Esercitazione W21D1 - Pratica 2

# Malware Analysis: Analisi dinamica basica

Fabio Benevento - 27/03/2024

## Traccia

Nella lezione teorica, 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:

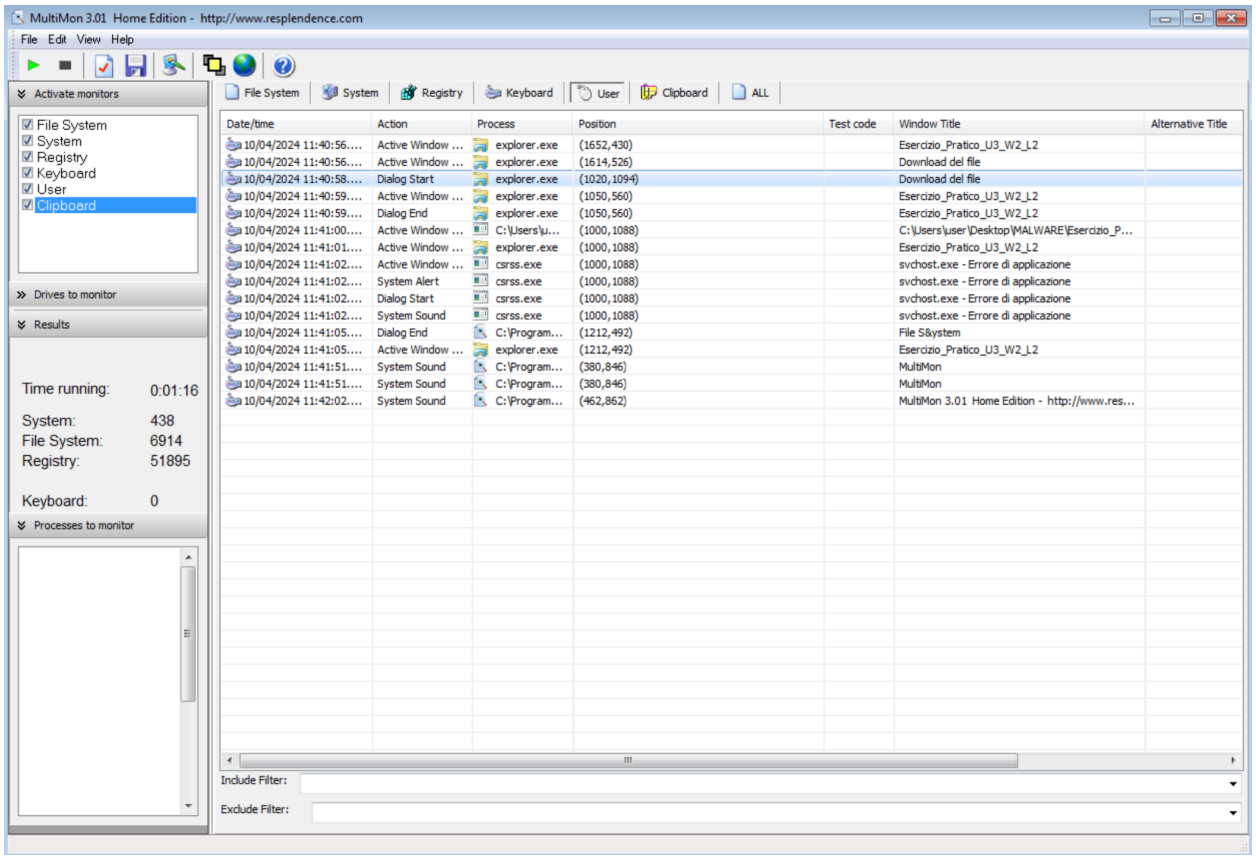
- Identificare eventuali azioni del malware sul file system utilizzando multimon https://www.resplendence.com/multimon Identificare eventuali altre azioni del malware
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

## Implementazione

Il tool Multimon presenta funzionalità simili a ProcMon per l'individuazione delle azioni d un processo, nel nostro caso di un malware. Purtroppo la versione 3.01 presenta un malfunzionamento per cui non è possibile utilizzare la funzionalità di filtro.

Il tool presenta delle sezioni che sono molto utili per capire il comportamento dell'applicazione. Infatti, oltre agli eventi di sistema, sul file system o sul registro è possibile catturare i tasti premuti sulla tastiera (Keyboard), gli oggetti presenti negli appunti (Clipboard) e gli eventi scatenati dall'utente (User).

L'immagine seguente mostra proprio la sezione User catturati in seguito all'esecuzione del malware. In esso è possibile individuare gli errori dell'applicazione dovuti a svchost.exe (in Windows 7 il malware non parte correttamente) che causano l'apparizione della finestra di dialogo e il suono di errore.


MultiMon 3.01 Home Edition - http://www.resplendence.com
File Edit View Help
Activate monitors
File System
System
Registry
Keyboard
User
Clipboard
Drives to monitor
Results
Time running: 0:01:16
System: 438
File System: 6914
Registry: 51895
Keyboard: 0
Processes to monitor
File System
System
Registry
Keyboard
User
Clipboard
ALL
Date/time
Action
Process
Position
Test code
Window Title
Alternative Title
10/04/2024 11:40:56.... Active Window ... explorer.exe (1652,430) Esercizio_Pratico_U3_W2_L2
10/04/2024 11:40:56.... Active Window ... explorer.exe (1614,526) Download del file
10/04/2024 11:40:58.... Dialog Start explorer.exe (1020,1094) Download del file
10/04/2024 11:40:59.... Active Window ... explorer.exe (1050,560) Esercizio_Pratico_U3_W2_L2
10/04/2024 11:40:59.... Dialog End explorer.exe (1050,560) Esercizio_Pratico_U3_W2_L2
10/04/2024 11:41:00.... Active Window ... C:\Users\u... (1000,1088) C:\Users\user\Desktop\MALWARE\Esercizio_P...
10/04/2024 11:41:01.... Active Window ... explorer.exe (1000,1088) Esercizio_Pratico_U3_W2_L2
10/04/2024 11:41:02.... Active Window ... csrss.exe (1000,1088) svchost.exe - Errore di applicazione
10/04/2024 11:41:02.... System Alert csrss.exe (1000,1088) svchost.exe - Errore di applicazione
10/04/2024 11:41:02.... Dialog Start csrss.exe (1000,1088) svchost.exe - Errore di applicazione
10/04/2024 11:41:02.... System Sound csrss.exe (1000,1088) svchost.exe - Errore di applicazione
10/04/2024 11:41:05.... Dialog End C:\Program... (1212,492) File S&ystem
10/04/2024 11:41:05.... Active Window ... explorer.exe (1212,492) Esercizio_Pratico_U3_W2_L2
10/04/2024 11:41:51.... System Sound C:\Program... (380,846) MultiMon
10/04/2024 11:41:51.... System Sound C:\Program... (380,846) MultiMon
10/04/2024 11:42:02.... System Sound C:\Program... (462,862) MultiMon 3.01 Home Edition - http://www.res...
Include Filter:
Exclude Filter: