Seyfullah KILIÇ Follow

Oct 25, 2017 · 4 min read · Listen

Hacking Cryptocurrency Miners with OSINT Techniques

NOTE: All the methods I have explained are at your own risk

Sponsored by https://swordeye.io

SWORDEYE

swordeye.io

We will be gathering critical data for Cryptocurrency Miners (Bitcoin[Antminer] and Ethereum[Claymore]) in this article.

Many Cryptocurrency miners tools and software need the internet connection to send/receive data. So that, they have some vulnerability for attackers.

Reconnaissance the Antminer!

The best bitcoin ASIC miner is Antminer S9/S7. The miner's hardware use "lighttpd/1.4.32" web server and some of these have open SSH Port. There is an exploit for "Lighttpd 1.4.31" version. However, you can not access the server with this exploit.

The webpage on the web server is protected by "Digest HTTP Authentication". The critical point is that miners need username and password to log in.

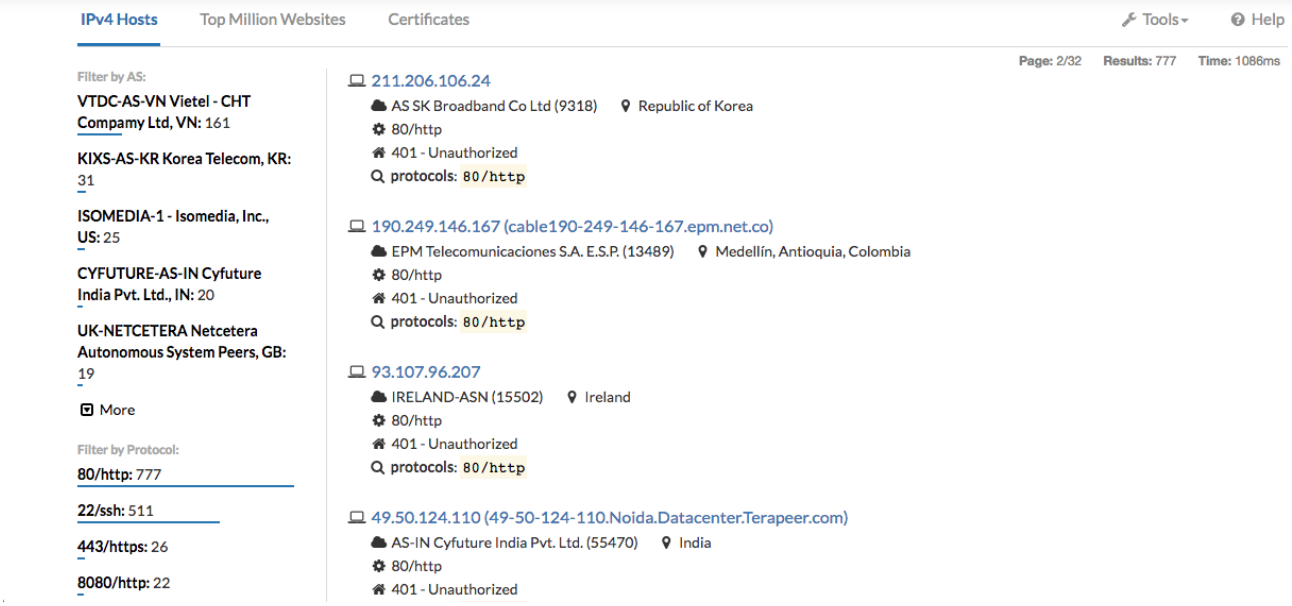
80.http.get.body_sha256	a0a8e1aa8fcbca7d2596c72c9132e79af36588990c236c435a210e09168feb08
80.http.get.headers.content_length	351
80.http.get.headers.content_type	text/html
80.http.get.headers.server	lighttpd/1.4.32
80.http.get.headers.unknown	{u'value': u'Sat, 22 Jan 2000 09:19:12 GMT', u'key': u'date'}
80.http.get.headers.www_authenticate	Digest realm="antMiner Configuration", nonce="76bd3b6617882d389102170ba3990b9c", qop="auth"
80.http.get.metadata.description	lighttpd 1.4.32
80.http.get.metadata.product	lighttpd
80.http.get.metadata.version	1.4.32
80.http.get.status_code	401
80.http.get.status_line	401 Unauthorized

antMiner configuration page uses "Digest Authentication"

