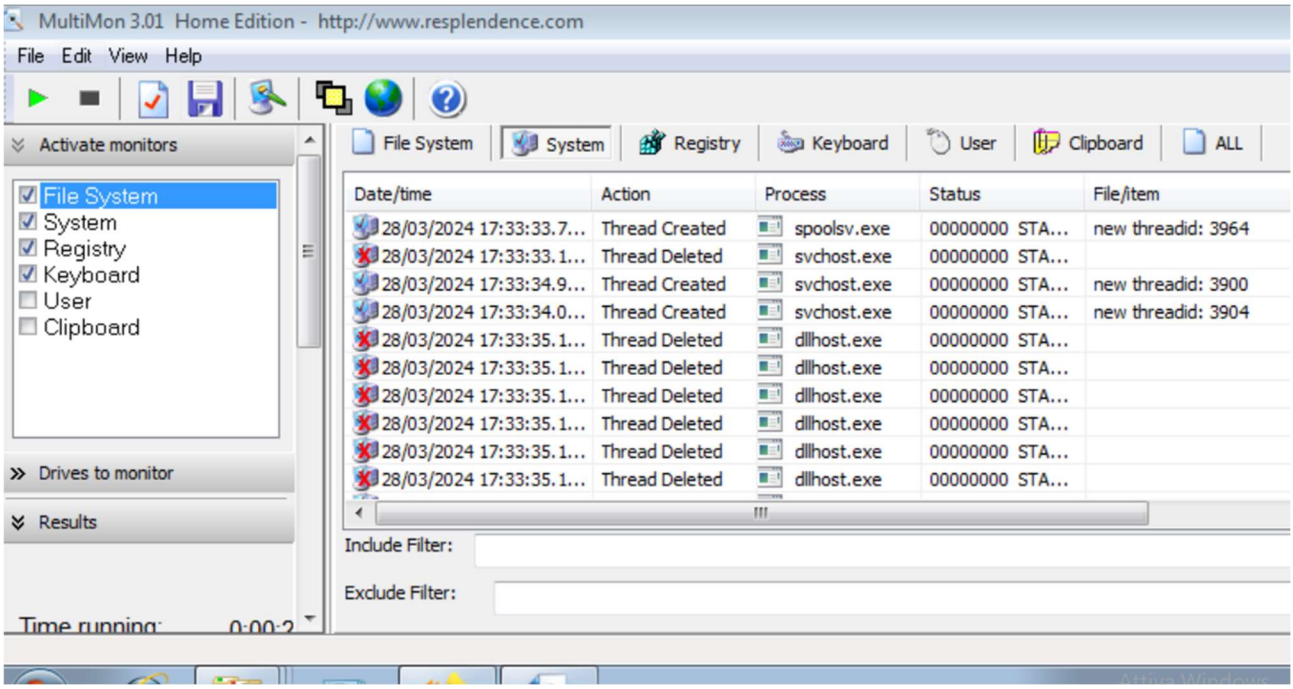
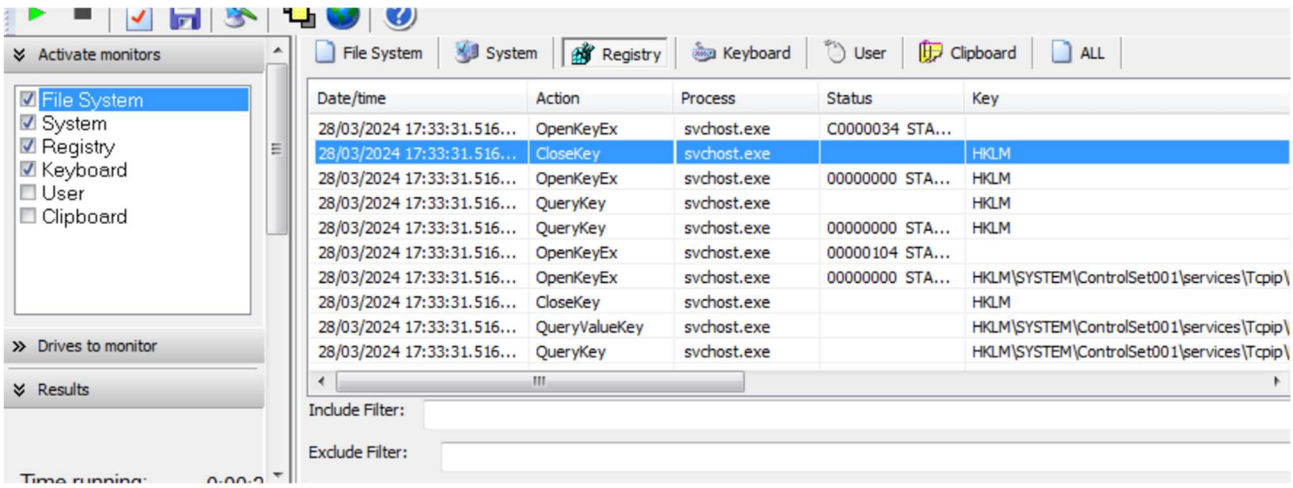
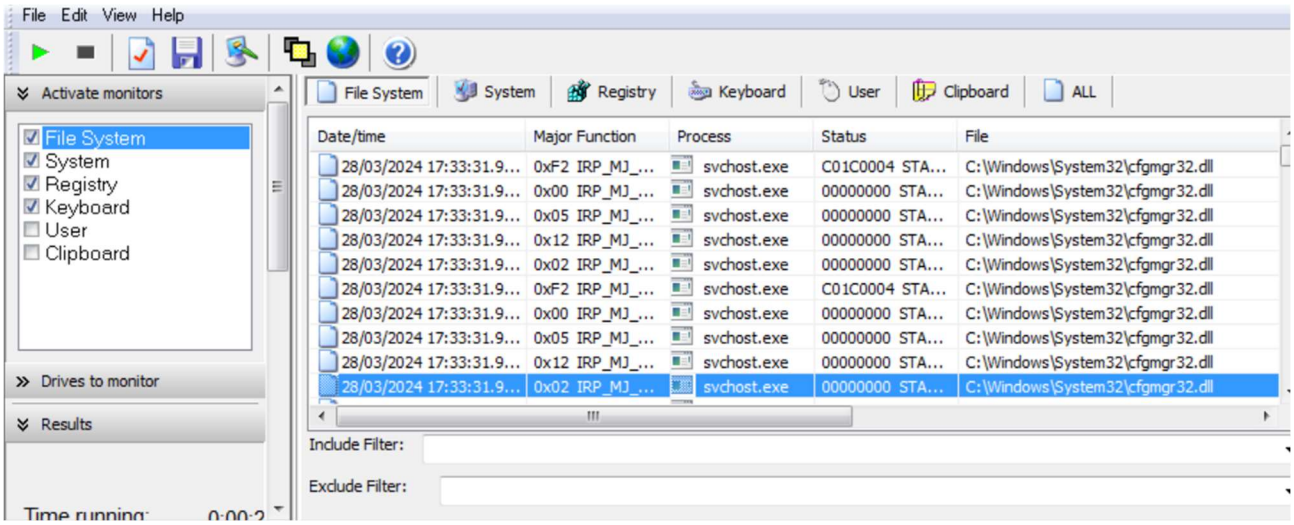
Traccia:

Nella lezione teorica, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica. Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando multimon https://www.resplendence.com/multimon
- Identificare eventuali altre azioni del malware
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.






File Edit View Help
Activate monitors
File System
System
Registry
Keyboard
User
Clipboard
Drives to monitor
Results
Time running:
File System
System
Registry
Keyboard
User
Clipboard
ALL
Date/time
Major Function
Process
Status
File
28/03/2024 17:33:31.9... 0xF2 IRP_MJ_... svchost.exe C01C0004 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x00 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x05 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x12 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x02 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0xF2 IRP_MJ_... svchost.exe C01C0004 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x00 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x05 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x12 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
28/03/2024 17:33:31.9... 0x02 IRP_MJ_... svchost.exe 00000000 STA... C:\Windows\System32\cfgmgr32.dll
Include Filter:
Exclude Filter: