# S10 L2

Report esercizio “Malware analysis”

GiuliaSalani

# INDICE

# TRACCIA

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

1. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor;
2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor;
3. Provare a profilare il malware in base alla correlazione tra «operation» e Path;

# REPORT

## 1. PREMESSA: MALWARE ANALYSIS

### 1.1 DEFINIZIONE DI ANALISI DINAMICA BASICA

L'analisi dinamica del malware è un processo investigativo che prevede **l'esecuzione sicura di un eseguibile sospetto in un ambiente controllato.**

Durante l'esecuzione, vengono monitorate attività quali i tentativi di comunicazione di rete, le modifiche ai file di sistema e l'interazione con i processi in esecuzione. Gli strumenti di analisi dinamica possono registrare il comportamento del malware, catturare i pacchetti di rete generati e rilevare eventuali modifiche al registro di sistema.

Questo metodo offre una comprensione in tempo reale delle azioni del malware, inclusi i tentativi di auto-propagazione e le vulnerabilità sfruttate. L'analisi dinamica è essenziale per comprendere la natura e le capacità del malware, nonché per sviluppare misure di sicurezza adeguate.

### 1.2 PROCESS MONITOR

Process Monitor è un'utilità di monitoraggio del sistema per ambienti Windows che offre una dettagliata visione in tempo reale delle attività del sistema operativo.

Sviluppato da Microsoft, Process Monitor registra e visualizza informazioni sulle operazioni di sistema, inclusi i tentativi di accesso ai file, le operazioni di registro, e l'esecuzione dei processi.

Attraverso una ricca interfaccia grafica, gli utenti possono filtrare e analizzare le attività del sistema, consentendo una diagnosi approfondita di problemi, la tracciatura delle attività dei processi e la rilevazione di comportamenti sospetti, come quelli associati ai malware.

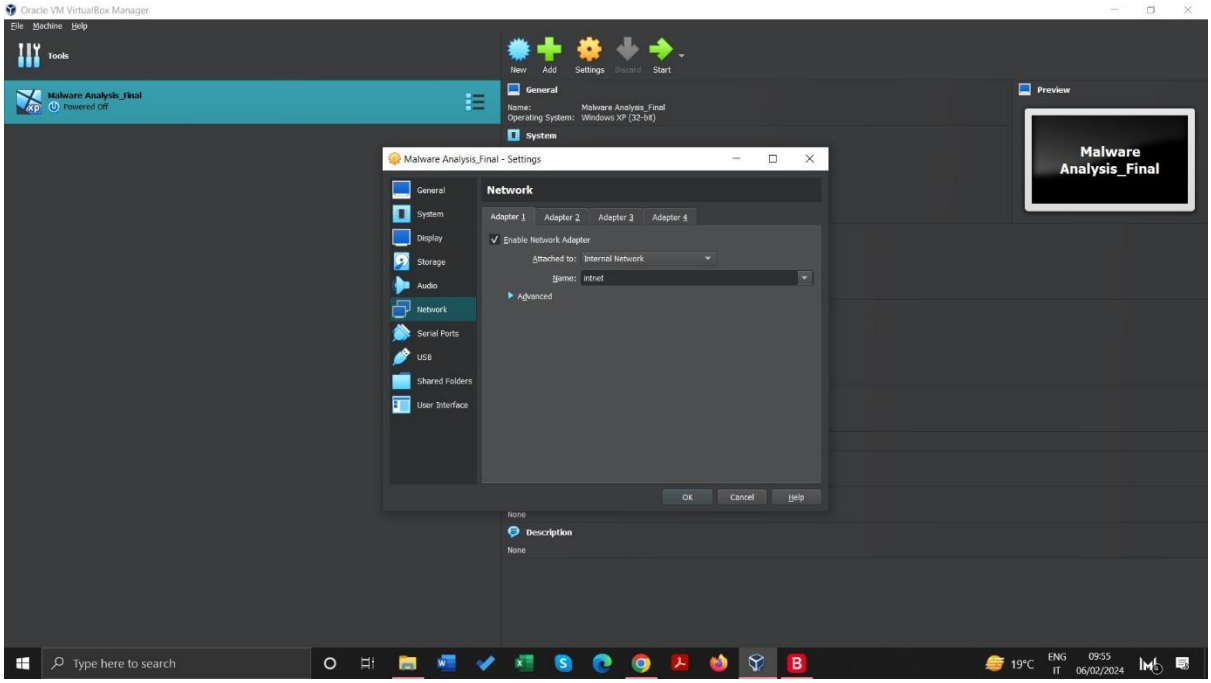
Process Monitor è uno strumento essenziale per gli amministratori di sistema e gli analisti di sicurezza per comprendere e risolvere problematiche legate alle attività del sistema in tempo reale.

### 1.3 PREPARAZIONE AMBIENTE: ISTRUZIONI

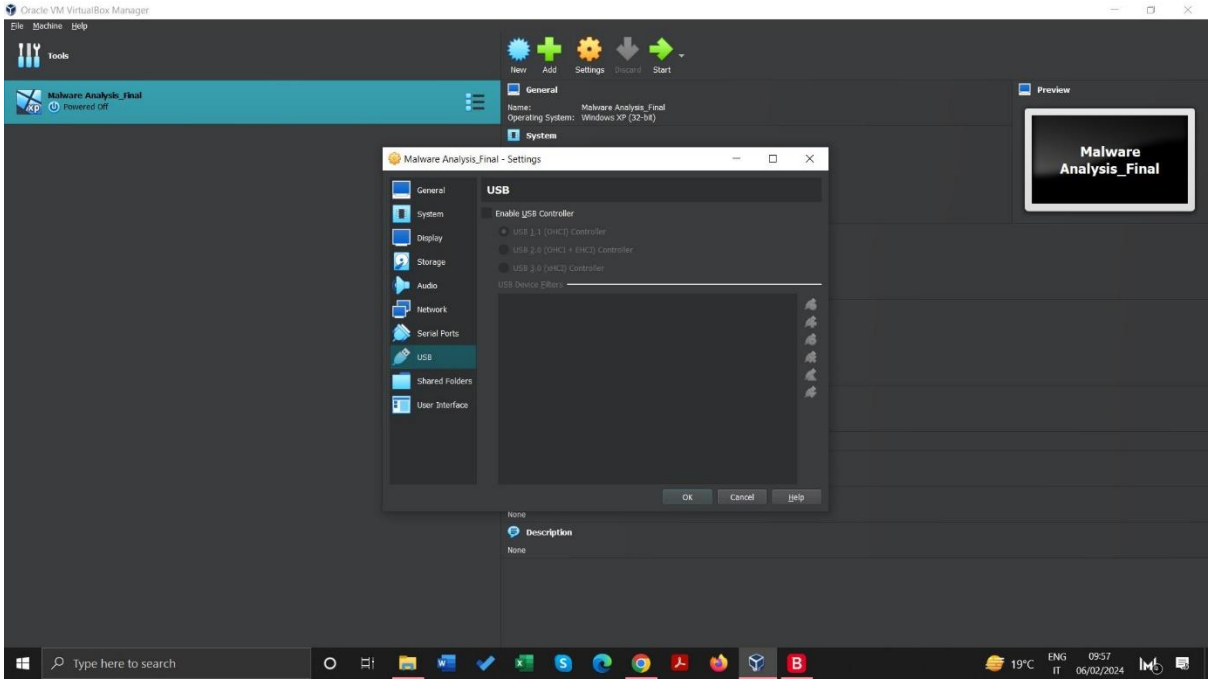
La corretta preparazione dell'ambiente è un passaggio fondamentale prima della vera e propria Analisi Dinamica. Si compone di alcune misure necessarie a tutelare la macchina ospite.

Apriamo Oracle VM Virtualbox, selezioniamo la nostra macchina virtuale e poi il pulsante "Settings".

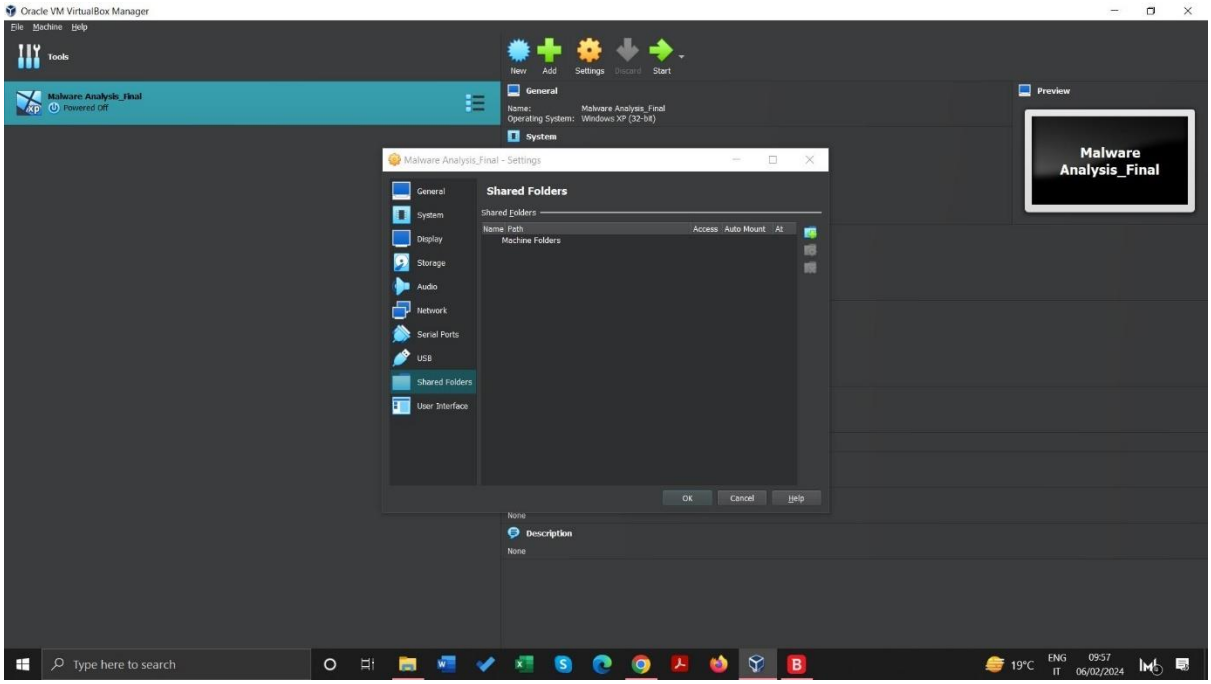
Spostiamoci sulla tab Network. Se l'analisi fosse statica, potremmo lavorare senza NIC attive, ma siccome stiamo lavorando in analisi dinamica, è necessario attivare una NIC che metteremo però in modalità internal:



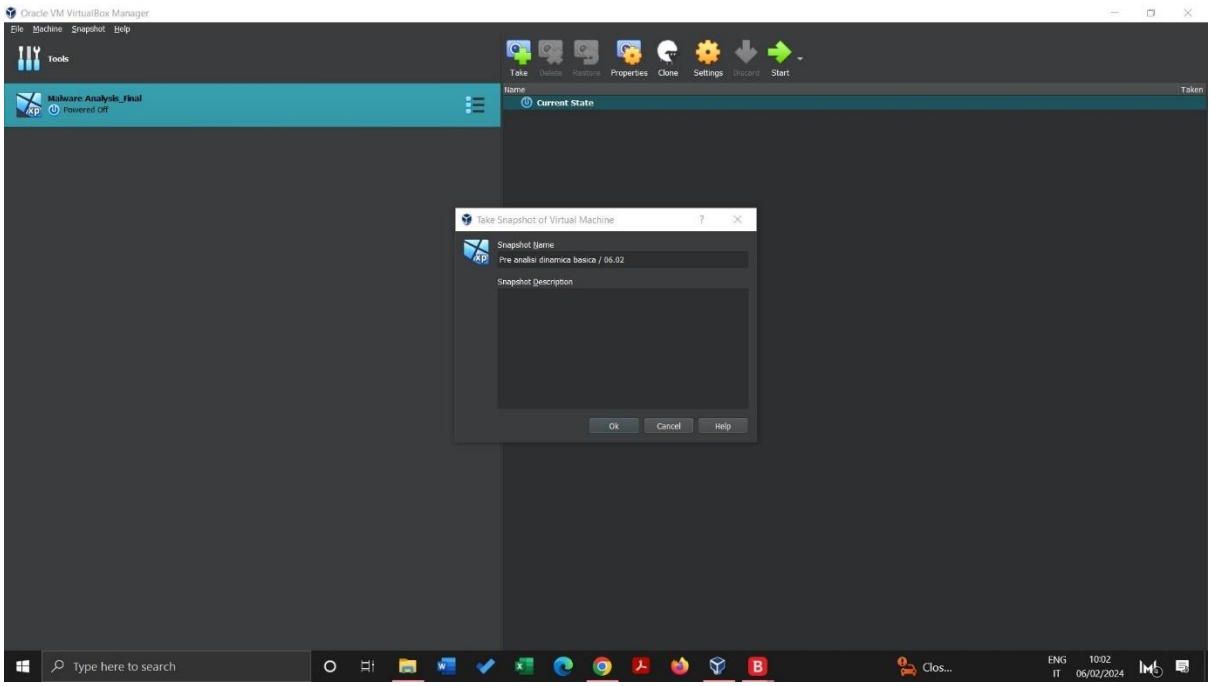

Spostiamoci ora su USB e assicuriamoci che l'opzione sia disabilitata, per evitare qualsiasi propagazione che utilizzi questo mezzo:



