# SANS ISC: Malware Analysis with elastic-agent and Microsoft Sandbox - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

**isc.sans.edu**/forums/diary/Malware+Analysis+with+elasticagent+and+Microsoft+Sandbox/27248/

Malware Analysis with elastic-agent and Microsoft Sandbox

Guy
522
Posts
ISC
Handler
Mar
27th
2021

Microsoft describes the "Windows Sandbox supports simple configuration files, which provide a minimal set of customization parameters for Sandbox. [...] Windows Sandbox configuration files are formatted as XML and are associated with Sandbox via the .wsb file extension."[6]

Since both, the latest version elastic-agent (7.11+) support antivirus detection, I followed the instructions listed here [1] to configure an agent to test its detection capabilities. For my workstation, I used VMware with a fully patched Windows 10 and saved the current configuration with a snapshot. I wanted to combine both of these features; the elastic-agent and the Microsoft sandbox feature [4][5][6] to analyze my malware sample. Since the Microsoft sandbox doesn't retain anything after it is shutdown, I figure this would be a good alternative vs. restoring my previous VMware snapshot every time I tested a suspicious filename.

One minor inconvenient, if I want to use the agent, I need to add it every time to Elasticsearch to use it. If the elastic-agent isn't installed, Microsoft Defender is enabled. Here is a list of tools to either install or consider installing in the sandbox when it starts:

- Elastic-agent with malware policy (in VMware client and Sandbox client)
- MS SysMon
- MS TCPView
- Consider adding: PowerShell Script Block Logging, example here
- Wireshark to capture traffic from host
- Other browsers: Chrome & Firefox
- PeStudio
- Python
- Internet Services Simulation Suite: INetSim
- Didier Stevens suite of tools
- Proxy setup on VMware client to monitor traffic
- Any other tools you might find useful during the analysis such as this package by @mentebinaria

When starting the sandbox, using a script configured for this purpose, it can automatically load the tools needed with a batch file (MalwareAnalysis.wsb). Here is my example:

```
<Configuration>
  <vGPU>Enable</vGPU>
  <AudioInput>Enable</AudioInput>
  <VideoInput>Enable</VideoInput>
  <ProtectedClient>Enable</ProtectedClient>
  <MappedFolders>
    <MappedFolder>
      <HostFolder>C:\Sandbox</HostFolder>
      <ReadOnly>true</ReadOnly>
    </MappedFolder>
  </MappedFolders>
<LogonCommand>
   <Command>C:\users\WDAGUtilityAccount\Desktop\Sandbox\SBConfig.bat</Command>
</LogonCommand>
</Configuration>
```

Because everything is deleted when you shutdown the sandbox (including the browser, it must be reloaded with the current version every time), I needed a way to automatically start/add/load/update what I needed to perform some basic analysis. I use a batch file I preconfigured with everything I needed to accomplish this task. Here is what I have (C:\Sandbox\SBConfig.bat):

```
REM Copy elastic-agent to C:\Program Files
C:\Windows\System32\xcopy.exe /i /s C:\Users\WDAGUtilityAccount\Desktop\Sandbox\elastic-agent "C:\Program Files\elastic-agent"
```

```
REM Install Sysmon64, vcredist_x86
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\Sysmon64.exe -i -accepteula
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\vcredist_x86.exe /q
```

```
REM Add Elastic certificate authority to Sandbox
C:\Windows\System32\certutil.exe -addstore root C:\Users\WDAGUtilityAccount\Desktop\Sandbox\ca.crt
C:\Windows\System32\certutil.exe -addstore root C:\Users\WDAGUtilityAccount\Desktop\Sandbox\stargate.crt
```

```
REM Install new Microsoft Edge
start /wait C:\Users\WDAGUtilityAccount\Desktop\Sandbox\MicrosoftEdgeEnterpriseX64.msi /quiet /norestart
```

```
REM Install Python
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\python-3.9.2-amd64.exe /quiet InstallAllUsers=1 PrependPath=1
Include_test=0
```

```
REM Execute PowerShell scripts
Powershell.exe -executionpolicy remotesigned -File
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\ChangeExecutionPolicy.ps1
Powershell.exe -executionpolicy remotesigned -File
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\ScriptBlockLogging.ps1
```

```
REM Install Wireshark
REM Install npcap manually. Silent only supported with OEM
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\Wireshark-win64-3.4.4.exe /S /D /desktopicon=yes
C:\Users\WDAGUtilityAccount\Desktop\Sandbox\npcap-1.20.exe
```

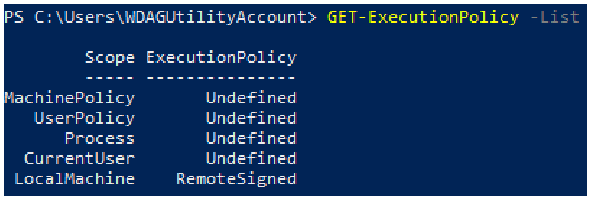
The file npcap is last because I'm using the free edition vs. the OEM which will ask to finish the installation after it starts the installer. Before you can enable ScriptBlockLogging in the Sandbox, I need to enable the PowerShell ExecutionPolicy to allow RemoteSigned. This is the command in my script to make that change (ChangeExecutionPolicy.ps1):

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
```

To verify the change was applied, as PowerShell admin, execute the following command:

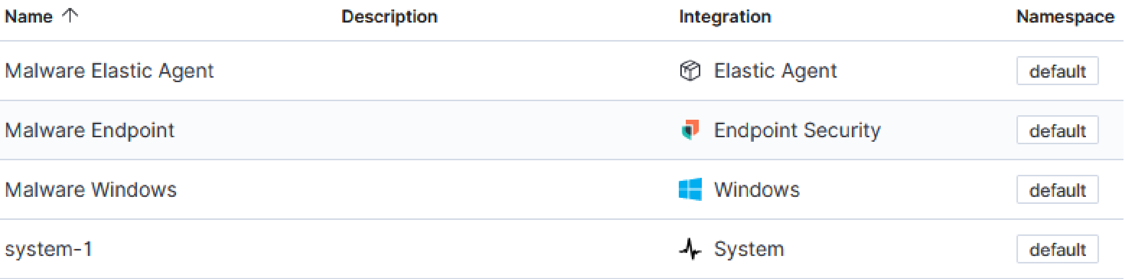
```
Get-ExecutionPolicy -List
```

Producing the following result:



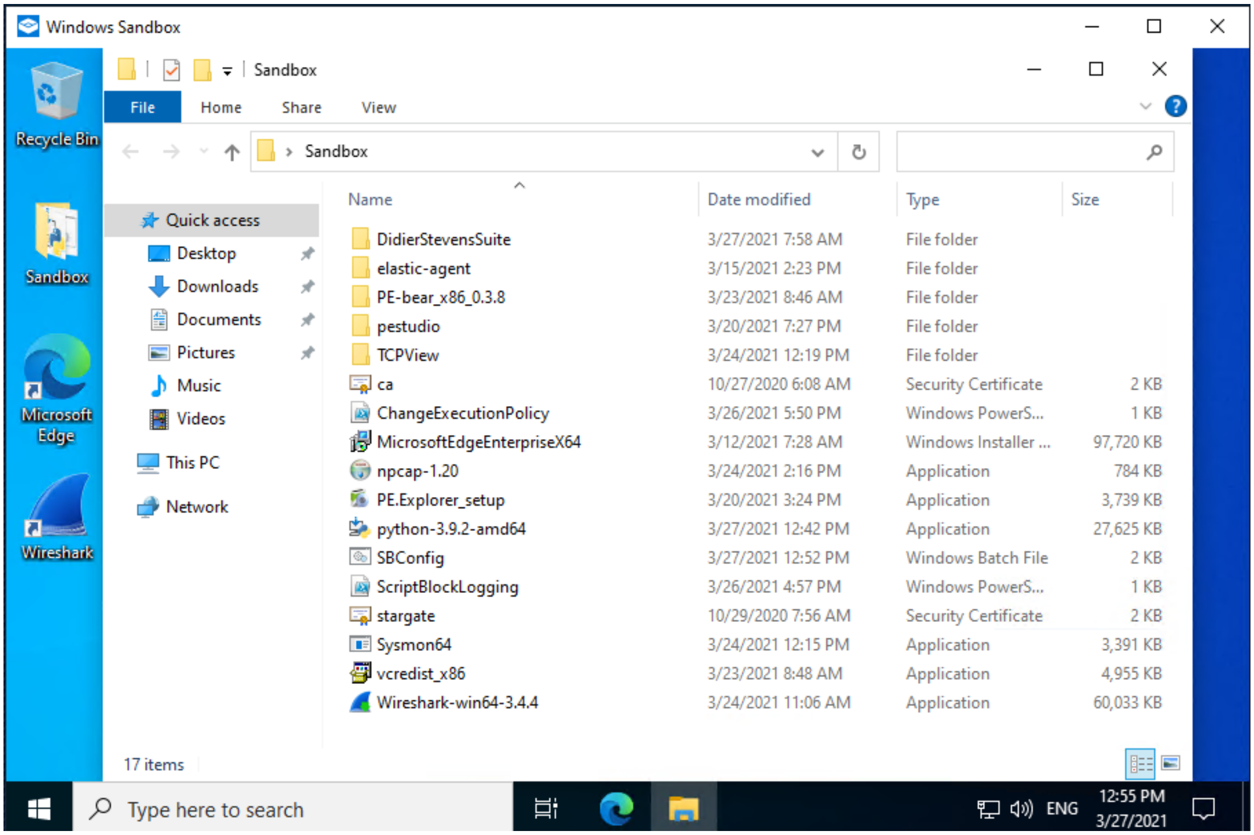
```
PS C:\Users\WDAGUtilityAccount> GET-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process       Undefined
  CurrentUser       Undefined
 LocalMachine    RemoteSigned
```

Following the example listed here in this Elastic blog, it is time to create a policy, add the elastic-agent to Elasticsearch (pre-copied with the batch file SBConfig.bat) to run the sample file and monitor its activity. This is the four application part of the policy I configured for my agent:



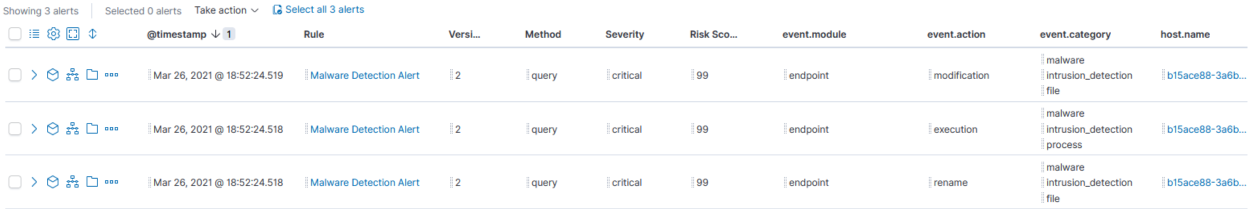
| Name ↑ | Description | Integration | Namespace |
|---|---|---|---|
| Malware Elastic Agent | | Elastic Agent | default |
| Malware Endpoint | | Endpoint Security | default |
| Malware Windows | | Windows | default |
| system-1 | | System | default |

After launching the script MalwareAnalysis.wsb to start the Sandbox, load, copy and install all the applications from the batch file, it is time to add the elastic-agent to the server, I am ready to launch the suspected malware file for analysis. Last month, my honeypot was uploaded a crypto miner file photo.scr and I'm going to use this file to submit the elastic-agent for analysis.



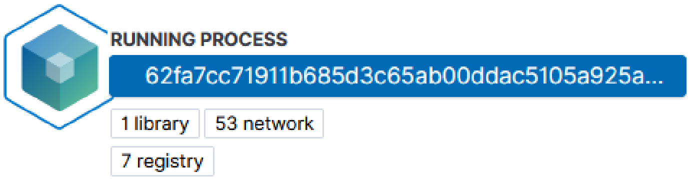
| Name | Date modified | Type | Size |
|---|---|---|---|
| DidierStevensSuite | 3/27/2021 7:58 AM | File folder | |
| elastic-agent | 3/15/2021 2:23 PM | File folder | |
| PE-bear_x86_0.3.8 | 3/23/2021 8:46 AM | File folder | |
| pestudio | 3/20/2021 7:27 PM | File folder | |
| TCPView | 3/24/2021 12:19 PM | File folder | |
