Malware analysis

Sommario

Traccia S10/L2

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
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra «operation» e Path

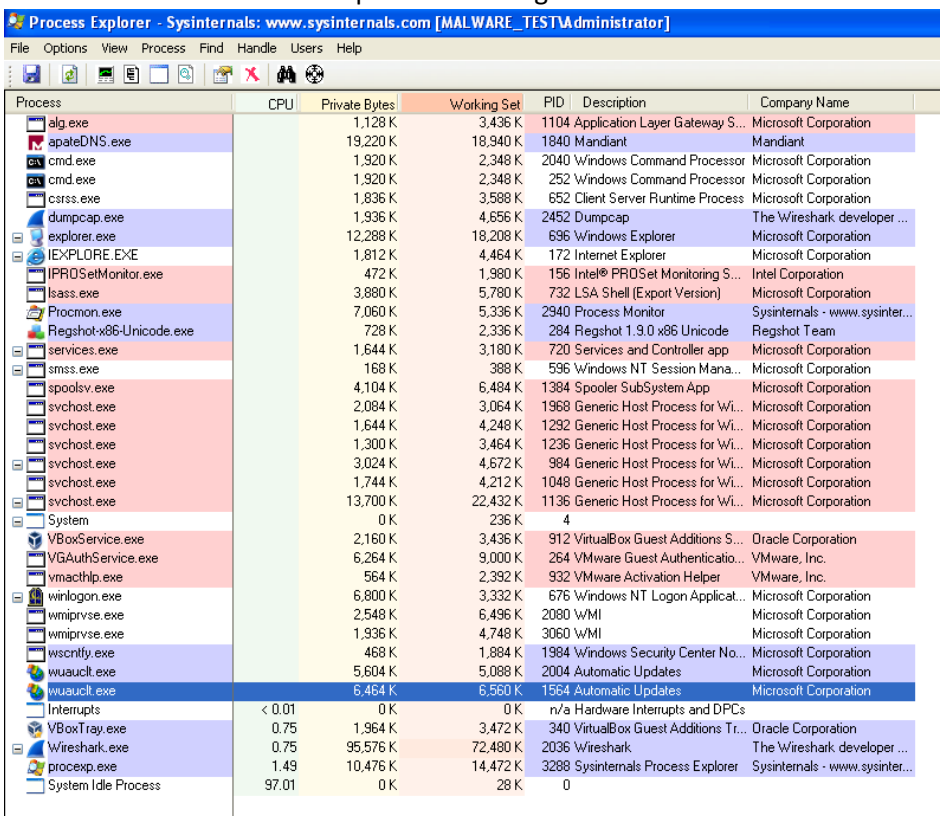
Per svolgere questo esercizio utilizzerò vari tool tra cui:

- Process Explorer, un tool che permette l'analisi dettagliata di tutti i processi in esecuzione su un sistema.
- 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.

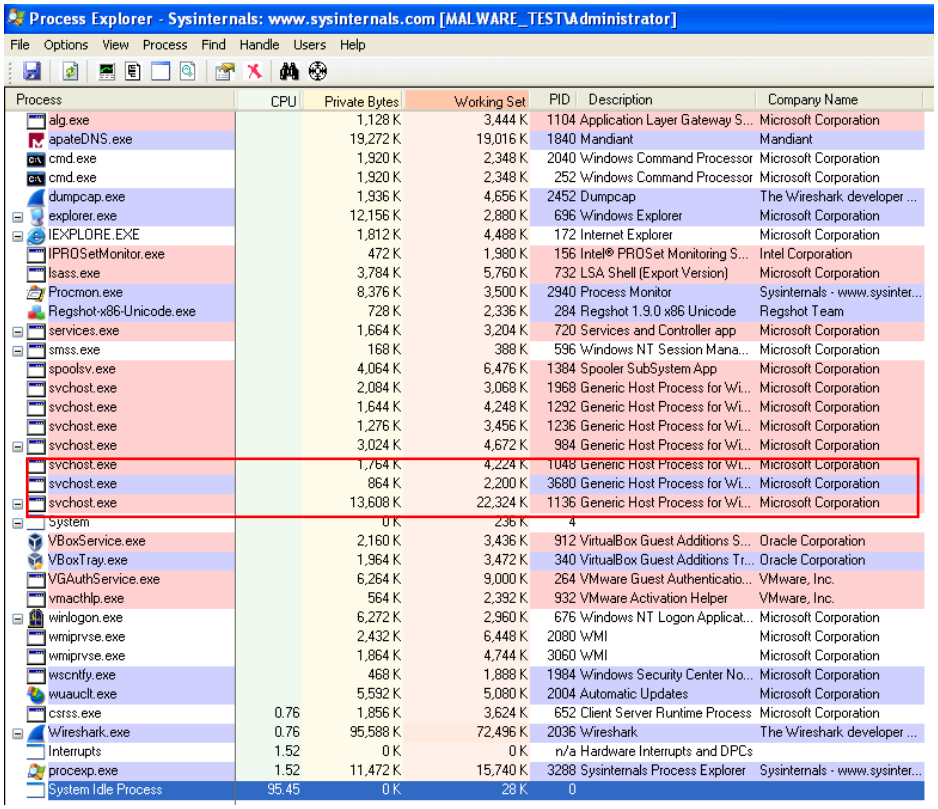
Analisi dei processi e del file system

Avviamo la cattura di process monitor e controlliamo process explorer prima dell'avvio del malware

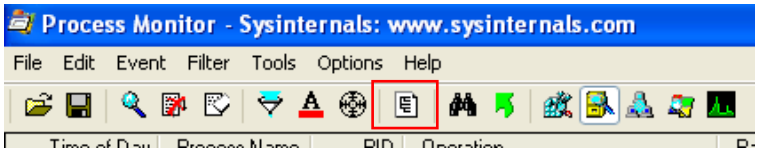
Inizialmente la situazione dei processi è la seguente:



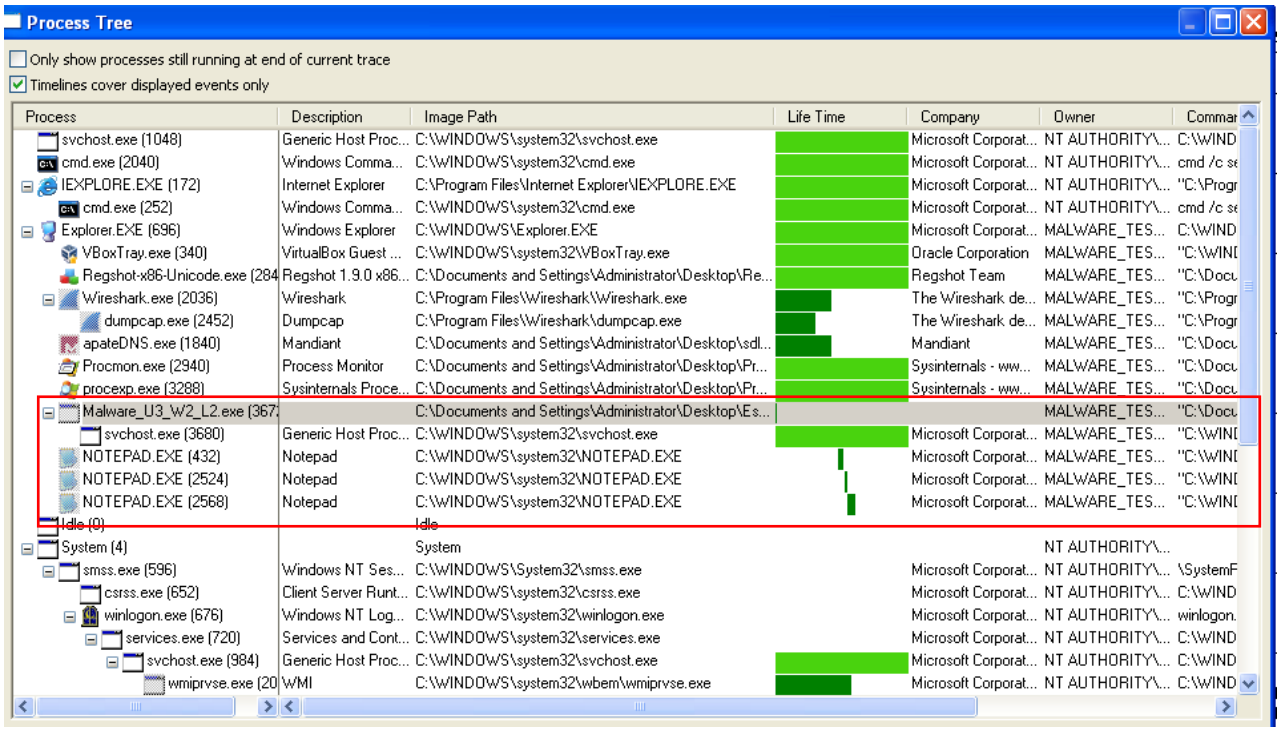
Dopo l'avvio del malware possiamo notare un nuovo processo con PID 3680 camuffato con un nome generico di un processo Windows



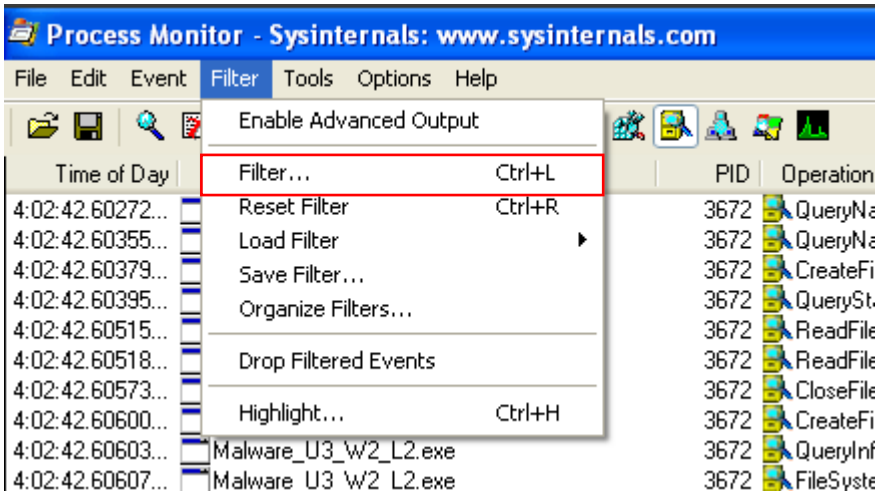
Ora andiamo su process monitor e clicchiamo su process tree

