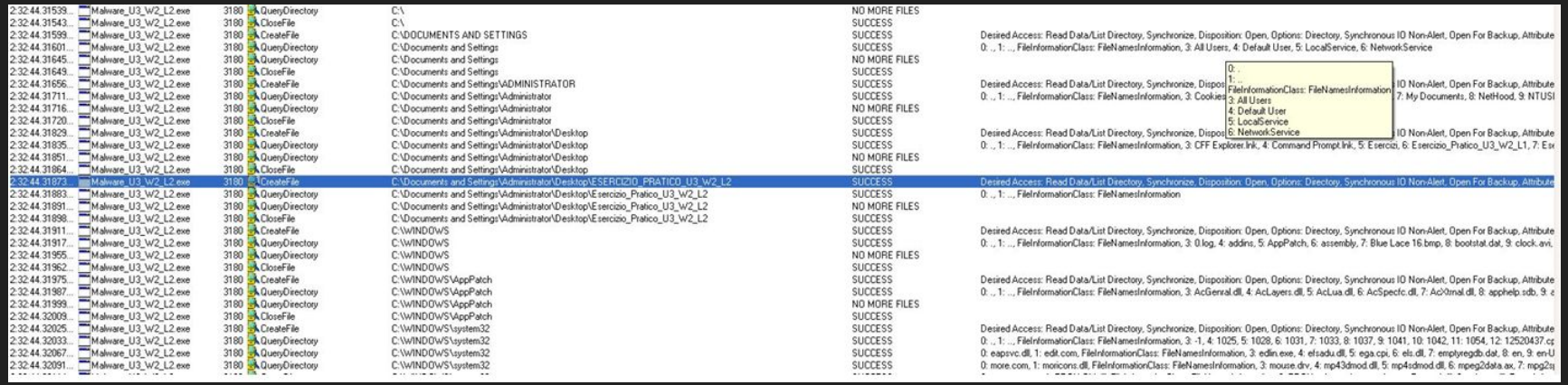
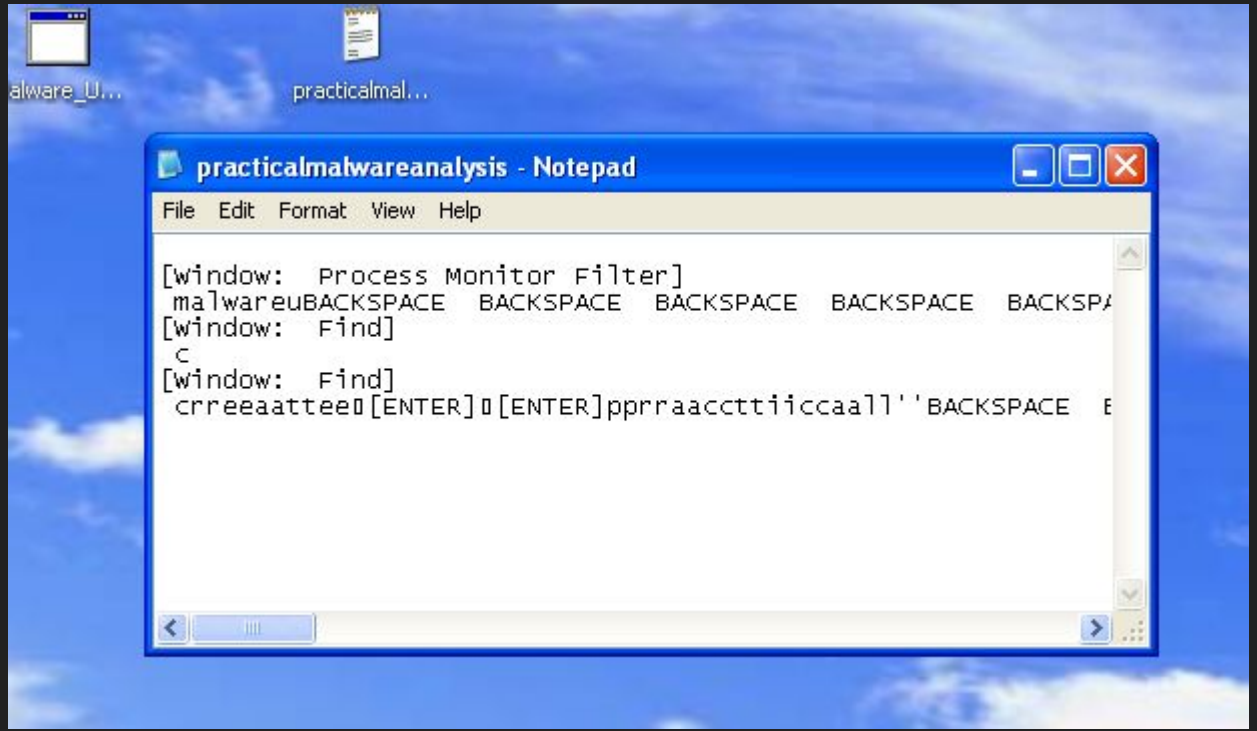
MALWARE ANALYSIS | DINAMICA BASICA

