Wykrywanie incydentów - lab 11

Zadanie 2

1. **Plik:** EB93600C45E8D7CF13C3AE86AA4D4999 (MD5) Raport: https://any.run/report/6afe31930267ea6ea80eef4ae7b933a4bfaab5169b3c9010ed58d7cc72fe9b35/be02ddce-aa29-4c3e-9823-4e59a656d166

   Klucz rejestru:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

   Plik wykonywalny: newbos2.exe

2. **Plik:** DEDC4F7F903354EA813ED739B0324680 (MD5) https://any.run/report/657407c250c426cfeb98c8483f329ab7b55c6e1f2ced9b7c367c02ff89ef8104/90874bff-1240-49b6-b505-5967bc7cbf14

   Klucz rejestru:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

   Plik wykonywalny: zkhvhzkatjpszadh.exe

3. **Plik:** 47363B94CEE907E2B8926C1BE61150C7 (MD5) https://any.run/report/45317968759d3e37282ceb75149f627d648534c5b4685f6da3966d8f6fca662d/f5e3c713-c0d3-4f8f-afe6-efdd56b33d88

   Klucz rejestru:
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

   Plik wykonywalny: 46695237.exe

Zadanie 4

1.

```
alert.severity = 4
description = Detects persistence registry keys. Modified by SOC Prime,
replaced condition "1 of them" with "selection_reg1d"
cron_schedule = 0 * * * *
```

```
disabled = 1
is_scheduled = 1
is_visible = 1
dispatch.earliest_time = -60m@m
dispatch.latest_time = now
search = (source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode="13" (TargetObject="*\\SOFTWARE\\Microsoft\\Windows NT\
\CurrentVersion\\Image File Execution Options\*\\GlobalFlag" OR
TargetObject="*\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\
\SilentProcessExit\*\\ReportingMode" OR TargetObject="*\\SOFTWARE\\Microsoft\
\Windows NT\\CurrentVersion\\SilentProcessExit\*\\MonitorProcess")
EventType="SetValue")
alert.suppress = 0
alert.track = 1
```

2.

```
alert.severity = 3
description = Detects a possible persistence mechanism using RUN key for
Windows Explorer and poiting to a suspicious folder
cron_schedule = 0 * * * *
disabled = 1
is_scheduled = 1
is_visible = 1
dispatch.earliest_time = -60m@m
dispatch.latest_time = now
search = (source="WinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode="13" TargetObject="*\\Microsoft\\Windows\\CurrentVersion\\Policies\
\Explorer\\Run" (Details="C:\\Windows\\Temp\\*" OR Details="C:\\ProgramData\\*"
OR Details="*\\AppData\\*" OR Details="C:\\$$Recycle.bin\\*" OR Details="C:\
\Temp\\*" OR Details="C:\\Users\\Public\\*" OR Details="C:\\Users\\Default\
\*")) | table Image,ParentImage
alert.suppress = 0
alert.track = 1
```