| ca | 10/27/2020 6:08 AM | Security Certificate | 2 KB |
| ChangeExecutionPolicy | 3/26/2021 5:50 PM | Windows PowerS... | 1 KB |
| MicrosoftEdgeEnterpriseX64 | 3/12/2021 7:28 AM | Windows Installer ... | 97,720 KB |
| npcap-1.20 | 3/24/2021 2:16 PM | Application | 784 KB |
| PE.Explorer_setup | 3/20/2021 3:24 PM | Application | 3,739 KB |
| python-3.9.2-amd64 | 3/27/2021 12:42 PM | Application | 27,625 KB |
| SBConfig | 3/27/2021 12:52 PM | Windows Batch File | 2 KB |
| ScriptBlockLogging | 3/26/2021 4:57 PM | Windows PowerS... | 1 KB |
| stargate | 10/29/2020 7:56 AM | Security Certificate | 2 KB |
| Sysmon64 | 3/24/2021 12:15 PM | Application | 3,391 KB |
| vcredist_x86 | 3/23/2021 8:48 AM | Application | 4,955 KB |
| Wireshark-win64-3.4.4 | 3/24/2021 11:06 AM | Application | 60,033 KB |

→ To view the results in Kibana, navigate Security -> Overview -> Detection alert trend
I look for activity that would indicate an alert triggered by malware and filter for the value, then View alerts to examine the flow of the activity. I can then select Analyze the content as to what this photo.scr file accessed or installed on the client. The agent captured 3 alerts:

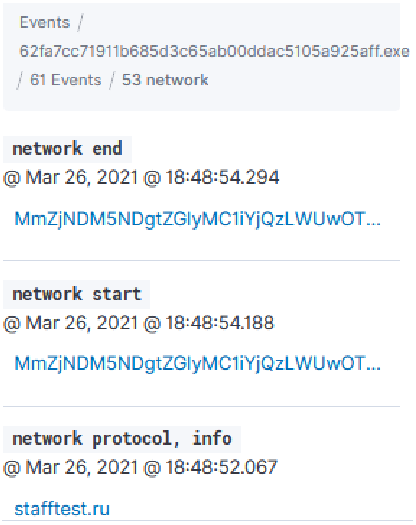


| @timestamp | Rule | Versi... | Method | Severity | Risk Sco... | event.module | event.action | event.category | host.name |
|---|---|---|---|---|---|---|---|---|---|
| Mar 26, 2021 @ 18:52:24.519 | Malware Detection Alert | 2 | query | critical | 99 | endpoint | modification | malware<br>intrusion_detection<br>file | b15ace88-3a6b... |
| Mar 26, 2021 @ 18:52:24.518 | Malware Detection Alert | 2 | query | critical | 99 | endpoint | execution | malware<br>intrusion_detection<br>process | b15ace88-3a6b... |
| Mar 26, 2021 @ 18:52:24.518 | Malware Detection Alert | 2 | query | critical | 99 | endpoint | rename | malware<br>intrusion_detection<br>file | b15ace88-3a6b... |

Next is to expand one of those alerts and analyze the activity, the elastic-agent identified: 1 library, 53 networks and 7 registry:



**Network Activty**



Events / 62fa7cc71911b685d3c65ab00ddac5105a925aff.exe / 61 Events / 53 network

`network end`
@ Mar 26, 2021 @ 18:48:54.294

MmZjNDM5NDgtZGlyMC1iYjQzLWUwOT...

