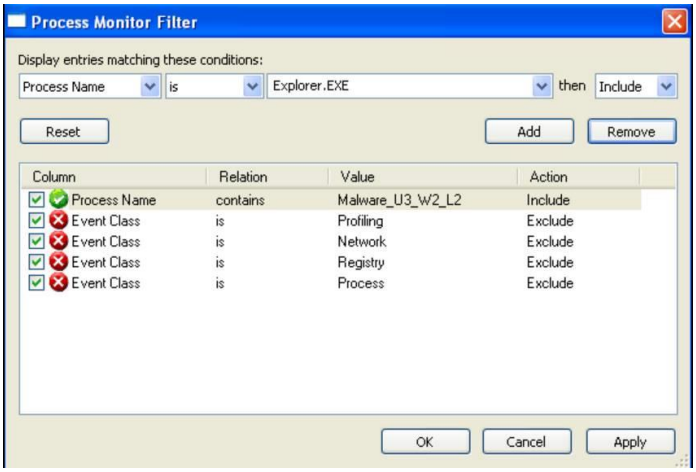
Esercizio 2 Settimana 10

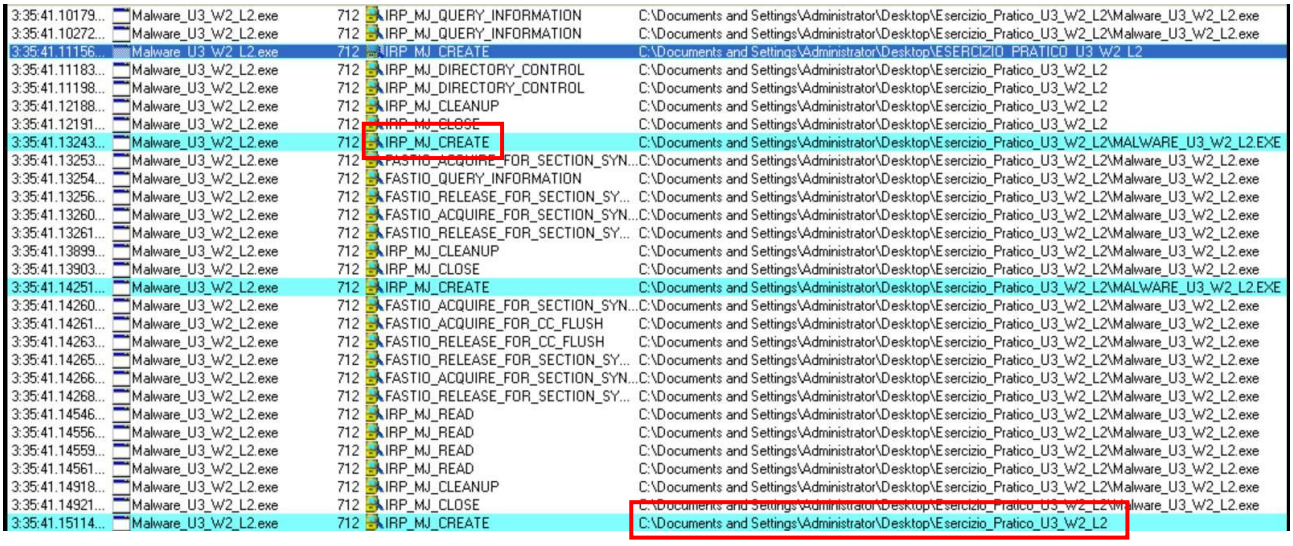
Analisi Dinamica Base

Al fine di analizzare il Malware dato, andiamo ad aprire ProcessMonitor (procmon) sulla nostra macchina vittima. Esso è un tool avanzato per Windows che 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. Una volta eseguito, procmon andrà a catturare diversi eventi in esecuzione e, per questo, si consiglia di avviarlo prima del nostro Malware. In questo caso andremo ad includere solo le tipologie di eventi che interessano il File System, i processi e thread e il registro attività.
Andiamo a configurare procmon come in figura inserendo tra i filtri il nome del file malevolo:



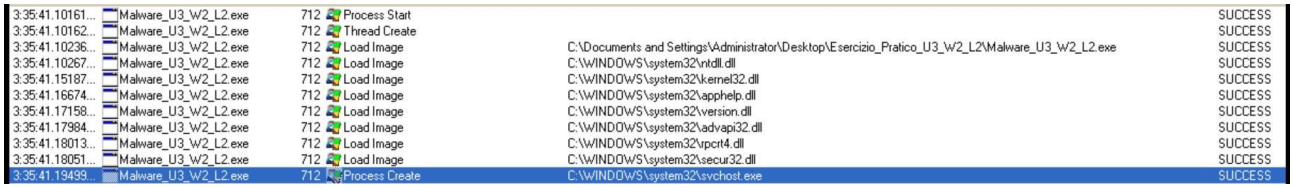
FILE SYSTEM ACTIVITY

Dalla figura sotto possiamo notare come procmon abbia filtrato i dati e ci mostri le chiamate, in particolare alla funzione IRP_MJ_CREATE che viene utilizzata nei driver Windows per la creazione di file o di comunicazione tra driver e applicativo. Inoltre notiamo che l'eseguibile sta agendo proprio sul path noto della cartella con il Malware all'interno.



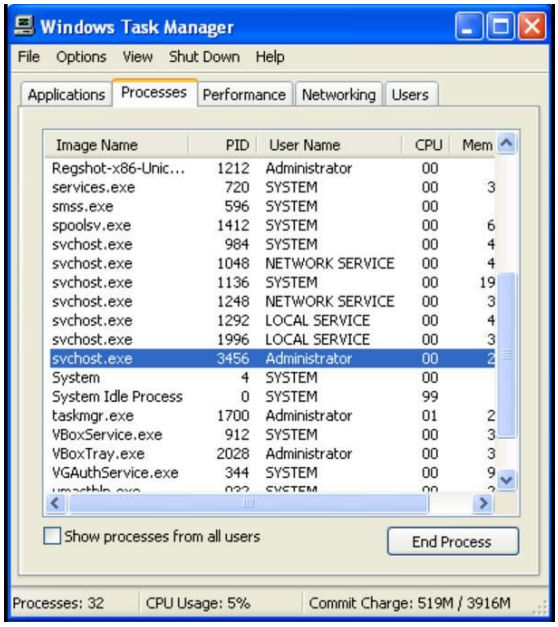
PROCESSI E THREAD

Per quando riguarda l'analisi su processi e thread, possiamo notare come il file malevolo crei un thread all'interno del PID explorer.exe, importi tutte le librerie necessarie ed, infine, crei un processo di sistema che ospita e gestisce determinati servizi nominato SVCHOST.EXE con relativo PID.



3:35:41.10161...	Malware_U3_W2_L2.exe	712	Process Start		SUCCESS
3:35:41.10162...	Malware_U3_W2_L2.exe	712	Thread Create		SUCCESS
3:35:41.10236...	Malware_U3_W2_L2.exe	712	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS
3:35:41.10267...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
3:35:41.15187...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS
3:35:41.16674...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS
3:35:41.17158...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS
3:35:41.17984...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
3:35:41.18013...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\vpcrt4.dll	SUCCESS
3:35:41.18051...	Malware_U3_W2_L2.exe	712	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
3:35:41.19499...	Malware_U3_W2_L2.exe	712	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS

```
Parent PID: 1832, Command line: "C:\Documents and Settings\Admini
Thread ID: 3368
Image Base: 0x400000, Image Size: 0xd000
Image Base: 0x7c900000, Image Size: 0xaf000
Image Base: 0x7c800000, Image Size: 0xf6000
Image Base: 0x77b40000, Image Size: 0x22000
Image Base: 0x77c00000, Image Size: 0x8000
Image Base: 0x77dd0000, Image Size: 0x9b000
Image Base: 0x77e70000, Image Size: 0x92000
Image Base: 0x77fe0000, Image Size: 0x11000
PID: 3456, Command line: "C:\WINDOWS\system32\svchost.exe"
Thread ID: 3368, User Time: 0.0000000, Kernel Time: 0.0468750
Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.046875
```



Abbiamo testato che con la chiusura forzata del processo, anche il nostro Malware smette di funzionare.

CONCLUSIONI

Tramite l'analisi appena descritta possiamo intuire il comportamento del file. In base alla correlazione tra operation e path, siamo andati ad ispezionare la cartella del Malware e ci siamo imbattuti in un file .txt che prima non era presente; all'interno notiamo come siano riportati gli input di tutte le ricerche eseguite sui nostri programmi quando era necessario inserire manualmente dei filtri tramite l'utilizzo della nostra tastiera.

Il Malware può quindi essere classificato come un tipo KeyLogger: esso è un tipo di software progettato per registrare e monitorare le tastiere di un computer, catturando e memorizzando le informazioni digitate dagli utenti.