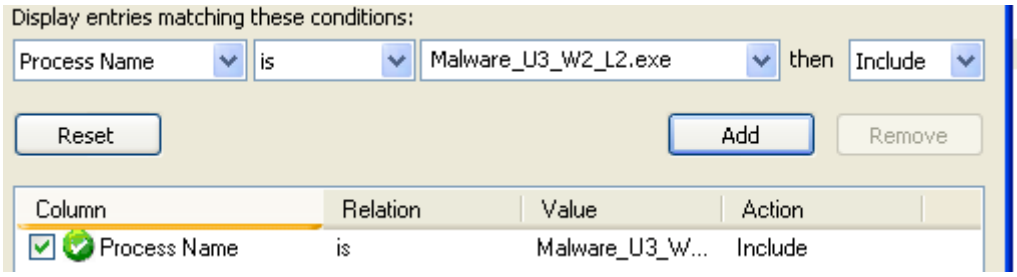
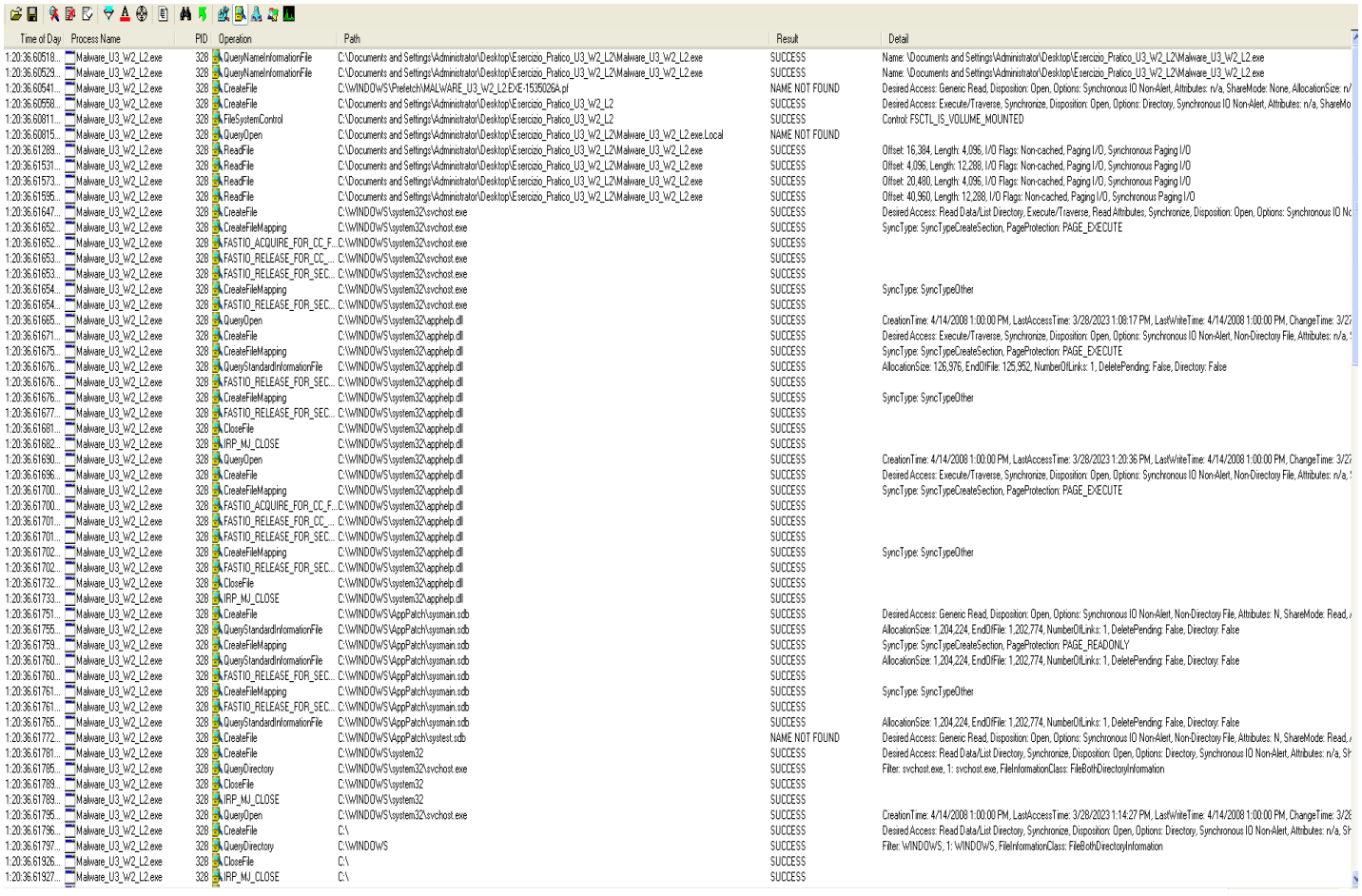
# ANALISI MALWARE