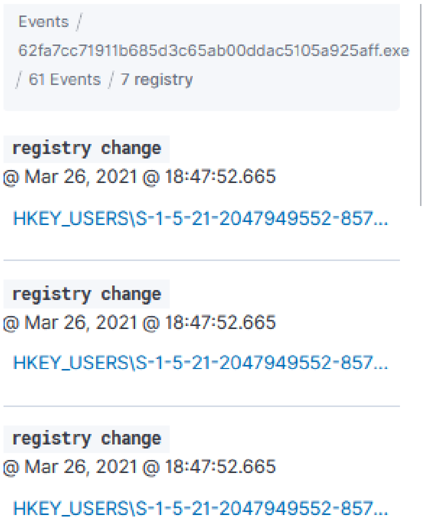
`network start`
@ Mar 26, 2021 @ 18:48:54.188

MmZjNDM5NDgtZGlyMC1iYjQzLWUwOT...

`network protocol, info`
@ Mar 26, 2021 @ 18:48:52.067

stafftest.ru

## Registry Activity



Events / 62fa7cc71911b685d3c65ab00ddac5105a925aff.exe / 61 Events / 7 registry

`registry change`
@ Mar 26, 2021 @ 18:47:52.665

HKEY_USERS\S-1-5-21-2047949552-857...

`registry change`
@ Mar 26, 2021 @ 18:47:52.665

HKEY_USERS\S-1-5-21-2047949552-857...

`registry change`
@ Mar 26, 2021 @ 18:47:52.665

HKEY_USERS\S-1-5-21-2047949552-857...

Each one of the can be expanded to drill further into what happened on the host.

## Indicator of Compromise

SHA256
807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d  Photo.scr
[2021-02-08 07:06:36] [1693] [ftp_21_tcp 29914] [103.232.236.239:64149] info: Stored 1578496 bytes of data

Domains

stafftest[.]ru
iqtesti[.]ru
jobtests[.]ru
prtests[.]ru
qptest[.]ru
pstests[.]ru
testpsy[.]ru
profetest[.]ru
hrtests[.]ru

This is one of many tasks Windows Sandbox could be used such as accessing suspicious sites, running untrusted software and scripts starting with Windows network or vGPU disable, without the fear of impacting your normal Windows installation. These various tasks can be accomplished by creating  separate .wsb Sanbox script.

[1] https://www.elastic.co/blog/how-to-build-a-malware-analysis-sandbox-with-elastic-security
[2] https://www.elastic.co/endpoint-security/
[3] https://www.elastic.co/guide/en/security/current/install-endpoint.html
[4] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-overview
[5] https://techcommunity.microsoft.com/t5/windows-kernel-internals/windows-sandbox/ba-p/301849

[6] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file
[7] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
[8] https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
[9] https://github.com/mentebinaria/retoolkit?s=09
[10] https://www.virustotal.com/gui/file/807126cbae47c03c99590d081b82d5761e0b9c57a92736fc8516cf41bc564a7d/detection
[11] https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.1

-----------

Guy Bruneau IPSS Inc.
My Handler Page
Twitter: GuyBruneau
gbruneau at isc dot sans dot edu