It's known that we need some information or keywords to collect data with OSINT techniques. That information is the keyword including "antMiner Configuration" in HTTP headers which appears each time I send a request to the server

I have searched on censys.io and shodan.io with some specific dorks and collected the IP addresses.

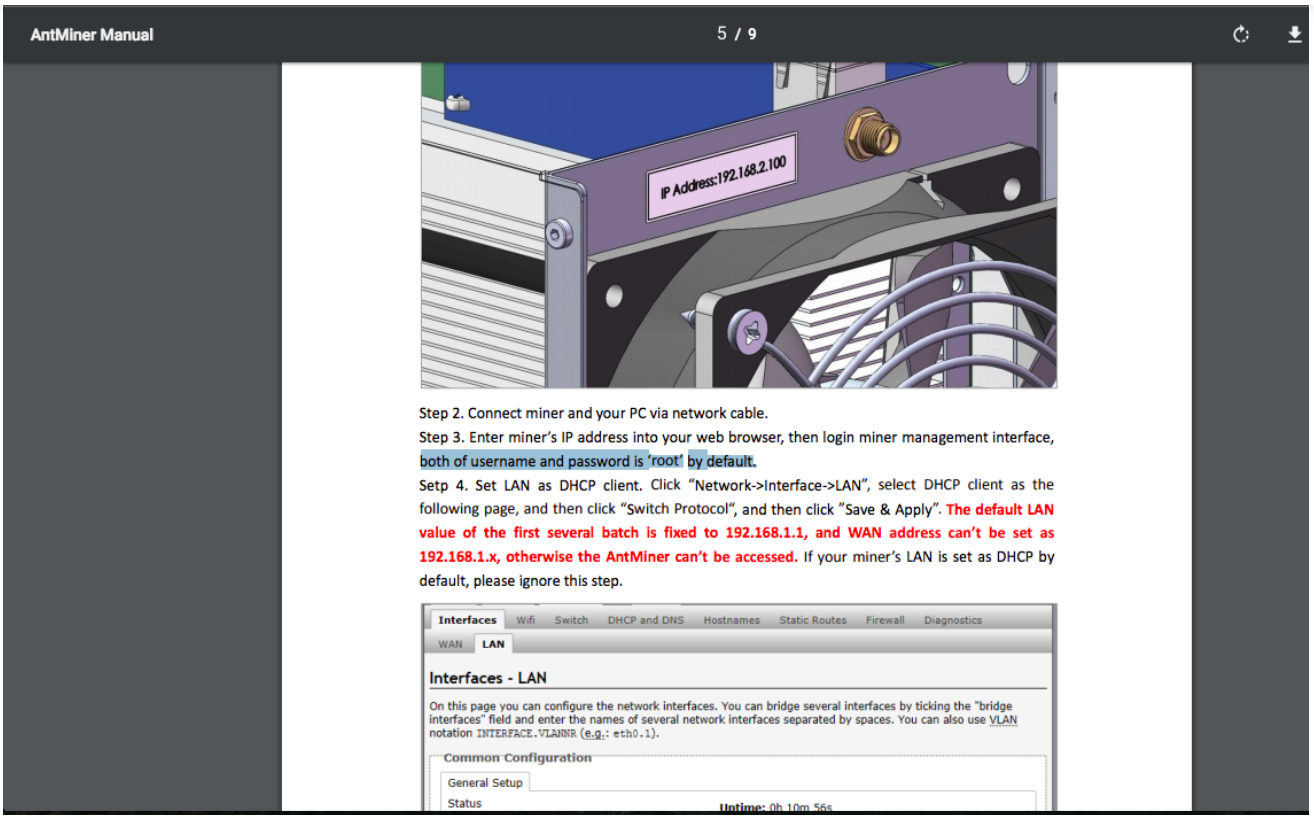
```
(antminer) AND protocols.raw: "80/http" AND 80.http.get.title: "401"
```



