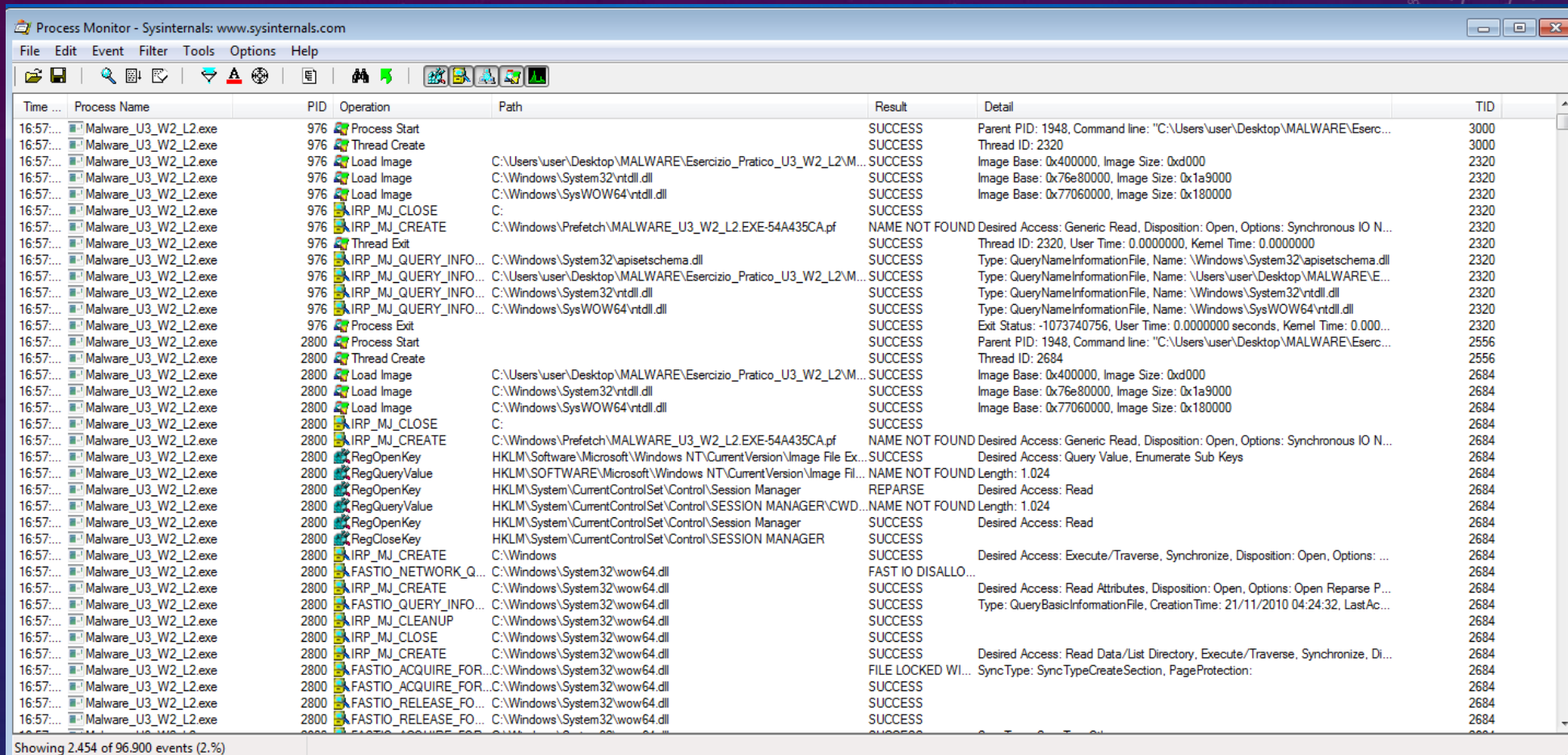


The background is a dark blue gradient with a subtle pattern of white dots. On the left side, there are several concentric circles and a large circular scale with degree markings from 140 to 260. Some of the circles have arrows indicating a clockwise direction. The text is positioned on the right side of the image.

