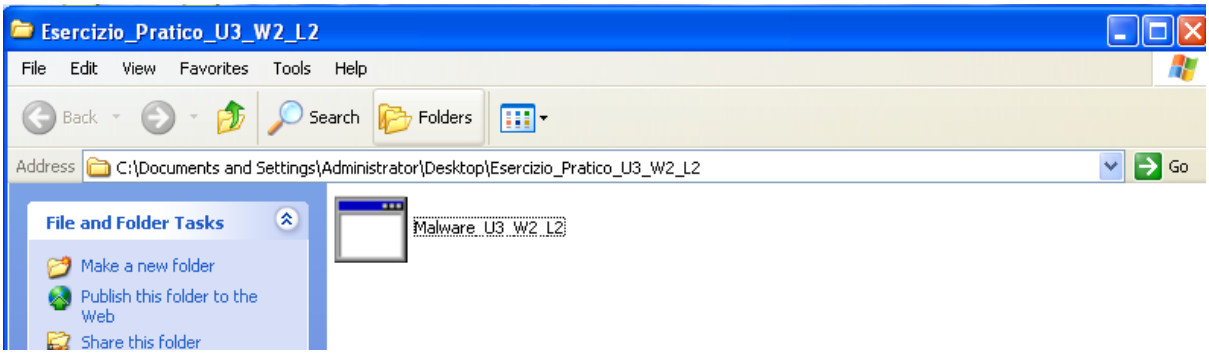
Esercizio 28-03

Traccia: come approfondimento pratico del concetto di analisi dinamica visto in lezione, analizzare il file eseguibile nella cartella “Esercizio_Pratico_U3_W2_L2” presente sul desktop della vostra macchina virtuale dedicata all’analisi dei malware e rispondere ai seguenti quesiti:

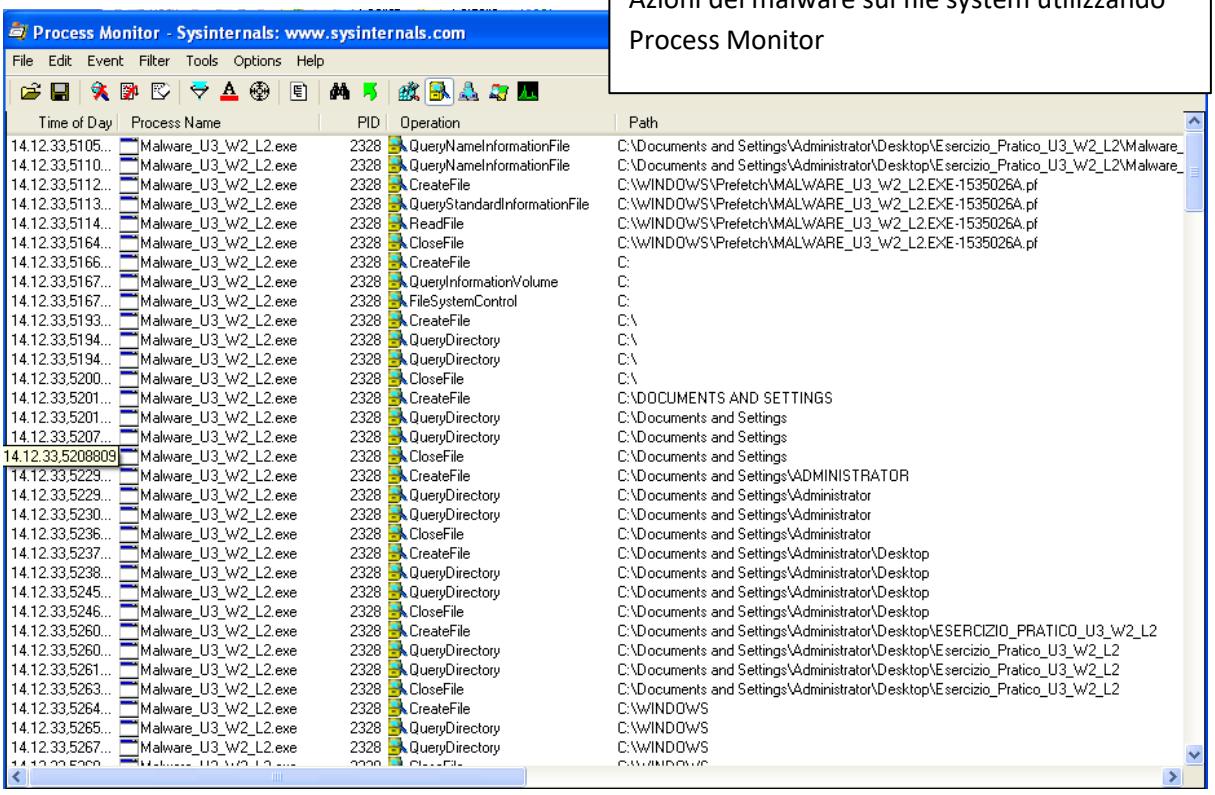
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Provare a profilare il malware in base alla correlazione tra “operation” e Path

Suggerimento: per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione Create File su path noti (ad esempio il path dove è presente l’eseguibile del malware).

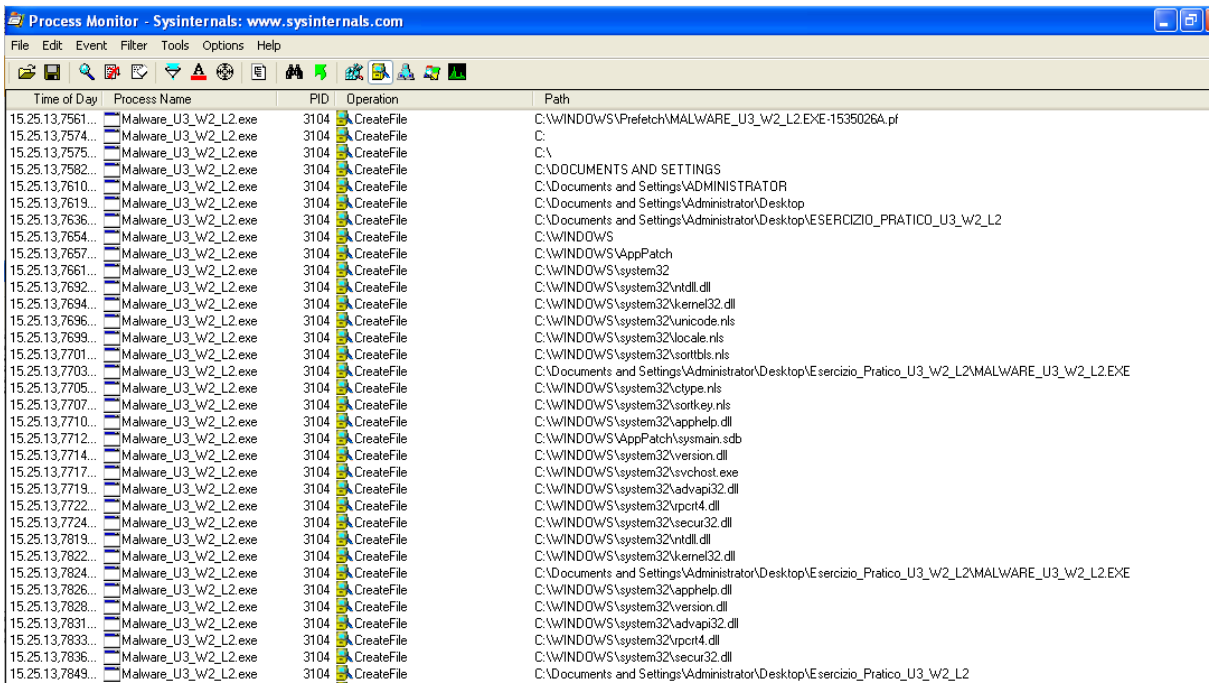
Dopo aver avviato Process Monitor si esegue il malware



