

Copia di Esercitazione WEEK 21 D1

Analisi dinamica basica

Ettore Farris

Descrizione sintetica

Traccia:

Nella lezione teorica, 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 (procmon)*
- *Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor*
- *Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (le differenze)*

Suggerimento:

Per quanto riguarda le attività del malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione Create File su path noti (ad esempio il path dove è presente l'eseguibile del malware).

Creare istantanea da Virtualbox della macchina prima di iniziare per poterla ripristinare in caso di problemi (o al limite fare il clone).

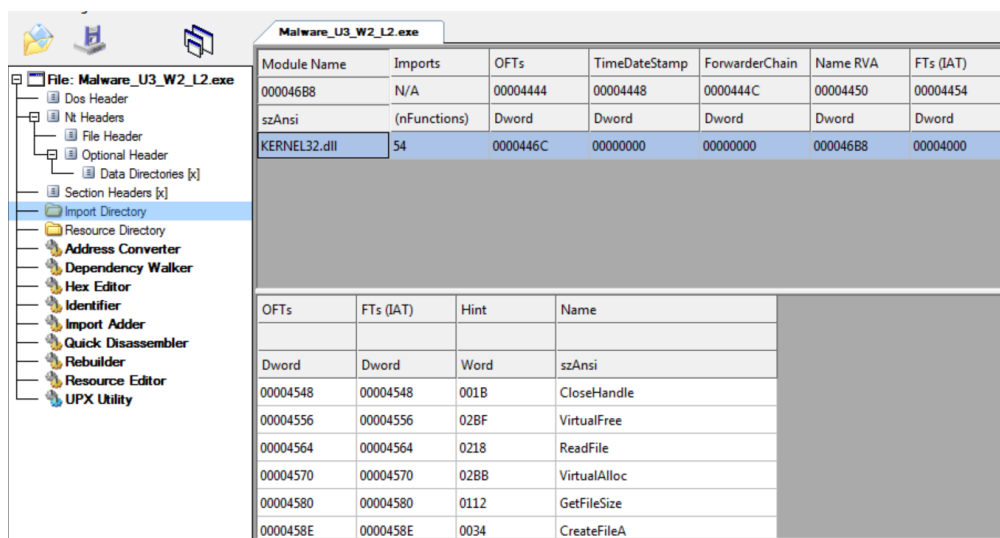
Analisi statica

Strings e analisi statica delle librerie

Per prima cosa svolgiamo un'analisi statica sul malware. Lanciamo il tool *strings* per ricercare stringhe interessanti sull'eseguibile:

```
cmd: Segna C:\Windows\system32\CMD.exe - strings C:\Users\user\Desktop\MAL
=9@
A9@
CloseHandle
VirtualFree
ReadFile
VirtualAlloc
GetFileSize
CreateFileA
ResumeThread
SetThreadContext
WriteProcessMemory
VirtualAllocEx
GetProcAddress
GetModuleHandleA
ReadProcessMemory
GetThreadContext
CreateProcessA
FreeResource
SizeofResource
LockResource
LoadResource
FindResourceA
GetSystemDirectoryA
Sleep
KERNEL32.dll
GetCommandLineA
GetVersion
ExitProcess
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
```

Notiamo la presenza della libreria di sistema KERNEL32.dll e funzioni usate dal programma come CreateFile, ReadFile, VirtualFree ecc... Proviamo ad effettuare un'analisi con CFFExplorer per confermare i risultati ottenuti.



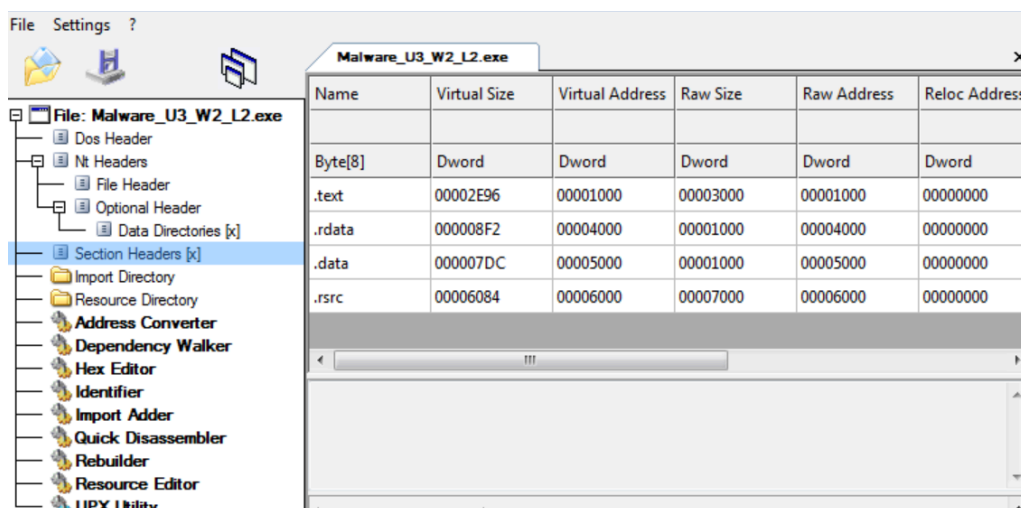
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000

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

Notiamo quindi che il malware chiama la libreria di sistema KERNEL32.dll che interagisce con il sistema operativo per manipolazione dei file, gestione della memoria ecc... Confermiamo anche la presenza delle funzioni trovate con l'utility strings.

Headers

Sempre con CFFExplorer, possiamo vedere la presenza degli headers *.text*, *.rdata*, *.data*, *.rsrc*.



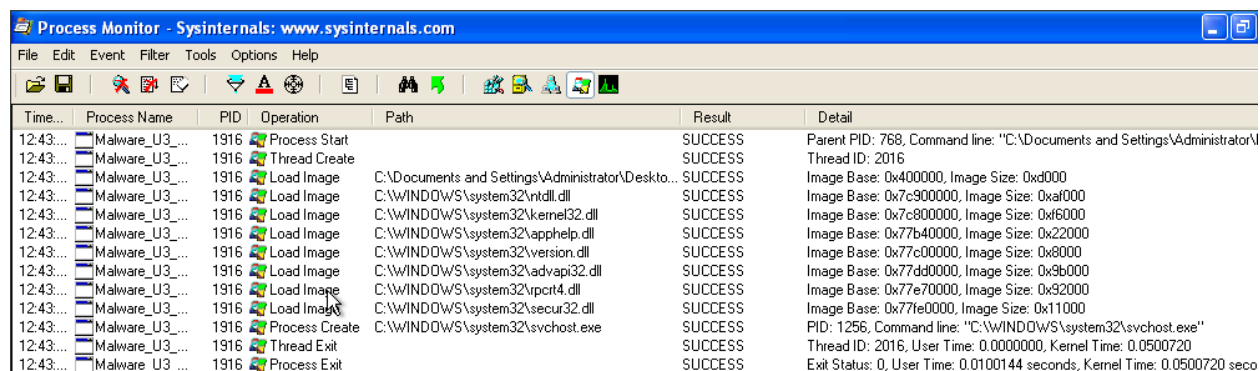
Dati generali sull'eseguibile

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malw...
File Type	Portable Executable 32
File Info	Microsoft Visual C++ 6.0
File Size	52.00 KB (53248 bytes)
PE Size	52.00 KB (53248 bytes)
Created	Friday 08 April 2011, 13.55.00
Modified	Wednesday 17 January 2024, 18.48.15
Accessed	Friday 08 April 2011, 13.55.00
MD5	E2BF42217A67E46433DA8B6F4507219E
SHA-1	DAF263702F11DC0430D30F9BF443E7885CF91FCB

Analisi dinamica basica

Lanciamo *procmon* e subito dopo avviamo l'eseguibile.

- Processi e thread



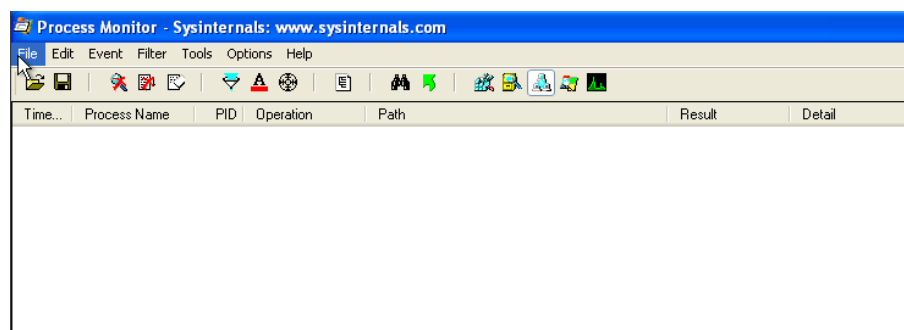
The screenshot shows the Process Monitor window with the following data:

Time...	Process Name	PID	Operation	Path	Result	Detail
12:43:...	Malware_U3_...	1916	Process Start		SUCCESS	Parent PID: 768, Command line: "C:\Documents and Settings\Administrator\...
12:43:...	Malware_U3_...	1916	Thread Create		SUCCESS	Thread ID: 2016
12:43:...	Malware_U3_...	1916	Load Image	C:\Documents and Settings\Administrator\Desкто...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x16000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
12:43:...	Malware_U3_...	1916	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x771e0000, Image Size: 0x11000
12:43:...	Malware_U3_...	1916	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1256, Command line: "C:\WINDOWS\system32\svchost.exe"
12:43:...	Malware_U3_...	1916	Thread Exit		SUCCESS	Thread ID: 2016, User Time: 0.000000, Kernel Time: 0.0500720
12:43:...	Malware_U3_...	1916	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time: 0.0500720 seco

Una volta avviato l'eseguibile, il malware carica una serie di librerie *.dll* che vengono ospitate dal processo *svchost.exe* per poter essere eseguite. Il processo *svchost.exe* infatti è processo di sistema generico di Windows, che può ospitare uno o più servizi del sistema operativo (le librerie *dll*), Per questo motivo, è spesso sfruttato da autori di malware per realizzare dei file malevoli in grado di “nascondersi” all'interno dei numerosi servizi di Windows per agire più o meno indisturbati.

- Eventi di rete

Il malware non cerca di connettersi ad internet o ad altri host della rete.



The screenshot shows the Process Monitor window with the following data:

Time...	Process Name	PID	Operation	Path	Result	Detail
---------	--------------	-----	-----------	------	--------	--------

- Azioni sul file system

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
1:27:3...	Malware_U3...	1396	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: E...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: E...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	CreateFile	C:\WINDOWS\system32\securl32.dll	SUCCESS	Desired Access: E...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\securl32.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	CreateFileApp...	C:\WINDOWS\system32\securl32.dll	SUCCESS	SyncType: SyncTy...
1:27:3...	Malware_U3...	1396	ReadFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Offset: 164,864, Le...
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:\WINDOWS\system32\securl32.dll	SUCCESS	
1:27:3...	Malware_U3...	1396	CloseFile	C:	SUCCESS	
1:27:3...	Malware_U3...	1396	CreateFile	C:\Documents and Settings\Administrator\Des...	SUCCESS	Desired Access: E...
1:27:3...	Malware_U3...	1396	FileSystemContro...	C:\Documents and Settings\Administrator\Des...	SUCCESS	Control FSCTL_IS...
1:27:3...	Malware_U3...	1396	QueryOpen	C:\Documents and Settings\Administrator\Des...	NAME NOT FOUND	
1:27:3...	Malware_U3...	1396	ReadFile	C:\Documents and Settings\Administrator\Des...	SUCCESS	Offset: 16,384, Len...
1:27:3...	Malware_U3...	1396	ReadFile	C:\Documents and Settings\Administrator\Des...	SUCCESS	Offset: 4,096, Leng...

