlike Bitcoin, can be mined by average computers. Unsurprisingly, many malware authors jumped in to compromise new hosts to deliver Monero-based mining malware.



An important milestone in the history of cryptomining happened around mid-September when a company called Coinhive launched a service that could start mining for Monero directly within a web browser using a simple JavaScript library.

To differentiate browser-based mining from other previous forms, many started to label these instances as JavaScript Miners or Browser Miners.

Figure 1: Coinhive, a "Crypto Miner for your Website."

Now every website owner has the ability to monetize their content simply from users visiting their page. While the idea had a lot of merit, its implementation was a disaster and lead to immediate abuse.

Coinhive is not the only service that facilitates JavaScript mining, but it is by far the most popular, which is why we will focus on it in this paper.

From drive-by download to drive-by mining

"Drive-by download" is a term often used to describe web-based threats when a computer becomes infected by simply visiting a website, without any other interaction required.

In their heyday, exploit kits ruled the world of drive-by downloads and were feared by many, especially as they sometimes used zero-day vulnerabilities that caught software vendors by surprise, allowing to infect even the most up-to-date systems.

But as exploit kit activity dwindled, malware authors went for other distribution methods, which meant using more social engineering tricks.

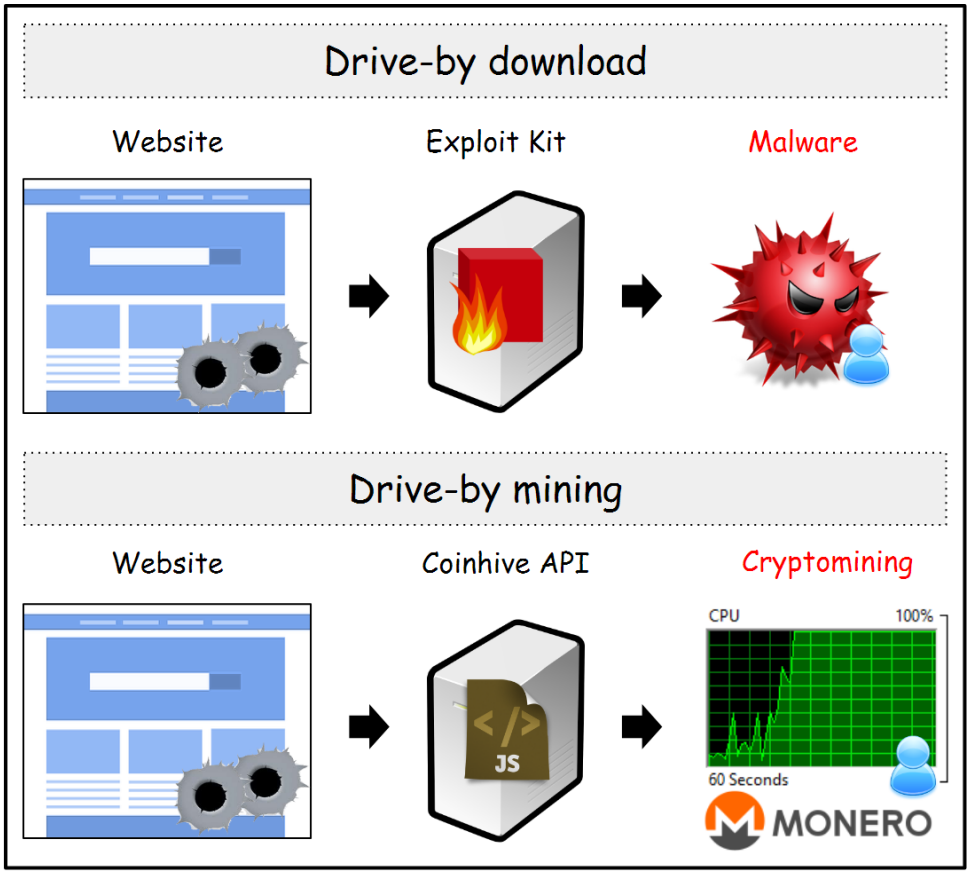


Figure 2: Diagram comparing drive-by download and drive-by mining.

Similar to drive-by-downloads, browser-based mining flourished almost overnight and was rolled out in such a way that users had no idea it was happening to them. Such was the case with The Pirate Bay, which started to turn visitors to its site into cryptocurrency miners without their knowledge or consent.

These incidents are also referred to as "cryptojacking", an interesting term that includes the notion of hijacking, which happens to be the computer resources of visitors.

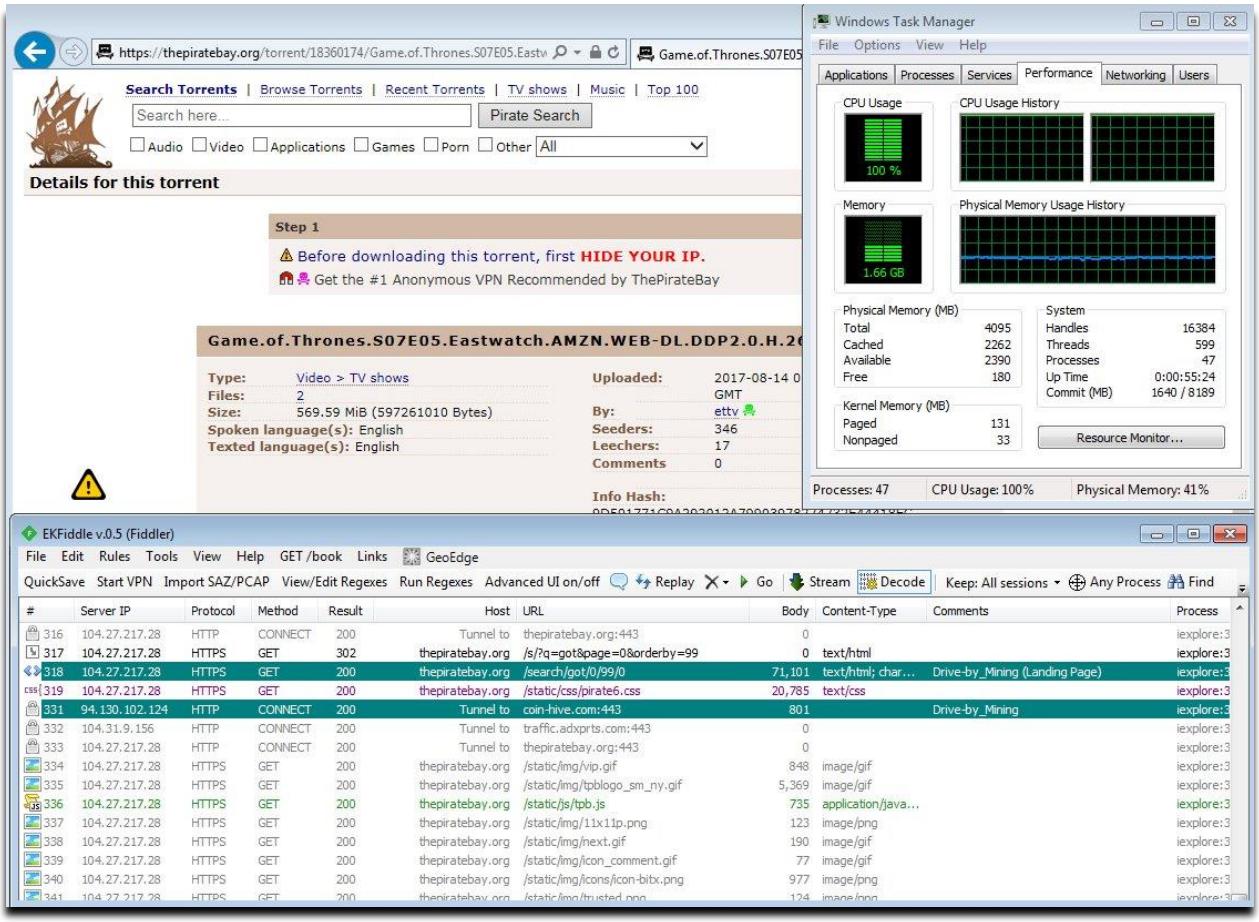


Figure 3: Popular Torrent site The Pirate Bay using visitors' CPU to mine Monero.

Unlike drive-by downloads that push malware, drive-by mining focuses on utilizing the processing power of visitors' computers to mine cryptocurrency. While both are automatic and silent processes, the early implementation of the Coinhive API allowed for abuse by running the code full throttle, therefore maxing out the users' CPU, as seen in Figure 3.

Just about any site

Any average computer – and even phone – can be used to produce certain kinds of digital currency. One of obvious signs of drive-by mining activity is a slow computer or a particularly warm device, which means the Coinhive API has not been configured properly and mining activity is taking too many system resources.

While there may not have been malicious intent in mind, this JavaScript-based cryptocurrency mining was released to the world before there was any proper discussion on how to use it responsibly.

Early adopters of the technology were torrent portals and video streaming websites that typically rely on aggressive ads to monetize their content. On those sites, pop unders and other delivery methods that are designed to bypass ad blockers are common place, showing a lack of respect for the visitor's web experience and safety. For this reason, the integration of web-based cryptomining (often times on top of existing ads) without any kind of warning, was not a big surprise.

