

Obbiettivo:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

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 Process Monitor (procmon) oppure se ci sono problemi multimon
- 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 tra «operation» e Path.

Suggerimento:

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione **Create File** su path noti (ad esempio il path dove è presente l'eseguibile del malware).

Prima Fase

Come prima cosa andiamo a fare velocemente un'analisi statica base sul Malware dato, per poi confermare il tutto nell'analisi Dinamica base chiesta nell'esercitazione di oggi.

Utilizziamo il tool CFF explorer e analizzando il malware, troviamo una libreria importata che riguarda il file System contenente 54 funzioni e la divisione in 4 sezioni.

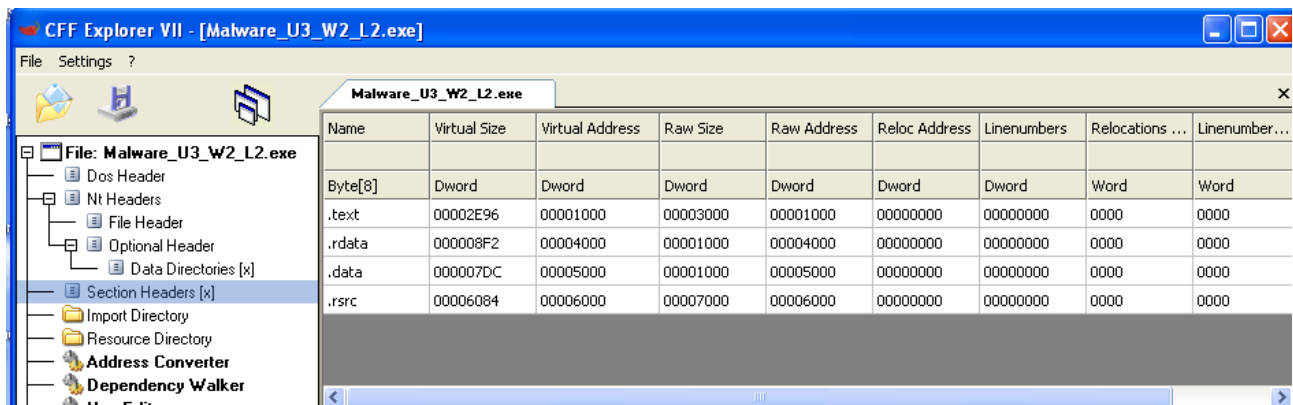
CFF Explorer VII - [Malware_U3_W2_L2.exe]

File Settings ?

Malware_U3_W2_L2.exe

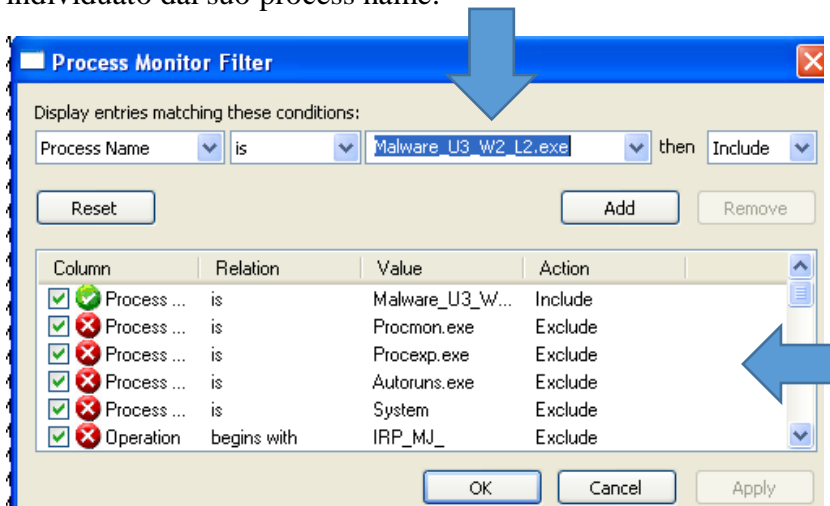
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
000046B8	N/A	00004444	00004448	0000444C	00004450	00004454
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00004548	00004548	001B	CloseHandle
00004556	00004556	02BF	VirtualFree
00004564	00004564	0218	ReadFile
00004570	00004570	02BB	VirtualAlloc
00004580	00004580	0112	GetFileSize
0000458F	0000458F	0034	CreateFileA

