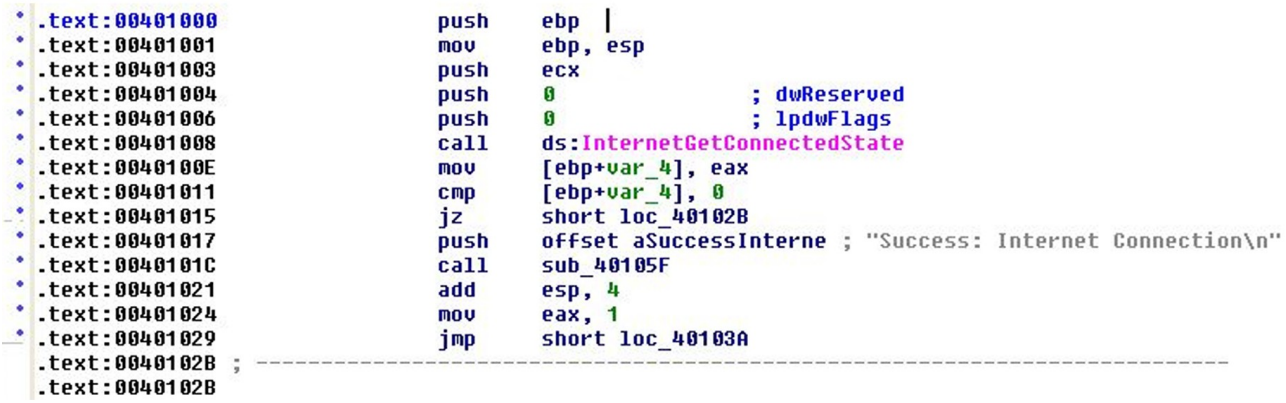
Relazione S10L4

Identificare i costrutti noti in base al codice assembly dato:



```
.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
```

Le istruzioni:

push ebp

mov ebp, esp

indicano la creazione di uno stack.

Le istruzioni:

push 0 ; dwReserved

push 0 ; lpdwFlags

call ds:InternetGetConnectedState

indicano due variabili settate a 0 che vengono poi passate come parametri della funzione **Internet-GetConnectedState.** Il primo parametro è un valore DWORD che indica lo stato della connessione mentre il secondo è un valore riservato che dev'essere impostato a 0.

Avremo quindi che nel codice verrà chiamata la funzione **internetGetConnectedState(param1, param2)** e avrà in ingresso due parametri.

Le istruzioni

mov [ebp+var_4], eax

cmp [ebp+var_4], 0

jz short loc_40102B

indicano che il valore in eax viene copiato nella variabile ebp+var_4 e che viene fatto un compare tra questa variabile e 0.

Viene fatto un jump zero che salta alla locazione indicata se lo zero flag è settato a 1, più precisa-mente alla loc_40102B. Nel caso non sia settato lo ZF vengono eseguite le seguenti istruzioni:

push offset aSuccessInternet; “Success internet Connection\n”

call sub_40105F

add esp, 4

mov eax, 1

jmp short loc_40103A

Queste istruzioni indicano che viene pushato la stringa di connessione avvenuta con successo e viene chiamata una funzione all'indirizzo di memoria indicato. Viene aggiunto il valore 4 al valore presente in esp e copiato il valore 1 in eax. Poi viene fatto un jump su un indirizzo di memoria.

Quindi tutto questo blocco sarà un if che controllerà il valore di ebp+var_4 con 0 e se la condizione sarà vera farà il jump, ovvero andrà nel ramo dell'else altrimenti creerà la stringa di connessione avvenuta con successo. Verrà chiamata una funzione e verranno inizializzate due variabili, probabilmente visto il jump potrebbe essere l'inizio di un ciclo.

Davide Lecci