

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 filtrerà 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.

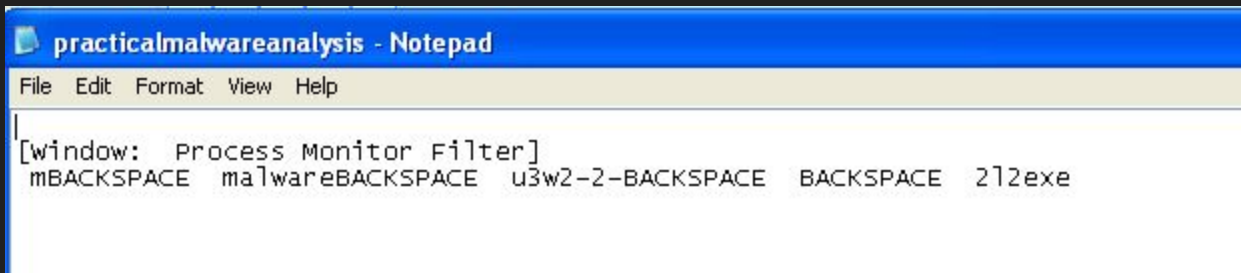
Identificare Azioni File System

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

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
21:00:21172	Malware_U3_W2_L2.exe	1228	Process Start		SUCCESS	Parent PID: 280, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe", Current directory: C:\Docume...
21:00:21173	Malware_U3_W2_L2.exe	1228	Thread Create		SUCCESS	Thread ID: 1208
21:00:21288	Malware_U3_W2_L2.exe	1228	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2	SUCCESS	Name: 'C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2'
21:00:21316	Malware_U3_W2_L2.exe	1228	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
21:00:21338	Malware_U3_W2_L2.exe	1228	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x0a000
21:00:21340	Malware_U3_W2_L2.exe	1228	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2	SUCCESS	Name: 'C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2'
21:00:21363	Malware_U3_W2_L2.exe	1228	CreateFile	C:\WINDOWS\system32\MALWARE_U3_W2_L2\ESERCIZIO_PRATICO_U3_W2_L2.txt	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened
21:00:21377	Malware_U3_W2_L2.exe	1228	QueryStandardInformationFile	C:\WINDOWS\system32\MALWARE_U3_W2_L2\ESERCIZIO_PRATICO_U3_W2_L2.txt	SUCCESS	AllocationSize: 8192, EndOfFile: 5,832, NumberOfLinks: 1, DeletePending: False, Directory: False
21:00:21390	Malware_U3_W2_L2.exe	1228	ReadFile	C:\WINDOWS\system32\MALWARE_U3_W2_L2\ESERCIZIO_PRATICO_U3_W2_L2.txt	SUCCESS	Offset: 0, Length: 5,832
21:00:21778	Malware_U3_W2_L2.exe	1228	CloseFile	C:\WINDOWS\system32\MALWARE_U3_W2_L2\ESERCIZIO_PRATICO_U3_W2_L2.txt	SUCCESS	
21:00:21763	Malware_U3_W2_L2.exe	1228	CreateFile	C:\	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, Delete, Allica...
21:00:21766	Malware_U3_W2_L2.exe	1228	QueryInformationVolume	C:\	SUCCESS	VolumeCreationTime: 3/20/2017 3:34:16 PM, VolumeSerialNumber: 0BBA-B021, SupportObjects: True, VolumeLabel
21:00:21766	Malware_U3_W2_L2.exe	1228	FileSystemControl	C:\	SUCCESS	Control FSCTL_FILE_PREFETCH
21:00:21865	Malware_U3_W2_L2.exe	1228	CreateFile	C:\	SUCCESS	Desired Access: Read Data List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
21:00:21860	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\	SUCCESS	0, 856285c339144039354e9a7b, 1, AUTOEXEC.BAT, FileInformationClass: FileNameInformation, 3, CONFIG.SYS, 4, Documents and Settings, 5, Internet, 6, IO SYS...
21:00:21901	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\	NO MORE FILES	
21:00:21975	Malware_U3_W2_L2.exe	1228	CloseFile	C:\	SUCCESS	
21:00:21985	Malware_U3_W2_L2.exe	1228	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
21:00:21989	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings	SUCCESS	0, ..., 1, FileInformationClass: FileNameInformation, 3, All Users, 4, Default User, 5, LocalService, 6, NetworkService
21:00:22009	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
21:00:22230	Malware_U3_W2_L2.exe	1228	CloseFile	C:\Documents and Settings	SUCCESS	
21:00:22573	Malware_U3_W2_L2.exe	1228	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
21:00:22577	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0, ..., 1, FileInformationClass: FileNameInformation, 3, Cookies, 4, Desktop, 5, Favorites, 6, Local Settings, 7, My Documents, 8, NetHood, 9, NTUSER.DAT, 10, ntuser.dat...
21:00:22586	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
21:00:22681	Malware_U3_W2_L2.exe	1228	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
21:00:22697	Malware_U3_W2_L2.exe	1228	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
21:00:22706	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0, ..., 1, FileInformationClass: FileNameInformation, 3, CFF Explorer, 4, Command Prompt, 5, Esercizio_Pratico_U3_W2_L1, 6, Esercizio_Pratico_U3_W2_L2, 7, Eserc...
21:00:22795	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
21:00:22808	Malware_U3_W2_L2.exe	1228	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
21:00:22938	Malware_U3_W2_L2.exe	1228	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	Desired Access: Read Data List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read...
21:00:22917	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0, ..., 1, FileInformationClass: FileNameInformation
21:00:22933	Malware_U3_W2_L2.exe	1228	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
21:00:22907	Malware_U3_W2_L2.exe	1228	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	

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 il 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.

Sysinternals: www.sysinternals.com

Tools Options Help



Process Name	PID	Operation	Path	Result	Detail
Malware_U3_W2_L2.exe	2132	Process Start		SUCCESS	Parent PID: 240, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio
Malware_U3_W2_L2.exe	2132	Thread Create		SUCCESS	Thread ID: 2136
Malware_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
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xa000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\iprt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
Malware_U3_W2_L2.exe	2132	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77e00000, Image Size: 0x11000
Malware_U3_W2_L2.exe	2132	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2140, Command line: "C:\WINDOWS\system32\svchost.exe"
Malware_U3_W2_L2.exe	2132	Thread Exit		SUCCESS	Thread ID: 2136, User Time: 0.0000000, Kernel Time: 0.0468750
Malware_U3_W2_L2.exe	2132	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: