EPICODE

Esercizio S10 – L2

TRACCIA

Configurare la macchina virtuale per l’analisi dinamica (il malware sarà effettivamente eseguito). Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L1» 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.  
• Modifiche del registro dopo il malware(le differenze).  
• Provare a profilare il malware in base alla correlazione tra «operation» e Path.

SOLUZIONE

Per iniziare l’esercizio di analisi dinamica bisogna creare un ambiente sicuro. Si è così configurato Windows 7 con una scheda di rete interna, si è disabilitato l’USB e si è creata un’istantanea da poter ripristinare nel caso in cui la macchina venga compromessa.

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

Successivamente si sono aperti i programmi Process Monitor (procmon) e Regshot. Dopo aver attivato la cattura su Process Monitor e aver effettuato il primo “shot” su Regshot si è avviato il malware di test. Dopo circa 30 secondi si è fermata la cattura e si è effettuato il secondo shot. Di seguito vengono mostrati i risultati del test e le analisi effettuate.

• Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon).

Immagine che contiene testo, schermata, software, numero

Descrizione generata automaticamente

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

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

• Modifiche del registro dopo il malware(le differenze)

Immagine che contiene testo, schermata, numero, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Carattere

Descrizione generata automaticamente

Sembra che il malware sia un rootkit. Tenta diverse operazioni creando file all’interno di “System 32” grazie al processo “conhost.exe” generato da “csrss.exe”.