01 Introduction
02 Incident Response and Investigation
03 Enriched Malware Analysis
04 Reconstructing the Original Attack
05 Threat Actor's TTP and Capabilities
06 Attacker's Profit
Introduction - whoami

• Ladislav Bačo

• Senior Security Consultant and Malware Analyst | LIFARS

• 10+ years of experiences in Computer Security, Computer Science and Education

• Former head of the Department of Cyber Threat Analysis | CSIRT.SK

• Practical hands-on with real APT and targeted attacks
Malware Analysis + ThreatIntel + OSInt... Why?

• Generic threat detections and threat descriptions by AV can be insufficient
• Malware Analysis can significantly accelerate DFIR process
• Need to know exact purpose and abilities of malware samples
• Threat Intelligence can reveal the origin of malware and associated Threat Actor
• Threat Intelligence can help to recover the missing pieces of puzzle
• Collect more relevant IOCs for Threat Hunting and Monitoring
What to search

- Hash
- Munin [https://github.com/Neo23x0/munin](https://github.com/Neo23x0/munin)
- URL
- Domain
- IP address
- FileName
- Category
- Tags
- Embedded strings
- Imphash
- Relations and similar samples
Where to search

- VirusTotal
- Hybrid-Analysis, Any.Run
- MalShare
- URLHaus
- Intezer
- Shodan, Censys
- ThreatConnect, RecordedFuture (browser plugin)
- NSRL database
- Lot of others, see
  - https://zeltser.com/malware-sample-sources/
  - https://malwareanalysis.tools/
  - https://osintframework.com/
Useful tools and platforms

- Maltego
- VirusTotal Graph API
  - [https://www.virustotal.com/graph/embed/6f26f5e068c2479fb69d7b5e2684af1f](https://www.virustotal.com/graph/embed/6f26f5e068c2479fb69d7b5e2684af1f)
- Intezer
- IDA Pro Plugin Community Edition
  - [https://youtu.be/cvJDpH7d-o](https://youtu.be/cvJDpH7d-o)
Case Study - CoinMiners

- March - May 2020
- Enterprise network with thousands of endpoints
- IT department noticed high load of some computers caused by regsvr32 running as a service
- There are also some odd autoruns-related stuff (tasks, services)
- After sample submission the AV company reported the file as CoinMiner
- Scan by one antivirus does not revealed nothing interesting, but after manual upload of DLLs associated with regsvr32 the AV company identified it as a CoinMiner
- Let's start with the Incident Response and Forensic Analysis
Running Processes and Persistence

➢ As a part of incident response process, there were collected the auto-starting items
➢ SysInternals Autoruns
➢ Signatures checks
➢ NSRL checks

<table>
<thead>
<tr>
<th>Name</th>
<th>PID</th>
<th>User</th>
<th>CPU</th>
<th>Threads</th>
<th>Opened Files</th>
<th>Connections</th>
<th>Start Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>svc</td>
<td>svchost.exe...</td>
<td>Signature</td>
<td>NSRL</td>
<td>MTS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svc</td>
<td>svchost.exe...</td>
<td>HashFound</td>
<td>2018-09-15T02:07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>svc</td>
<td>msuc.exe</td>
<td>HashFound</td>
<td>2018-09-15T02:07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cmd</td>
<td>locale.nls</td>
<td>NameFound</td>
<td>2018-09-15T02:07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>con</td>
<td>SortDefault...</td>
<td>HashFound</td>
<td>2018-09-15T02:07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>irp</td>
<td>svchost.exe</td>
<td>NameFound</td>
<td>2018-09-15T02:07</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Irp wercpl.dll

bac wshbth. name: wercplsupporte.dll
svcpquotnp.path: C:\Windows\System32\wercplsupporte.dll
Ran Apps: 3866576
ptx adat.dll md5: 3e9350230df413dc88fb4a8116c2673b
Reg dhcpsvsha256b: b31f7152a547fa41c3f9c5617b2cd7131a93f7c328bf6da360dc1586ba18dc
Sys winnr. signature: NotSigned
smc nlaapi. nsl: NotFound
nnt dhcpsvsha256: 2020-04-25T07:58:26
win IPHLAPI: 2020-05-29T03:48:38.379789
nt dnsapi. nsl: 2020-05-29T03:58:53.082208
win mssock.dll < OK >
ser wldp.dll
isa powprof.dll C:\Windows\System32\powprof.dll VerificationError; NameFound 2018-09-15T02:07
fon msas1.dll C:\Windows\System32\msas1.dll VerificationError; NameFound 2018-09-15T02:07
svc kernel.appc... C:\Windows\System32\kernel.appc... VerificationError; NameFound 2018-09-15T02:07
fon profap1.dll C:\Windows\System32\profap1.dll VerificationError; NameFound 2018-09-15T02:07
svc msvecp_win.dll C:\Windows\System32\msvecp_win.dll VerificationError; NameFound 2018-09-15T02:07

--- < OK >
CoinMiners samples

- Initial analysis
- String search
- XMRig CoinMiner
- Monero cryptocurrency
CoinMiners Samples

- Manual Analysis
- Strings, Imports, exports
  - Exported functions DllRegisterServer and `fackaaxv`
- Mutex `Samplexn07`
  - Can be used as IOC for monitoring and hunting
- String search on Hybrid-Analysis => similar samples
CoinMiners samples

- Analysis of another DLL
- Strings, Disassembling
Schtasks Backdoor

- Forensic Analysis revealed x.bat file and couple of suspicious tasks
- x.bat content:
  ```powershell
echo off
exit
```
  ```
regsvr32.exe /u /s /i:"c:\windows\temp\scripttempx.tks" scrobj.dll
```
- The file scripttempx.tks contained nccat payload
- 4-years old Schtasks-Backdoor
  - [https://github.com/re4lity/Schtasks-Backdoor](https://github.com/re4lity/Schtasks-Backdoor)
DLLs dropped by IIS

- Forensic Analysis revealed the DLLs in C:\Windows\Temp; dropped by IIS
- Mixed mode assembly; empty C# class + native reverse shell
- Differences:

![Code Snippet]

- Maybe exploitation of ASP.NET vulnerability => CVE-2019-18935 in Telerik Web UI
Another Persistence and Remediation

- WMI Event Subscription
  - Event Filter (time based)
  - Event Consumer (cmd.exe)
  - Binding

- IR => Cleaning the malicious artifacts => powershell script => executed wersplsupport (???)

- Analysis of Process Monitor log revealed COR_Profiler (for .NET applications) via CLSID
Intermezzo

➢ What did we discover until now?
➢ Samples:
  ➢ XMRig-based CoinMiners
  ➢ DLL Installer for CoinMiners
  ➢ Schtasks-Backdoor
  ➢ Telerik WebUI exploit and mixed-mode DLLs with reverse shell
➢ Persistence:
  ➢ Services
  ➢ Scheduled tasks
  ➢ WMI Event Subscription
  ➢ COR_Profiler
  ➢ Wercplsupport(e), regsvr32, rundll32, CLSID, Environment Variables
Enrichment of our Findings

➢ Too many samples, how did they infect the system and create all of the persistence?

➢ Search malware repositories for relevant samples from February-May 2020
  ➢ Bingo on Any.Run
Samples from Threat Intelligence

- ZIP archive from Any.run
- xg.dll - XMRig CoinMiner
- comhij.dll - DLL Installer, used also as COR_Profiler
- x.mof - WMI Event Subscription
- nwgold DLL, rn.bat, set.bat - unknown
Samples from Threat Intelligence

- Batch files:
  - `rn.bat` - installer script
  - `set.bat` - unpacker script
  - `let.exe` and `set.zip` (?)

---

```
@echo off
if exist c:\programdata\set.zip ( del c:\programdata\set.zip )
if exist c:\programdata\set.zip.tmp ( del c:\programdata\set.zip.tmp )
c:\programdata\let.exe -t -p c:\programdata\rn.bat -l 11121 -d {88C3F05E-0D50-440b-a531-95550C24C678}
c:\programdata\xg.dll c:\programdata\x.mof c:\programdata\x.mof
```
Hunting for set.zip and let.exe

➢ One submission of set.zip on Hybrid-Analysis
  ➢ It can be download with vetted account
  ➢ Contains let.exe, too

let.exe - Juicy Potato Local Privilege Exploit
  ➢ https://github.com/ohpe/juicy-potato
Last sample: nwgold DLL

- Mixed-mode DLL called nwgold_2020042608284350_x86.dll
- Empty .NET class
- Native code – dropper of set.bat
- Looks familiar?
Remote Shell and nwgold Comparison
Video

My new blog post about the #BlueMockingbird #XMRig #CoinMiner malware samples. Where and how to find them, collect them and analyze them using @anyrun_app

#ThreatIntel #malwareanalysis #DFIR #cybersec

malwarelab.eu/posts/blue-moc...
app.any.run/tasks/318e4886...

https://twitter.com/ladislav_b/status/1273938499096494080
Attacker's profit

- XMRig configuration
- Extracted from PCap or memory dumps
- Crypto-mining pool parameters
- e.g. pass (or Worker ID): "fm1b1l2x"
- Track pools for statistics per attacker's accounts

<table>
<thead>
<tr>
<th>Account</th>
<th>Supportxmr.com</th>
<th>Xmr.nanopool.org</th>
<th>Minexmr.com</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 (Any.Run)</td>
<td>41.97</td>
<td>13.03</td>
<td>10.44</td>
<td>65.44</td>
</tr>
<tr>
<td>02 (private)</td>
<td>13.33</td>
<td>39.15</td>
<td>30.92</td>
<td>83.40</td>
</tr>
</tbody>
</table>

- Total profit: approx 150 XMR ~ 13k USD
- Damages: approx 50k-500k USD per victim
Summary

- Reconstruction of attack steps
- Blue Mockingbird capabilities and TTPs:
  - Public tools from GitHub
  - Slightly customized
  - Re-use of C&C server
  - "put-it-all-together" ability
  - Research, persistence
  - Own installers and unpackers
- Victim's Damages >> Attacker's Profit
Resources

- https://twitter.com/ladislav_b/status/127398499096494080
- https://redcanary.com/blog/blue-mockingbird-cryptominer/
- https://malwarelab.eu/posts/xmrig-blue-mockingbird/
- https://malwarelab.eu/posts/blue-mockingbird-hunting/
- https://github.com/re4lity/Schtasks-Backdoor
- https://github.com/xmrig/xmrig
- https://analyze.intezer.com/#/analyses/f5972783-5d57-43ca-8bb3-dca08741936f
- https://github.com/ohpe/juicy-potato
- https://app.any.run/tasks/66ab973a-cb28-4cd5-b91b-f747bc188bef/
- https://www.hybrid-analysis.com/sample/71fc0b93199d965d5a4f3f55850db7a4a60ffbc1afbcc5861a9309164e4439e9
- https://app.any.run/tasks/318e4886-35da-4d71-8610-fb6b3964d04b/
- https://app.any.run/tasks/265f984f-355a-4c72-9768-54dc89b7319b
- https://app.any.run/tasks/e6dc9624-1819-4fb7-b70e-75c879954d02/
THANK YOU
LIFARS
your digital world, secured
QUESTIONS?