censys.io search dorks

The system can be accessed by a brute-force attack on the HTTP port or SSH port.

Firstly, I needed a user guide to learn default HTTP username and password. After, I have searched on Google with “antminer default password” and found a website that includes User Guide.

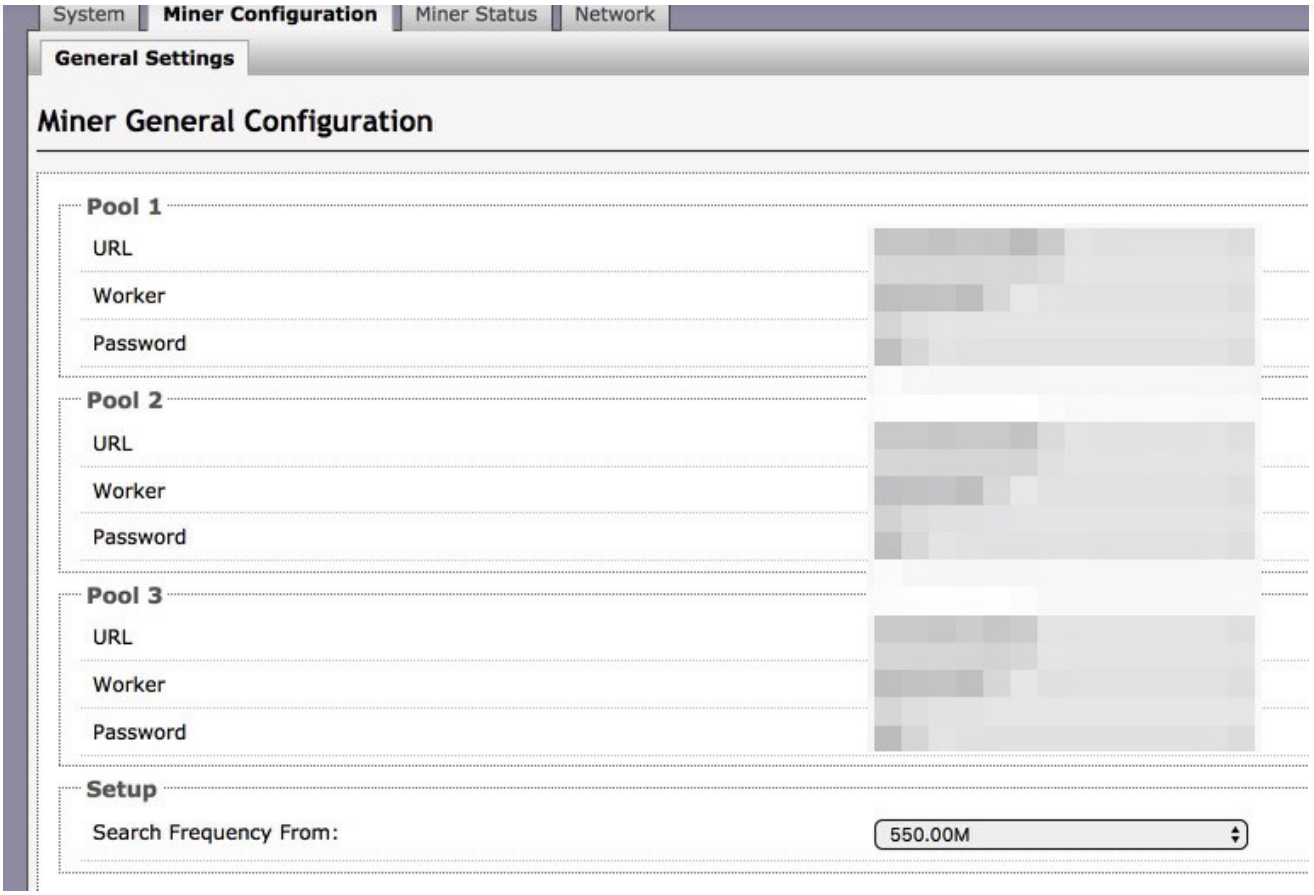


AntMiner User Manuel | We can obtain easily by searching

For this tutorial, I preferred to use hydra for brute-force attack (Bruteforcing HTTP Digest Authentication) with exposed most common 10.000 passwords. You can also use Burp Suite Intruder too.

```
hydra -l root -P commonPasswords.txt -vV {TARGET} http-get /
```

If you are lucky, you can access the configuration page.



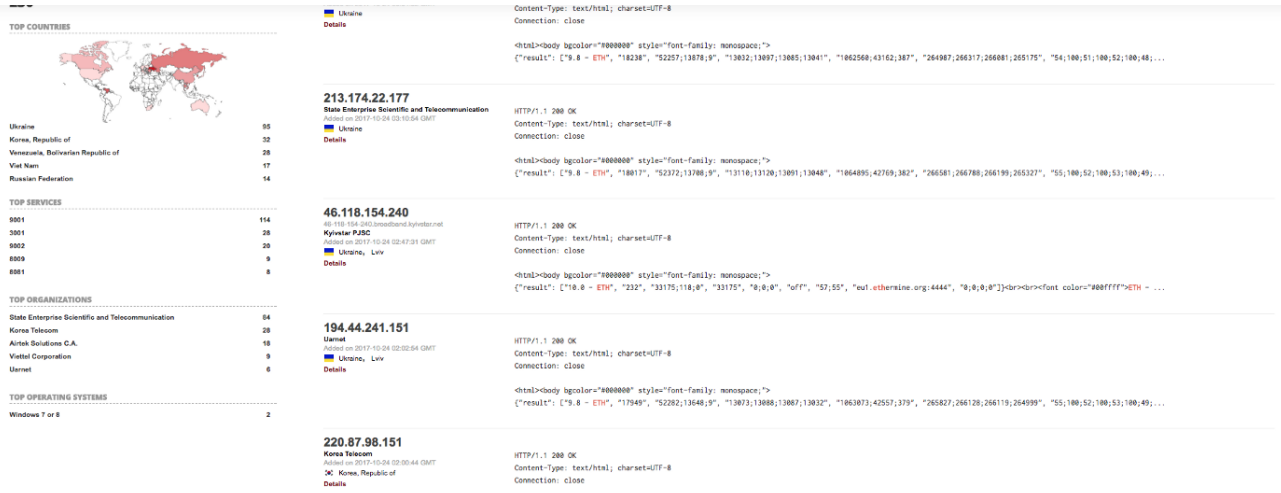
antMiner configuration page.

Attackers can edit the page as desired.

Claymore Miner Software

Another type of attack is also targeting the Claymore Miner Software (such as Altcoins, ethereum, zcash miner)

