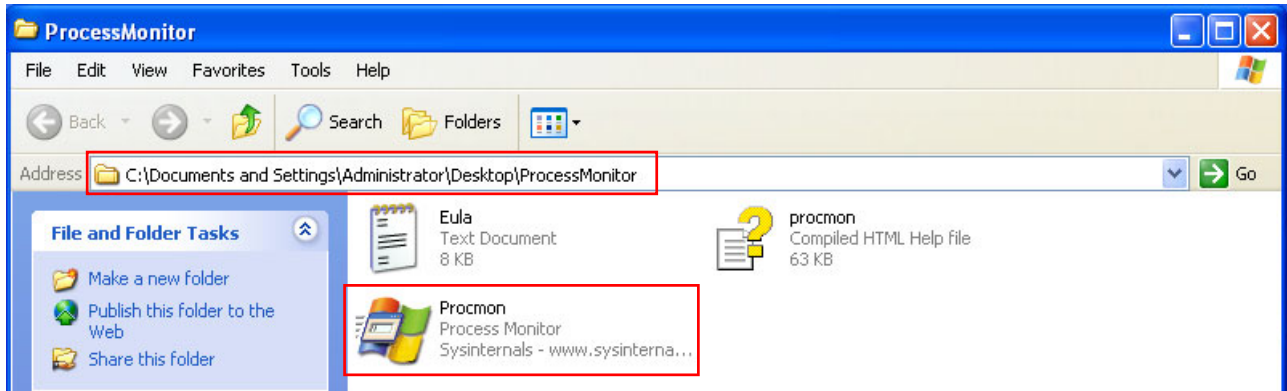


# ANALISI DINAMICA BASICA

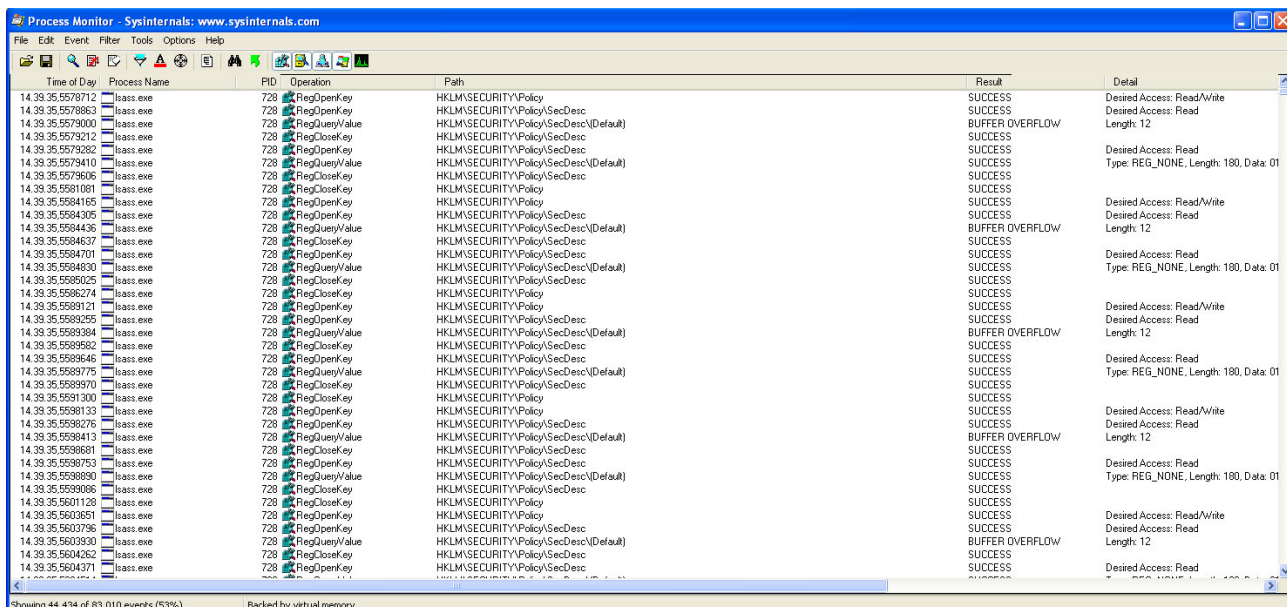
L'esercitazione di oggi consiste nella **ANALISI DINAMICA BASICA** del file eseguibile **"MALWARE\_U3\_W2\_L2"**

## FASE 1

Nella prima fase andiamo ad aprire il nostro Tool, già presente sulla nostra macchina **"Process Monitor"** (Procmon)

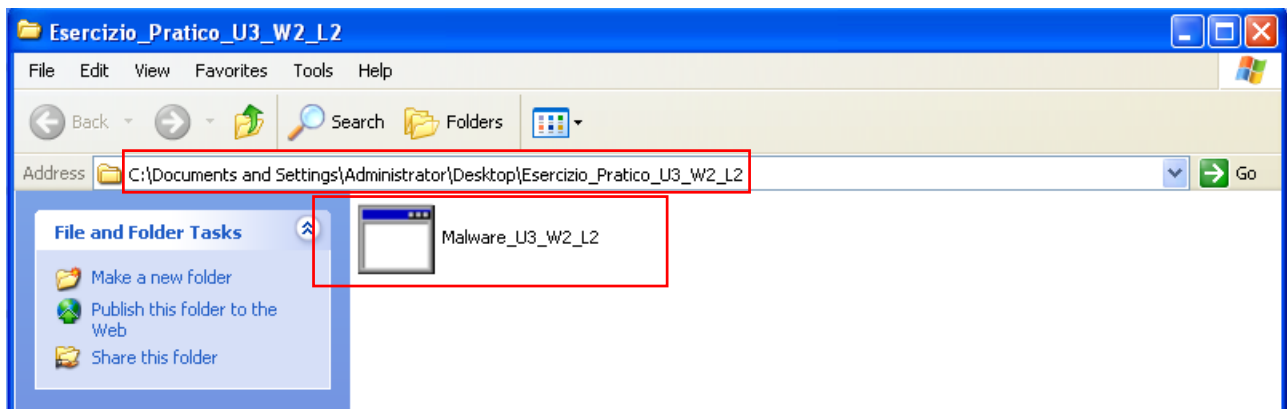


La schermata che ci si presenta inizialmente è una lista di processi attivi sulla nostra macchina

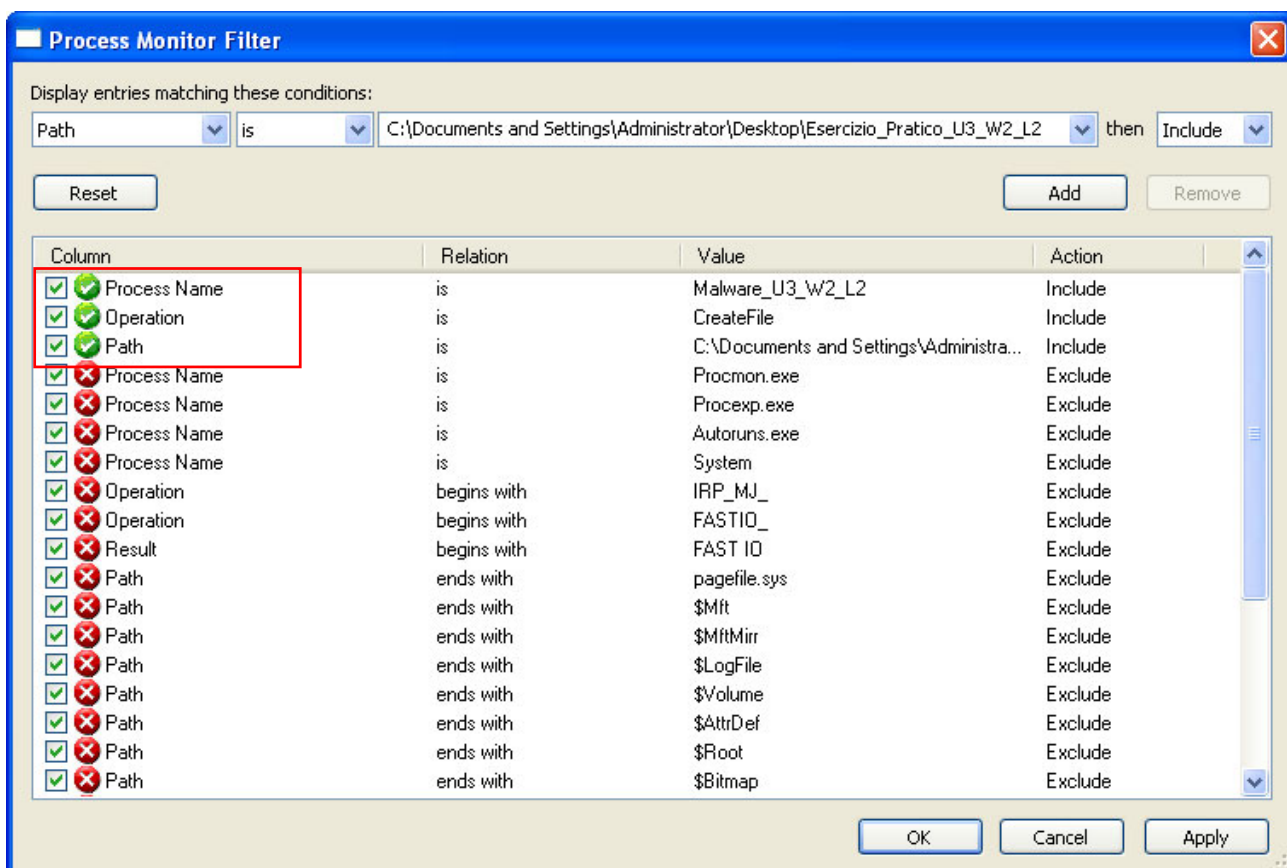


## FASE 2

Nella seconda fase andiamo ad aprire l'eseguibile contenente il codice malevolo



Una volta lasciato agire indisturbato il nostro eseguibile, andremo a creare dei filtri di “ricerca” su Procom.



In questo caso creeremo dei filtri per Nome / Creation file / Path

## FASE 3

Una volta applicati i filtri ci spostiamo nelle task “File System” e “Thread Activity”

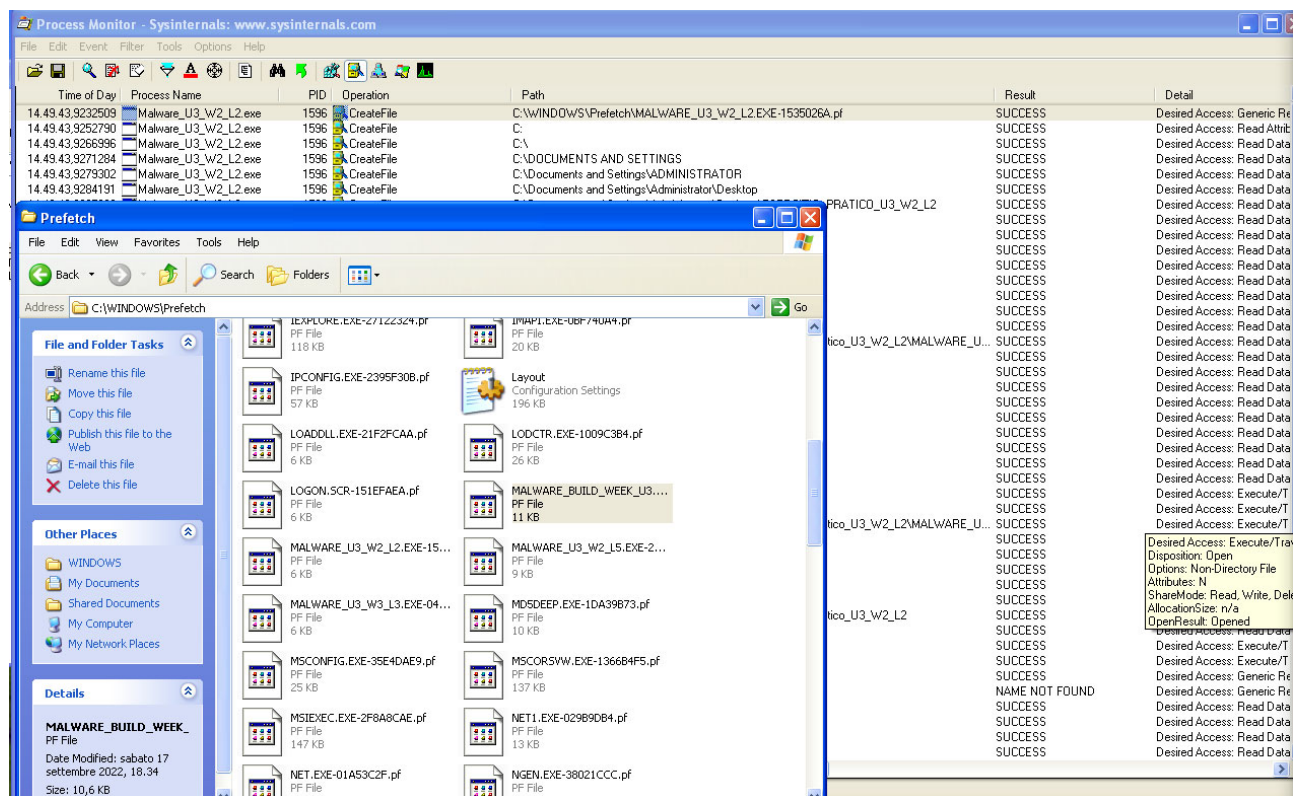
Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
14.49.43.9225731	Malware_U3_W2_L2.exe	1596	Process Start		SUCCESS	Parent PID: 18
14.49.43.9225759	Malware_U3_W2_L2.exe	1596	Thread Create		SUCCESS	Thread ID: 15
14.49.43.9229930	Malware_U3_W2_L2.exe	1596	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0
14.49.43.9231089	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0
14.49.43.9439918	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0
14.49.43.9521227	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0
14.49.43.9571571	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0
14.49.43.9666653	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0
14.49.43.9665911	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\vpct4.dll	SUCCESS	Image Base: 0
14.49.43.9671506	Malware_U3_W2_L2.exe	1596	Load Image	C:\WINDOWS\system32\secu32.dll	SUCCESS	Image Base: 0
14.49.43.9768062	Malware_U3_W2_L2.exe	1596	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 960, Con
14.49.44.9799284	Malware_U3_W2_L2.exe	1596	Thread Exit		SUCCESS	Thread ID: 15
14.49.44.9800357	Malware_U3_W2_L2.exe	1596	Process Exit		SUCCESS	Exit Status: 0

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
14.49.43.9377647	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	
14.49.43.9379013	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\locale.nls	SUCCESS	
14.49.43.9380066	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	
14.49.43.9380955	Malware_U3_W2_L2.exe	1596	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	
14.49.43.9382008	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	
14.49.43.9383369	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	
14.49.43.9384419	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
14.49.43.9385880	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	
14.49.43.9386953	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
14.49.43.9388478	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
14.49.43.9389537	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
14.49.43.9391045	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\vpct4.dll	SUCCESS	
14.49.43.9392096	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\secu32.dll	SUCCESS	
14.49.43.9393462	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Ac
14.49.43.9394384	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType:
14.49.43.9395096	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType:
14.49.43.9396418	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Ac
14.49.43.9397745	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType:
14.49.43.9398097	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType:
14.49.43.9398868	Malware_U3_W2_L2.exe	1596	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS	Desired Ac
14.49.43.9399315	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	SyncType:
14.49.43.9399644	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	SyncType:
14.49.43.9400301	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Ac
14.49.43.9402145	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType:
14.49.43.9402480	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType:
14.49.43.9403731	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Ac
14.49.43.9404919	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType:
14.49.43.9405265	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType:
14.49.43.9406559	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Ac
14.49.43.9411615	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType:
14.49.43.9411950	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType:
14.49.43.9413227	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\vpct4.dll	SUCCESS	Desired Ac
14.49.43.9414174	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\vpct4.dll	SUCCESS	SyncType:
14.49.43.9414607	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\vpct4.dll	SUCCESS	SyncType:
14.49.43.9415887	Malware_U3_W2_L2.exe	1596	CreateFile	C:\WINDOWS\system32\secu32.dll	SUCCESS	Desired Ac
14.49.43.9417149	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\secu32.dll	SUCCESS	SyncType:
14.49.43.9417476	Malware_U3_W2_L2.exe	1596	CreateFileMapping	C:\WINDOWS\system32\secu32.dll	SUCCESS	SyncType:
14.49.43.9417876	Malware_U3_W2_L2.exe	1596	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 4.0
14.49.43.9418379	Malware_U3_W2_L2.exe	1596	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 16.
14.49.43.9418527	Malware_U3_W2_L2.exe	1596	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 20.
14.49.43.9418663	Malware_U3_W2_L2.exe	1596	ReadFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 40.
14.49.43.9422921	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
14.49.43.9424147	Malware_U3_W2_L2.exe	1596	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	

Showing 493 of 2.866.790 events (0.0%)

Backed by virtual memory

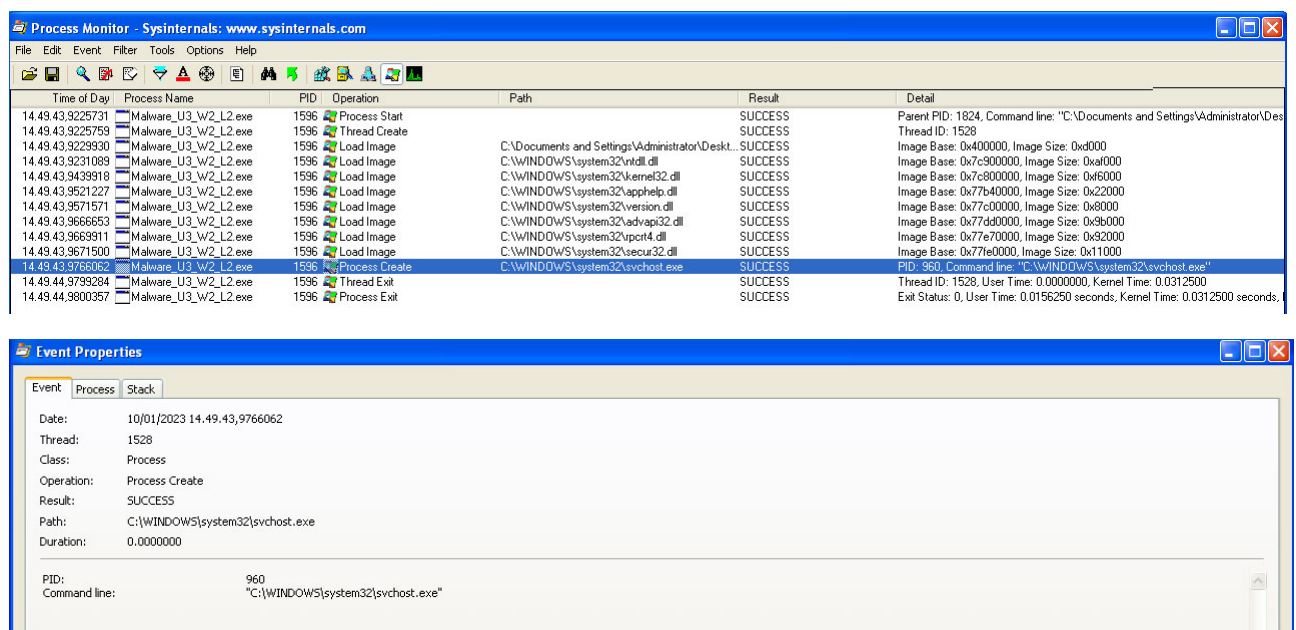
Con la Creazione del filtro create file, possiamo notare la creazione di un file con estensione .pf



Il **prefetch** è una tecnica usata nei microprocessori per accelerare l'esecuzione dei programmi riducendo gli stati di attesa [...].

["https://it.wikipedia.org/wiki/Prefetch"](https://it.wikipedia.org/wiki/Prefetch)

Il nostro file eseguibile oltre alla creazione del file .pf ha creato anche un processo svchost.exe. Questo processo nativo di windows è stato alterato



["https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8-felb38AhUGS\\_EDHawICKEQFnoECB0QAw&url=https%3A%2F%2Fwww.avast.com%2Fc-what-is-svchost-file&usg=AOvVaw1-36XNW\\_kl81afbrldYmBE"](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwi8-felb38AhUGS_EDHawICKEQFnoECB0QAw&url=https%3A%2F%2Fwww.avast.com%2Fc-what-is-svchost-file&usg=AOvVaw1-36XNW_kl81afbrldYmBE)

["https://www.virustotal.com/gui/file/ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce"](https://www.virustotal.com/gui/file/ae8a1c7eb64c42ea2a04f97523ebf0844c27029eb040d910048b680f884b9dce) con uno score negativo di **59/72**

The screenshot shows a Windows Explorer window with the following details:

- Title Bar:** Esercizio\_Pratico\_U3\_W2\_L2
- Address Bar:** C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2
- File List:**
  - practicalmalwareanalysis (Text Document, 1 KB)
- Taskbar:** The active window is titled 'Esercizio\_Pratico\_U3\_W2\_L2'.