Scendiamo su Shared Folders e assicuriamoci che non vi siano cartelle condivise, sempre per evitare di mantenere punti scoperti che il malware potrebbe utilizzare per diffondersi:




Infine, andremo a creare un'istantanea della macchina virtuale nel suo stato attuale. Questo ci permetterà di ripristinarla al termine delle operazioni per tornare ad avere un ambiente sicuro su cui lavorare. Possiamo farlo tramite la sezione Tools, che si trova a sua volta nella sezione Machine, con il pulsante Take. Diamo un nome all'istantanea, clicchiamo su OK e il gioco è fatto:

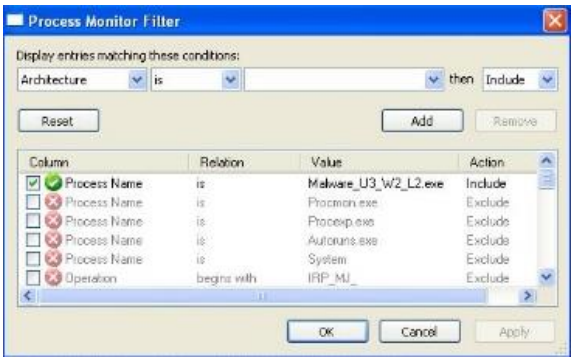



Ora possiamo avviare la macchina.

## 2. ANALISI

Per l'esercizio di oggi utilizzeremo il software Process Monitor (o Procmon) e il malware evidenziato in consegna: Esercizio_Pratico_U3_W2_L2. Entrambi si trovano sul desktop della macchina virtuale.

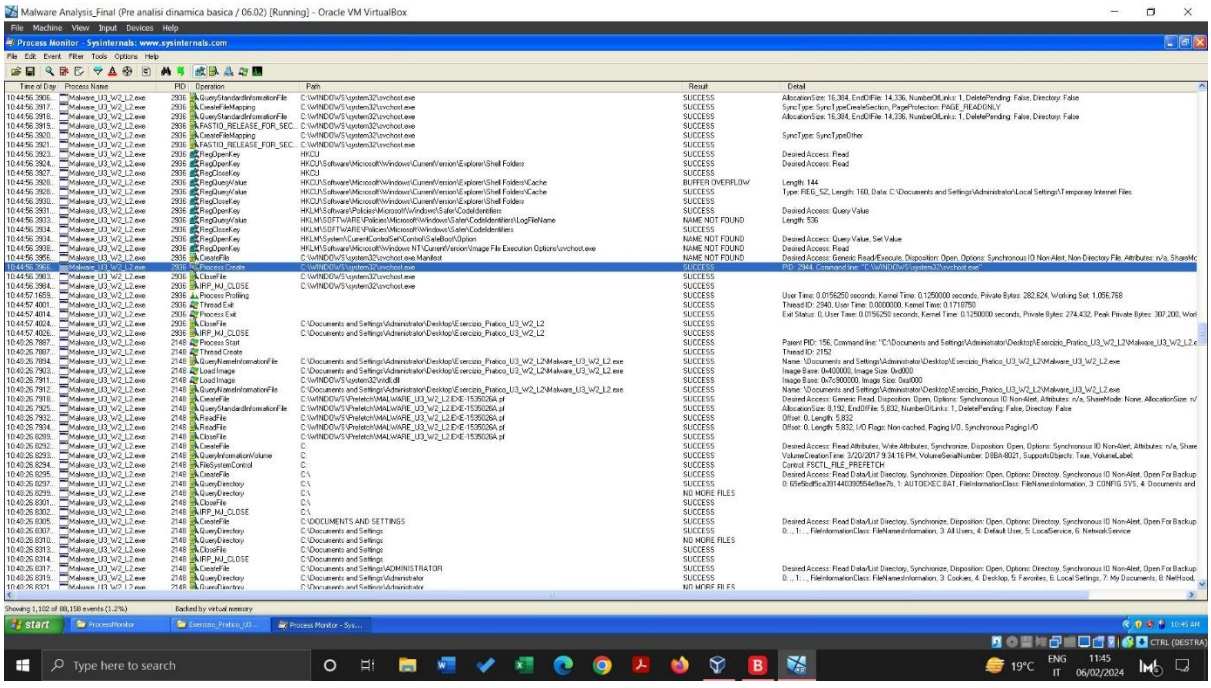
Lanciamo Process Monitor e creiamo il seguente filtro, ovvero comunichiamo al software di includere tutti quei Processi il cui nome corrisponde all'eseguibile del malware:




Spostiamoci sul destkop e lanciamo il malware. Per lanciarlo, basterà eseguirlo facendo doppio click sulla sua icona. Torniamo su Procmon ed analizziamo il risultato.

### 2.1 PROCESS CREATE

Nella lista evidenziata dalla cattura di Procmon, notiamo fra le altre cose l'operazione Process Create, ovvero è stato creato un processo svchost.exe:

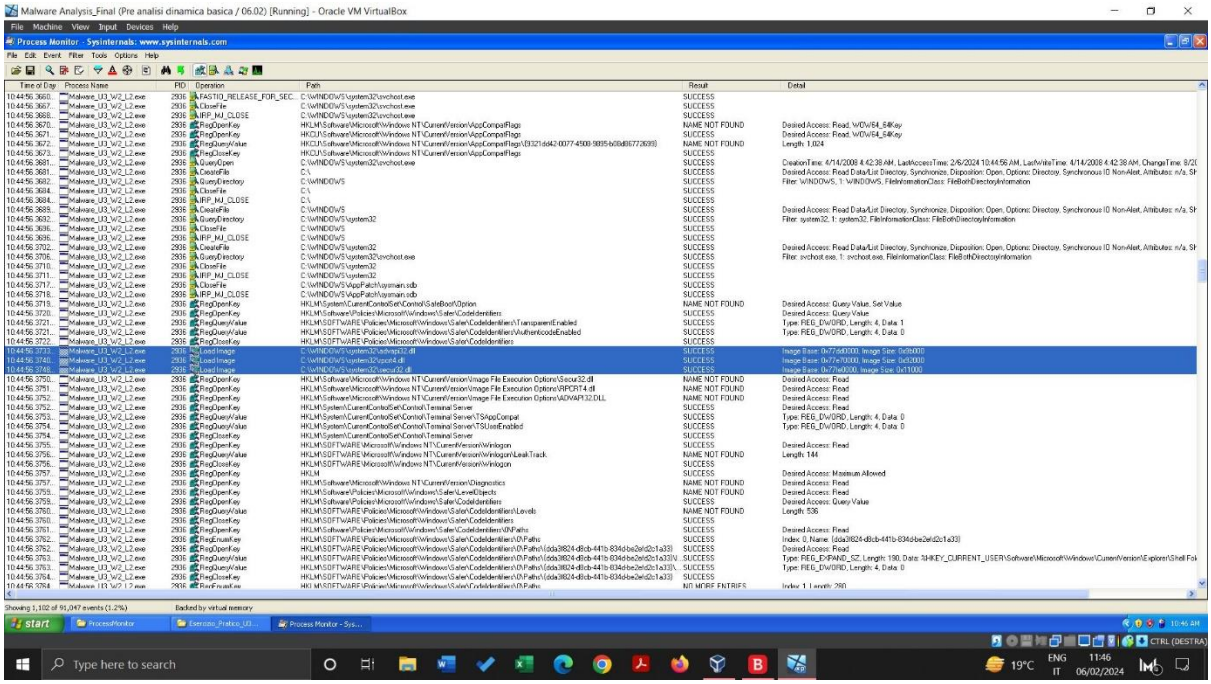



Il processo svchost.exe su Windows è un processo di sistema essenziale che funge da host per i servizi di sistema di Windows. Questo processo può ospitare uno o più servizi del sistema operativo, consentendo una maggiore modularità e facilitando la gestione dei servizi da parte del sistema operativo.

Nel caso della nostra analisi, si tratta quindi di un tentativo del malware di mimetizzarsi o celarsi tra i processi di sistema legittimi di Windows.

