S10L2.

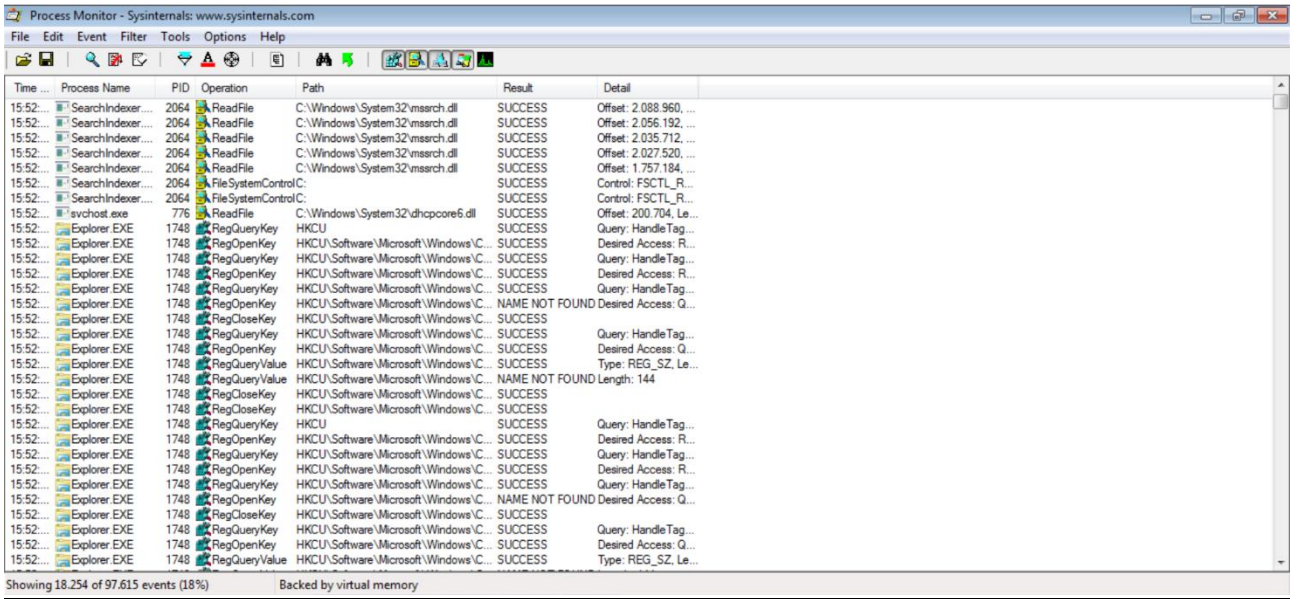
BENVENUTI LUIGI

Traccia:

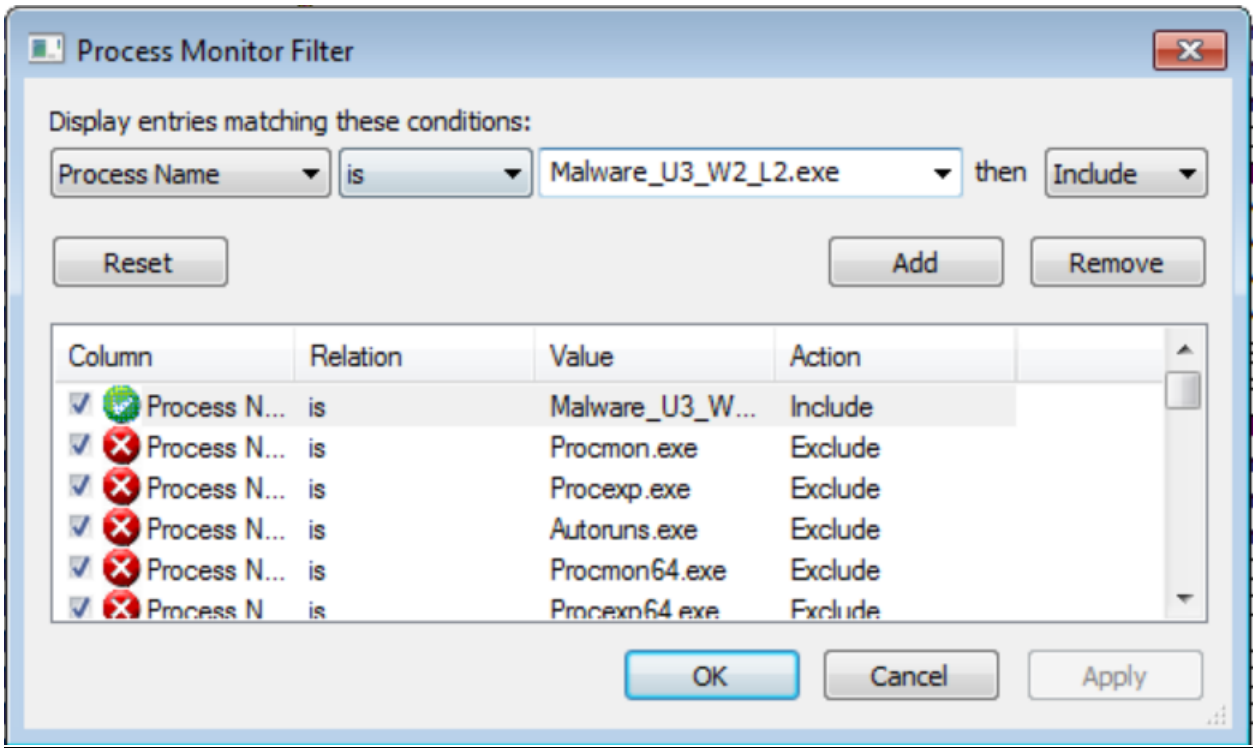
Configurare la macchina virtuale per l'analisi dinamica (il malwaresarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul file system utilizzando ProcessMonitor (procmon) .
- 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.

Procmon:



Procmon (filter):



Il malware è dunque un **keylogger**, in grado di generare un file di testo e salvare al suo interno i tasti digitati dall'utente.

RegShot: