Malware Analysis

Analisi Dinamica Basica

Traccia

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.

Process Monitor

Prima di tutto avviamo Process Monitor settiamo i nostri filtri:

Impostiamo il filtro Process name ed inseriamo il nome del Malware:

Malware_U3_W2_L2.exe

in questo modo il tool filtrera solo per i processi con questo nome.

Avviamo quindi il malware con un doppio click sul file eseguibile.

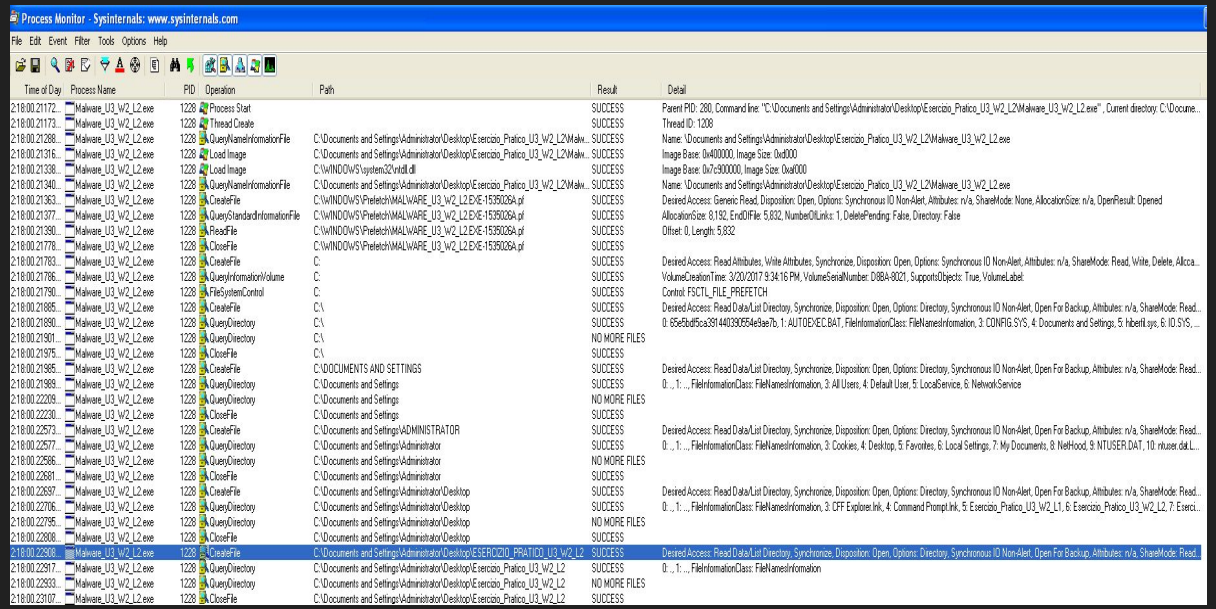
Eseguito il malware si aprirà una finestra di terminale e si andrà a chiudere in pochi secondi.

Spostiamoci su Process monitor per vedere la scansione.

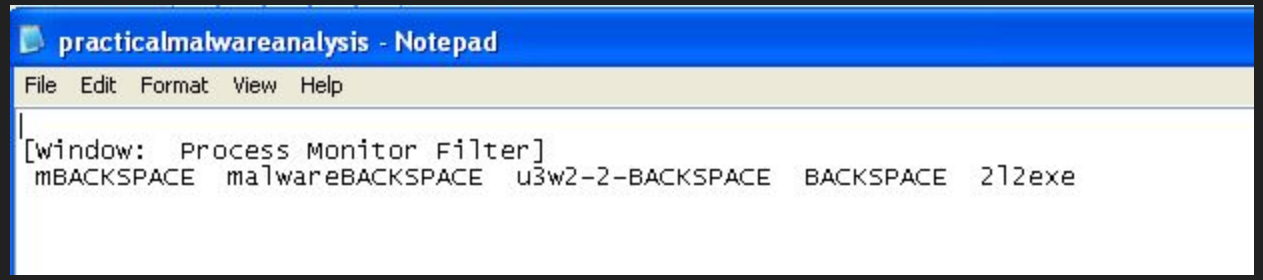
Identificare Azioni File System

Come mostrato in figura il malware ha svolto diverse azioni, soffermiamoci su quella CreateFile come suggerito dalla traccia:

