Analisi malware dinamica basica

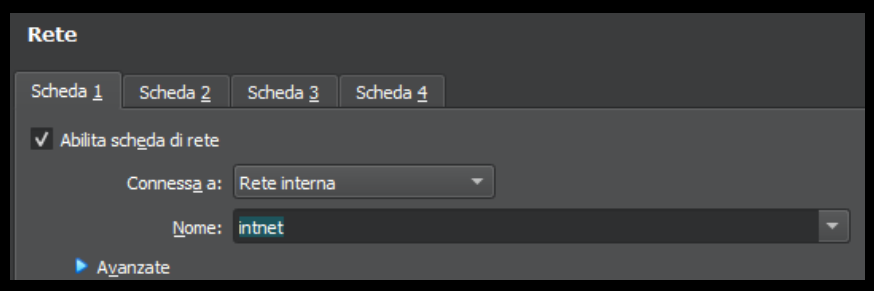
Richiesta: Configurare la macchina per l'analisi dinamica, eseguire il malware L2 presente nella VM win7.

Rispondere ai seguenti quesiti:
1. Identificare azioni del malware sul file system utilizzando process monitor
2. Identificare azioni del malware su processi e thread utilizzando process monitor
3. Modifiche del registro dopo il malware (le differenze)

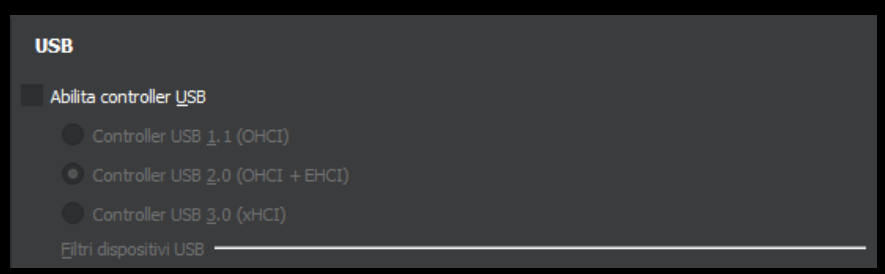
Configurazione macchina

Prima di eseguire il malware, assicuriamoci di settare l'ambiente di test in maniera adeguata.
Procediamo attraverso le seguenti pratiche:

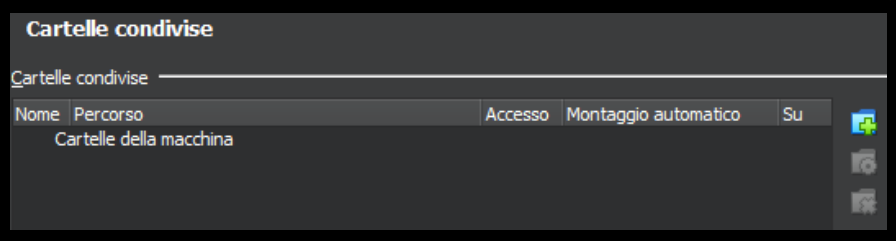
1. Configurazione scheda di rete: Impostiamo la macchina virtuale su rete interna, in modo da non comunicare con l'host reale.



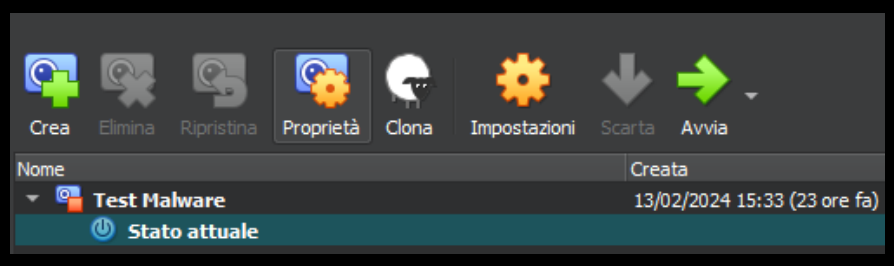
2. Disabilitare la possibilità di rilevare chiavette USB connesse alla macchina fisica.



3. Non condividere cartelle tra host e guest.



4. Creare delle istantanee prima dell'esecuzione del malware.

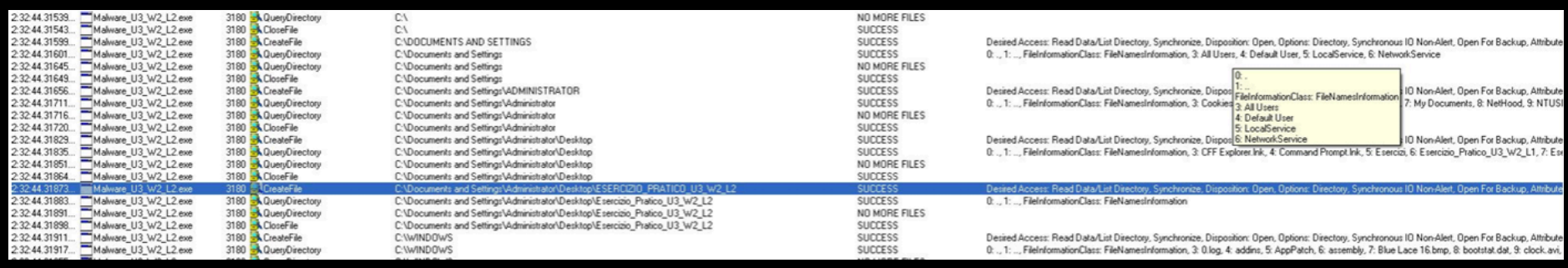


Esecuzione Malware
Una volta configurata la macchina virtuale, procediamo a lanciare il malware. Per l'analisi del malware utilizzeremo Process Monitor e Regshot.

Process Monitor: Tool avanzato per windows, permette di monitorare processi e thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuato su un sistema operativo.

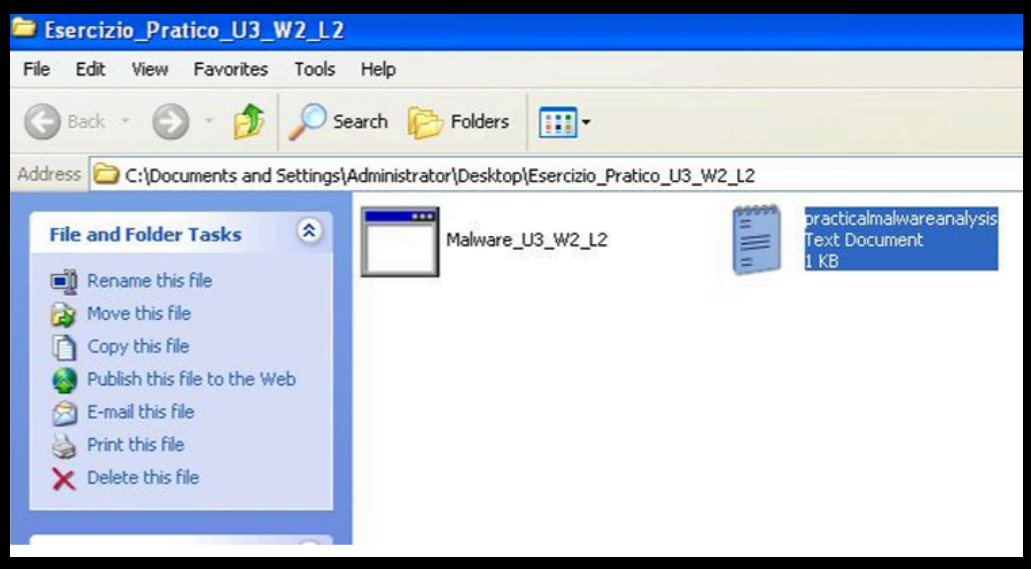
Regshot: Tool che permette di salvare un'istantanea delle chiave di registro, in modo da poter analizzare le differenze pre e post esecuzione malware.

Avviamo il malware e osserviamone le azioni attraverso Process Monitor.
Insieriamo il filtro per mostrare solo le attività del malware.



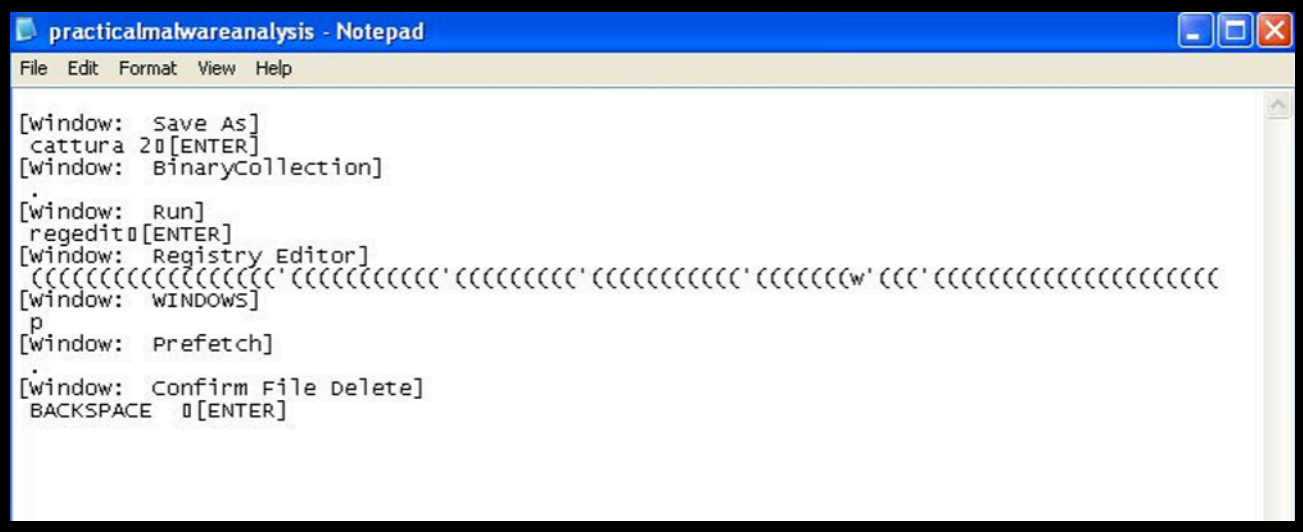
Notiamo che il malware nella sezione "operations" esegue azioni come create file, read file, close file, associate al path di corrispondenza.
In particolare, l'azione evidenziata è molto curiosa, ci fa capire che esso ha creato un file.txt nella cartella dove risiede il malware.

Verifichiamo:



Il file.txt è stato effettivamente creato con successo (practicalmalwareanalysis).

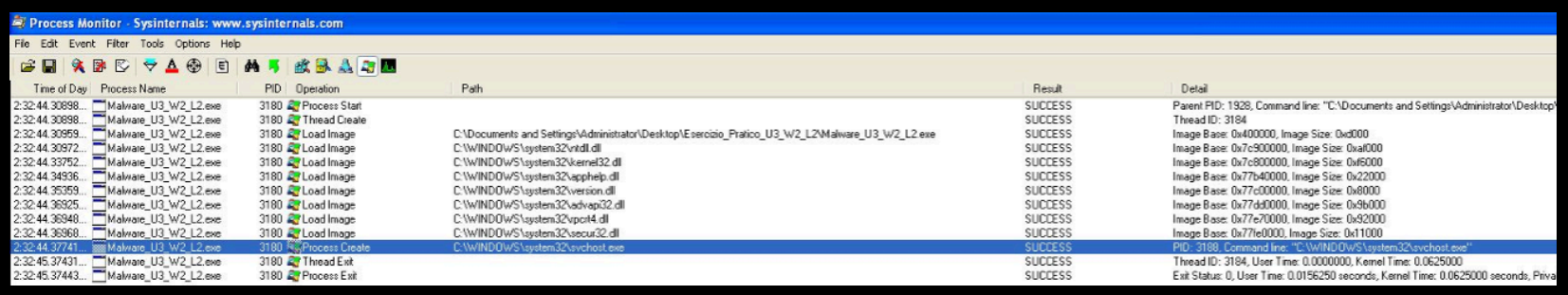
Osserviamone il contenuto:



Dalla lettura del file possiamo facilmente dedurre che si tratti di un Keylogger, un malware capace di registrare le digitazioni da parte della tua tastiera.
Un malware reale avrebbe inviato i dati contenuti nel file direttamente ad una destinazione malevola, un possibile attaccante.

Identificazione processi e thread

Utilizzando Processo Monitor, possiamo filtrare i processi e i thread avviati dal malware.



Notiamo come il malware utilizzi l'operazione load image per caricare l'esecuzione e le librerie necessarie per il funzionamento.

Troviamo Process Create che serve per creare un processo, in particolar modo possiamo osservare come crei un processo legittimo di windows "svchost.exe" in modo da camuffarsi come processo valido, per poi auto eliminarsi, in modo tale da rendere molto più difficile l'individuazione.