**Assignment 2: Dynamic Analysis By Kevin Harianto**

Registry Modification for Process Launch

Q1-1: Provide a screenshot of your settings and their execution. (2.5 points)

A screenshot of a computer program

Description automatically generated

Q1-2: Use a tool to show this persistence mechanism in your VM. Describe the tool used and include a screenshot of the tool displaying the setup. (3 points)

Tool: Autoruns

A screenshot of a computer

Description automatically generated

^Setup of explorer to run automatically from the command “reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\iexplore.exe" /v GlobalFlag /t REG\_DWORD /d 512”

Tool: RegEdit

A screenshot of a computer program

Description automatically generated

^The modification of value with the Reporting mode and Monitoring Process can be showcased on Registry Editor from the command “reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\iexplore.exe" /v ReportingMode /t REG\_DWORD /d 1” as well as “reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\iexplore.exe" /v MonitorProcess /d "C:\windows\system32\notepad.exe"”.

Note: I was unable to find the values on the tool “Autoruns” itself due to how it primarily focuses on the programs that run on startup and not the values embedded.

Q2-2:

A computer screen with white text

Description automatically generated

^Successfully Executing the malware sample.

A screenshot of a computer

Description automatically generated

^Suspicious Executions within svchost.exe was found.

A screenshot of a computer

Description automatically generated

^Within the svchost.exe, suspicious Strings were found within the svchost.exe properties inside the processes highlighted by Process Hacker. This reveals process hollowing as the malware sample is revealed to be launching as a suspended state as “svchost.exe” where the actual code is replaced with the malicious code -showcased by the suspicious strings found within the properties in Process Hacker- as highlighted when investigating the properties.