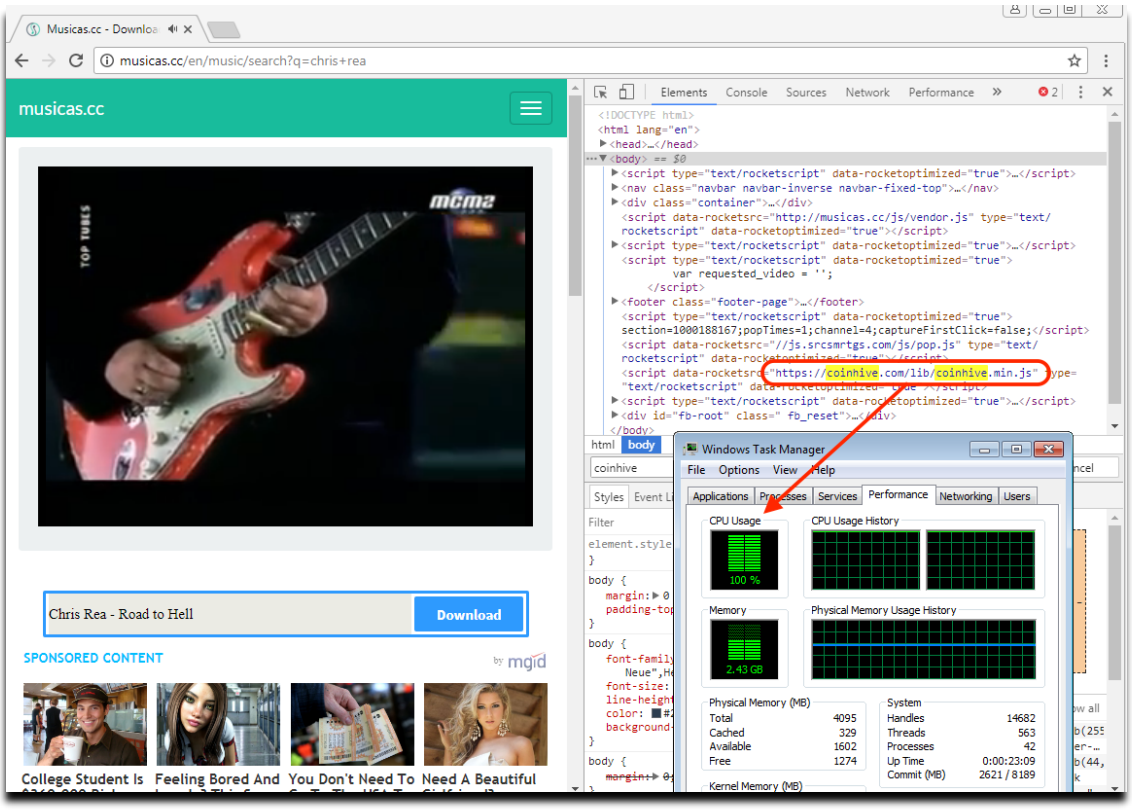


Figure 4: A video/music streaming site runs a miner in the background.

Ironically, in many cases the mining isn't only running unbeknownst to end users but also to site owners themselves. For instance, CBS's Showtime was reported as running a miner on its site for a brief period of time which resulted in some bad PR.

Additionally, web security company Sucuri has identified several campaigns affecting various platforms, including WordPress and Magento, where compromised sites are injected with mining code. Attackers are going to great lengths to obfuscate the payload and still rely on the original Coinhive API that does not require user approval to run.

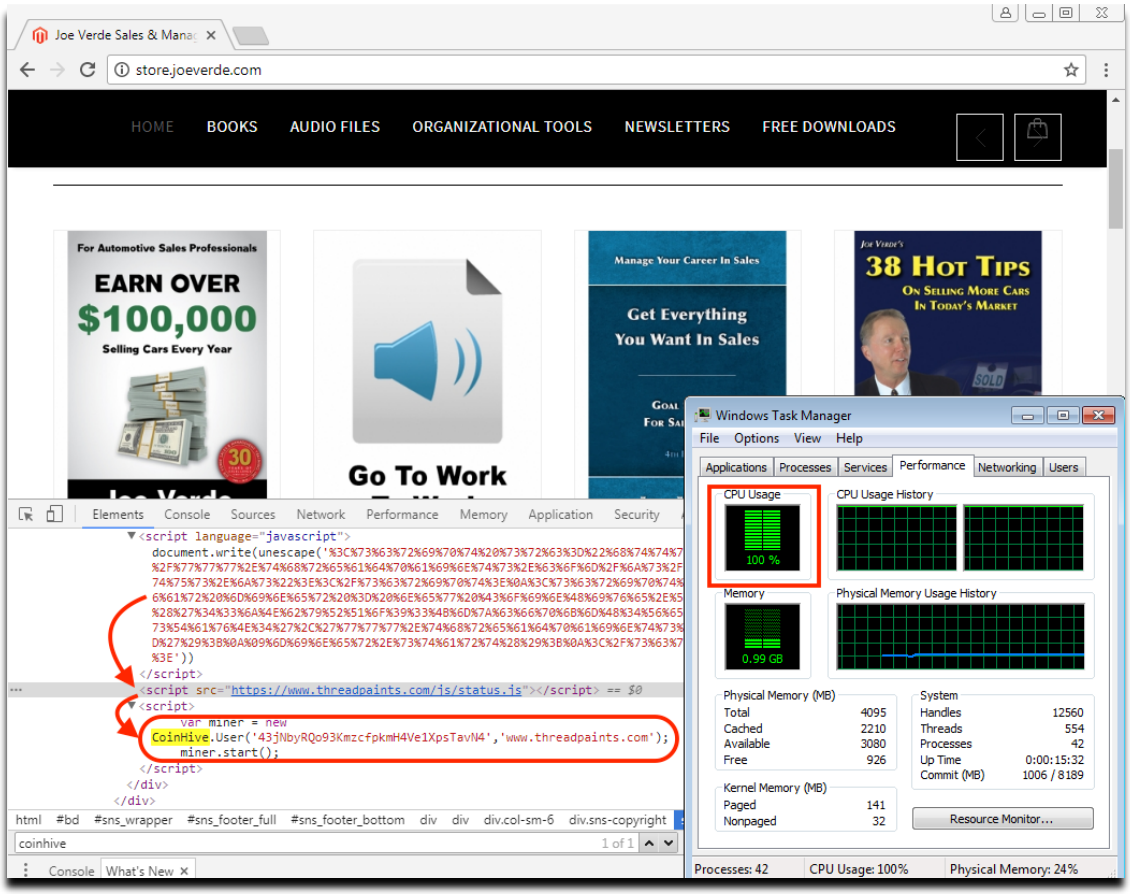


Figure 5: A compromised site has been injected with the Coinhive script.

On its own, a hacked site may not draw much traffic, but attackers can mass scan the web for vulnerabilities and compromise hundreds, or even thousands of sites at once. One way to connect those hacked sites together is by checking the Coinhive's site key they are using. If it is the same, it's likely that they are part of the same infection campaign.

In a few cases, threat actors are double dipping to deliver their intended payload but also inserting some cryptomining. For instance, rogue advertisers have used online ads to load the mining code surreptitiously in malvertising attacks.

There is also the case of tech support scammers that use browser lockers to scare victims into thinking they have a virus. The greedy scammers thought that silently mining while users are pondering what to do was a good idea.

With scale comes profit

Mining cryptocurrency requires resources as those computers consume electricity that comes out of your power bill. To be profitable, the mining activity must cost less than the power consumption it generates. According to SpiderLabs, mining in the US would add between about $2.90 to $5 per month to your electricity bill per machine.

What's interesting about drive-by mining is that it makes use of other people's machines and the more web traffic you can generate, the more chances you have of solving crypto challenges and get a payout. Imagine a website like *thepiratebay[.]org,* which brings in an estimated 282 million visitors a month who spend an average of 5 minutes on the site.

TorrentFreak ran some numbers based on a typical user with a mid-range laptop that would make for a hashrate of 30 h/s. The Pirate Bay would get 127.5 XMR per month, which was roughly $12,000 at the time the article was published.

Figure 6: Monero (XMR) versus US Dollars (USD) over time.

Forced miners from around the world

Ever since we started detecting and blocking Coinhive domains, we were astounded by the numbers. On average, we have been registering about 8 million blocks per day, preventing unauthorized drive-by mining onto our users.

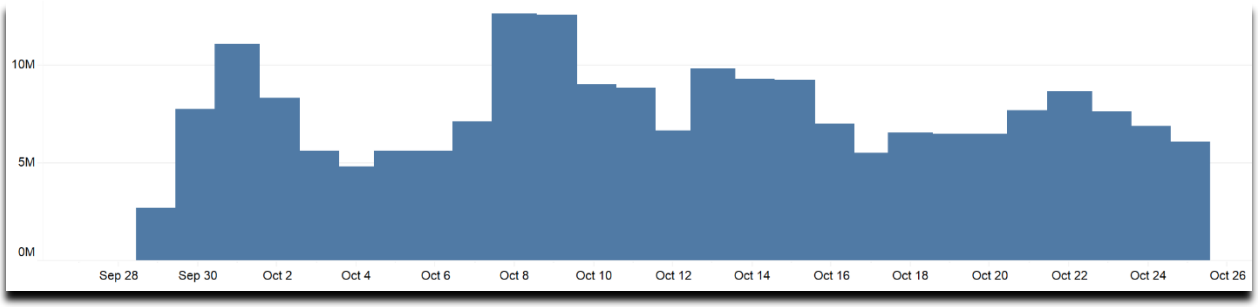


Figure 7: A month worth of blocks for Coinhive's domains and proxies (in millions).

The following maps and charts are based on telemetry data we collected for about a month since Coinhive's inception. We added up every time we blocked domains and proxies involved with drive-by mining and cross-referenced it with the user's country of origin.

