Traccia: Configurare la macchina virtuale per l’analisi dinamica (il malwaresarà 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)

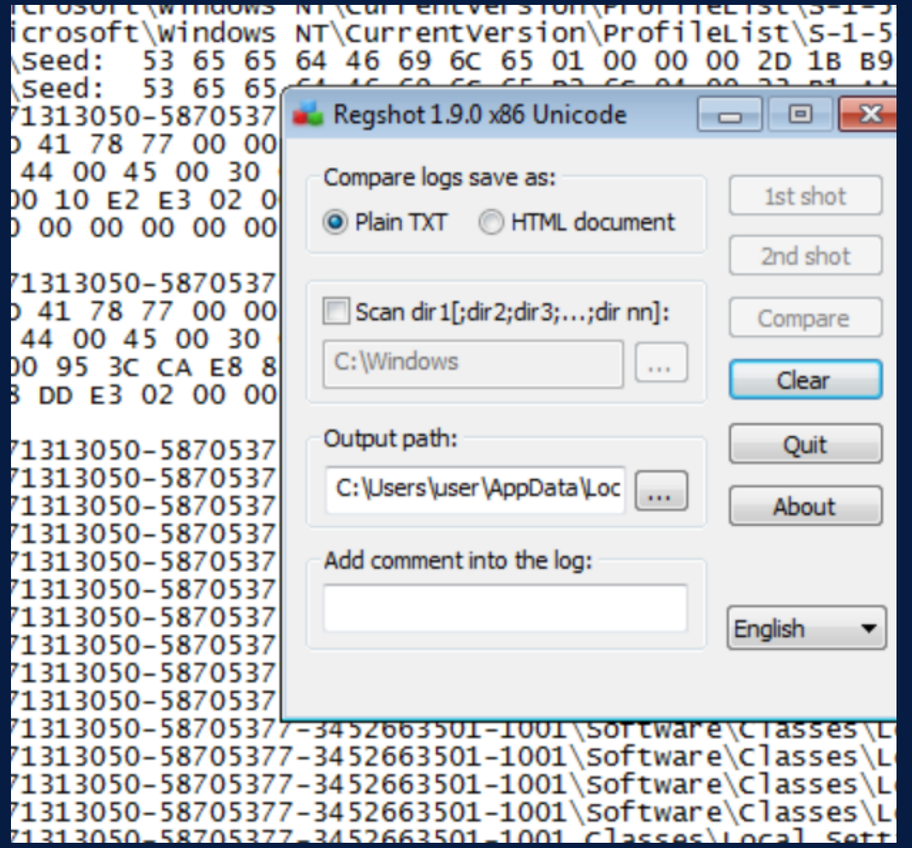
- Identificare eventuali azioni del malwaresu processi e threadutilizzando ProcessMonitor

- Modifiche del registro dopo il malware(le differenze)

- Provare a profilare il malwarein base alla correlazione tra «operation» e Path.

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

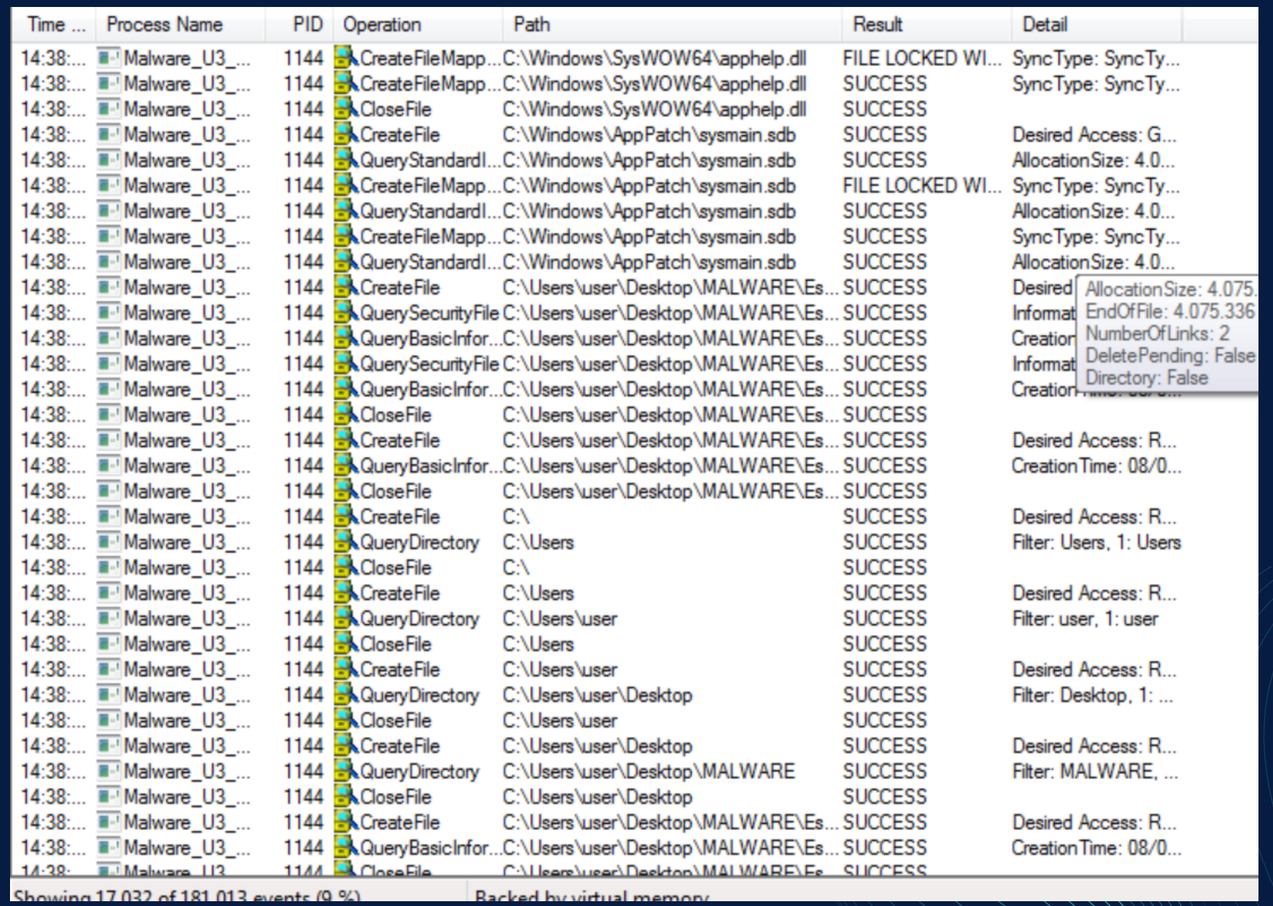
.. e una seconda con malware avviato.



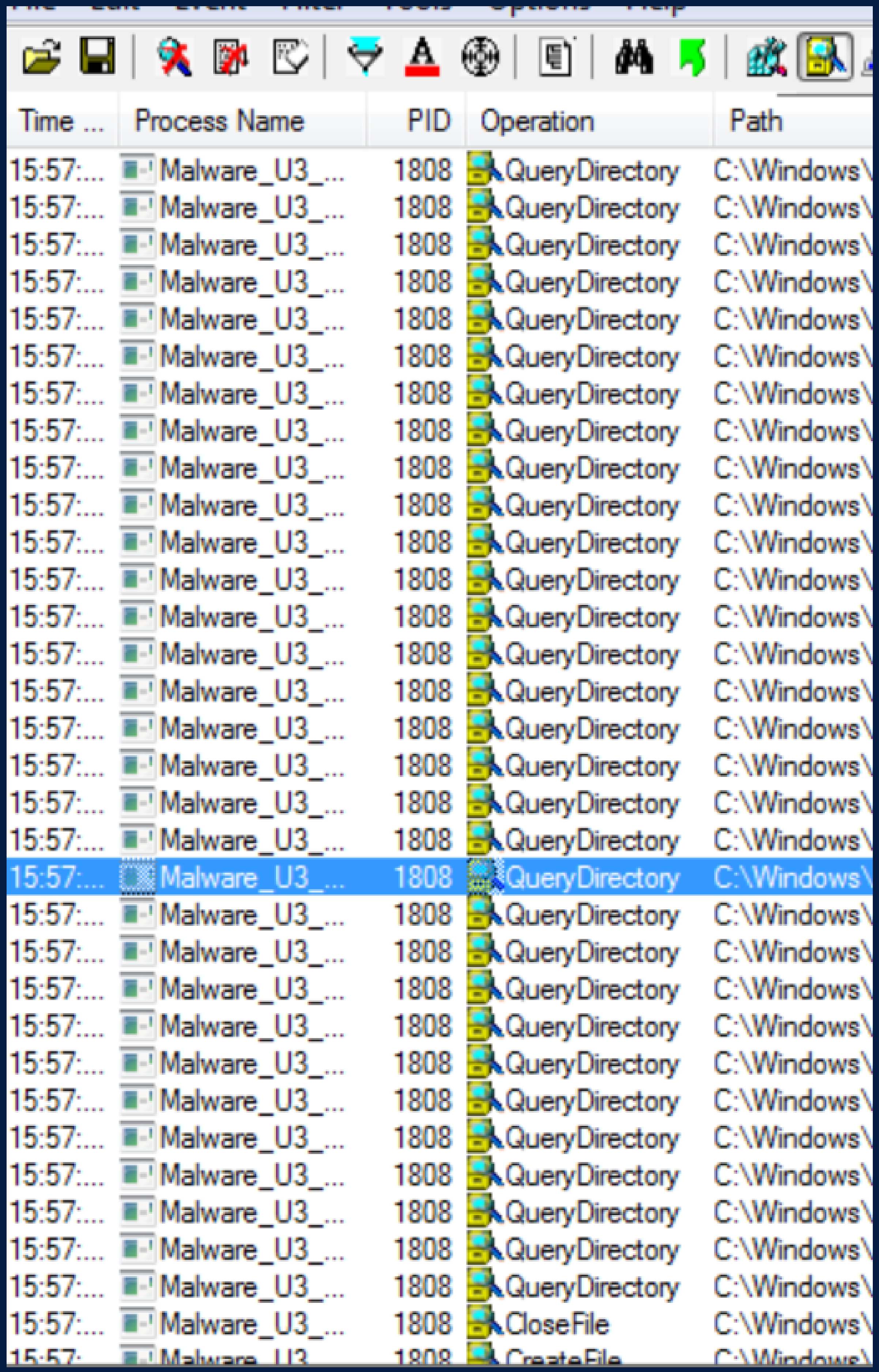
Tasto destro sul malware.exe, “Risoluzione problemi” e infine “avvia il programma” permette che il malware venga eseguito.

Avvio, process monitor per vedere le attività del malware.

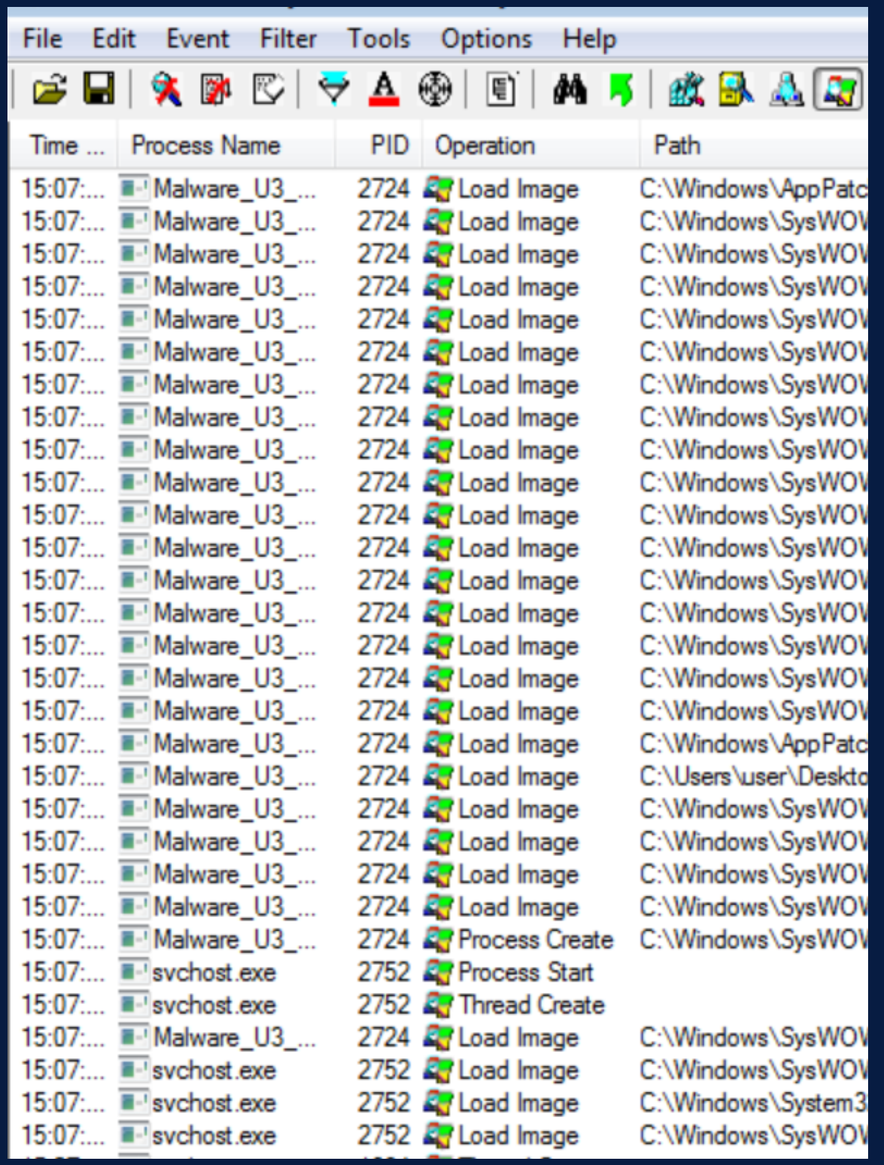
PROCESS MONITOR:
Permette di monitorare i processi ed i thread attivi, l’attività di rete, l’accesso ai file e le chiamate di sistema effettuate su un sistema operativo. È un tool molto utilizzato per monitorare eventuali processi o attività create dal malware in esecuzione su un sistema



