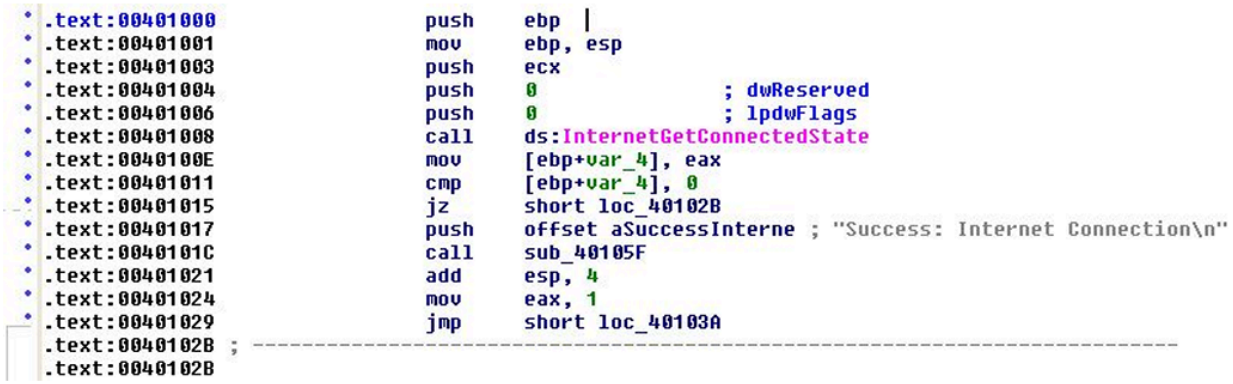
Esercitazione W22D4

Costrutti C - Assembly

Fabio Benevento - 05/04/2024

Traccia

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



```
.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
```

Implementazione

L'estratto di codice sembra fare riferimento alla chiamata di una funzione, nello specifico InternetGetConnectedState, che dal nome fa supporre si occupi molto probabilmente di effettuare un controllo sullo stato di connessione di rete.

Le prime 2 istruzioni, predispongono lo stack per la funzione chiamata, quindi vengono passati 3 parametri, ecx , dwReserved e lpdwFlags, gli ultimi due valorizzati a 0.

Tramite l'istruzione call, viene effettivamente richiamata la funzione il cui risultato viene immagazzinato nel registro eax.

Il risultato viene quindi comparato con il valore 0. In caso positivo viene effettuato un salto ad un'area di codice al di fuori dello snippet, altrimenti (valore diverso da 0 ovvero connessione presente) viene stampato a video il messaggio "Success: Internet Connection\n".

Le restanti istruzioni completano l'esecuzione della funzione ripulendo lo stack.