

Adrian.Amarfii 10/01/2023  
Report  
Task

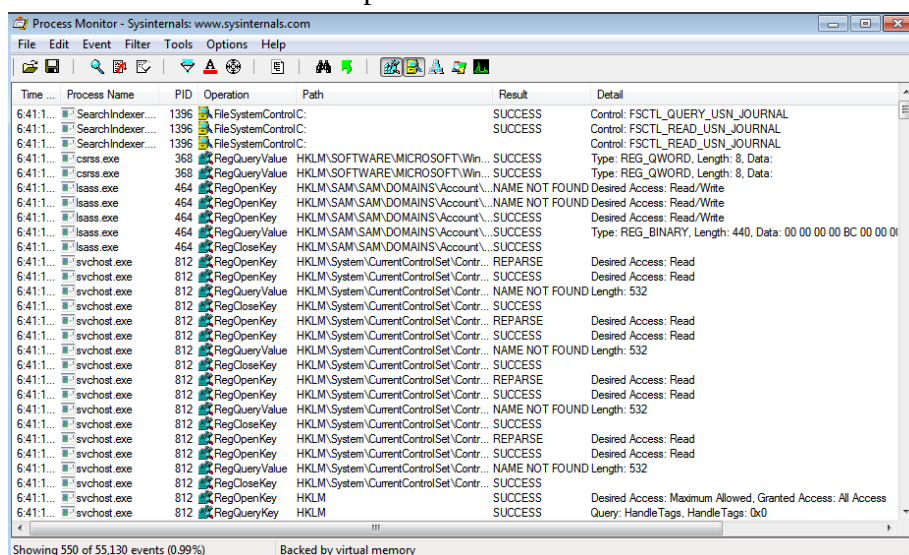
**Traccia:**

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

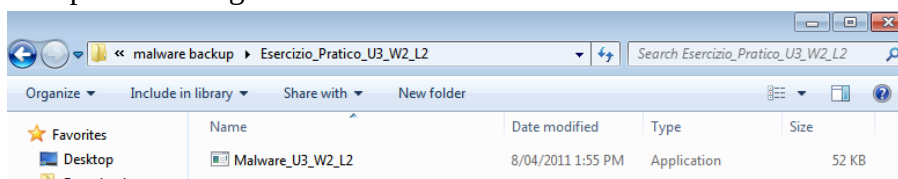
Con riferimento al file eseguibile contenuto nella cartella «**Esercizio\_Pratico\_U3\_W2\_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando 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.

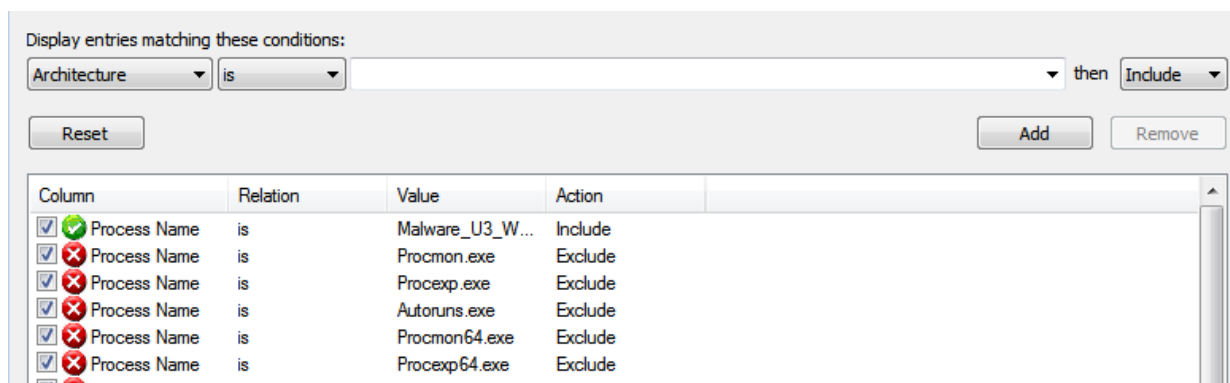
Procediamo con l'apertura del nostro tool → Process Monitor → procmon  
La schermata che visualizziamo è una lista processi attivi sulla nostra macchina.



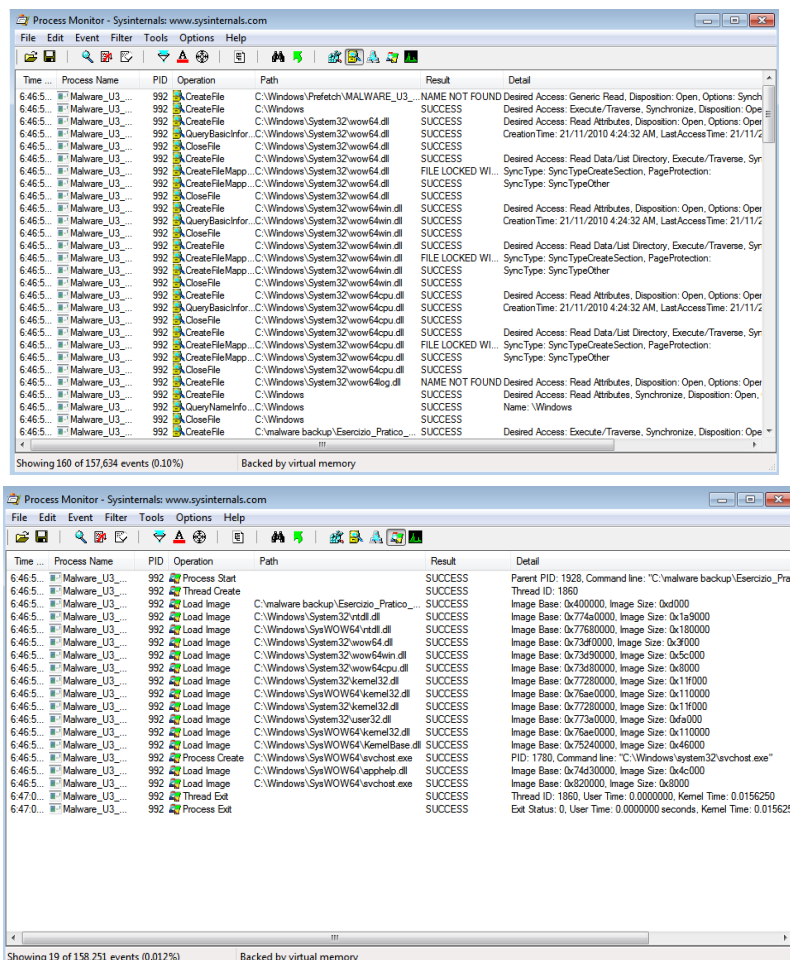
Adesso apriamo l'eseguibile con il codice malevolo



