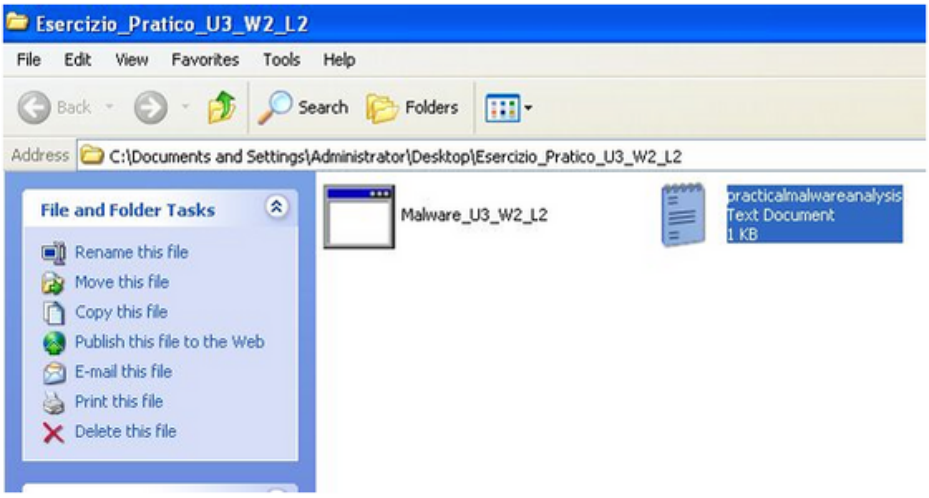
Analisi dinamica basica

Traccia:
Nella lezione teorica del mattino, 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 Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor Provare a profilare il malware in base alla correlazione tra «operation» e Path.

L'analisi dinamica del malware, contrariamente all'analisi statica, si concentra sull'osservazione del comportamento di un file sospetto durante la sua esecuzione in un ambiente controllato. Questo tipo di analisi è essenziale per comprendere le azioni effettive del malware, come la manipolazione di file, processi e la comunicazione di rete. Utilizzando strumenti come Process Monitor (Procmon), gli analisti possono rilevare in tempo reale le operazioni effettuate dal malware sul sistema operativo.

Identificazione delle Azioni sul File System
Per iniziare l'analisi, è necessario avviare Procmon prima dell'esecuzione del malware per catturare tutte le sue attività. Dopo l'avvio del malware, identificato come "Malware_U3_W2_L2.exe", e una cattura di circa un minuto, si ferma la registrazione per analizzare le operazioni registrate. È importante assicurarsi che Procmon sia effettivamente attivo e non bloccato, come indicato dalla presenza o assenza di una "X" rossa sull'icona di cattura.
Applicando un filtro per visualizzare solo le attività relative al processo del malware, si osservano operazioni chiave come "Create File", "Read File" e "Close File" con i relativi percorsi. Un esempio significativo è la creazione di un file di testo nel percorso dove risiede il malware, suggerendo un'operazione diretta sul file system. L'analisi del file creato, denominato "practicalmalwareanalysis", rivela che il malware registra i tasti premuti dall'utente, un comportamento tipico dei keylogger.



Identificazione delle Azioni su Processi e Thread
Oltre alle operazioni sul file system, l'analisi con Procmon permette di identificare azioni del malware sui processi e sui thread. Filtrando gli eventi per questi elementi, si notano operazioni come "Load Image" per il caricamento del malware e delle sue librerie necessarie, e "Process Create" per la creazione di nuovi processi. In particolare, il malware sembra creare un processo chiamato "svchost.exe", un nome comunemente utilizzato da processi legittimi di Windows, nel tentativo di mascherare la sua presenza e attività sul sistema infetto.
Conclusioni Finali
Dall'analisi dinamica emerge che il malware analizzato adotta una strategia multiplo: inizialmente cerca di celare la sua esecuzione mediante la creazione di un processo con un nome legittimo, "svchost.exe", per evitare rilevamenti da parte di soluzioni antivirus o anti-malware. Successivamente, esegue la sua funzione principale, agendo come un keylogger per catturare e salvare gli input da tastiera dell'utente in un file specificamente creato a questo scopo, "practicalmalwareanalysis", situato nella stessa cartella dell'eseguibile. Questo approccio riflette una sofisticata conoscenza delle tecniche di evasione e di raccolta dati, evidenziando l'importanza dell'analisi dinamica nell'identificare e comprendere il comportamento effettivo dei malware. L'abilità del malware di mascherare le sue operazioni sotto processi legittimi e di registrare input sensibili dell'utente dimostra il suo potenziale impatto dannoso e la necessità di adottare strategie di sicurezza informatica proattive e multilivello.