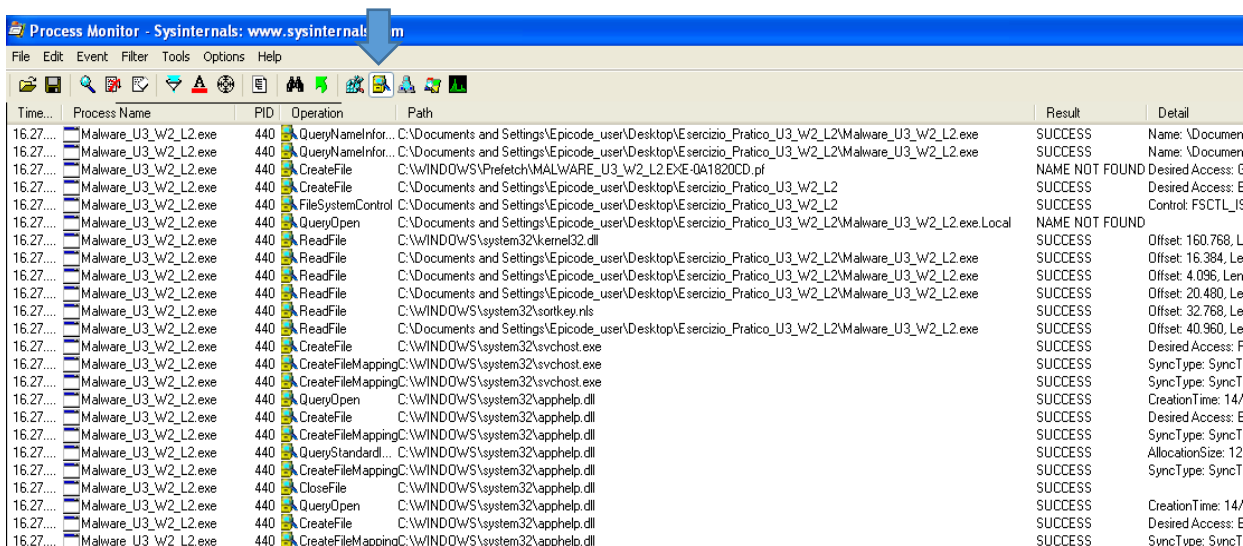


Seconda fase

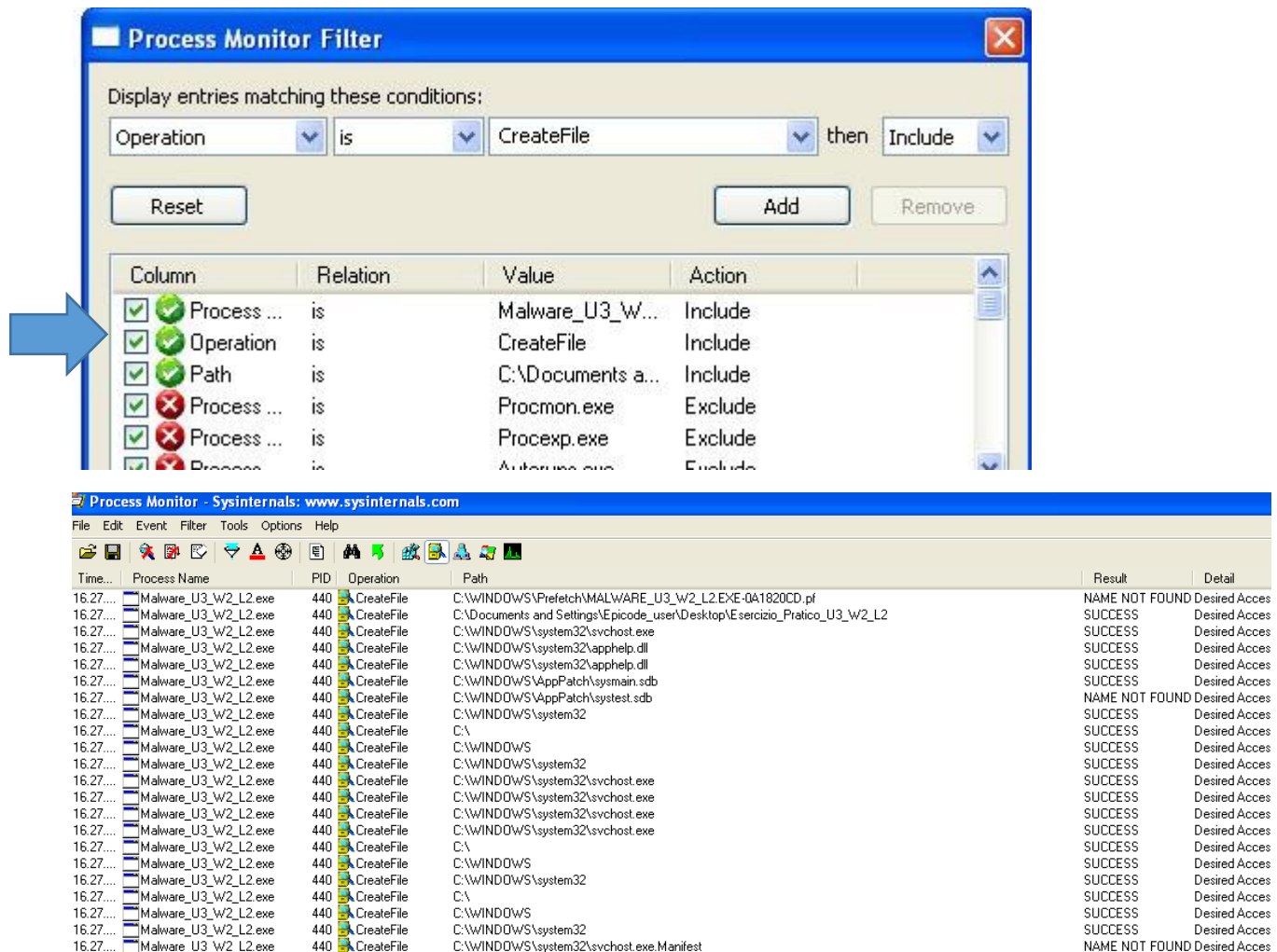
Adesso andiamo ad effettuare l'analisi dinamica basica del nostro Malware, per fare ciò dobbiamo avviare il relativo file eseguibile. In questo caso utilizzeremo il tool **Process Monitor**, utilizzando il filtro del tool possiamo filtrare appunto le operazioni che va a compiere il nostro Malware, individuato dal suo process name.



Dopo di che monitorando le attività del Malware, possiamo vedere tutte le operazioni che effettua sul file system della macchina, visualizziamo le operazioni solo nel file system selezionando l'icona indicata dalla freccia nella barra dei comandi.



Andiamo a ricercare anche altre operazioni sempre grazie al filtro del tool, come ad esempio le operation, in particolare l'operazione Create File, i processi attivati dal Malware e i thread.



The image shows the 'Process Monitor Filter' dialog box and the main 'Process Monitor' window. The dialog box is configured to filter for 'Operation is CreateFile' and then 'Include'. The main window displays a list of events where the 'Malware_U3_W2_L2.exe' process performs 'CreateFile' operations on various system files and paths.

Process Monitor Filter Configuration:

- Display entries matching these conditions:
- Operation is CreateFile then Include
- Buttons: Reset, Add, Remove

