IoT, Cybercriminal's paradise

Attila Marosi

Senior Threat Researcher

OSCE, OSCP, ECSA, CEH

attila.marosi@{sophos.com | gmail.com}

PGP ID: 3782A65A

PGP FP.:

4D49 1447 A4E1 F016 F833
8700 8853 60A7 3782 A65A

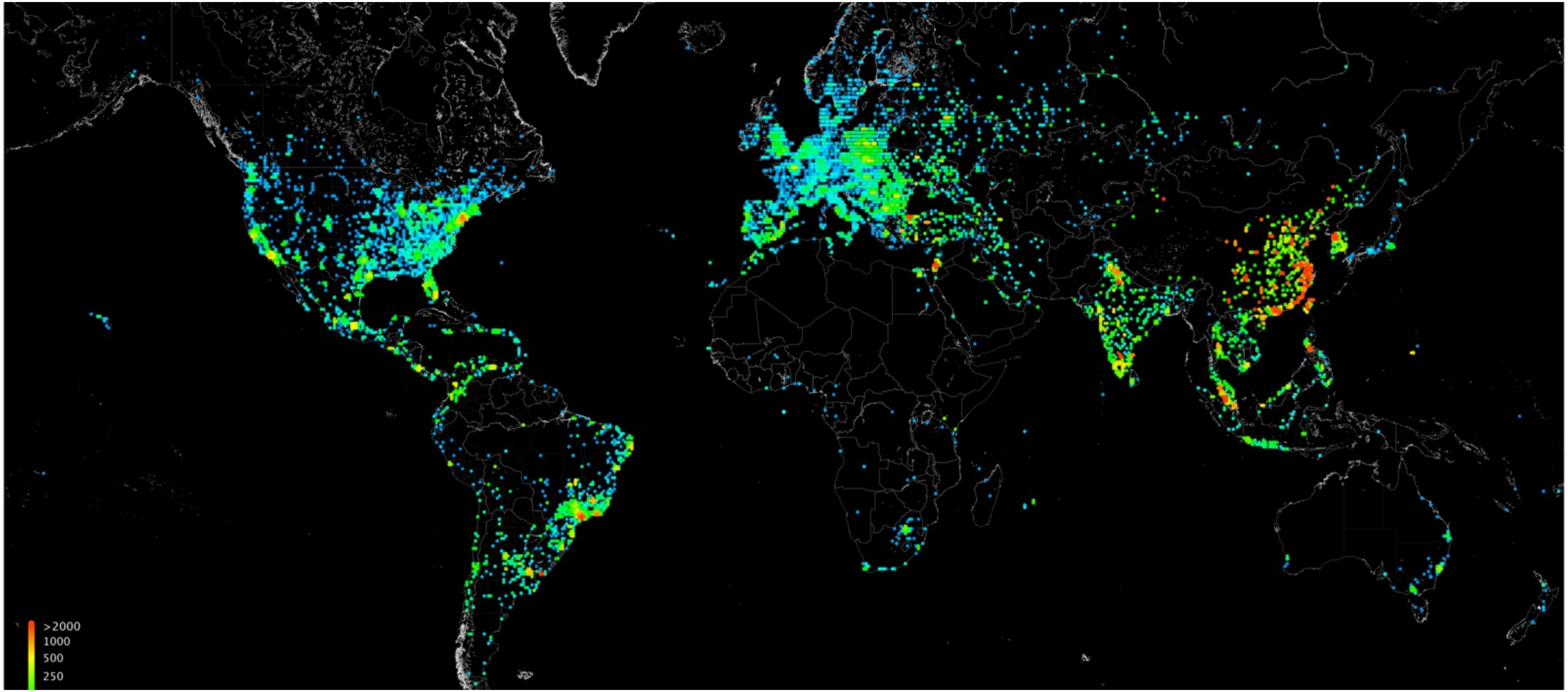
SOPHOS

If I were a criminal… a lazy one

- I would like to earn good money
- I would not want to work a lot
- I would hide myself as much as I could

What are the top stories recently

Carna project

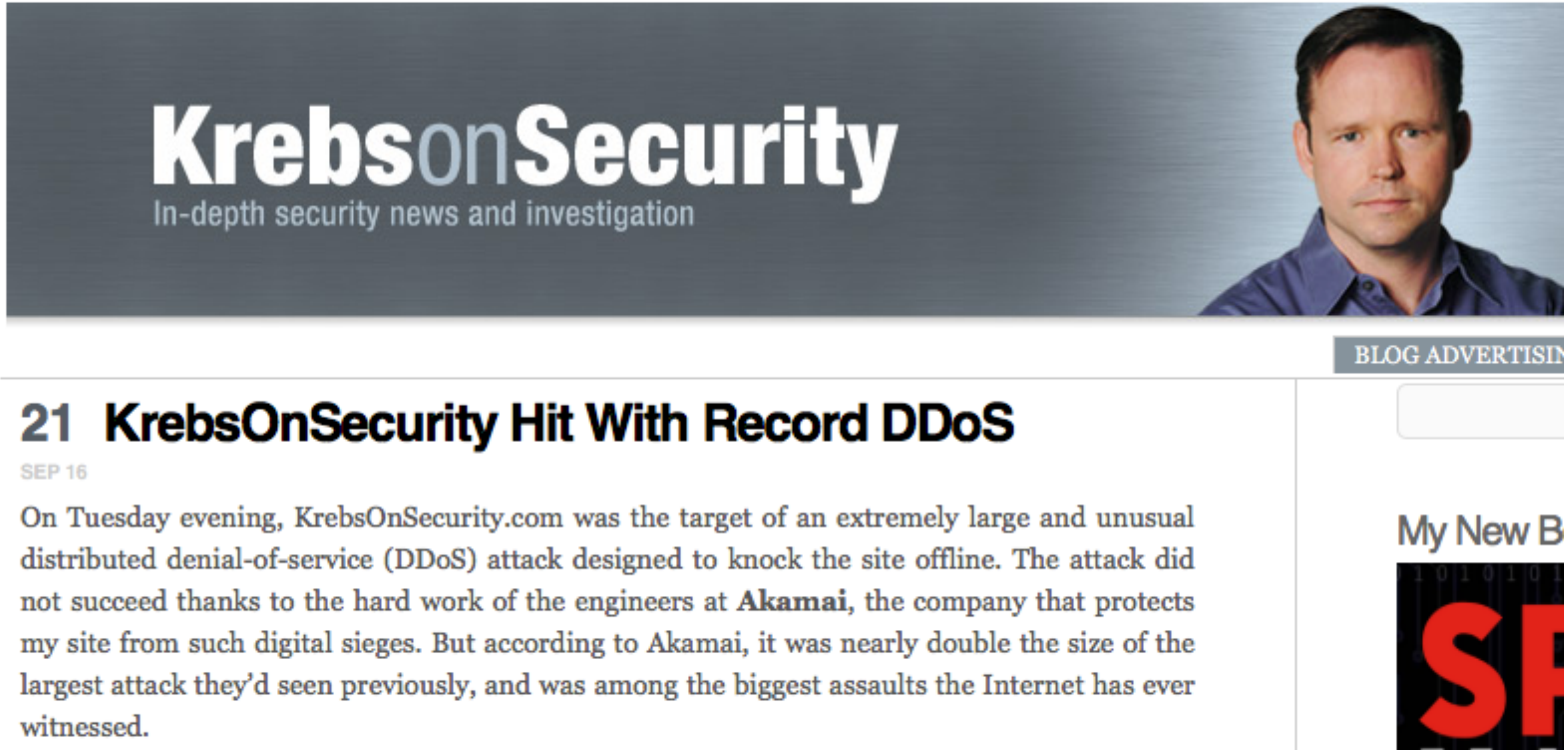


2012, 420K infected devices

ReinCarna (a ProsumWare)

```
# telnet 73.xxx.xxx.210
Trying 73.xxx.xxx.210...

REINCARNA / Linux.Wifatch

Your device has been infected by REINCARNA / Linux.Wifatch.

We have no intent of damaging your device or harm your privacy in any way.

Telnet and other backdoors have been closed to avoid further infection of
this device. Please disable telnet, change root/admin passwords, and/or
update the firmware.

This software can be removed by rebooting your device, but unless you take
steps to secure it, it will be infected again by REINCARNA, or more harmful
software.

This remote disinfection bot is free software. The source code
is currently available at https://gitlab.com/rav7teif/linux.wifatch

Team White <rav7teif@ya.ru>
```

KrebsOnSecurity hit with record DDoS



KrebsonSecurity

In-depth security news and investigation

BLOG ADVERTISIN

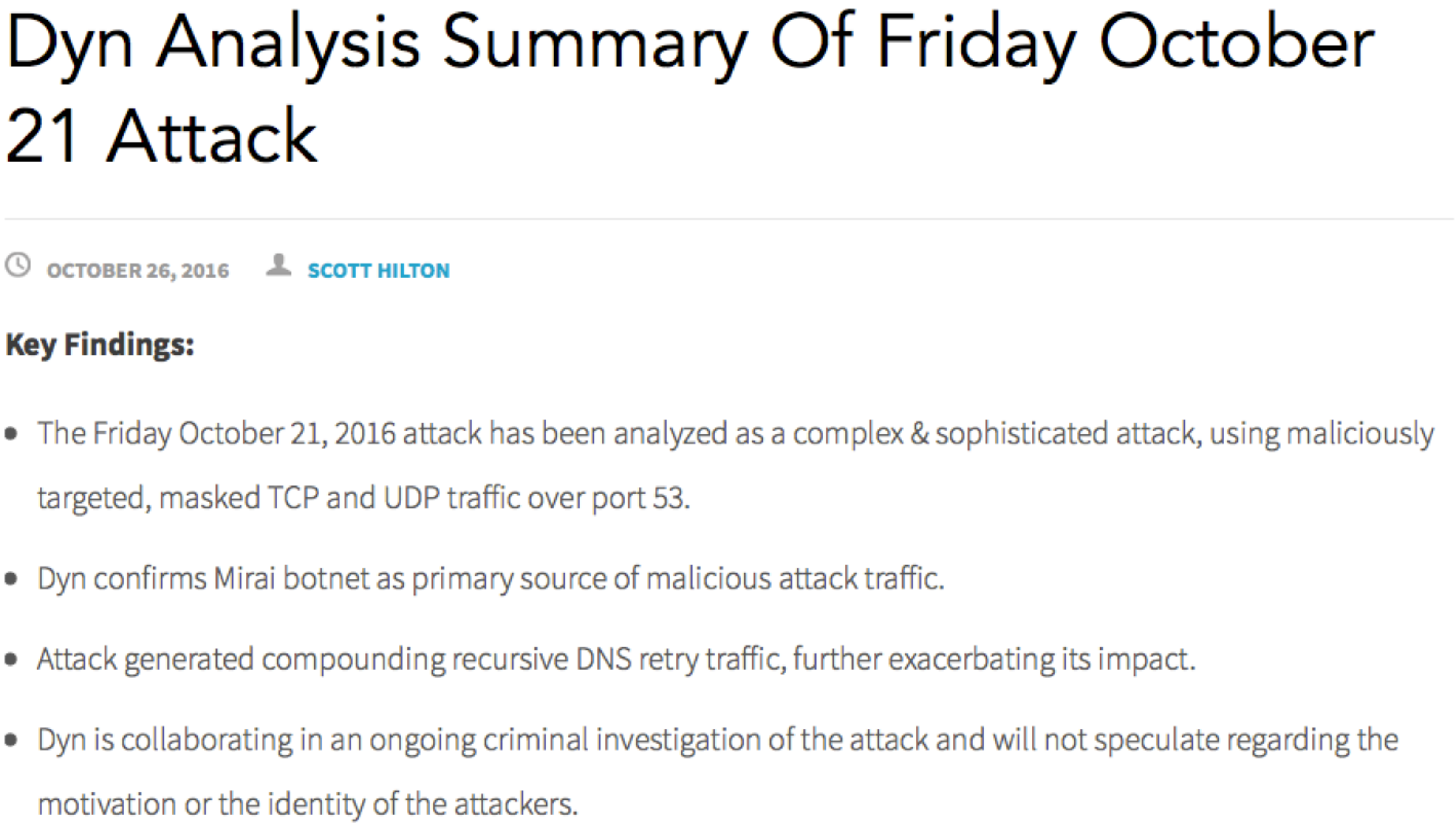
21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

My New B

Dyn was attacked by Mirai botnet



Dyn Analysis Summary Of Friday October 21 Attack

OCTOBER 26, 2016 SCOTT HILTON

Key Findings:

- The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, masked TCP and UDP traffic over port 53.
- Dyn confirms Mirai botnet as primary source of malicious attack traffic.
- Attack generated compounding recursive DNS retry traffic, further exacerbating its impact.
- Dyn is collaborating in an ongoing criminal investigation of the attack and will not speculate regarding the motivation or the identity of the attackers.

- Twitter
- SoundCloud
- Spotify

These are too complex for most of the criminals ...

- Carna, Reincarna, Mirai ... these are complex malware and they had needed knowledge to be developed
- we need less complex solution because we are lazy

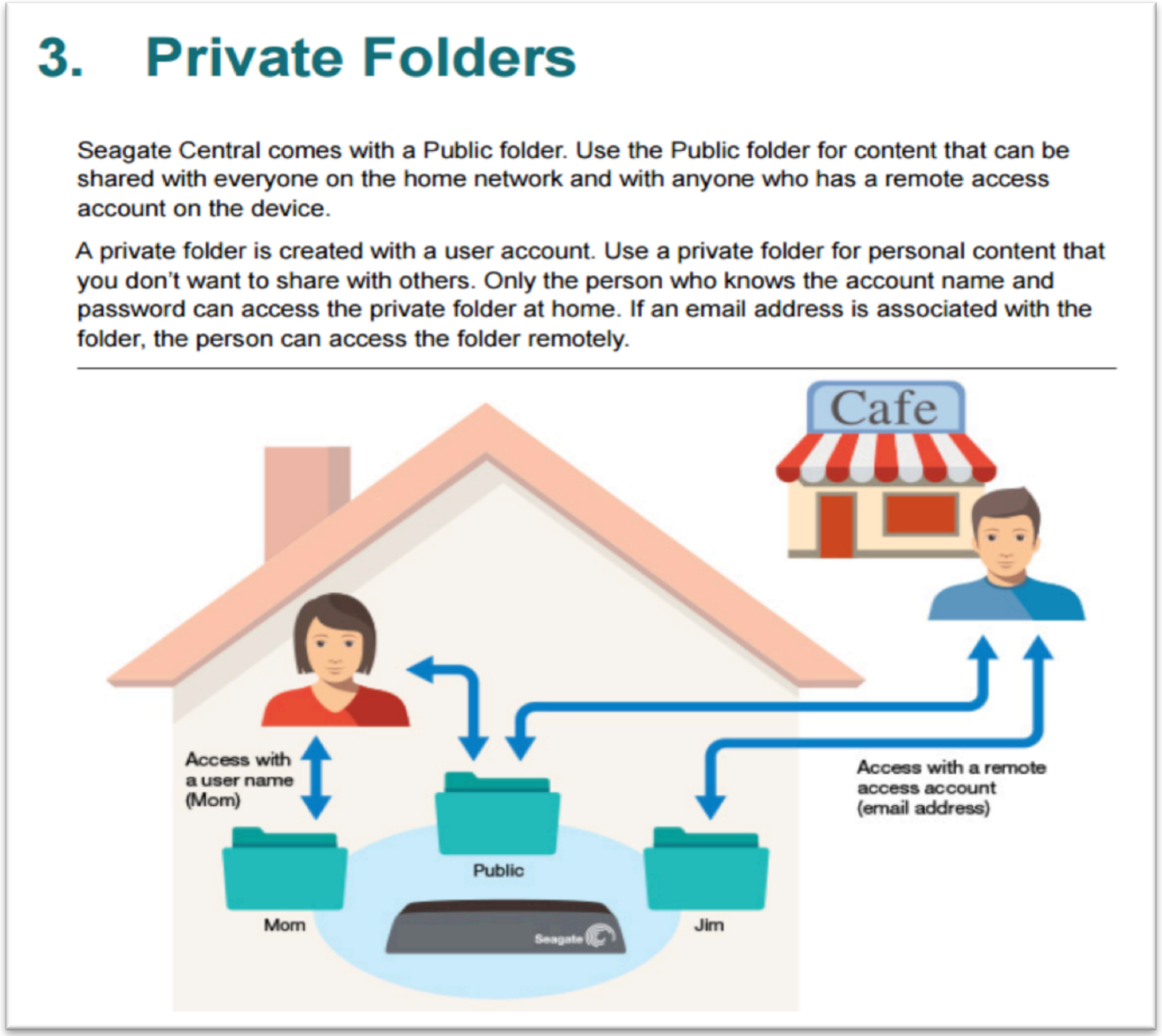
Working a couple of days for half a million of dollar!?

SOPHOS

Seagate Central

LACIE CloudBox

Seagate Central



3. Private Folders

Seagate Central comes with a Public folder. Use the Public folder for content that can be shared with everyone on the home network and with anyone who has a remote access account on the device.

A private folder is created with a user account. Use a private folder for personal content that you don't want to share with others. Only the person who knows the account name and password can access the private folder at home. If an email address is associated with the folder, the person can access the folder remotely.

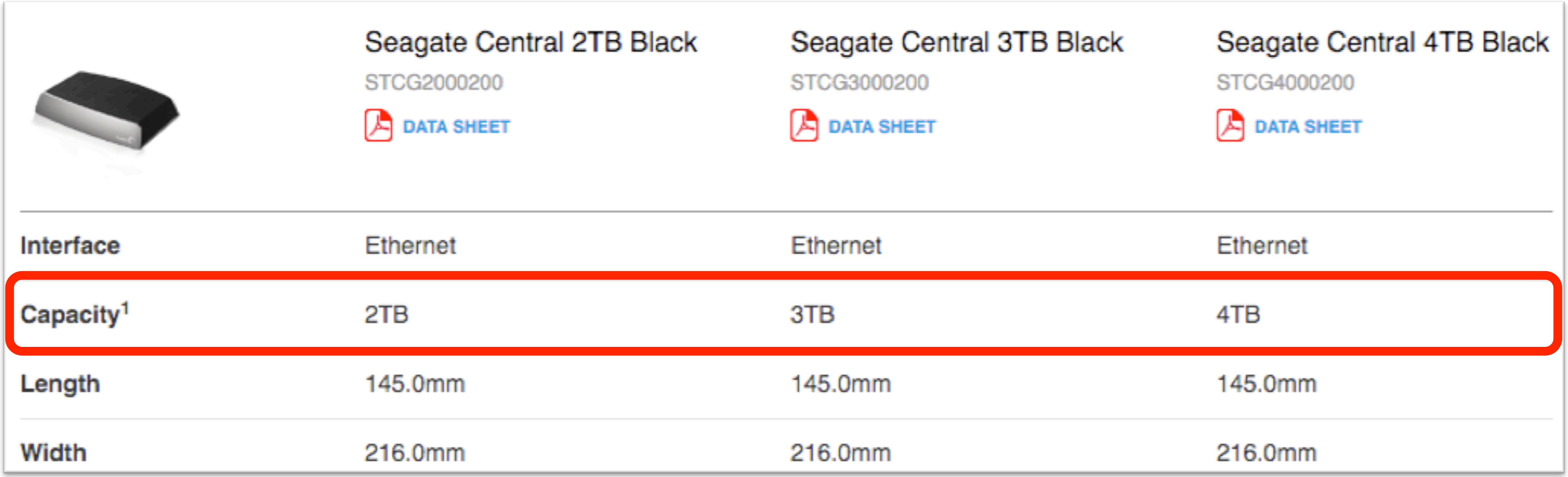
Cafe
Access with a user name (Mom)
Access with a remote access account (email address)
Public
Mom
Jim
Seagate

Design flaw:

- The default (anonymous) user cannot be deactivated!
- If the device is enabled for remote access, all the accounts will be available on the device, **including the anonymous user.**

Seagate Central

383 * 2 TB = 766 TB (free cloud)



	Seagate Central 2TB Black STCG2000200 DATA SHEET	Seagate Central 3TB Black STCG3000200 DATA SHEET	Seagate Central 4TB Black STCG4000200 DATA SHEET
Interface	Ethernet	Ethernet	Ethernet
Capacity[1]	2TB	3TB	4TB
Length	145.0mm	145.0mm	145.0mm
Width	216.0mm	216.0mm	216.0mm

Seagate Central

```
:~# ftp 90.xxx.xx.4
Connected to 90.xxx.xxx.4.
220 Welcome to Seagate Central Shared Storage FTP service.
Name (90.xxx.xxx.4:root): anonymous

ftp> dir

drwxrwsrwx    5 65534    65534          65536 Mar 14 19:29 Public

ftp> cd Public

ftp> dir

150 Here comes the directory listing.
-rw-r--r--    1 0        65534             46 Mar 14 18:52 Seagate Centra[…].url
drwxrwsrwx    3 65534    65534          65536 Feb 25 16:35 Music
-rwxrwxrwx    1 65534    65534        1578496 Feb 25 16:35 Photo.scr
drwxrwsrwx    2 65534    65534          65536 Feb 18 18:49 Photos
drwxrwsrwx    2 65534    65534          65536 Mar 10 22:21 Videos
```

Mal/Miner-C

MAL/MINER-C

CryptoCoin miner

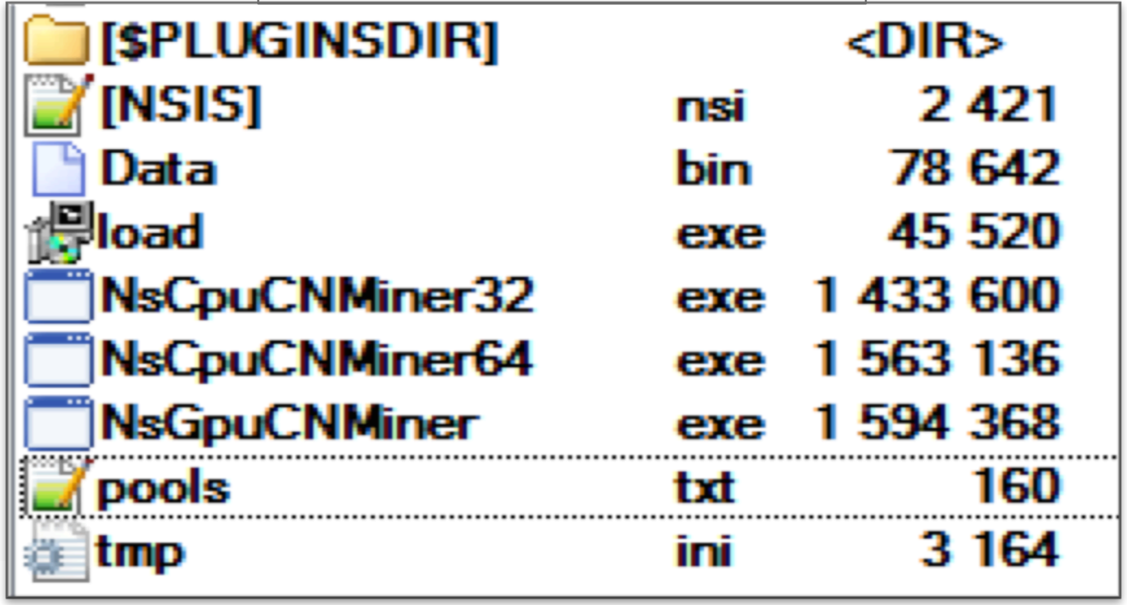
Monero

- Monero (XMR) is an open source cryptocurrency
- created in **April 2014**
- focuses on privacy,
- decentralisation and scalability.
- Unlike many cryptocurrencies that are derivatives of Bitcoin, Monero is based on the CryptoNote protocol and possesses significant algorithmic differences relating to blockchain obfuscation. (Wikipedia)

Mal/Miner-C

Icon of the malware

Components of the malware



[$PLUGINSDIR]		<DIR>
[NSIS]	nsi	2 421
Data	bin	78 642
load	exe	45 520
NsCpuCNMiner32	exe	1 433 600
NsCpuCNMiner64	exe	1 563 136
NsGpuCNMiner	exe	1 594 368
pools	txt	160
tmp	ini	3 164

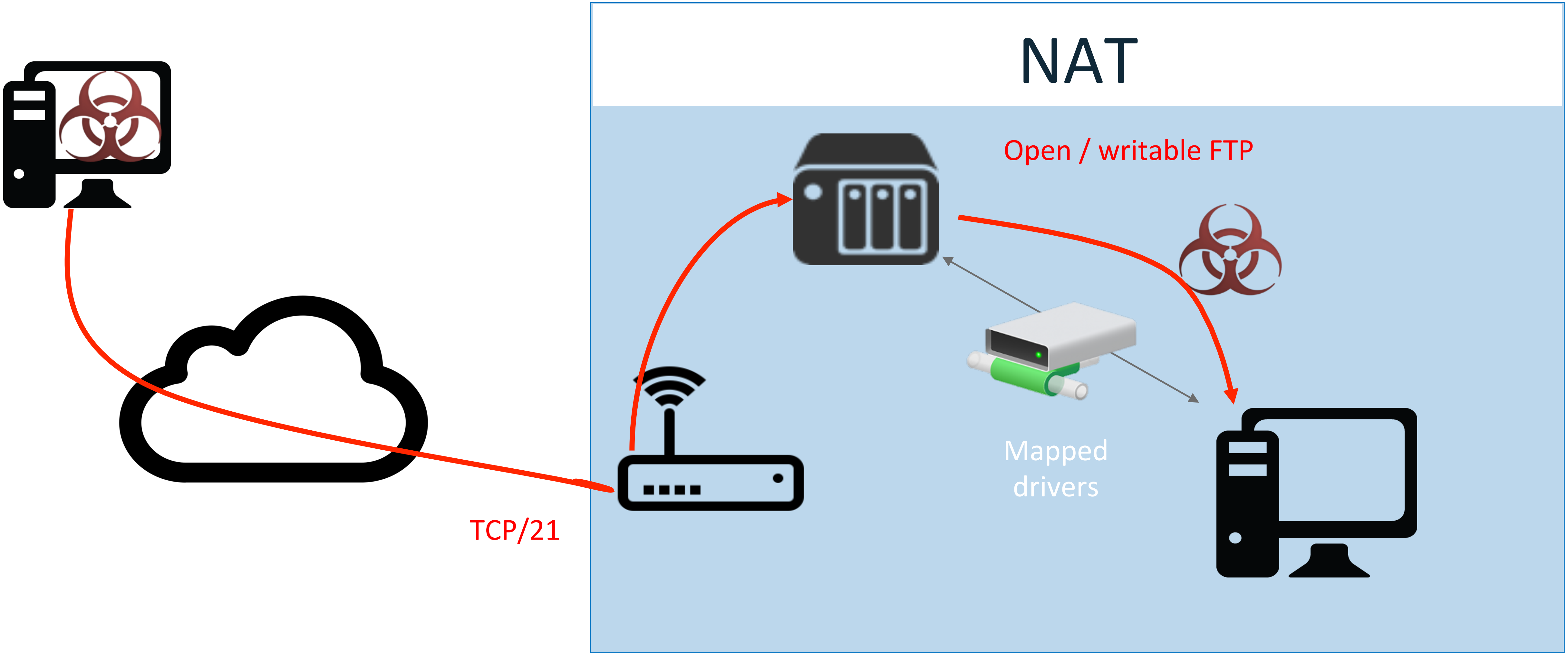
Stock component, freely available

```
66b965d1ee4013c80f7e0e27725e43f3d316325a NsGpuCNMiner.exe
fd358cfe41c7aa3aa9e4cf62f832d8ae6baa8107 NsCpuCNMiner32.exe
ce1fbf382e89146ea5a22ae551b68198c45f40e4 NsCpuCNMiner64.exe
(https://bitcointalk.org/index.php?topic=647251.0)
```

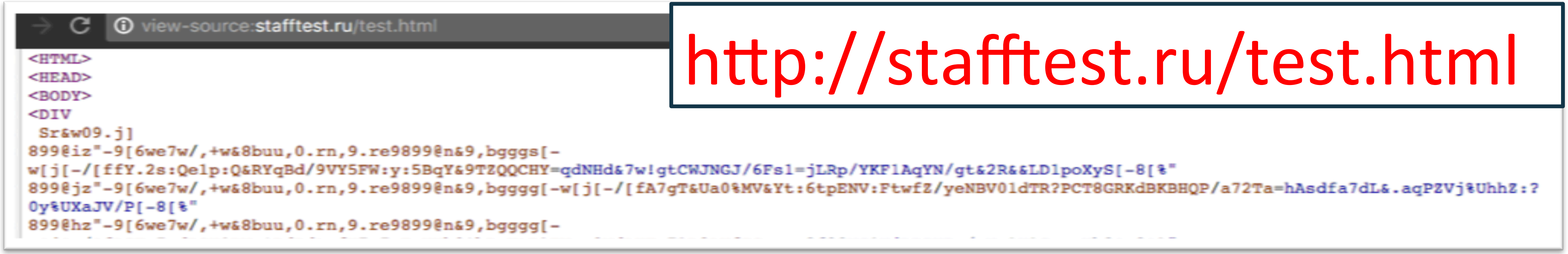
Mal/Miner-C (tftp.exe)

1. Generating random IP addresses
2. Open FTP connection to the server
3. Copying an instance of Mal/Miner-C to all of the folder can be access

Mal/Miner-C (spreading via tftp.exe)



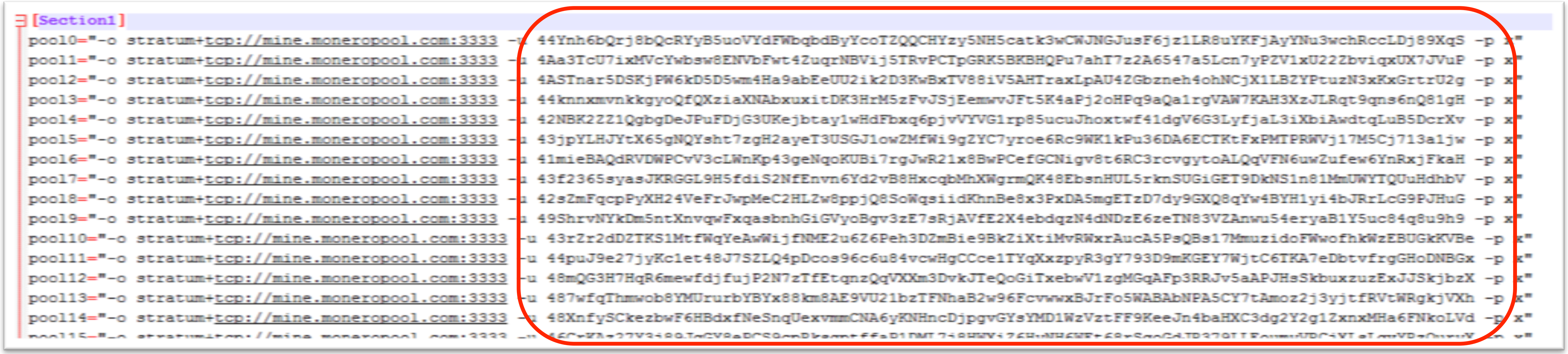
Mal/Miner-C (moneropool)



```
<HTML>
<HEAD>
<BODY>
<DIV
 Sr&w09.j]
899@iz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggs[-
w[j[-/[ffY.2s:Qe1p:Q&RYqBd/9VY5FW:y:5BqY&9TZQQCHY=qdNHd&7w!gtCWJNGJ/6Fs1=jLRp/YKF1AqYN/gt&2R&&LD1poXyS[-8[%"
899@jz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-w[j[-/[fA7gT&Ua0%MV&Yt:6tpENV:FtwfZ/yeNBV01dTR?PCT8GRKdBKBHQP/a72Ta=hAsdfa7dL&.aqPZVj%UhhZ:?
0y%UXaJV/P[-8[%"
899@hz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-
```

http://stafftest.ru/test.html

After deobfuscated by ROT47 with a custom character set:

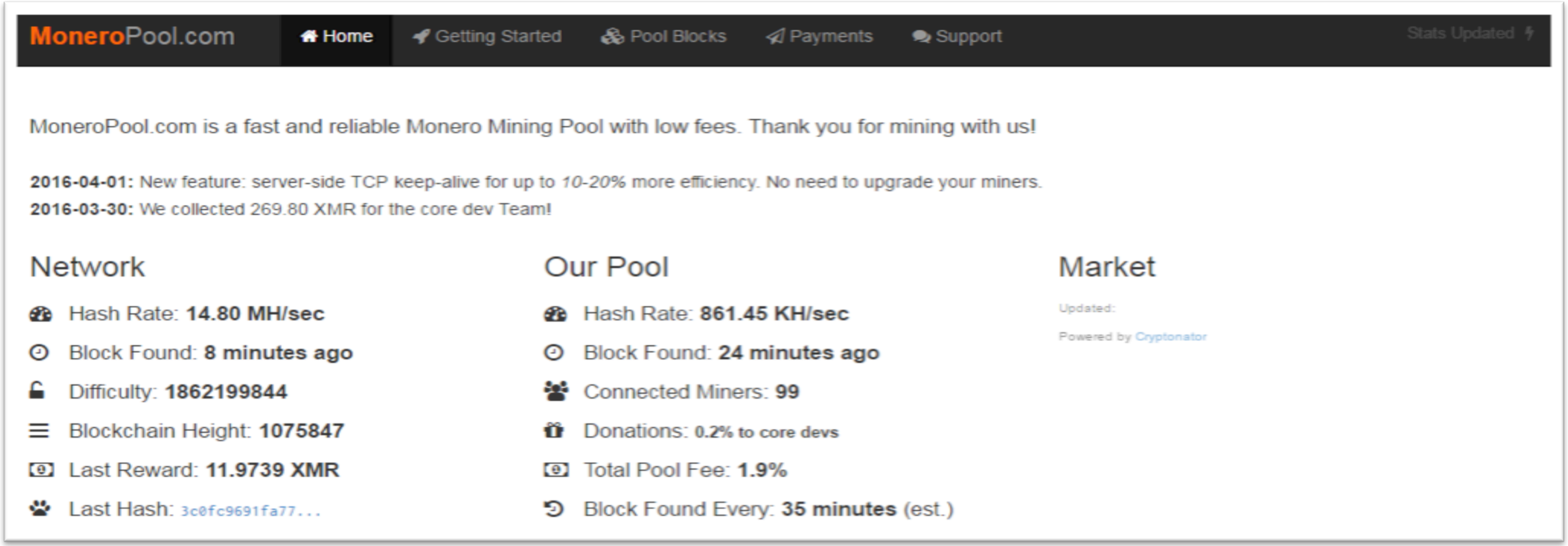


```
[Section1]
pool0="-o stratum+tcp://mine.moneropool.com:3333 -u 44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS -p x"
pool1="-o stratum+tcp://mine.moneropool.com:3333 -u 4Aa3TcU7ixMVcYwbsw8ENVbFwt4ZuqrNBVij5TRvPCTpGRK5BKBHQPu7ahT7z2A6547a5Lcn7yPZV1xU22ZbviqxUX7JVuP -p x"
pool2="-o stratum+tcp://mine.moneropool.com:3333 -u 4ASTnar5DSKjPW6kD5D5wm4Ha9abEeUU2ik2D3KwBxTV88iV5AHTraxLpAU4ZGbzneh4ohNCjX1LBZYPtuzN3xKxGrtrU2g -p x"
pool3="-o stratum+tcp://mine.moneropool.com:3333 -u 44knnxmvnkkgyoQfQXziaXNAbxuxitDK3HrM5zFvJSjEemwvJFt5K4aPj2oHPq9aQa1rgVAW7KAH3XzJLRqt9qns6nQ81gH -p x"
pool4="-o stratum+tcp://mine.moneropool.com:3333 -u 42NBK2ZZ1QgbgDeJPuFDjG3UKejbtay1wHdFbxq6pjvVYVG1rp85ucuJhoxtwf41dgV6G3LyfjaL3iXbiAwdtqLuB5DcrXv -p x"
pool5="-o stratum+tcp://mine.moneropool.com:3333 -u 43jpYLHJYtX65gNQYsht7zgH2ayeT3USGJ1owZMfWi9gZYC7yroe6Rc9WK1kPu36DA6ECTKtFxPMTPRWVj17M5Cj713a1jw -p x"
pool6="-o stratum+tcp://mine.moneropool.com:3333 -u 41mieBAQdRVDWPCvV3cLWnKp43geNqoKUBi7rgJwR21x8BwPCefGCNigv8t6RC3rcvgytoALQqVFN6uwZufew6YnRxjFkaH -p x"
pool7="-o stratum+tcp://mine.moneropool.com:3333 -u 43f2365syasJKRGGL9H5fdiS2NfEnvn6Yd2vB8HxcgbMhXWgrmQK48EbsnHUL5rknSUGiGET9DkNS1n81MmUWYTQUuHdhbV -p x"
pool8="-o stratum+tcp://mine.moneropool.com:3333 -u 42sZmFqcpPyXH24VeFrJwpMeC2HLZw8ppjQ8SoWgsiidKhnBe8x3PxDA5mgETzD7dy9GXQ8qYw4BYH1yi4bJRrLcG9PJHuG -p x"
pool9="-o stratum+tcp://mine.moneropool.com:3333 -u 49ShrvNYkDm5ntXnvqwFxqasbnhGiGVyoBgv3zE7sRjAVfE2X4ebdqzN4dNDzE6zeTN83VZAnwu54eryaB1Y5uc84q8u9h9 -p x"
pool10="-o stratum+tcp://mine.moneropool.com:3333 -u 43rZr2dDZTKS1MtfWqYeAwWijfNME2u6Z6Peh3DZmBie9BkZiXtiMvRWxrAucA5PsQBs17MmuzidoFWwofhkWzEBUGkKVBe -p x"
pool11="-o stratum+tcp://mine.moneropool.com:3333 -u 44puJ9e27jyKc1et48J7SZLQ4pDcos96c6u84vcwHgCCce1TYqXxzpyR3gY793D9mKGEY7WjtC6TKA7eDbtvfrgGHoDNBGx -p x"
pool12="-o stratum+tcp://mine.moneropool.com:3333 -u 48mQG3H7HqR6mewfdjfujP2N7zTfEtqnzQqVXXm3DvkJTeQoGiTxebwV1zgMGqAFp3RRJv5aAPJHsSkbuxzuzExJJSkjbzX -p x"
pool13="-o stratum+tcp://mine.moneropool.com:3333 -u 487wfqThmwob8YMUrurbYBYx88km8AE9VU21bzTFNhaB2w96FcvwwxBJrFo5WABAbNPA5CY7tAmoz2j3yjtfRVtWRgkjVXh -p x"
pool14="-o stratum+tcp://mine.moneropool.com:3333 -u 48XnfySCkezbwF6HBdxfNeSnqUexvmmCNA6yKNHncDjpgvGYsYMD1WzVztFF9KeeJn4baHXC3dg2Y2g1ZxnxMHa6FNkoLVd -p x"
```

Let's speak about money

SOPHOS

Mal/Miner-C (moneropool.com)



MoneroPool.com is a fast and reliable Monero Mining Pool with low fees. Thank you for mining with us!

2016-04-01: New feature: server-side TCP keep-alive for up to *10-20%* more efficiency. No need to upgrade your miners.
2016-03-30: We collected 269.80 XMR for the core dev Team!

Network

- Hash Rate: **14.80 MH/sec**
- Block Found: **8 minutes ago**
- Difficulty: **1862199844**
- Blockchain Height: **1075847**
- Last Reward: **11.9739 XMR**
- Last Hash: 3c0fc9691fa77...

Our Pool

- Hash Rate: **861.45 KH/sec**
- Block Found: **24 minutes ago**
- Connected Miners: **99**
- Donations: **0.2% to core devs**
- Total Pool Fee: **1.9%**
- Block Found Every: **35 minutes** (est.)

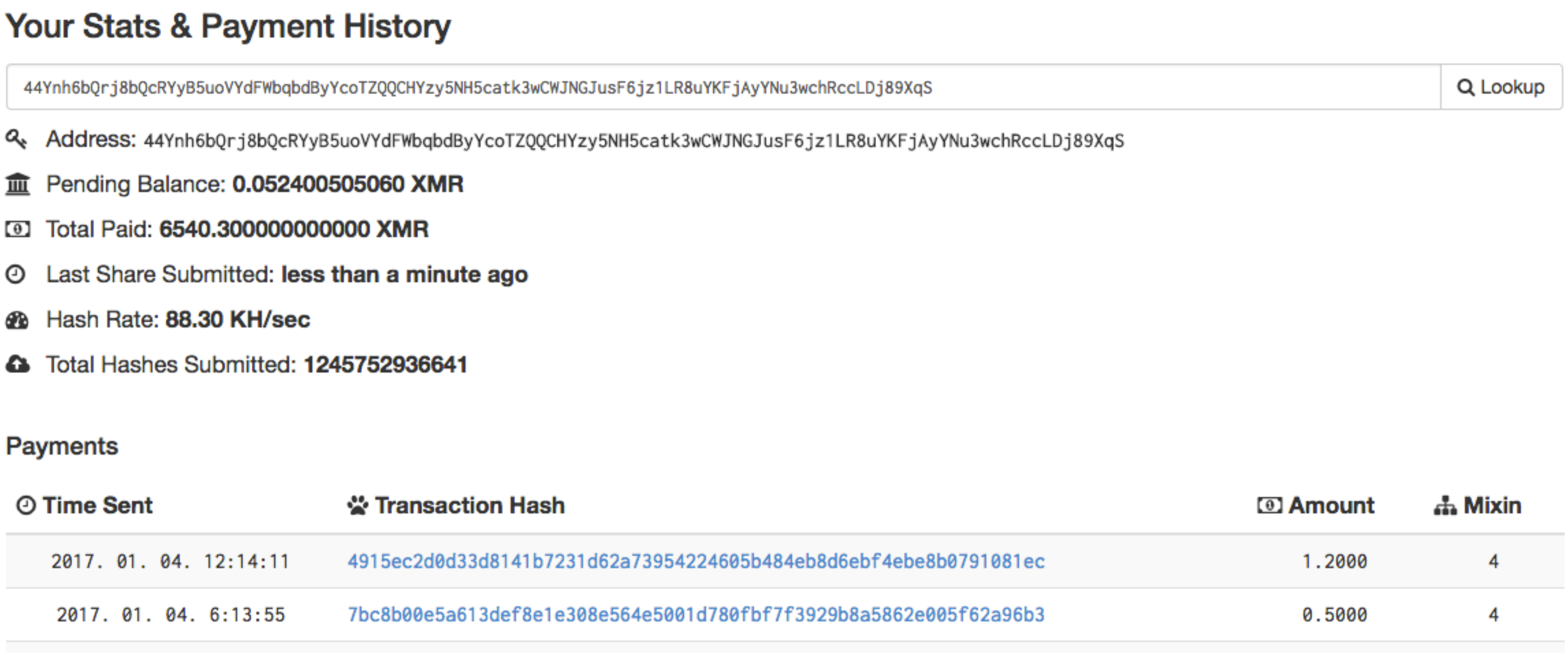
Market

Updated:

Powered by Cryptonator

```
stratum+tcp://mine.moneropool.com:3333
stratum+tcp://xmr.hashinvest.net:1111
stratum+tcp://monero.crypto-pool.fr:3333
stratum+tcp://mine.cryptoescrow.eu:3333
```

Mal/Miner-C (moneropool.com)



