Web-based Cryptojacking in the Wild

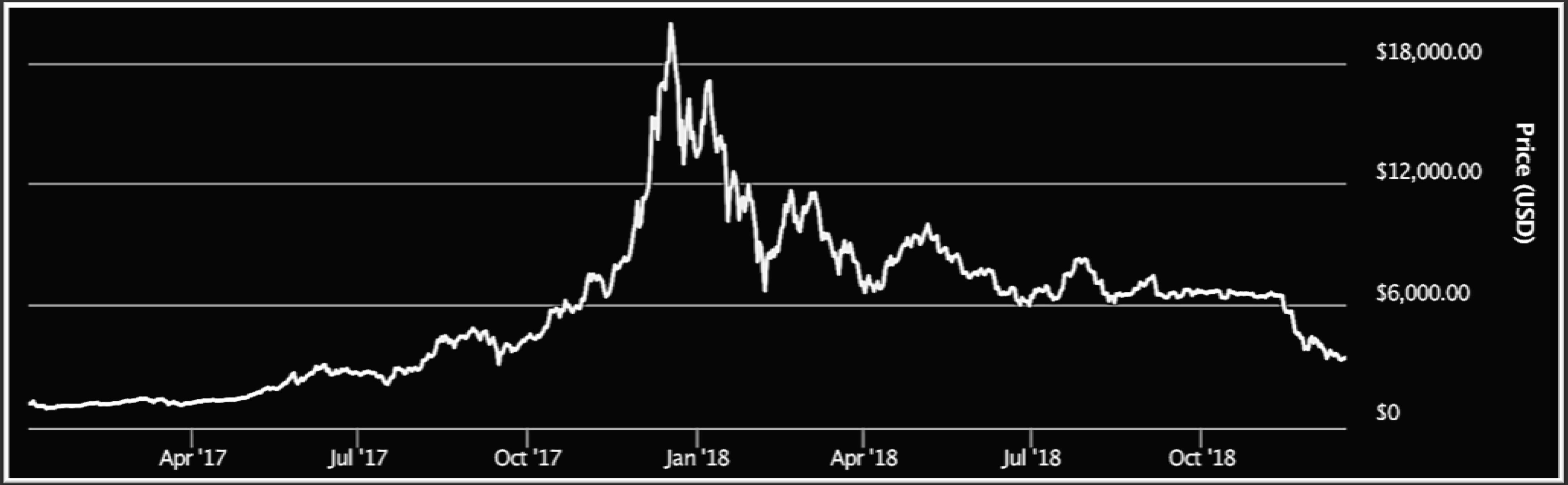
Marius Musch (@m4riuz)

TU Braunschweig

Joint work with Christian Wressnegger (@chwress)

Martin Johns (@datenkeller) and Konrad Rieck (@mlsec)