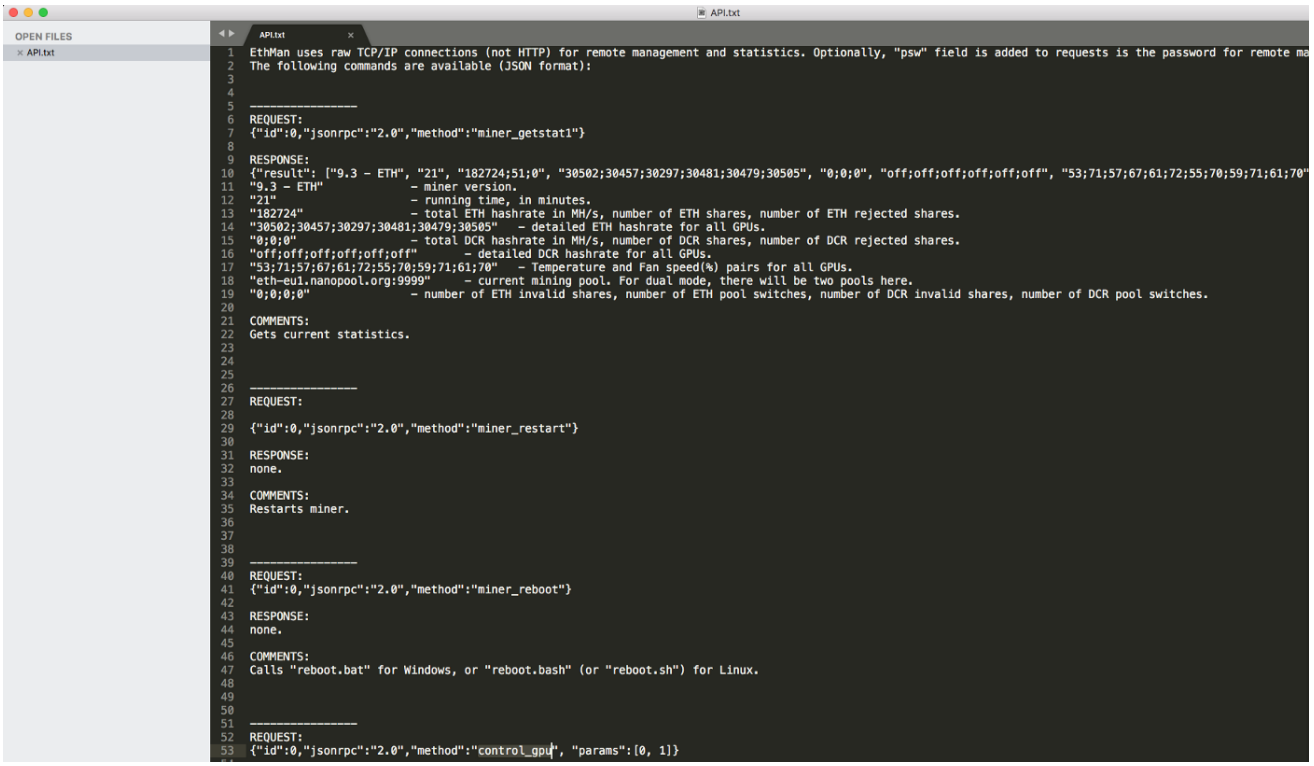
I've made another search on shodan.io with some specific dorks.



Dorks: “ETH — Total Speed:”

You can send some JSON packets with Claymore Remote Manager API to manage the miner server remotely.

In here, we control GPUs (disable, dual mode etc.) or edit the config.txt to change the pool wallet address with sending some commands.



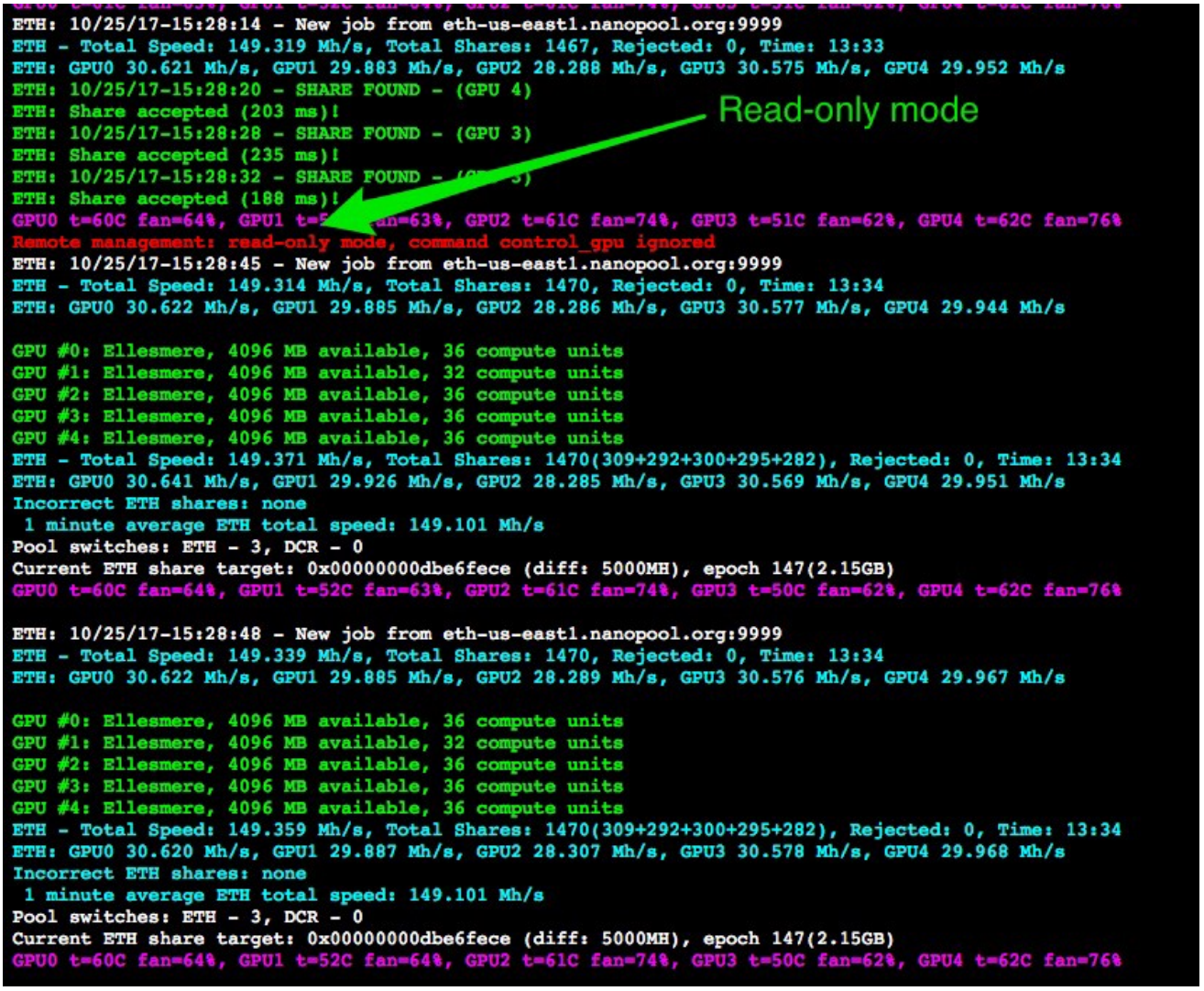
Claymore Remote Manager API.txt

We will send “miner_restart” or “control_gpu” command to detect whether it is read-

This code gives the statistics of the miner server.

