

Esercizio 30-03

Traccia: identificare i costrutti noti visti durante la lezione teorica presenti nell'estratto di codice di un malware (immagine qui sotto).

Bonus: provare ad ipotizzare che funzionalità è implementata nel codice assembly

Indizio: la funzione `InternetGetConnectedState` prende in input 3 parametri e permette di controllare se una macchina ha accesso ad internet

```
.text:00401000      push    ebp |
.text:00401001      mov     ebp, esp
.text:00401003      push    ecx
.text:00401004      push    0          ; dwReserved
.text:00401006      push    0          ; lpdwFlags
.text:00401008      call    ds:InternetGetConnectedState
.text:0040100E      mov     [ebp+var_4], eax
.text:00401011      cmp     [ebp+var_4], 0
.text:00401015      jz      short loc_40102B
.text:00401017      push    offset aSuccessInterne ; "Success: Internet Connection\n"
.text:0040101C      call    sub_40105F
.text:00401021      add     esp, 4
.text:00401024      mov     eax, 1
.text:00401029      jmp     short loc_40103A
.text:0040102B ; -----
.text:0040102B
```

Questo codice utilizza una logica paragonabile al costrutto if-else del linguaggio C: una volta chiamata la funzione `InternetGetConnectedState`, viene restituito un valore (1=connessione riuscita; 0=connessione fallita), questo valore viene salvato nel registro EAX.

Successivamente il codice sposta il valore di EAX nella `var_4` del registro EBP e lo compara con il valore "0".

Se i due valori corrispondono si attiva `jz` che salta all'indirizzo 40102B, probabilmente l'inizio di della parte di codice dove viene gestita la casistica di mancata connessione a Internet (0=0 => accesso non riuscito => 0 = 0 che porta ad avere lo Zero Flag con valore di 1 che permette l'attivazione di `jz`), questa parte di codice può essere interpretata come "if".

Qualora invece la comparazione risultasse sbagliata (connessione riuscita = 1 => 1≠0), `jz` viene ignorato e si arriva alla funzione `sub_40105F` che stampa a schermo la stringa dell'indirizzo di memoria e dopo aver riportato il valore "1" nel registro EAX salta all'indirizzo di memoria 40103A, questa parte di codice può essere interpretata come "else".

Bonus: la funzionalità di questo codice è stabilire o meno se la macchina ha accesso a Internet e se stampare a schermo un messaggio di successo "Success: Internet Connection", mentre se non ha accesso ad Internet passa ad un'altra porzione di codice.