The cryptocurrency hype



Bitcoin to USD exchange rate, 2017 – 2018. Source: coinmarketcap.com

Mining

1. State + Nonce
2. Calculate hash
3. Compare to target
4. Repeat

Profits

- Shiny new coins

Costs

- Hardware
- Electricity

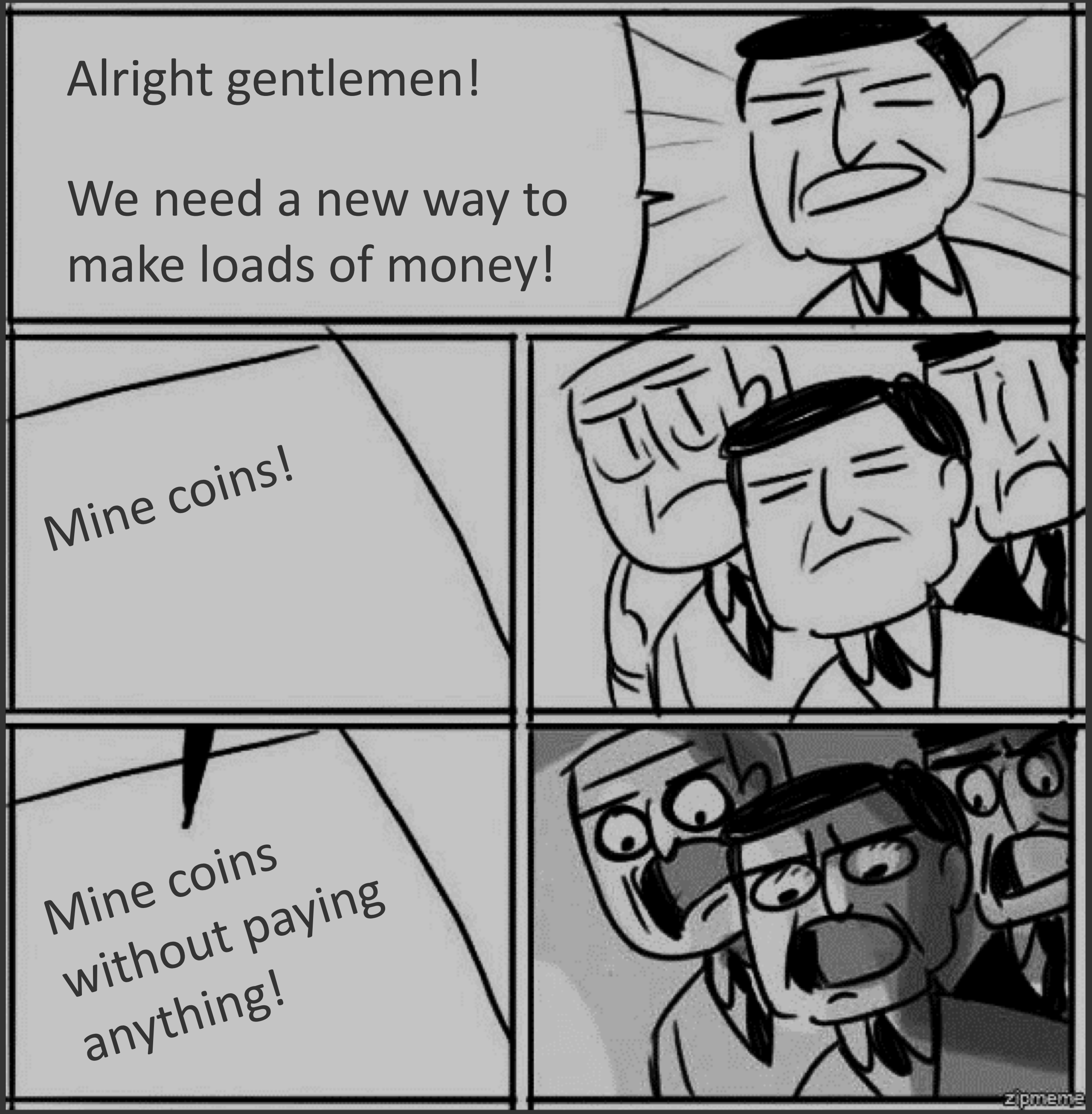
Mining pool

Consistent reward

```
=> auth: {version:7, site_key:"yQu...cOz"}
<= authed: {token:"", hashes:0}
<= job: {blob:"070...103", target:“00ffffff"}

=> submit: {nonce:"99bd1d53", result:“00c...ee9"}
<= hash_accepted: {hashes:256}

=> submit: {nonce:"f40ef4ed", result:“009...4a3"}
<= hash_accepted: {hashes:512}
```


Alright gentlemen!

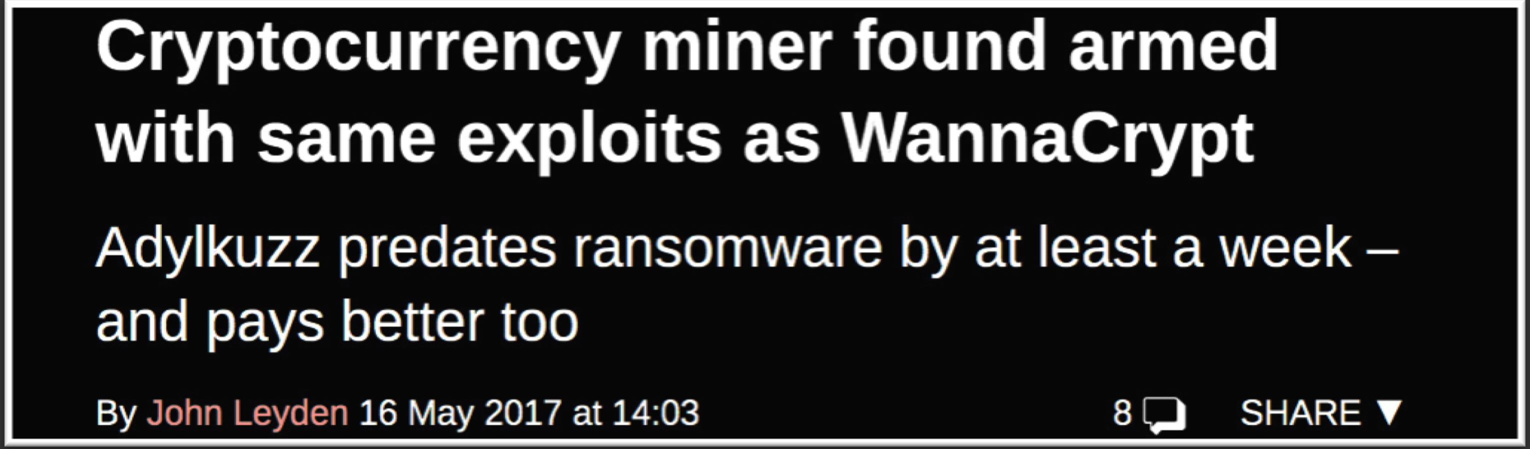
We need a new way to make loads of money!

Mine coins!

Mine coins without paying anything!

zipmeme

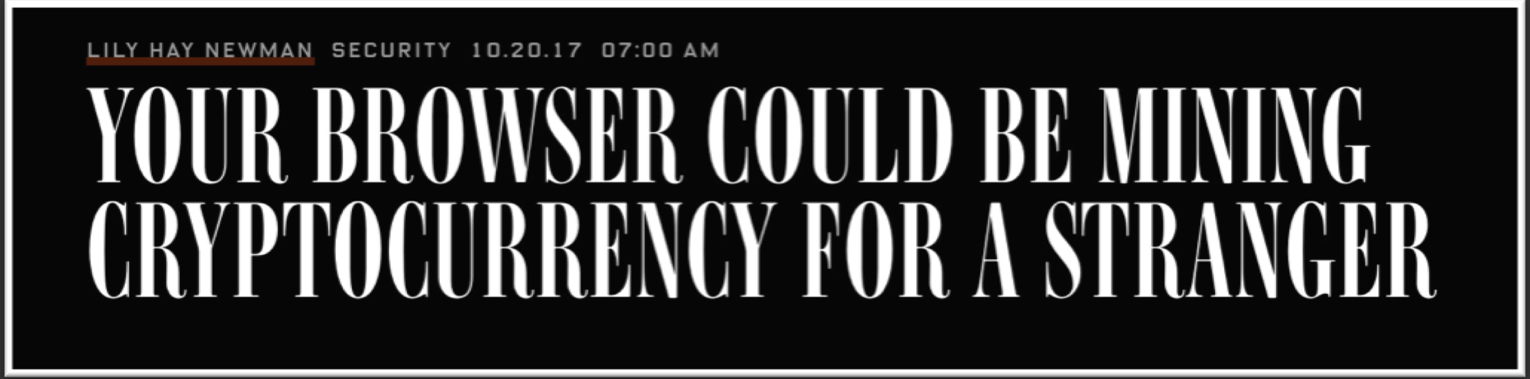
News (from 2017)



Cryptocurrency miner found armed with same exploits as WannaCrypt

Adylkuzz predates ransomware by at least a week – and pays better too

By John Leyden 16 May 2017 at 14:03 8 SHARE ▼



LILY HAY NEWMAN SECURITY 10.20.17 07:00 AM

YOUR BROWSER COULD BE MINING CRYPTOCURRENCY FOR A STRANGER

Web-based cryptojacking

Mining in the browser

Fast execution

- WebAssembly

Multi-threading

- WebWorkers

Efficient communication

- WebSockets

Proof of work

Wait, but mining on the CPU?

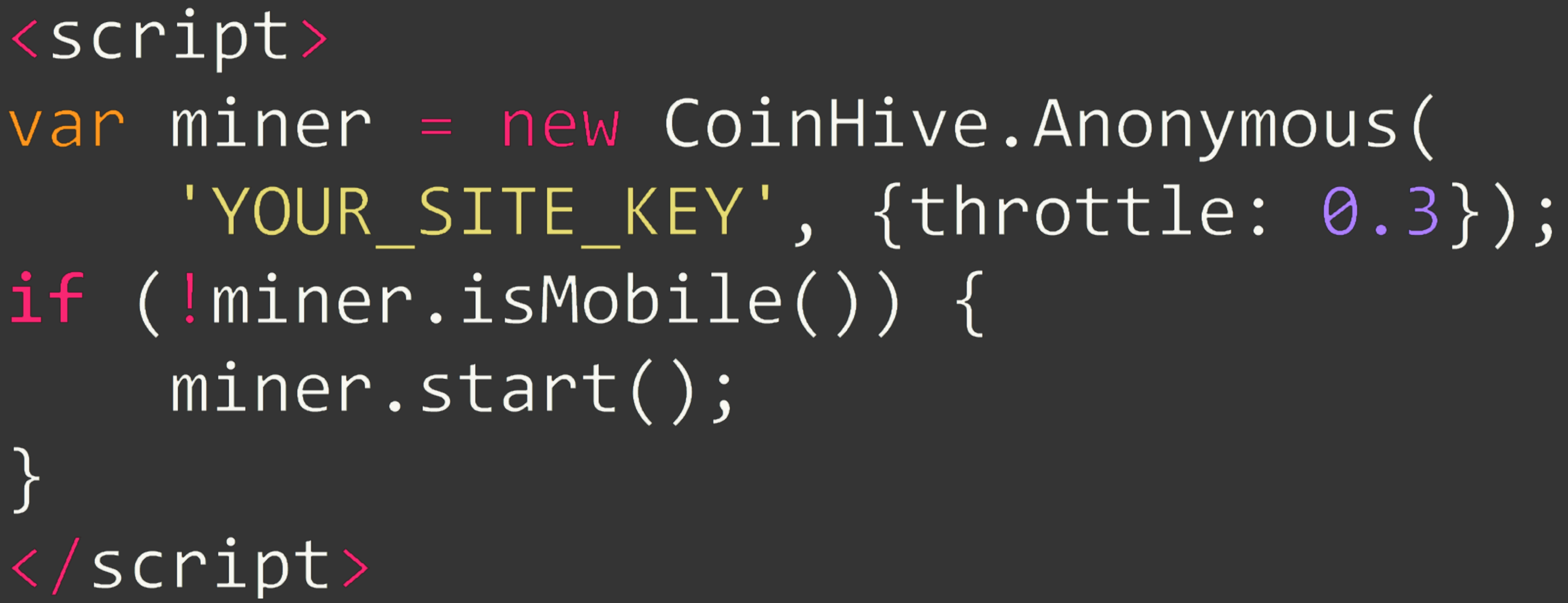
Bitcoin: SHA-256

- GPU = ~30x CPUs
- ASIC = ~400x GPUs

Monero: Cryptonight

- Not much difference

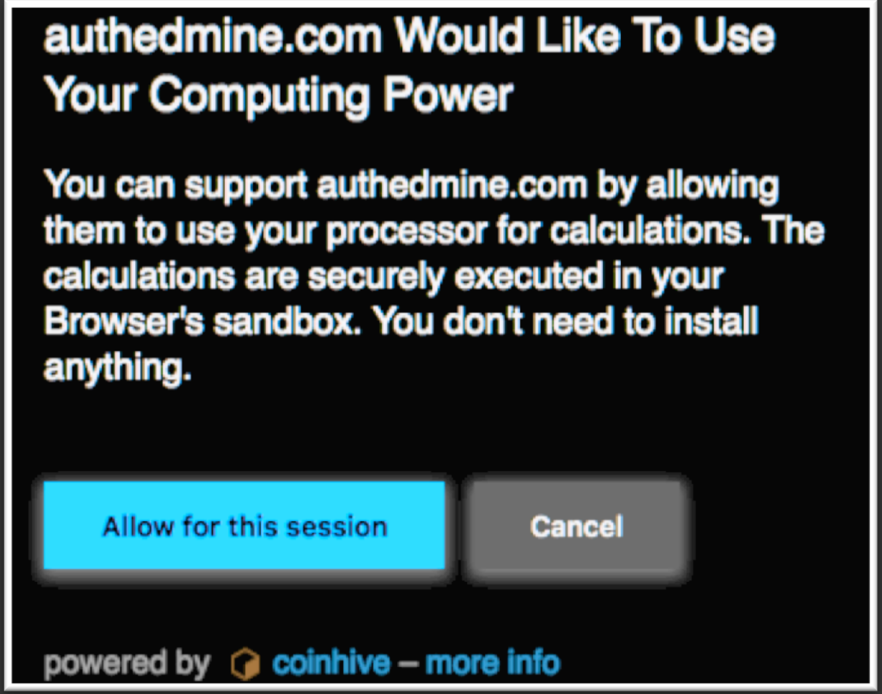
Thus CoinHive was born



```
<script>
var miner = new CoinHive.Anonymous(
    'YOUR_SITE_KEY', {throttle: 0.3});
if (!miner.isMobile()) {
    miner.start();
}
</script>
```

Detection

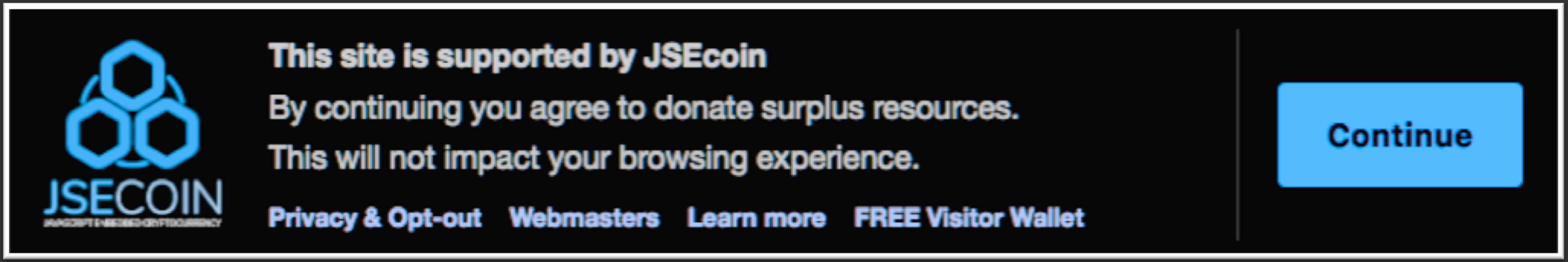
Not all mining is evil



authedmine.com Would Like To Use Your Computing Power

You can support authedmine.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.

