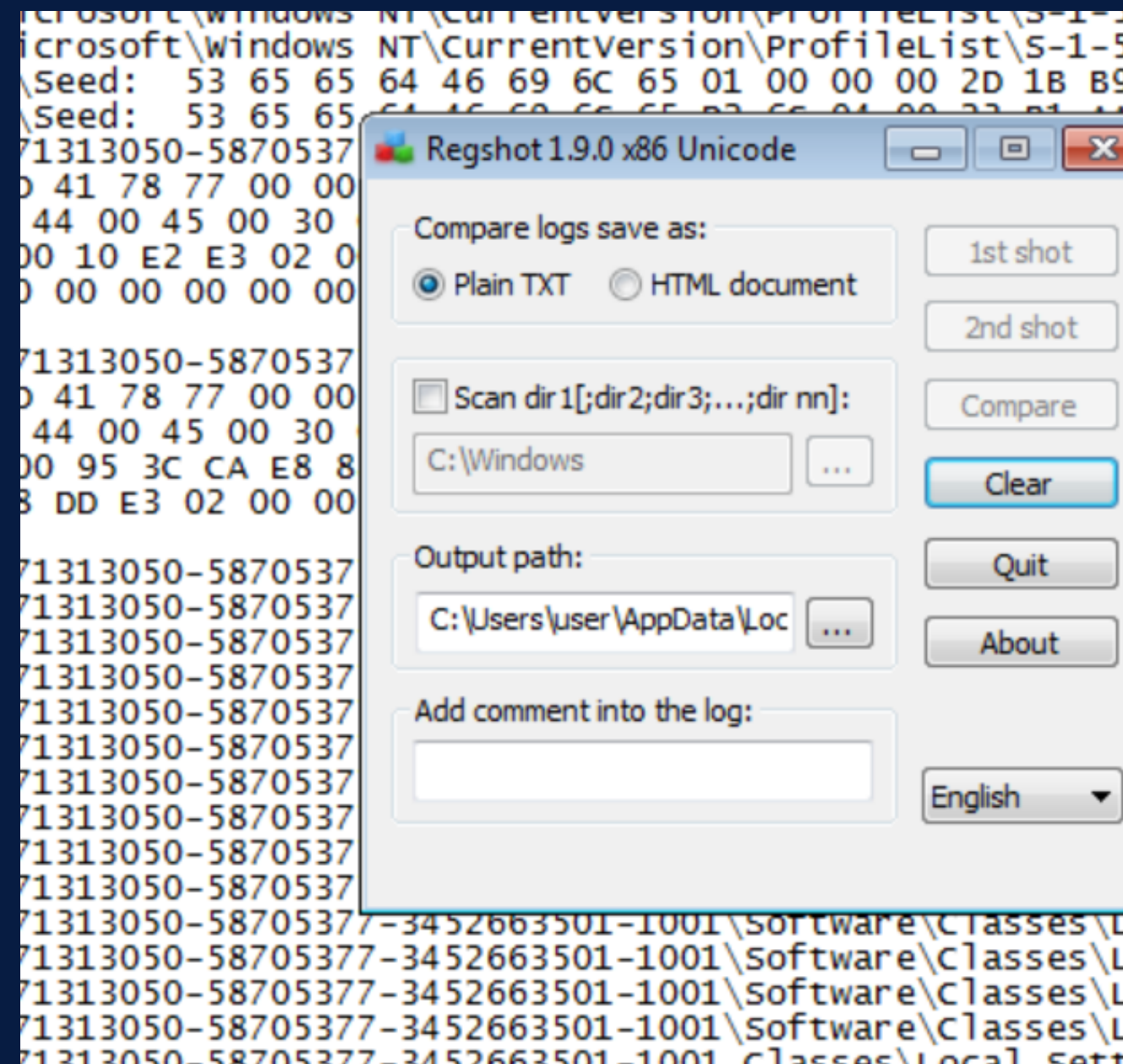

Traccia: Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor
- Modifiche del registro dopo il malware (le differenze)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Mediante regshot ottengo una prima istantanea,
senza che il malware sia avviato

.. e una seconda con malware avviato.



Tasto destro sul malware.exe, “Risoluzione problemi” e infine “avvia il programma” permette che il malware venga eseguito.

Avvio, process monitor per vedere le attività del malware.

PROCESS MONITOR:

Permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo. È un tool molto utilizzato per monitorare eventuali processi o attività create dal malware in esecuzione su un sistema

Time ...	Process Name	PID	Operation	Path	Result	Detail
14:38:...	Malware_U3_...	1144	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WI...	SyncType: SyncTy...
14:38:...	Malware_U3_...	1144	CreateFileMapp...	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTy...
14:38:...	Malware_U3_...	1144	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: G...
14:38:...	Malware_U3_...	1144	QueryStandardI...	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
14:38:...	Malware_U3_...	1144	CreateFileMapp...	C:\Windows\AppPatch\sysmain.sdb	FILE LOCKED WI...	SyncType: SyncTy...
14:38:...	Malware_U3_...	1144	QueryStandardI...	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
14:38:...	Malware_U3_...	1144	CreateFileMapp...	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
14:38:...	Malware_U3_...	1144	QueryStandardI...	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 4.0...
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired AllocationSize: 4.075...
14:38:...	Malware_U3_...	1144	QuerySecurityFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Informa EndOfFile: 4.075.336
14:38:...	Malware_U3_...	1144	QueryBasicInfor...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Creation NumberOfLinks: 2
14:38:...	Malware_U3_...	1144	QuerySecurityFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Informa DeletePending: False
14:38:...	Malware_U3_...	1144	QueryBasicInfor...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Creation Directory: False
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryBasicInfor...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	CreationTime: 08/0...
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryDirectory	C:\Users	SUCCESS	Filter: Users, 1: Users
14:38:...	Malware_U3_...	1144	CloseFile	C:\	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryDirectory	C:\Users\user	SUCCESS	Filter: user, 1: user
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users\user	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryDirectory	C:\Users\user\Desktop	SUCCESS	Filter: Desktop, 1: ...
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users\user	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users\user\Desktop	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryDirectory	C:\Users\user\Desktop\MALWARE	SUCCESS	Filter: MALWARE, ...
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users\user\Desktop	SUCCESS	
14:38:...	Malware_U3_...	1144	CreateFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Desired Access: R...
14:38:...	Malware_U3_...	1144	QueryBasicInfor...	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	CreationTime: 08/0...
14:38:...	Malware_U3_...	1144	CloseFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	

Showing 17,032 of 181,013 events (9.4%) Backed by virtual memory

AZIONI DEL MALWARE SUI FYLE SYSTEM

Time ...	Process Name	PID	Operation	Path
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	QueryDirectory	C:\Windows\
15:57:...	Malware_U3_...	1808	CloseFile	C:\Windows\
15:57:...	Malware_U3_...	1808	Create File	C:\Windows\

AZIONI DEL MALWARE SUI PROCESS AND THREADS

Time ...	Process Name	PID	Operation	Path
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\AppPatc
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Users\user\Desktop
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	Malware_U3_...	2724	Process Create	C:\Windows\SysWOV
15:07:...	svchost.exe	2752	Process Start	
15:07:...	svchost.exe	2752	Thread Create	
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOV
15:07:...	svchost.exe	2752	Load Image	C:\Windows\SysWOV
15:07:...	svchost.exe	2752	Load Image	C:\Windows\System3
15:07:...	svchost.exe	2752	Load Image	C:\Windows\SysWOV

Effettuo 2a istantanea, con
malware attivo e comparo :

HKEY_LOCAL_MACHINE: include le
impostazioni comuni per tutti gli
utenti del sistema
indipendentemente dalle loro
preferenze

HKEY_USERS: raggruppa le
impostazioni di tutti gli utenti
connessi al sistema

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 14:31:33 , 2024/2/13
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys deleted: 2
-----
HKLM\SYSTEM\ControlSet001\services\PROCMON
HKLM\SYSTEM\CurrentControlSet\services\PROCMON

-----
Keys added: 5
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY
HKLM\SYSTEM\ControlSet001\services\Malserv
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LE
HKLM\SYSTEM\CurrentControlSet\services\Mal
HKU\S-1-5-21-3771313050-58705377-3452663501

-----
Values deleted: 6
-----
HKLM\SYSTEM\ControlSet001\services\PROCMON
HKLM\SYSTEM\ControlSet001\services\PROCMON
HKLM\SYSTEM\ControlSet001\services\PROCMON
HKLM\SYSTEM\CurrentControlSet\services\PROCMON
HKLM\SYSTEM\CurrentControlSet\services\PROCMON
HKLM\SYSTEM\CurrentControlSet\services\PROCMON

-----
Values added: 17
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY
HKLM\SYSTEM\ControlSet001\services\Malserv
```

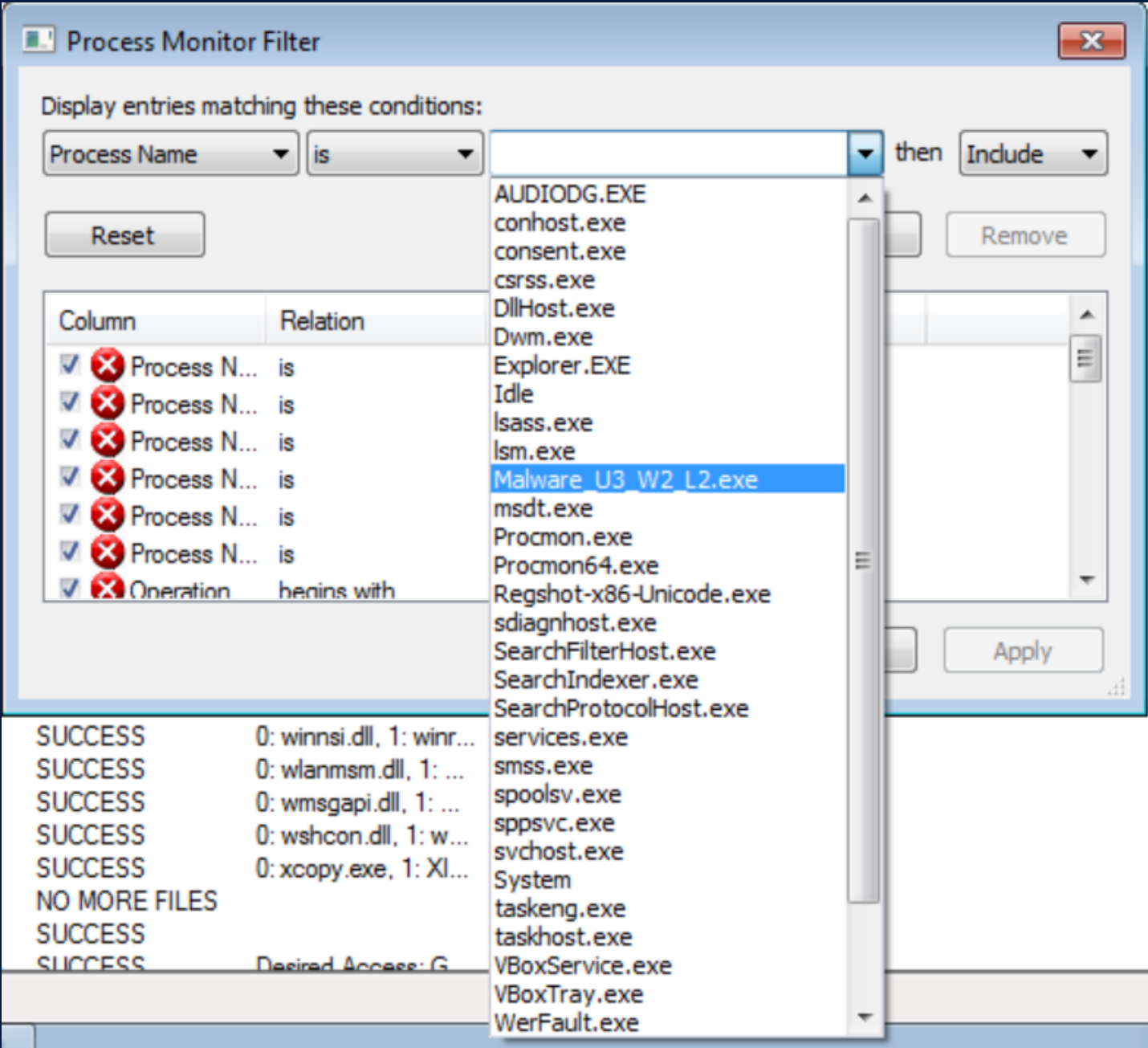
```
-----
values modified: 12
-----
HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\ProfileList\S-1
HKLM\SOFTWARE\Microsoft\windows NT\CurrentVersion\ProfileList\S-1
HKLM\SYSTEM\ RNG\Seed: 53 65 65 64 46 69 6C 65 01 00 00 00 2D 1B
HKLM\SYSTEM\ RNG\Seed: 53 65 65 64 46 69 6C 65 D2 6C 04 00 23 B1
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
8 00 00 00 00 3D 41 78 77 00 00 00 00 00 00 16 00 00 00 00 00 01
00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 3
00 00 00 00 00 00 10 E2 E3 02 00 00 00 00 68 00 01 00 00 00 00
1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 62
00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
8 00 00 00 00 3D 41 78 77 00 00 00 00 00 00 16 00 00 00 00 00 01
00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 3
00 00 00 00 00 00 95 3C CA E8 88 5E 00 00 62 DE 87 FB FE 07 00 00
0 00 00 00 00 E8 DD E3 02 00 00 00 00 08 00 00 00 00 00 00 B5
00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsof
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\software\Classes
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_classes\Local se
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_classes\Local se
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_classes\Local se
```


PROFILARE IL MALWARE CORRELANTE

<<OPERATION>> E <<PATH>>

Andando su “Filt” e nuovamente “Filt”, ho il display dove filtro il malware.

Il tipo di malware agisce sul file system del S.O., nascondendosi come un processo di Windows. Tipico di un trojan, il quale innietta dati malevoli, modifica i file del sistema e li compromette.



Time ...	Process Name	PID	Operation	Path	Result	Detail
15:07:...	Malware_U3_...	2724	Process Profiling		SUCCESS	User Time: 0.0000...
15:07:...	Malware_U3_...	1984	Process Profiling		SUCCESS	User Time: 0.0000...