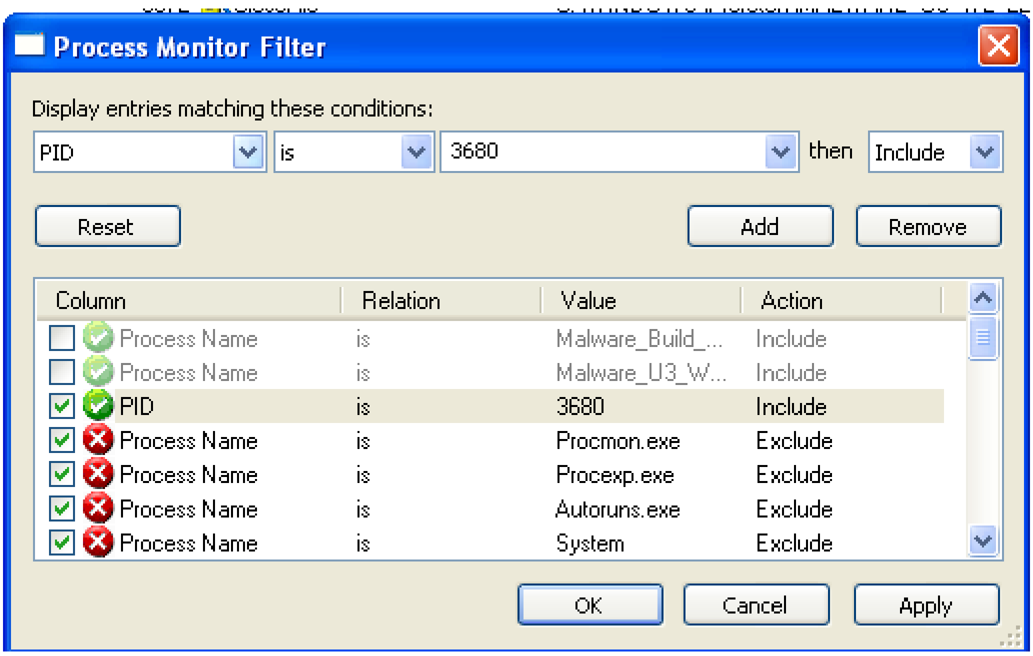


Possiamo notare che il processo svchost.exe è figlio del processo padre del malware. Notiamo anche i processi del blocco note, nonostante non sia mai stato avviato direttamente.

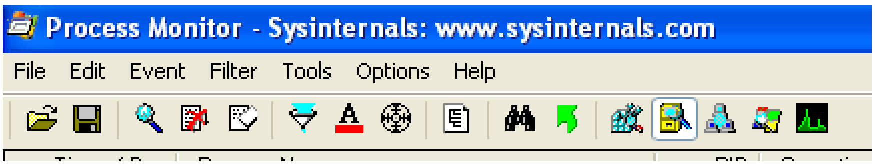


Procediamo con l'analisi di questo processo. Andiamo su filtri e applichiamo un filtro per il processo con pid 3680