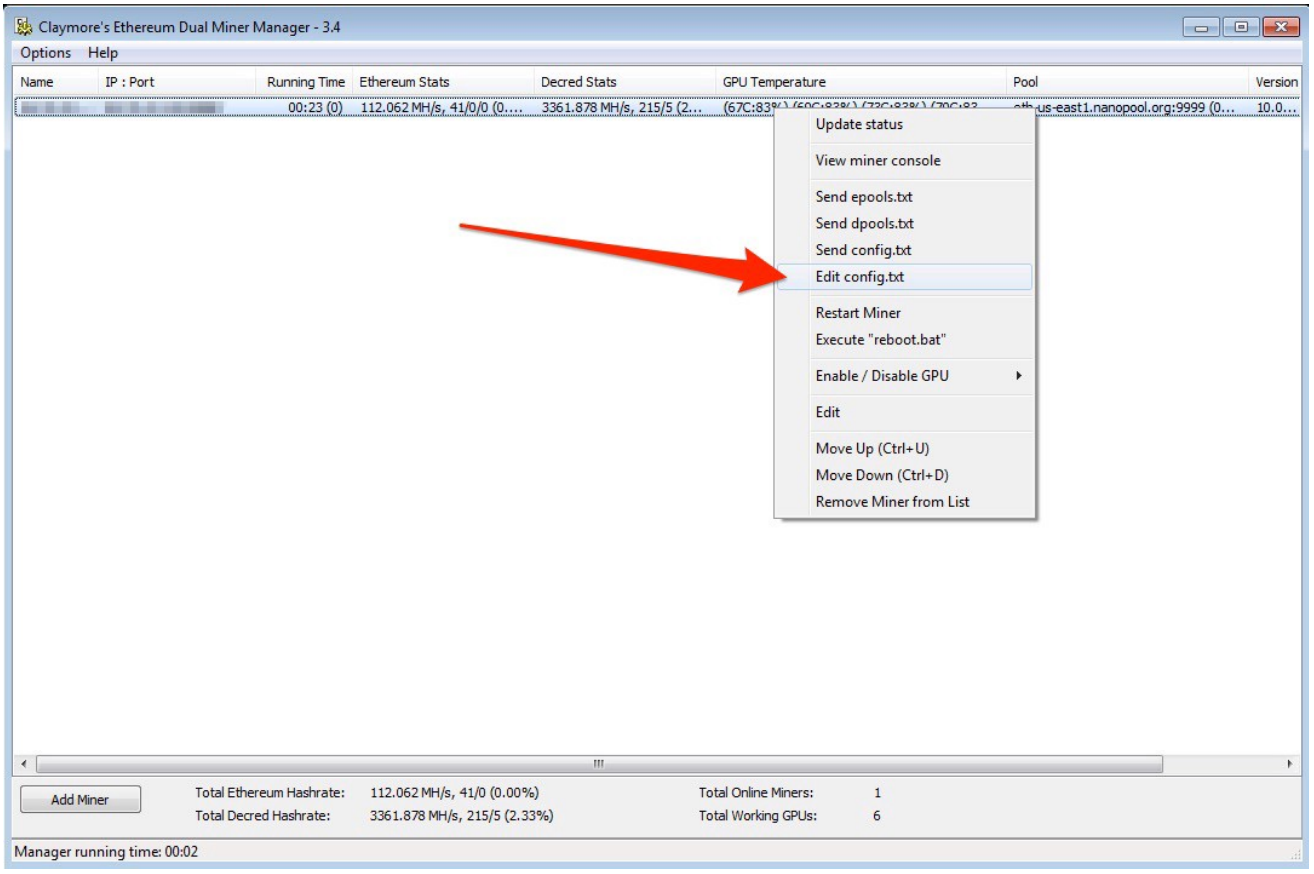
After that, we try to send command with “control_gpu” to detect whether it is read-only or write/read.

We received an error with the code sent below.

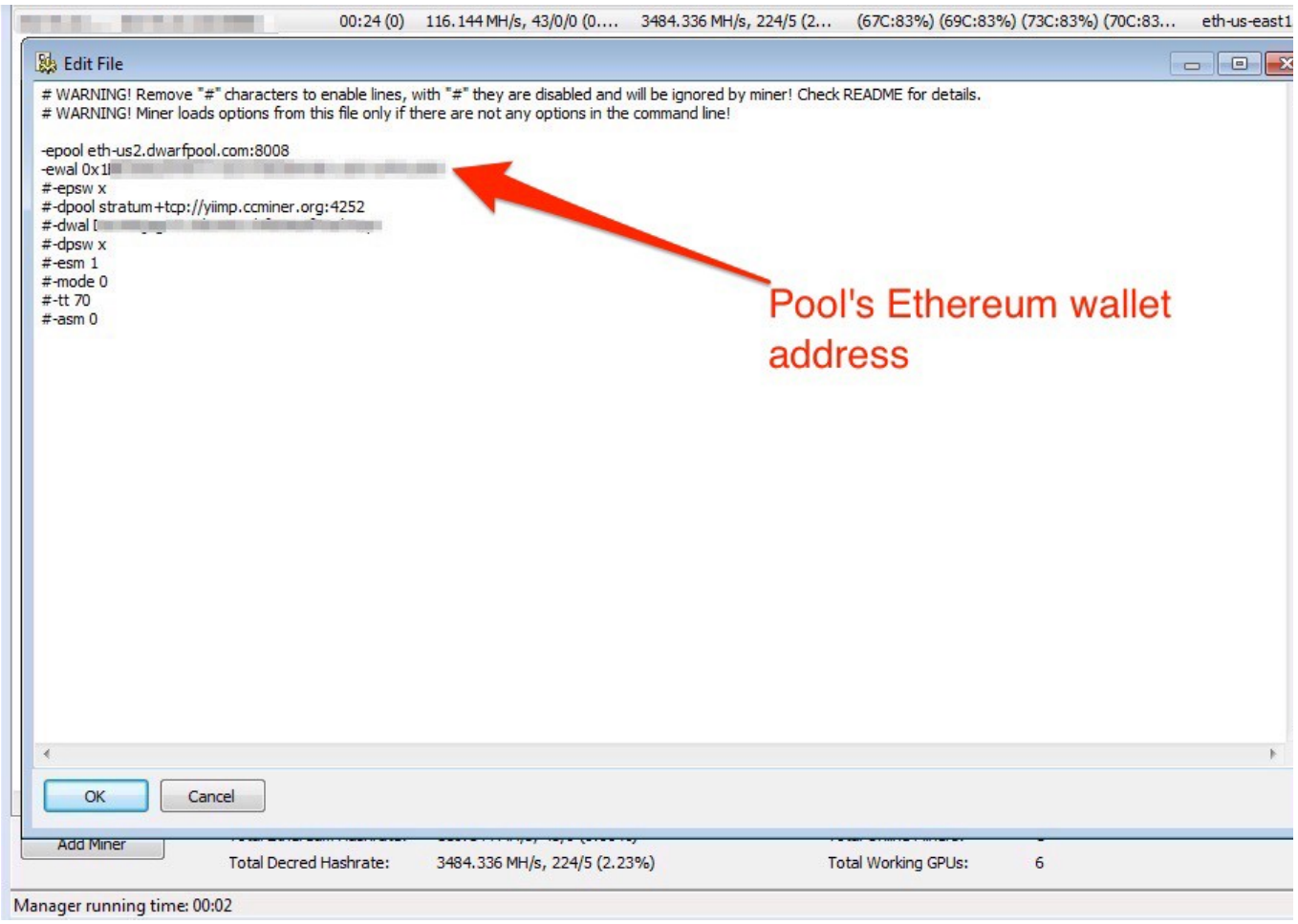


Restarting miner server

Claymore Remote Manager also allows you edit the config file with using JSON format (sending json file). However, you can edit easily with using the Claymore's Ethereum Dual Miner Manager on Windows also can change pool wallet address too.



if you have read/write permission, you can edit config.txt



You can see/edit pool's wallet address

Hacking Fantasy :)

- I did not try command injection on Claymore Miner Software with sending JSON command. If it has vulnerability, you can access the server without having read/write permission.
- 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 :)

Donation

BTC: 3EcwymByc9J3HaBFHrnXM6qZixTm2SrDpo
ETH: 0xde8f1d620a547e0819e9652536b3dd8ffac15f21