S10L2

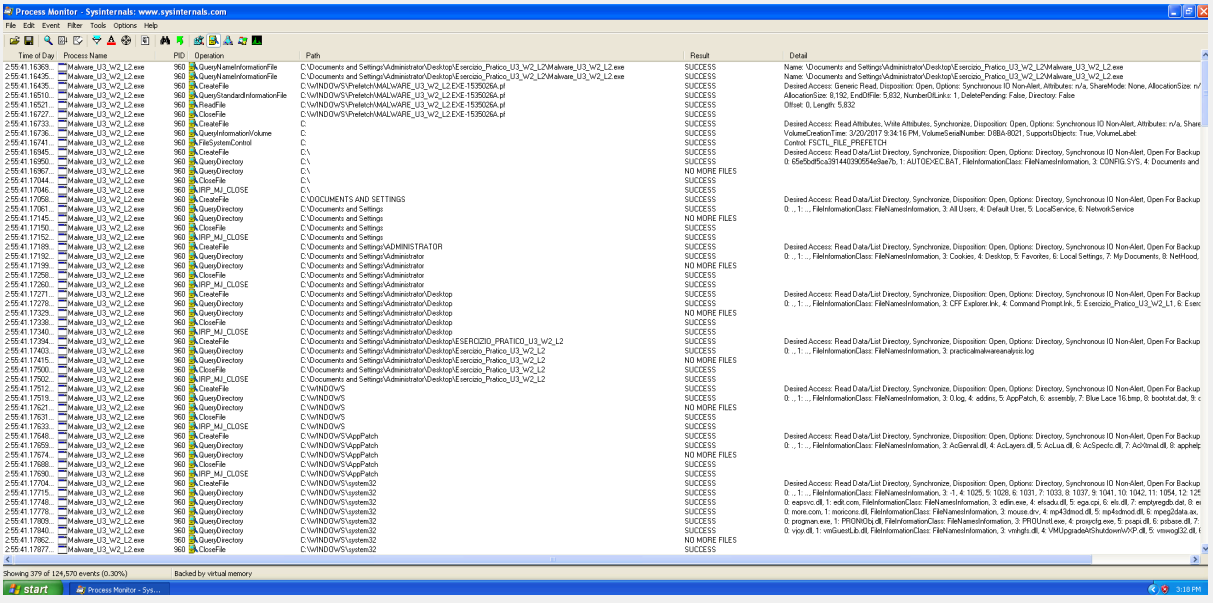
Traccia:

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.**

Traccia 1

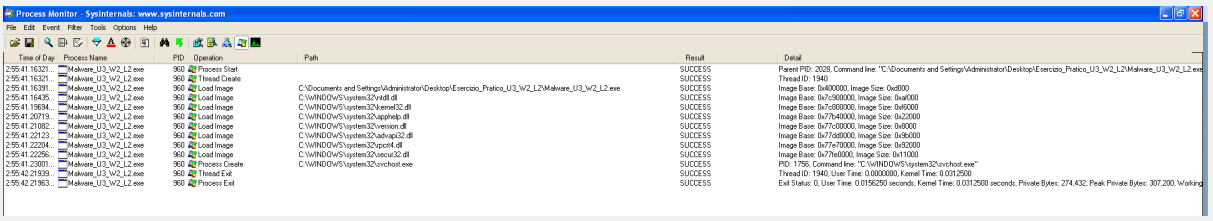
Identificare eventuali azioni del malware sul file system utilizzando Process Monitor



Malware_U3_W2_L2.exe	960	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_\
Malware_U3_W2_L2.exe	960	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_\
Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe	960	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe	960	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe	960	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe	960	CreateFile	C:
Malware_U3_W2_L2.exe	960	QueryInformationVolume	C:

Traccia 2

- **Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor**



2:55:41.16321...	Malware_U3_W2_L2.exe	960	Process Start		
2:55:41.16321...	Malware_U3_W2_L2.exe	960	Thread Create		
2:55:41.16391...	Malware_U3_W2_L2.exe	960	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	
2:55:41.16435...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\ntdll.dll	
2:55:41.19694...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\kernel32.dll	
2:55:41.20719...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\apphelp.dll	
2:55:41.21082...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\version.dll	
2:55:41.22123...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\advapi32.dll	
2:55:41.22204...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\rpcrt4.dll	
2:55:41.22256...	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\secur32.dll	
2:55:41.23001...	Malware_U3_W2_L2.exe	960	Process Create	C:\WINDOWS\system32\svchost.exe	
2:55:42.21939...	Malware_U3_W2_L2.exe	960	Thread Exit		
2:55:42.21963...	Malware_U3_W2_L2.exe	960	Process Exit		

Traccia 3

- **Provare a profilare il malware in base alla correlazione tra «operation» e Path.**

Utilizziamo le icone per filtrare gli eventi riguardanti processi e thread. Vediamo alcune funzioni molto interessanti come Load Image che viene utilizzata per «caricare» per l'esecuzione il malware e le librerie (.dll) necessarie, e poi vediamo «Process Create» che serve per creare un processo. Sembra che il nostro malware stia creando un processo chiamato «svchost.exe» che generalmente è un processo valido di Windows. Questo è un altro comportamento frequente dei malware, cercare di camuffare la loro esecuzione sotto un processo con un nome valido per eludere eventuali antivirus / anti malware.