

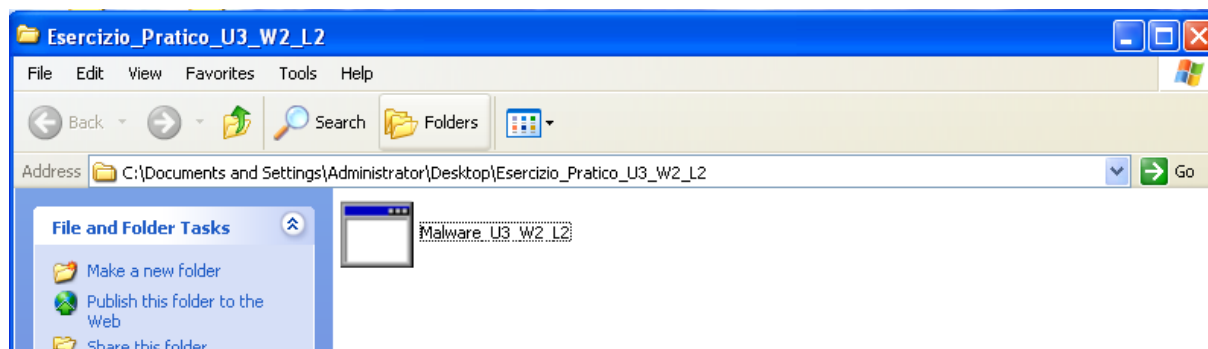
## Esercizio 28-03

Traccia: come approfondimento pratico del concetto di analisi dinamica visto in lezione, analizzare il file eseguibile nella cartella “Esercizio\_Pratico\_U3\_W2\_L2” presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware e rispondere ai seguenti quesiti:

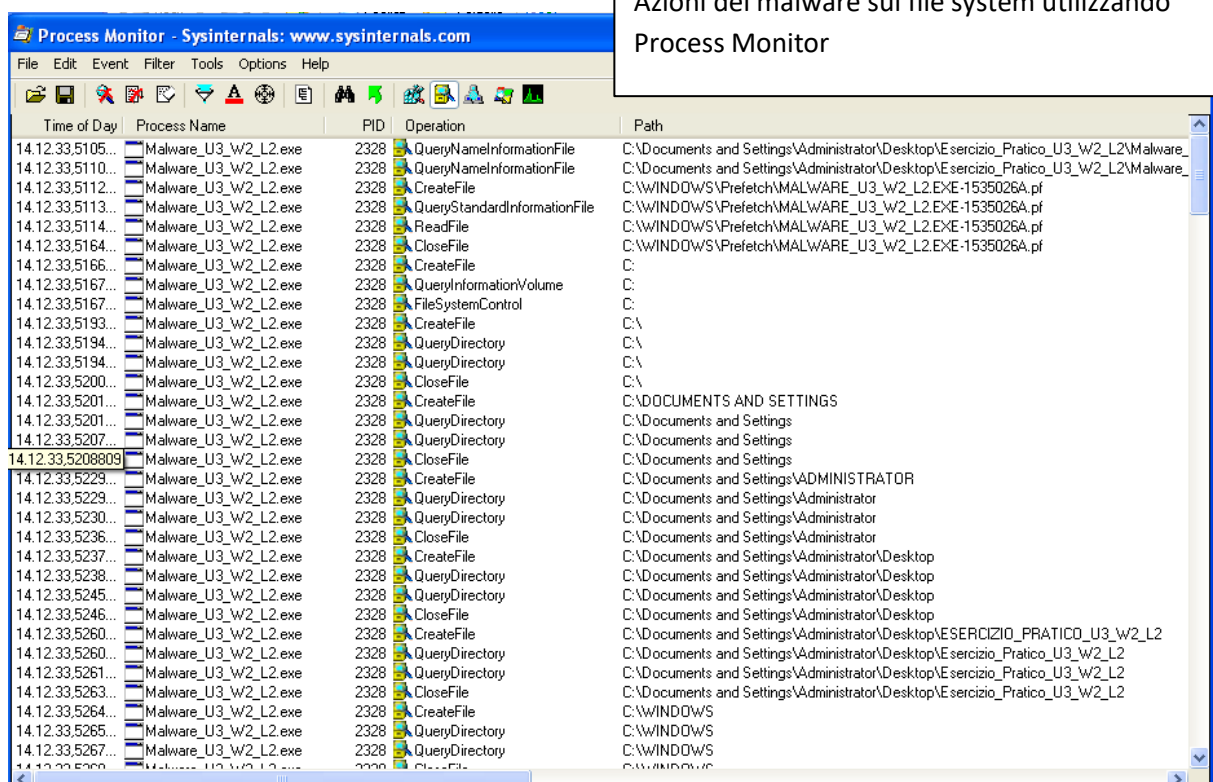
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra “operation” e Path

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’e eseguibile del malware).

Dopo aver avviato Process Monitor  
si esegue il malware



Azioni del malware sul file system utilizzando  
Process Monitor



## Aggiunta del filtro sull'operazione "CreateFile"

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

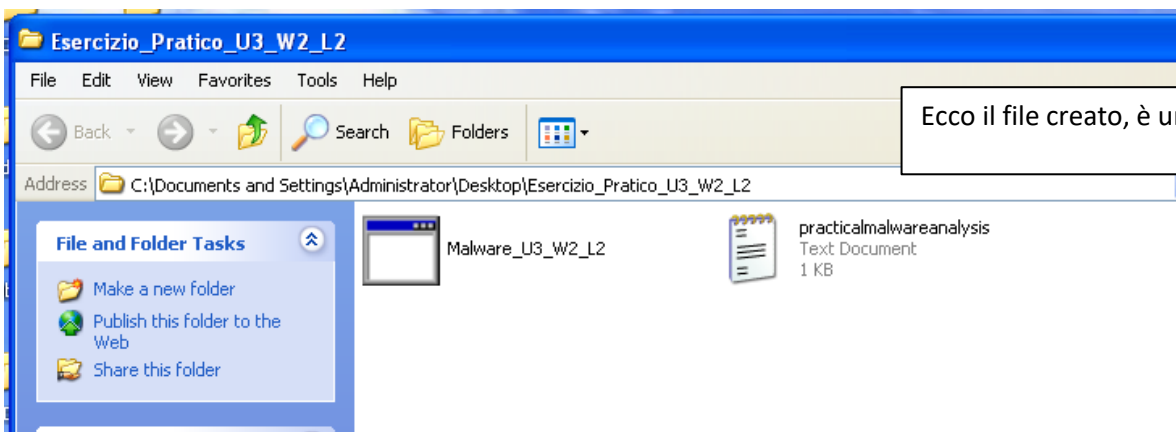
Time of Day	Process Name	PID	Operation	Path
15.25.13.7561...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
15.25.13.7574...	Malware_U3_W2_L2.exe	3104	CreateFile	C:
15.25.13.7575...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\
15.25.13.7582...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\DOCUMENTS AND SETTINGS
15.25.13.7610...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\ADMINISTRATOR
15.25.13.7619...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\Administrator\Desktop
15.25.13.7636...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2
15.25.13.7654...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS
15.25.13.7657...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\AppPatch
15.25.13.7661...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32
15.25.13.7692...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\ntdll.dll
15.25.13.7694...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\kernel32.dll
15.25.13.7696...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\unicode.nls
15.25.13.7699...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\locale.nls
15.25.13.7701...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\sorttbls.nls
15.25.13.7703...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE
15.25.13.7705...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\ctype.nls
15.25.13.7707...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\sortkey.nls
15.25.13.7710...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\apphelp.dll
15.25.13.7712...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb
15.25.13.7714...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\version.dll
15.25.13.7717...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\svchost.exe
15.25.13.7719...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\advapi32.dll
15.25.13.7722...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\vpicr4.dll
15.25.13.7724...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\secur32.dll
15.25.13.7819...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\ntdll.dll
15.25.13.7822...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\kernel32.dll
15.25.13.7824...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE
15.25.13.7826...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\apphelp.dll
15.25.13.7828...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\version.dll
15.25.13.7831...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\advapi32.dll
15.25.13.7833...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\vpicr4.dll
15.25.13.7836...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\WINDOWS\system32\secur32.dll
15.25.13.7849...	Malware_U3_W2_L2.exe	3104	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2

Si nota una operazione di creazione di un file nella directory del malware

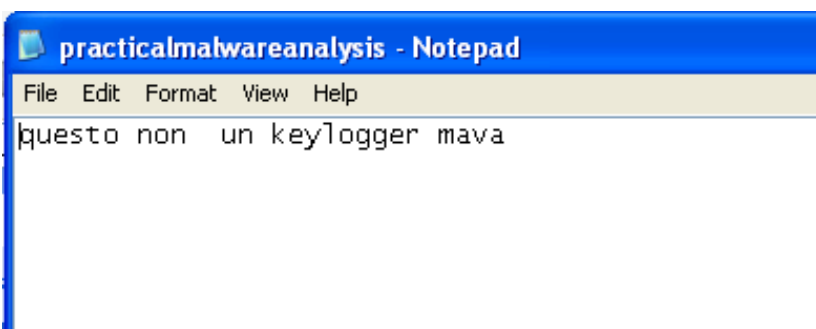
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