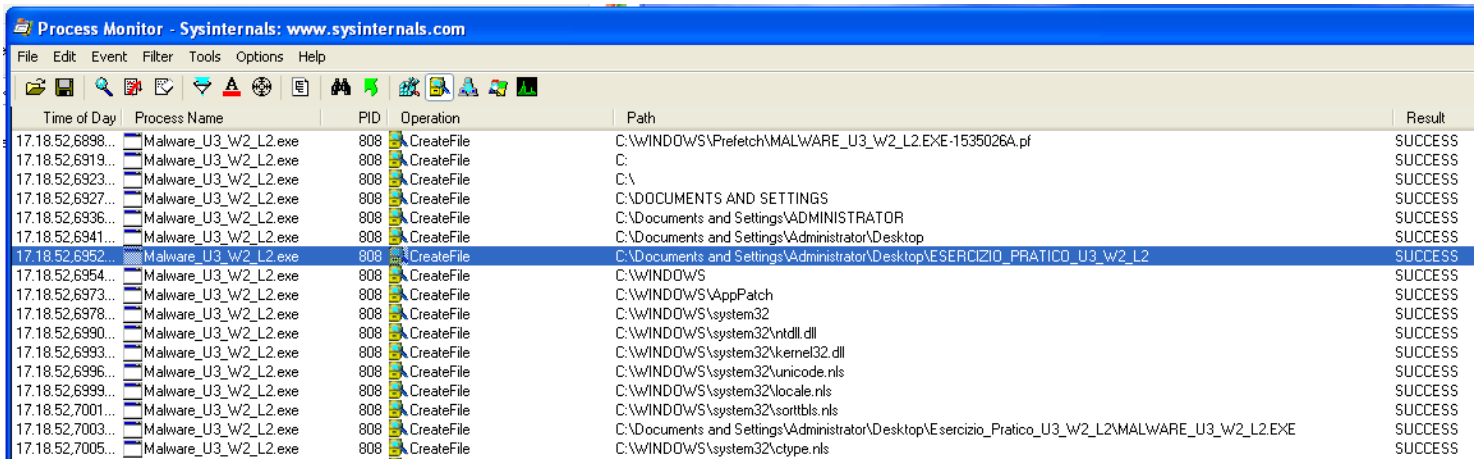
Azioni del malware sul file system utilizzando Process Monitor

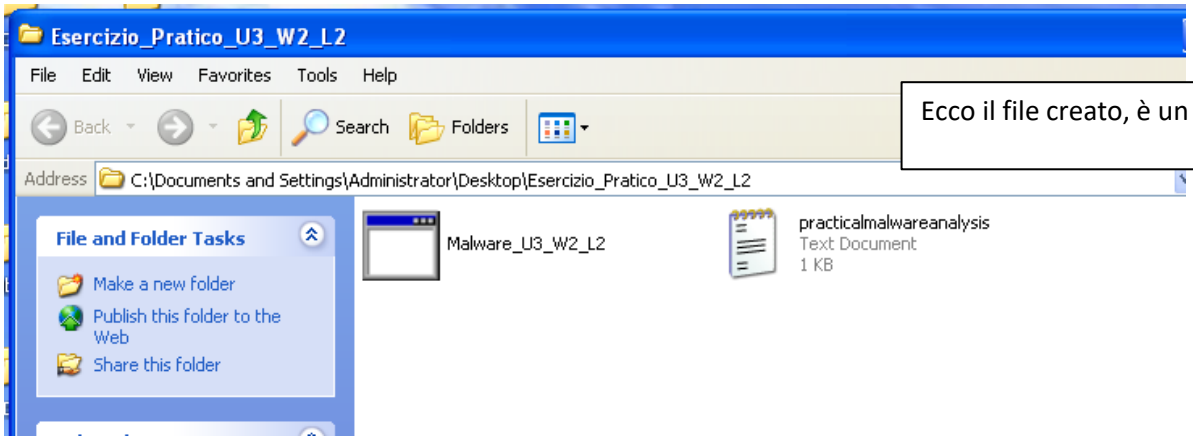


Aggiunta del filtro sull'operazione "CreateFile"

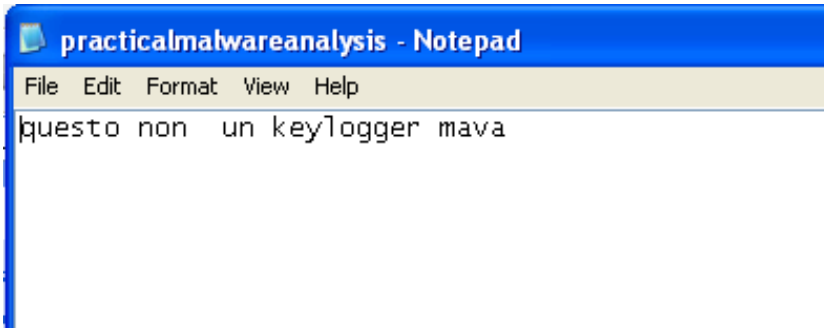


Si nota una operazione di creazione di un file nella directory del malware

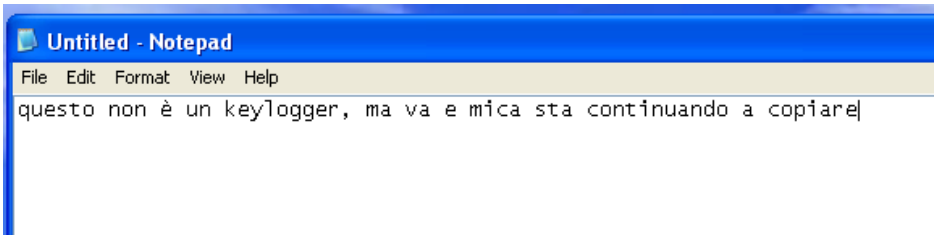




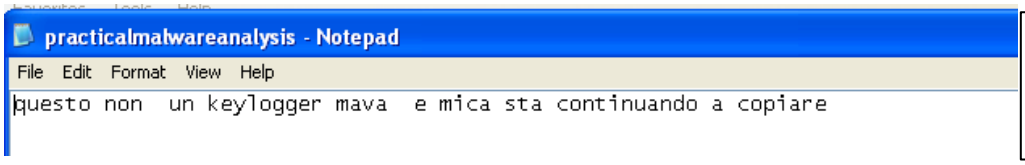
Ecco il file creato, è un file .txt



Il file contiene gli appunti che stavo prendendo durante l'analisi!



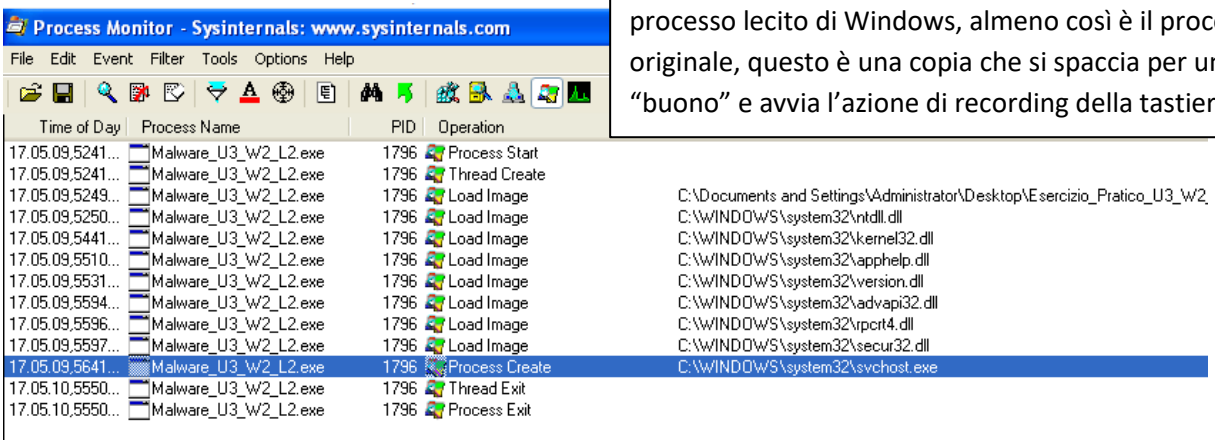
Per verificare se il processo è ancora attivo decido di aggiornare i miei appunti sul Notepad



Il file .txt continua ad aggiornarsi, il malware apre proprio un keylogger

Tornando su Process Monito possiamo vedere le azioni del malware su processi e thread.

Il malware crea un processo chiamato "svchost.exe" un processo lecito di Windows, almeno così è il processo originale, questo è una copia che si spaccia per un processo "buono" e avvia l'azione di recording della tastiera



Conclusione:

Il malware carica le librerie di cui ha bisogno ed avvia il processo di keylogging, i dati che cattura li trascrive in un file .txt nella cartella del malware.