Analisi Dinamica Basica

Avvio dell'eseguibile

Time of Day	Process Name	PID	Operation
10:06:57.4688...	Malware_U3_W2_L2.exe	2016	Process Start
10:06:57.4689...	Malware_U3_W2_L2.exe	2016	Thread Create

Filtriamo gli eventi catturati con l'opzione "Process and Thread activity" del processo *Malware_U3_W2_L2.exe*

Time of Day	Process Name	PID	Operation	Path
10:06:57.4688...	Malware_U3_W2_L2.exe	2016	Process Start	
10:06:57.4689...	Malware_U3_W2_L2.exe	2016	Thread Create	
10:06:57.4709...	Malware_U3_W2_L2.exe	2016	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
10:06:57.4711...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\ntdll.dll
10:06:57.5328...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\kernel32.dll
10:06:57.5467...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\apphelp.dll
10:06:57.5540...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\version.dll
10:06:57.5621...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\advapi32.dll
10:06:57.5627...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\rpcrt4.dll
10:06:57.5630...	Malware_U3_W2_L2.exe	2016	Load Image	C:\WINDOWS\system32\secur32.dll
10:06:57.5730...	Malware_U3_W2_L2.exe	2016	Process Create	C:\WINDOWS\system32\svchost.exe
10:06:58.5682...	Malware_U3_W2_L2.exe	2016	Thread Exit	
10:06:58.5682...	Malware_U3_W2_L2.exe	2016	Process Exit	

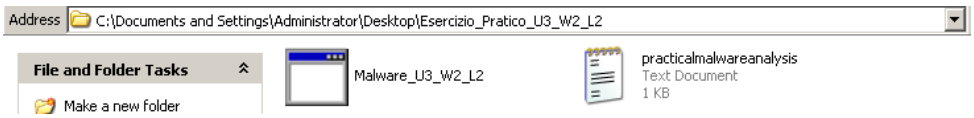
Utilizziamo come filtro "Parent PID" il numero PID dell'eseguibile del malware per verificare se il processo principale abbia causato l'avvio di altri processi come infatti è successo con il processo *svchost.exe*.

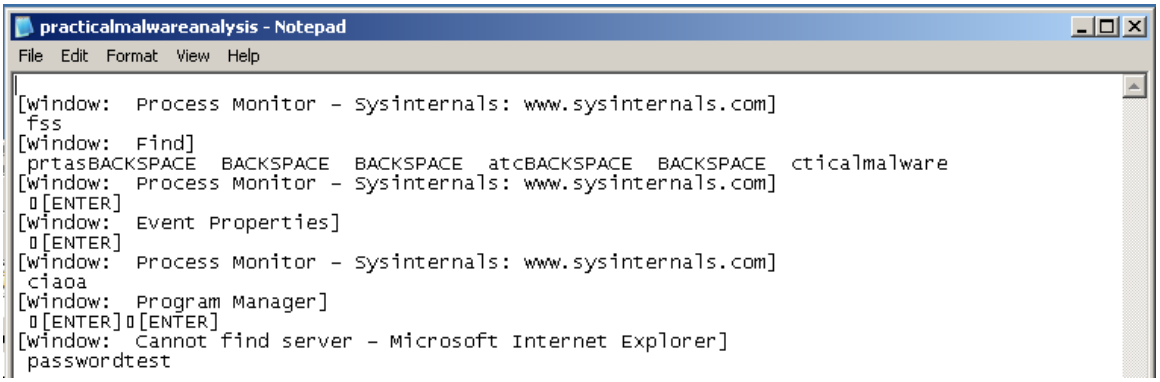
Time of Day	Process Name	PID	Operation	Path
10:06:57.5730...	svchost.exe	180	Process Start	
10:06:57.5730...	svchost.exe	180	Thread Create	
10:06:57.5758...	svchost.exe	180	Load Image	C:\WINDOWS\system32\ntdll.dll
10:06:57.6442...	svchost.exe	180	Load Image	C:\WINDOWS\system32\kernel32.dll
10:06:57.6455...	svchost.exe	180	Load Image	C:\WINDOWS\system32\user32.dll
10:06:57.6458...	svchost.exe	180	Load Image	C:\WINDOWS\system32\gdi32.dll
10:06:57.6501...	svchost.exe	180	Load Image	C:\WINDOWS\system32\shimeng.dll
10:06:57.6590...	svchost.exe	180	Load Image	C:\WINDOWS\AppPatch\AcGenral.dll
10:06:57.6593...	svchost.exe	180	Load Image	C:\WINDOWS\system32\advapi32.dll
10:06:57.6596...	svchost.exe	180	Load Image	C:\WINDOWS\system32\rpcrt4.dll
10:06:57.6599...	svchost.exe	180	Load Image	C:\WINDOWS\system32\secur32.dll
10:06:57.6622...	svchost.exe	180	Load Image	C:\WINDOWS\system32\winmm.dll
10:06:57.6626...	svchost.exe	180	Load Image	C:\WINDOWS\system32\ole32.dll
10:06:57.6629...	svchost.exe	180	Load Image	C:\WINDOWS\system32\msvcrt.dll
10:06:57.6633...	svchost.exe	180	Load Image	C:\WINDOWS\system32\oleaut32.dll
10:06:57.6667...	svchost.exe	180	Load Image	C:\WINDOWS\system32\msacm32.dll
10:06:57.6671...	svchost.exe	180	Load Image	C:\WINDOWS\system32\version.dll
10:06:57.6687...	svchost.exe	180	Load Image	C:\WINDOWS\system32\shell32.dll
10:06:57.6692...	svchost.exe	180	Load Image	C:\WINDOWS\system32\shlwapi.dll
10:06:57.6696...	svchost.exe	180	Load Image	C:\WINDOWS\system32\userenv.dll
10:06:57.6738...	svchost.exe	180	Load Image	C:\WINDOWS\system32\uxtheme.dll
10:06:57.7591...	svchost.exe	180	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
10:06:57.7854...	svchost.exe	180	Load Image	C:\WINDOWS\system32\comctl32.dll

Verifichiamo che entrambi i processi non abbiamo creato file sul sistema. Dallo screenshot che segue è possibile constatare la creazione di un file denominato *practicalmalwareanalysis.log*

10:07:04.3484...	svchost.exe	180	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3489...	svchost.exe	180	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3490...	svchost.exe	180	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3494...	svchost.exe	180	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3495...	svchost.exe	180	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3496...	svchost.exe	180	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3497...	svchost.exe	180	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log
10:07:04.3499...	svchost.exe	180	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log

Cerchiamo e apriamo tale file per verificarne il contenuto.





Aprendo il file di log è possibile vedere come sia in corso un dump della tastiera suddiviso per finestra nella quale sono stati premuti i tasti.

Sempre lo stesso processo *svchost.exe* con PID 180 è responsabile della scrittura e conseguente aggiornamento del file di log *practicalmalwareanalysis.log* ogni volta che vengono premuti tasti sulla tastiera.