

Dall’estratto di questo codice deduciamo che il malware sta utilizzando una combinazione di tecniche per ottenere persistenza nel sistema operativo e sta probabilmente operando come un Trojan, poiché cerca di nascondere la sua presenza e eseguire azioni dannose sul sistema senza il consenso dell'utente.

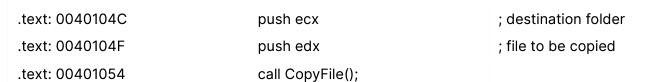
Tipo di Malware: Trojan

Chiamate di funzione principali:

SetWindowsHook(): Questa funzione viene utilizzata per impostare un hook di Windows, specificamente un hook del mouse in questo caso. Gli hooks di Windows consentono a un'applicazione di monitorare il comportamento del sistema o di intercettare eventi come l'input dell'utente. Nel contesto di un malware, potrebbe essere utilizzato per registrare l'input dell'utente o per monitorare l'attività del mouse allo scopo di raccogliere informazioni sensibili.



CopyFile(): Questa funzione viene utilizzata per copiare un file da una posizione all'altra nel sistema operativo. Nel contesto di un malware, potrebbe essere utilizzata per copiare se stessa in una posizione specifica, probabilmente all'interno della cartella di avvio o di sistema, al fine di garantire la sua esecuzione automatica all'avvio del sistema.



Metodo di persistenza:

Il malware utilizza la funzione CopyFile() per copiare se stesso in una posizione specifica, probabilmente all'interno della cartella di avvio o di sistema. Questo assicura che il malware venga eseguito automaticamente ogni volta che il sistema operativo viene avviato, garantendo così la sua persistenza nel sistema. La copia potrebbe essere mascherata come un file legittimo o utilizzare un nome simile a un processo di sistema per evitare la rilevazione da parte degli utenti.

BONUS

Analisi a basso livello delle istruzioni presenti nel codice:

.text: 00401010 push eax

Questa istruzione mette il contenuto del registro eax nello stack.

.text: 00401014 push ebx

Analogamente, mette il contenuto del registro ebx nello stack.

.text: 00401018 push ecx

Mette il contenuto del registro ecx nello stack.

.text: 0040101C push WH\_Mouse

Questa istruzione mette il valore WH\_Mouse nello stack. WH\_Mouse è probabilmente un valore numerico che indica il tipo di hook da impostare (nel caso specifico, un hook per il mouse).

.text: 0040101F call SetWindowsHook()

Effettua una chiamata alla funzione SetWindowsHook() per impostare l'hook di Windows.

.text: 00401040 XOR ECX,ECX

Esegue un'operazione di XOR tra il registro ecx e se stesso, impostando il registro ecx a zero.

.text: 00401044 mov ecx, [EDI]

Copia il contenuto del puntatore memorizzato nel registro EDI nel registro ecx. Questo suggerisce che il malware sta ottenendo un percorso per una cartella dalla memoria.

EDI = «path to startup\_folder\_system»

Un commento indica che il registro EDI contiene il percorso alla cartella di avvio di sistema.

.text: 00401048 mov edx, [ESI]

Copia il contenuto del puntatore memorizzato nel registro ESI nel registro edx. Questo suggerisce che il malware sta ottenendo un percorso per un file dalla memoria.

ESI = path\_to\_Malware

Un commento indica che il registro ESI contiene il percorso al malware stesso.

.text: 0040104C push ecx

Mette il percorso della cartella di avvio di sistema nello stack.

.text: 0040104F push edx

Mette il percorso del malware nello stack.

.text: 00401054 call CopyFile()

Effettua una chiamata alla funzione CopyFile() per copiare il malware nella cartella di avvio di sistema.