REPORT 10/01/2023

FACCILONGO DOMENICO

ANALISI DINAMICA BASICA

TASK

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:

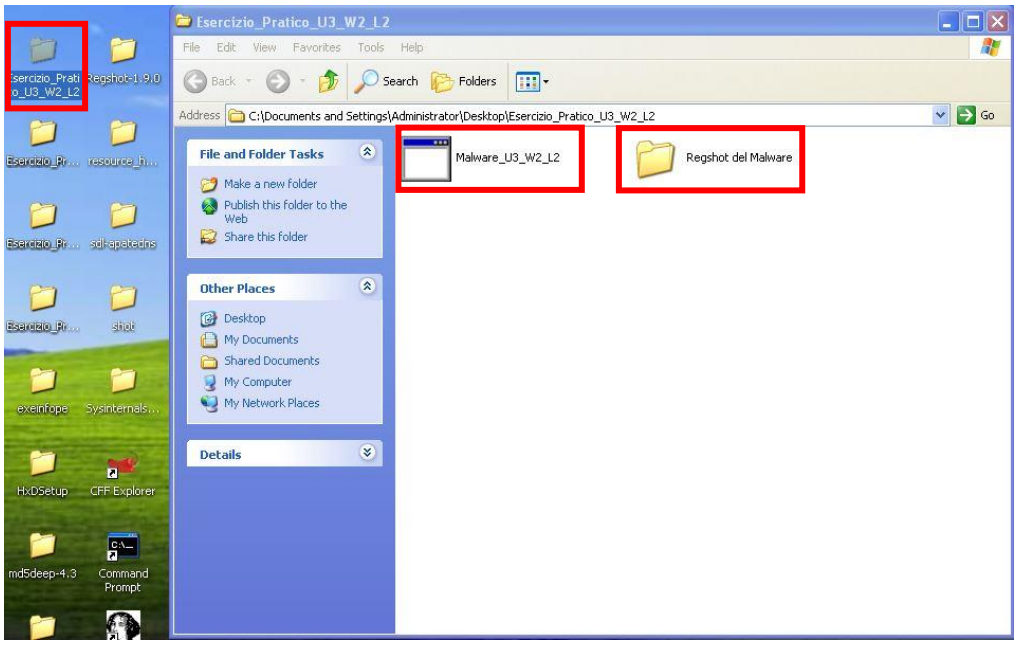
- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor (procmon) oppure se ci sono problemi multimon
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Modifiche del registro dopo il malware (le differenze)

- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

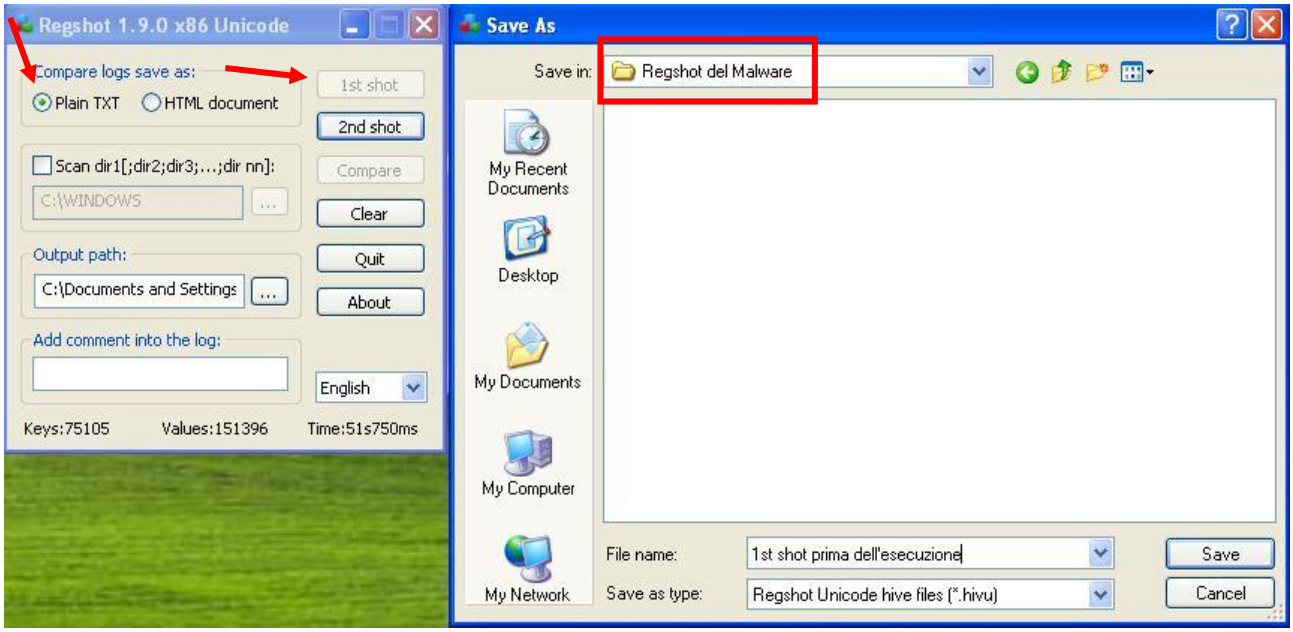
ANALISI E VALUTAZIONE

Il virus che prenderemo in esame si trova nella cartella del Desktop della macchina virtuale Malware_Analysis, il cui nome della cartella è **Esercizio_Pratico_E2_W2_L2** e al suo interno il Malware.

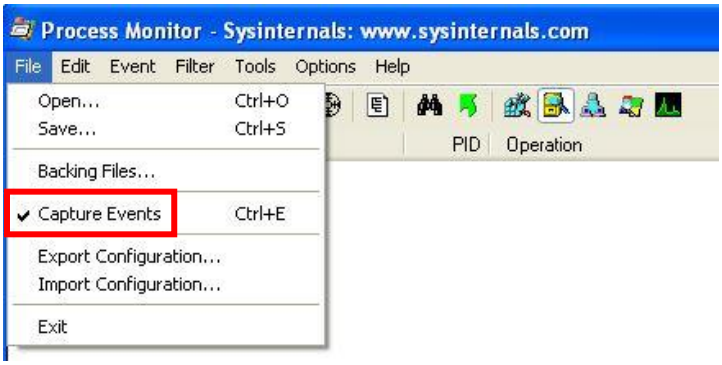
Come prima cosa, che ci servirà successivamente, andiamo a creare una cartella dal nome **Regshot del Malware**, come in figura sottostante:



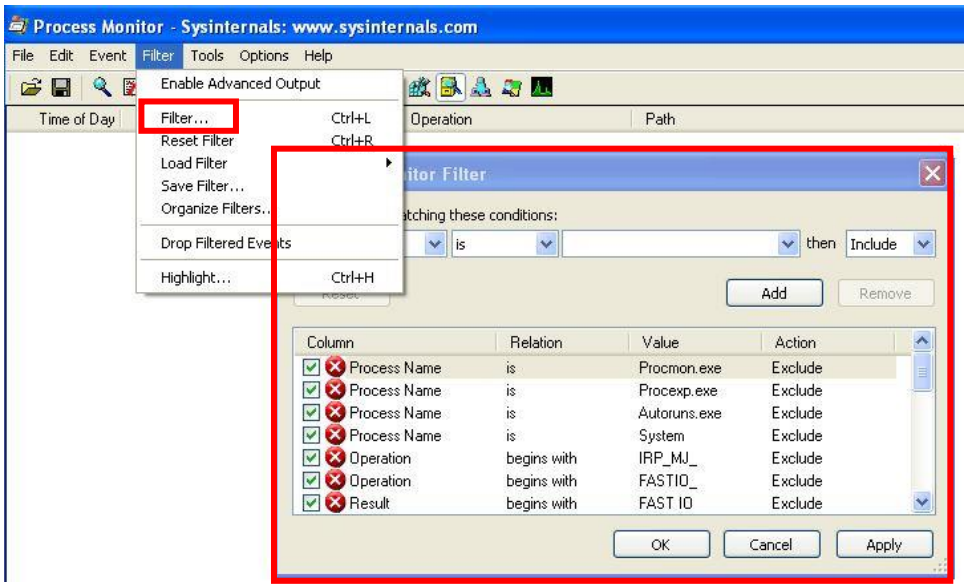
Come passo successivo andiamo ad aprire il tool **REGSHOT** dove, prima di eseguire il malware al fine di andarlo ad analizzare, effettuiamo una prima cattura dell'istantanea del dispositivo. Per farlo clicchiamo su "1st shot", assicuriamoci di aver spuntato *Plain TXT* e successivamente clicchiamo su **Shot and Save**. La finestra che si aprirà ci permetterà di andare a salvare il file dell'istantanea del dispositivo, il quale andremo a posizionarlo nella cartella creata precedentemente dal nome **Regshot del Malware**.



Prima di proseguire con il secondo shot andiamo ad aprire il secondo tool **PROCESS MONITOR (POCMON),** dal quale anche in questo caso dobbiamo assicurarci di avere il filtraggio dei processi attivo, come immagine seguente:



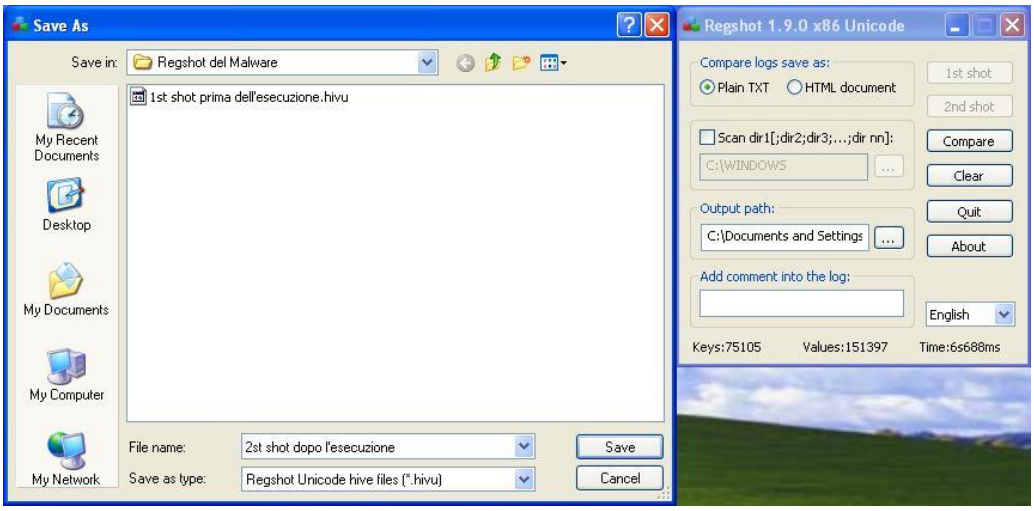
Sempre sullo stesso tool andiamo a creare il filtro che ci servirà successivamente al fine di ottenere solo ed esclusivamente il nome del processo interessato. Per farlo andiamo sulla sezione **Filter** e clicchiamo ancora su **Filter…** dal quale si aprirà la finestra come in figura sottostante:



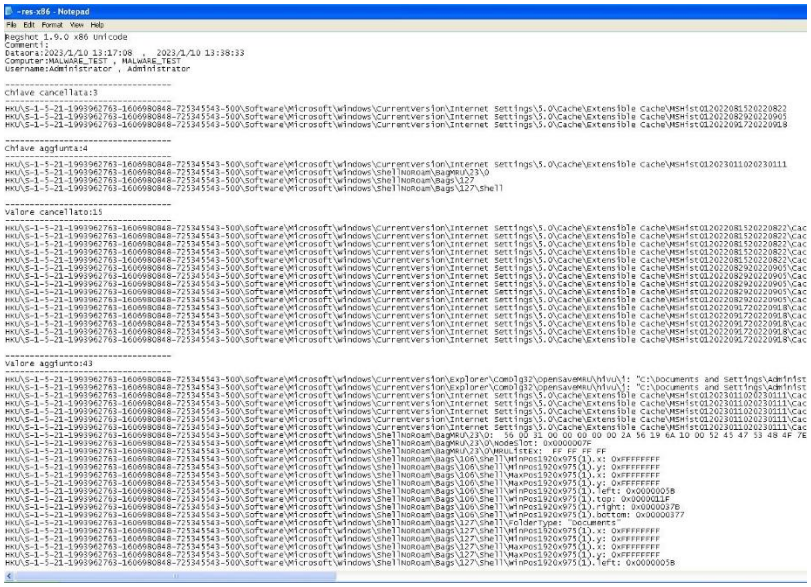
Lasciamo questa finestra e, concluso le fasi iniziali, andiamo ad **eseguire il Malware**.

RGSHOT:

Come prima cosa andiamo ad esaminare Rgshot, il quale, riprendendo dove eravamo rimasti andiamo ad eseguire il secondo shot come nel primo passaggio precedente:



Infine possiamo andare a cliccare sul tasto **Compare** il quale ci apriprà un file.txt con al suo interno una serie di processi che sono stati effettuati tra il primo e il secondo shot, ovvero quando abbiamo eseguito il malware. Il risultato è pressocchè questo:



Processi che sono stati sviluppati, tra cui ritroviamo anche le **Key**.

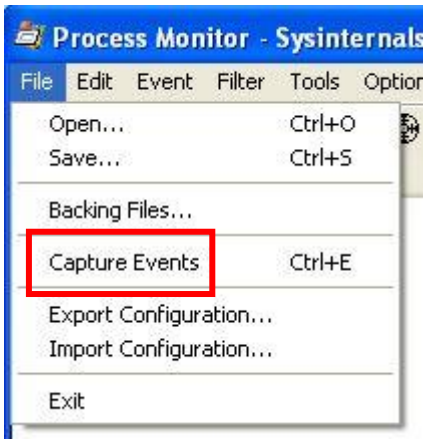
Prima di andarle ad esaminare insieme con il secondo tool è l'ultimo dato ovvero quello che ci indica quante variazioni sono state identificate, nel nostro caso:

```
---------------------------------------
Variazioni totali:83
---------------------------------------
```

Quindi possiamo dedurre che sono stati effettuati alcune modifiche.

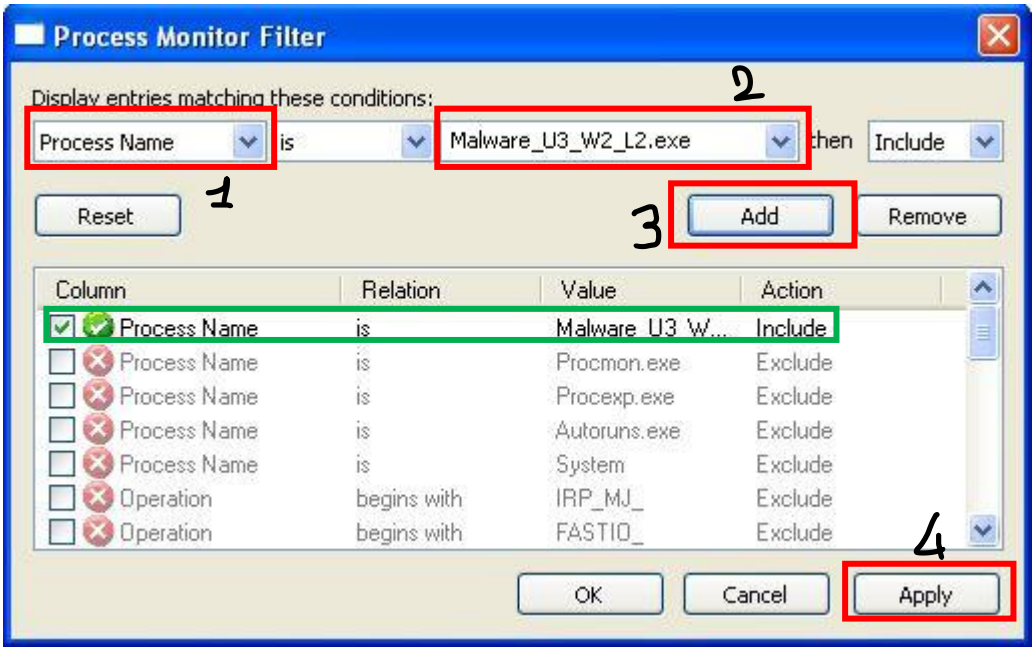
PROCMON:

Utilizzando invece quest'altro tool come prima cosa andiamo a chiudere il filtraggio dei processi che abbia abilitato inizialmente andando a spuntare la sezione come in figura:



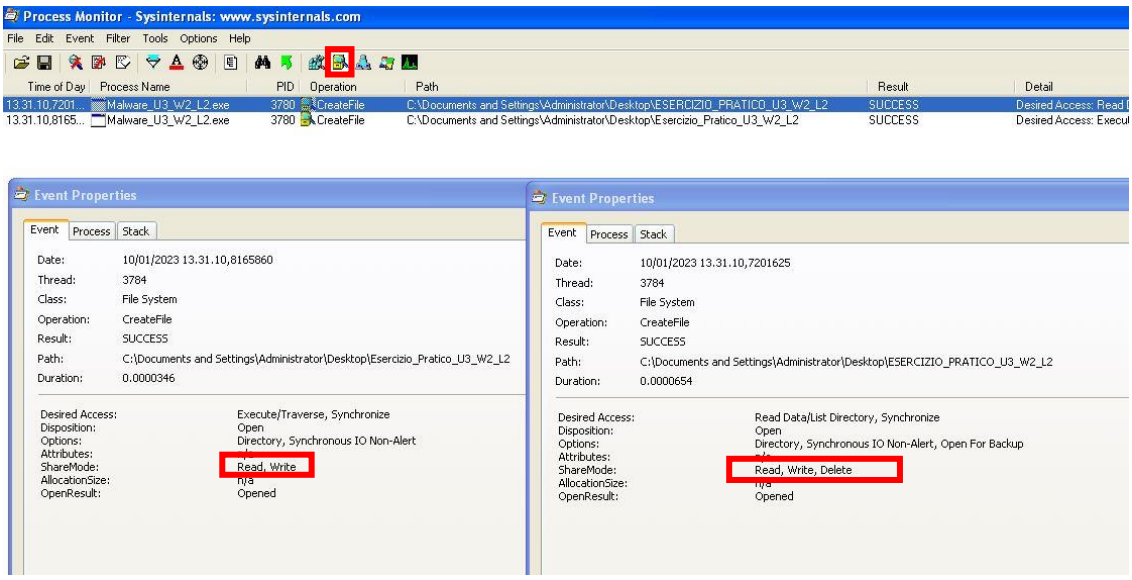
Come passaggio successivo dobbiamo andare creare il filtro che ci permette di individuare i processi del nostro Malware eseguito, e per farlo andiamo sulla sezione filtri che abbiamo lasciato precednetemente. I passaggi da seguire sono i seguenti:

Process Name (da tendina) → Malware_U3_W2_L2.exe (da tendina) → Add → Apply



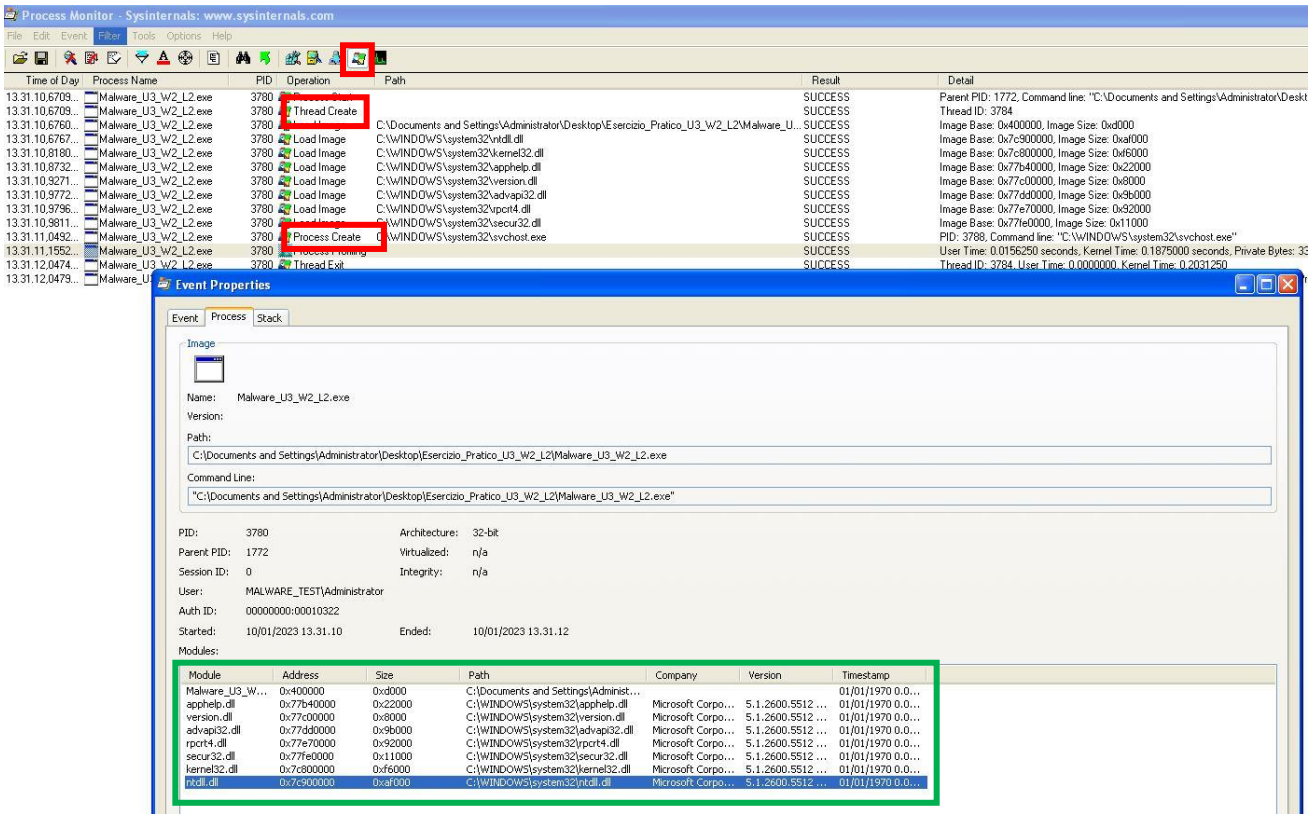
Stessa cosa dobbiamo fare per creare dei filtri che ci permettano di avere solo ed esclusivamente come Path quello del Malware, ovvero della sua cartella. Il procedimento di aggiunta filtro è lo stesso con la differenza di dover inserire nel primo riquadro il **path** e nel secondo riquadro incollare il path del Malware. Stessa cosa andiamo a fare per creare un filtro che ha come oggetto **CreatFile**.

Dopo aver creato tutti i filtri possiamo andare ad analizzare i risultati ottenuti, andando a spuntare solo l'icona indicata in figura il quale fa riferimento a **FileSystem**, i quali sono:



Aprendo i due processi ottenuti questo ci permette di capire che il primo processo ha concesso al malware di creare una cartella su Desktop dello stesso nome della cartella già esistente ma in Maiuscolo, e subito dopo, ci scrive sopra e infine la elimina. Questo ci permette di intuire che il Malware arriva a fare operazioni sulla macchina come creazione, lettura, scrittura ed esucozione.

La prova del Nove arriva quando andiamo invece ad analizzare i Processi e Thread del virus. In questo caso dobbiamo spuntare **Show Process and Thread**



Da immagine sopra si può notare come il Malware è arrivato a creare un nuovo Processo da cui al suo interno ritroviamo diverse librerie importate (riquadro verde in figura).

CONCLUSIONE

Possiamo pertanto concludere supponendo che il Malware è di tipo Trojan il quale acquisisce permessi dalla macchina vittima, dopo chiaramente la sua esecuzione, e che in modo “incognito” arriva a creare processi, cartelle, ottenere dati sensibili e poter prendere il controllo della macchina vittima da remoto.