Hunting with Sysmon to Unveil the Evil

Felipe “Pr0teus” Esposito
@pr0teusBR

Rodrigo “Sp0oKeR” Montoro
@spookerlabs
About us

Felipe Esposito
@pr0teusbr
Senior Researcher Tenchi Security
Senior Instructor at BlueOps

Rodrigo Montoro
@spookerlabs
Senior Researcher Tenchi Security
Senior Instructor at BlueOps
Motivation
Agenda

● Sysmon Basics

● Sysmon Field Hunter (SFH)
  ○ Events analyzed
  ○ Structure
  ○ Scoring Library
  ○ Results

● SFH & Elastic for the Hunting
SYSMON
Sysmon

- Launched August of 2014
- Current Version 10.4
- 22 events
- Last update September/2019
 Sysmon Capabilities

- Process creation
- DNS queries
- Network Connections
- Registry modifications
- File creation
- WMI Events
- Very flexible configuration file
Sysmon

Event Properties - Event 1, Sysmon

Event Type: CreateKey
ProcessGuid: {243f52d9-eb0c-5d87-0000-0010424e0500}
ProcessId: 4840
Image: C:\Windows\Explorer.EXE
TargetObject: HKUS-1-5-21-2975874552-2426477775-714492526-500\Software\Microsoft\Internet Explorer\Toolbar

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 12
Level: Information
User: SYSTEM
OpCode: Info
More Information: Event Log Online Help

Task Category: Registry object added or deleted (i)
Computer: WIN-G9N4R7ROQH
Sysmon Field Hunter (SFH)
What is SFH?

- Analysis based mostly in an unique event
- Flexible scoring system
- Hunting tool
- Alert Fatigue helper
- Not a silver bullet
SFH flow structure
Events Coverage (1st phase)

- Process Creation
  - Event ID 1
- Registry Events
  - Event ID 12
  - Event ID 13
  - Event ID 14

SYSMON
Future Events Coverage (2nd phase)

- Network Connection
  - Event ID 3
- File Create
  - Event ID 11
- WMI Events
  - Event ID 19
  - Event ID 20
  - Event ID 21
SFH in the Shell

[root@elastic sysmonfieldhunter]# python sfh.py -h
usage: sfh.py [-h] -i INDEX -t TIMEFRAME -s SIZE -q QUERY -e EVENTID -m MODE
[-db DATABASES] [-summary SUMMARY] [-save] [--tag TAG]

Sysmon Field Hunter - BlueOps Labs

optional arguments:
  -h, --help                show this help message and exit
  -i INDEX, --index INDEX   Index name
  -t TIMEFRAME, --timeframe TIMEFRAME
                            Timeframe
  -s SIZE, --size SIZE      Number max events response
  -q QUERY, --query QUERY   query filter
  -e EVENTID, --eventid EVENTID
                            Sysmon EventID
  -m MODE, --mode MODE      low / medium / high / paranoid
  -db DATABASES, --databases DATABASES
                            directory with db files (default db/)
  -summary SUMMARY, --summary SUMMARY
                            Just show general stats
  -save, --save             Save results to Elasticsearch
  --tag TAG                 Add a TAG
Event ID 1: Process Creation

```
{ "event": {
    "action": "Process Create (rule: ProcessCreate)",
    "created": "2019-10-06T16:32:00.384Z",
    "module": "sysmon",
    "category": "process",
    "type": "process_start",
    "kind": "event",
    "code": 1
}
},
"process": {
"args": [
    "C:\Windows\system32\PING.EXE",
    "uol.com.br"
],
"working_directory": "C:\Users\Administrator\",
"parent": {
    "args": [
        "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
    ],
    "name": "powershell.exe",
    "entity_id": "{52c960fe-e171-5d9a-0000-001096321300}"
}
},
"user": {
    "domain": "WIN-KBJR7N0PMAA",
    "name": "Administrator"
}
```
Event ID 12 13 14: Registry Events

```
"process": {
  "entity_id": "{52c960fe-b9ca-5d9a-0000-00100b508000}"
},
"pid": 4396,
"executable": "C:\\Windows\\system32\\reg.exe",
"name": "reg.exe"
},
"channel": "Microsoft-Windows-Sysmon/Operational",
"record_id": 1602,
"opcode": "Info",
"event_id": 13,
"provider_name": "Microsoft-Windows-Sysmon",
"event_data": {
  "EventType": "SetValue",
  "TargetObject": "HKLM\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\osk.exe\\Debugger",
  "Details": "C:\\windows\\system32\\cmd.exe"
},
"provider_guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}"
},
"task": "Registry value set (rule: RegistryEvent)"
},
"event": {
  "created": "2019-10-07T04:06:36.566Z",
  "kind": "event",
  "code": 13,
  "action": "Registry value set (rule: RegistryEvent)",
  "module": "sysmon"
}
```
Scoring Library - Event ID 1

- admin access
- whitelist process
- creator company
- cli regex
- work hours
- cli byte count
- (entropy + score)*
- token
- directory path*
- common commands*
- parent versus process*
- host risk*
- command hash*
- entropy
Scoring Library - Event ID 12, 13, 14

- work Hour
- whitelist process
- blacklist registry
- event Type
- targetobject
- entropy
Scoring samples (1 / 5)

id: Pu8XgW0BL6gH7RcNEonr
eventid: 1
Parent Process: C:\Windows\System32\cmd.exe
Process Name: C:\Windows\System32\reg.exe
Whitelist: 2.2
User: IEUser
score_user: 5
company: Microsoft Corporation
score_company: -0.9
token: -1.3
commandline: reg save HKLM\sam sam
entropy: 3.48171457299
score_size: -0.4
msghour: Work Hour Time
result: SUSPICIOUS
score: 2.9
<table>
<thead>
<tr>
<th><strong>id:</strong></th>
<th>Mu8XgW0BL6gH7RcNEonr</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>timestamp:</strong></td>
<td>2019-07-19T15:09:40.973Z</td>
</tr>
<tr>
<td><strong>eventid:</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Parent Process:</strong></td>
<td>C:\Windows\System32\svchost.exe</td>
</tr>
<tr>
<td><strong>Process Name:</strong></td>
<td>C:\Windows\System32\consent.exe</td>
</tr>
<tr>
<td><strong>Whitelist:</strong></td>
<td>-2</td>
</tr>
<tr>
<td><strong>User:</strong></td>
<td>SYSTEM</td>
</tr>
<tr>
<td><strong>score_user:</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>company:</strong></td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td><strong>score_company:</strong></td>
<td>-0.9</td>
</tr>
<tr>
<td><strong>token:</strong></td>
<td>0.8</td>
</tr>
<tr>
<td><strong>commandline:</strong></td>
<td>consent.exe 4516 288 0000023C0CA1FA70</td>
</tr>
<tr>
<td><strong>entropy:</strong></td>
<td>4.09698689377</td>
</tr>
<tr>
<td><strong>score_size:</strong></td>
<td>-0.4</td>
</tr>
<tr>
<td><strong>msghour:</strong></td>
<td>Work Hour Time</td>
</tr>
<tr>
<td><strong>result:</strong></td>
<td>REGULAR</td>
</tr>
<tr>
<td><strong>score:</strong></td>
<td>-1.2</td>
</tr>
<tr>
<td>id:</td>
<td>Fu8XgW0BL6gH7RcNEonr</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>timestamp:</td>
<td>2019-07-19T14:57:15.776Z</td>
</tr>
<tr>
<td>eventid:</td>
<td>1</td>
</tr>
<tr>
<td>Parent Process:</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td>
</tr>
<tr>
<td>Process Name:</td>
<td>C:\Windows\System32\mavinject.exe</td>
</tr>
<tr>
<td>Whitelist:</td>
<td>2.2</td>
</tr>
<tr>
<td>User:</td>
<td>IEUser</td>
</tr>
<tr>
<td>score_user:</td>
<td>5</td>
</tr>
<tr>
<td>company:</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>score_company:</td>
<td>-0.9</td>
</tr>
<tr>
<td>token:</td>
<td>-1.3</td>
</tr>
<tr>
<td>cmdline:</td>
<td>&quot;C:\Windows\system32\mavinject.exe&quot; 3912 /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055\src\x64\T1055.dll</td>
</tr>
<tr>
<td>entropy:</td>
<td>5.10632716065</td>
</tr>
<tr>
<td>score_size:</td>
<td>0.2</td>
</tr>
<tr>
<td>msghour:</td>
<td>Work Hour Time</td>
</tr>
<tr>
<td>result:</td>
<td>SUSPICIOUS</td>
</tr>
<tr>
<td>score:</td>
<td>3.5</td>
</tr>
</tbody>
</table>
### Scoring samples (4 / 5)

