Traccia:

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica. Provate ad ipotizzare che funzionalità è implementata nel codice assembly.

Hint: La funzione internetgetconnectedstate prende in input 3 parametri e permette di controllare se una macchina ha accesso ad Internet.

Dal codice assembly fornito, sembra che il malware stia controllando lo stato della connessione Internet e stampando un messaggio di successo se la connessione è attiva.

- I comandi `push ebp` e `mov ebp, esp` sono tipici dell'inizio di una funzione, dove vengono salvati il puntatore alla base dello stack (EBP) e il puntatore allo stack (ESP).

- Il malware utilizza la funzione `InternetGetConnectedState` per controllare lo stato della connessione Internet.

- Successivamente, il malware confronta il valore restituito da `InternetGetConnectedState` con 0 e, se il valore è uguale a 0, salta a `loc_40102B`, altrimenti stampa il messaggio "Success: Internet Connection" e salta a `loc_40103A`.

- Dall'aspetto del codice, sembra che ci sia una sezione di codice mancante tra gli indirizzi `0040102B` e `0040102F`.

- L'istruzione `mov eax, 1` sembra essere utilizzata per impostare il valore di ritorno della funzione a 1.

- Infine, il malware salta a `loc_40103A`, probabilmente per continuare l'esecuzione del codice successivo dopo la verifica della connessione Internet.

In breve, sembra che il malware stia controllando se c'è una connessione Internet attiva e, se presente, stampa un messaggio di successo.