Cryptojacking = Starts automatically, without explicit consent



This site is supported by JSEcoin

By continuing you agree to donate surplus resources.

This will not impact your browsing experience.

Static detection

URL blacklist

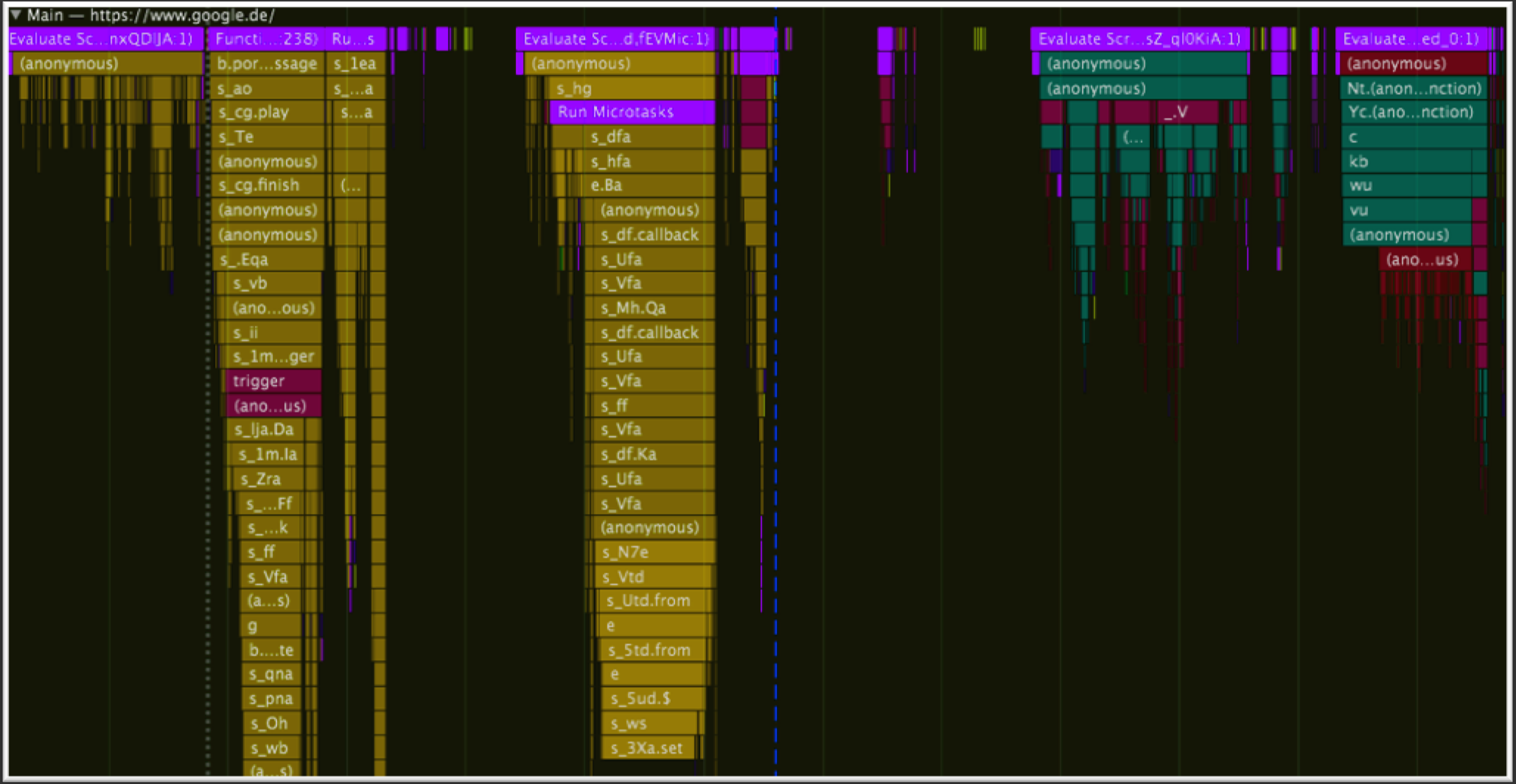
- *://*/*coinhive.min.js*
- *://*.cdn-jquery.host/*
- *://*.estream.to/player.js*

Known strings

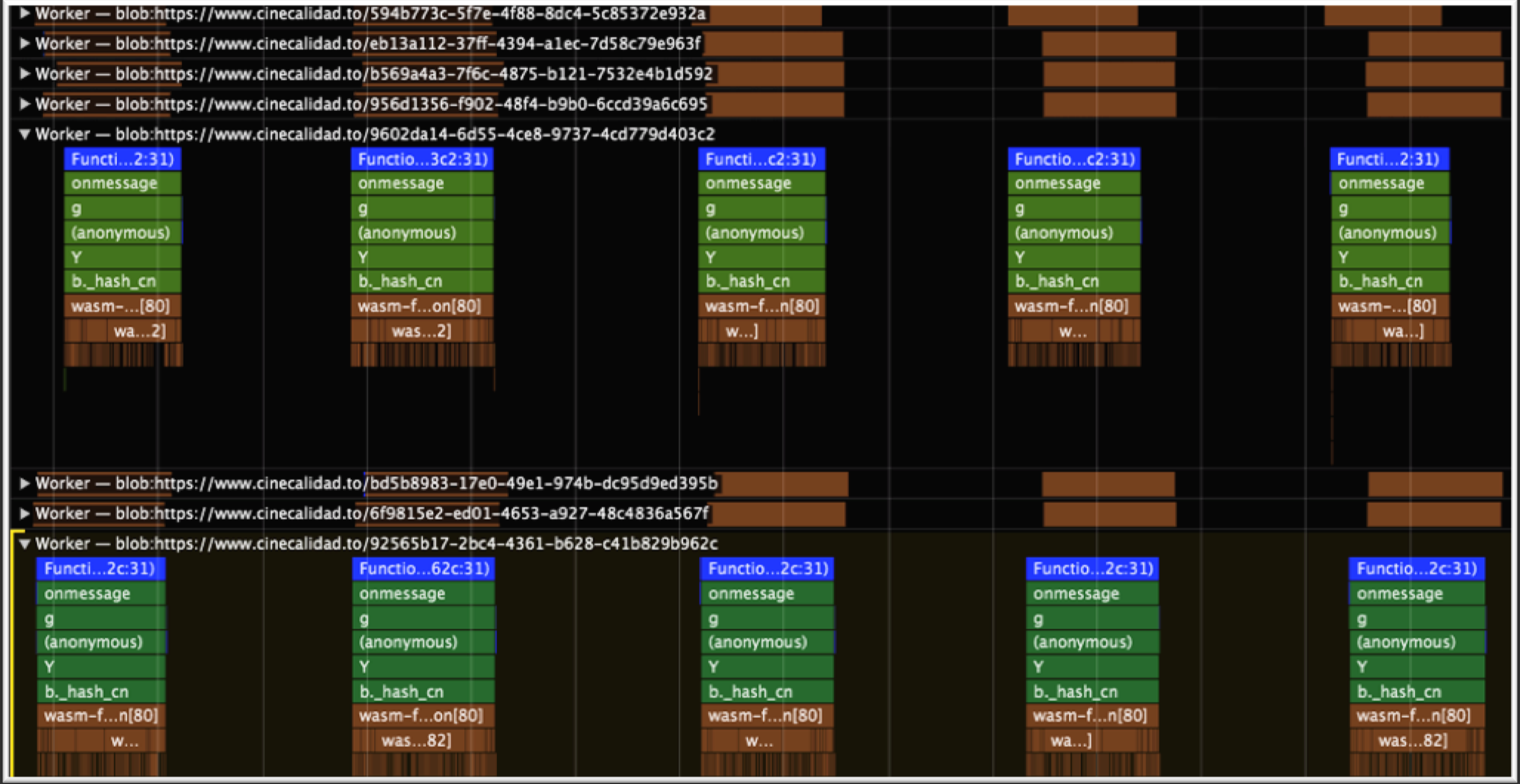
- miner.start();
- window.CoinHive
- CryptonightWASMWrapper

```
if (this['\x5f\x75\x73\x65\x72']) {
    _0x8f4c0c['\x74\x79\x70\x65'] = _0x3cdb('0x44’);
    _0x8f4c0c['\x75\x73\x65\x72'] = this['\x5f\x75\x73\x65\x72']();
} else if (this['\x5f\x67\x6f\x61\x6c']) {
    _0x8f4c0c['\x74\x79\x70\x65'] = '\x74\x6f\x6b\x65\x6e’;
    _0x8f4c0c[_0x3cdb('0x46')] = this[_0x3cdb('0x47’)];
}
if (this['\x70\x61\x72\x61\x6d\x73']['\x72\x65\x66']) {
    _0x8f4c0c['\x72\x65\x66'] = this['\x70\x61\x72\x61\x6d\x73’]
}
if (this[_0x3cdb('0x33')]) {
    _0x8f4c0c[_0x3cdb('0x48')] = this[_0x3cdb('0x33')];
}
this['\x5f\x73\x65\x6e\x64'](_0x3cdb('0x49'), _0x8f4c0c);
```

Execution traces



Execution traces

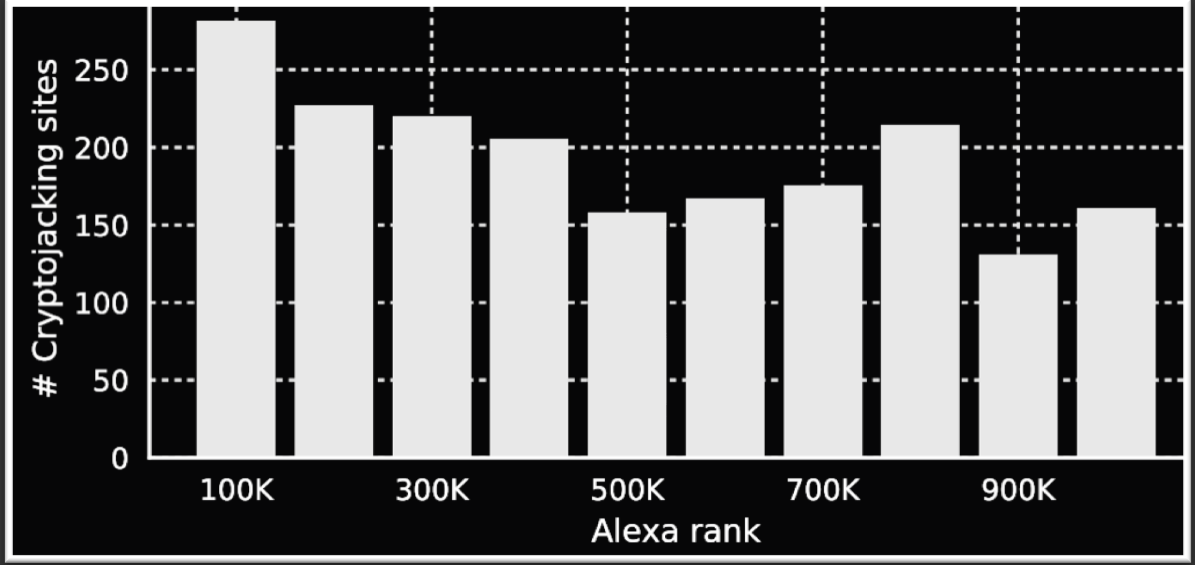

▶ Worker — blob:https://www.cinecalidad.to/594b773c-5f7e-4f88-8dc4-5c85372e932a
▶ Worker — blob:https://www.cinecalidad.to/eb13a112-37ff-4394-a1ec-7d58c79e963f
▶ Worker — blob:https://www.cinecalidad.to/b569a4a3-7f6c-4875-b121-7532e4b1d592
▶ Worker — blob:https://www.cinecalidad.to/956d1356-f902-48f4-b9b0-6ccd39a6c695
▼ Worker — blob:https://www.cinecalidad.to/9602da14-6d55-4ce8-9737-4cd779d403c2
Functi…2:31)
Functio…3c2:31)
Functi…c2:31)
Functio…c2:31)
Functi…2:31)
onmessage
g
(anonymous)
Y
b._hash_cn
wasm-…[80]
wasm-f…on[80]
wasm-f…n[80]
wa…2]
was…2]
w…]
w…
wa…]
▶ Worker — blob:https://www.cinecalidad.to/bd5b8983-17e0-49e1-974b-dc95d9ed395b
▶ Worker — blob:https://www.cinecalidad.to/6f9815e2-ed01-4653-a927-48c4836a567f
▼ Worker — blob:https://www.cinecalidad.to/92565b17-2bc4-4361-b628-c41b829b962c
Functi…2c:31)
Functio…62c:31)
Functio…2c:31)
onmessage
g
(anonymous)
Y
b._hash_cn
wasm-f…n[80]
wasm-f…on[80]
w…
was…82]
wa…]

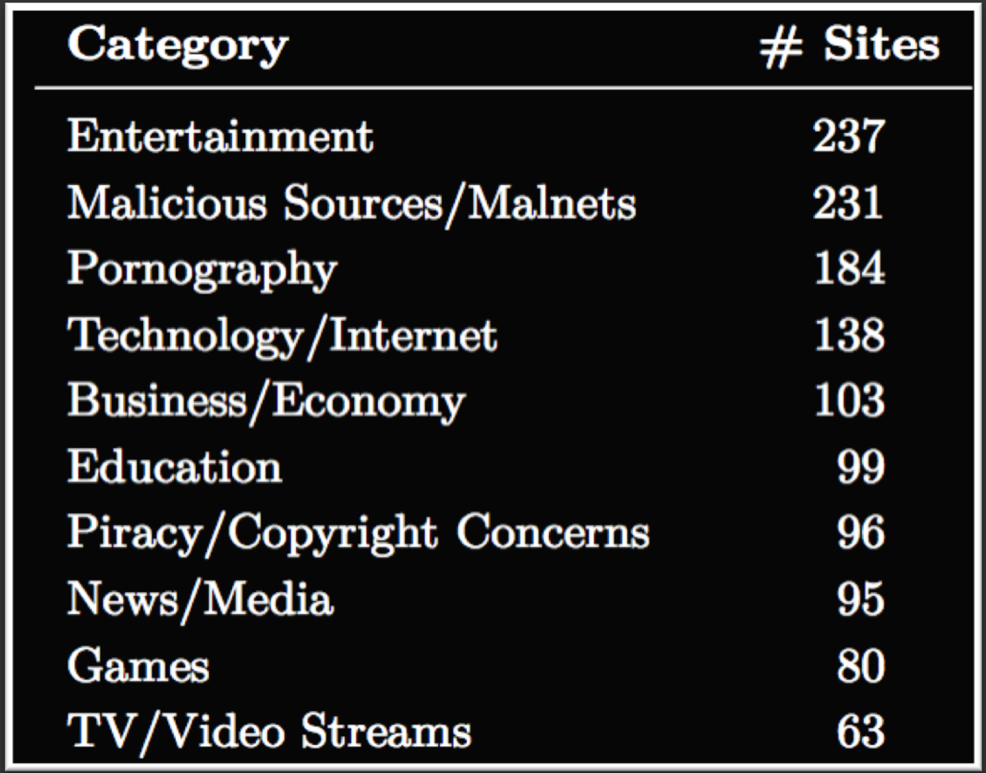
Results

Prevalence on 1M sites

Total: ~2,500 sites

-> About 1 in 500





Category	# Sites
Entertainment	237
Malicious Sources/Malnets	231
Pornography	184
Technology/Internet	138
Business/Economy	103
Education	99
Piracy/Copyright Concerns	96
News/Media	95
Games	80
TV/Video Streams	63

Daily revenue

Top 10

- 400,000 visitors
- 6 minutes
- 0.8 XMR -> ~180€/day

Average

- 25,000 visitors
- 3 minutes
- 0.025 XMR -> ~5€/day

Money flow

Monero

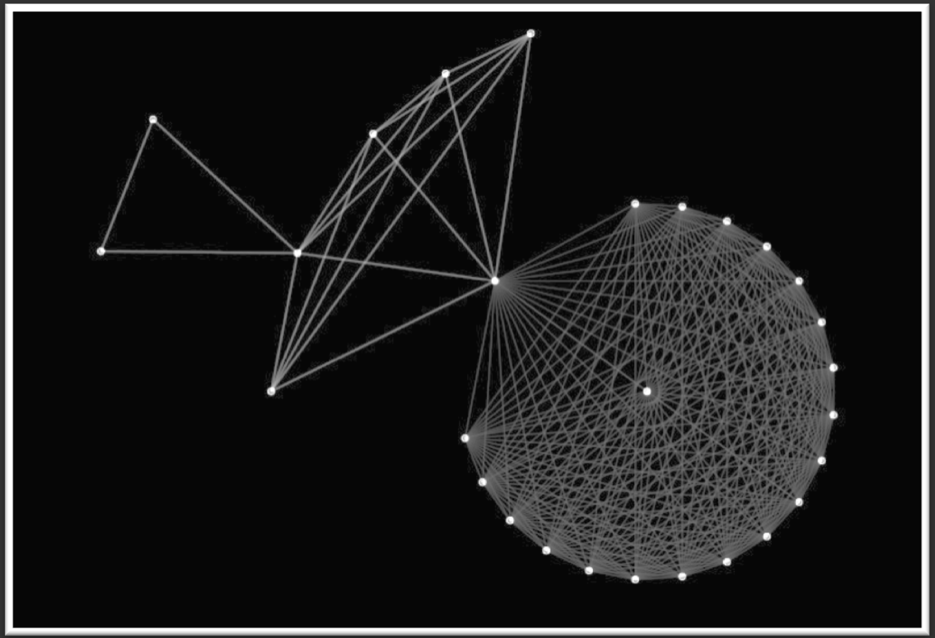
- Untraceable payments
- Unlinkable transactions