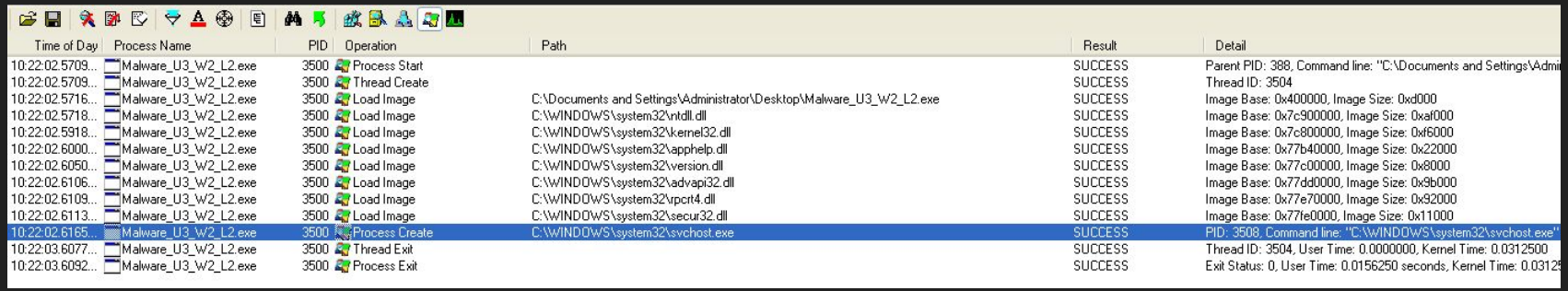
S10 - L2



Come possiamo vedere all'interno di procmod, dopo aver eseguito il file "Malware_U3_W2_L2", questo malware ha fatto parecchie cose alla nostra VM. Uno di questi è creare un file .txt nella directory in cui si trova il programma.

Infatti, possiamo vedere un nuovo file nella stessa directory del programma (Desktop). Aprendo il nuovo file denominato "practicalmalwarea nalysis" possiamo vedere che sembra essere un file con il contenuto di un keylogger, che verrà sicuramente inviato a un utente malintenzionato.





Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:22:02.5709...	Malware_U3_W2_L2.exe	3500	Process Start		SUCCESS	Parent PID: 388, Command line: "C:\Documents and Settings\Admi
10:22:02.5709...	Malware_U3_W2_L2.exe	3500	Thread Create		SUCCESS	Thread ID: 3504
10:22:02.5716...	Malware_U3_W2_L2.exe	3500	Load Image	C:\Documents and Settings\Administrator\Desktop\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
10:22:02.5718...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
10:22:02.5918...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
10:22:02.6000...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
10:22:02.6050...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
10:22:02.6106...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
10:22:02.6109...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
10:22:02.6113...	Malware_U3_W2_L2.exe	3500	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
10:22:02.6165...	Malware_U3_W2_L2.exe	3500	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 3508, Command line: "C:\WINDOWS\system32\svchost.exe"
10:22:03.6077...	Malware_U3_W2_L2.exe	3500	Thread Exit		SUCCESS	Thread ID: 3504, User Time: 0.0000000, Kernel Time: 0.0312500
10:22:03.6092...	Malware_U3_W2_L2.exe	3500	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0312

Andando nella parte superiore dell'interfaccia utente di Procmon, possiamo filtrare per "thread e processi". Una volta filtrato, troviamo azioni interessanti, come Load Image che serve per "caricare" l'esecuzione del malware e la libreria necessaria (.dll), e possiamo vedere "Process Create" che serve per creare un processo, in questo caso un processo chiamato svchost.exe, un processo Windows integrale. Questo ci dice che il malware sta cercando di nascondersi, prendendo il nome di un processo legittimo invece che di uno evidentemente allarmante.

Sembra che quando il programma viene avviato, richiama alle librerie necessarie di manera runtime, poi crea un servizio con nome falso, un servizio che potrebbe essere il keylogger visto previamente. Questo keylogger sicuramente andrá inviato ad un utente malintenzionato.