

Traccia:

Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito).

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:

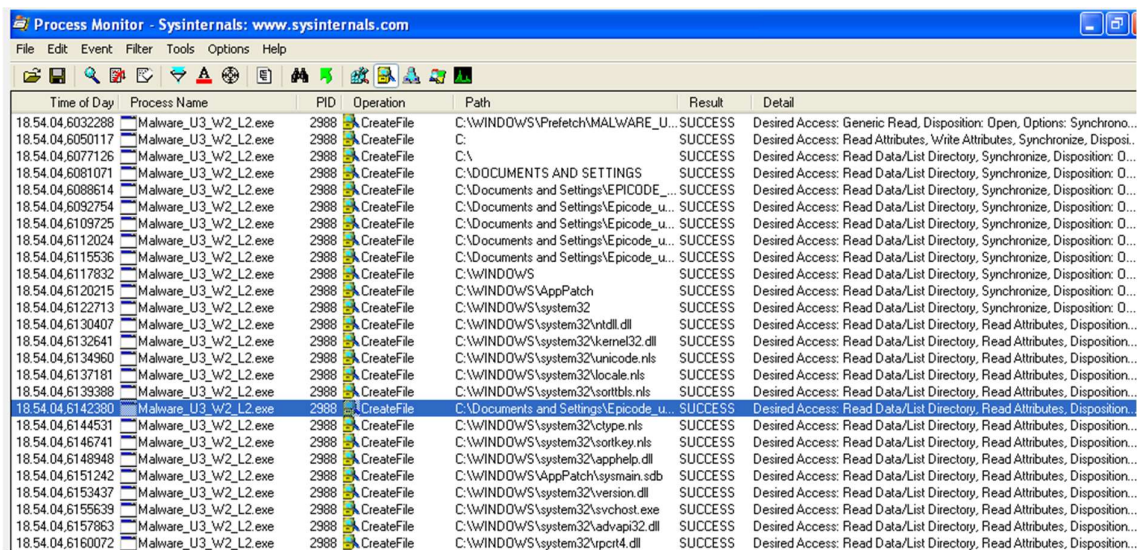
- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor (procmon) oppure se ci sono problemi **multimon** <https://www.resplendence.com/multimon> <https://multimon.it.uptodown.com/windows/download/23982> versione 2.5 per XP
- Identificare eventuali azioni del malware 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.

Suggerimento:

Per quanto riguarda le attività dal 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).

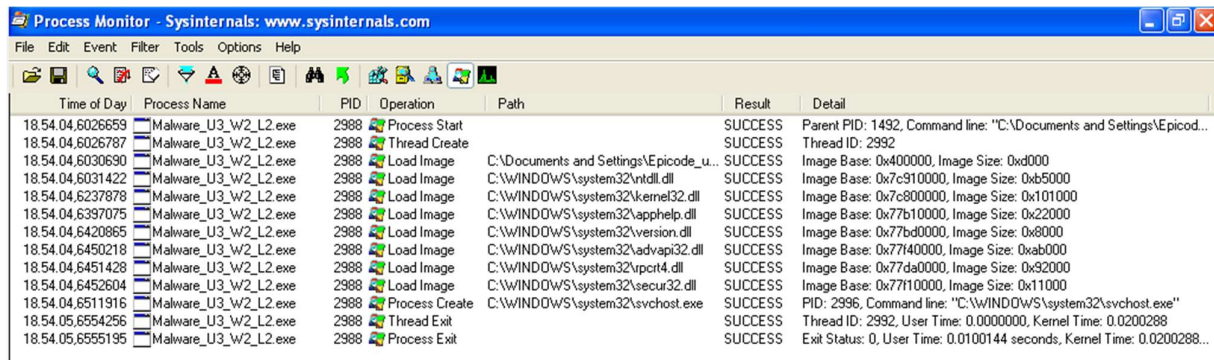
Creare istantanea da Virtualbox della macchina Windows XP prima di avviare il malware per poter ripristinare in caso di problemi (o al limite fare il clone)

Tramite l'utilizzo del tool Procmon combinato ai filtri del nome del file e dell'azione "CreateFile" abbiamo individuato le azione nel file system.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
18.54.04.6032288	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchron...
18.54.04.6050117	Malware_U3_W2_L2.exe	2988	CreateFile	C:\	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposi...
18.54.04.6077126	Malware_U3_W2_L2.exe	2988	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6081071	Malware_U3_W2_L2.exe	2988	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6088614	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6092754	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6109725	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6112024	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6115536	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6117832	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6120215	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6122713	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: O...
18.54.04.6130407	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6132641	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6134960	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6137181	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6139388	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6142380	Malware_U3_W2_L2.exe	2988	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6144531	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6146741	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6148948	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6151242	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6153437	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6155639	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6157863	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...
18.54.04.6160072	Malware_U3_W2_L2.exe	2988	CreateFile	C:\WINDOWS\system32\vpct4.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition...

Dai processi e thread relativi a questo file abbiamo constatato che crea un secondo processo in cui andrà a “mascherarsi”, nello specifico svchost.exe



Time of Day	Process Name	PID	Operation	Path	Result	Detail
18:54:04.6026659	Malware_U3_W2_L2.exe	2988	Process Start		SUCCESS	Parent PID: 1492, Command line: "C:\Documents and Settings\Epicod...
18:54:04.6026787	Malware_U3_W2_L2.exe	2988	Thread Create		SUCCESS	Thread ID: 2992
18:54:04.6030690	Malware_U3_W2_L2.exe	2988	Load Image	C:\Documents and Settings\Epicod..._u...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
18:54:04.6031422	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c910000, Image Size: 0xb5000
18:54:04.6237878	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x101000
18:54:04.6397075	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b10000, Image Size: 0x22000
18:54:04.6420865	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77bd0000, Image Size: 0x8000
18:54:04.6450218	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77f40000, Image Size: 0xab000
18:54:04.6451428	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77da0000, Image Size: 0x92000
18:54:04.6452604	Malware_U3_W2_L2.exe	2988	Load Image	C:\WINDOWS\system32\securlib.dll	SUCCESS	Image Base: 0x77f10000, Image Size: 0x11000
18:54:04.6511916	Malware_U3_W2_L2.exe	2988	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2996, Command line: "C:\WINDOWS\system32\svchost.exe"
18:54:05.6554256	Malware_U3_W2_L2.exe	2988	Thread Exit		SUCCESS	Thread ID: 2992, User Time: 0.0000000, Kernel Time: 0.0200288
18:54:05.6555195	Malware_U3_W2_L2.exe	2988	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time: 0.0200288...

Possiamo constatare che il programma si tratta di un keylogger che tiene traccia di quanto digitato in un file .txt presente nella stessa cartella dell'eseguibile.



Malware_U3_W2_L2



practicalmalwareanalysis
Documento di testo
1 KB