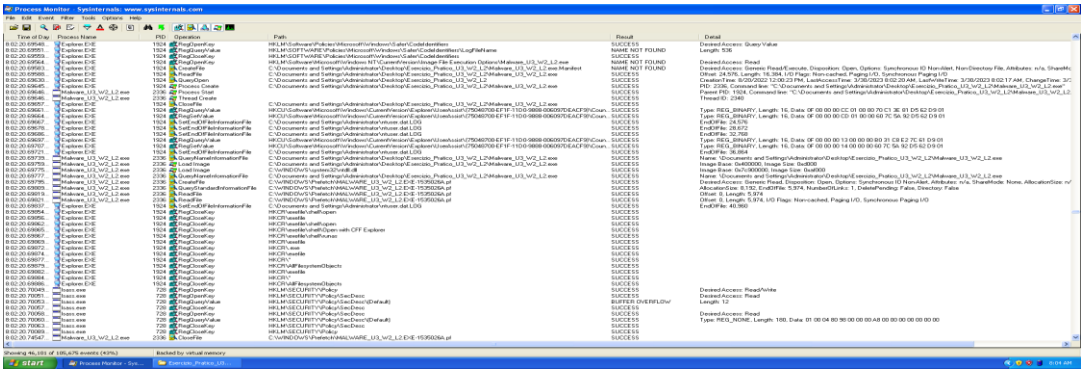
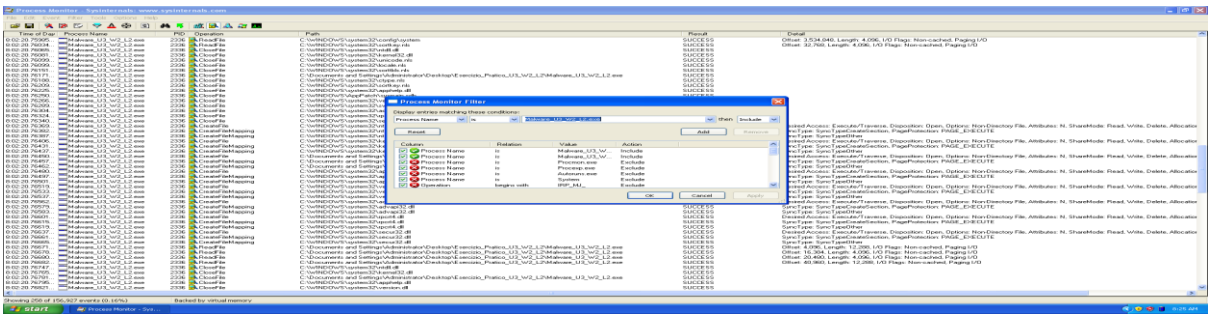
1) IDENTIFICARE AZIONI MALWARE SUI FILE SYSTEM USANDO PROCESS MONITOR

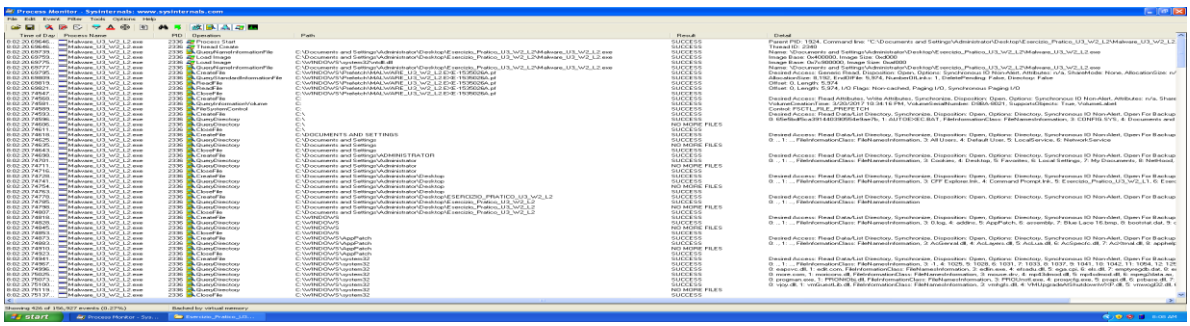
A. Facciamo partire prima ProcMon e successivamente lanciamo il malware. Stoppiamo dopo qualche minuto la cattura e vediamo tutti gli eventi catturati (se sono impostati tutti i filtri ovvero quelli di rete, dei file system, dei process, di registro e di profilazione, già tutti impostati di default).

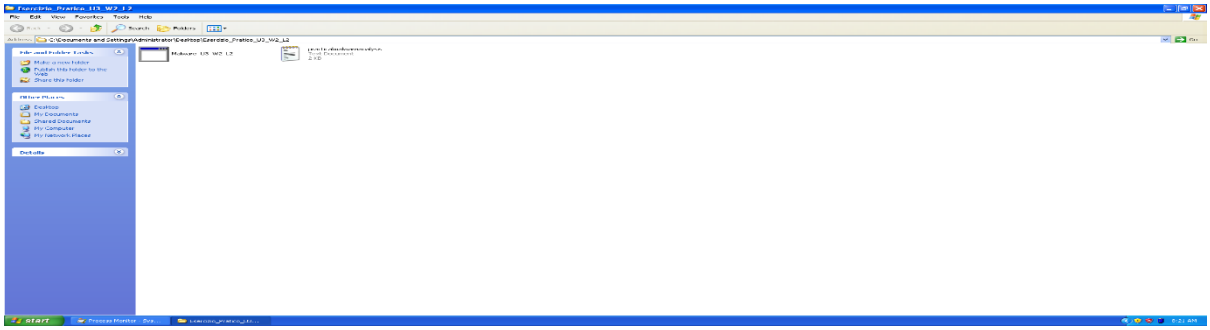
N.B potrebbe essere impostato di default un particolare filtro che impedisce la cattura degli eventi, se in tal caso vediamo che ProcMon "sembri" non funzionare o fornire nessun risultato, fare RESET FILTER e riprovare.



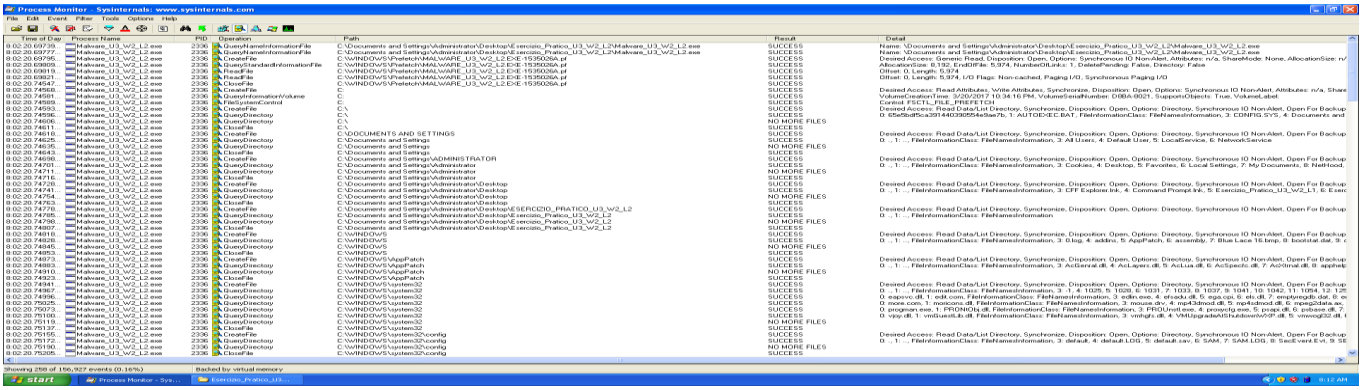
B. Adesso inseriamo il ***filtro*** per mostrare solo quegli eventi che hanno il nome Malware_U3_W2_L2
(filter – filter – process name – Malware_U3_W2_L2.exe – add - apply)
Tra le <<operation>> notiamo **Create file**, **Read File**, **Close File**, **Query Directory**
Inoltre viene creato un file **.txt** nella cartella del malware denominato <<**practicalMalwareAnalysis**>>
(possiamo aprirlo e analizzarlo per capire che tipo di malware è)





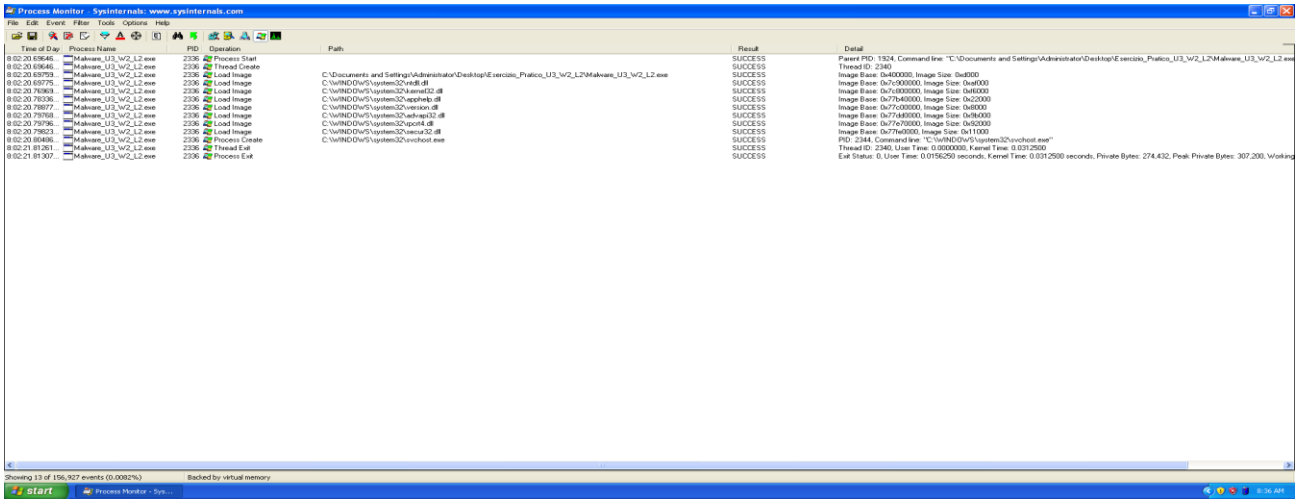


C. Usando la stessa cattura, impostiamo il filtro <<show file system activity>>



2) *IDENTIFICARE AZIONI MALWARE SU PROCESSI E THREAD USANDO PROCMON*

Usando la stessa cattura di ProcMon, impostiamo il filtro <<show thread and process activity>>



Possiamo notare:

- Nelle <<operation>> le funzioni **Load Image** e le relative librerie**(.dll)** usate per caricare ed eseguire il malware
- Sempre nelle <<operation>> la funzione **Process Create** per creare un processo. Il processo in questione è denominato *svc.host.exe* (è un processo valido di windows), per cui il malware si camuffa come processo valido per eludere i sistemi di difesa.

3) *PROFILAZIONE MALWARE IN BASE ALLA CORRELAZIONE "OPERATION – PATH "*

- Aprendo il file txt creato nella cartella del malware, notiamo che vengono catturati gli input dell'utente immessi, per cui il malware si camuffa creando un processo che per il firewall è un processo valido e poi lancia l'attacco ovvero un keylogger, memorizzando ciò che l'utente digita all'interno di un file