

a. Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon):

Come prima cosa, prima di avviare il Malware, avvio Process Monitor, che inizierà a monitorare i processi:

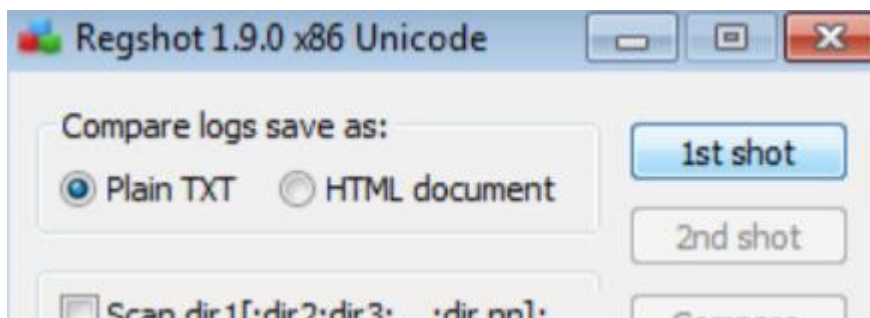
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day Process Name PID Operation Path Result Detail

13:07:20.3093...	Explorer.EXE	1156	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 427.520. Length: 13.824. I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority...
13:07:20.3093...	SearchIndexer...	1544	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 359.936. Length: 4.096. I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority...
13:07:20.3095...	Idle	0	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 197.6718750 seconds, Private Bytes: 0. Working Set: 24...
13:07:20.3095...	csrss.exe	248	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 360.448, Working Set...
13:07:20.3095...	csrss.exe	324	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.1250000 seconds, Private Bytes: 1.748.992, Working S...
13:07:20.3097...	wininit.exe	372	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 1.314.816, Working S...
13:07:20.3097...	csrss.exe	380	Process Profiling		SUCCESS	User Time: 0.0781250 seconds, Kernel Time: 0.1562500 seconds, Private Bytes: 1.798.144, Working S...
13:07:20.3097...	winlogon.exe	408	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 2.686.976, Working S...
13:07:20.3097...	services.exe	464	Process Profiling		SUCCESS	User Time: 0.0625000 seconds, Kernel Time: 0.2343750 seconds, Private Bytes: 4.440.064, Working S...
13:07:20.3097...	lsass.exe	480	Process Profiling		SUCCESS	User Time: 0.1093750 seconds, Kernel Time: 0.0781250 seconds, Private Bytes: 2.879.488, Working S...
13:07:20.3097...	lsim.exe	488	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 2.207.744, Working S...
13:07:20.3097...	svchost.exe	592	Process Profiling		SUCCESS	User Time: 0.0468750 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 3.293.184, Working S...
13:07:20.3097...	VBoxService.exe	656	Process Profiling		SUCCESS	User Time: 0.000000 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 1.994.752, Working S...
13:07:20.3097...	svchost.exe	716	Process Profiling		SUCCESS	User Time: 0.0468750 seconds, Kernel Time: 0.0312500 seconds, Private Bytes: 2.846.720, Working S...
13:07:20.3097...	svchost.exe	808	Process Profiling		SUCCESS	User Time: 0.1093750 seconds, Kernel Time: 0.1250000 seconds, Private Bytes: 16.277.504, Working...
13:07:20.3097...	svchost.exe	852	Process Profiling		SUCCESS	User Time: 0.0000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 4.247.552, Working S...
13:07:20.3097...	svchost.exe	880	Process Profiling		SUCCESS	User Time: 0.1093750 seconds, Kernel Time: 0.1250000 seconds, Private Bytes: 23.531.520, Working...
13:07:20.3097...	AUDIODG EXE	964	Process Profiling		SUCCESS	User Time: 0.0468750 seconds, Kernel Time: 0.1093750 seconds, Private Bytes: 15.921.152, Working...
13:07:20.3098...	svchost.exe	264	Process Profiling		SUCCESS	User Time: 0.0156250 seconds, Kernel Time: 0.0312500 seconds, Private Bytes: 3.969.024, Working S...
13:07:20.3098...	svchost.exe	556	Process Profiling		SUCCESS	User Time: 0.0312500 seconds, Kernel Time: 0.0781250 seconds, Private Bytes: 9.506.816, Working S...

Poi faccio un'istantanea del registro con Regshot (sempre prima di avviare il malware):

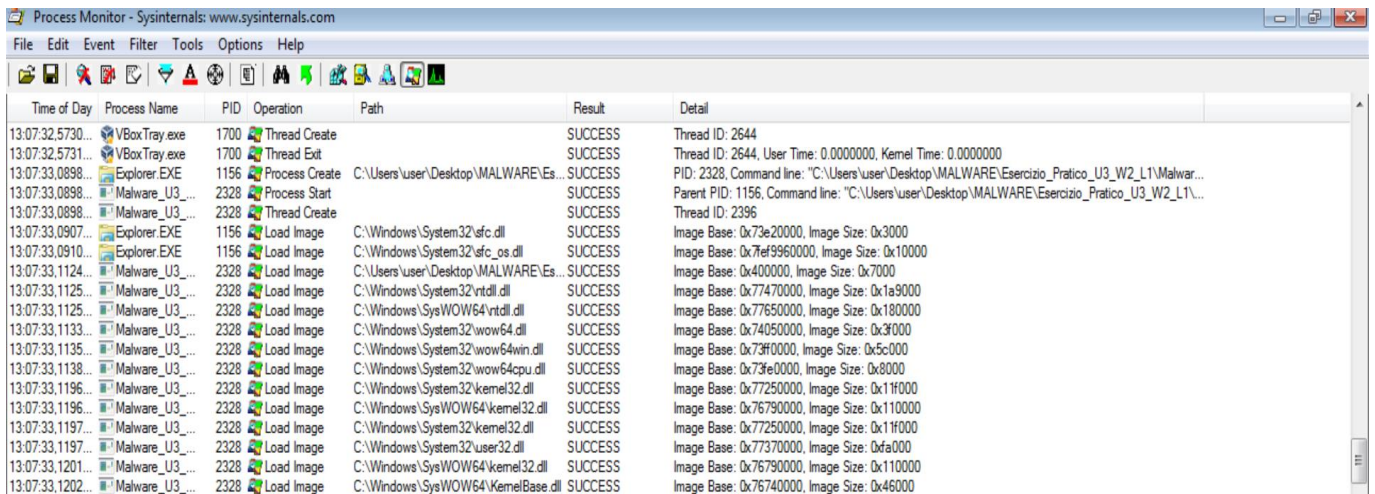


Adesso avvio il malware, aspetto qualche secondo, rivado su Process Monitor e stoppo la cattura.

Vado a vedere le azioni del malware sul file system:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
13:07:33.1737...	Malware_U3_...	2328	CloseFile	C:\Windows\SysWOW64\vm32.dll	SUCCESS	
13:07:33.1737...	Malware_U3_...	2328	CreateFile	C:\Windows\SysWOW64\vm32.dll	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options:...
13:07:33.1738...	Malware_U3_...	2328	CreateFileMapping	C:\Windows\SysWOW64\vm32.dll	FILE LOCKED WI...	Sync Type: SyncTypeCreateSection, PageProtection:...
13:07:33.1738...	Malware_U3_...	2328	CreateFileMapping	C:\Windows\SysWOW64\vm32.dll	SUCCESS	Sync Type: SyncTypeOther
13:07:33.1739...	Malware_U3_...	2328	CloseFile	C:\Windows\SysWOW64\vm32.dll	SUCCESS	
13:07:33.1753...	Explorer.EXE	1156	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Name: \Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
13:07:33.1754...	Explorer.EXE	1156	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Shar...
13:07:33.1754...	Explorer.EXE	1156	QueryBasicInfo...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	CreationTime: 19/01/2011 11:10:42, LastAccessTime: 19/01/2011 11:10:42, LastWriteTime: 17/01/2...
13:07:33.1754...	Explorer.EXE	1156	CloseFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	
13:07:33.1755...	Explorer.EXE	1156	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchro...
13:07:33.1755...	Explorer.EXE	1156	QueryDirectory	C:\Users	SUCCESS	Filter: Users, 1: Users
13:07:33.1755...	Explorer.EXE	1156	CloseFile	C:\	SUCCESS	
13:07:33.1755...	Explorer.EXE	1156	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchro...
13:07:33.1755...	Explorer.EXE	1156	QueryDirectory	C:\Users\user	SUCCESS	Filter: user, 1: user
13:07:33.1755...	Explorer.EXE	1156	CloseFile	C:\Users	SUCCESS	
13:07:33.1756...	Explorer.EXE	1156	CreateFile	C:\Users\user	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchro...
13:07:33.1756...	Explorer.EXE	1156	QueryDirectory	C:\Users\user\Desktop	SUCCESS	Filter: Desktop, 1: Desktop
13:07:33.1756...	Explorer.EXE	1156	CloseFile	C:\Users\user	SUCCESS	
13:07:33.1756...	Explorer.EXE	1156	CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchro...
13:07:33.1756...	Explorer.EXE	1156	QueryDirectory	C:\Users\user\Desktop\MALWARE	SUCCESS	Filter: MALWARE, 1: MALWARE
13:07:33.1757...	Explorer.EXE	1156	CloseFile	C:\Users\user\Desktop	SUCCESS	
13:07:33.1757...	Explorer.EXE	1156	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Name: \Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
13:07:33.1758...	Explorer.EXE	1156	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, Shar...
13:07:33.1758...	Explorer.EXE	1156	QueryBasicInfo...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	CreationTime: 19/01/2011 11:10:42, LastAccessTime: 19/01/2011 11:10:42, LastWriteTime: 17/01/2...

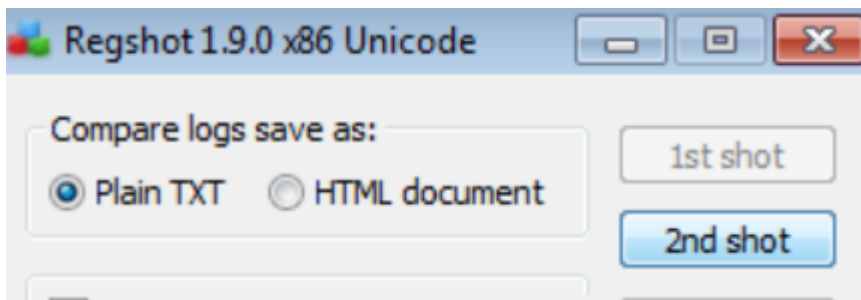
b. Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor:



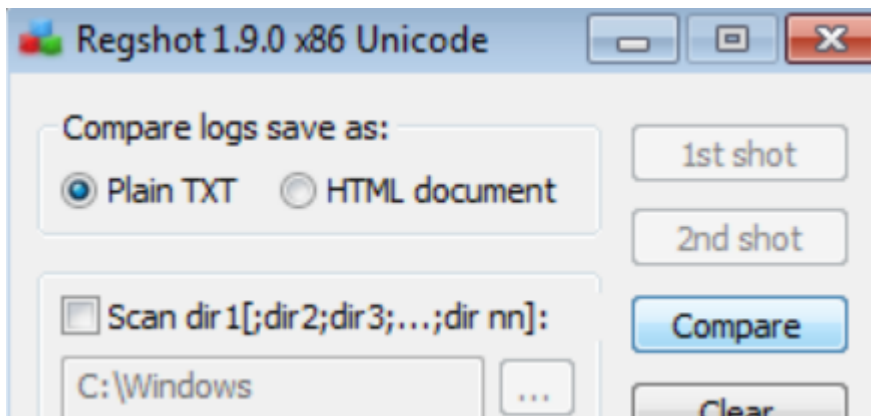
Time of Day	Process Name	PID	Operation	Path	Result	Detail
13:07:32.5730...	VBoxTray.exe	1700	Thread Create		SUCCESS	Thread ID: 2644
13:07:32.5731...	VBoxTray.exe	1700	Thread Exit		SUCCESS	Thread ID: 2644, User Time: 0.0000000, Kernel Time: 0.0000000
13:07:33.0898...	Explorer.EXE	1156	Process Create	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malwar...	SUCCESS	PID: 2328, Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malwar...
13:07:33.0898...	Malware_U3_...	2328	Process Start		SUCCESS	Parent PID: 1156, Command line: "C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\...
13:07:33.0898...	Malware_U3_...	2328	Thread Create		SUCCESS	Thread ID: 2396
13:07:33.0907...	Explorer.EXE	1156	Load Image	C:\Windows\System32\sfcdll.dll	SUCCESS	Image Base: 0x73e20000, Image Size: 0x3000
13:07:33.0910...	Explorer.EXE	1156	Load Image	C:\Windows\System32\sfcdll.dll	SUCCESS	Image Base: 0x73e20000, Image Size: 0x3000
13:07:33.1124...	Malware_U3_...	2328	Load Image	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malwar...	SUCCESS	Image Base: 0x400000, Image Size: 0x7000
13:07:33.1125...	Malware_U3_...	2328	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77470000, Image Size: 0x1a9000
13:07:33.1125...	Malware_U3_...	2328	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77650000, Image Size: 0x180000
13:07:33.1133...	Malware_U3_...	2328	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x74050000, Image Size: 0x3f000
13:07:33.1135...	Malware_U3_...	2328	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73f00000, Image Size: 0x5c000
13:07:33.1138...	Malware_U3_...	2328	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x73f00000, Image Size: 0x5c000
13:07:33.1138...	Malware_U3_...	2328	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77250000, Image Size: 0x1f000
13:07:33.1196...	Malware_U3_...	2328	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76790000, Image Size: 0x1f0000
13:07:33.1197...	Malware_U3_...	2328	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x77250000, Image Size: 0x1f000
13:07:33.1197...	Malware_U3_...	2328	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x77370000, Image Size: 0xfa000
13:07:33.1201...	Malware_U3_...	2328	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76790000, Image Size: 0x1f0000
13:07:33.1202...	Malware_U3_...	2328	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76790000, Image Size: 0x1f0000

c. Modifiche del registro dopo il malware(le differenze):

Successivamente, acquisisco una seconda istantanea del registro con Regshot:



E vado a comparare le due istantanee (quella prima del malware e quella dopo):



[illegible]

Sono state tolti 6 valori, ne sono stati aggiunti 28.

Ci sono stati in totale 54 cambiamenti rispetto alla prima istantanea.