

TASK:

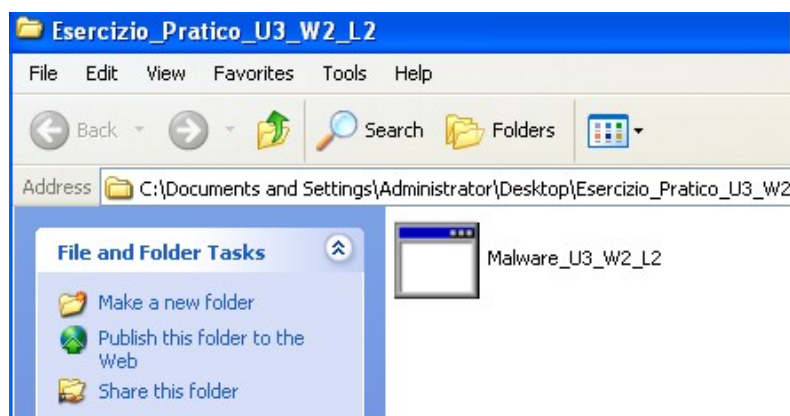
Con riferimento al file eseguibile “Esercizio_Pratico_U3_W2_L2.exe” rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system usando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware (le differenze)
- Provare a profilare il malware in base alla correlazione <<operation>> e Path

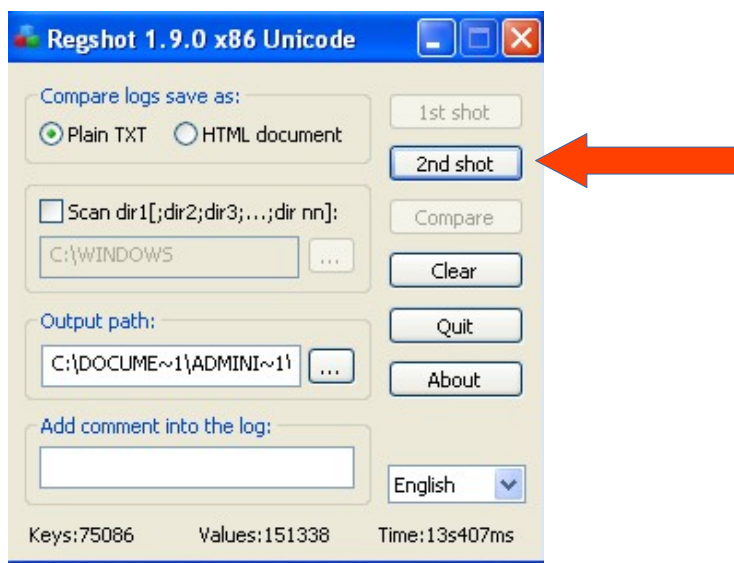
Dopo avere avviato la macchina la prima cosa che ho fatto è stata quella di avviare il tool Regshot tramite il quale ho fatto una prima istantanea prima di avviare :



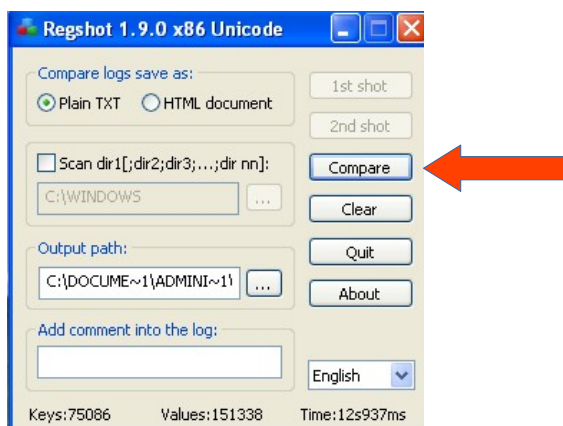
A questo punto sono andato ad avviare Process monitor. Una volta avviato il programma ed essermi accertato che stesse catturando gli eventi mi sono spostato nella cartella contenente il malware per l'esercitazione pratica di oggi:



Dopo avere avviato il malware sono tornato su Regshot per eseguire la seconda istantanea:



Una volta effettuata la seconda istantanea ho avviato quindi la comparazione tra i registri prima e dopo che ho lanciato il malware e il programma mi ha restituito un file txt in cui sono mostrate le differenze:



```
- res-x86_0010 - Notepad
File Edit Format View Help

Regshot 1.9.0 x86 Unicode
Comments:
Date/time: 2023/1/10 14:05:41 , 2023/1/10 14:06:18
Computer: MALWARE_TEST MALWARE_TEST
Username: Administrator , Administrator

values added: 10

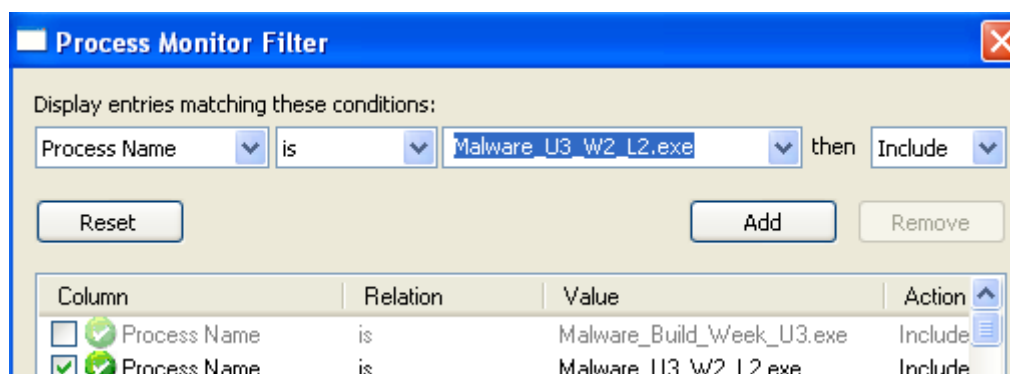
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\MinPos1920x977(1).x : 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\WinPos1920x977(1).y : 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\MaxPos1920x977(1).x : 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\MaxPos1920x977(1).y : 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\WinPos1920x977(1).left : 0x00000016
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\WinPos1920x977(1).top : 0x00000016
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\WinPos1920x977(1).right : 0x00000036
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\WinPos1920x977(1).bottom : 0x00000025
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\ScrollPos1920x977(1).x : 0x00000000
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\Bags\{06\Shell\ScrollPos1920x977(1).y : 0x00000000

values modified: 9

HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed: A7 3A B5 08 1C 1E DC F4 31 C0 43 19 32 91 07 D3 71 76 91 87 65 5A FB 2D DF 43 01 A5 EB 01 F7
HKLM\SOFTWARE\Microsoft\Cryptography\RNGSeed: B9 A4 OF 22 18 3E EE 40 E0 BB 80 59 FA 39 67 E3 B9 A4 7F 77 53 CD CE 67 17 81 EF 3C 01 DC 00 59
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\EventMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\EventMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile1: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile1: "c:\windows\system32\ESENT.dll"
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75487000-EF1F-11D0-9888-000000000000}
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75487000-EF1F-11D0-9888-000000000000}
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75487000-EF1F-11D0-9888-000000000000}
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75487000-EF1F-11D0-9888-000000000000}
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75487000-EF1F-11D0-9888-000000000000}
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\BagMRU\MRUListEx: 02 00 00 00 06 00 00 07 00 00 00
HKU\S-1-5-21-1993962763-1606980848-72345543-500\Software\Microsoft\Windows\Shell\NORoam\BagMRU\MRUListEx: 17 00 00 00 02 00 00 06 00 00 00
```

Da questo file possiamo vedere come il malware ha modificato 19 voci dei registri, aggiungendo 10 valori e modificandone 9.

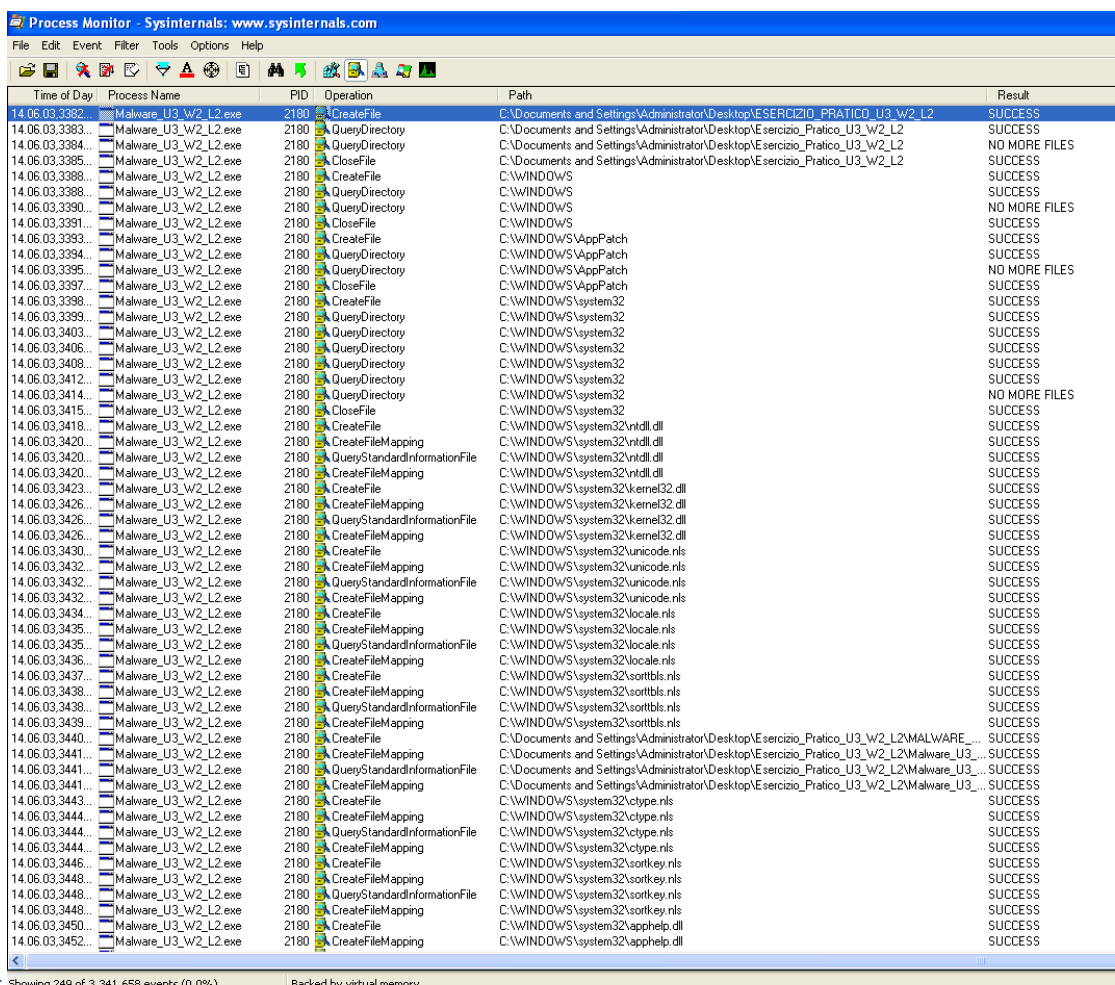
A questo punto sono tornato su Process Monitor. Qua sono andato a modificare i filtri in modo di avere a schermo solo eventi collegati al processo con nome “Esercizio_Pratico_U3_W2_L2.exe”:



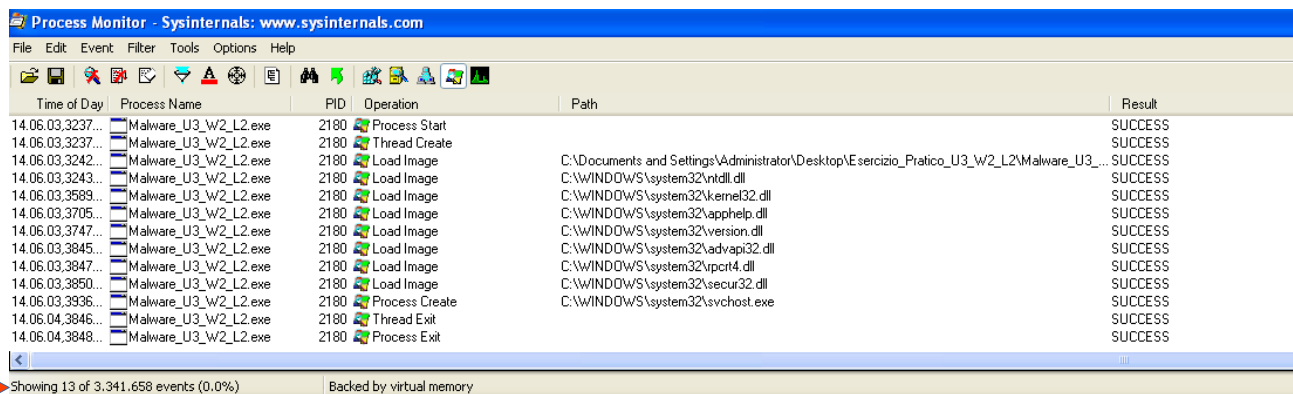
Tenendo attivi tutti gli eventi possibili ho ottenuto un totale di 418 eventi:



Riguardo agli eventi riguardanti il file system ho trovato un totale di 249 eventi:

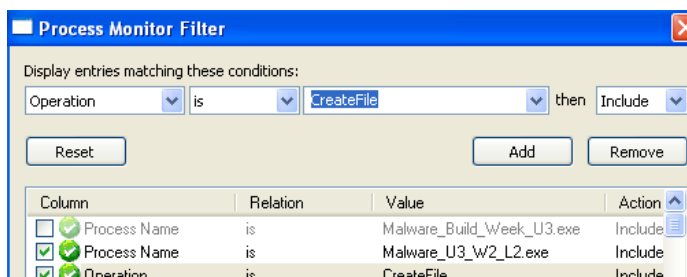


Riguardo invece eventuali azioni nell'ambito di processi e thread ho trovato un totale di 13 eventi:

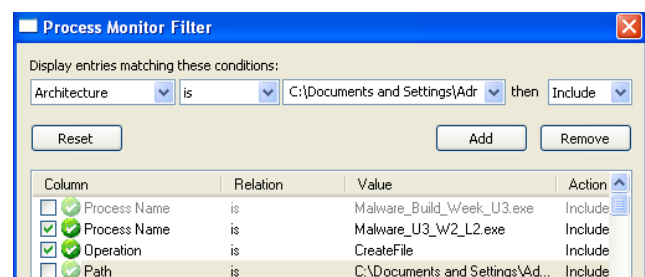


Time of Day	Process Name	PID	Operation	Path	Result
14.06.03.3237...	Malware_U3_W2_L2.exe	2180	Process Start		SUCCESS
14.06.03.3237...	Malware_U3_W2_L2.exe	2180	Thread Create		SUCCESS
14.06.03.3242...	Malware_U3_W2_L2.exe	2180	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_...	SUCCESS
14.06.03.3243...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
14.06.03.3589...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS
14.06.03.3705...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS
14.06.03.3747...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS
14.06.03.3845...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
14.06.03.3847...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\vpct4.dll	SUCCESS
14.06.03.3850...	Malware_U3_W2_L2.exe	2180	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
14.06.03.3936...	Malware_U3_W2_L2.exe	2180	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS
14.06.04.3846...	Malware_U3_W2_L2.exe	2180	Thread Exit		SUCCESS
14.06.04.3848...	Malware_U3_W2_L2.exe	2180	Process Exit		SUCCESS

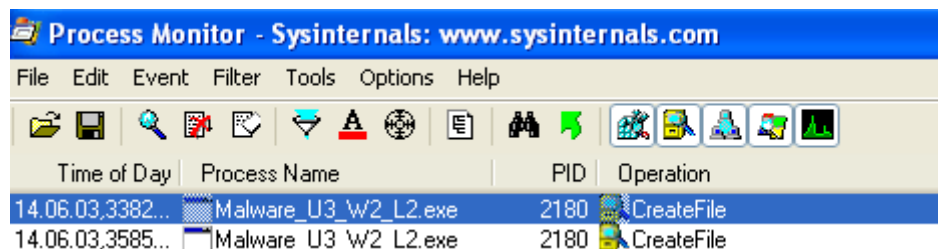
Andando a rendere più stringenti i filtri, aggiungendo un tipo specifico di operazione, come il CreateFile, e specificando un path di interesse, in questo caso “C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2” ho ottenuto il seguente riscontro:



Column	Relation	Value	Action
<input type="checkbox"/> Process Name	is	Malware_Build_Week_U3.exe	Include
<input checked="" type="checkbox"/> Process Name	is	Malware_U3_W2_L2.exe	Include
<input checked="" type="checkbox"/> Operation	is	CreateFile	Include



Column	Relation	Value	Action
<input type="checkbox"/> Architecture	is	C:\Documents and Settings\Ad...	Include
<input checked="" type="checkbox"/> Process Name	is	Malware_Build_Week_U3.exe	Include
<input checked="" type="checkbox"/> Process Name	is	Malware_U3_W2_L2.exe	Include
<input checked="" type="checkbox"/> Operation	is	CreateFile	Include
<input type="checkbox"/> Path	is	C:\Documents and Settings\Ad...	Include



Time of Day	Process Name	PID	Operation
14.06.03.3382...	Malware_U3_W2_L2.exe	2180	CreateFile
14.06.03.3585...	Malware_U3_W2_L2.exe	2180	CreateFile

Andando a controllare nella cartella possiamo effettivamente notare come sia stato creato un file di testo che inizialmente non era presente:

