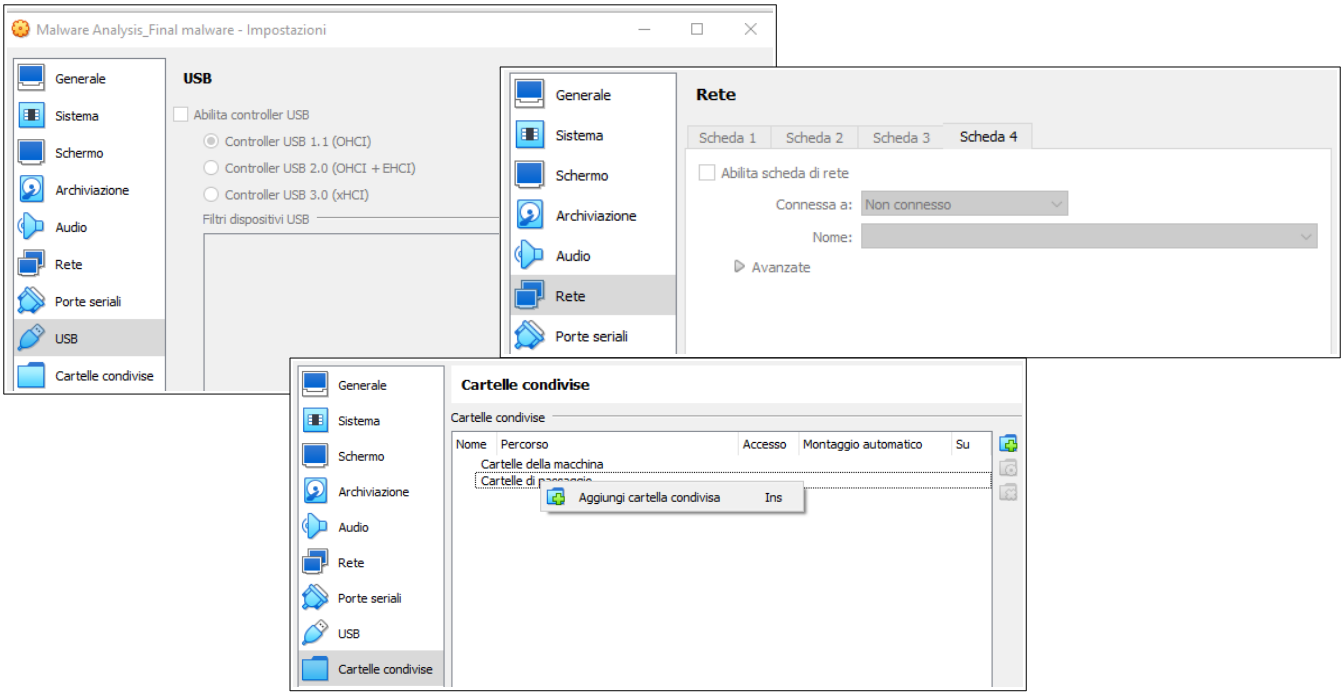
Analisi Dinamica Basica

Obiettivo: Effettuare un'analisi dinamica basica di un Malware su Windows XP 32 bit.

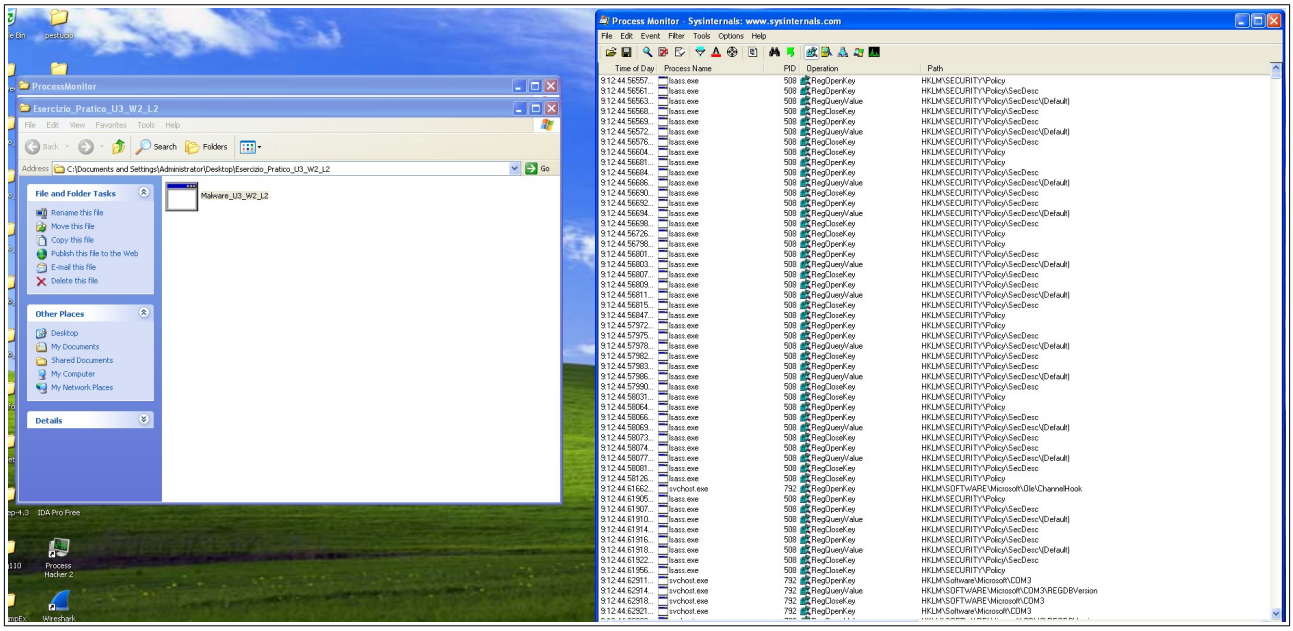
1) Macchina Offline

Prima di iniziare mi sono assicurato che la macchina virtuale fosse completamente *offline* e senza alcun collegamento con la macchina **Host Principale** controllando **Scheda di Rete Disattiva**, Porte **USB disattivate** e **Cartelle Condivise non collegate**.

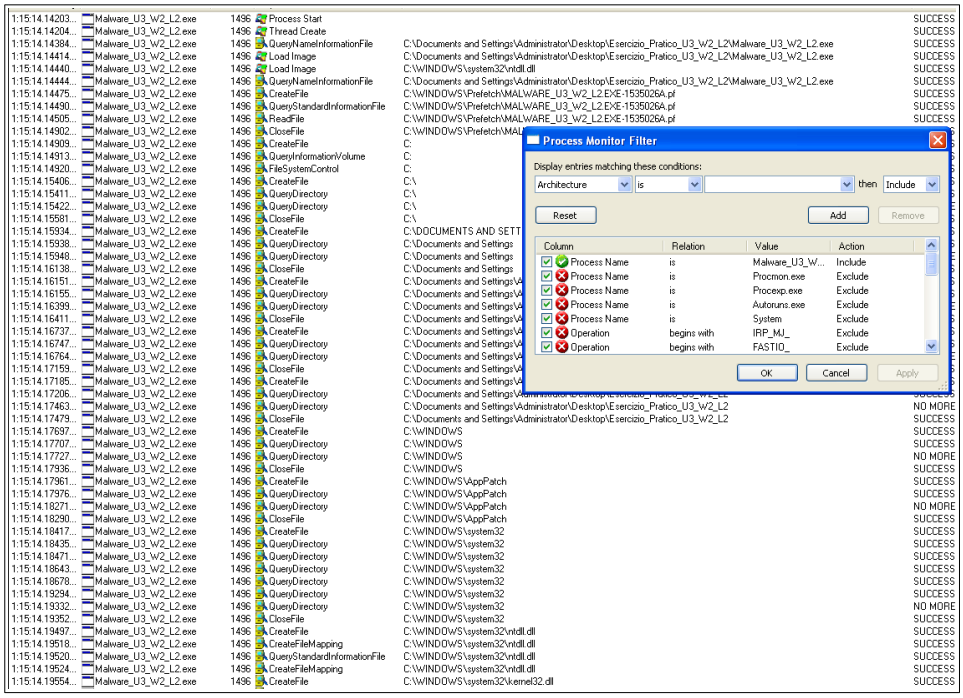


2) Avvio ProcMon e Malware

La traccia chiede di utilizzare il tool **Process Monitor** per analizzare il comportamento del **Malware**. Per cominciare ho avviato il tool per poi cliccare sul file *.exe* che la traccia chiede.



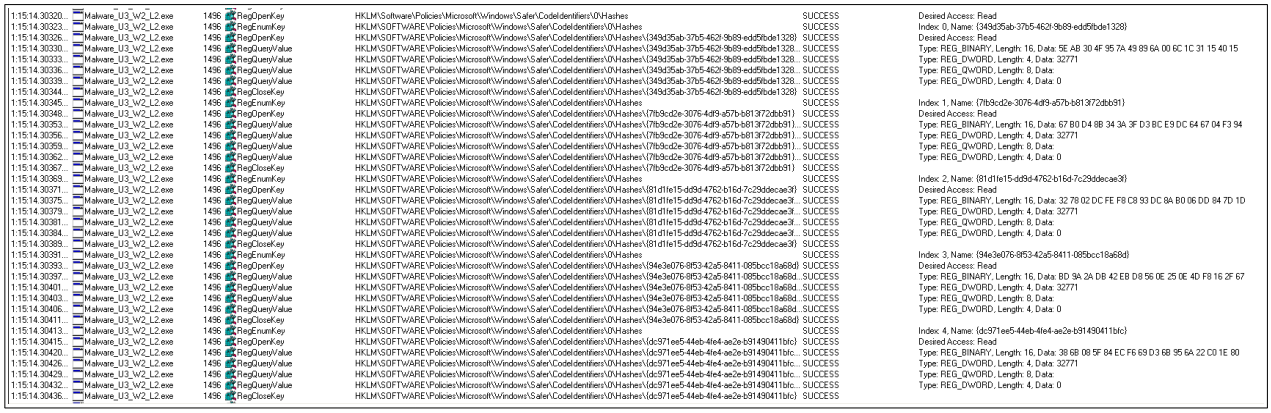
Essendo un tool che monitora continuamente i processi della macchina ho utilizzato un filtro per mostrare soltanto le modifiche riguardo il **Malware avviato (Malware_U3_W2_L2)**



Successivamente ho utilizzato i vari *switch* per poter controllare le singole tipologie di eventi.

3) Eventi di Registro

Il primo *switch* si riferisce alle attività relative alle **Chiavi di Registro** del Sistema Operativo.



Le attività svolte sui registri da questo Malware sono principalmente

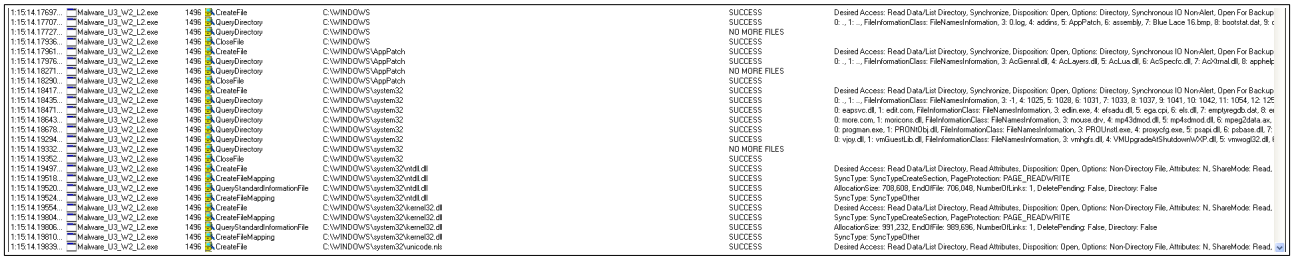
- **Elencare** le Chiavi di Registro in una Directory (**RegEnumKey**);
- **Aprire** le Chiavi sopracitate, o tentare almeno di aprirle (**RegOpenKey**);
- **Interrogare** le Chiavi stesse per ottenerne i valori specifici (**RegQueryValue**).

Nell'analisi vengono analizzate le chiavi di registro delle categorie **HKEY_CURRENT_USER** e **HKEY_LOCAL_MACHINE** (**HKCU** e **HKLM**).

Permettere ad un Malware di leggere le **Chiavi di Registro** è molto pericoloso; potrebbe ottenere l'accesso ad informazioni sensibili o compromettere le impostazioni di sicurezza del Sistema.

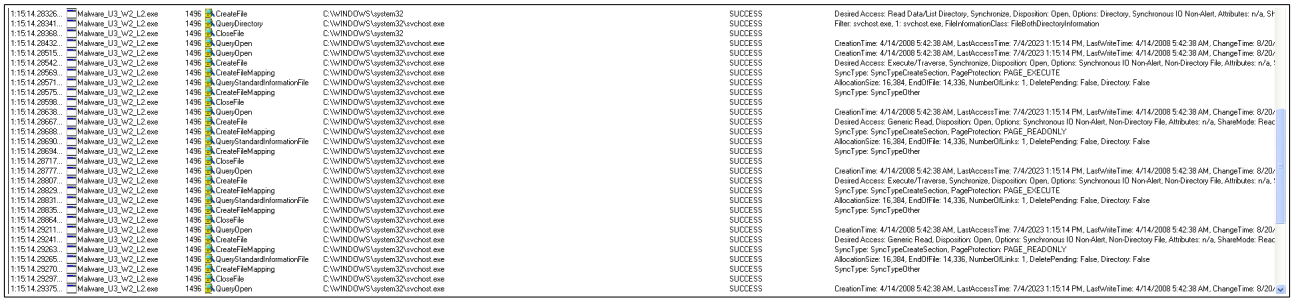
4) File System

Il secondo *switch* mostra invece attività relative ai **File System** di **Windows**.



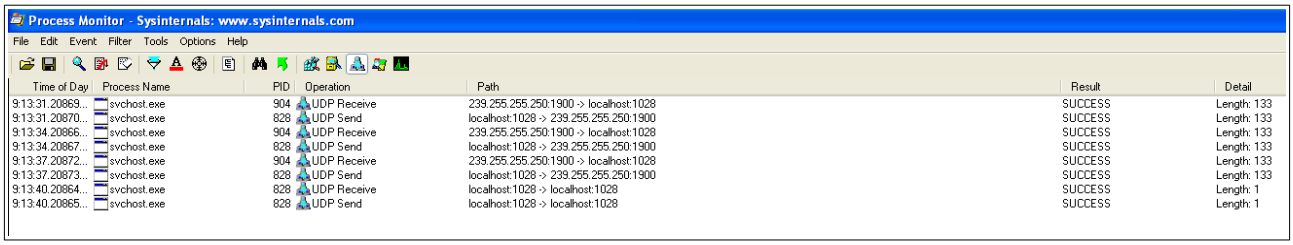
Nella prima parte dell'analisi il Malware crea o importa le librerie di cui ha bisogno per funzionare e per interagire col Sistema Operativo (k**ernel32**), con i Registri (**advapi32.dll**), con la gestione delle Operazioni di sicurezza (**secur32.dll**) e altre.

Nella seconda parte dell'analisi invece il **Malware** crea e "killa" il processo ***svchost.exe***, probabilmente per mascherare le modifiche che vuole effettuare al Sistema o sfruttare il processo legittimo per eseguire il proprio codice malevolo.



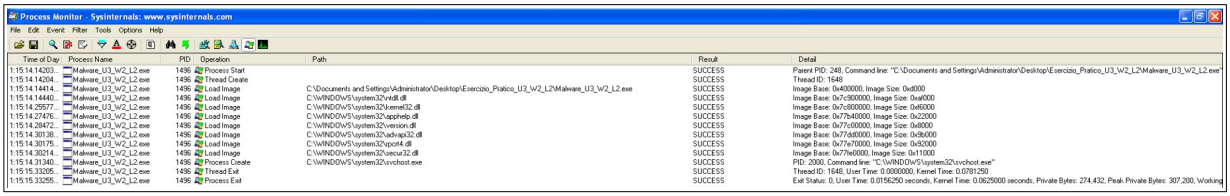
5) Flussi di Rete

Il terzo *switch* elenca le attività che vengono svolte sulla Rete da parte del **Malware**; nell'analisi effettuata non ci sono attività di questo tipo.



6) Processi e Thread

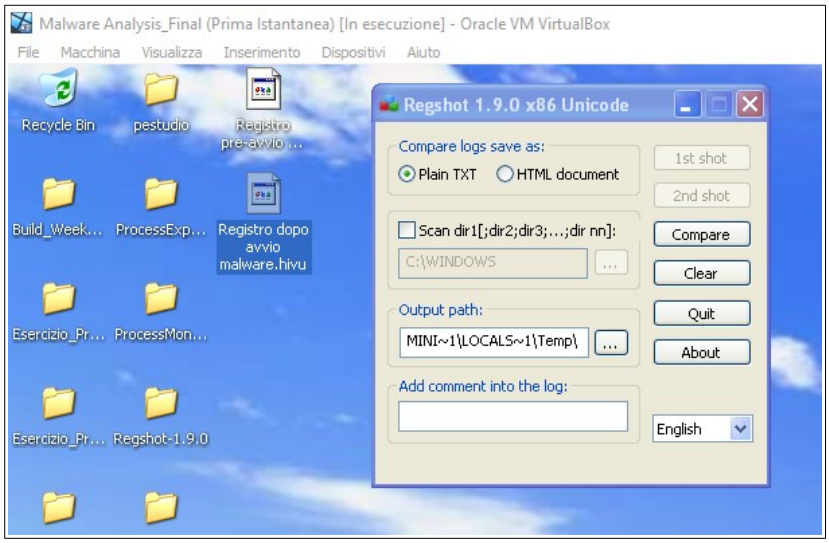
Il quarto *switch* mostra le attività relative ai **Processi e Thread** che il **Malware** avvia o meno.



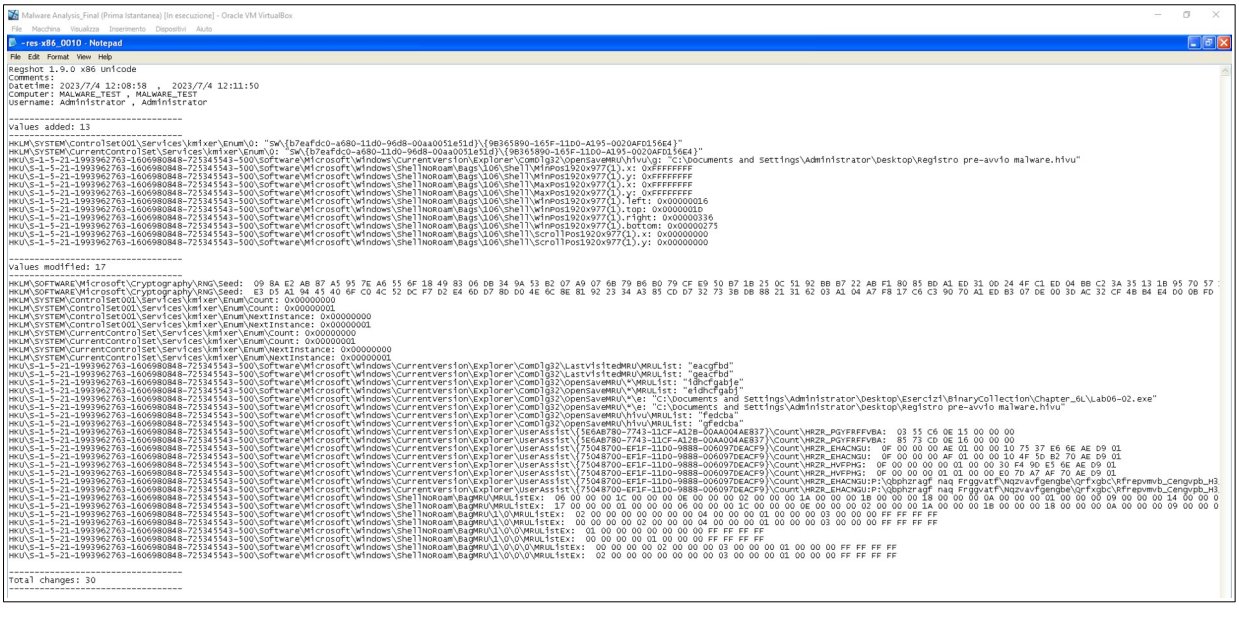
Si possono notare i caricamenti delle varie librerie (alcune viste prima) e la creazione del processo ***svchost.exe*** sopracitato dal momento che viene avviato per poi "killarsi" automaticamente.

7) Modifiche del Registro

Grazie al tool **Regshot** si possono creare delle *Istantanee* pre e dopo l'avviamento di un **Malware** per poterle confrontare e osservare le modifiche che vengono eseguite sulle **Chiavi di Registro**.



Salvando il 1st (*pre-avvio Malware*) e 2nd shot (*post avvio Malware*) possiamo grazie al tool confrontarli in un file di testo che potremo successivamente salvare dove vogliamo.



Ci sono stati da come leggiamo *30 modifiche* alle **Chiavi di Registro** con relativi **Path**.

8) Conclusioni

Alla luce dei risultati della scansione con **Process Monitor** e con **Regshot** posso supporre che questo **Malware** crei una serie di Processi **svchost.exe** per poi "killarli". Ogni processo creato probabilmente apporta ognuno delle modifiche al **Registro di Sistema** e poi si chiude per non farsi scoprire dal **Sistema**.