MALWARE ANALYSIS

W24D4 - Pratica

Parametri passati alla funzione *main*:

I seguenti sono passati nella funzione *main:*

argc: Questo intero che rappresenta il numero di argomenti passati al programma alla sua esecuzione.

argv: Questo puntatore è array di puntatori esso contiene elementi corrispondenti ad argomenti comando.

envp: Questo paramento contiene variabili d'ambiente che utilizzano chiave-valore che forniscono informazioni sull'ambiente di esecuzione del programma, come i percorsi di sistema, preferenze utente e impostazioni lingua.

Variabili utilizzate nella funzione:

- *hModule*: Una variabile DWORD 32 bit che memorizza l'handle del modulo.
- *Data*: Un array di byte utilizzato per memorizzare dati.
- *var_117*: Una variabile a byte singolo.
- *var_8*: Una variabile DWORD a 32 bit che memorizza un indirizzo di un puntatore.
- *var_4*: Una variabile DWORD a 32 bit utilizzata per lo storage temporaneo.

Librerie importate e utilizzate dal Malware:

Tra le librerie utilizzate troviamo: *kernel32.dll* questa libreria importa la funzione *ds:GetModuleHandleA:* che a sua volta permette iniettare codice malevolo caricando una libreria dannosa e *ds:GetModuleFileNameA:* Importata sempre da *kernel32.dll* può recuperare il percorso del file eseguibile.

Locazione di memoria:

La locazione di memoria *00401021* è un istruzione ad una chiamata *ds:RegCreateKeyExA* essa

può essere utilizzata per creare o manipolare una chiave del registro di Windows.

L'istruzione *“push” offset SubKey* è un'istruzione che in assembly viene utilizzata per inserire il valore dell'offset di una variabile chiamata SubKey nello stack della CPU.

In questo caso la funzione *RegCreateKeyExA* precedente, potrebbe essere utilizzata per passare l'indirizzo di memoria della variabile SubKey come parametro alla funzione. Questo consente di accedere e utilizzare il valore di SubKey.

In conclusione "push" *offset SubKey* è stata utilizzata per passare l'indirizzo di memoria di una variabile come parametro a una funzione, consentendo di accedere a quel valore durante l'esecuzione del malware.

Utilizzando IDA possiamo notare che alla locazione *00401047* viene effettuata una “call” (chiamata) al parametro *ds:RegSetValueExA*, questa operazione è usata per passare la funzione *RegSetValueExA* all’interno del segmento di dati *ds.*

Sezioni/Segmenti del Malware:

La sezione di codice "*.text*" all'interno dell'eseguibile .exe sembra tentare di creare una nuova chiave nel registro di Windows utilizzando la funzione *RegCreateKeyExA*. Esso può essere utilizzato per manipolare l'esecuzione e l'avvio di alcune applicazioni.

Solitamente la creazione o la modifica delle chiavi di registro è una tecnica comune utilizzata dal malware per stabilire la persistenza su un sistema o manomettere l'esecuzione dei programmi.

Analisi dinamica:

Il malware in questione al suo avvio effettua la funzione *RegCloseKey* è una funzione dell'API di Windows utilizzata per chiudere un'handle a una chiave del Registro di Windows.

Il malware può utilizzare la funzione *RegCloseKey* per pulire la propria presenza, modificare le impostazioni del sistema o eseguire azioni dannose al sistema.

Successivamente il malware utilizza le seguenti funzioni:

RegOpenKey: Questa funzione viene utilizzata per aprire una determinata chiave del Registro di sistema. Questa funzione può essere sfruttata per accedere a una chiave specifica in modo da poter leggere o modificarne il contenuto.

RegQueryValue: Questa funzione viene utilizzata per recuperare il valore all'interno di una chiave del Registro di sistema. Tramite *RegQueryValue* il malware può trovare informazioni sensibili o per verificare la presenza di determinate impostazioni nel Registro di sistema.

RegSetInfoKey: Questa funzione viene utilizzata per impostare una chiave del Registro di sistema. L’eseguibile malevolo utilizza *RegSetInfoKey* per modificare le autorizzazioni di accesso, i permessi di scrittura o altre impostazioni di una chiave del Registro di sistema con il fine di nascondere la propria presenza o impedire la rimozione.

L’utilizzo di queste funzioni può permettere al malware di nascondere o midificare le chiavi del Registro.

La modifica dei file avviene probabilmente tramite le operazioni IRP (Input/Output Request Packet sfruttando *IRP_MJ* con permessi di sistema, esso può essere sfruttato per creare o modificare file, creare una persistenza sul sistema o danneggiare il sistema operativo.