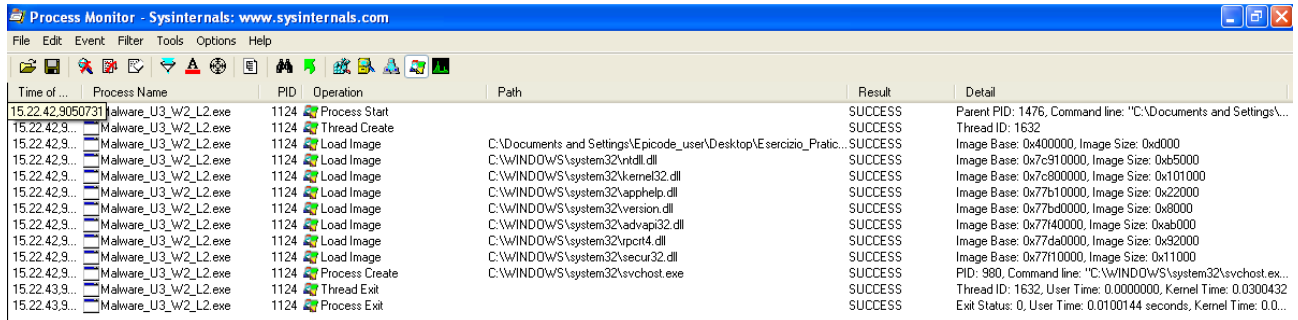


Pratica S10L2

Dopo aver messo in sicurezza la macchina virtuale e creato un'istantanea, andiamo ad avviare Process Monitor e a fare un primo snapshot delle chiavi di registro attraverso il programma Regshot. Fatte queste operazioni possiamo avviare il malware contenuto nell'esercizio.

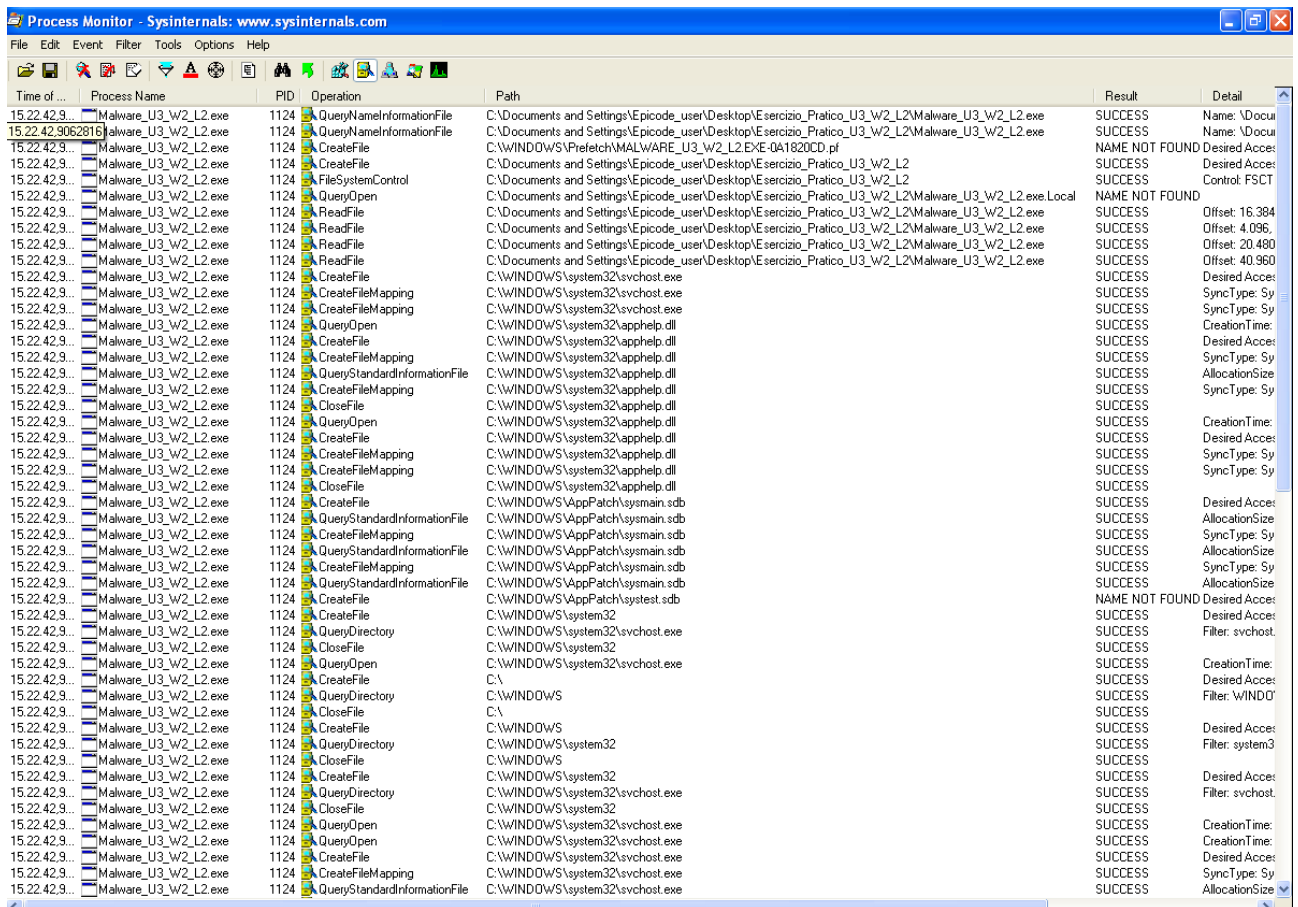
Andando ad analizzare con Processmon possiamo andare a filtrare per nome del processo. Ci accorgiamo che il malware è andato a creare il seguente processo sul sistema:



Time of ...	Process Name	PID	Operation	Path	Result	Detail
15:22:42.9065731	Malware_U3_W2_L2.exe	1124	Process Start		SUCCESS	Parent PID: 1476, Command line: "C:\Documents and Settings\...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Thread Create		SUCCESS	Thread ID: 1632
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c910000, Image Size: 0xb5000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0x101000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b10000, Image Size: 0x22000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77bd0000, Image Size: 0x8000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77140000, Image Size: 0xab000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\ipcrt4.dll	SUCCESS	Image Base: 0x77da0000, Image Size: 0x32000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Load Image	C:\WINDOWS\system32\securl32.dll	SUCCESS	Image Base: 0x77110000, Image Size: 0x11000
15:22:42.9...	Malware_U3_W2_L2.exe	1124	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 980, Command line: "C:\WINDOWS\system32\svchost.exe...
15:22:43.9...	Malware_U3_W2_L2.exe	1124	Thread Exit		SUCCESS	Thread ID: 1632, User Time: 0.0000000, Kernel Time: 0.0300432
15:22:43.9...	Malware_U3_W2_L2.exe	1124	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0100144 seconds, Kernel Time: 0.0...

vediamo quindi che il malware richiama diverse librerie di sistema e crea il processo svchost.exe, in modo da essere scambiato per un processo legittimo di sistema. Andiamo adesso a filtrare per TID 1632, avendo notato che viene avviato un Thread con tale id

Possiamo andare a filtrare adesso per modifiche al file system:



Time of ...	Process Name	PID	Operation	Path	Result	Detail
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryNameInformationFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Name: \Docu...
15:22:42.9062816	Malware_U3_W2_L2.exe	1124	QueryNameInformationFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Name: \Docu...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-0A1820CD.pf	NAME NOT FOUND	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	FileSystemControl	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Control: FSCT...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	NAME NOT FOUND	
15:22:42.9...	Malware_U3_W2_L2.exe	1124	ReadFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Offset: 16,384
15:22:42.9...	Malware_U3_W2_L2.exe	1124	ReadFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Offset: 4,096
15:22:42.9...	Malware_U3_W2_L2.exe	1124	ReadFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Offset: 20,480
15:22:42.9...	Malware_U3_W2_L2.exe	1124	ReadFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratic...	SUCCESS	Offset: 40,960
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryStandardInformationFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\AppPatch\sysstet.sdb	NAME NOT FOUND	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Acces...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: Sy...
15:22:42.9...	Malware_U3_W2_L2.exe	1124	QueryStandardInformationFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize...

