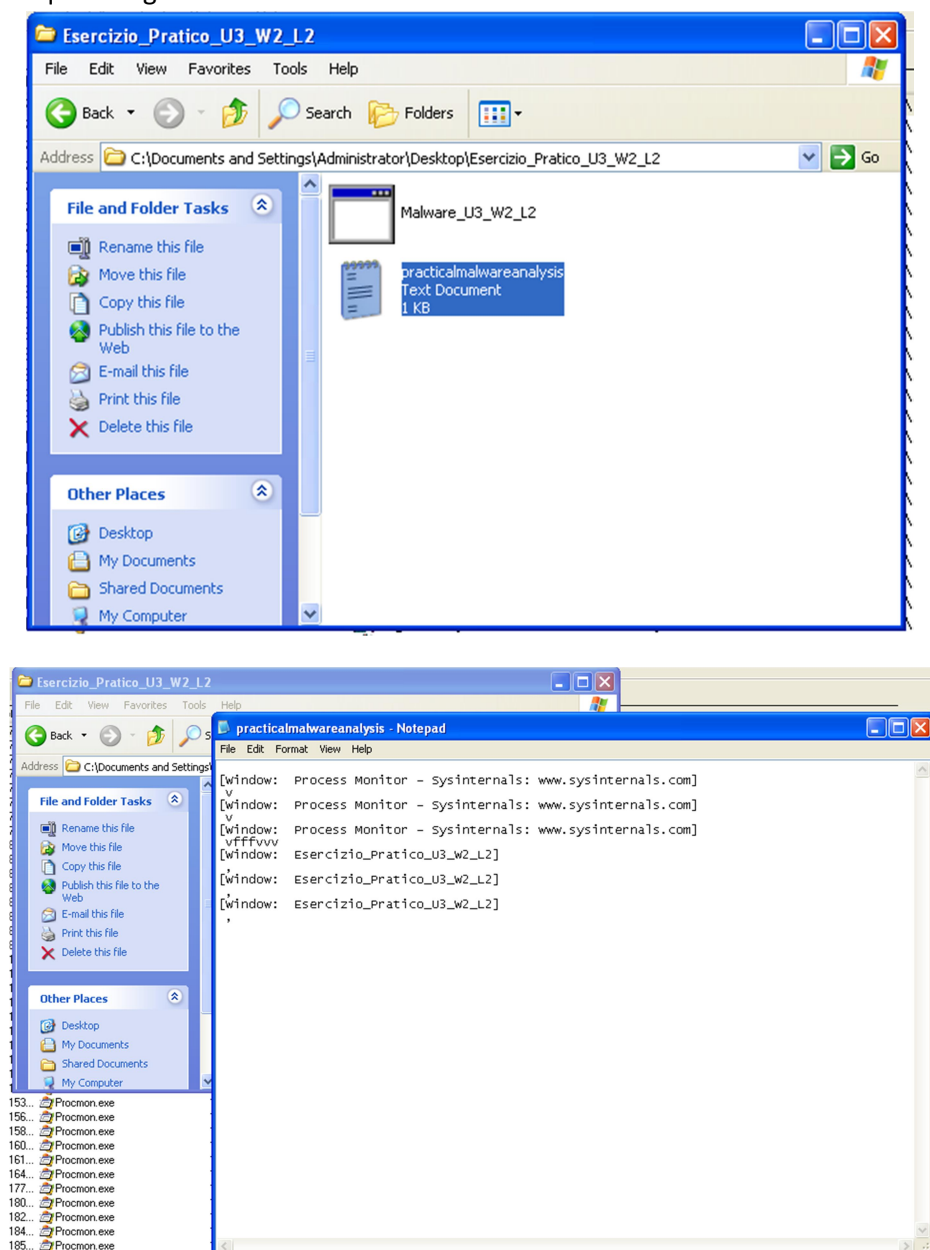


2:32:44.31538...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\	NO MORE FILES	
2:32:44.31543...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\	SUCCESS	
2:32:44.31548...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	
2:32:44.31561...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings	SUCCESS	
2:32:44.31565...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings	NO MORE FILES	
2:32:44.31568...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings	SUCCESS	
2:32:44.31571...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	
2:32:44.31776...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\ADMINISTRATOR	NO MORE FILES	
2:32:44.31720...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	
2:32:44.31825...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR\Desktop	SUCCESS	
2:32:44.31825...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\ADMINISTRATOR\Desktop	SUCCESS	
2:32:44.31821...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR\Desktop	NO MORE FILES	
2:32:44.31824...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR\Desktop	SUCCESS	
2:32:44.31873...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31883...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\ADMINISTRATOR\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31891...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\ADMINISTRATOR\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
2:32:44.31898...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\ADMINISTRATOR\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31911...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS	SUCCESS	
2:32:44.31917...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS	NO MORE FILES	
2:32:44.31925...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS	SUCCESS	
2:32:44.31932...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS	SUCCESS	
2:32:44.31975...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS\AppPatch	NO MORE FILES	
2:32:44.31987...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	
2:32:44.31989...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
2:32:44.32003...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	
2:32:44.32025...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\WINDOWS\System32	SUCCESS	
2:32:44.32033...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	SUCCESS	
2:32:44.32067...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	SUCCESS	
2:32:44.32091...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\WINDOWS\System32	NO MORE FILES	