AZIONI DEL MALWARE SUI FYLE SYSTEM



AZIONI DEL MALWARE SUI PROCESS AND THREADS

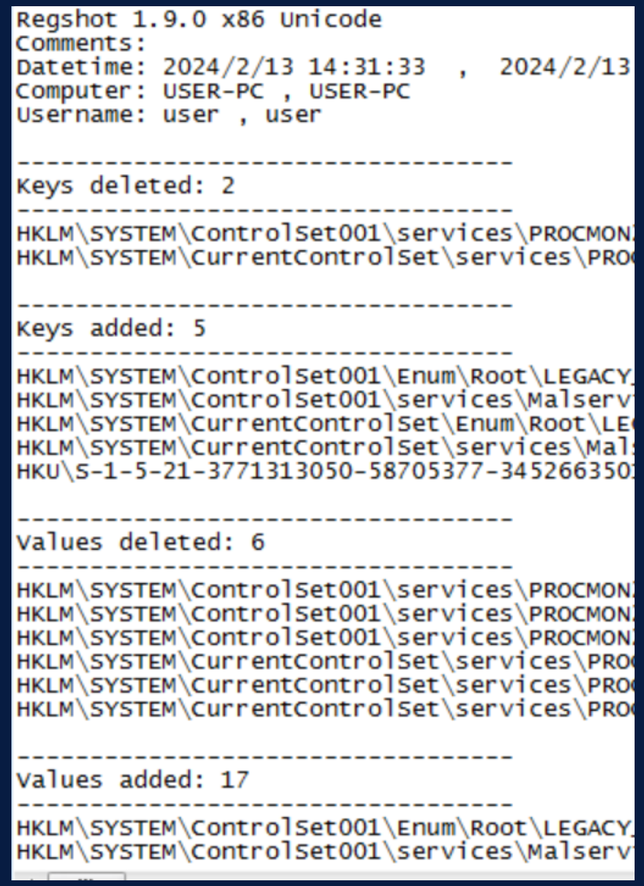


Time ...	Process Name	PID	Operation	Path
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\AppPatc
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOW
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOW
15:07:...	Malware_U3_...	2724	Load Image	C:\Windows\SysWOW
15:07:...	Malware_U3_...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

Effettuo 2a instantanea, 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



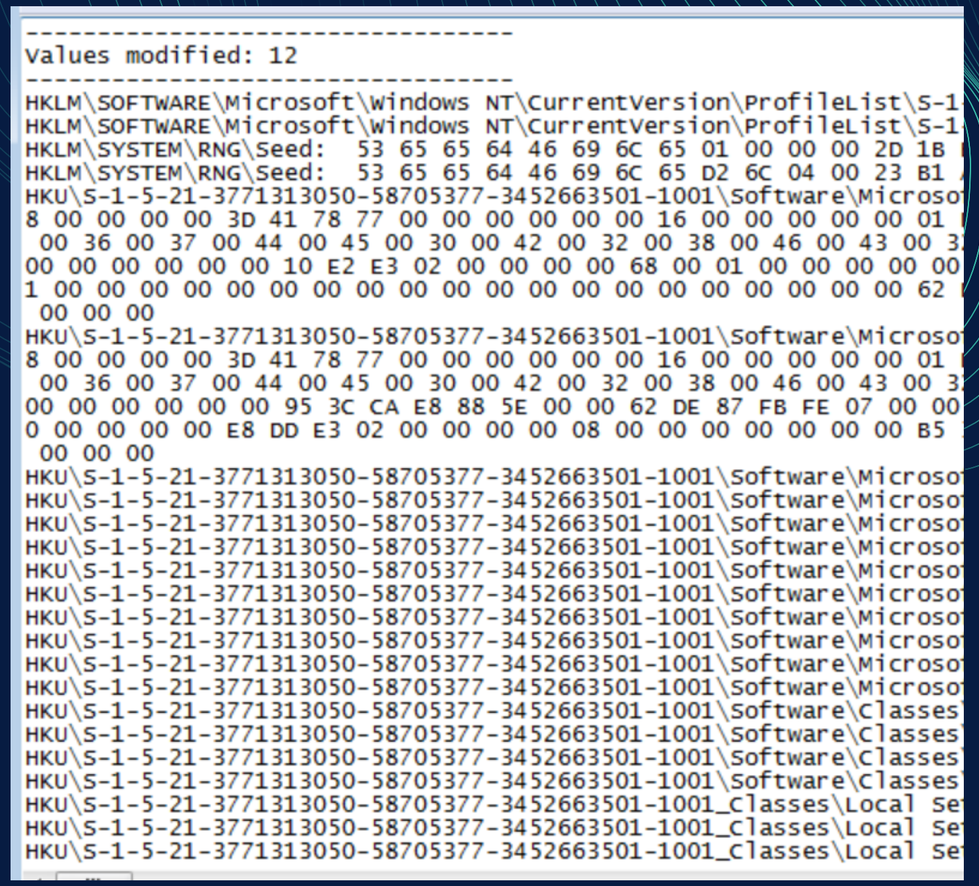
```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 14:31:33  ,  2024/2/13
Computer: USER-PC , USER-PC
Username: user , user

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

----------------------------------
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-1-5-21-3771313050-58705377-345266350

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

----------------------------------
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\Microso
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 00
1 00 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\Microso
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 00 B5
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microso
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.