Notiamo che ci sono parecchie operation di tipo “create file”, quindi andiamo a filtrare ulteriormente per questo tipo di operation:

l'accesso ai file di registro al percorso

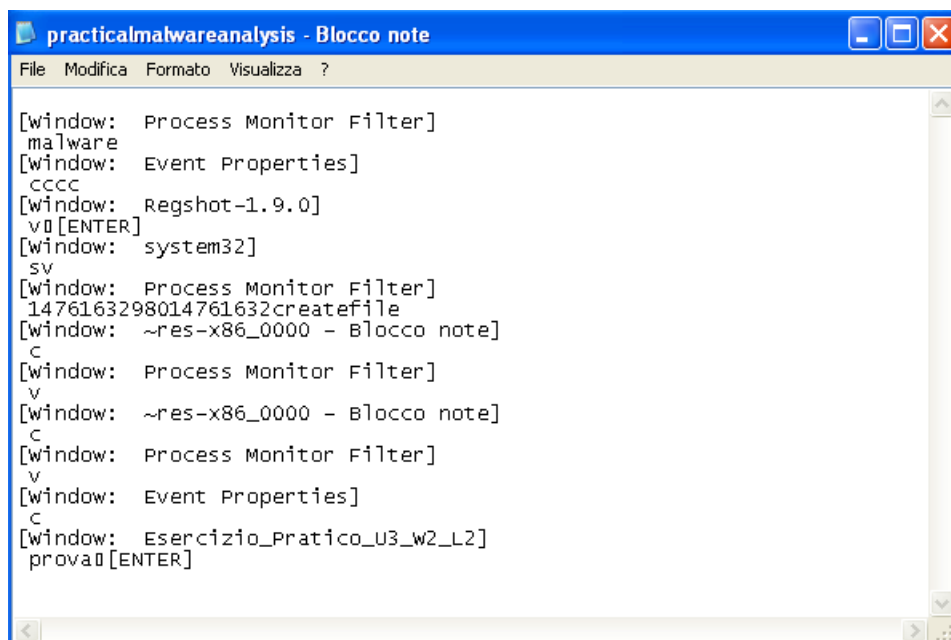
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes\

ad esempio potrebbe far sì che il malware usi queste informazioni per non venire rilevato dalle policy di sicurezza del sistema

Infine notiamo che il malware usa queste impostazioni per creare dei log su blocco note che salva nella stessa cartella di avvio dello stesso, come possiamo notare dalla riga selezionata:

15.22.42.9...	Malware_U3_W2_L2.exe	1124	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-0A1820CD.pf	NAME NOT FOUND	Desired Access: G
15.22.42.9083175	Malware_U3_W2_L2.exe	1124	CreateFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: E
15.22.42.9...	Malware_U3_W2_L2.exe	1124	FileSystemControl	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Control: FSCTL_15
15.22.42.9	Malware_U3_W2_L2.exe	1124	OpenFile	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe.log	NAME NOT FOUND	

Aprendo questo file ci accorgiamo che gli eventi fatti dall'utente vengono loggati su tale file di testo, ad esempio vediamo come il malware abbia rilevato l'apertura di process monitor ed i filtri applicati. Ho infine creato una cartella di prova per confermare tale ipotesi:



```
practicalmalwareanalysis - Blocco note
File  Modifica  Formato  Visualizza  ?

[window: Process Monitor Filter]
malware
[window: Event Properties]
cccc
[window: Regshot-1.9.0]
v0 [ENTER]
[window: system32]
sv
[window: Process Monitor Filter]
1476163298014761632createfile
[window: ~res-x86_0000 - Blocco note]
c
[window: Process Monitor Filter]
v
[window: ~res-x86_0000 - Blocco note]
c
[window: Process Monitor Filter]
v
[window: Event Properties]
c
[window: Esercizio_Pratico_U3_W2_L2]
prova0 [ENTER]
```

Il comportamento sembra quindi quello di uno spyware