Assembly analysis

Richiesta: Dato il seguente estratto di codice di un Malware, rispondere ai seguenti quesiti:
1. Identificare i costrutti noti
2. Ipotizzare la funzionalità –esecuzione ad alto livello
3. BONUS: studiare e spiegare ogni singola riga di codice

```
.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
```

Identificazione costrutti noti

Analizzando il codice possiamo identificare:

“cmp [ebp+var_4]”, 0 seguito da “jz short loc_40102B”
Questo rappresenta il costrutto if in C.
cmp confronta il valore della variabile var_4 con 0 e jz (jump if zero) salta al punto indicato se il risultato del confronto è zero (cioè se var_4 è uguale a zero).

“push offset aSuccessInterne; “Success: Internet Connection\n”
“call sub_40105F”
Questo, implicitamente, potrebbe rappresentare else.
Se la condizione dell'if non è soddisfatta (cioè se il sistema è connesso a Internet), il programma non esegue il salto jz e prosegue con le istruzioni successive, che in questo caso includono la stampa o il log di un messaggio.

Funzionalità

Osservando il codice, si può dedurre che:

1. Chiama una funzione API di windows: Il malware chiama InternetGetConnectedState, una funzione dell'API di Windows che determina lo stato della connessione a Internet del sistema.

```
push    0                       ; dwReserved
push    0                       ; lpdwFlags
call    ds:InternetGetConnectedState
```

2. Verifica il valore di ritorno: Dopo la chiamata a InternetGetConnectedState, il malware verifica il valore di ritorno che è stato memorizzato nella variabile locale [ebp+var_4]. Se il valore è zero (che potrebbe indicare che non c'è connessione a Internet), il malware esegue un salto condizionale a loc_40102B.

```
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

3. Gestione casistica successo: Qui, sembra che il malware stia preparando a stampare o loggare un messaggio di successo ("Success: Internet Connection\n") e chiama una subroutine (che potrebbe essere una funzione di stampa o di log) a sub_40105F con questo messaggio come parametro.

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40105F
```

Report finale

La funzionalità complessiva di questo frammento sembra essere la verifica della connettività Internet del sistema e, in base al risultato, esegue azioni differenti (come loggare un messaggio di successo se c'è connettività).