World view

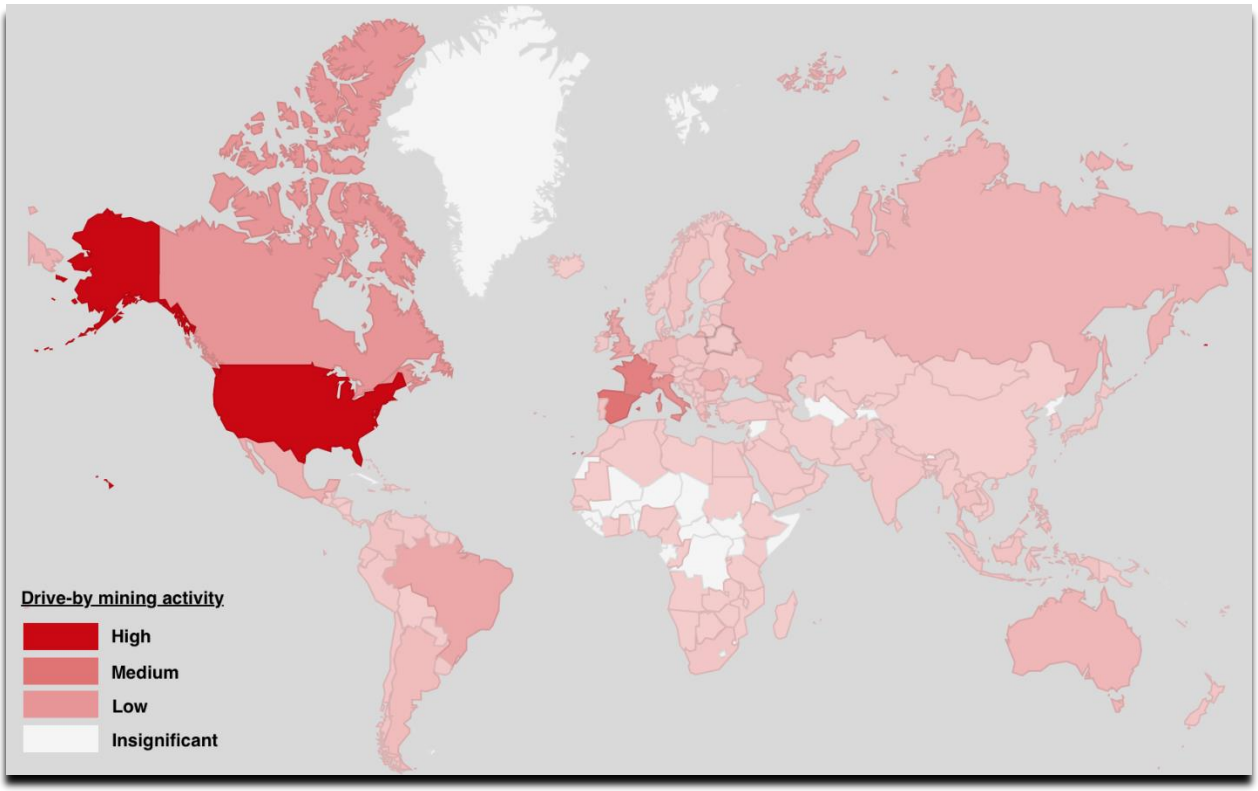


Figure 8: World view of blocked drive-by mining activity based on user geolocation.

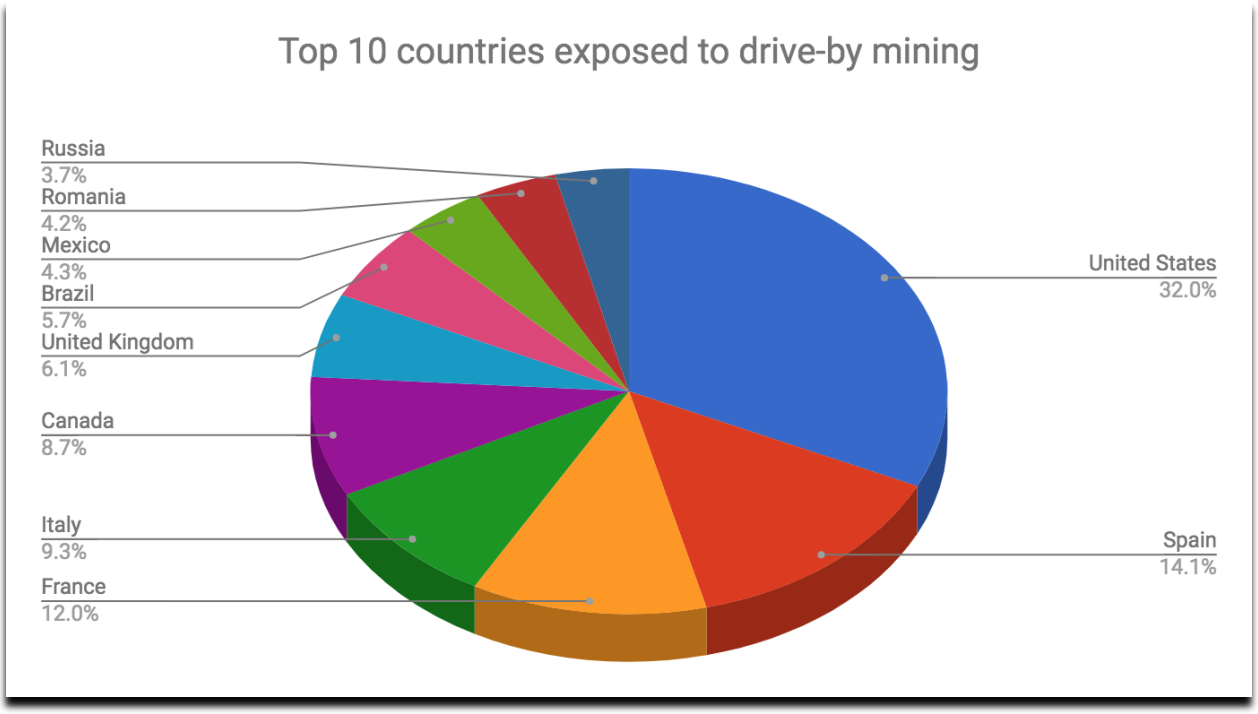


Figure 9: US and Spain top the list of countries most impacted by drive-by mining.

US map

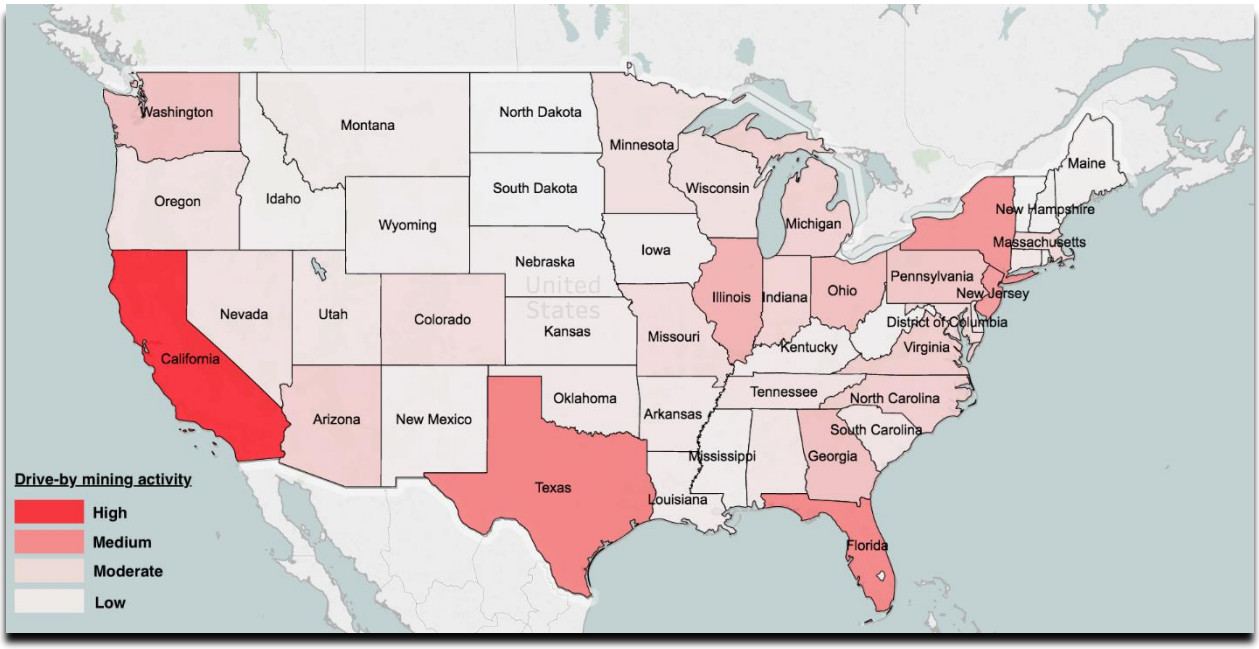


Figure 10: California, Florida, and Texas rank high for drive-by mining.

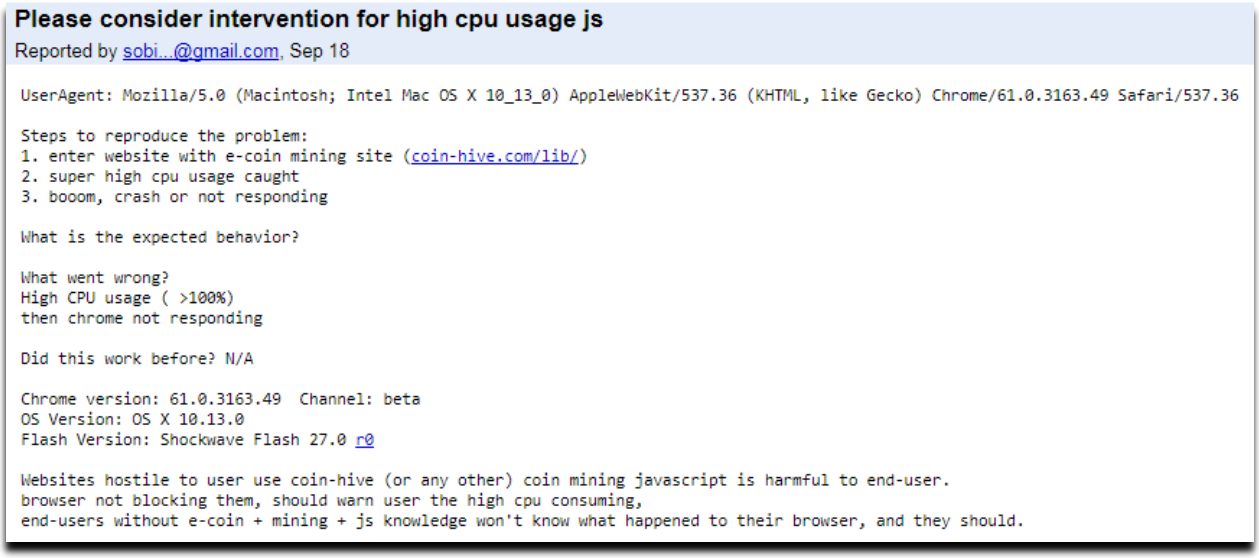
Ethical and legal aspects

The Pirate Bay incident was a starting point for many discussions about the ethical and even legal aspects of unsolicited cryptomining. Some people argued that running unwanted code on people's machines may have legal implications, while others claimed that this was perfectly normal for websites to do so.

Prolonged mining at full capacity may affect computers and mobile devices as well, especially if those are not ventilated properly. A case could be made for irresponsible use of a mining application, in case of hardware failure.

Perhaps the most contentious point was the lack of user awareness and the fact that too many sites were simply not enforcing any sort of throttling, resulting in excessive amounts of CPU being consumed for a degraded overall web experience.

Many security companies as well as various ad blockers, have started to block Coinhive and other cryptomining domains as a result. Browser makers are also weighing in their options following complaints of unwanted and high CPU usage.



Please consider intervention for high cpu usage js

Reported by sobi...@gmail.com, Sep 18

```
UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.49 Safari/537.36

Steps to reproduce the problem:
1. enter website with e-coin mining site (coin-hive.com/lib/)
2. super high cpu usage caught
3. booom, crash or not responding

What is the expected behavior?

What went wrong?
High CPU usage ( >100%)
then chrome not responding

Did this work before? N/A

Chrome version: 61.0.3163.49  Channel: beta
OS Version: OS X 10.13.0
Flash Version: Shockwave Flash 27.0 r0

Websites hostile to user use coin-hive (or any other) coin mining javascript is harmful to end-user.
browser not blocking them, should warn user the high cpu consuming,
end-users without e-coin + mining + js knowledge won't know what happened to their browser, and they should.
```

Figure 11: A Chromium forum post dated Sept 18

As soon as efforts to block cryptomining became apparent, we started seeing services that offered to bypass those blocks by using proxies, for example.

It was to be expected, of course, but this cat-and-mouse game ends up being at the expense of the user. Any site that continues to silently force cryptominers may earn a negative mark and get itself blacklisted, ultimately resulting in a drop in web traffic.