CoinHive

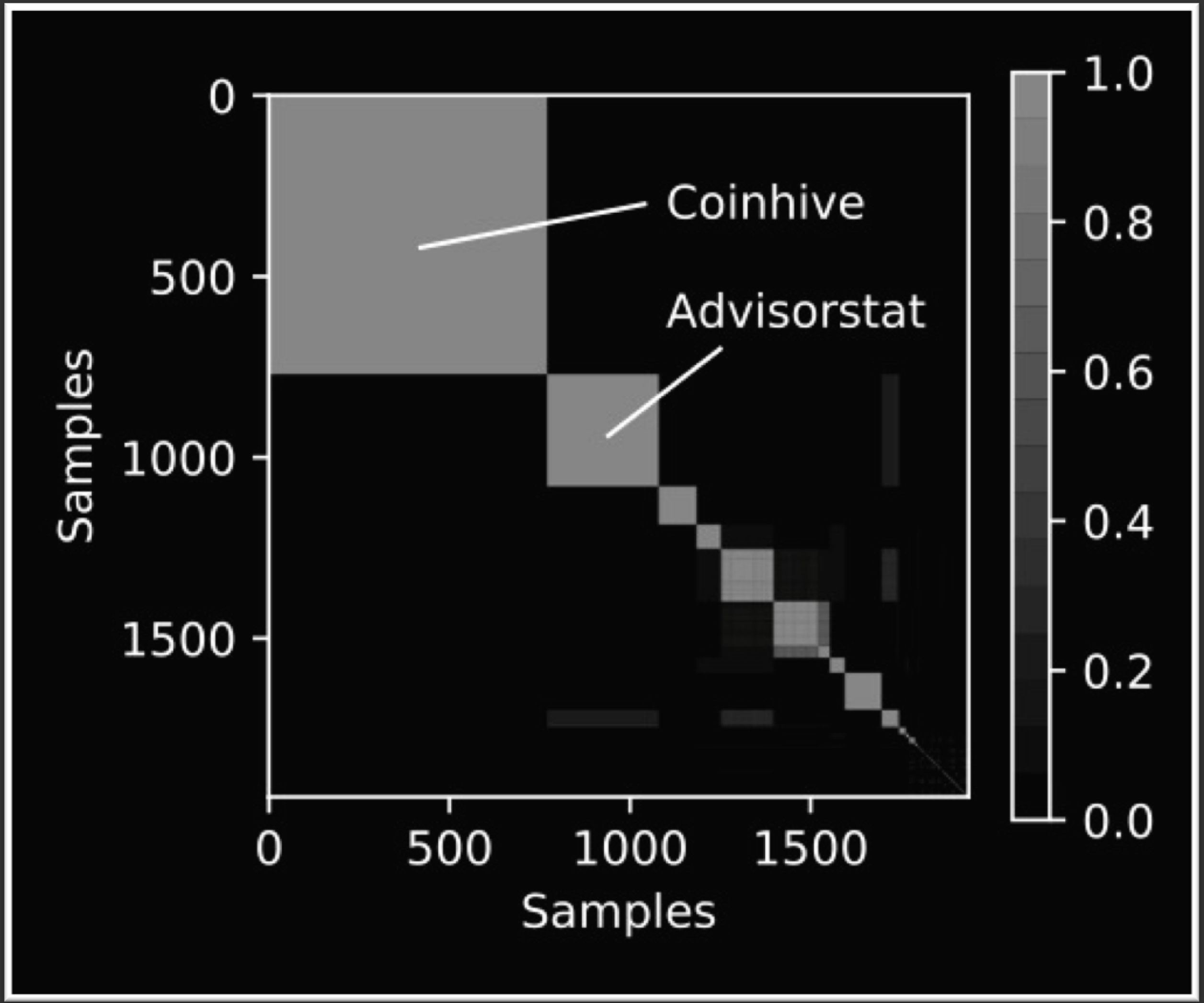
- Sitekey != Wallet address
- 570 sitekeys on 830 sites

Web artifacts

- Same mining script
- Same WebSocket backend

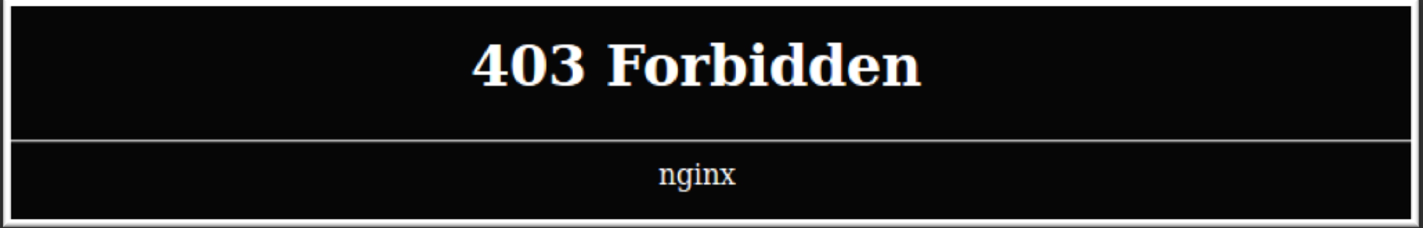


Code similarity



Case study

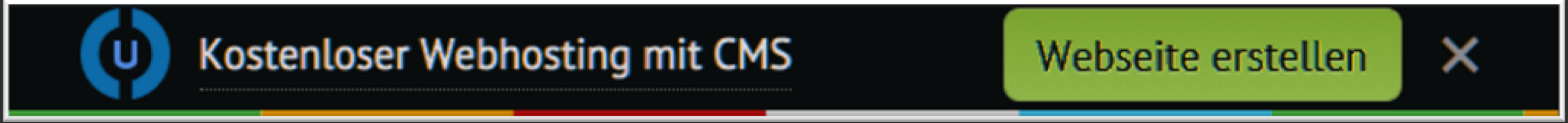
311 sites with miner from advisorstat.space



403 Forbidden

nginx

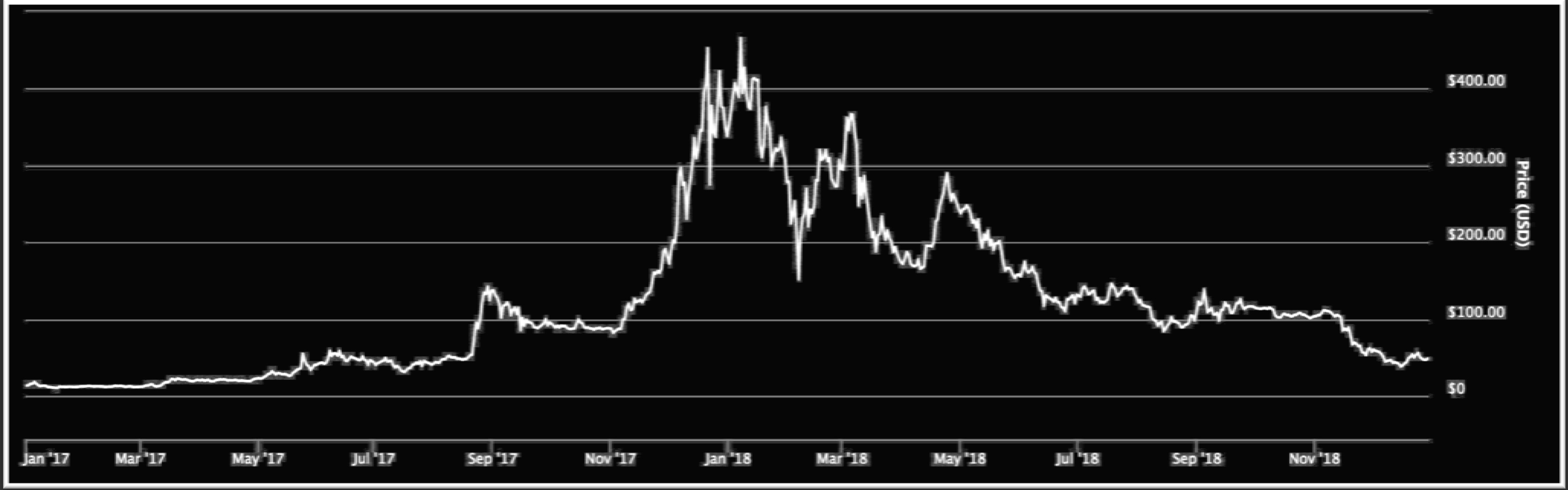
Included via this banner



Kostenloser Webhosting mit CMS

moradu.com -> netrevgo.com -> advisorstat.space

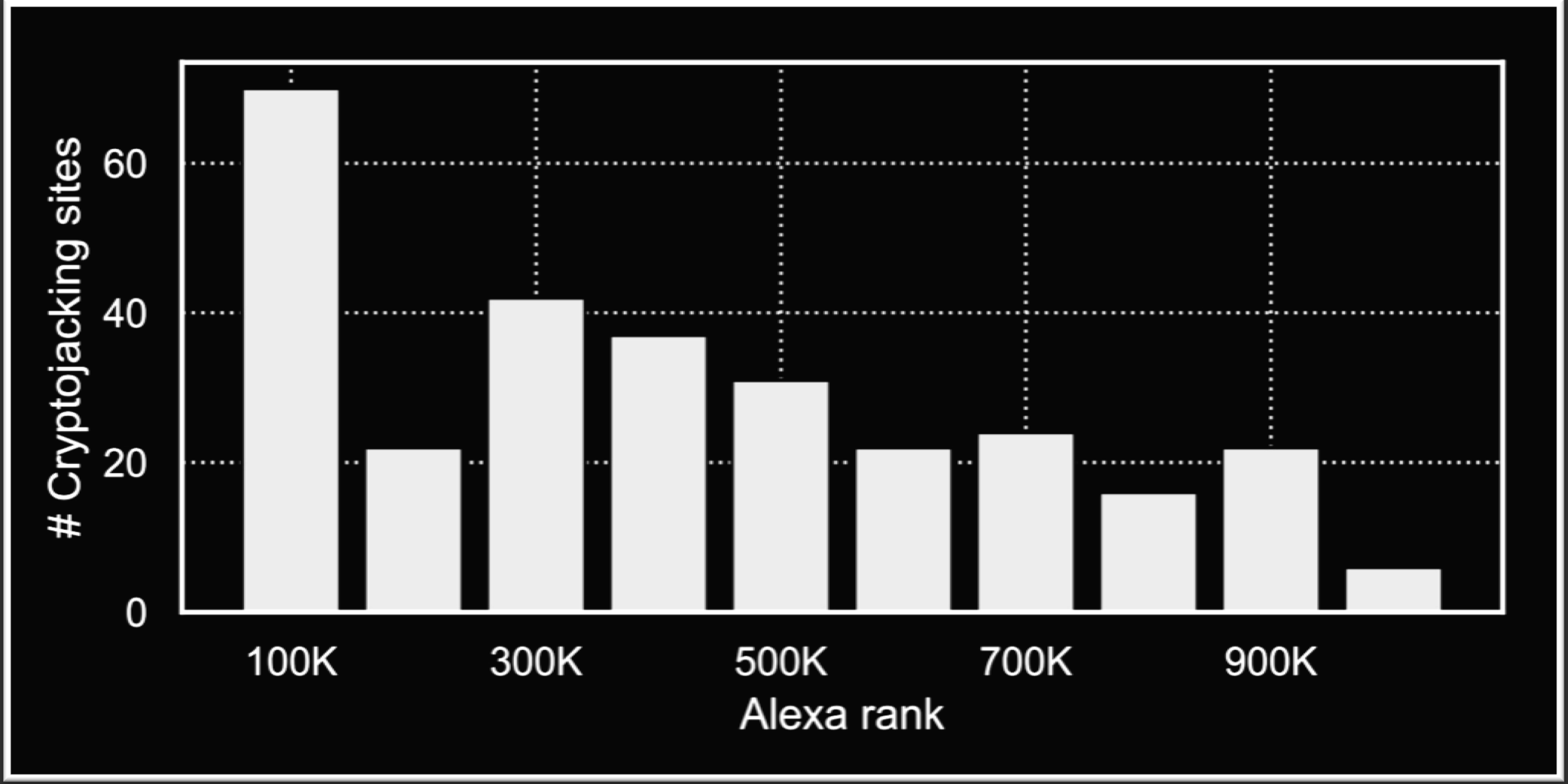
How about today



Monero to USD exchange rate, 2017 – 2018. Source: coinmarketcap.com

~ 1€/day for average website

How about today



Only ~300 miners now

Thanks for listening :)

Questions?

Contact

- m.musch@tu-bs.de
- @m4riuz

IAS INSTITUTE FOR APPLICATION SECURITY

Institute of System Security

Technische Universität Braunschweig