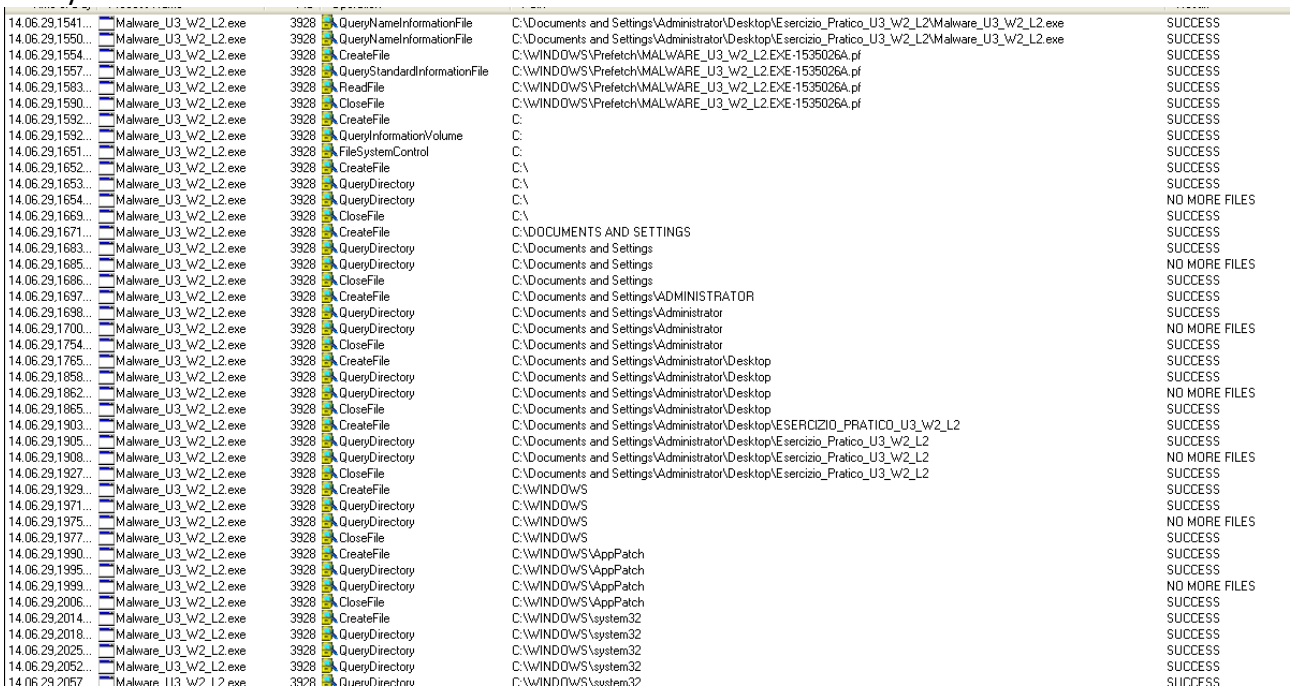
ANALISI DINAMICA MALWARE

FRANCESCO PERSICHETTI

L'esercizio consiste nel:

- Identificare azioni del malware sul file system utilizzando Process Monitor
- Identificare azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware
- Profilare il malware in base alla correlazione tra operation e Path
- Fare un'istantanea

Facciamo partire il process monitor che va ad analizzare il comportamento del nostro malware sul file system