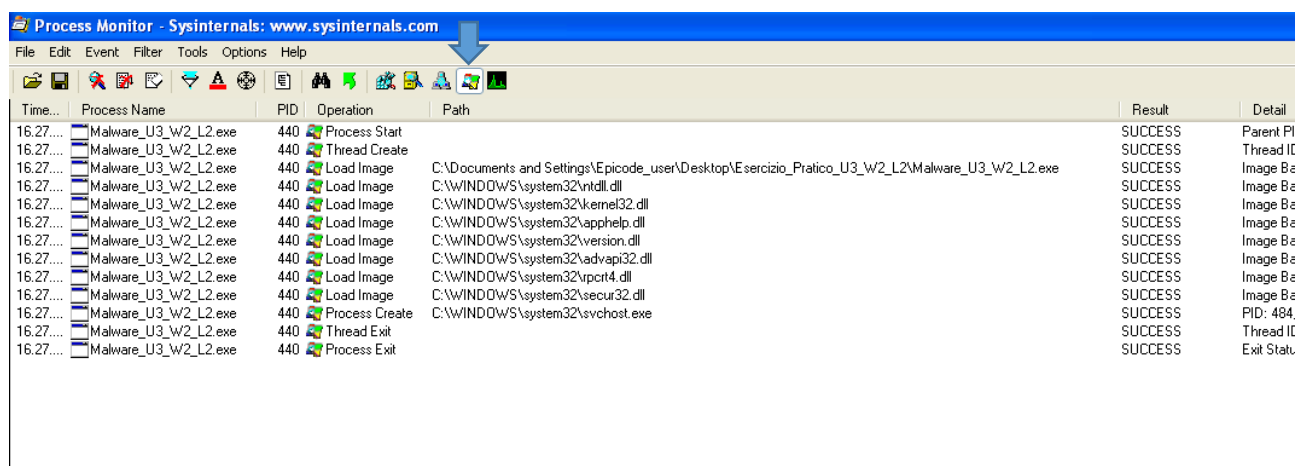
Process Monitor Filter List:

Column	Relation	Value	Action
Process ...	is	Malware_U3_W...	Include
Operation	is	CreateFile	Include
Path	is	C:\Documents a...	Include
Process ...	is	Procmon.exe	Exclude
Process ...	is	Procexp.exe	Exclude
Process ...	is	Automa.exe	Exclude

Process Monitor - Sysinternals: www.sysinternals.com

Time...	Process Name	PID	Operation	Path	Result	Detail
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-0A1820CD.pf	NAME NOT FOUND	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	NAME NOT FOUND	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND	Desired Access

Per visualizzare solo i processi e i thread selezioniamo l'icona indicata dalla freccia nella barra degli strumenti.

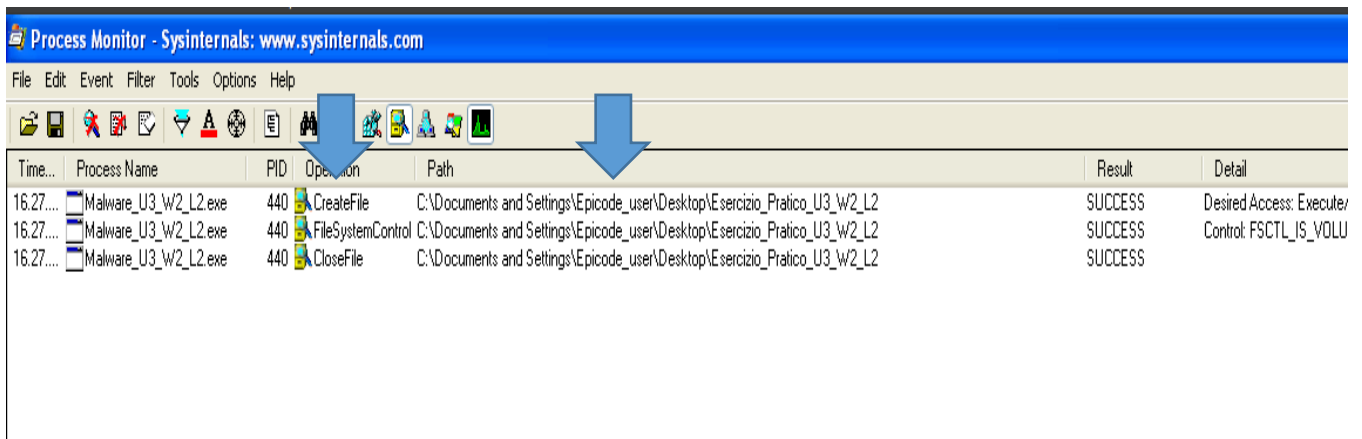


The image shows the 'Process Monitor' window with the 'Process' and 'Thread' icons selected in the toolbar. The main window displays a list of events where the 'Malware_U3_W2_L2.exe' process performs 'Process Start', 'Thread Create', 'Load Image', 'Process Create', 'Thread Exit', and 'Process Exit' operations.

Process Monitor - Sysinternals: www.sysinternals.com

Time...	Process Name	PID	Operation	Path	Result	Detail
16.27...	Malware_U3_W2_L2.exe	440	Process Start		SUCCESS	Parent PI
16.27...	Malware_U3_W2_L2.exe	440	Thread Create		SUCCESS	Thread ID
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\vpct4.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base
16.27...	Malware_U3_W2_L2.exe	440	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 484
16.27...	Malware_U3_W2_L2.exe	440	Thread Exit		SUCCESS	Thread ID
16.27...	Malware_U3_W2_L2.exe	440	Process Exit		SUCCESS	Exit Status

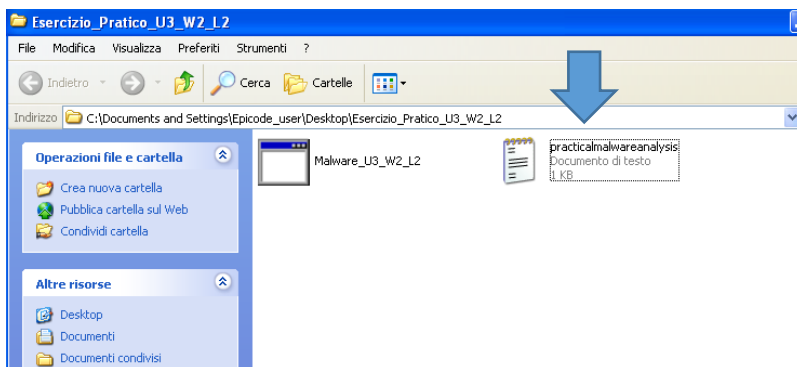
Analizzando nello specifico il path della cartella dove si trova il Malware, possiamo notare come viene rilevata la creazione del file da parte del Malware che troviamo anche direttamente nella cartella. Che possiamo dedurre sia un Keylogger.



The screenshot shows the Process Monitor application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains various icons for file operations. The main table displays the following data:

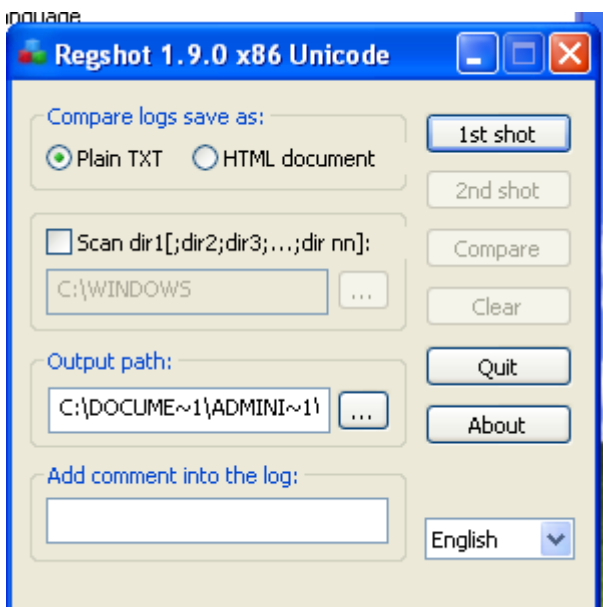
Time...	Process Name	PID	Operation	Path	Result	Detail
16.27...	Malware_U3_W2_L2.exe	440	CreateFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/
16.27...	Malware_U3_W2_L2.exe	440	FileSystemControl	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Control: FSCTL_IS_VOLLU
16.27...	Malware_U3_W2_L2.exe	440	CloseFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	

Two blue arrows point from the toolbar icons to the "CreateFile" and "FileSystemControl" rows in the table.



Terza fase

Infine possiamo notare anche come il Malware analizzato modifichi anche le chiavi di registro, per controllare ciò utilizziamo il tool **Regshot**, che effettua due shot prima e dopo il lancio del Malware.



```
-res-x86_0010 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 unicode
Comments:
Datetime: 2023/1/10 14:26:47 , 2023/1/10 14:27:19
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

-----
Values modified: 5
-----
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: AE DE 77 87 33 CD E6 20 3B FB 6D 9E FA CC C
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: B5 B4 6C 28 B3 D3 B0 E6 3B 03 22 08 13 4A 6
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\CurrentVersion\
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bag
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\windows\ShellNoRoam\Bag

-----
Total changes: 5 ←
-----
```