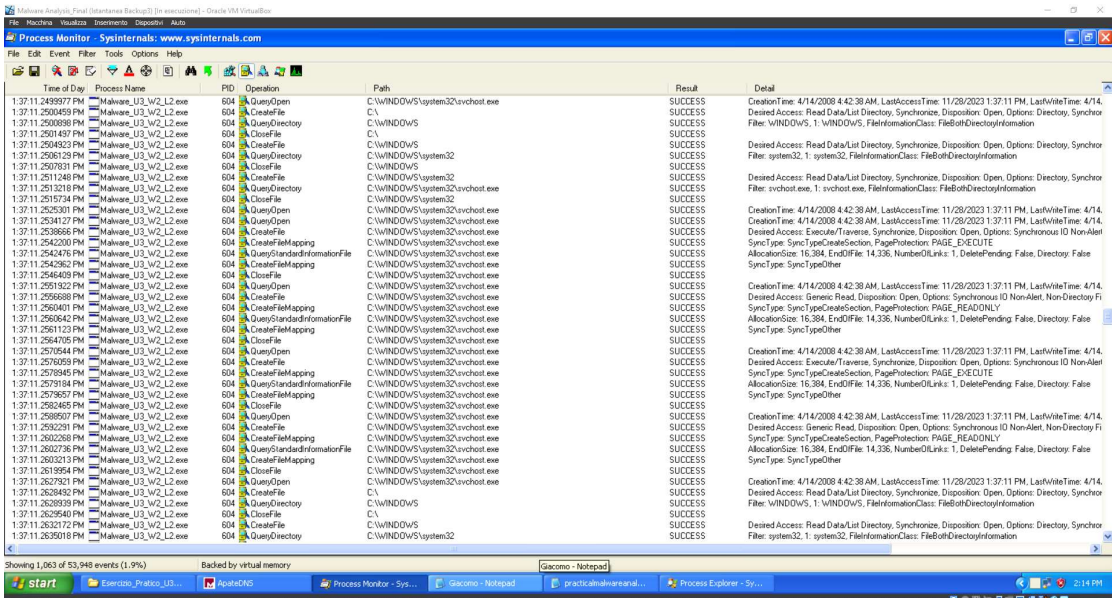
Pratica S10-L2 Analisi dinamica basica

L'esercizio di oggi consiste nell'analizzare un malware attraverso un'analisi dinamica.

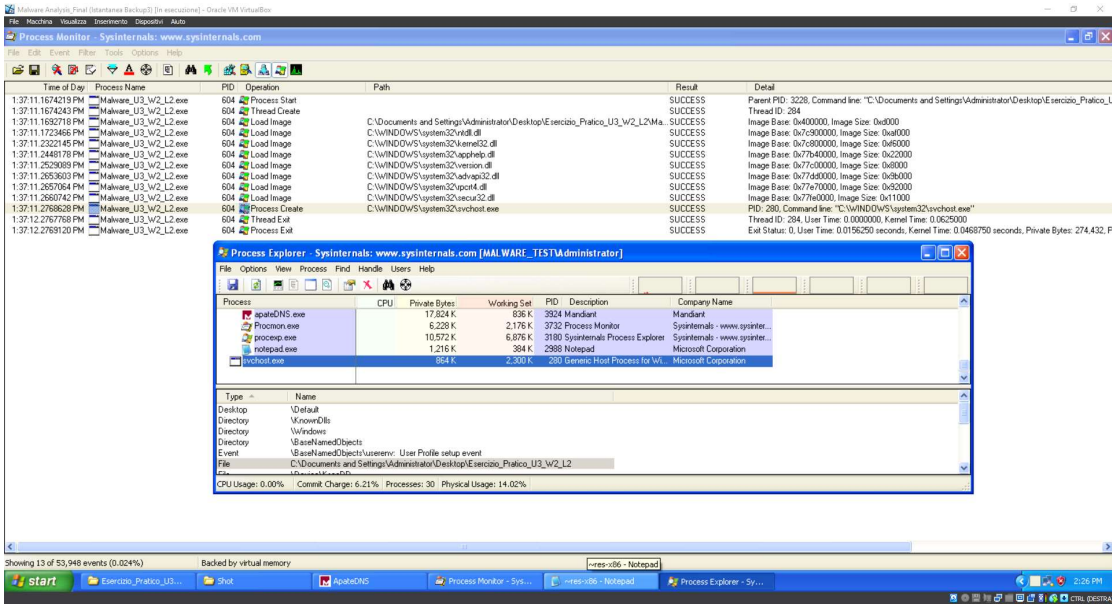
Come tool ho utilizzato Process Monitor e Regshot, una volta avviati i programmi ho lanciato il malware e possiamo vedere i risultati trovati:

1. File system



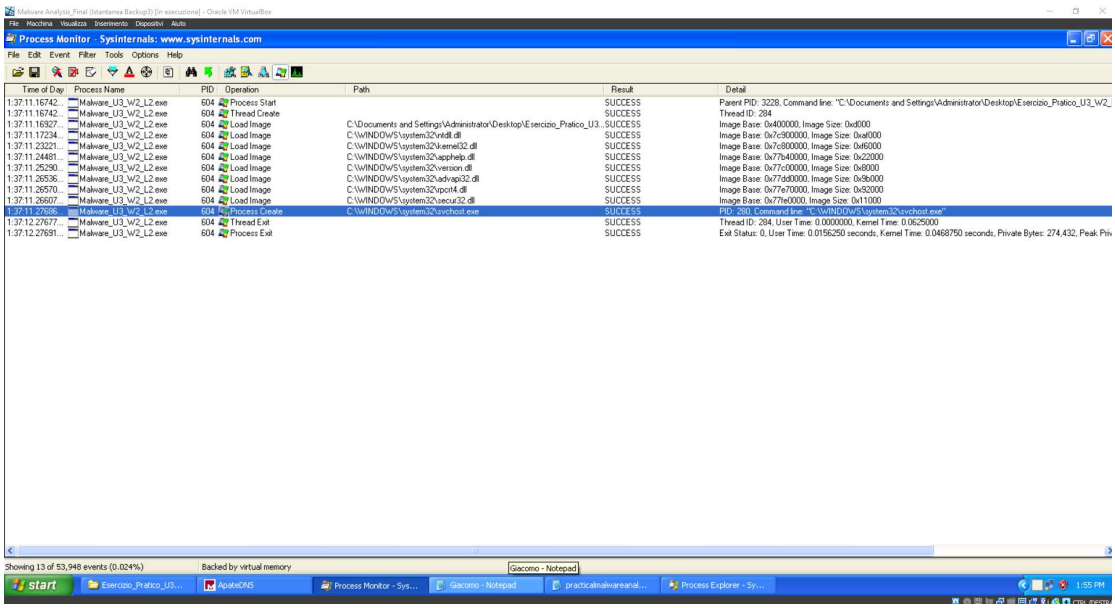
Qui possiamo notare come il malware si è inserito nel nostro pc e ha creato un nuovo processo chiamandosi svchost.exe mascherandosi in mezzo a tanti altri.

Qui sotto un dimostrazione:



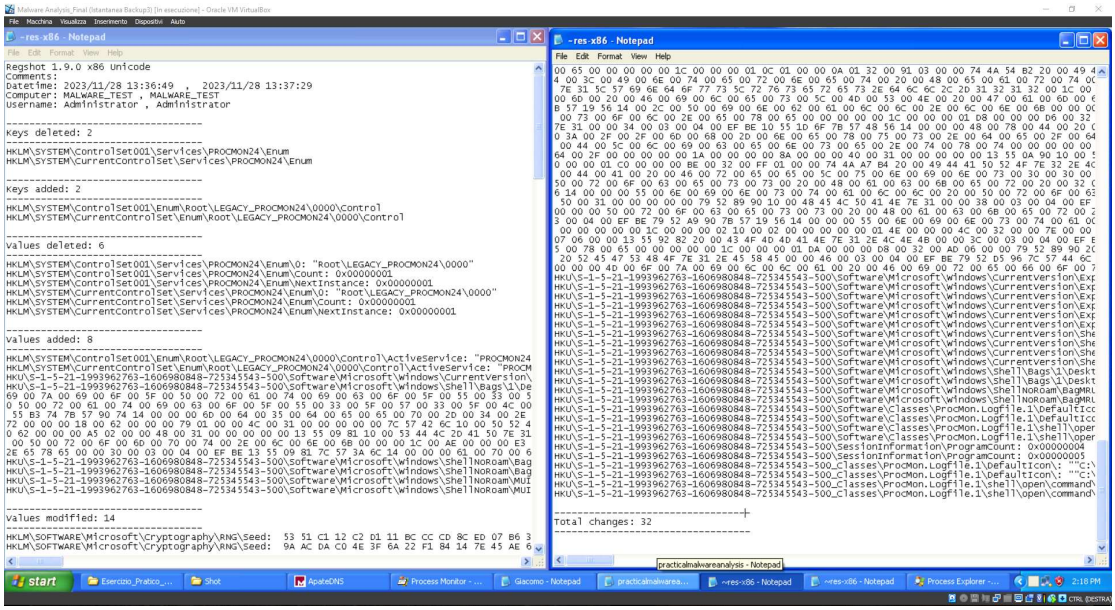
Una volta killato questo processo il malware smette di funzionare e il pc non crasha.

2.Processi e thread



Possiamo vedere come il malware ha creato un processo con l'annesso thread con PID 280, una volta creato il processo rimane attivo finchè non viene killato e/o viene spento il pc.

3. Le modifiche di registro



Questo è il risultato della scansione prima e dopo il lancio del malware tramite Regshot, vediamo che ci sono stati tanti cambiamenti e delle informazioni criptate.

Questo malware è un keylogger e possiamo notarlo perchè dentro la cartella del malware si è creato un file notepad dove teneva registrato tutto ciò che veniva

inserito con la tastiera e le applicazioni aperte.