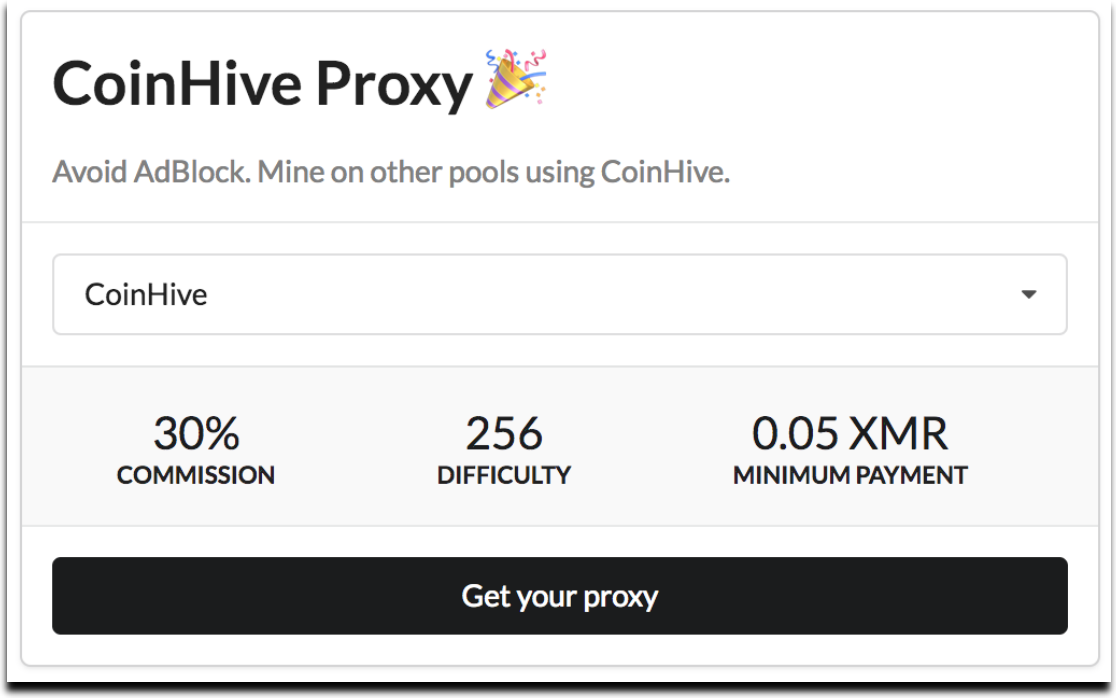


Figure 12: A service designed to evade ad blockers.

While proxies and obfuscation techniques will continue to exist, Coinhive could not ignore the issue that was staring in its face, and quickly responded with a new API that can prevent website owners from forcing the cryptomining onto their visitors. In short, this new initiative allows end users to opt in or out.

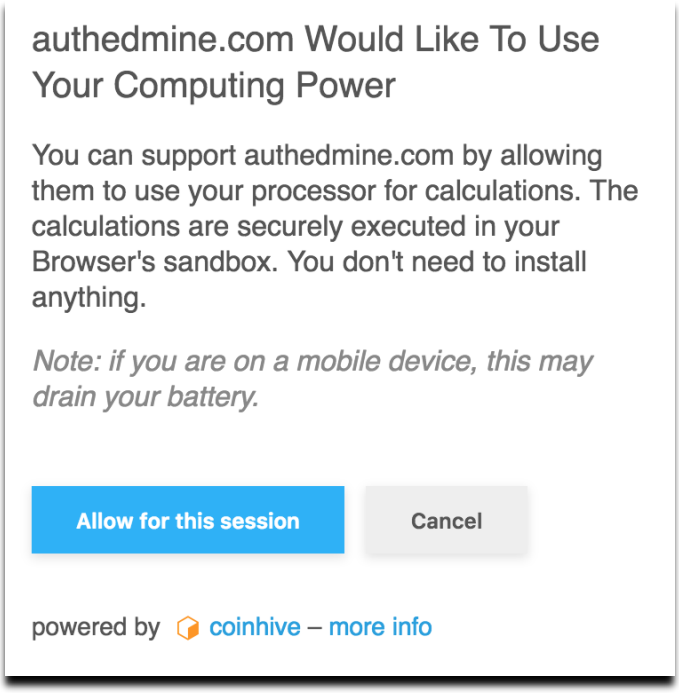


Figure 13: The new API, allowing visitors to opt-in.

In a statement, Coinhive reiterated its initial vision with the important caveat of responsible use. By this measure, it hopes ad blockers and antivirus products will not interfere.

"We believe that browser based mining can be a viable alternative for intrusive and annoying ads if used honestly and with consent by the user. We kindly ask Adblock and Antivirus Vendors to support us."

However, this new API won't immediately stop the drive-by mining abuse until the old API (still active) is completely retired. And while Coinhive appears to be making steps towards better integration, others might not be.

There is so much interest around cryptocurrencies that heists are common place. In fact, the first major incident to target Coinhive has already happened. Attackers took control of Coinhive's DNS records and pointed them to a third-party server, thereby making all the profit from mining transactions. However, it's worth noting that Coinhive took responsibility and ensured lost revenue would be reimbursed.

Conclusion

Coinhive is the first to admit its surprise at how quickly their project has taken off. While they had a part to play in the misuse of their technology, the same could be said for website owners that kept things on the down low, rather than notifying their visitors about this new monetization tool.

Browser-based cryptomining has a lot in its favor though, considering that the online ad industry has been dealt many blows over the past few years, in large part due to the increased usage of ad blockers.

In the end, the future success of web-based mining as a business model will be based on honest communication with users and the almost mandatory opt-in, which is the main characteristic that differentiates it from drive-by mining.

However, the same kind of abuse we have witnessed over the years with ads (i.e. malvertising) has already manifested itself and is perpetrated by dubious website owners or criminals.

The problem can be summarized by a fundamental question asked many a times: “Are you running a coin miner on your site or have you been hacked.” Clearly, trust can only be gained with transparency.