S10L2 - MALIZIA MARCO | DATASHIELDS

TRACCIA
In questo report descrivo dettagliatamente l'analisi dinamica che ho condotto su un malware eseguibile presente nella cartella Esercizio_Pratico_U3_W2_L2 situata sul desktop della macchina virtuale dedicata all'analisi dei malware.
L'obiettivo dell'analisi è rispondere ai seguenti quesiti:

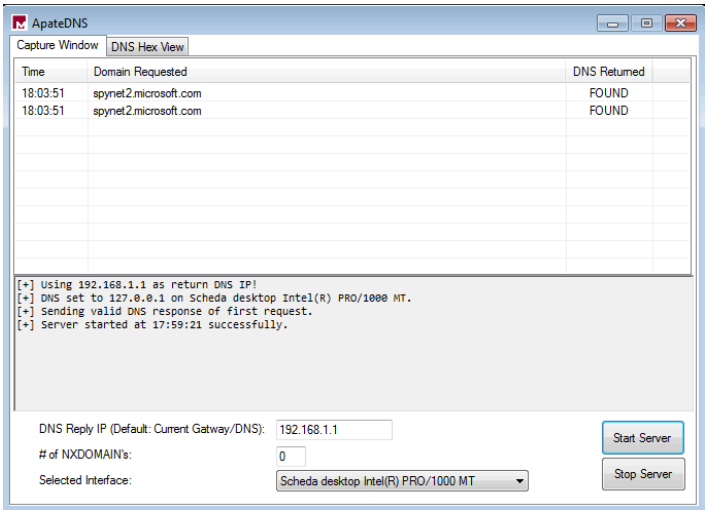
- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (Procmon).
- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor.
- Rilevare le modifiche del registro dopo l'esecuzione del malware.
- Profilare il malware in base alla correlazione tra «operation» e Path.

SVOLGIMENTO

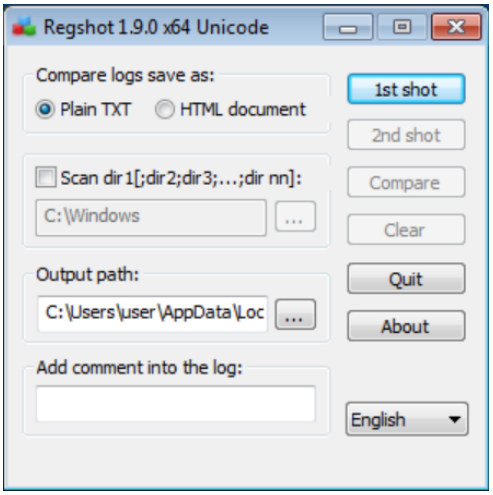
1. Per prima cosa configuriamo la macchina virtuale per l'analisi dinamica in modo tale che ci consenta di lavorare in modo più sicuro:
    - Nelle impostazioni di rete impostiamo inizialmente la connessione NAT per scaricare pacchetti e software necessari, per poi impostarla su INTERNA cosi da garantirci meno possibilità di propagazione del file malevolo.
    - Disabilitiamo inoltre l'opzione riguardante i device usb per evitare che il malware si propaghi anche sulla macchina fisica.

    Una volta scaricati i software necessari possiamo creare un'istantanea della macchina virtuale, in modo tale da avere un backup qualora ce ne fosse bisogno.

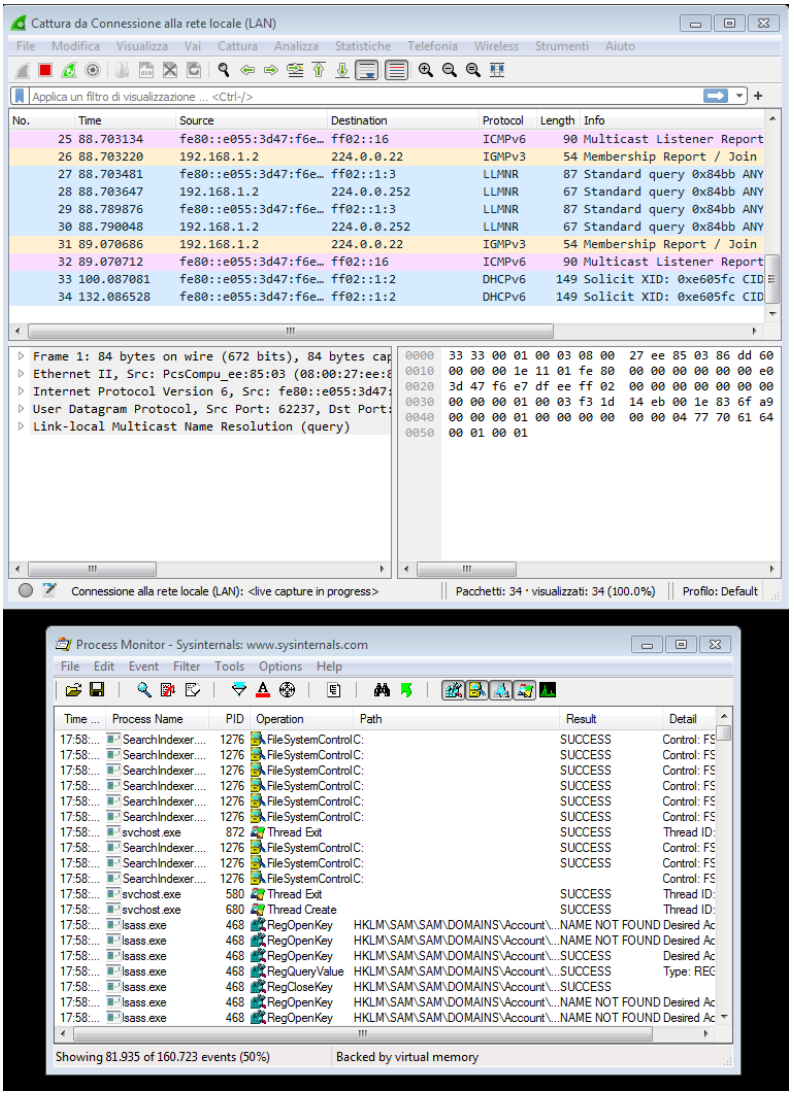
2. Una volta tornati su rete INTERNA possiamo configurare l'indirizzo IP su statico, cosi da poter configurare il server in apaceDNS, dove ci verrà richiesto l'indirizzo IP Gateway



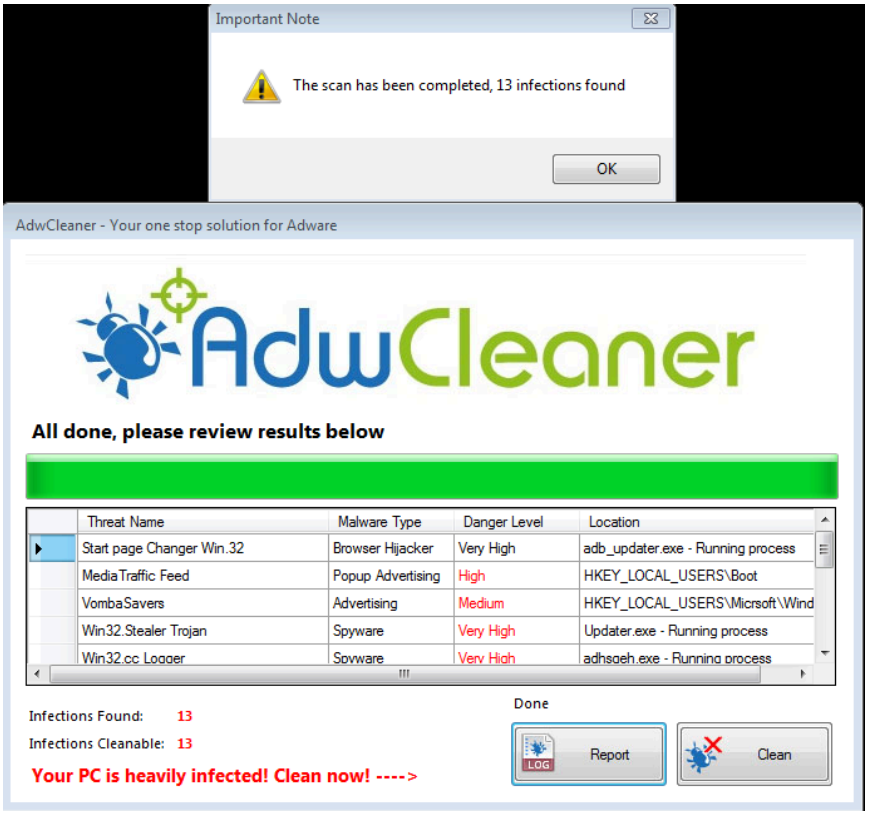
3. Proseguiamo avviando Regshot, tool necessario per creare un'istantanea del registro cosi da poter visionare probabili modifiche effettuate dall'esecuzione del Malware.



4. Prima di eseguire il file malevolo è necessario avviare i software di ascolto, quali Wireshark e Procmon, fondamentali per poter avere in tempo reale ogni operazione eseguita dal Malware da testare.

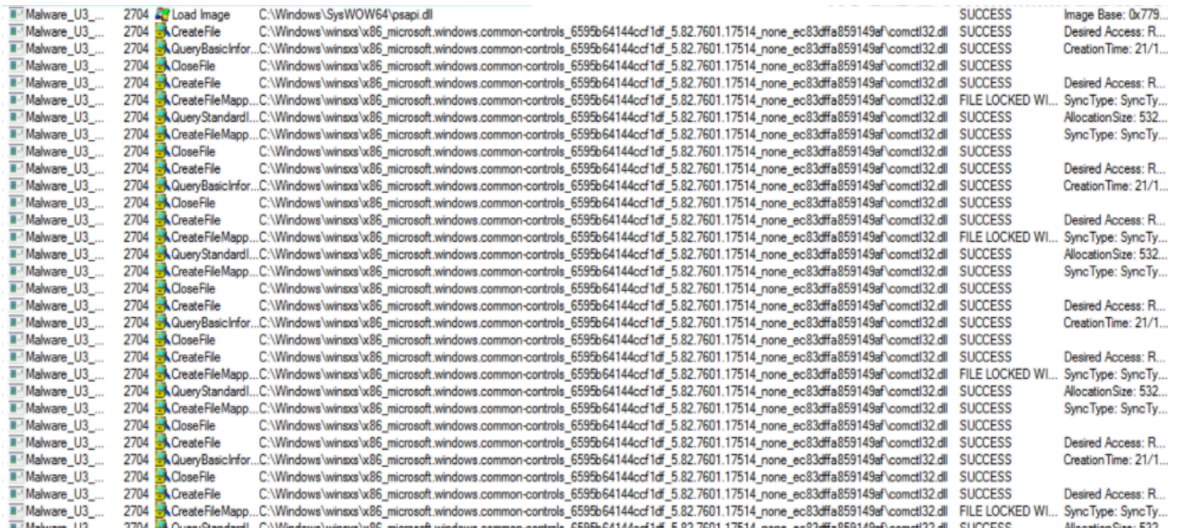


5. Procediamo avviando l'eseguibile malevolo ADWCLEANER che, come possiamo vedere dalla gui, effettuerà uno scan.



Ovviamente essendo un Malware va a far finta di collaborare con la macchina e ci da un messaggio finto simulando una scansione del pc in cui vengono segnalati 13 infezioni e alcuni problemi sulla macchina, in realtà spostandosi sul tool di PROCMON possiamo visionare che ha eseguito molte operazioni dubbie che ci mostrano le vere intenzioni del file malevolo.
Analizzando i risultati su PROCMON possiamo vedere che ci sono:

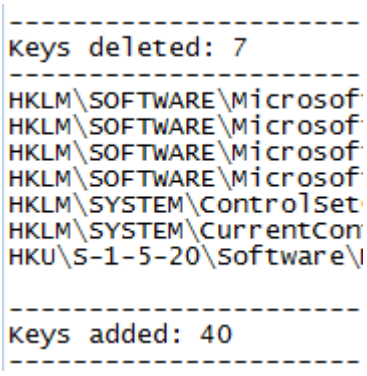
- richieste di creazione file
- richieste di registro
- modifiche di file di sistema



6. Analizzando meglio le operazioni possiamo notare che le operazioni riguardanti la creazione di file, sono andate a toccare file nelle directory molto critiche come **C:\Windows\SysWOW64** e **C:\Windows\System32**.
   Inoltre le richieste di lettura e modifica file hanno scritto dati su file di sistema importanti alterandone cosi il funzionamento e l'affidabilità.
   Per quanto riguarda le operazioni di thread possiamo notare principalmente due gruppi, PROCESS CREATE e THREAD CREATE.
   Il primo riguarda la creazione di nuovi processi, inclusi diversi eseguibili **svchost.exe** che potrebbero essere utilizzati per nascondere attività malevole, mentre il secondo, creazione di nuovi thread all'interno di processi esistenti, suggerendo che il malware potrebbe tentare di iniettare codice nei processi legittimi per eseguire le sue operazioni.

7. Per quanto riguarda le modifiche riguardanti il registro, grazie a PROCMON, abbiamo notato che ci sono richieste di "RegSetValue e RegCreateKey" in cui sostanzialmente il malware ha creato e modificato chiavi di registro per garantire l'esecuzione automatica all'avvio del sistema e potenzialmente per alterare configurazioni di sicurezza.
   Un altro gruppo di operazioni potenzialmente dannose riguarda l'aggiunta di chiavi nel path indicato, **HKLM\Software\Microsoft\Windows\CurrentVersion\Run,** che dopo una ricerca, ci ha indicato che il malware ha la garanzia di essere eseguito automaticamente all'avvio del sistema.

8. Tornando su REGSHOT possiamo eseguire un secondo shot del registro per andare a comparare le due situazioni, pre e post malware attack.



   Come possiamo vedere ci sono alcune modifiche, tra le tante scansionate abbiamo l'eliminazione di alcune chiavi di sistema, che successivamente sono state sostituite con l'aggiunta di molte altre chiavi che, come detto pocanzi, rappresentano una situazione molto critica.
   Inoltre possiamo visionare in fondo alla comparazione il numero di mutazioni di registro effettuate dal malware. (purtroppo lo screenshot del registro non è reperibile)

9. In conclusione, volevamo sottolineare l'importanza dell'analisi dinamica, poichè ha rivelato che il malware esegue diverse operazioni malevole, tra cui la modifica di file di sistema, la creazione di processi sospetti e la modifica del registro per garantire sua la persistenza. Le tecniche utilizzate dal malware includono l'alterazione di directory critiche e l'uso di processi legittimi per mascherare le sue attività.
   Utilizzare strumenti come Procmon è cruciale per monitorare e analizzare tali comportamenti, al fine di sviluppare misure di difesa efficaci contro minacce simili.
   Questo report fornisce una visione dettagliata delle attività del malware e delle tecniche utilizzate per identificare e analizzare il problema, rappresentando un esempio pratico di come condurre un'analisi dinamica in un ambiente controllato.