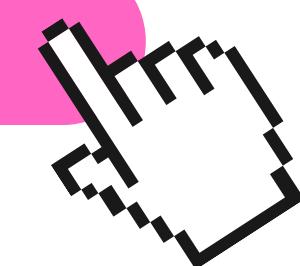


WRITTEN BY NOEMI DE MARTINO

S10/L4

COSTRUTTI C – ASSEMBLY X86



TRACCIA

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti Esercizio Linguaggio Assembly vis ti durante la lezione teorica. Provate ad ipotizzare che funzionalità è implementata nel codice assembly.

Consegna:

1. Identificare i costrutti noti (e s. while, for, if, switch, ecc.)
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
* .text:00401006          push    0
* .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 ; -----
```

1. IDENTIFICAZIONE DEI COSTRUTTI NOTI

if

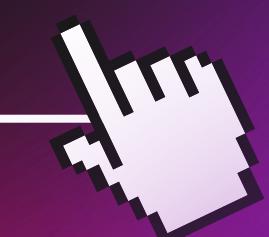
Il confronto con cmp e il salto condizionale con jz indicano una struttura di controllo tipo if.

call

Invoca una funzione.

jmp

Salta incondizionatamente a una determinata istruzione, indicando un ciclo o un salto.



2. IPOTIZZARE LA FUNZIONALITÀ

Il codice sembra verificare la presenza di una connessione a Internet utilizzando la funzione **InternetGetConnectedState**.

Se la connessione è presente, viene eseguita una specifica routine per gestire questo stato; altrimenti, il flusso del programma segue un percorso diverso.



3.BONUS: STUDIARE E SPIEGARE OGNI SINGOLA RIGA DI CODICE

push ebp: Salva il vecchio valore del registro base pointer (**EBP**).

mov ebp, esp: Imposta il registro base pointer (**EBP**) all'attuale valore dello stack pointer (**ESP**), per creare un nuovo stack frame.

push ecx: Salva il valore del registro **ECX**.

push O: Passa due parametri con valore O alla funzione InternetGetConnectedState.



3.BONUS: STUDIARE E SPIEGARE OGNI SINGOLA RIGA DI CODICE

call ds: Chiama la funzione di Windows API per verificare lo stato della connessione a Internet.

mov [ebp+var_4], eax: Salva il risultato della funzione in una variabile locale.

cmp [ebp+var_4], 0: Confronta il risultato con 0.

jz short loc_40102B: Se il risultato è zero, salta alla gestione della condizione di assenza di connessione.



3.BONUS: STUDIARE E SPIEGARE OGNI SINGOLA RIGA DI CODICE

push offset aSuccessInterne: Se la connessione è attiva, prepara il messaggio di successo.

call sub_40105F: Chiama una funzione per gestire il messaggio di successo (probabilmente lo stampa).

add esp, 4: Ripristina lo stack pointer dopo la chiamata della funzione.

mov eax, 1: Imposta il registro EAX a 1 per indicare successo.

jmp short loc_40103A: Salta alla fine del blocco di codice per terminare.

