Analisi dinamica basica

Traccia:

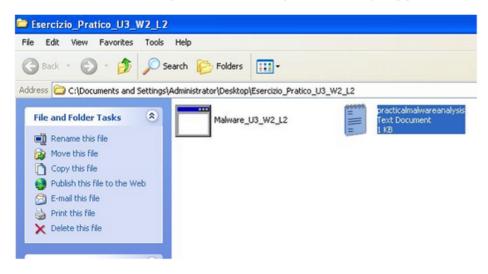
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica. Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, 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.



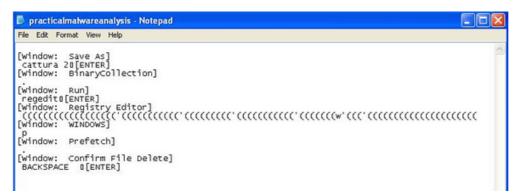
Identificazione delle Azioni su Processi e Thread

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 antimalware. 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.





※ Process Mandar - Systemathy www.systemath.com Fine tot: Ever Fiber Took Options Heb 応日 東京で ウム寺 図 典末 成込みで置									
					Time of Day: Process Name	PID Operation	Pub.	Rest	Detail
					:324430090 Malnare_U3_W2_L2-exe	3100 All Process Start		SUCCESS	Farest PID: 1928, Command line: "C1/Documents and Settings/Vidninis
132.44.30898 Malmare, U3, W2, L2 eve	3100 2 Thread Deale		SUCCESS	Thread ID: 3164					
132.44.30959 Malware U3,W2,L2 eve	3190 All Load Image	C \Documents and Settings\Administrato\Decktop\Esercisio, Pratico_U2_W2_L2Mdware_U2_W2_L2 eve	SUCCESS	Image Base: 0x400000; Image Size: 0xd000					
32.44.30972. Malmare US W2 L2 eve	2190 All Load Image	C:NvINDOv/S/upsten32/vidil.dll	SUCCESS	Image Base: 0x7c900000, Image Siox: 0xel000					
32.44.33752 Malware U3 W2 L2 eve	3190 2 Load Image	C:\laft\00\signs\2\kens02\kens02\d	SUCCESS	Image Base: 0x7c800000, Image Size: 0x6000					
32.44.34936 "Malware U3_W2_L2.eve	2190 A Load Image	C:NrfNDOvrS/usstem22/apphelp.dl	SUCCESS	Image Bank 0x77b40000, Image Sizk 0x22000					
3244.35359. Malware U3 W2 L2 eve	3190 2 Load Image	C VoRXO Ovr5 (under 22 version dil	SUCCESS	Image Bane: 0x77x00000, Image Size: 0x8000					
32.44.36525 "Malware U3 W2 L2 eve	2190 A Load Image	C NeWOOWS (system 22 and repolit) all	SUCCESS	Image Bane: 0x77dd0000, Image Size: 0x9b000					
32.44.36348 "Malmare U3 W2 L2 eve	3190 All Load Image	C \\n!\NOO\n'\S\upstand2\upor\l.dl	SUCCESS	Image Bane: 0x77x70000, Image Size: 0x92000					
32.44.36968 "Malware U3 W2 L2 eve	2190 A Load Image	C \land \text{\tince{\text{\tex{\tin\text{\texi}\text{\text{\text{\text{\text{\texi}\tint{\text{\text{\text{\texi}\text{\text{\texi}\tint{\text{\texi}\tint{\text{\text{\texi}\tint{\text{\texi}\text{\texit{\text{\tex{	SUCCESS	Image Base: 0x77le0000, Image Size: 0x11000					
32.44.37741 Malean US W2 L2 ess	2000 Ft. Process Create	C Neth D Over Content 2 Archest eve	SUCCESS	PD: 2688. Command line: "C NeWOOWS content22 and not easi."					
32.45.37431 "Malmare US_W2_L2.eve	2100 😂 Thread Exit		SUCCESS	Thread ID: 3164, User Time: 0.0000000, Kernel Time: 0.0625000					
3245 37643 Malmare U3 W2 L2 eve	2100 R Process Ent		SUCCESS	Exit Status: 0. User Time: 0.0156250 seconds. Kernel Time: 0.0625000					