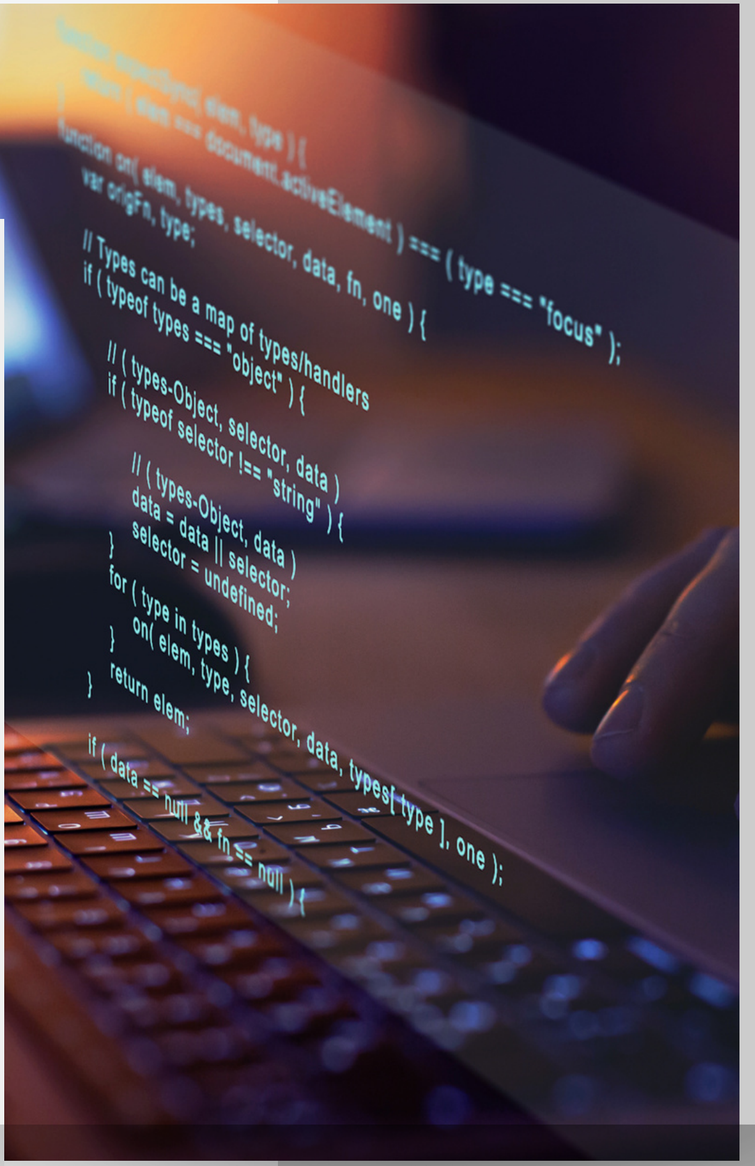
COSTRUTTI C - ASSEMBLY X86

MATTIA PASTORELLI

COMANDA

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 : 004010011                   cmp     [ebp+var_4], 0
- text : 004010015                    jz      short loc_40102B
- text : 004010017                    push    offset aSuccessInterne ; “Success:
Internet Connection\n”
- text : 00401001C                    call    sub_40105F
- text : 004010021                   add     esp, 4
- text : 004010024                    mov    eax, 1
- text : 004010029                    jmp     short loc_40103A
- text : 00401002B  ; ---------------------------------------------
-------------------------------------------------------------------
------------------
- text : 00401002B
```



CICLO IF/ELSE

In questa fase del ciclo assembly è ciò che potrebbe essere tradotto nel ciclo If/Else del linguaggio C.

Il comando **CMP** è un comando che mette a comparazione il valore di var_4 con 0
E con il comando **JZ** prende il comando precedente e valuta se il valore è uguale a zero e salterà direttamente alla porzione di codice (loc_40103B), altrimenti continuerà lungo il codice.
Comando **JMP** salta immediatamente alla porzione del codice loc_40103A

```
- text : 004010011          cmp   [ebp+var_4], 0
- text : 004010015           jz    short loc_40102B


- text : 004010029          jmp   short loc_40103A
```

FUNZIONAMENTO

Sembra che il codice sia progettato per controllare lo stato della connessione Internet utilizzando "InternetGetConnectedState" e, in caso di esito positivo, verrà stampato un messaggio di successo.

BONUS: SPIEGAZIONE CODICE

```
1.- text : 00401000                    push   ebp
2.- text : 00401001                    mov    ebp, esp
3.- text : 00401003                    push   ecx
4.- text : 00401004                    push   0          ; dwReserved
5.- text : 00401006                    push   0          ; lpdwFlags
6.- text : 00401008                    call
   ds:InternetGetConnectedState
7.- text : 0040100E                    mov    [ebp+var_4], eax
8.- text : 004010011                   cmp    [ebp+var_4], 0
9.- text : 004010015                    jz     short loc_40102B
10.- text : 004010017                   push   offset aSuccessInterne ;
   “Success: Internet Connection\n”
11.- text : 00401001C                   call   sub_40105F
12.- text : 004010021                   add    esp, 4
13.- text : 004010024                    mov   eax, 1
14.- text : 004010029                    jmp    short loc_40103A
15.- text : 00401002B  ; ---------------------------------------
   ---------------------------------------------------------
   ---------------------------------
16.- text : 00401002B
```

1. Pone il valore nel registro EBP nello stack
2. Copia il valore ESP in EBP
3. Mette il valore in ECX nello stack
4. Mette il valore 0 nello stack e lo passa come dwReserved per la funzione
5. Mette il valore 0 nello stack e lo passa come lpdwFlags per la funzione
6. Chiama la funzione InternetGetConnectedState per valutare se la connessione è attiva
7. Copia il risultato dato dalla funzione precedente (EAX) in EBP + VAR_4
8. Pone a confronto il valore 0 con il risultato della funzion
9. Se è uguale a 0 salta direttamente all’etichetta loc_40102B se non avviene connessione
10. Immette la stringa nello stack (Avvenuta connessione)
11. Chiama una subroutine sub_40105F per stampare il risultato di avvenuta connessione
12. Ripristina lo stack dopo la chiamata alla subroutine
13. Copia il valore 1 nel registro EAX, indicando che la connessione è avvenuta con successo
14. Salta direttamente all’etichetta loc_40103A
15. E’ un commento