

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 del 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

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit View Filter Tools Options Help					
Time of Day	Process Name	PID	Operation	Path	Result
255:41:18302	Malware_U3_W2_L2.exe	960	QueryInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
255:41:18425	Malware_U3_W2_L2.exe	960	QueryInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
255:41:18435	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:18501	Malware_U3_W2_L2.exe	960	QueryStandardInformationFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:18521	Malware_U3_W2_L2.exe	960	ReadFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:18527	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:18533	Malware_U3_W2_L2.exe	960	CreateFile	C:\	SUCCESS
255:41:18736	Malware_U3_W2_L2.exe	960	QueryInformationVolume	C:\	SUCCESS
255:41:18741	Malware_U3_W2_L2.exe	960	FileSystemControl	C:\	SUCCESS
255:41:18845	Malware_U3_W2_L2.exe	960	CreateFile	C:\	SUCCESS
255:41:18950	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\	SUCCESS
255:41:18957	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\	NO MORE FILES
255:41:19044	Malware_U3_W2_L2.exe	960	CreateFile	C:\	SUCCESS
255:41:19046	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\	SUCCESS
255:41:19058	Malware_U3_W2_L2.exe	960	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
255:41:19081	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings	SUCCESS
255:41:19145	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings	NO MORE FILES
255:41:19150	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings	SUCCESS
255:41:19152	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\Documents and Settings	SUCCESS
255:41:19189	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS
255:41:19195	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS
255:41:19198	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES
255:41:19258	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator	SUCCESS
255:41:19260	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator	SUCCESS
255:41:19271	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
255:41:19295	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS
255:41:19328	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES
255:41:19328	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
255:41:19340	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop	SUCCESS
255:41:19344	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
255:41:19403	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
255:41:19415	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES
255:41:19500	Malware_U3_W2_L2.exe	960	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
255:41:19502	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
255:41:19512	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS	SUCCESS
255:41:19513	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS	SUCCESS
255:41:19621	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS	NO MORE FILES
255:41:19623	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS	SUCCESS
255:41:19623	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\WINDOWS	SUCCESS
255:41:19646	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19659	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19674	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	NO MORE FILES
255:41:19686	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19689	Malware_U3_W2_L2.exe	960	IRP_MJ_CLOSE	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19704	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19716	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19776	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19776	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19789	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19840	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS
255:41:19862	Malware_U3_W2_L2.exe	960	QueryDirectory	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	NO MORE FILES
255:41:19877	Malware_U3_W2_L2.exe	960	CreateFile	C:\WINDOWS\system32\malware_U3_W2_L2\EIE-15930264.pl	SUCCESS

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

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:55:41.16321	Malware_U3_W2_L2.exe	960	Process Start		SUCCESS	Parent PID: 2038, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"
2:55:41.16321	Malware_U3_W2_L2.exe	960	Thread Create		SUCCESS	Thread ID: 1940
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	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
2:55:41.16435	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.19694	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.20719	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.21082	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.22123	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.22204	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.22256	Malware_U3_W2_L2.exe	960	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77000000, Image Size: 0x0000
2:55:41.23001	Malware_U3_W2_L2.exe	960	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1795, Command line: "C:\WINDOWS\system32\svchost.exe"
2:55:42.21939	Malware_U3_W2_L2.exe	960	Thread Exit		SUCCESS	Thread ID: 1940, User Time: 0.000000, Kernel Time: 0.001250
2:55:42.21963	Malware_U3_W2_L2.exe	960	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0196250 seconds, Kernel Time: 0.0012500 seconds, Private Bytes: 274,432, Peak Private Bytes: 307,200, Working

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.