Creiamo un filtro per visualizzare una volta avviata la scansione solo il nostro malware inserendo come process name il nome aggiungendo l'estensione exe e mettendo 'include', cosi' facendo visualizzeremo solo quello che combina il malware




Filtrando i processi visualizziamo le attività relative al file system.



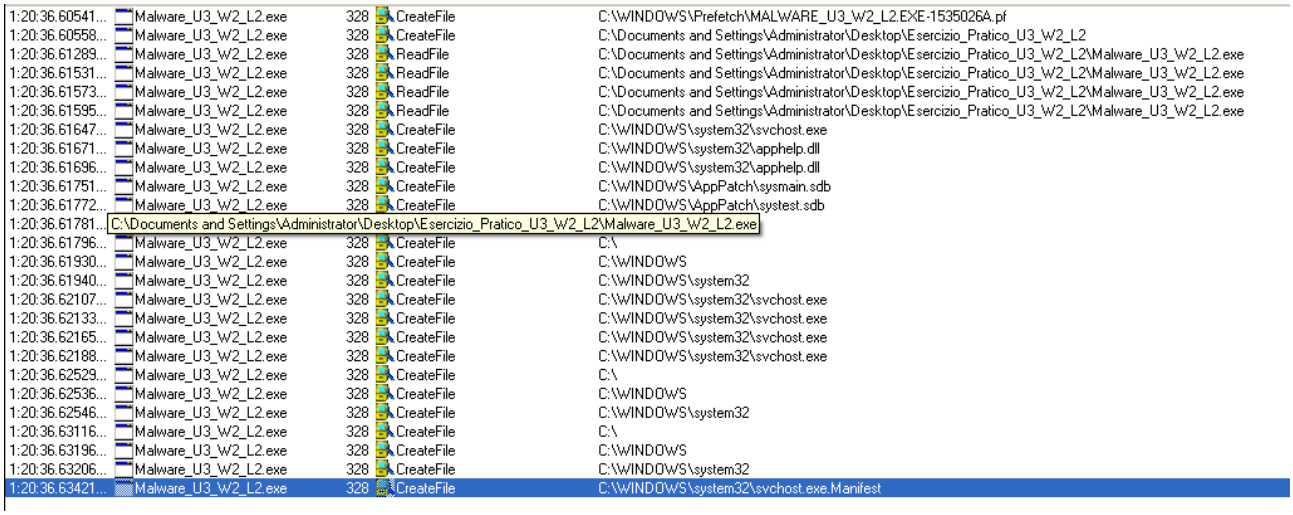
# ANALISI MALWARE

Qui inseriamo un altro filtro per visualizzare solo le azioni del malware su processi e thread

| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 1:20:36.60464... | Malware_U3_W2_L2.exe | 328 | Process Start | | SUCCESS | Parent PID: 1856, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.e |
| 1:20:36.60464... | Malware_U3_W2_L2.exe | 328 | Thread Create | | SUCCESS | Thread ID: 888 |
| 1:20:36.6052414 PM | Malware_U3_W2_L2.exe | 328 | Load Image | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe | SUCCESS | Image Base: 0x400000, Image Size: 0xd000 |
| 1:20:36.60528... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Image Base: 0x7c900000, Image Size: 0xaf000 |
| 1:20:36.60822... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Image Base: 0x7c800000, Image Size: 0xf6000 |
| 1:20:36.61739... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Image Base: 0x77b40000, Image Size: 0x22000 |
| 1:20:36.62090... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\version.dll | SUCCESS | Image Base: 0x77c00000, Image Size: 0x8000 |
| 1:20:36.62967... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Image Base: 0x77dd0000, Image Size: 0x9b000 |
| 1:20:36.62974... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS | Image Base: 0x77e70000, Image Size: 0x92000 |
| 1:20:36.62982... | Malware_U3_W2_L2.exe | 328 | Load Image | C:\WINDOWS\system32\secur32.dll | SUCCESS | Image Base: 0x77fe0000, Image Size: 0x11000 |
| 1:20:36.63428... | Malware_U3_W2_L2.exe | 328 | Process Create | C:\WINDOWS\system32\svchost.exe | SUCCESS | PID: 428, Command line: "C:\WINDOWS\system32\svchost.exe" |
| 1:20:37.52794... | Malware_U3_W2_L2.exe | 328 | Process Profiling | | SUCCESS | User Time: 0.0100144 seconds, Kernel Time: 0.0100144 seconds, Private Bytes: 274,432, Working Set: 983,040 |
| 1:20:37.64032... | Malware_U3_W2_L2.exe | 328 | Thread Exit | | SUCCESS | Thread ID: 888, User Time: 0.0000000, Kernel Time: 0.0100144 |
| 1:20:37.64045... | Malware_U3_W2_L2.exe | 328 | Process Exit | | SUCCESS | Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time: 0.0100144 seconds, Private Bytes: 266,240, Peak Private Bytes: 299,008, Worki |

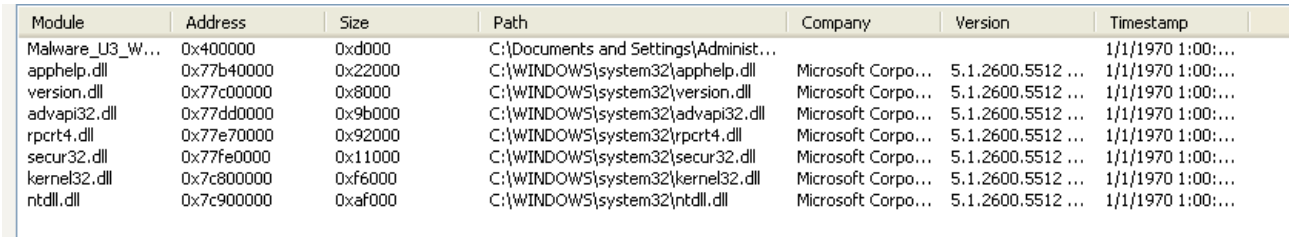
Possiamo anche visualizzare per quanto tempo resta attiva l'exe sul nostro pc


Questo malware importa librerie, crea e legge file



| | | | | |
|---|---|---|---|---|
| 1:20:36.60541... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf |
| 1:20:36.60558... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 |
| 1:20:36.61289... | Malware_U3_W2_L2.exe | 328 | ReadFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe |
| 1:20:36.61531... | Malware_U3_W2_L2.exe | 328 | ReadFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe |
| 1:20:36.61573... | Malware_U3_W2_L2.exe | 328 | ReadFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe |
| 1:20:36.61595... | Malware_U3_W2_L2.exe | 328 | ReadFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe |
| 1:20:36.61647... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe |
| 1:20:36.61671... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\apphelp.dll |
| 1:20:36.61696... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\apphelp.dll |
| 1:20:36.61751... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\AppPatch\sysmain.sdb |
| 1:20:36.61772... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\AppPatch\systest.sdb |
| 1:20:36.61781... | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe | | | |
| 1:20:36.61796... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\ |
| 1:20:36.61930... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS |
| 1:20:36.61940... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32 |
| 1:20:36.62107... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe |
| 1:20:36.62133... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe |
| 1:20:36.62165... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe |
| 1:20:36.62188... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe |
| 1:20:36.62529... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\ |
| 1:20:36.62536... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS |
| 1:20:36.62546... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32 |
| 1:20:36.63116... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\ |
| 1:20:36.63196... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS |
| 1:20:36.63206... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32 |
| 1:20:36.63421... | Malware_U3_W2_L2.exe | 328 | CreateFile | C:\WINDOWS\system32\svchost.exe.Manifest |