Una volta aperto lo lasciamo indisturbato per qualche minuto e andiamo a creare filtri per la ricerca su Process Monitor



Dopo aver applicato i filtri andiamo in FILE SYSTEM e THREAD ACTIVITY:



The image displays two screenshots of the Process Monitor application, showing detailed system activity for a process named 'Malware\_U3...'. The top screenshot is filtered for 'FILE SYSTEM' activity, showing a series of file operations such as 'CreateFile', 'CloseFile', 'QueryBasicInfo', 'CreateFileMap', and 'QueryBasicInfo'. The bottom screenshot is filtered for 'THREAD ACTIVITY', showing the process starting, creating threads, and loading various system DLLs like 'ntdll.dll', 'kernel32.dll', 'user32.dll', and 'GDI32.dll'.

Time	Process Name	PID	Operation	Path	Result	Detail
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\Prefetch\MALWARE_U3...	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synch...
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Ope...
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Ope...
6:46:5...	Malware_U3...	992	QueryBasicInfo	C:\Windows\System32\wow64.dll	SUCCESS	Creation Time: 21/11/2010 4:24:32 AM, LastAccess Time: 21/11/2...
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Syn...
6:46:5...	Malware_U3...	992	CreateFileMap	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PageProtection:...
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Sync Type: SyncTypeOther
6:46:5...	Malware_U3...	992	QueryBasicInfo	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Ope...
6:46:5...	Malware_U3...	992	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	Creation Time: 21/11/2010 4:24:32 AM, LastAccess Time: 21/11/2...
6:46:5...	Malware_U3...	992	CreateFileMap	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PageProtection:...
6:46:5...	Malware_U3...	992	CreateFileMap	C:\Windows\System32\wow64win.dll	SUCCESS	Sync Type: SyncTypeOther
6:46:5...	Malware_U3...	992	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Ope...
6:46:5...	Malware_U3...	992	QueryBasicInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Creation Time: 21/11/2010 4:24:32 AM, LastAccess Time: 21/11/2...
6:46:5...	Malware_U3...	992	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
6:46:5...	Malware_U3...	992	CreateFileMap	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PageProtection:...
6:46:5...	Malware_U3...	992	CreateFileMap	C:\Windows\System32\wow64cpu.dll	SUCCESS	Sync Type: SyncTypeOther
6:46:5...	Malware_U3...	992	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Ope...
6:46:5...	Malware_U3...	992	CreateFile	C:\Windows\...	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open...
6:46:5...	Malware_U3...	992	QueryNameInfo	C:\Windows\...	SUCCESS	Name: Windows
6:46:5...	Malware_U3...	992	CloseFile	C:\Windows\...	SUCCESS	
6:46:5...	Malware_U3...	992	CreateFile	C:\malware backup\Esercizio_Pratico...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Ope...

Time	Process Name	PID	Operation	Path	Result	Detail
6:46:5...	Malware_U3...	992	Process Start		SUCCESS	Parent PID: 1928, Command line: "C:\malware backup\Esercizio_Pra...
6:46:5...	Malware_U3...	992	Thread Create		SUCCESS	Thread ID: 1860
6:46:5...	Malware_U3...	992	Load Image	C:\malware backup\Esercizio_Pratico...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0x1a5000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x773d0000, Image Size: 0x180000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73d00000, Image Size: 0x3f000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x73d90000, Image Size: 0x5c000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73d80000, Image Size: 0x8000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77280000, Image Size: 0x11f000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x773e0000, Image Size: 0x110000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77380000, Image Size: 0xfaf000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76ae0000, Image Size: 0x110000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\SysWOW64\kernelBase.dll	SUCCESS	Image Base: 0x75240000, Image Size: 0x45000
6:46:5...	Malware_U3...	992	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 1780, Command line: "C:\Windows\system32\svchost.exe"
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x74d30000, Image Size: 0x4c000
6:46:5...	Malware_U3...	992	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x820000, Image Size: 0x8000
6:47:0...	Malware_U3...	992	Thread Exit		SUCCESS	Thread ID: 1860, User Time: 0.0000000, Kernel Time: 0.0156250
6:47:0...	Malware_U3...	992	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.015625

Come possiamo notare ci ha creato un process svchost.exe → Di solito questo processi sono sicuri ma molto spesso i hacker cercano di imitare il file e in più ha cercato di creare un file Malware con estensione .pf → tecnica usata nei microprocessori per ridurre i stati di attesa e accelerare l’ecuzione. Con l’aiuto di VirusTotal riusciamo a vedere che si Tratta di un Trojan