



Traccia:

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:

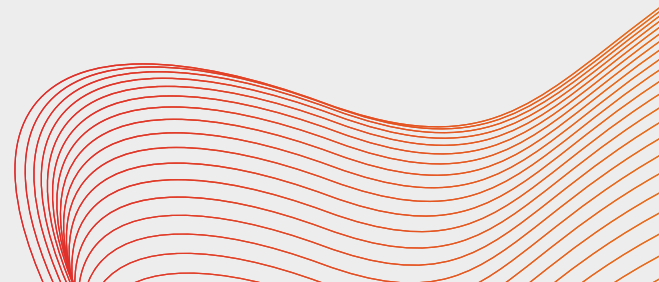
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.



Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Filter Tools Options Help					
Time of Day	Process Name	PID	Operation	Path	Result Detail
9:25:23.3763194 AM	Malware_U3_W2_L2.exe	3440	Process Start		SUCCESS Parent PID: 1896, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"
9:25:23.37632...	Malware_U3_W2_L2.exe	3440	Thread Create		SUCCESS Thread ID: 3444
9:25:23.37655...	Malware_U3_W2_L2.exe	3440	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
9:25:23.37690...	Malware_U3_W2_L2.exe	3440	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS Image Base: 0x400000, Image Size: 0xd000
9:25:23.37718...	Malware_U3_W2_L2.exe	3440	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS Image Base: 0x7c900000, Image Size: 0xa1000
9:25:23.37723...	Malware_U3_W2_L2.exe	3440	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
9:25:23.37755...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1539026A.pf	SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a
9:25:23.37780...	Malware_U3_W2_L2.exe	3440	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1539026A.pf	SUCCESS AllocationSize: 8,192, EndOfFile: 5,832, NumberOfLinks: 1, DeletePending: False, Directory: False
9:25:23.37799...	Malware_U3_W2_L2.exe	3440	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1539026A.pf	SUCCESS Offset: 0, Length: 5,832
9:25:23.37836...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1539026A.pf	SUCCESS
9:25:23.37844...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\	SUCCESS Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, Share
9:25:23.37849...	Malware_U3_W2_L2.exe	3440	QueryInformationVolume	C:\	SUCCESS VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D8BA-8021, SupportsObjects: True, VolumeLabel
9:25:23.37853...	Malware_U3_W2_L2.exe	3440	FileSystemControl	C:\	SUCCESS Control: FSCTL_FILE_PREFETCH
9:25:23.37860...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.37866...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\	SUCCESS 0: 65e58df5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInformation, 3: CONFIG.SYS, 4: Documents and
9:25:23.37881...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\	NO MORE FILES
9:25:23.37897...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\	SUCCESS
9:25:23.37912...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.37917...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
9:25:23.37929...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings	NO MORE FILES
9:25:23.37937...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\Documents and Settings	SUCCESS
9:25:23.37955...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.37961...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Settings, 7: My Documents, 8: NetHood,
9:25:23.37970...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES
9:25:23.37978...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\Documents and Settings\Administrator	SUCCESS
9:25:23.38018...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.38032...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: CFF Explorer.lnk, 4: Command Prompt.lnk, 5: Esercizio_Pratico_U3_W2_L1, 6: Esercizio_Pratico_U3_W2_L2
9:25:23.38051...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES
9:25:23.38071...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
9:25:23.38096...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.38115...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log
9:25:23.38140...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
9:25:23.38161...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
9:25:23.38216...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\WINDOWS	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.38236...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16.bnp, 8: bootstat.dat, 9: bootstat.dat
9:25:23.38264...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS	NO MORE FILES
9:25:23.38282...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\WINDOWS	SUCCESS
9:25:23.38316...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\WINDOWS\AppPatch	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.38341...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: AcGenial.dll, 4: AcLayers.dll, 5: AcLus.dll, 6: AcSpecic.dll, 7: Ac0tinal.dll, 8: apphelp
9:25:23.38373...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES
9:25:23.38410...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\WINDOWS\AppPatch	SUCCESS
9:25:23.38440...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\WINDOWS\system32	SUCCESS Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:25:23.38463...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\system32	SUCCESS 0: ., 1: ., FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125
9:25:23.38502...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\system32	SUCCESS 0: easprvc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edim.exe, 4: efradu.dll, 5: ega.cpl, 6: els.dll, 7: emptyregdb.dat, 8: ei
9:25:23.38535...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\system32	SUCCESS 0: more.com, 1: monicons.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43mod.dll, 5: mp43dmod.dll, 6: mpeg2data.ax,
9:25:23.38571...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\system32	SUCCESS 0: program.exe, 1: PRONIObj.dll, FileInformationClass: FileNamesInformation, 3: PROUnl.exe, 4: proxytj.exe, 5: psapi.dll, 6: psbase.dll, 7:
9:25:23.38593...	Malware_U3_W2_L2.exe	3440	QueryDirectory	C:\WINDOWS\system32	SUCCESS 0: vjpy.dll, 1: vmGuestLib.dll, FileInformationClass: FileNamesInformation, 3: vmhgs.dll, 4: VMUppgradeShutdownVSP.dll, 5: vmwgs32.dll, 6:
9:25:23.38615...	Malware_U3_W2_L2.exe	3440	CloseFile	C:\WINDOWS\system32	NO MORE FILES
9:25:23.38637...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS
9:25:23.38672...	Malware_U3_W2_L2.exe	3440	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read
9:25:23.38678...	Malware_U3_W2_L2.exe	3440	QueryStandardInformationFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
9:25:23.38774...	Malware_U3_W2_L2.exe	3440	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS AllocationSize: 708,608, EndOfFile: 708,048, NumberOfLinks: 1, DeletePending: False, Directory: False
9:25:23.38819...	Malware_U3_W2_L2.exe	3440	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS SyncType: SyncTypeOther