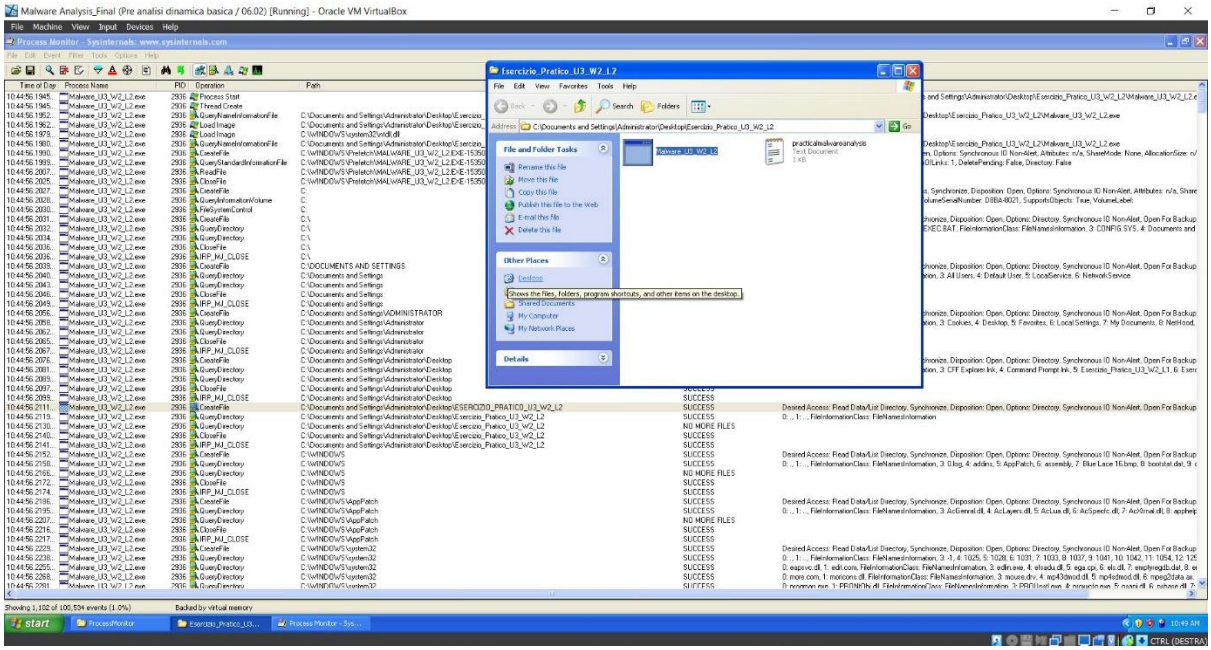
## 2.2 LOAD IMAGE

Notiamo poi le operazioni di Load Image che, come possiamo leggere dal path, costituiscono con tutta probabilità caricamenti di librerie:

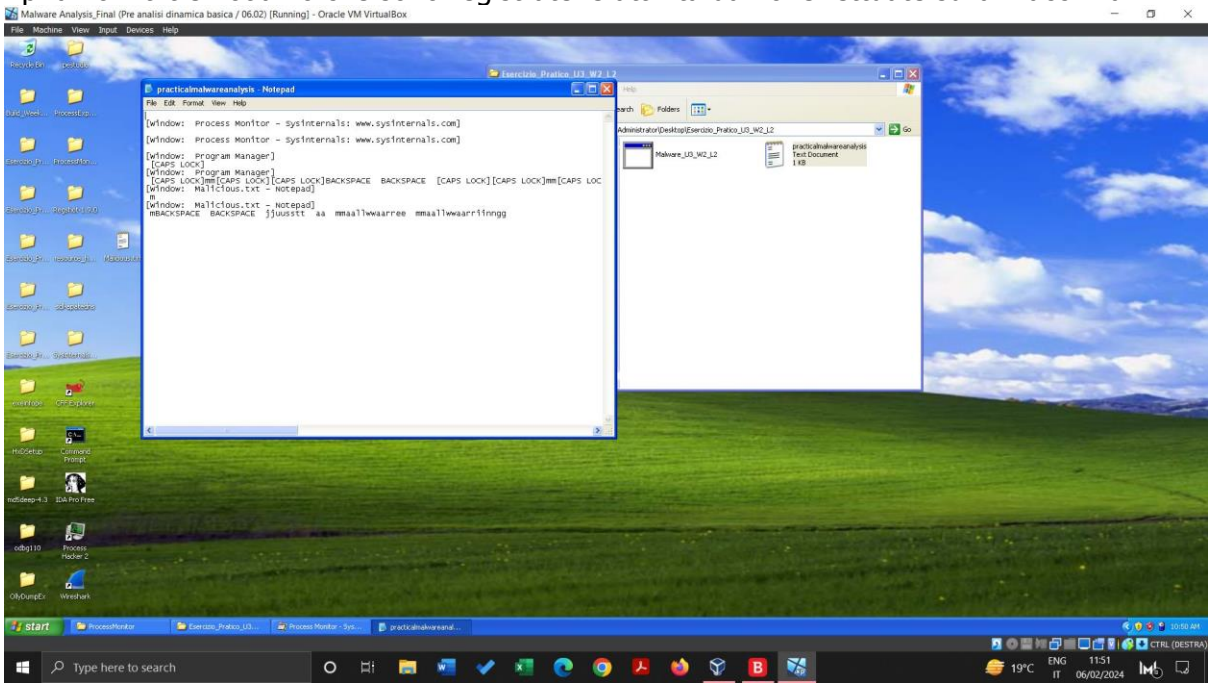


## 2.3 CREATE FILE

Un'operazione cattura poi la nostra attenzione: si tratta della creazione di un file all'interno della cartella dove si trova il malware. Vediamo che effettivamente nella cartella è comparso un file .txt che prima non era presente:

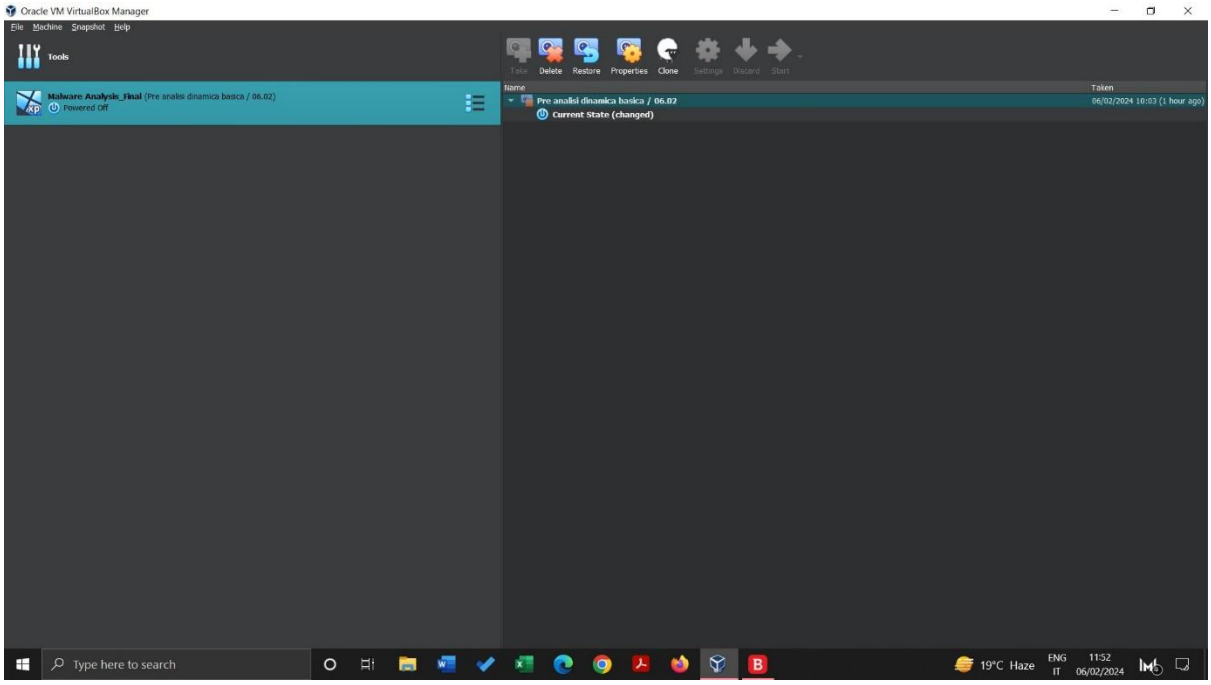


Apriamo il txt e notiamo che sono registrate le attività da noi effettuate sulla macchina:

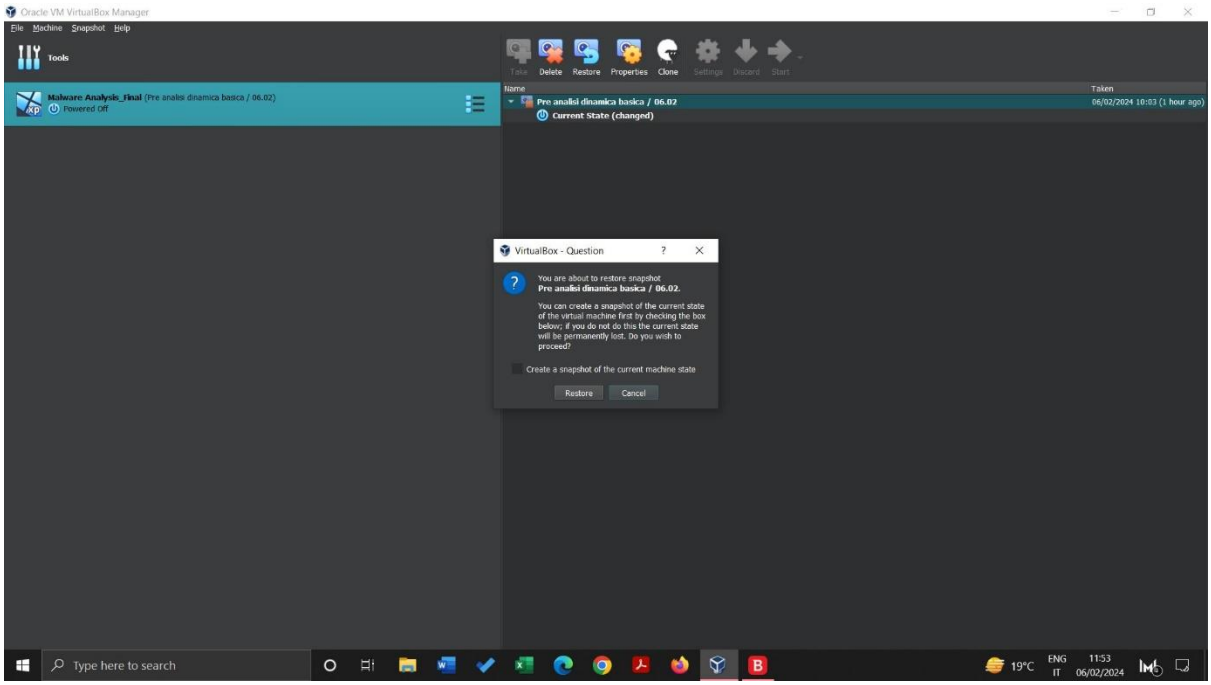


## 3. SISTEMAZIONE AMBIENTE: ISTRUZIONI

Al termine della cattura, chiudere Procmon e spegnere la macchina virtuale. Ripristinare la macchina all'istantanea che abbiamo scattato prima di effettuare l'analisi dinamica è essenziale per creare un ambiente intonso e sicuro per il prossimo test. Farlo è molto semplice, è sufficiente cliccare sul nome dell'istantanea creata precedentemente e cliccare l'icona Restore:




Confermare Restore, eliminando la spunta dall'opzione che ci permetterebbe di creare un'istantanea dello stato attuale, ovvero quello compromesso:



## CONSIDERAZIONE FINALI

Abbiamo preparato un ambiente sicuro in cui svolgere l'esercitazione di analisi dinamica basica, che è stata svolta utilizzando Process Monitor.

Tale software ha permesso di registrate diverse operazioni e in particolare una ha catturato la nostra attenzione, infatti si trattava della creazione di un file .txt nello stesso percorso in cui si trovava il malware. Aprendolo, è stato possibile notare che venivano appuntate tutte le attività svolte sulla macchina. Questo ha permesso di dedurre che il malware in questione è un key logger.

Un malware keylogger è progettato per infiltrarsi in un sistema informatico, registrare in modo stealthy le sequenze di tasti digitate dall'utente e inviare queste informazioni a un server remoto controllato dal malintenzionato. Il suo obiettivo principale è catturare dati sensibili come password, username e informazioni finanziarie. Operando in background, il keylogger può raccogliere in modo continuo le informazioni digitate, compromettendo la privacy dell'utente. Può essere distribuito attraverso e-mail di phishing, siti web dannosi o exploit software. Alcuni keylogger possono anche catturare screenshot del desktop e informazioni sensibili da app di messaggistica. La sua presenza spesso sfugge alla rilevazione, rendendo cruciale l'uso di software antivirus aggiornato e pratiche di sicurezza informatica avanzate per prevenirne l'infezione.