

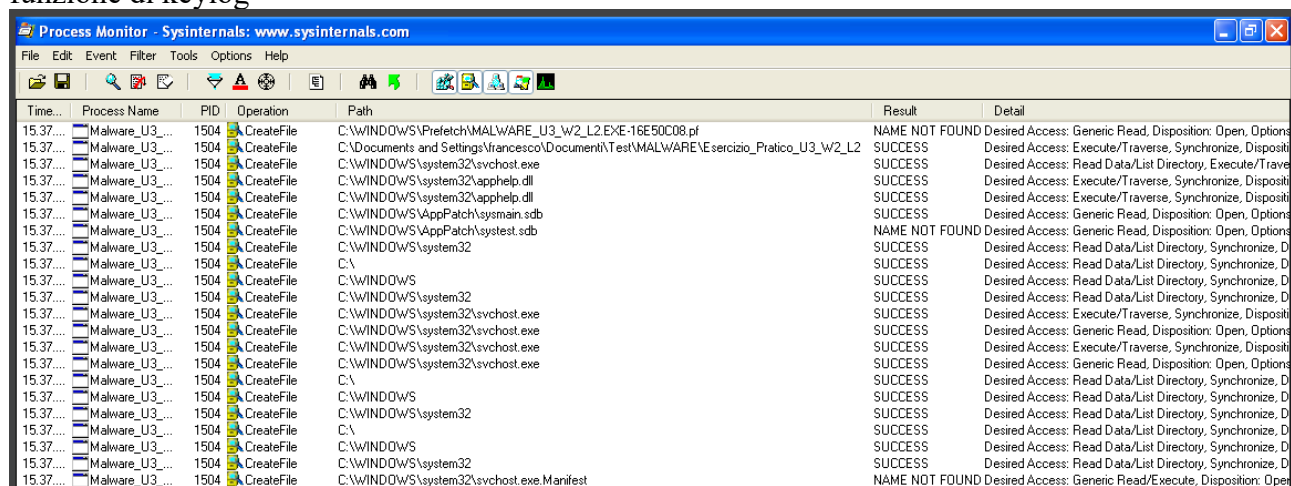
Analisi dinamica del virus

Siamo andati ad analizzare il virus in modo dinamico su un ambiente controllato.

Prima di iniziare l'analisi abbiamo disabilitato i controller usb di virtual box e impostato il mouse con connessione ps/2.

All'interno di windows 7 il malware non funziona correttamente, non riesce ad accedere ai comandi delle librerie richiesti e non riesce a scrivere il file del keylogger.

Se portato in windows xp, creando una rete privata tra xp e windows 7, senza lasciargli interazioni dirette con internet o con la macchina principale, possiamo notare la creazione del file e la corretta funzione di keylog



The screenshot shows the Process Monitor application window with the title bar 'Process Monitor - Sysinternals: www.sysinternals.com'. The interface includes a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar with various icons. The main area displays a table of file operations. The table has columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The operations listed are all 'CreateFile' actions performed by 'Malware_U3_W2_L2' with PID 1504. The paths include various system files and directories, such as 'C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-16E50C08.pf', 'C:\Documents and Settings\francesco\Documents\Test\MALWARE\Esercizio_Pratico_U3_W2_L2', 'C:\WINDOWS\system32\svchost.exe', 'C:\WINDOWS\system32\apphelp.dll', 'C:\WINDOWS\AppPatch\sysmain.sdb', 'C:\WINDOWS\system32\sysrest.sdb', 'C:\WINDOWS\system32', 'C:\', 'C:\WINDOWS', 'C:\WINDOWS\system32', 'C:\WINDOWS\system32\svchost.exe', and 'C:\WINDOWS\system32\svchost.exe.Manifest'. The results are mostly 'SUCCESS', with some 'NAME NOT FOUND' errors for specific paths. The details column provides additional information about the desired access and disposition for each operation.

Time...	Process Name	PID	Operation	Path	Result	Detail
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-16E50C08.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\Documents and Settings\francesco\Documents\Test\MALWARE\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Execute/Trave...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\sysrest.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositi...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, D...
15.37....	Malware_U3_...	1504	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND	Desired Access: Generic Read/Execute, Disposition: Open...



Malware_U3_W2_L2



practicalmalwareanalysis

Documento di testo

1 KB