MALWARE ANALYSIS

S10/L2

NELL'ESERCIZIO DI OGGI ANDIAMO AD ESEGUIRE UN ANALISI DINAMICA BASICA



Time ...	Process Name	PID	Operation	Path	Result	Detail	TID
16:57:...	Malware_U3_W2_L2.exe	976	Process Start		SUCCESS	Parent PID: 1948, Command line: "C:\Users\user\Desktop\MALWARE\Eserc...	3000
16:57:...	Malware_U3_W2_L2.exe	976	Thread Create		SUCCESS	Thread ID: 2320	3000
16:57:...	Malware_U3_W2_L2.exe	976	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000	2320
16:57:...	Malware_U3_W2_L2.exe	976	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x76e80000, Image Size: 0x1a9000	2320
16:57:...	Malware_U3_W2_L2.exe	976	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77060000, Image Size: 0x180000	2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_CLOSE	C:	SUCCESS		2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_CREATE	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO N...	2320
16:57:...	Malware_U3_W2_L2.exe	976	Thread Exit		SUCCESS	Thread ID: 2320, User Time: 0.0000000, Kernel Time: 0.0000000	2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_QUERY_INFO...	C:\Windows\System32\apisetschema.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\System32\apisetschema.dll	2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_QUERY_INFO...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	Type: QueryNameInformationFile, Name: \Users\user\Desktop\MALWARE\E...	2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_QUERY_INFO...	C:\Windows\System32\ntdll.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\System32\ntdll.dll	2320
16:57:...	Malware_U3_W2_L2.exe	976	IRP_MJ_QUERY_INFO...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\SysWOW64\ntdll.dll	2320
16:57:...	Malware_U3_W2_L2.exe	976	Process Exit		SUCCESS	Exit Status: -1073740756, User Time: 0.0000000 seconds, Kernel Time: 0.000...	2320
16:57:...	Malware_U3_W2_L2.exe	2800	Process Start		SUCCESS	Parent PID: 1948, Command line: "C:\Users\user\Desktop\MALWARE\Eserc...	2556
16:57:...	Malware_U3_W2_L2.exe	2800	Thread Create		SUCCESS	Thread ID: 2684	2556
16:57:...	Malware_U3_W2_L2.exe	2800	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\M...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000	2684
16:57:...	Malware_U3_W2_L2.exe	2800	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x76e80000, Image Size: 0x1a9000	2684
16:57:...	Malware_U3_W2_L2.exe	2800	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77060000, Image Size: 0x180000	2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CLOSE	C:	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CREATE	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO N...	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Ex...	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image Fil...	NAME NOT FOUND	Length: 1.024	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWD...	NAME NOT FOUND	Length: 1.024	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Read	2684
16:57:...	Malware_U3_W2_L2.exe	2800	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CREATE	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: ...	2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_NETWORK_Q...	C:\Windows\System32\wow64.dll	FAST IO DISALLO...		2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CREATE	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P...	2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_QUERY_INFO...	C:\Windows\System32\wow64.dll	SUCCESS	Type: QueryBasicInformationFile, Creation Time: 21/11/2010 04:24:32, LastAc...	2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CLEANUP	C:\Windows\System32\wow64.dll	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CLOSE	C:\Windows\System32\wow64.dll	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	IRP_MJ_CREATE	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Di...	2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_ACQUIRE_FOR...	C:\Windows\System32\wow64.dll	FILE LOCKED Wl...	Sync Type: Sync TypeCreateSection, PageProtection:	2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_ACQUIRE_FOR...	C:\Windows\System32\wow64.dll	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_RELEASE_FO...	C:\Windows\System32\wow64.dll	SUCCESS		2684
16:57:...	Malware_U3_W2_L2.exe	2800	FASTIO_RELEASE_FO...	C:\Windows\System32\wow64.dll	SUCCESS		2684

Showing 2,454 of 96,900 events (2.%)

Utilizziamo il programma «Process Monitor» per identificare eventuali azioni del malware eseguiamo il file «Esercizio_Pratico_U3_W2_L2» ed effettuiamo una cattura impostando il nome «Esercizio_Pratico_U3_W2_L2.exe» come filtro per selezionare solo i processi che ci interessano.

❖ SELEZIONIAMO SOLO LE AZIONI RILEVATE SUL FILE SYSTEM DEL MALWARE

Una delle righe che troviamo è la creazione di un file andiamo a vedere che tipo di file è...

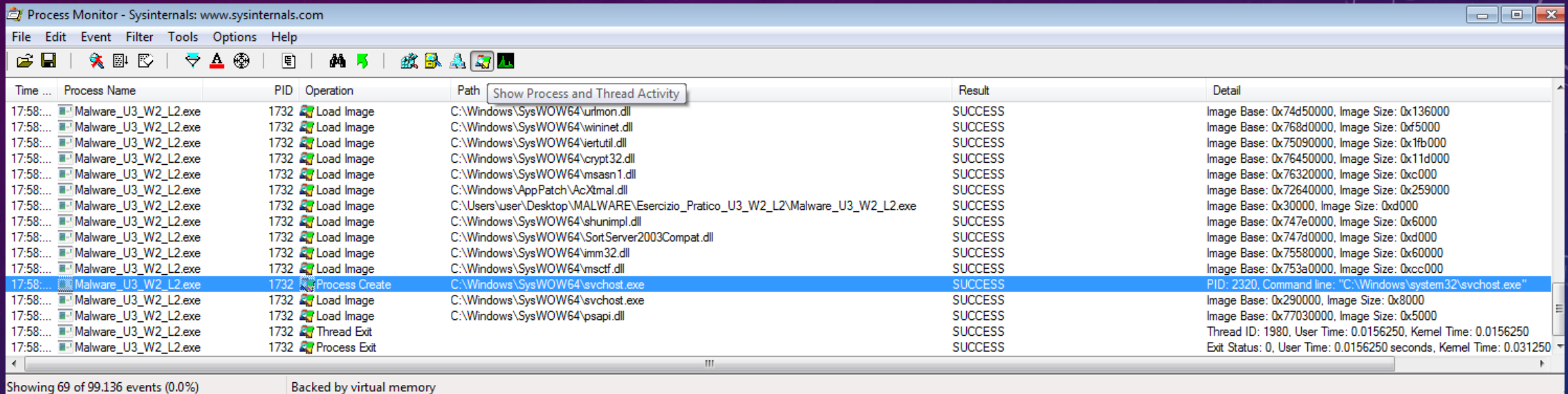
Time ...	Process Name	PID	Operation	Show File System Activity	Result	Detail
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_CLOSE	C:	SUCCESS	
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_CREATE	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Optic
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_QUERY_INFO...	C:\Windows\System32\apisetschema.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\Sys
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_QUERY_INFO...	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Type: QueryNameInformationFile, Name: \Users\user\D
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_QUERY_INFO...	C:\Windows\System32\ntdll.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\Sys
17:26:...	Malware_U3_W2_L2.exe	3064	IRP_MJ_QUERY_INFO...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Type: QueryNameInformationFile, Name: \Windows\Sys
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CLOSE	C:	SUCCESS	
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CREATE	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-54A435CA.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Optic
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CREATE	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispo
17:26:...	Malware_U3_W2_L2.exe	1856	FASTIO_NETWORK_Q...	C:\Windows\System32\wow64.dll	FAST IO DISALLOWED	
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CREATE	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Op
17:26:...	Malware_U3_W2_L2.exe	1856	FASTIO_QUERY_INFO...	C:\Windows\System32\wow64.dll	SUCCESS	Type: QueryBasicInformationFile, Creation Time: 21/11/
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CLEANUP	C:\Windows\System32\wow64.dll	SUCCESS	
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CLOSE	C:\Windows\System32\wow64.dll	SUCCESS	
17:26:...	Malware_U3_W2_L2.exe	1856	IRP_MJ_CREATE	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Tra
17:26:...	Malware_U3_W2_L2.exe	1856	FASTIO_ACQUIRE_FOR...	C:\Windows\System32\wow64.dll	FILE LOCKED WITH ONLY READERS	Sync Type: Sync TypeCreateSection, PageProtection:
17:26:...	Malware_U3_W2_L2.exe	1856	FASTIO_ACQUIRE_FOR...	C:\Windows\System32\wow64.dll	SUCCESS	
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	

Apriamo la cartella del Malware vediamo che è stata creato un file di tipo .txt «practicalmalwareanalysis»

Il contenuto del file acquisisce alcuni caratteri della tastiera utilizzati durante l'esecuzione del malware, ed è un comportamento solito di malware «Keylogger»



SELEZIONIAMO SOLO LE AZIONI RILEVATE SU PROCESSI E THREAD DEL MALWARE



Time ...	Process Name	PID	Operation	Path	Result	Detail
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x74d50000, Image Size: 0x136000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x768d0000, Image Size: 0xf5000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\iertutil.dll	SUCCESS	Image Base: 0x75090000, Image Size: 0x1fb000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x76450000, Image Size: 0x11d000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Image Base: 0x76320000, Image Size: 0xc000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\AppPatch\AcXtma1.dll	SUCCESS	Image Base: 0x72640000, Image Size: 0x259000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x30000, Image Size: 0xd000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\shnimpl.dll	SUCCESS	Image Base: 0x747e0000, Image Size: 0x6000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\Sort.Server2003Compat.dll	SUCCESS	Image Base: 0x747d0000, Image Size: 0xd000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x75580000, Image Size: 0x60000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x753a0000, Image Size: 0xcc000
17:58:...	Malware_U3_W2_L2.exe	1732	Process Create	C:\Windows\SysWOW64\svchost.exe	SUCCESS	PID: 2320, Command line: "C:\Windows\system32\svchost.exe"
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\svchost.exe	SUCCESS	Image Base: 0x290000, Image Size: 0x8000
17:58:...	Malware_U3_W2_L2.exe	1732	Load Image	C:\Windows\SysWOW64\psapi.dll	SUCCESS	Image Base: 0x77030000, Image Size: 0x5000
17:58:...	Malware_U3_W2_L2.exe	1732	Thread Exit		SUCCESS	Thread ID: 1980, User Time: 0.0156250, Kernel Time: 0.0156250
17:58:...	Malware_U3_W2_L2.exe	1732	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.031250

Showing 69 of 99.136 events (0.0%) Backed by virtual memory

Facciamo un'altra cattura con Process Monitor, filtrando solo gli eventi che riguardano processi e thread. Vediamo varie funzioni tra cui «Load Image» che carica le librerie .dll per l'esecuzione del malware e «Process Create» che appunto serve per creare un processo. In questo caso viene creato un processo con il nome «svchost.exe» che è effettivamente un processo valido di Windows, ma che in questo caso viene usato per nascondere il malware dietro un nome valido e in questo modo, confondere gli antivirus del nostro sistema.

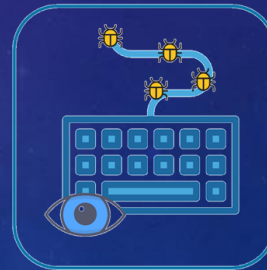
CONSIDERAZIONI FINALI DOPO L'ANALISI

Abbiamo visto che questo malware cerca di mascherarsi creando il processo «svchost.exe», dopo di che fa partire un keylogger che salva i caratteri che vengono digitati in un file di tipo .txt creato nella cartella dove si trova il malware eseguibile

«MALWARE_U3_W2_L2»



«svchost.exe»



«Keylogger»