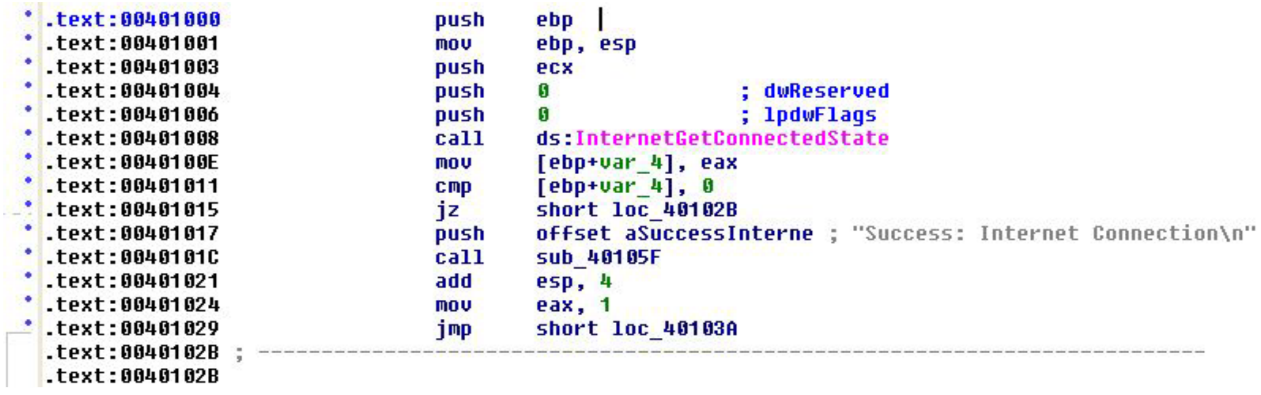
Assembly X86 - Costrutti C

Analisi del seguente codice assembly



Il codice assembly è una porzione di codice di un malware. Di seguito riporto i costrutti noti:

- La prima riga corrisponde all'indirizzo di memoria della prima istruzione del codice mostrato. Questa istruzione viene utilizzata per salvare il valore del registro ebp nello stack. In seguito, il valore del registro ebp viene utilizzato per creare una nuova cornice di attivazione per la funzione corrente, consentendo all'assembly di gestire le variabili locali e i parametri della funzione in modo appropriato.
  In sintesi, questa istruzione fa parte della prolog della funzione, ovvero delle istruzioni che vengono eseguite all'inizio della funzione per inizializzare lo stack e configurare l'ambiente di esecuzione.

- Le istruzioni **push ebp e mov ebp**, esp creano una nuova cornice di attivazione per la funzione corrente.
  PS: Il simbolo | viene spesso utilizzato nella programmazione come separatore visivo per distinguere parti di codice. In questo caso specifico. Tuttavia, non ha alcun effetto sulle istruzioni eseguite dalla CPU e viene semplicemente ignorato dal compilatore.
- Le istruzioni **push ecx, push 0 e push 0** caricano i parametri di input per la funzione InternetGetConnectedState.
- **Call ds:InternetGetConnectedState** chiama la funzione InternetGetConnectedState.
- **Mov [ebp+var_4]**, eax salva il valore restituito dalla funzione nella variabile locale [ebp+var_4].
- **Cmp [ebp+var_4]**, 0 confronta il valore restituito con zero.
- **Jz short loc_40102B** salta all'istruzione situata all'indirizzo loc_40102B se il confronto precedente è falso (cioè se il valore restituito è diverso da zero).
- **Push offset aSuccessInterne ; "Success: Internet Connection\n"** carica l'indirizzo della stringa "Success: Internet Connection\n" nello stack.
- **Call sub_40105F** chiama la funzione sub_40105F, passando come parametro l'indirizzo della stringa appena caricata.
- **Add esp**, 4 elimina il parametro dalla pila.

- **Mov eax**, 1 salva il valore 1 nel registro eax.
- **Jmp short loc_40103A** salta all'istruzione situata all'indirizzo loc_40103A.
- L'etichetta **loc_40102B** indica l'inizio di una nuova sezione di codice.
- L'etichetta **loc_40103A** indica la fine della funzione corrente.

In sintesi, il codice assembly controlla se la macchina in cui è eseguito ha accesso ad internet. Se il controllo ha successo, viene visualizzato un messaggio di "Success" e il valore 1 viene salvato nel registro eax. Il codice potrebbe essere parte di una funzionalità più ampia del malware che richiede l'accesso ad internet per funzionare correttamente.