

Analizzando le eventuali azioni del malware sul file system possiamo vedere come il malware abbia fatto varie azioni come creare file e fare query directory per leggere gli attributi (come dimensione, data di creazione, data di modifica) di un file o di una cartella ed eseguire operazioni su un gruppo di file, ad esempio copiare, spostare o eliminare file specifici in una directory, per quanto riguarda il “create File” possiamo notare che va a farlo su path che portano alla modifica del sistema di Win come Windows Common Control, shell32 ecc.

10:02...	Malware_U3_...	1800	SetEndOfFileIn...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 8,192
10:02...	Malware_U3_...	1800	SetEndOfFileIn...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 8,192
10:02...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Desired Access: G...
10:02...	Malware_U3_...	1800	CreateFileMap...	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTy...
10:02...	Malware_U3_...	1800	QueryStandardI...	C:\WINDOWS\system32\shell32.dll	SUCCESS	AllocationSize: 8.4...
10:02...	Malware_U3_...	1800	CreateFileMap...	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTy...
10:02...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll.12...	NAME NOT FOUND	Desired Access: G...
10:02...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll.12...	NAME NOT FOUND	Desired Access: G...

Time...	Process Name	PID	Operation	Path	Result	Detail
9:02:3...	Malware_U3_...	1920	CreateFile	C:\Documents and Settings\Davide\De...	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\Documents and Settings\Davide\De...	SUCCESS	0: ..; 1: ..., FileInfor...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\Documents and Settings\Davide\De...	NO MORE FILES	
9:02:3...	Malware_U3_...	1920	CloseFile	C:\Documents and Settings\Davide\De...	SUCCESS	
9:02:33.6608785 AM	Malware_U3_...	1920	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS	SUCCESS	0: ..; 1: ..., FileInfor...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS	NO MORE FILES	
9:02:3...	Malware_U3_...	1920	CloseFile	C:\WINDOWS	SUCCESS	
9:02:3...	Malware_U3_...	1920	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ..; 1: ..., FileInfor...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
9:02:3...	Malware_U3_...	1920	CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
9:02:3...	Malware_U3_...	1920	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ..; 1: ..., FileInfor...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: en-US; 1: encap...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: mlogmgr.dll; 1: ...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: rassapi.dll; 1: ras...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: winsta.dll; 1: win...
9:02:3...	Malware_U3_...	1920	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	
9:02:3...	Malware_U3_...	1920	CloseFile	C:\WINDOWS\system32	SUCCESS	
9:02:3...	Malware_U3_...	1920	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	CreateFileMap...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
9:02:3...	Malware_U3_...	1920	QueryStandardI...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	AllocationSize: 708...
9:02:3...	Malware_U3_...	1920	CreateFileMap...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
9:02:3...	Malware_U3_...	1920	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	CreateFileMap...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
9:02:3...	Malware_U3_...	1920	QueryStandardI...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	AllocationSize: 991...
9:02:3...	Malware_U3_...	1920	CreateFileMap...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
9:02:3...	Malware_U3_...	1920	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: R...
9:02:3...	Malware_U3_...	1920	CreateFileMap...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: SyncTy...

Showing 1,410 of 32,720 events (4.3%) Backed by virtual memory

Le azioni del malware su processi e thread che possiamo notare utilizzando il process monitor sono l’ avvio di processi: caricamento di immagini (load image) e la creazione di thread.

Time...	Process Name	PID	Operation	Path	Result	Detail
t:47:1...	Explorer.EXE	1408	Thread Exit		SUCCESS	Thread ID: 1656, ...
t:47:1...	Explorer.EXE	1408	Thread Create		SUCCESS	Thread ID: 268
t:47:1...	svchost.exe	988	Thread Exit		SUCCESS	Thread ID: 1732, ...
t:47:1...	svchost.exe	988	Thread Create		SUCCESS	Thread ID: 1164
t:47:1...	svchost.exe	988	Thread Create		SUCCESS	Thread ID: 2000
t:47:1...	Explorer.EXE	1408	Process Create	C:\Documents and Settings\Davide\De...	SUCCESS	PID: 1140, Comma...
t:47:1...	Malware_U3_...	1140	Process Start		SUCCESS	Parent PID: 1408, ...
t:47:1...	Malware_U3_...	1140	Thread Create		SUCCESS	Thread ID: 1488
t:47:1...	Malware_U3_...	1140	Load Image	C:\Documents and Settings\Davide\De...	SUCCESS	Image Base: 0x400...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
t:47:1...	svchost.exe	1044	Thread Create		SUCCESS	Thread ID: 780
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
t:47:1...	csrss.exe	580	Thread Create		SUCCESS	Thread ID: 196
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\vpport4.dll	SUCCESS	Image Base: 0x77e...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\wininet.dll	SUCCESS	Image Base: 0x771...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\crypt32.dll	SUCCESS	Image Base: 0x77a...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\msasn1.dll	SUCCESS	Image Base: 0x77b...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Image Base: 0x771...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x774...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f...
t:47:1...	Malware_U3_...	1140	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft...	SUCCESS	Image Base: 0x773...
t:47:2...	Explorer.EXE	1408	Thread Exit		SUCCESS	Thread ID: 1068, ...
t:47:2...	svchost.exe	988	Thread Exit		SUCCESS	Thread ID: 2000, ...
t:47:2...	svchost.exe	988	Thread Exit		SUCCESS	Thread ID: 1164, ...
t:47:2...	Malware_U3_...	1140	Thread Create		SUCCESS	Thread ID: 1328

Showing 282 of 71,797 events (0.39%) Backed by virtual memory