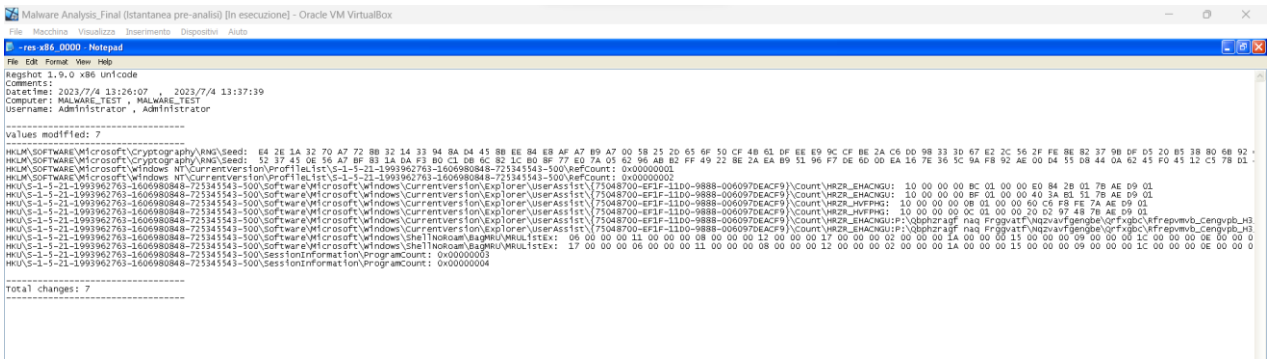
Epicode Unit 3 Week 2

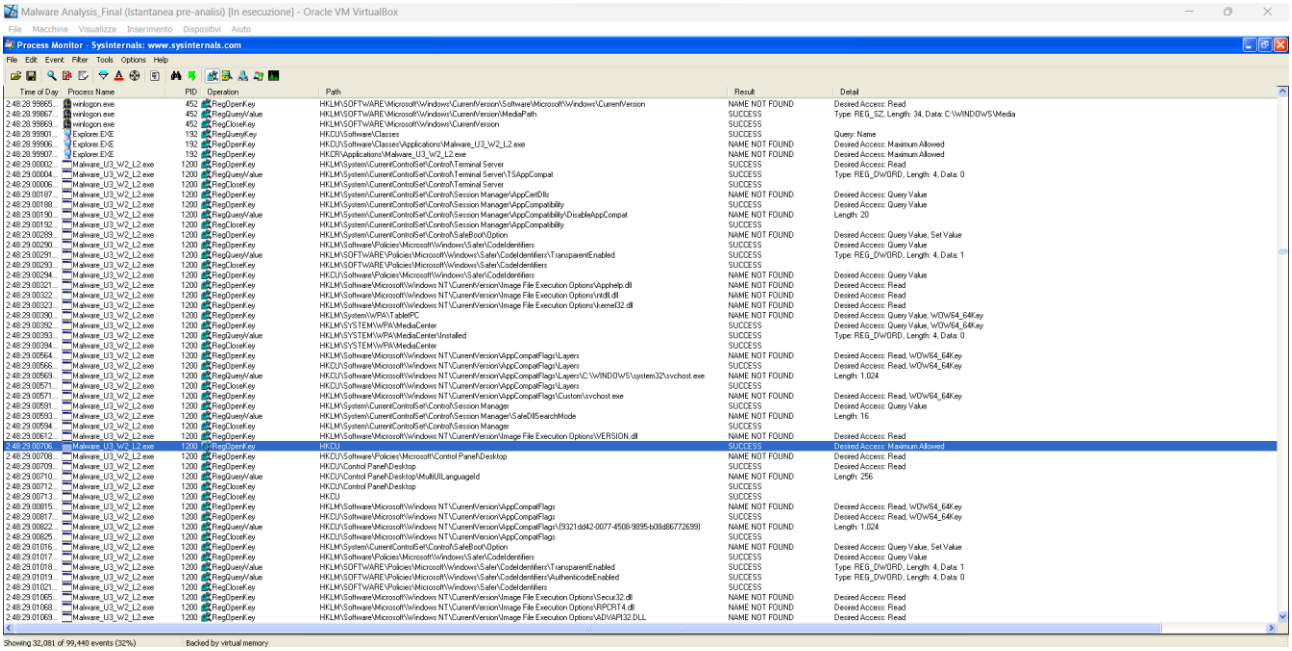
Dynamic Basic Analysis

Nell'esercitazione odierna è richiesto allo studente di analizzare il comportamento di un Malware durante la sua esecuzione.

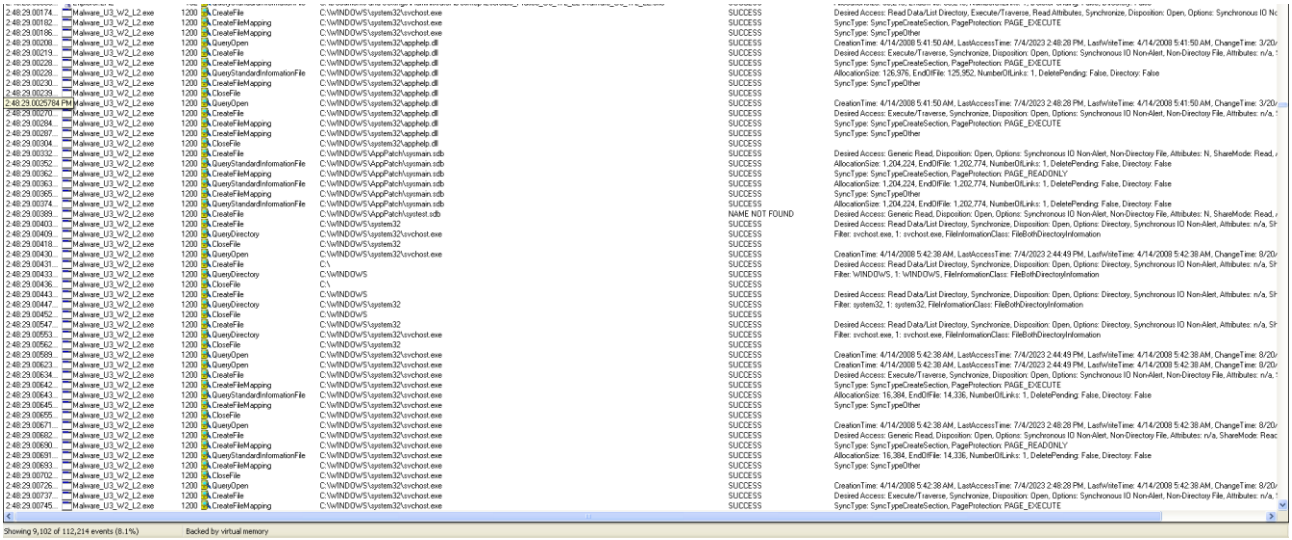
Si procede dunque con l'avvio di Procmon per effettuare tale analisi, iniziando con lo studio di eventuali modifiche alle chiavi di registro, anche eseguendo una comparazione con Regshot.



Il tool evidenzia sette differenze tra lo stato della macchina prima e dopo l'avvio dell'eseguibile da studiare. Si procede dunque allo studio di tali modifiche applicando il filtro dei registri al tool Process Monitor.

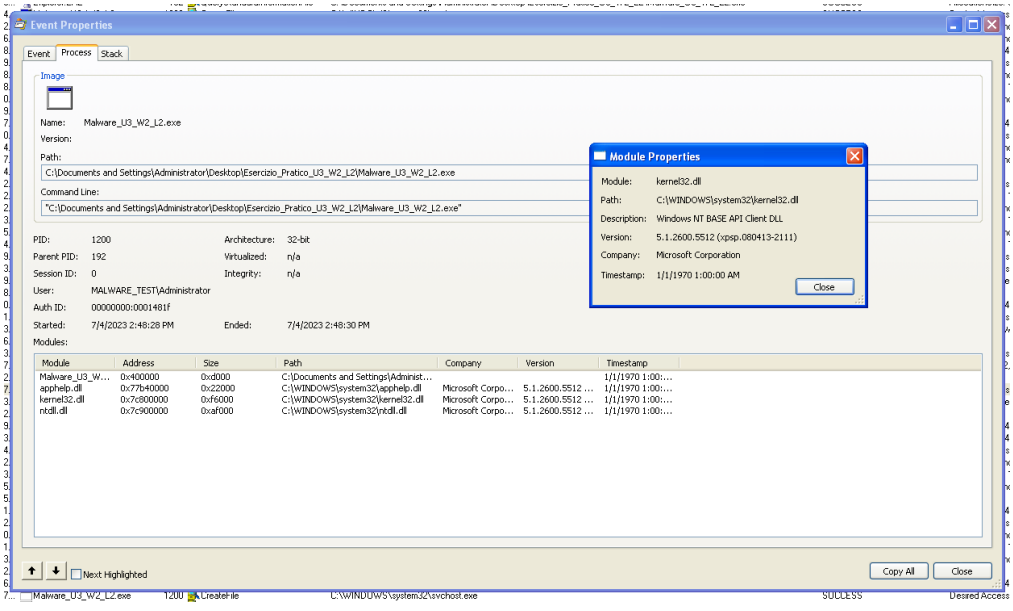


Si procede dunque con lo studio del File System di Windows per cercare di individuare eventuali comportamenti dell'eseguibile.



Come si può notare ancora prima di analizzare i processi nello specifico, il malware crea numerosi file sia su path "nascosti" o specifici del File System Windows, sia nello stesso path in cui esso stesso si trova, tanto che si può notare che dopo l'avvio dell'eseguibile un documeto appare nella stessa cartella (Si può dunque pensare ad un probabile Spyware o Keylogger).

Analizzando più nello specifico i processi, inoltre, possiamo anche individuare ulteriori informazioni circa le azioni e le librerie usate per la creazione dei file, andando via via ricostruendo il comportamento del programma. Si noti in particolare la creazione di SVChost.exe, molto spesso utilizzato dai Malware Programmer per celare i processi malevoli dei loro programmi.



In ultima battuta si procede con l'analisi dei Thread. Utilizzando l'apposito filtro di Process Monitor si può giungere al risultato mostrato nello screen successivo.

Come si può notare, in seguito alla creazione del processo ed ad una serie di "load image", il nuovo processo inizializzato dal malware viene lanciato ("process Start").

Conclusioni:

Alla luce di quanto analizzato, in particolare le modifiche delle chiavi di registro, la creazione del file nel path del malware, il costante aumento dei processi come segnalato da Procmon, potremmo ipotizzare che l'eseguibile in questione sia un worm in continua replicazione. Quello che è sicuro, alla luce del file creato e costantemente aggiornato nel path del malware, è che tale programma funzioni anche come keylogger.