Proviamo a filtrare il report di Procmon per visualizzare esclusivamente le attività correlate al processo denominato "Malware_U3_W2_L2.exe". Dando un'occhiata al report, notiamo alcune operazioni che catturano l'attenzione nella colonna "operation", come "Create File", "Read File" e "Close File", insieme ai rispettivi percorsi dei file coinvolti.

2:32:44.31864...	Malware_U3_W2_L2.exe	3180	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
2:32:44.31873...	Malware_U3_W2_L2.exe	3180	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:32:44.31883...	Malware_U3_W2_L2.exe	3180	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	

Da questa riga vediamo che è stato creato un file .txt nella cartella del malware



Esaminiamo il contenuto del file per osservare che contiene una registrazione di alcuni caratteri digitati sulla tastiera durante l'esecuzione del malware. Questo è un comportamento tipico dei keylogger.

Process Monitor Sysinternals: www.sysinternals.com				
File Edit Event Filter Tools Options Help				
Time of Day	Process Name	PID	Operation	Path
2:32:44.30886	Malware_U3_W2_L2.exe	3180	Process Start	
2:32:44.30886	Malware_U3_W2_L2.exe	3180	Thread Create	
2:32:44.30959	Malware_U3_W2_L2.exe	3180	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Phatico_U3_W2_L2\Malware_U3_W2_L2.exe
2:32:44.30972	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\url.dll
2:32:44.33752	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\kernel.dll
2:32:44.34936	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\apphelp.dll
2:32:44.35159	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\version.dll
2:32:44.36325	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\advapi32.dll
2:32:44.36348	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\user32.dll
2:32:44.36368	Malware_U3_W2_L2.exe	3180	Load Image	C:\WINDOWS\system32\user32.dll
2:32:44.37421	Malware_U3_W2_L2.exe	3180	Process Create	C:\WINDOWS\system32\svchost.exe
2:32:45.37431	Malware_U3_W2_L2.exe	3180	Thread Exit	
2:32:45.37443	Malware_U3_W2_L2.exe	3180	Process Exit	

Nel report, notiamo l'utilizzo di alcune funzioni intriganti come "Load Image", impiegata per caricare il malware e le relative librerie (.dll) necessarie per l'esecuzione. Successivamente, osserviamo l'attività di "Process Create", che sembra essere finalizzata alla creazione di un processo denominato "svchost.exe", comunemente associato ai processi legittimi di Windows. Questo suggerisce un comportamento tipico dei malware, che cercano di mascherare la loro presenza sotto il nome di processi validi al fine di evitare la rilevazione da parte di software antivirus o anti-malware.