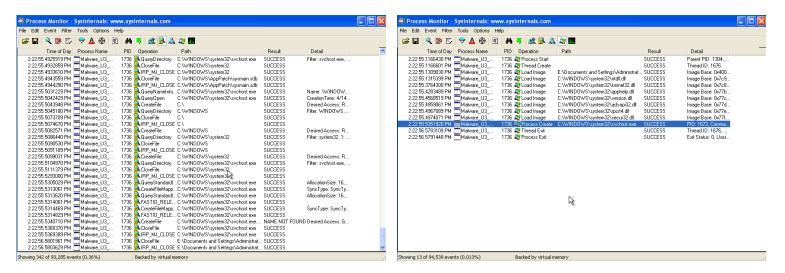
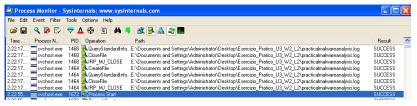
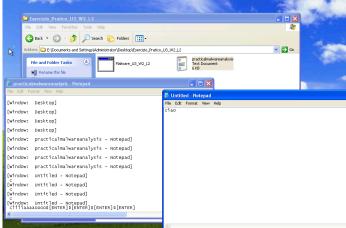
2. Malware analysis: Analisi dinamica basica

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2»

- Process Monitor







Il malware crea un Process Monitoring che mostra in tempo reale le operazioni effettuate sul computer.

In questo caso dagli screen possiamo vedere come una volta avviato il malware, esso sfrutti un processo diverso per camuffarsi e creare un file dal nome practicalmalwareanalysis.log all'interno della stessa cartella dove risiete il malware.

Il processo sfruttato, svchost.exe, è parte integrante del sistema operativo per la sua corretta funzione. Il malware lo sfrutta per nascondersi al suo interno e sfruttarlo.

Testando il programma possiamo vedere come in figura, come il kaylogger ci restituisca la scritta ciao nel file creato.