Report di Analisi del Malware

Introduzione

In questa esercitazione, ho utilizzato il tool MultiMon su una macchina virtuale Windows 7 per eseguire un'analisi dinamica di un malware. L'obiettivo è stato identificare le azioni del malware sul file system, processi e thread, e le modifiche al registro di sistema. Di seguito, fornisco un report dettagliato dei passaggi eseguiti e dei risultati ottenuti.

1. Preparazione dell'Ambiente

Creazione di un'istantanea della macchina virtuale

Prima di iniziare l'analisi, ho creato un'istantanea della mia macchina virtuale Windows 7 utilizzando VirtualBox. Questo mi ha permesso di ripristinare lo stato originale della VM in caso di problemi durante l'analisi.

2. Download e Configurazione di MultiMon

Scarica e installa MultiMon

Ho scaricato MultiMon dal sito ufficiale e l'ho installato sulla mia macchina virtuale Windows 7.

3. Esecuzione di MultiMon

Avvio di MultiMon

Ho avviato MultiMon e configurato per monitorare le attività specifiche del malware. Ho selezionato le categorie di monitoraggio pertinenti: File System, System, Registry, Keyboard, User e Clipboard.

4. Configurazione di MultiMon

Filtri per il File System

Ho configurato i filtri di MultiMon per monitorare le operazioni di CreateFile, WriteFile, ReadFile, DeleteFile.

Filtri per Processi e Thread

Ho configurato i filtri di MultiMon per monitorare le operazioni di Process Create, Thread Create, Process Exit.

Filtri per il Registro

Ho configurato i filtri di MultiMon per monitorare le operazioni di RegSetValue, RegCreateKey, RegDeleteValue, RegDeleteKey.

5. Esecuzione del Malware

Ho eseguito il malware sulla VM, permettendo a MultiMon di catturare tutte le azioni compiute dal malware per circa 1-2 minuti. Successivamente, ho interrotto la cattura degli eventi cliccando sull'icona della lente con una "X" rossa.

6. Analisi delle Attività Catturate

Azioni sul File System

Ho cercato nel log di MultiMon le operazioni di CreateFile, WriteFile, ReadFile, DeleteFile.

Risultati:

- **CreateFile**: Ho identificato che il malware ha creato un file denominato Esercizio_Pratico_U3_W2_L2.
- **WriteFile**: Il malware ha scritto nel file creato precedentemente.
- **ReadFile**: Il malware ha letto diverse volte dal file creato.
- **DeleteFile**: Non sono state registrate operazioni di cancellazione di file.

Azioni su Processi e Thread

Ho cercato nel log di MultiMon le operazioni di Process Create, Thread Create, Process Exit.

Risultati:

- **Process Create**: Il malware ha creato un processo denominato Explorer.EXE.
- **Thread Create**: Sono stati creati diversi thread associati al processo Explorer.EXE.
- **Process Exit**: Il processo Explorer.EXE è stato terminato.

Modifiche al Registro

Ho cercato nel log di MultiMon le operazioni di RegSetValue, RegCreateKey, RegDeleteValue, RegDeleteKey.

Risultati:

- **RegSetValue**: Sono state registrate diverse modifiche alle chiavi di registro, indicando che il malware ha modificato le impostazioni del sistema.
- **RegCreateKey**: Non sono state registrate operazioni di creazione di nuove chiavi.
- **RegDeleteValue**: Non sono state registrate operazioni di eliminazione di valori di registro.
- **RegDeleteKey**: Non sono state registrate operazioni di eliminazione di chiavi di registro.

7. Salvare il Log

Ho salvato il log di MultiMon per ulteriori analisi e documentazione.

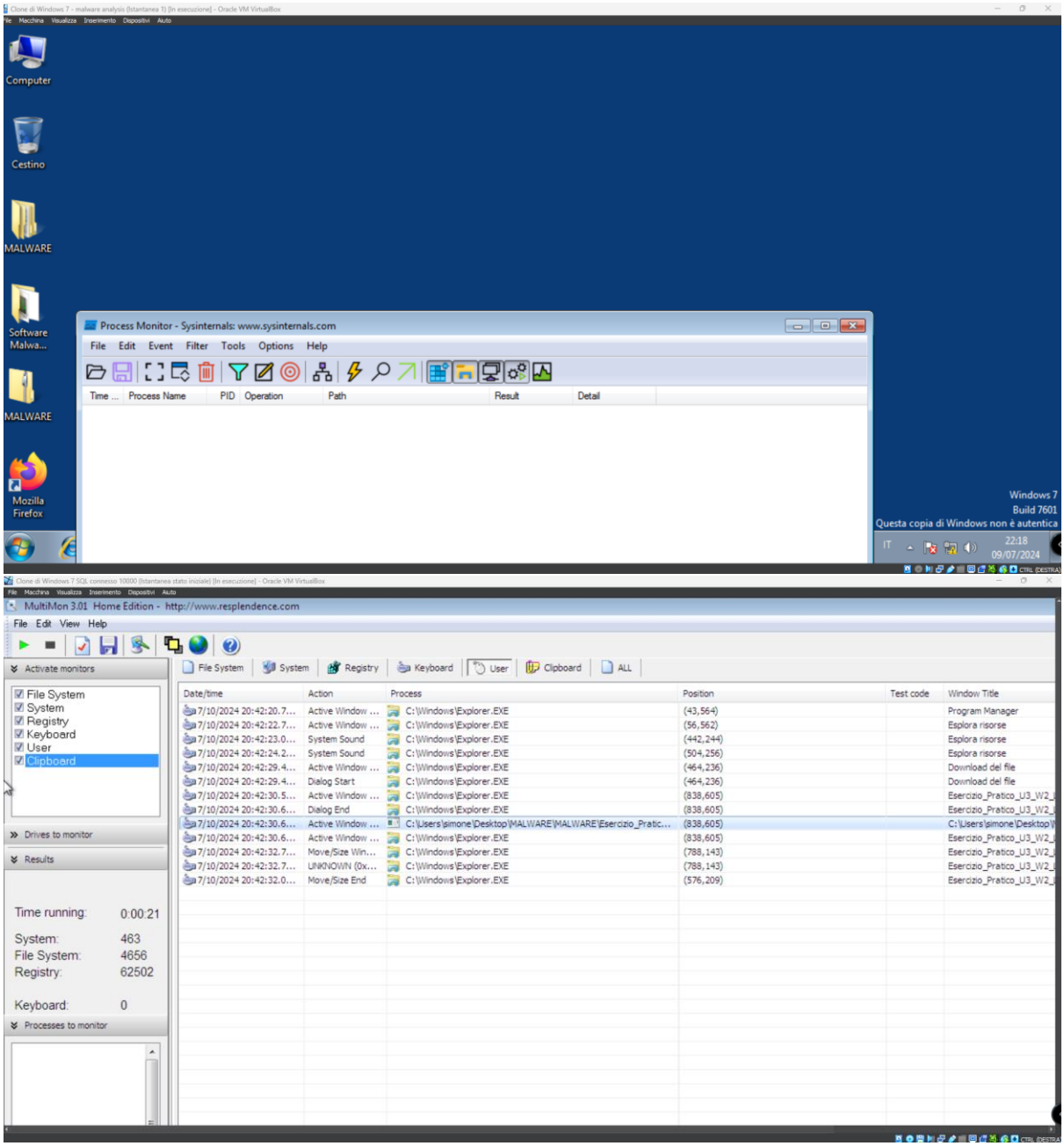
8. Ripristino della Macchina Virtuale

Dopo aver completato l'analisi, ho ripristinato la macchina virtuale utilizzando l'istantanea creata all'inizio.

Conclusioni

L'analisi dinamica del malware ha rivelato che il malware ha effettuato diverse operazioni di creazione, lettura e scrittura di file, oltre a creare e terminare processi e thread. Ha anche effettuato modifiche significative al registro di sistema. Questi comportamenti sono tipici di malware che cercano di monitorare le attività dell'utente, come un keylogger.

Screenshot


Computer
Cestino
MALWARE
Software Malwa...
MALWARE
Mozilla Firefox
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Windows 7
Build 7601
Questa copia di Windows non è autentica
IT
22:18
09/07/2024
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: 0:00:21
System: 463
File System: 4656
Registry: 62502
Keyboard: 0
Processes to monitor
File System System Registry Keyboard User Clipboard ALL
Date/time Action Process Position Test code Window Title
7/10/2024 20:42:20.7... Active Window ... C:\Windows\Explorer.EXE (43,564) Program Manager
7/10/2024 20:42:22.7... Active Window ... C:\Windows\Explorer.EXE (56,562) Esplora risorse
7/10/2024 20:42:23.0... System Sound C:\Windows\Explorer.EXE (442,244) Esplora risorse
7/10/2024 20:42:24.2... System Sound C:\Windows\Explorer.EXE (504,256) Esplora risorse
7/10/2024 20:42:29.4... Active Window ... C:\Windows\Explorer.EXE (464,236) Download del file
7/10/2024 20:42:29.4... Dialog Start C:\Windows\Explorer.EXE (464,236) Download del file
7/10/2024 20:42:30.5... Active Window ... C:\Windows\Explorer.EXE (838,605) Esercizio_Pratico_U3_W2_
7/10/2024 20:42:30.6... Dialog End C:\Windows\Explorer.EXE (838,605) Esercizio_Pratico_U3_W2_
7/10/2024 20:42:30.6... Active Window ... C:\Users\simone\Desktop\MALWARE\MALWARE\Esercizio_Pratic... (838,605) C:\Users\simone\Desktop\
7/10/2024 20:42:30.6... Active Window ... C:\Windows\Explorer.EXE (838,605) Esercizio_Pratico_U3_W2_
7/10/2024 20:42:32.7... Move/Size Win... C:\Windows\Explorer.EXE (788,143) Esercizio_Pratico_U3_W2_
7/10/2024 20:42:32.7... UNKNOWN (0x... C:\Windows\Explorer.EXE (788,143) Esercizio_Pratico_U3_W2_
7/10/2024 20:42:32.0... Move/Size End C:\Windows\Explorer.EXE (576,209) Esercizio_Pratico_U3_W2_