Esercitazione W21D1 - Pratica 1

Malware Analysis: Analisi dinamica basica

Fabio Benevento - 26/03/2024

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:

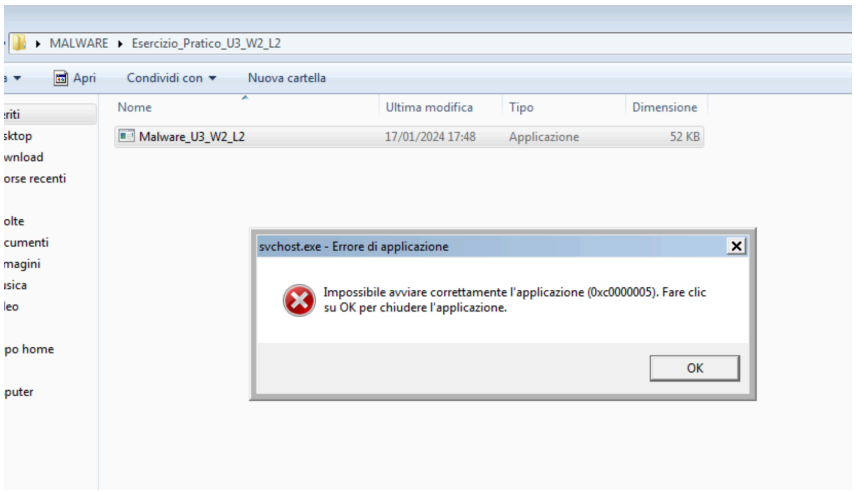
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
- Identificare le eventuali modifiche del registro dopo l'esecuzione del malware (le differenze)

Implementazione

Dopo aver avviato Procmon ho lanciato il malware Malware_U3_W2_L2, quindi dopo circa un minuto ho stoppato la cattura.

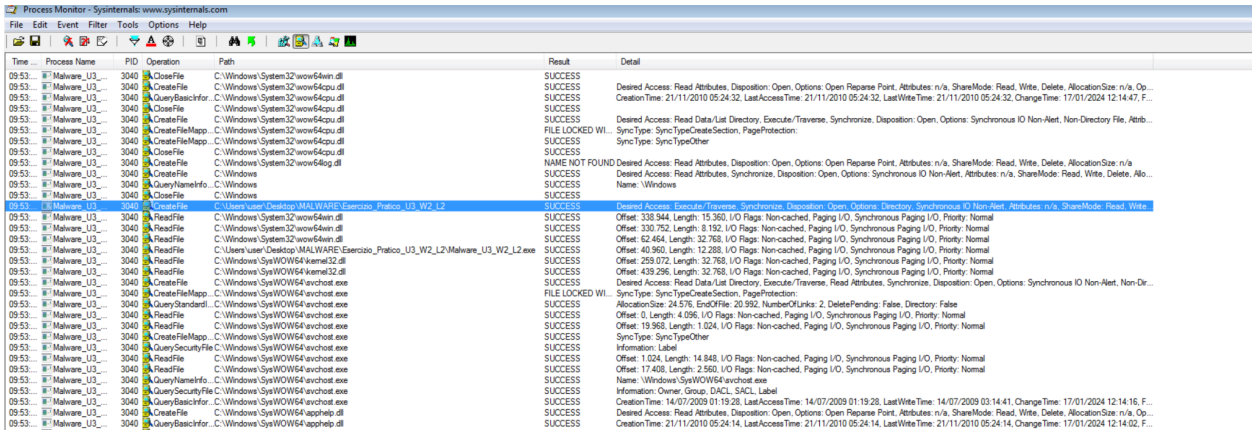
L'esecuzione del malware termina con un errore come mostrato in figura.

Una volta stoppata l'esecuzione ho filtrato per nome del processo al fine di limitare i risultati della cattura al solo malware.



1. Identificare eventuali azioni del malware sul file system

Filtrando ulteriolmente per i soli eventi del file system è possibile individuare numerose operazioni di creazione e lettura/scrittura di file. Alcune di queste vanno a buon fine (SUCCESS) altre invece vengono bloccate dal sistema operativo o comunque non vanno a buon fine (FILE LOCKED, NAME NOT FOUND...)

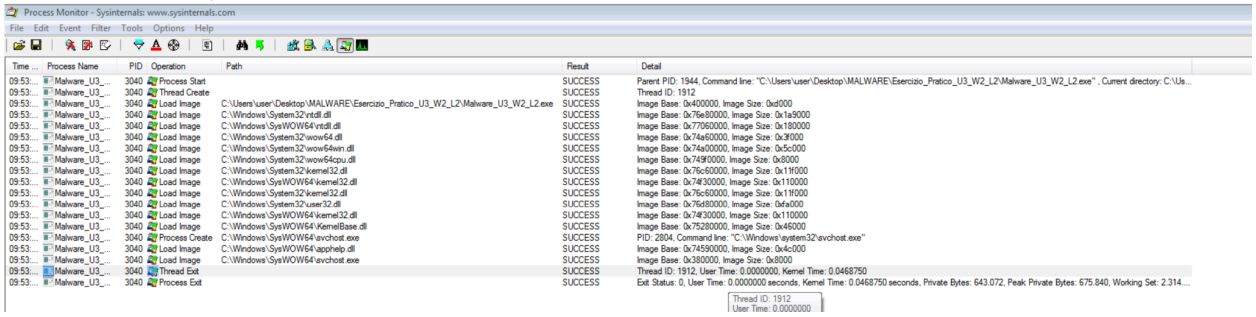


2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

Analizzando le operazioni svolte dal malware su processi e thread, è possibile notare che una volta partito il malware crea un nuovo thread, dopo di che effettua diverse operazioni di caricamento di librerie (Load Image).