<table>
<thead>
<tr>
<th>id</th>
<th>g08xgw0bl6gh7rcneycy</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventid:</td>
<td>1</td>
</tr>
<tr>
<td>Parent Process:</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</td>
</tr>
<tr>
<td>Process Name:</td>
<td>C:\Windows\System32\cmd.exe</td>
</tr>
<tr>
<td>Whitelist:</td>
<td>2.2</td>
</tr>
<tr>
<td>User:</td>
<td>IeUser</td>
</tr>
<tr>
<td>score_user:</td>
<td>5</td>
</tr>
<tr>
<td>company:</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>score_company:</td>
<td>-0.9</td>
</tr>
<tr>
<td>token:</td>
<td>-1.3</td>
</tr>
<tr>
<td>commandline:</td>
<td>&quot;C:\Windows\system32\cmd.exe&quot; /c &quot;cmd.exe /c &quot; net use \Target\C$ P@ssw0rd1 /u:DOMAIN\Administrator&quot;</td>
</tr>
<tr>
<td>entropy:</td>
<td>4.850693816</td>
</tr>
<tr>
<td>score_size:</td>
<td>-0.4</td>
</tr>
<tr>
<td>msghour:</td>
<td>Work Hour Time</td>
</tr>
<tr>
<td>result:</td>
<td>MALICIOUS</td>
</tr>
<tr>
<td>score:</td>
<td>10.9</td>
</tr>
</tbody>
</table>
Scoring samples (5 / 5)

id: LrVIWW0BOU6Q8auzWsfK
timestamp: 2019-09-22T12:02:50.450Z
eventid: 1
Parent Process: C:\Windows\System32\cmd.exe
Process Name: C:\Windows\System32\NETSTAT.EXE
Whitelist: 2.2
User: Administrator
score_user: 3
company: Microsoft Corporation
score_company: -0.9
token: -1.3
commandline: netstat -an
entropy: 2.68872187554
score_size: -0.4
msghour: Work Hour Time
result: REGULAR
score: 0.9

id: T08AZG0BL6gH7RcNSjx8
eventid: 1
Parent Process: C:\Windows\System32\cmd.exe
Process Name: C:\Windows\System32\NETSTAT.EXE
Whitelist: 2.2
User: BlueOps
score_user: 5
company: Microsoft Corporation
score_company: -0.9
token: 1.9
commandline: netstat -an
entropy: 2.68872187554
score_size: -0.4
msghour: Work Hour Time
result: MALICIOUS
score: 6.1
Hunting Analysis samples stats

<table>
<thead>
<tr>
<th>Command</th>
<th>Total Events</th>
<th>Sum</th>
<th>Avg Score</th>
<th>Regular</th>
<th>Suspicious</th>
<th>Malicious</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>26</td>
<td>-61.0</td>
<td>-2.34615384615</td>
<td>26</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>wmic</td>
<td>11</td>
<td>20.3</td>
<td>1.84545454545</td>
<td>9</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>reg.exe</td>
<td>13</td>
<td>32.3</td>
<td>2.48461538462</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>cmd.exe</td>
<td>164</td>
<td>487.4</td>
<td>2.97195121951</td>
<td>84</td>
<td>20</td>
<td>60</td>
</tr>
<tr>
<td>powershell</td>
<td>116</td>
<td>312.4</td>
<td>2.69310344828</td>
<td>51</td>
<td>35</td>
<td>30</td>
</tr>
<tr>
<td>conhost</td>
<td>576</td>
<td>-1640.7</td>
<td>-2.8484375</td>
<td>576</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
SFH & Elastic for the Hunting
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event saved</td>
<td></td>
</tr>
<tr>
<td>Parent Process</td>
<td>C:\Windows\explorer.exe</td>
</tr>
<tr>
<td>Process Name</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</td>
</tr>
<tr>
<td>User</td>
<td>tryme</td>
</tr>
<tr>
<td>Whitelist</td>
<td>2.2</td>
</tr>
<tr>
<td>_id</td>
<td>qvDVPG0BL6gH7RcN-o9M</td>
</tr>
<tr>
<td>_index</td>
<td>test-index</td>
</tr>
<tr>
<td>_score</td>
<td>1</td>
</tr>
<tr>
<td>_type</td>
<td>sysmon</td>
</tr>
<tr>
<td>CommandLine</td>
<td>C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe</td>
</tr>
<tr>
<td>Company</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>Entropy</td>
<td>4.456</td>
</tr>
<tr>
<td>EventId</td>
<td>1</td>
</tr>
<tr>
<td>Id</td>
<td>t_DKpG0BL6gH7RcNMX4Q</td>
</tr>
<tr>
<td>Message Hour</td>
<td>Outside Work Hour Window</td>
</tr>
<tr>
<td>Result</td>
<td>MALICIOUS</td>
</tr>
<tr>
<td>Score</td>
<td>6.1</td>
</tr>
<tr>
<td>Score Company</td>
<td>-0.9</td>
</tr>
<tr>
<td>Score Size</td>
<td>-0.4</td>
</tr>
<tr>
<td>Score User</td>
<td>5</td>
</tr>
<tr>
<td>Tag</td>
<td>SANS</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Oct 6, 2019 @ 22:56:10.879</td>
</tr>
</tbody>
</table>
### [SFH] - Top 10 Companies

<table>
<thead>
<tr>
<th>company.keyword: Descending</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Corporation</td>
<td>582</td>
</tr>
<tr>
<td>Sysinternals - <a href="http://www.sysinternals.com">www.sysinternals.com</a></td>
<td>9</td>
</tr>
<tr>
<td>?</td>
<td>4</td>
</tr>
<tr>
<td>Chocolatey Software, Inc.</td>
<td>2</td>
</tr>
<tr>
<td>Mozilla Corporation</td>
<td>1</td>
</tr>
<tr>
<td>Mozilla Foundation</td>
<td>1</td>
</tr>
</tbody>
</table>

### [SFH] - Top 10 Username

<table>
<thead>
<tr>
<th>User.keyword: Descending</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>212</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>191</td>
</tr>
<tr>
<td>NETWORK SERVICE</td>
<td>88</td>
</tr>
<tr>
<td>tryme</td>
<td>85</td>
</tr>
<tr>
<td>LOCAL SERVICE</td>
<td>17</td>
</tr>
<tr>
<td>DWM-4</td>
<td>2</td>
</tr>
<tr>
<td>UMFD-4</td>
<td>2</td>
</tr>
<tr>
<td>DWM-3</td>
<td>1</td>
</tr>
<tr>
<td>UMFD-3</td>
<td>1</td>
</tr>
</tbody>
</table>
Dashboard

[SFH] - General Results

471 REGULAR - Count
66 SUSPICIOUS - Count
62 MALICIOUS - Count

[SFH] - Total Events

[SFH] - Sum Score X Entropy

[SFH] - Events Result Timeline

[SFH] - Avg Score X Entropy
Different Behaviors (normal versus malicious)

Thanks Samir @SBousseaden for providing EVTX samples repo https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES
Types of possible hunting

- Results
- AvgScores (entropy, score result)
- Keywords search
- Spikes and Views correlation
Reduce alerts to analyze

Total Events: 4409
Sum: -1791.4
Avg Score: -0.406305284645
Regular: 3457
Suspicious: 792
Malicious: 160

Suspicious + Malicious
Removes 79%

Malicious
Removes 96%
Hunting Video Demonstration
Future

- Add more score vectors
- Integration with THE HELK Project
- Correlate between other sysmon events
- Analyze evtx files directly
- Create DB files based on hunting needs
- Export to others SIEM / Products
Conclusions

- Understand your endpoints behavior
- Create and test different DB’s
- Keep testing your endpoint security
- Hunting needs tuning, there is no magic
Thank you!

Felipe Esposito  
@pr0teusBR  
fesposito@tenchisecurity.com

Rodrigo Montoro  
@spookerlabs  
rmontoro@tenchisecurity.com