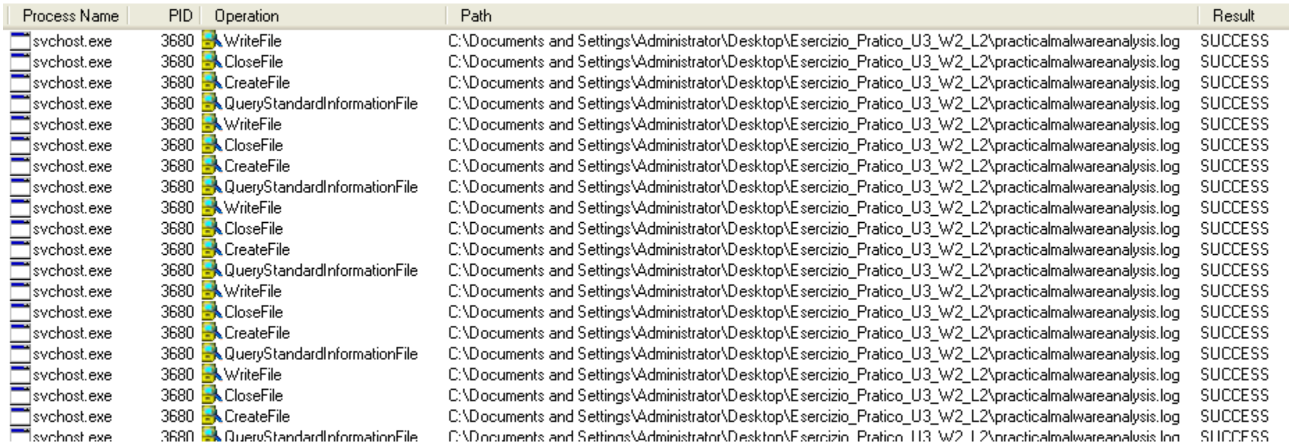




Selezioniamo il filtro per visualizzare solo le attività sul file system

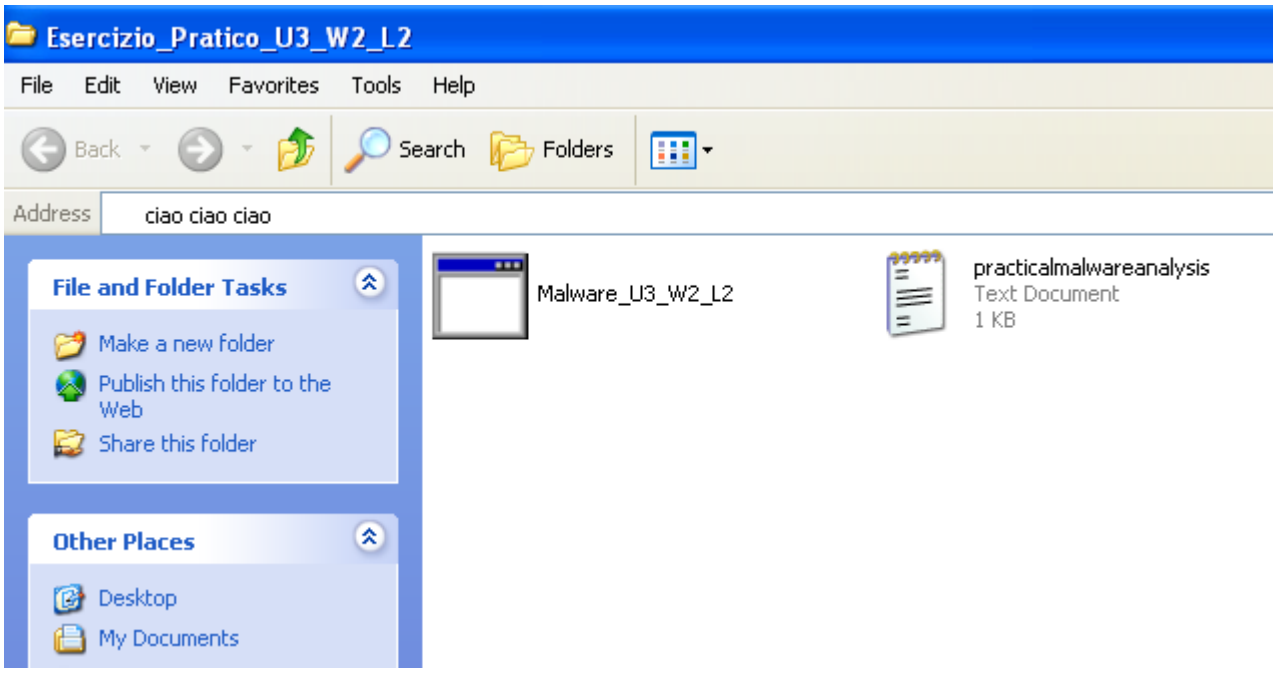


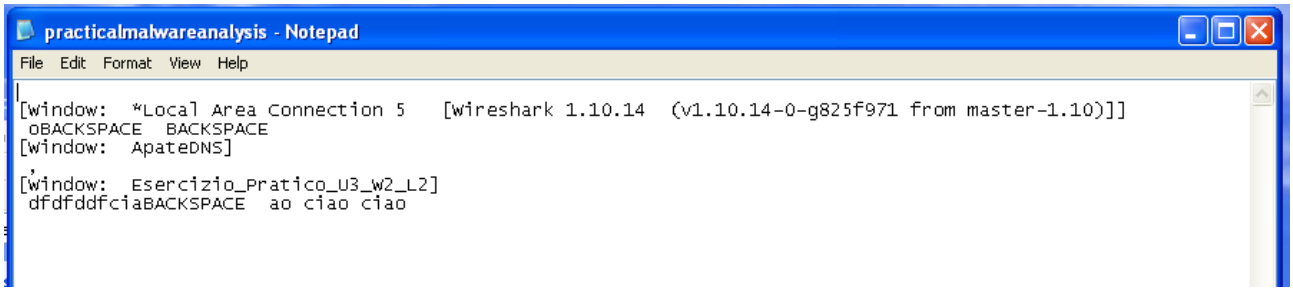
Possiamo notare che questo processo figlio crea un log all'interno della cartella in cui è presente il malware



Process Name	PID	Operation	Path	Result
svchost.exe	3680	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	WriteFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS
svchost.exe	3680	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\practicalmalwareanalysis.log	SUCCESS

Infatti, andando nella cartella è stato creato un file txt con all'interno delle stringhe che sembrano gli input della tastiera.





A quanto pare ci troviamo davanti ad un keylogger!