Your Stats & Payment History

44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS

Address: 44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS

Pending Balance: **0.052400505060 XMR**

Total Paid: **6540.300000000000 XMR**

Last Share Submitted: **less than a minute ago**

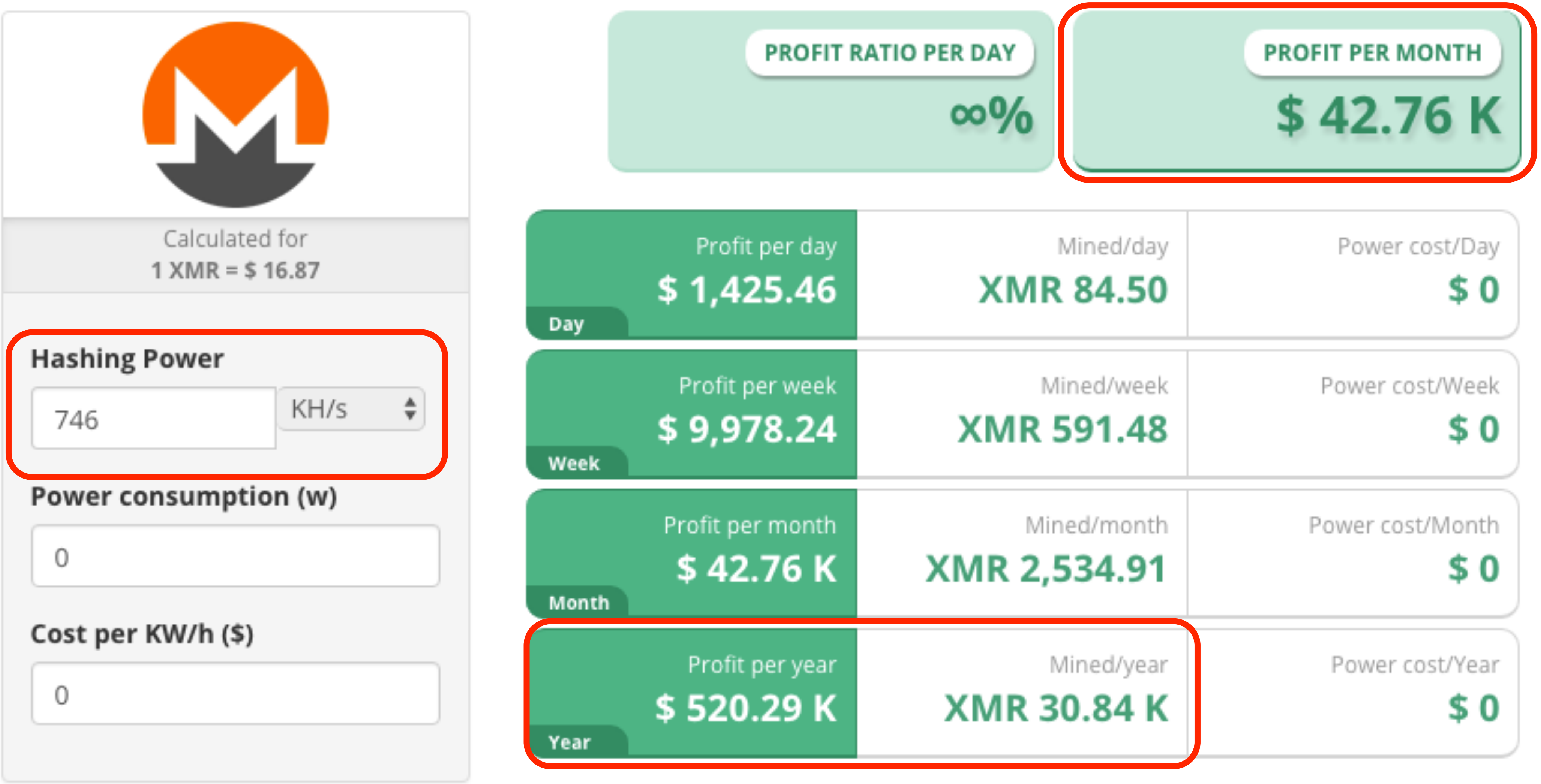
Hash Rate: **88.30 KH/sec**

Total Hashes Submitted: **1245752936641**

Payments

Time Sent	Transaction Hash	Amount	Mixin
2017. 01. 04. 12:14:11	4915ec2d0d33d8141b7231d62a73954224605b484eb8d6ebf4ebe8b0791081ec	1.2000	4
2017. 01. 04. 6:13:55	7bc8b00e5a613def8e1e308e564e5001d780fbf7f3929b8a5862e005f62a96b3	0.5000	4

Mal/Miner-C (profit calculation)



Calculated for
1 XMR = $ 16.87

Hashing Power

746 KH/s

Power consumption (w)

0

Cost per KW/h ($)

0

PROFIT RATIO PER DAY
∞%

PROFIT PER MONTH
$ 42.76 K

Day	Profit per day $ 1,425.46	Mined/day XMR 84.50	Power cost/Day $ 0
Week	Profit per week $ 9,978.24	Mined/week XMR 591.48	Power cost/Week $ 0
Month	Profit per month $ 42.76 K	Mined/month XMR 2,534.91	Power cost/Month $ 0
Year	Profit per year $ 520.29 K	Mined/year XMR 30.84 K	Power cost/Year $ 0

Total paid by MoneroPool is:

73.240 XMR

=

US$ 1.2 M

SOPHOS

World FTP scan

The result of the scan

SOPHOS

FTP test

1. Tries to login with Anonymous user on TCP port 21

2. Check, do we have write access on the devices or not?

FTP scan - init dataset

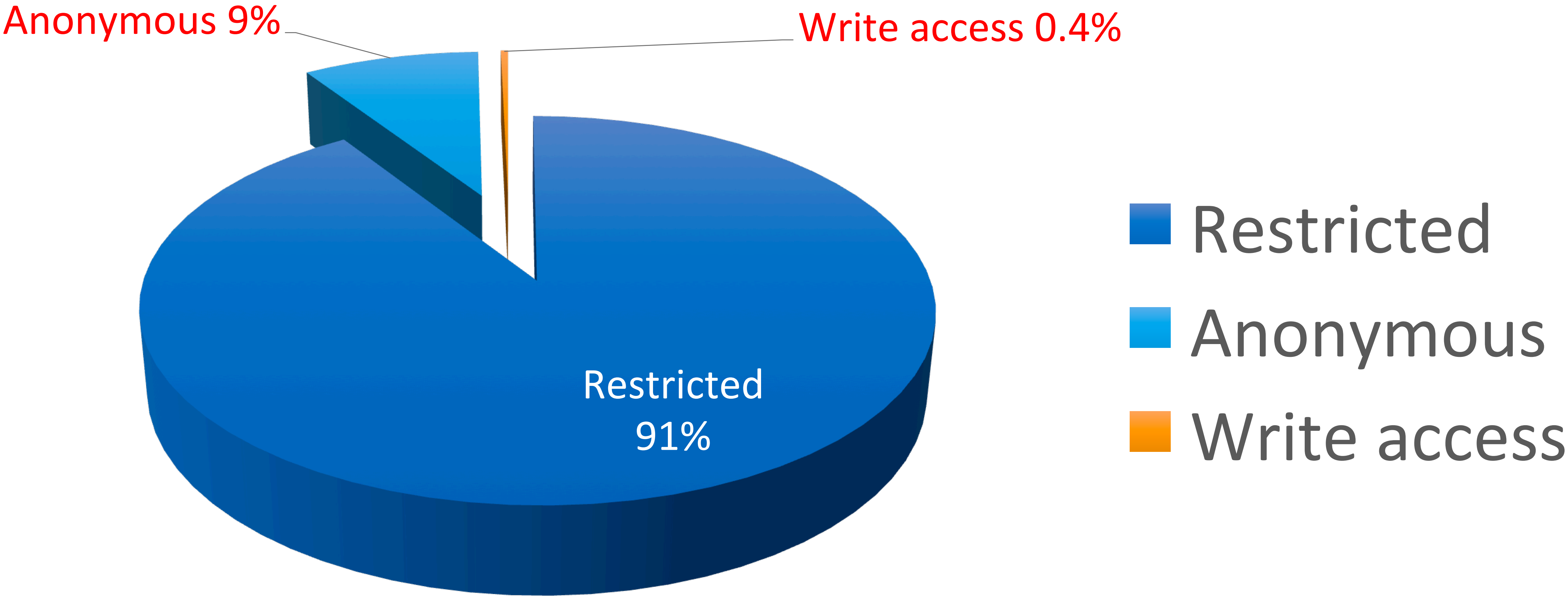
- From censys.io we got 12.350.314 IP addresses

12 million IP addresses

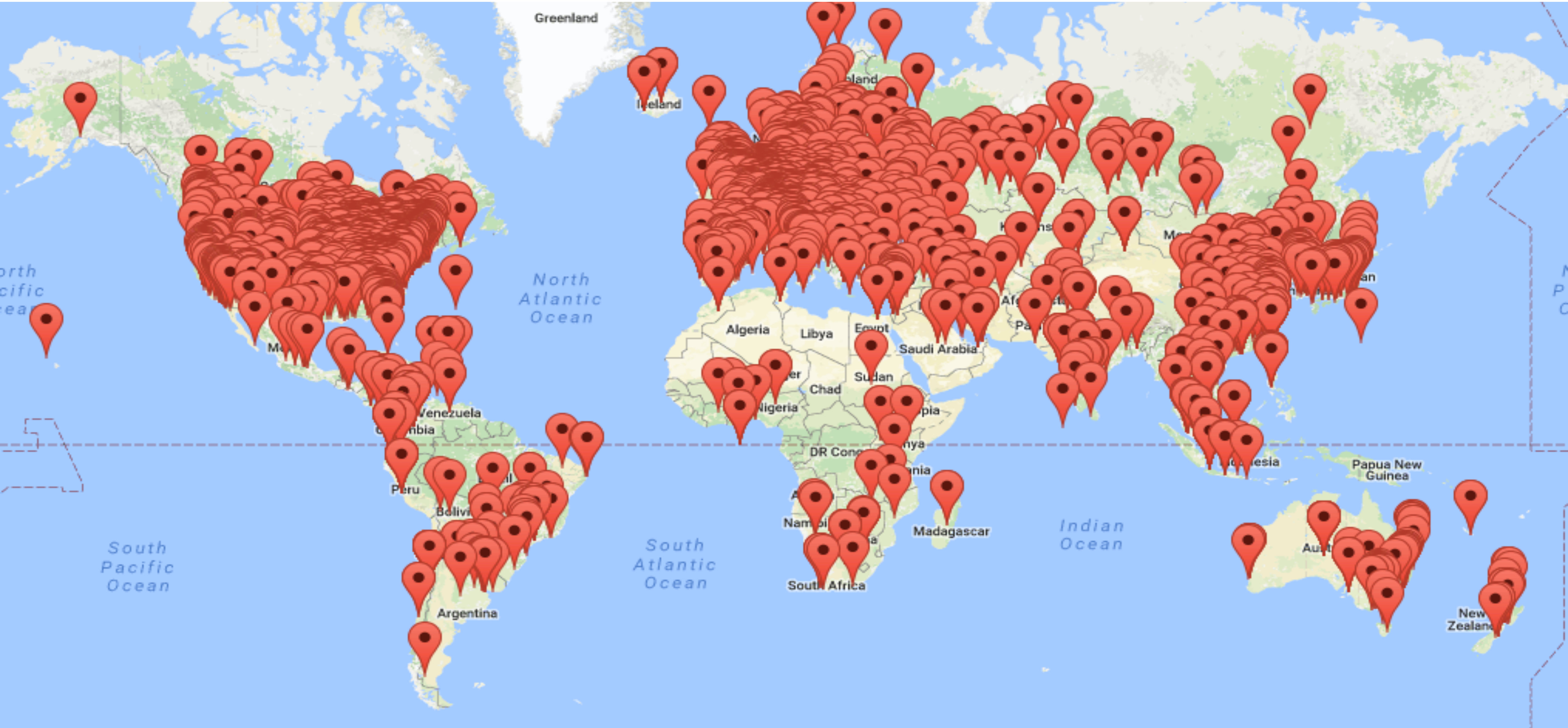
- And we have tested 3.426.381 IP addresses from this

3,5 million IP addresses

FTP scan result (one third - 3,5M devices)



10K (10337) FTP server where you can host your malware



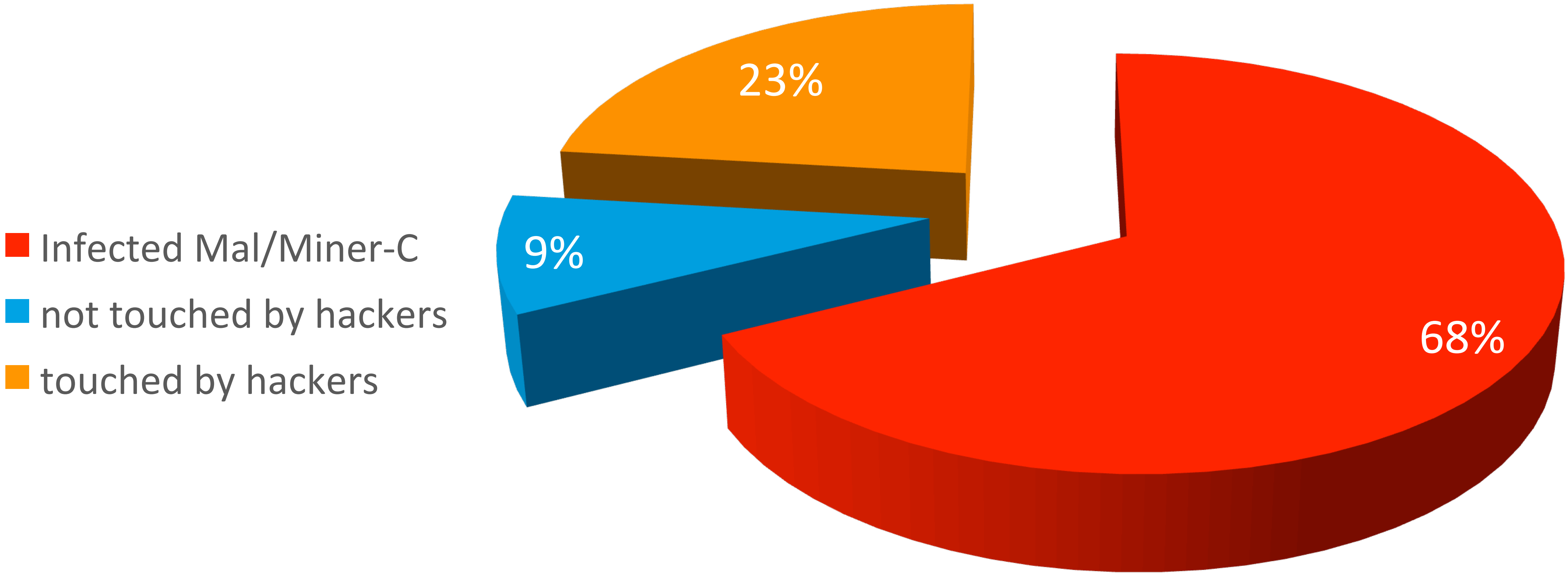
The results (extrapolation for 12M)

Using this ratio for 12 million of IP addresses means that:

~ 37K (37.050)

FTP server can be used to host malware!

FTP scan (one third – anonymous with rw access)



Final thoughts

- Even with this lazy malware criminals could earn more than US$1 million

- no need to develop a good malware to earn good money

- victims would have been protected following basic security steps

- using FTP service with right setting would prevent the spreading of this malware totally

Questions?

SOPHOS

Security made simple.

attila.marosi@sophos.com

attila.marosi@gmail.com

PGP ID: 3782A65A

PGP FP.: 4D49 1447 A4E1 F016 F833
8700 8853 60A7 3782 A65A