

## CONSEGNA S10L2

L'obiettivo di oggi, con riferimento al file eseguibile contenuto nella cartella "Esercizio\_Pratico\_U3\_W2\_L2", è quello di:

- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware (le differenze)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Prima di cominciare vorrei sottolineare che per questa analisi mi sono servito di Windows 7 e Windows XP, il primo mi è servito per usare alcuni programmi di analisi( come CFF Explorer), il secondo l'ho usato per lanciare il malware.

Nel contesto di un analisi dinamica basica, il malware viene studiato mentre è in esecuzione, ma è altresì importante una preventiva analisi statica: uno degli strumenti che si utilizzano in questo contesto è CFF Explorer.

Malware_U3_W2_L2.exe						
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000

Fig.1

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00004548	00004548	001B	CloseHandle
00004556	00004556	02BF	VirtualFree
00004564	00004564	0218	ReadFile
00004570	00004570	02BB	VirtualAlloc
00004580	00004580	0112	GetFileSize
0000458E	0000458E	0034	CreateFileA
0000459C	0000459C	022C	ResumeThread
000045AC	000045AC	0283	SetThreadContext
000045C0	000045C0	02E9	WriteProcessMemory
000045D6	000045D6	02BC	VirtualAllocEx

Fig.2

Dopo aver caricato il file malevolo sul tool, vediamo che l'unica libreria usata dal malware è la KERNEL32.dll e che sono state importate alcune funzioni molto interessanti, come CreateFileA, Read File e Closefile (Fig.1 e Fig.2).

Terminata questa breve analisi statica possiamo passare a quella dinamica. Per prima cosa ho avviato Process Monitor e il il malware. Dopo circa un minuto ho interrotto la cattura per poter analizzare il report. Prima di avviare la scansione, ho inserito nel filtro del tool il nome dell'eseguibile, così che ci vengano mostrati solo i risultati che ci interessano. Vediamo subito dal report che ci sono delle funzioni riportate molto interessanti, come Create, Read and Closefile. In Fig.3 possiamo vedere che tramite la funzione create File viene creato un file all'interno della cartella dove risiede il malware. (Fig.4)

QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Malware_test\MALWARE	NO MORE FILES
CloseFile	C:\Documents and Settings\Administrator\Desktop\Malware_test\MALWARE	SUCCESS
CreateFile	C:\Documents and Settings\Administrator\Desktop\Malware_test\MALWARE\Esercizio_Pratico_U3_W2_L2	SUCCESS
QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Malware_test\MALWARE\Esercizio_Pratico_U3_W2_L2	SUCCESS
CloseFile	C:\Documents and Settings\Administrator\Desktop\Malware_test\MALWARE\Esercizio_Pratico_U3_W2_L2	NO MORE FILES

Fig.3



Fig.4

Aprendo questo file di testo possiamo notare che il file ha acquisito alcuni caratteri da tastiera utilizzati durante l'esecuzione del malware, ne evinciamo che il malware potrebbe essere un Keylogger

Nella parte dei processi e thread invece, possiamo notare che è stato creato un processo, con Process Create, chiamato svchost.exe: sembra quindi che il malware cerchi di camuffarsi sotto un processo con un nome valido, per eludere eventuali antivirus / antimalware. (Fig.5)

Load Image	C:\WINDOWS\system32\advapi32.dll	Image Base: 0x77f40000, Image Size: 0xab000
Load Image	C:\WINDOWS\system32\rpcrt4.dll	Image Base: 0x77da0000, Image Size: 0x92000
Load Image	C:\WINDOWS\system32\secur32.dll	Image Base: 0x77f10000, Image Size: 0x11000
Process Create	C:\WINDOWS\system32\svchost.exe	PID: 924, Command line: "C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkDeps"

Fig.5

Possiamo quindi ipotizzare che il nostro malware, all'esecuzione, cerchi di camuffarsi creando un nuovo processo chiamato «svchost.exe», per poi lanciare la sua principale funzionalità ovvero un keylogger che salva i caratteri digitati dall'utente nel file «practicalmalwareanalysis». (Fig.6)

The screenshot shows a Windows Notepad application window with the title bar "practicalmalwareanalysis - Blocco note". The menu bar includes "File", "Modifica", "Formato", "Visualizza", and "?". The main text area contains several lines of text, each preceded by "[window:", indicating different command prompts or windows. The text demonstrates the use of the BACKSPACE key to delete characters:

- [window: ~res-x86 - Blocco note]
- [window: ~res-x86 - Blocco note]
- [window: ~res-x86 - Blocco note]
- [window: practicalmalwareanalysis - Blocco note]
- [window: practicalmalwareanalysis - Blocco note]
- [window: practicalmalwareanalysis - Blocco note]
- [window: BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE BACKSPACE]
- [window: Esercizio\_Pratico\_U3\_w2\_L2]
- [window: Esercizio\_Pratico\_U3\_w2\_L2]
- [window: Esercizio\_Pratico\_U3\_w2\_L2]
- [window: ddddddddddfffffffggggggfffff]
- [window: sysinternalsuite]

Fig.6