

## Analisi Dinamica Basica

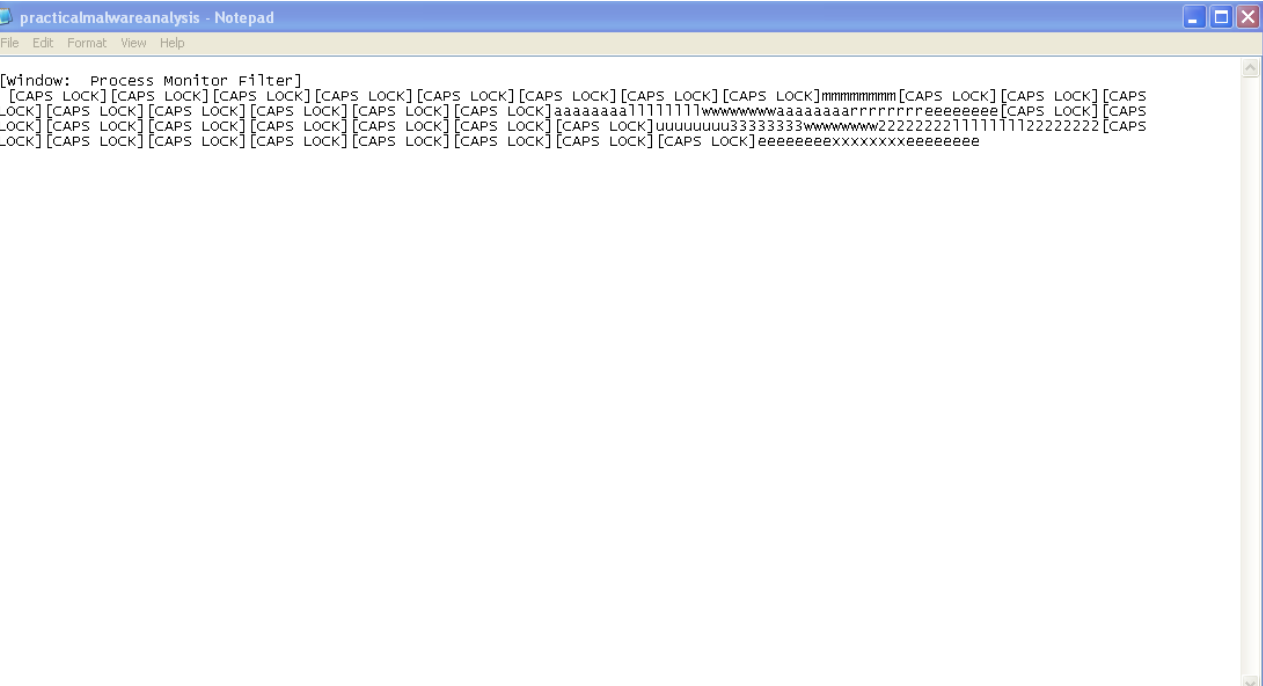
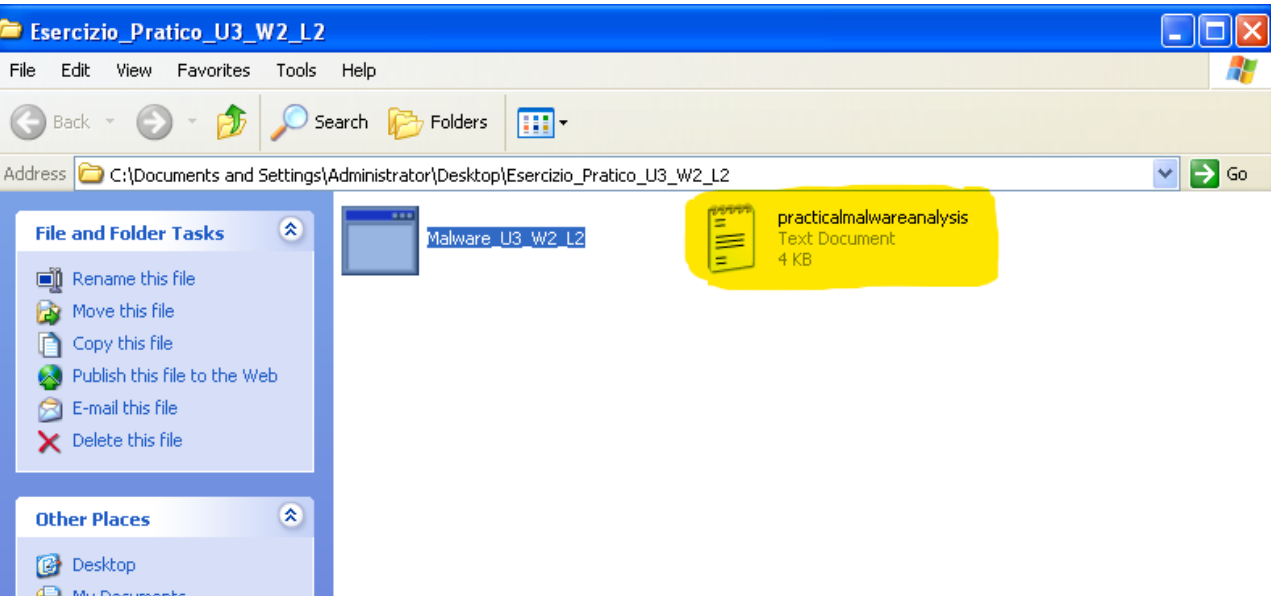
### Traccia:

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:

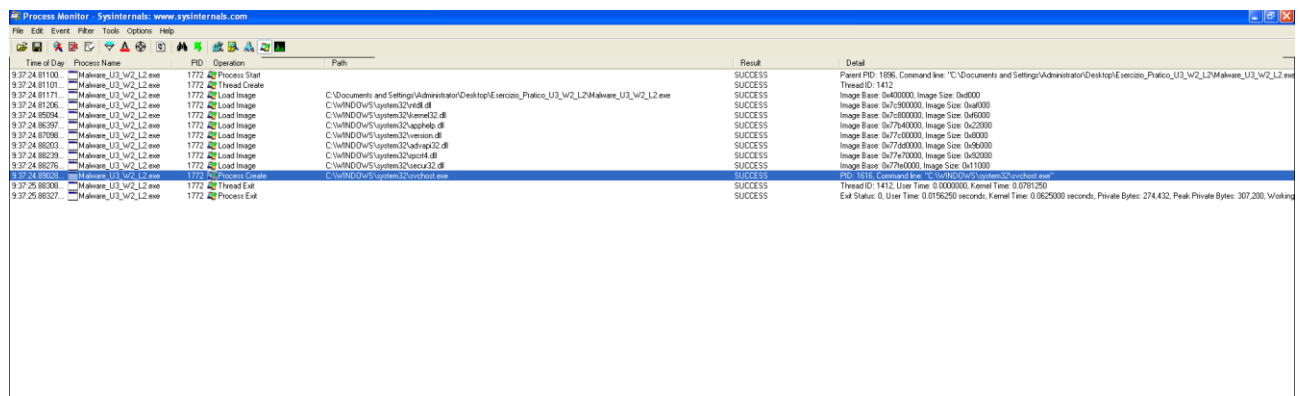
1. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
3. Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Come richiesto dall'esercizio, andiamo ad analizzare le azioni del malware che impattano sul file system, per fare ciò utilizziamo ProcMon, un tool che ci permette di monitorare i processi in esecuzione sulla macchina:

[illegible]



Utilizzando la cattura precedente di ProcMon e cliccando sull'icona "Processi e Thread" andiamo a filtrare i processi che appartengono a quella categoria.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
9/3/24 8:11:00	Malware_U3_W2_L2.exe	1772	Process Start		SUCCESS	Parent PID: 1896, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"
9/3/24 8:11:01	Malware_U3_W2_L2.exe	1772	Thread Create		SUCCESS	Thread ID: 1412
9/3/24 8:11:01	Malware_U3_W2_L2.exe	1772	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x6000
9/3/24 8:11:06	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x6000
9/3/24 8:11:04	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0x6000
9/3/24 8:11:07	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\GDI32.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0x2000
9/3/24 8:11:09	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x4000
9/3/24 8:11:03	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0x6000
9/3/24 8:11:09	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\ole32.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0x6000
9/3/24 8:11:06	Malware_U3_W2_L2.exe	1772	Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x77400000, Image Size: 0x11000
9/3/24 8:11:06	Malware_U3_W2_L2.exe	1772	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0196250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 274,432, Peak Private Bytes: 307,200, Working Set: 1,048,576

Abbiamo notato che il malware crea un processo chiamato Svchost.exe, che è il nome di un processo generalmente valido di Win. Questo comportamento è tipico dei malware che vogliono camuffare la loro identità e nascondendosi dalle analisi degli antivirus/antimalware così come dalle indagini approfondite di un utente.

Il malware cerca di camuffarsi chiamandosi Svchost, poi esegue la sua funzione principale di Key Logger salvando tutti i caratteri digitati dall'utente in un file chiamato practicalmalwareanalysis.