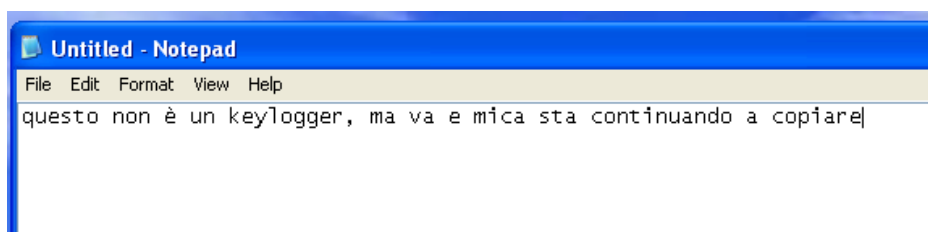
Time of Day	Process Name	PID	Operation	Path	Result
17.18.52.6898...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
17.18.52.6919...	Malware_U3_W2_L2.exe	808	CreateFile	C:	SUCCESS
17.18.52.6923...	Malware_U3_W2_L2.exe	808	CreateFile	C:\	SUCCESS
17.18.52.6927...	Malware_U3_W2_L2.exe	808	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
17.18.52.6936...	Malware_U3_W2_L2.exe	808	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS
17.18.52.6941...	Malware_U3_W2_L2.exe	808	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
17.18.52.6952...	Malware_U3_W2_L2.exe	808	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
17.18.52.6954...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS	SUCCESS
17.18.52.6973...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\AppPatch	SUCCESS
17.18.52.6978...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32	SUCCESS
17.18.52.6990...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS
17.18.52.6993...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS
17.18.52.6996...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS
17.18.52.6999...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS
17.18.52.7001...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS
17.18.52.7003...	Malware_U3_W2_L2.exe	808	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS
17.18.52.7005...	Malware_U3_W2_L2.exe	808	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS



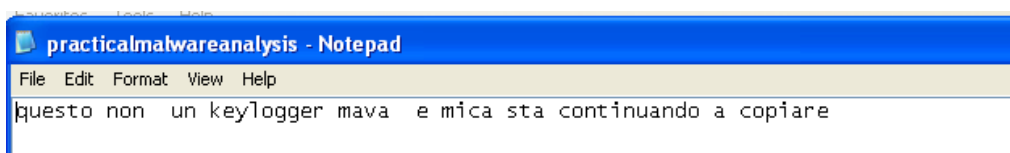
Ecco il file creato, è un file .txt



Il file contiene gli appunti che stavo prendendo durante l'analisi!



Per verificare se il processo è ancora attivo decido di aggiornare i miei appunti sul Notepad



Il file .txt continua ad aggiornarsi, il malware apre proprio un keylogger

Tornando su Process Monitor possiamo vedere le azioni del malware su processi e thread.

Il malware crea un processo chiamato "svchost.exe" un processo lecito di Windows, almeno così è il processo originale, questo è una copia che si spaccia per un processo "buono" e avvia l'azione di recording della tastiera

Process Monitor - Sysinternals: <a href="http://www.sysinternals.com">www.sysinternals.com</a>			
File Edit Event Filter Tools Options Help			
Time of Day	Process Name	PID	Operation
17.05.09,5241...	Malware_U3_W2_L2.exe	1796	Process Start
17.05.09,5241...	Malware_U3_W2_L2.exe	1796	Thread Create
17.05.09,5249...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5250...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5441...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5510...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5531...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5594...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5596...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5597...	Malware_U3_W2_L2.exe	1796	Load Image
17.05.09,5641...	Malware_U3_W2_L2.exe	1796	Process Create
17.05.10,5550...	Malware_U3_W2_L2.exe	1796	Thread Exit
17.05.10,5550...	Malware_U3_W2_L2.exe	1796	Process Exit

C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2  
C:\WINDOWS\system32\ntdll.dll  
C:\WINDOWS\system32\kernel32.dll  
C:\WINDOWS\system32\apphelp.dll  
C:\WINDOWS\system32\version.dll  
C:\WINDOWS\system32\advapi32.dll  
C:\WINDOWS\system32\rpcrt4.dll  
C:\WINDOWS\system32\secur32.dll  
C:\WINDOWS\system32\svchost.exe

#### Conclusione:

Il malware carica le librerie di cui ha bisogno ed avvia il processo di keylogging, i dati che cattura li trascrive in un file .txt nella cartella del malware.