Il malware è andato a creare un file.txt all'interno della cartella ESERCIZIO_PRATICO_U3_W2_L2



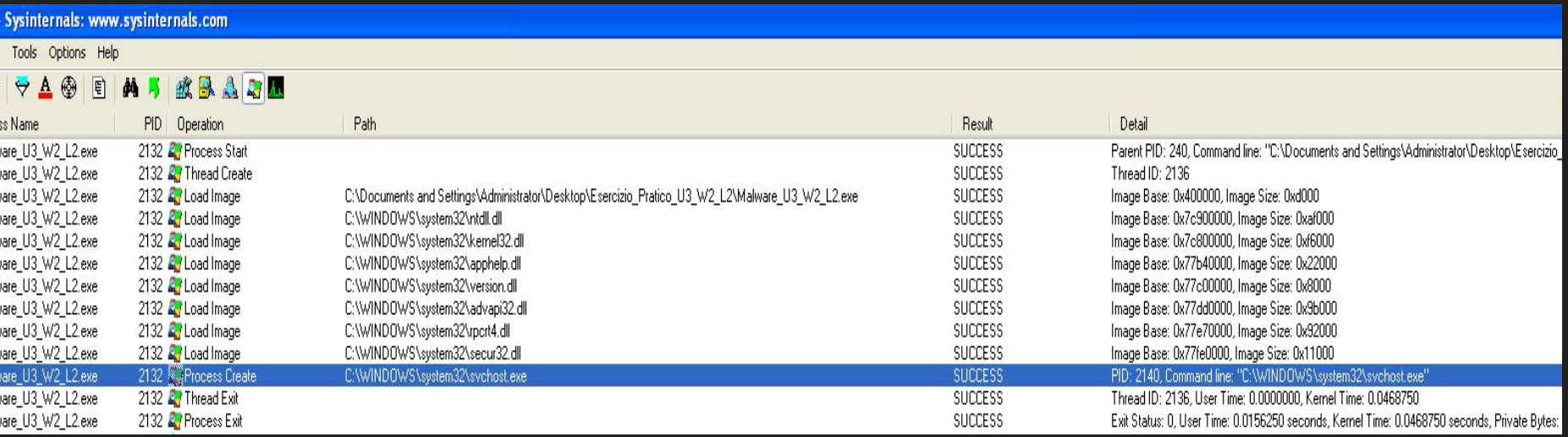
Come vedremo nella prossima slide il file creato è un testo con scritto tutto quello che è stato digitato sulla tastiera da quando è stato avviato il malware.



Qui notiamo che al file è stato dato il nome praticamalwareanalysis, siamo all'interno di Process Monitor Filter, e abbiamo inserito i filtro per cercare i processi eseguiti dal malware.
Tuttavia non sono riuscito a capire perchè una volta cancellato questo file e riprovata la procedura il malware non vada creare un nuovo file ogni volta.

Indentificare Azioni su Processi e Threads

Infine andiamo a valutare quali processi compie il malware:
é interessante vedere che il malware crea un processo per falsificare il suo nome prima dell'esecuzione con *svchost.exe*.
Questo processo, infatti, funge da shell per il caricamento di file DLL (Dynamic-link library) che comprendono librerie software che vengono caricate, in modo dinamico, in fase di esecuzione invece di essere collegate staticamente ad un file eseguibile in fase di compilazione.
E tuttavia risaputo che è stato spesso utilizzato dai creatori di malware per nasconderli.



ss Name	PID	Operation	Path	Result	Detail
are_U3_W2_L2.exe	2132	Process Start		SUCCESS	Parent PID: 240, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_
are_U3_W2_L2.exe	2132	Thread Create		SUCCESS	Thread ID: 2136
are_U3_W2_L2.exe	2132	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
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
are_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
are_U3_W2_L2.exe	2132	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2140, Command line: "C:\WINDOWS\system32\svchost.exe"
are_U3_W2_L2.exe	2132	Thread Exit		SUCCESS	Thread ID: 2136, User Time: 0.0000000, Kernel Time: 0.0468750
are_U3_W2_L2.exe	2132	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: