Sysmon Monitoring different way

Marek Mikita

About me

- System manager
- Husband, father
- @spyx_myky
- ...love to learn new things :)

Sysmon 101

- Monitor and log system activity to the Windows event log
- Provides detailed information about process creations, network connections, changes to file creation time, etc..
- Collecting logs for SIEM for further analysis

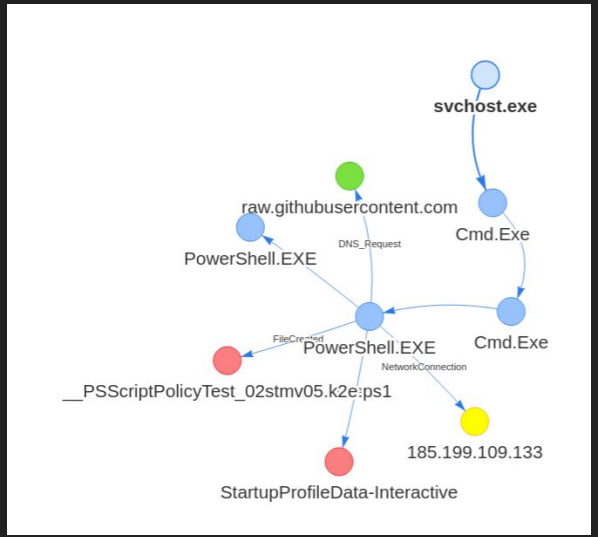
What if sysmon was an graph?

Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime: 2021-04-27 13:38:35.103
ProcessGuid: {6e6de1d8-13db-6088-6700-000000002a00}
ProcessId: 5864
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
FileVersion: 89.0.4389.128
Description: Google Chrome
Product: Google Chrome
Company: Google LLC
OriginalFileName: chrome.exe
CommandLine: "C:\Program Files\Google\Chrome\Application\chrome.exe"
CurrentDirectory: C:\Program Files\Google\Chrome\Application\
User: DESKTOP-MRV87VT\kali
LogonGuid: {6e6de1d8-13bb-6088-a2d1-0a0000000000}
LogonId: 0xAD1A2
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=287F37A4EAC018D616476501C4CD021ADD6E35D8,MD5=E60C84B6FB6336A79DD4F6DF02401606,
0130AE721EAE956E549E01E2D8404D29
ParentProcessGuid: {6e6de1d8-13c5-6088-5600-000000002a00}
ParentProcessId: 4832
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE

Introduce SysmonGraph

- Graphical representation of sysmon logs
- Simple UI
- Use Neo4J database (cypher queries)
- Lots (lots, lost) of javascript :)
- Powershell script to acquire logs
- https://github.com/spyx/SysmonGrahp

```
└─$ sudo docker-compose up -d
Recreating docker_web_1 ... done
Starting docker_neo4j_1 ... done
```



Demo Time

Thank you

Any Q&A via discord or twitter :)