**Report S10 L2**

**Analisi Dinamica Basica**

**Traccia:**

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:

1. Identificare eventuali azioni del malware sul file system utilizzando Process Monitor
2. Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor
3. Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Come richiesto dall’esercizio, andiamo ad analizzare le azioni del malware che impattano sul file system, per fare ciò utilizziamo ProcMon, un tool che ci permette di monitorare i processi in esecuzione sulla macchina:

Immagine che contiene testo, schermata, numero, software

Descrizione generata automaticamente

Analizzando i processi ci siamo accorti di un processo che crea un file di testo chiamato praticalmalwareanalysis nella cartella dove risiede il malware.

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Apriamo il file per notare che contiene alcuni dei nostri caratteri inseriti da tastiera, questo è un tipico comportamento dei Key Logger

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Utilizzando la cattura precedente di ProcMon e cliccando sull’icona “Processi e Thread” andiamo a filtrare i processi che appartengono a quella categoria.

Immagine che contiene testo, software, linea, numero

Descrizione generata automaticamente

Abbiano notato che il malware crea un processo chiamato Svchost.exe, che è il nome di un processo generalmente valido di Win. Questo comportamento è tipico dei malware che vogliono camuffare la loro identità e nascondendosi dalle analisi degli antivirus/antimalware così come dalle indagini approfondite di un utente.

Il malware cerca di camuffarsi chiamandosi Svchost, poi esegue la sua funzione principale di Key Logger salvando tutti i caratteri digitati dall’utente in un file chiamato praticalmalwareanalysis.