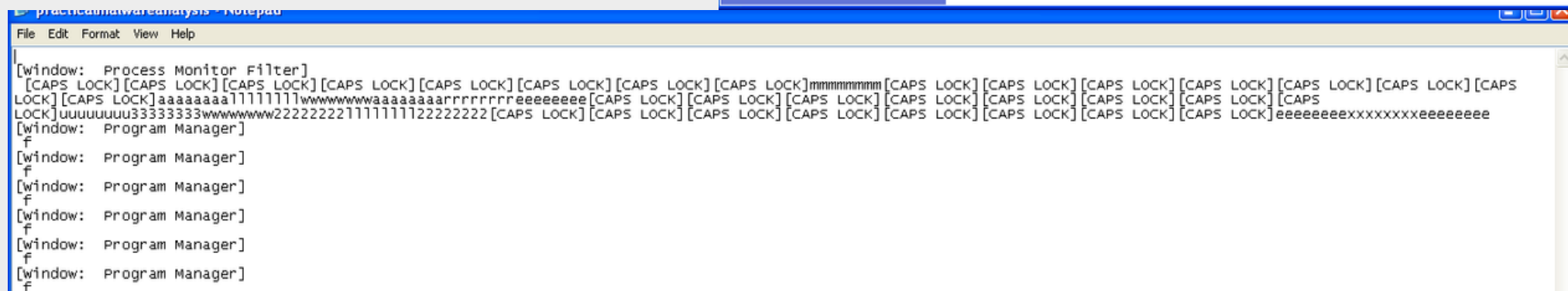
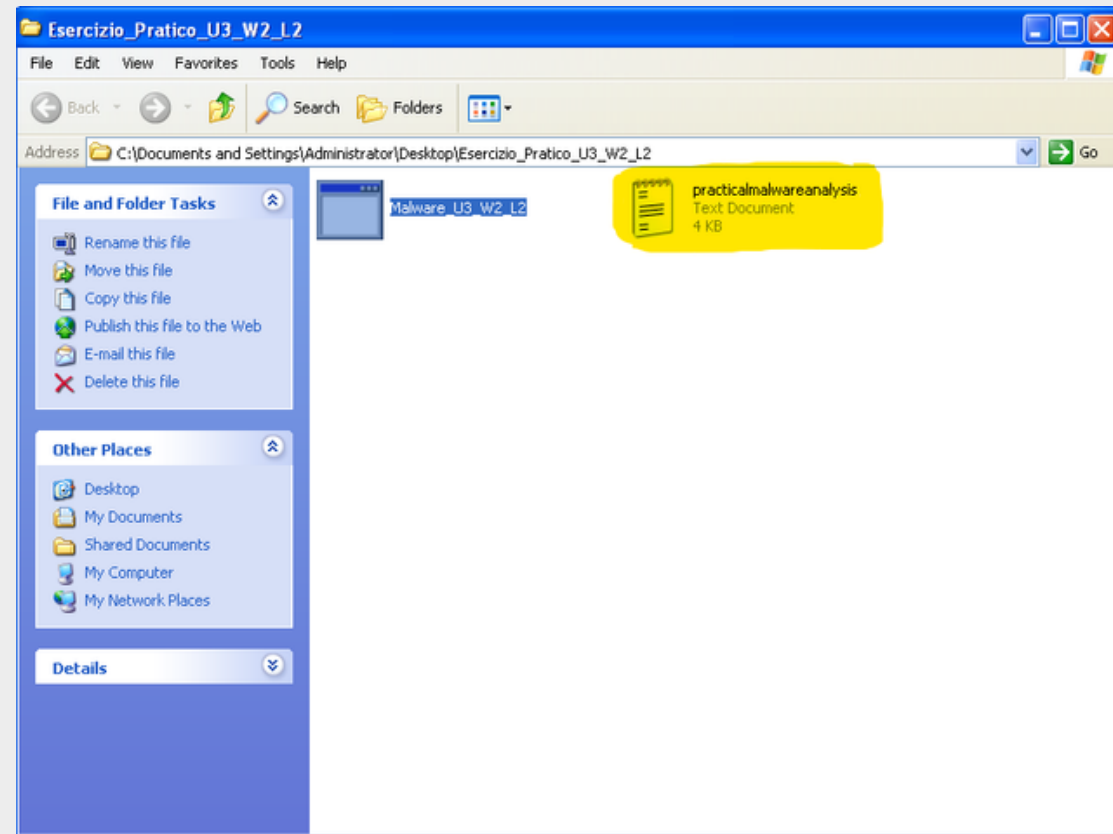
Utilizzando **Process monitor** possiamo controllare i processi in esecuzione sulla macchina.

Avviando il malware notiamo un processo che crea un file di testo **“practicalmalwareanalysis”** nella stessa cartella del malware



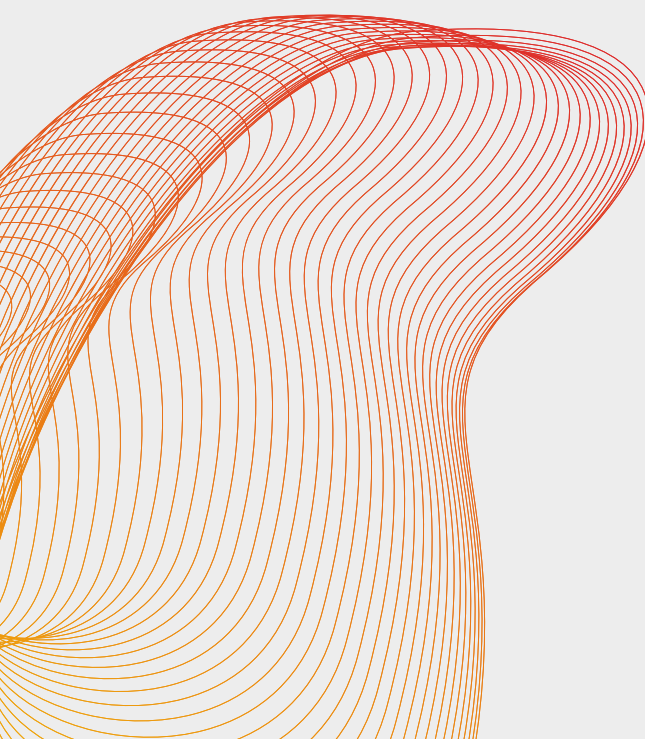


chiaro segno che si tratta di un





Approfondimento: **KeyLogger**



Un keylogger è un tipo di software o dispositivo progettato per registrare e memorizzare le tastate effettuate su una tastiera del computer. La sua funzione principale è catturare le informazioni digitate dall'utente, inclusi username, password, messaggi di testo e altre informazioni sensibili.

Process Monitor - Sysinternals: www.sysinternals.com

Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
7:24.81100...	Malware_U3_W2_L2.exe	1772	Process Start		SUCCESS	Parent PID: 1896, Command line: "C:\Documents and Settings\Administrator\Desktop\...
7:24.81101...	Malware_U3_W2_L2.exe	1772	Thread Create		SUCCESS	Thread ID: 1412
7:24.81171...	Malware_U3_W2_L2.exe	1772	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
7:24.81206...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
7:24.85094...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
7:24.86397...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
7:24.87098...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
7:24.88203...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
7:24.88239...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\vpport4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
7:24.88276...	Malware_U3_W2_L2.exe	1772	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x777e0000, Image Size: 0x11000
7:24.89028...	Malware_U3_W2_L2.exe	1772	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1616, Command line: "C:\WINDOWS\system32\svchost.exe"
7:25.88908...	Malware_U3_W2_L2.exe	1772	Thread Exit		SUCCESS	Thread ID: 1412, User Time: 0.0000000, Kernel Time: 0.0781250
7:25.88327...	Malware_U3_W2_L2.exe	1772	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0625000 seconds, Private

Utilizzando la cattura precedente di ProcMon e cliccando sull'icona "Processi e Thread" andiamo a filtrare i processi che appartengono a quella categoria.

Tra i processi trovati si trova "Svchost.exe", nome di un processo legittimo di Windows. Il malware è quindi progettato per camuffarsi da processo legittimo per passare inosservato