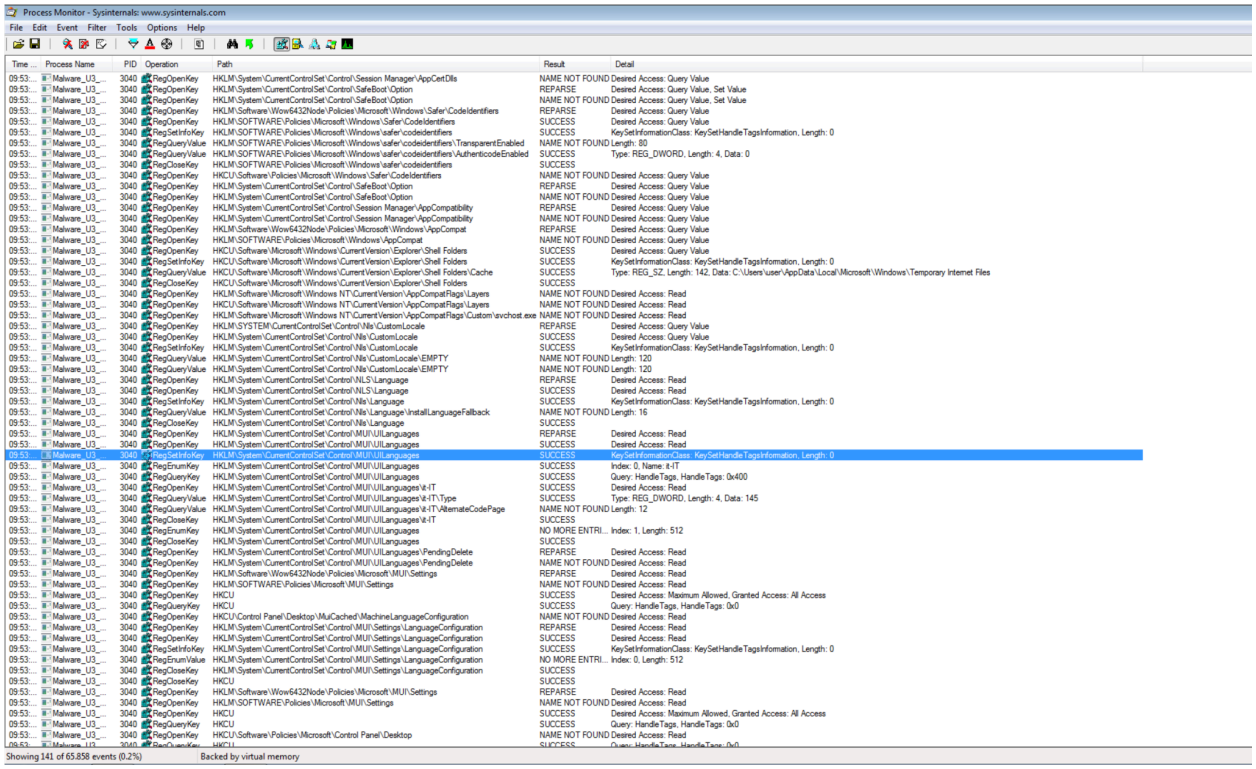
Nel mezzo di queste operazioni ciò che salta all'occhio è un tentativo da parte del malware di creare un sottoprocesso con nome svchost.exe. Svchost.exe è un processo

normalmente presente nei sistemi operativi Windows. Molto probabilmente il malware tenta di avviare delle operazioni “nascondendosi” dietro il processpo lecito svchost.exe. L’operazione va a buon fine e viene creato un nuovo processo con PID 2804



3. Identificare le eventuali modifiche del registro dopo l’esecuzione del malware

Filtrando all’interno di Procmon per le sole operazioni relative al registro di sistema, è possibile identificare numerose operazioni di lettura/scrittura di chiavi del registro.



Prendendo in esame tra le tante la riga selezionata, ad esempio, esso riguarda la modifica (RegSetHotKey) di una chiave sotto il path (HLKM\System\CurrentControlSet\Control\MUI\UILanguages) che fa quindi supporre la modifica di chiavi inerenti la lingua di sistema. Cliccando sull'evento per maggiori dettagli è possibile vedere che la chiave nello specifico è la chiave KeySetHandleTagInformation e l'operazione va a buon fine (SUCCESS.)