S10L4

Rosario Z.

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica.

Analisi del codice assembly del malware:

Analisi del codice

Il codice inizia con la funzione sub_401000.
Questa funzione esegue le seguenti operazioni:
Push ebp: Salva il valore del registro ebp sullo stack.
Mov ebp, esp: Imposta il registro ebp su esp.
Push ecx: Salva il valore del registro ecx sullo stack.
Push 1pdwFlags: Salva il valore della variabile 1pdwFlags sullo stack.
Call ds:InternetGetConnectedState: Chiama la funzione InternetGetConnectedState per controllare se il computer è connesso a Internet.
Mov [ebp+var_4], eax: Memorizza il valore restituito dalla funzione InternetGetConnectedState nella variabile [ebp+var_4].
Cmp [ebp+var_4], 8: Confronta il valore della variabile [ebp+var_4] con 8.
Jz short loc_401028: Se il valore della variabile [ebp+var_4] è uguale a 8, salta alla posizione loc_401028.
Push offset aSuccessInterne: Salva l'indirizzo della stringa "Success: Internet Connection\n" sullo stack.
Call sub_40117F: Chiama la funzione sub_40117F per stampare la stringa "Success: Internet Connection\n".
Jmp short loc_40103A: Salta alla posizione loc_40103A.
Loc_401028: Push offset aError1: Salva l'indirizzo della stringa "Error 1.1: No Internet\n" sullo stack.
Add esp, 4: Incrementa il valore del registro esp di 4.
Push 1NoInte: Salva il valore 1 sullo stack.
Call sub_40117F: Chiama la funzione sub_40117F per stampare la stringa "Error 1.1: No Internet\n".
Add esp, 4: Incrementa il valore del registro esp di 4.
Jmp short loc_40103A: Salta alla posizione loc_40103A.
Loc_40103A:
Mov esp, ebp: Ripristina il valore del registro esp da ebp.
Pop ebp: Ripristina il valore del registro ebp dallo stack.
Retn: Restituisce il controllo al chiamante.

Questo codice va a visualizzare lo stato della connessione ad internet.