| | | | | | |
|---|---|---|---|---|---|
| 14.06.29,1541... | Malware_U3_W2_L2.exe | 3928 | QueryNameInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe | SUCCESS |
| 14.06.29,1550... | Malware_U3_W2_L2.exe | 3928 | QueryNameInformationFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe | SUCCESS |
| 14.06.29,1554... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf | SUCCESS |
| 14.06.29,1557... | Malware_U3_W2_L2.exe | 3928 | QueryStandardInformationFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf | SUCCESS |
| 14.06.29,1583... | Malware_U3_W2_L2.exe | 3928 | ReadFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf | SUCCESS |
| 14.06.29,1590... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf | SUCCESS |
| 14.06.29,1592... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C: | SUCCESS |
| 14.06.29,1592... | Malware_U3_W2_L2.exe | 3928 | QueryInformationVolume | C: | SUCCESS |
| 14.06.29,1651... | Malware_U3_W2_L2.exe | 3928 | FileSystemControl | C: | SUCCESS |
| 14.06.29,1652... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\ | SUCCESS |
| 14.06.29,1653... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\ | SUCCESS |
| 14.06.29,1654... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\ | NO MORE FILES |
| 14.06.29,1669... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\ | SUCCESS |
| 14.06.29,1671... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\DOCUMENTS AND SETTINGS | SUCCESS |
| 14.06.29,1683... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings | SUCCESS |
| 14.06.29,1685... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings | NO MORE FILES |
| 14.06.29,1686... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\Documents and Settings | SUCCESS |
| 14.06.29,1697... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\Documents and Settings\ADMINISTRATOR | SUCCESS |
| 14.06.29,1698... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator | SUCCESS |
| 14.06.29,1700... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator | NO MORE FILES |
| 14.06.29,1754... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\Documents and Settings\Administrator | SUCCESS |
| 14.06.29,1765... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS |
| 14.06.29,1858... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop | SUCCESS |
| 14.06.29,1862... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop | NO MORE FILES |
| 14.06.29,1865... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS |
| 14.06.29,1903... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2 | SUCCESS |
| 14.06.29,1905... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS |
| 14.06.29,1908... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | NO MORE FILES |
| 14.06.29,1927... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS |
| 14.06.29,1929... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\WINDOWS | SUCCESS |
| 14.06.29,1971... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS | SUCCESS |
| 14.06.29,1975... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS | NO MORE FILES |
| 14.06.29,1977... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\WINDOWS | SUCCESS |
| 14.06.29,1990... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\WINDOWS\AppPatch | SUCCESS |
| 14.06.29,1995... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\AppPatch | SUCCESS |
| 14.06.29,1999... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\AppPatch | NO MORE FILES |
| 14.06.29,2006... | Malware_U3_W2_L2.exe | 3928 | CloseFile | C:\WINDOWS\AppPatch | SUCCESS |
| 14.06.29,2014... | Malware_U3_W2_L2.exe | 3928 | CreateFile | C:\WINDOWS\system32 | SUCCESS |
| 14.06.29,2018... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\system32 | SUCCESS |
| 14.06.29,2025... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\system32 | SUCCESS |
| 14.06.29,2052... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\system32 | SUCCESS |
| 14.06.29,2057... | Malware_U3_W2_L2.exe | 3928 | QueryDirectory | C:\WINDOWS\system32 | SUCCESS |

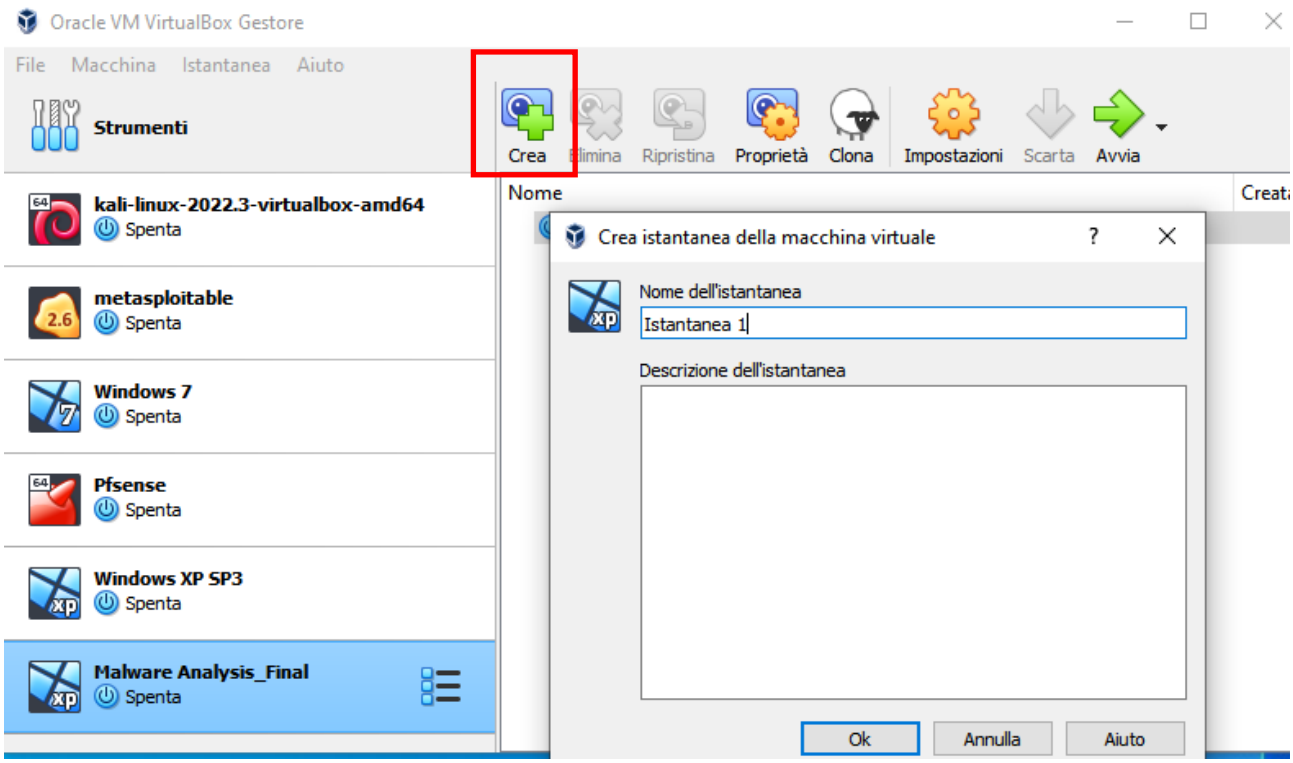
Stessa procedura lo facciamo inserendo il filtro operation e thread per andare a identificare eventuali azioni del malware

| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 14.06.29,1525... | Malware_U3_W2_L2.exe | 3928 | Process Start | | SUCCESS | Parent PID: 1832, Command line: "C:\Documents and Settings\Administrato |
| 14.06.29,1526... | Malware_U3_W2_L2.exe | 3928 | Thread Create | | SUCCESS | Thread ID: 3932 |
| 14.06.29,1545... | Malware_U3_W2_L2.exe | 3928 | 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 |
| 14.06.29,1550... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Image Base: 0x7c900000, Image Size: 0xaf000 |
| 14.06.29,2620... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Image Base: 0x7c800000, Image Size: 0xf6000 |
| 14.06.29,2952... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Image Base: 0x77b40000, Image Size: 0x22000 |
| 14.06.29,3062... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\version.dll | SUCCESS | Image Base: 0x77c00000, Image Size: 0x8000 |
| 14.06.29,3347... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Image Base: 0x77dd0000, Image Size: 0x9b000 |
| 14.06.29,3353... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS | Image Base: 0x77e70000, Image Size: 0x92000 |
| 14.06.29,3358... | Malware_U3_W2_L2.exe | 3928 | Load Image | C:\WINDOWS\system32\secur32.dll | SUCCESS | Image Base: 0x77fe0000, Image Size: 0x11000 |
| 14.06.29,3558... | Malware_U3_W2_L2.exe | 3928 | Process Create | C:\WINDOWS\system32\svchost.exe | SUCCESS | PID: 3936, Command line: "C:\WINDOWS\system32\svchost.exe" |
| 14.06.30,3485... | Malware_U3_W2_L2.exe | 3928 | Thread Exit | | SUCCESS | Thread ID: 3932, User Time: 0.0000000, Kernel Time: 0.1406250 |
| 14.06.30,3489... | Malware_U3_W2_L2.exe | 3928 | Process Exit | | SUCCESS | Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.1406250 sec |

Il malware attacca il processo svchost.exe individuato nel filtro "operation" di prima che di solito è un processo utilizzato da Microsoft per nascondere più servizi dietro ad un unico processo, andando a veder i moduli utilizzati si mnota come il rpocesso si avvalga della libreria rpcrt4.dll che è usato per la comunicazione di rete internet; infatti si vedono molto pacchetti TCP e UDP viaggiare verso un server esterno

Questo ci va pensare ad un trojan come tipo di malware poiché prende il possesso del pc vittima rendendolo un pc “zombie” da poter controllare e utilizzare in una botnet

Per ritornare alla situazione iniziale della macchina virtuale, a prima dell’esecuzione del malware, in caso l’esecuzione possa alterare la configurazione della nostra macchina; prima di svolgere l’esercitazione ho fatto un’istantanea della macchina virtuale. Così facendo nel caso la mia macchina virtuale venisse compromessa potrei ristabilire la macchina alle impostazioni originali




Una volta creata avremo due “situazioni” una sarà quella attuale e l’altra la nostra copia di salvataggio, ovviamente se vorremo utilizzare la nuova istantanea dovremo selezionarla e ripristinarla prima di avviare la macchina, altrimenti avvieremo sempre quella corrotta