Esercizio 2 Settimana 10

Oggi andremo ad effettuare un’analisi dinamica di un malware. A differenza di quella statica, l’analisi dinamica va ad analizzare un malware eseguendo lo stesso (in ambiente protetto) in modo tale da poter capire il comportamento e le funzionalità del malware.

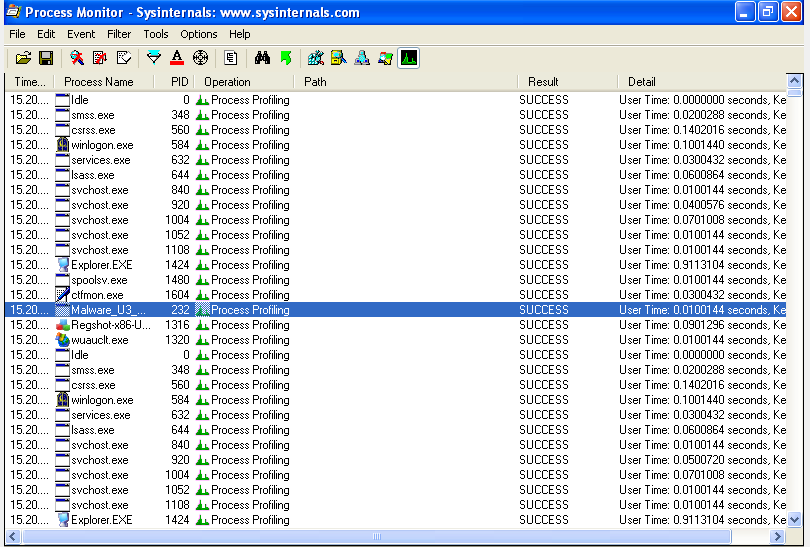
Partiamo avviando alcuni programmi che ci saranno utili:

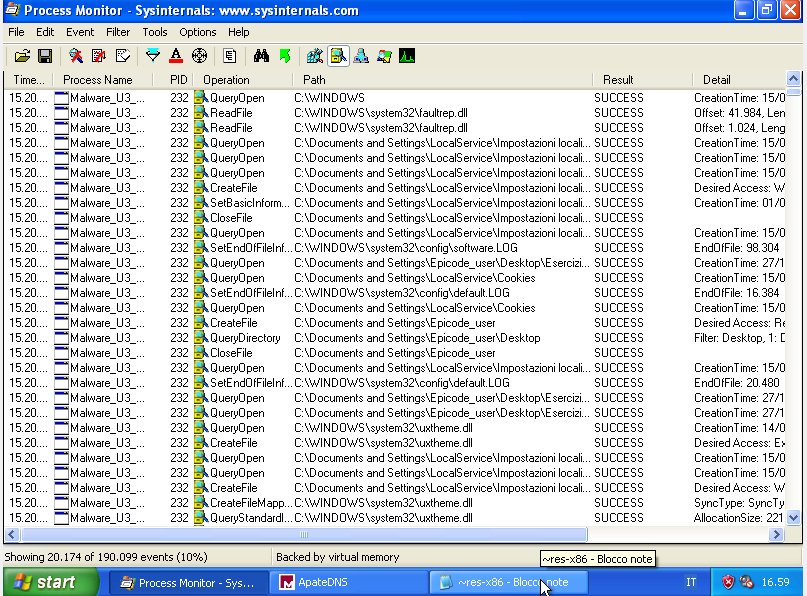
* Process Monitor;
* RegShot.

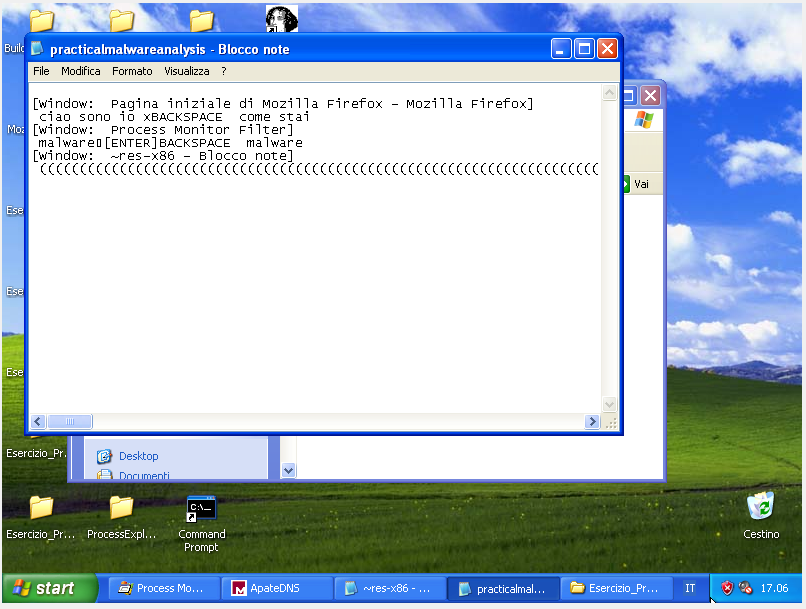
Il primo ci servirà per tenere traccia di tutti i processi in esecuzione sulla nostra macchina virtuale, il secondo ci servire per confrontare le differenze delle chiavi di registro una volta che avvieremo il malware.

Una volta avviati i nostri programmi, procederemo all’esecuzione del malware.

Potremo notare, dopo un po’ che esso sarà in esecuzione, i seguenti risultati su Process Monitor:





Tra le varie voci presenti, notiamo che è presente nel percorso dello stesso malware una query “Create file” con stato success. Possiamo quindi dedurre che il malware ha creato un file a nostra insaputa e, indagando, noteremo che il file è stato salvato allo stesso percorso in cui è presente il malware. Dopo alcune prove, sono riuscito a capire che il malware è un keylogger, in quanto va a memorizzare i tasti che premo su tastiera all’interno del file.