Web Cryptomining in the .CH Zone

Antoine Neuenschwander
antoine.neuenschwander@switch.ch

54th TF-CSIRT Meeting
May 24th 2018, Warsaw
Agenda

• Superfast Intro to Cryptomining
  Blockchain, Proof of Work
• Mining in the Browser with Coinhive
• Who deploys miners in the .CH Zone?
• What is SWITCH doing about it?
Blockchain

Block #12

Block #13

Block #14

Block #15

Block #16

Block #17

<table>
<thead>
<tr>
<th>Transaction Amount</th>
<th>From</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 $</td>
<td>Yves</td>
<td>Katja</td>
</tr>
<tr>
<td>35 $</td>
<td>Andreas</td>
<td>Daniel</td>
</tr>
<tr>
<td>1,850,480 $</td>
<td>Yves</td>
<td>Antoine</td>
</tr>
</tbody>
</table>
Proof of Work

• Think of a worldwide lottery
• Numbers are drawn every 2 – 10 mins
• Have as many tickets as you want can

\[
\text{hash} = \text{SHA1(SHA1(X))} =
\begin{array}{c}
\text{0000000000000086de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b}
\text{0000000000000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}
\end{array}
\]
Evolution of Bitcoin Hardware

- CPU mining
- GPU mining
- FPGA mining
- ASIC mining

- 2008
- 2010
- 2011
Photo credit: Trustnodes.com
# Algorithm Comparison

<table>
<thead>
<tr>
<th>Algorithm Name</th>
<th>Limitation</th>
<th>Current Network Hash-Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>hashcash-SHA256</td>
<td>CPU-bound</td>
<td>25 EH/s</td>
</tr>
<tr>
<td>CryptoNight</td>
<td>Memory-bound</td>
<td>1 GH/s</td>
</tr>
</tbody>
</table>

![Diagram of a computer processor with Memory Controller, Core, L1 cache, L2 cache, Queue, and Shared L3 Cache.]
Coinhive offers a **JavaScript miner** for the **Monero** Blockchain that you can embed in your website. Your users run the miner directly in their Browser and mine XMR for you in turn for an ad-free experience, in-game currency or whatever incentives you can come up with.
Running Coinhive

```html
<script src="https://coinhive.com/lib/miner.min.js" async"></script>

var miner = new CoinHive.Anonymous('5fjY1u0KgQMNRexHsnXMpUESxN6K3SWY');
miner.start();
</script>
```
coinhive.min.js

WEBASSEMBLY
## Performance

<table>
<thead>
<tr>
<th>CPU</th>
<th>L2</th>
<th>L3</th>
<th>Hashes/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple A7 1.4 GHz</td>
<td>2x 512 KB</td>
<td>4 MB</td>
<td>16</td>
</tr>
<tr>
<td>Intel Core i7 3.5 GHz</td>
<td>2x 256 KB</td>
<td>4 MB</td>
<td>30</td>
</tr>
<tr>
<td>Intel Core i7 2.9 GHz</td>
<td>4x 256 KB</td>
<td>8 MB</td>
<td>50</td>
</tr>
<tr>
<td>Intel Xeon E5-1620 3.7 GHz</td>
<td>4x 256 KB</td>
<td>10 MB</td>
<td>60</td>
</tr>
</tbody>
</table>
### Revenue Computation

**0.00005884 XMR per 1M hashes**

**1 XMR = 188 USD**

<table>
<thead>
<tr>
<th># Systems</th>
<th>Duration</th>
<th>Hash Rate</th>
<th>Hashes</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 h</td>
<td>50 H/s</td>
<td>180’000</td>
<td>USD 0.0000105912</td>
</tr>
<tr>
<td>100</td>
<td>1 h</td>
<td>50 H/s</td>
<td>18'000'000</td>
<td>USD 0.00105912</td>
</tr>
<tr>
<td>10’000</td>
<td>1 h</td>
<td>50 H/s</td>
<td>1’800’000’000</td>
<td>USD 0.10593</td>
</tr>
<tr>
<td>120’000</td>
<td>5 min</td>
<td>50 H/s</td>
<td>1’800'000'000</td>
<td>USD 0.10593</td>
</tr>
</tbody>
</table>

*Revenue = payout \cdot 10^{-6} \cdot N \cdot duration \cdot hashrate*
Crawling the .CH Zone

- scrapy
- scrapy
- scrapy
- ...
- scrapy

redis / logstash

Elastic search
Who’s mining on your Back?

90 Jan 2018
105 Apr 2018
116 May 2018

of the 1.2 mio accessible .CH domains (0.01%)
## Compared to other TLDs

<table>
<thead>
<tr>
<th>TLD</th>
<th>Accessible Domains</th>
<th># Cryptominers</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>.fr</td>
<td>2,302,097</td>
<td>400</td>
<td>0.017%</td>
</tr>
<tr>
<td>.li</td>
<td>34,086</td>
<td>6</td>
<td>0.017%</td>
</tr>
<tr>
<td>.ch</td>
<td>1,264,329</td>
<td>116</td>
<td>0.009%</td>
</tr>
<tr>
<td>.se</td>
<td>1,142,395</td>
<td>79</td>
<td>0.007%</td>
</tr>
</tbody>
</table>
Affected CMS (.ch)
Reasons for Cryptomining?

1. Operator mines with the user’s consent

2. Operator placed a secret cryptominer

3. Site has been compromised and a cryptominer was injected
Legitimate Use

Welcome to AdfreeTV
Watch TV and movies online for free without ads.

AdfreeTV is an alternative to PrimeWire. Instead of displaying annoying ads and popups all over the place, AdfreeTV is supported by visitors like you allowing us to borrow their processor for calculations to mine crypto-currency while browsing and streaming video on the site. These calculations are securely executed in your browser's sandbox; nothing is installed on your device. We throttle the processor usage to a maximum of 60% on desktop computers and 20% on mobile devices. This process uses very little bandwidth - far less than what would be used to serve ads. You shouldn't even notice this process taking place.

AdfreeTV simply scrapes data from PrimeWire.ag and displays it here without all the clutter. If PrimeWire is down it is likely that our website will not function 100% properly. Unlike PrimeWire, AdfreeTV is responsive (mobile-friendly) so it will look great on any device you use! Another benefit of using AdfreeTV is we have included a fix for the notorious “blank white screen” that has plagued PrimeWire for sometime now.

By using this website you accept and allow us to borrow your processor to mine the crypto-currency Monero. If you are curious about how many hashes your processor is completing per second just open up your browser’s console - we log the hashrate every five seconds.

Return to the Home page

Disclaimer: This site does not store any files on its server. All contents are provided by non-affiliated third parties.
Obviously a Hacked Site
Browser Addons

Search: My Add-ons ○ Available Add-ons

**Mining Blocker**
This free Crypto Mining Blocker for Firefox, blocks all CPU-Crypto Miners before...

**Coin Mining Blocker**
Block JavaScript coin mining scripts at network level

**NotMINING.org**
EN: Check if your favorite website is mining or not. Developed by Adan K. Martin & Jose C. Ga...

**MinimaList**
Simple To-Do list with a minimalist notebook look. Add, edit and delete your tasks with a sin...

**NoMiner - Block Coin Miners**
Easily stop coin miners from using your computer resources.

**CryptoTab**
CryptoTab allows you to mine Bitcoins right in your Firefox Browser and multiply your incom...

**Mines**
The classic game of Minesweeper recreated for Firefox. Includes several interesting variatio...

**No Coin**
Stop coin miners on the web!
Adblocker Evasion
Intentional, Secret Mining
Combating cybercrime

Under certain conditions, the registries for the ".ch" and ".swiss" domain are required to block domain names suspected of being used for phishing, for the distribution of harmful software ("malware") or to support such activities.

The measures to combat cybercrime using domain names as laid down in the Ordinance on Internet Domains (OID; CC 784.104.2 revised on 1 January 2018) apply to top-level internet domains for the management of which the Confederation is responsible, i.e. the ".ch" and ".swiss" domains; in particular,

https://www.admin.ch/opc/de/classified-compilation/20141744/index.html
Reasons for Cryptomining?

1. Operator mines with the user’s consent

2. Operator placed a secret cryptominer

3. Site has been compromised and a cryptominer was injected
Asking for Consent

yourdomain.com Would Like To Use Your Computing Power

You can support yourdomain.com by allowing them to use your processor for calculations. The calculations are securely executed in your Browser's sandbox. You don't need to install anything.

Note: if you are on a mobile device, this may drain your battery.

Allow for this session    Cancel

powered by coinhive — more info

All websites across the EU are now required to ask your permission to place cookies on your machine, and you can read more about it.

Session Settings  ✓ Accept Cryptomining
A Sneaky Case

The most popular free solution to US and European Cookie Laws

European and American laws require that digital publishers give visitors to their sites and apps information about their use of cookies and other forms of local storage. These laws also require that consent be obtained. A breach of these regulations can result in a fine of up to $500,000.

Download Script  Wordpress Plugin
Looks Familiar?

http://cookiescript.info/libs/cookieconsent.6.min.js
Working for a better digital world
Internationale Kooperationen

Security
- APWG
- CERT.at
- DNS-OARC
- enisa
- Europol
- First
- Team Cymru
- TF-CSIRT

Trust & Identity
- eduGAIN
- GÉANT
- REFEDS
- SIRTIFI
- Shibboleth

Network
- GÉANT
- IEEE
- IETF
- RIPE NCC

Infrastructure & Data Services
- Digital Infrastructures for Research 2017
- e-IRG Reflection Group
- FiWARE
- GÉANT
- GLIF
- H2020 Bula
- OGC
- OpenStack
- ORG

More
- Arge Software
- DIH
- Eduserv
- EDUCAUSE
- ICANN
- SURF
- ZK

© 2018 SWITCH | 32