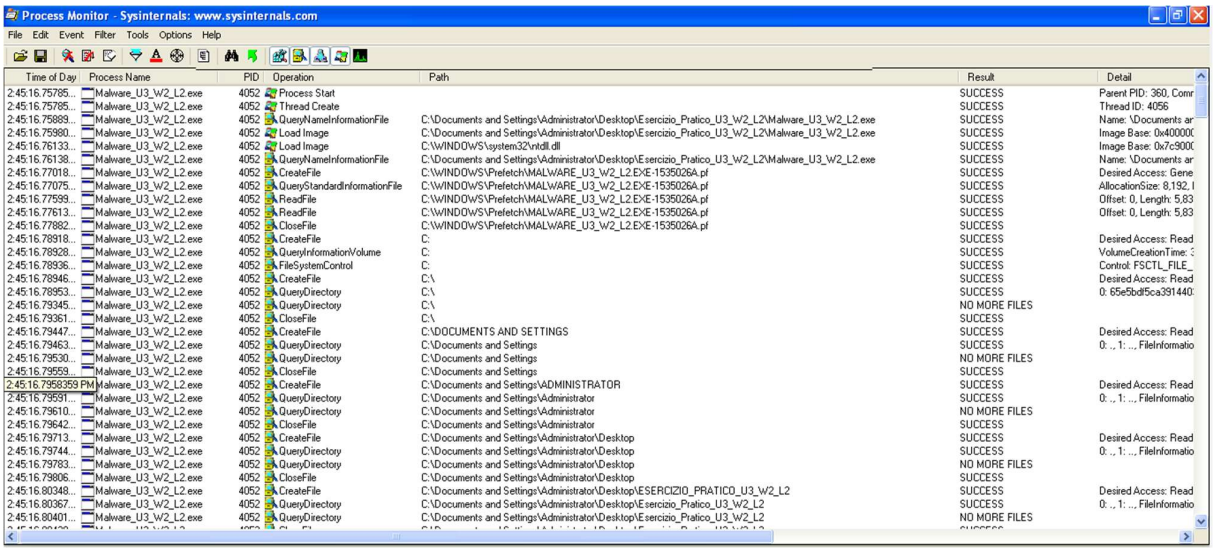
ESERCIZIO S10-L2

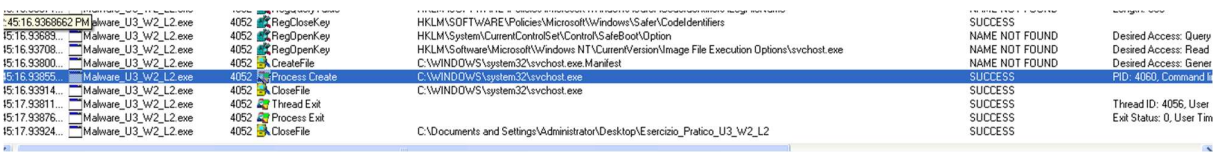
Lo scopo dell'esercizio è quello di effettuare un'analisi dinamica basica su un malware presente nella macchina virtuale e rispondere ai seguenti quesiti:

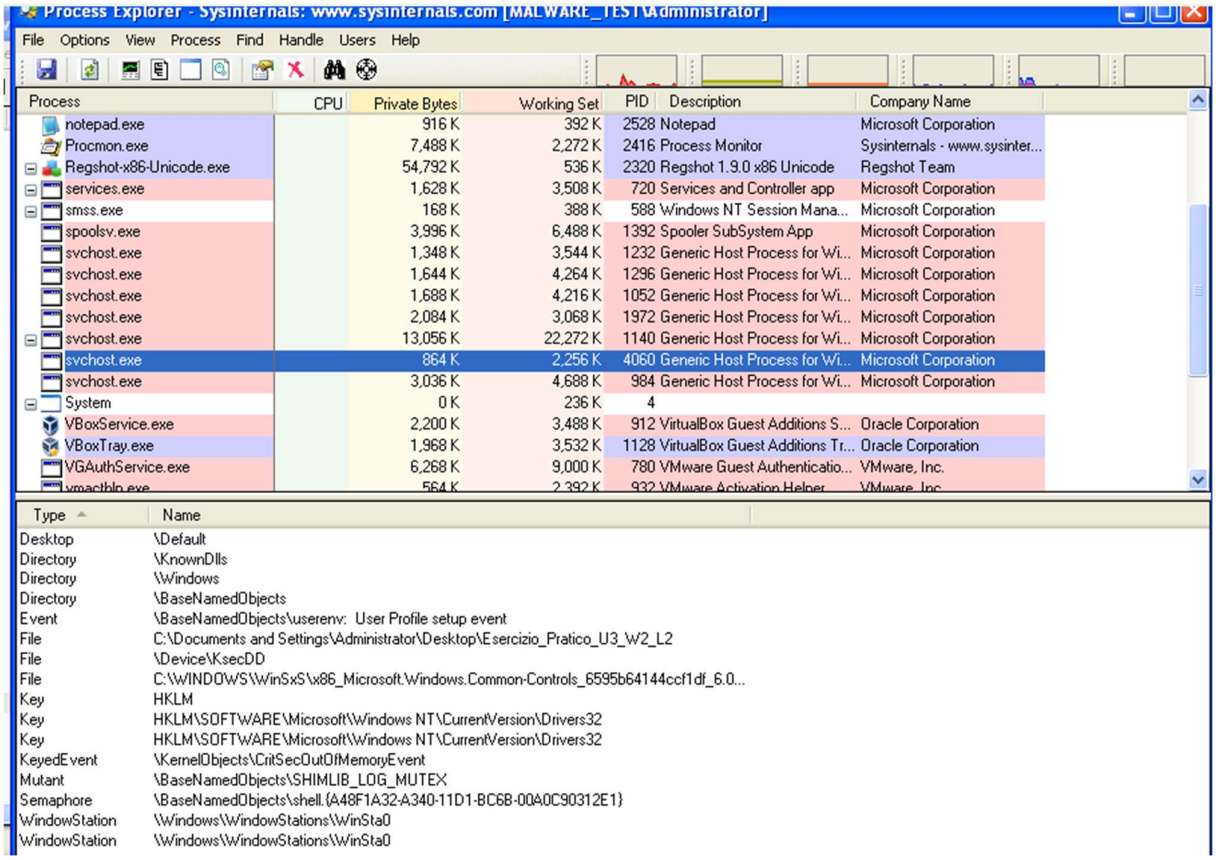
- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor
- Identificare eventuali azioni del malware su processi e thread utilizzando ProcessMonitor
- Modifiche del registro dopo il malware (le differenze)
- Provare a profilare il malware in base alla correlazione tra operation e path.

Per identificare azioni del malware sul file system, ho filtrato i processi mettendo il nome del malware, in questo modo vedrò solo le entry del processo indicato, in questo modo si vede che fa delle azioni quali "createfile", "writefile" e "closefile".



Inoltre vediamo che crea un processo "svchost" apparentemente innocuo. Il malware fa questa azione per nascondersi.





Se filtriamo il pid 4060 notiamo che viene scritto continuamente un file “practicemalwareanalisys” che si trova nella stessa cartella del malware, aprendo questo file vediamo che compare il pid che avevo inserito, quindi si presuppone che sia un keylogger, cioè un malware che prende tutto quello che digito.