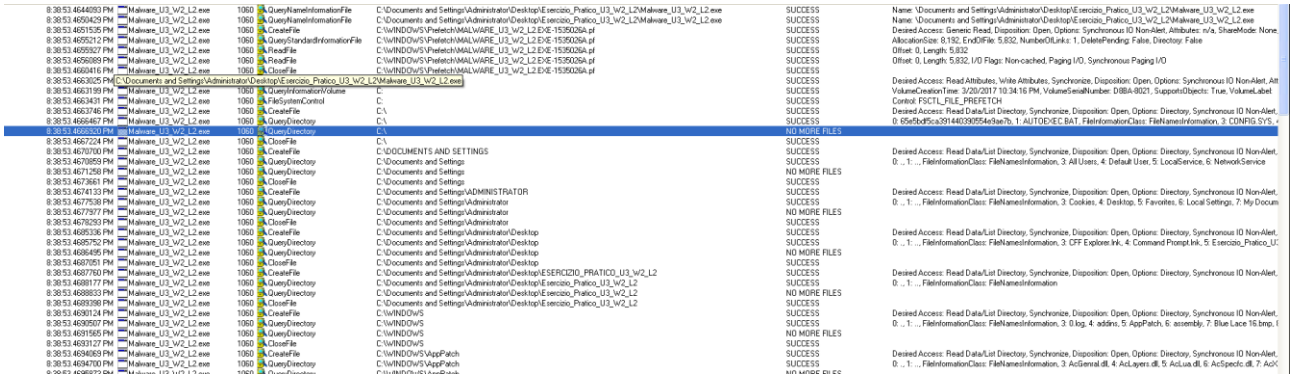
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

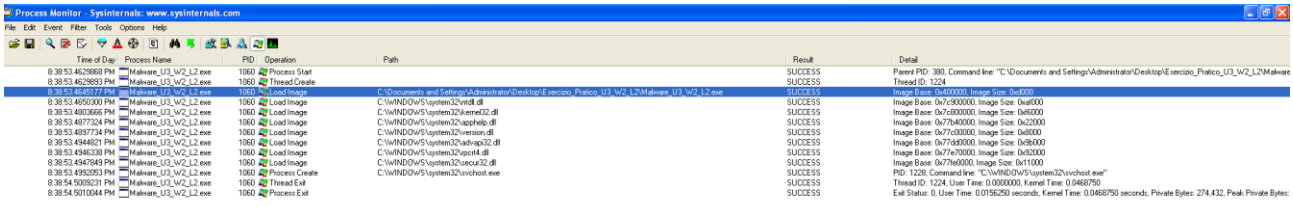
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

Notiamo una serie di cambiamenti sul file system, creazione file, rimozione in varie directories

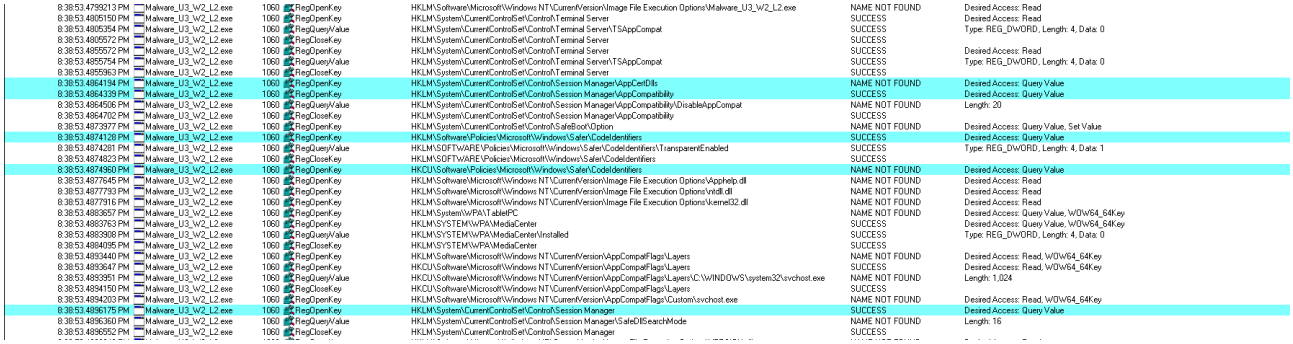


- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

Notiamo come il malware abbia lanciato una serie di processi:



- Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (le differenze)



Traccia:

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:

2 Identificare eventuali azioni del malware sul file system utilizzando multimon https://www.resplendence.com/multimon

D Identificare eventuali altre azioni del malware

0 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).

Creare istantanea da Virtualbox della macchina Windows XP prima di iniziare per poter ripristinare in caso di problemi (o al limite fare il clone)