Queste sono le librerie in questione



| Module | Address | Size | Path | Company | Version | Timestamp |
|---|---|---|---|---|---|---|
| Malware_U3_W... | 0x400000 | 0xd000 | C:\Documents and Settings\Administ... | | | 1/1/1970 1:00:... |
| apphelp.dll | 0x77b40000 | 0x22000 | C:\WINDOWS\system32\apphelp.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| version.dll | 0x77c00000 | 0x8000 | C:\WINDOWS\system32\version.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| advapi32.dll | 0x77dd0000 | 0x9b000 | C:\WINDOWS\system32\advapi32.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| rpcrt4.dll | 0x77e70000 | 0x92000 | C:\WINDOWS\system32\rpcrt4.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| secur32.dll | 0x77fe0000 | 0x11000 | C:\WINDOWS\system32\secur32.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| kernel32.dll | 0x7c800000 | 0xf6000 | C:\WINDOWS\system32\kernel32.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |
| ntdll.dll | 0x7c900000 | 0xaf000 | C:\WINDOWS\system32\ntdll.dll | Microsoft Corpo... | 5.1.2600.5512 ... | 1/1/1970 1:00:... |

# ANALISI MALWARE

## QUI UNA BREVE DESCRIZIONE DELLE LIBRERIE

apphelp.dll è un module connesso con Microsoft® Windows® Operating System da Microsoft Corporation.
Processi non di sistema come apphelp.dll provengono da software installati nel sistema. Poiché la maggior parte delle applicazioni memorizza i dati sul disco rigido e nel registro di sistema, è probabile che il computer abbia subito frammentazione e accumuli di voci non valide che possono aver influito sulle prestazioni del Pc

version.dll è un modulo che contiene le funzioni dell'interfaccia di programmi applicativi (API) usate per la versione di Windows che controlla dalle applicazioni sul NT di Windows.
version.dll è un processo di sistema necessario perché il PC funzioni correttamente. Non lo si deve rimuovere.

advapi32.dll è una parte di una libreria avanzata di servizi di api che supporta i numerosi api compreso i molti chiamate di registrazione e di sicurezza.
advapi32.dll è un processo di sistema necessario perché il PC funzioni correttamente. Non lo si deve rimuovere.

rpcrt4.dll è il Remote Procedure Call (RPC) api, usato dalle applicazioni di Windows per la rete e la comunicazione del Internet.
rpcrt4.dll è un processo di sistema necessario perché il PC funzioni correttamente. Non lo si deve rimuovere.

Il file secur32.dll è l'interfaccia SSP per sistemi operativi Windows che contiene i moduli di sicurezza. Ci sono più di quaranta i file. Dll che sono collegati staticamente a Secur32.dll, con settantasei funzioni esportate in tutto. D'altra parte, funzioni importate dal file sono quelli che sono attributi dei file seguenti: ADVAPI32.DLL, kernel32.dll e ntdll.dll. Questo è un processo di sistema importante che dovrebbe essere in picco funzionanti in ogni momento. Il file è un plug-in per i Service Provider sicura, dove SSP riceve richieste dal sistema per le funzioni che supporta, e il file secur32.dll è responsabile del caricamento dei provider di servizi condivisi. Se uno dei file collegati al Secur32.dll non caricare, o si trova mancanti dal sistema; secur32.dll non verrà caricato, e si verificherà un errore di sistema. Questo è un file system che non dovrebbe essere revocata o modificata. Il file si trova nella cartella predefinita di Windows System 32.

kernel32.dll è il Microsoft Windows Kernel più importante. La funzionalità che richiama la maggior parte delle funzioni delle finestre è collegata a questo DLL del nocciolo in qualche modo.
kernel32.dll è un processo di sistema necessario perché il PC funzioni correttamente. Non lo si deve rimuovere.