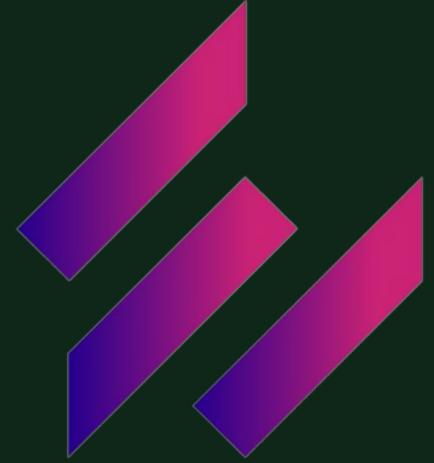


Malware analysis

S10

Team



GIORNO 4

ЛЧ

Linguaggio Assembly parte 2

Traccia giorno 4

Traccia: La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti Esercizio Linguaggio Assembly 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 ; -----
```

Identificare i costrutti

1. Identificare i costrutti noti (e s. while, for, if, switch, ecc.)

```
1.    00401000      push  ebp  
2.    00401001      mov   ebp,esp  
  
3.    00401003      push  ecx  
4.    00401004      push  0 ; dwReserved  
5.    00401006      push  0 ; lpdwFlags  
6.    00401008      call   ds:InternetGetConnectedState  
  
7.    0040100E      mov   [ebp+var_4], eax  
  
8.    00401011      cmp   [ebp+var_4],0  
9.    00401015      jz    short loc_40102B  
10.   00401017      push  offset aSuccessInterne ; "Succ....\n"  
11.   0040101C      call   sub_40105F  
12.   00401021      add   esp,4  
13.   00401024      mov   eax,1  
  
14.   00401029      jmp   short loc_40103A  
15.   0040102B  
16.   0040102B
```

Costrutto if



Ipotizzare la funzionalità

2. Ipotizzare la funzionalità – esecuzione ad alto livello

Questa porzione di codice assembly è progettata per verificare lo stato della connessione a Internet su un sistema Windows. Utilizza la funzione InternetGetConnectedState della libreria WinINet per determinare se il sistema è attualmente connesso a Internet e agisce di conseguenza.

Il malware chiama la funzione internetgetconnectedstate e ne controlla con un «if» il valore di ritorno. Se il valore di ritorno (return) della funzione è diverso da 0, allora vuol dire che c'è una connessione attiva.

Pseudocodice C:

```
state = internetgetconnectedstate (par1,0,0);
If (state !=0) printf ("Active connection");
Else return 0;
```



Bonus

3. BONUS: studiare e spiegare ogni singola riga di codice

01

Impostazione del Frame dello Stack

push ebp

mov ebp, esp

- Salva il valore corrente del puntatore di base (ebp) sullo stack.
- Imposta il puntatore di base (ebp) all'attuale puntatore dello stack (esp), creando un nuovo frame dello stack.

02

Salvataggio del Registro ecx

push ecx

- Salva il valore del registro ecx sullo stack per preservarlo, poiché sarà utilizzato nel corso della funzione.

03

Preparazione dei Parametri per InternetGetConnectedState

push 0 ; dwReserved

push 0 ; lpdwFlags

Imposta i parametri richiesti dalla funzione InternetGetConnectedState:

- lpdwFlags è un puntatore a una variabile che riceve la descrizione della connessione, ma qui non viene utilizzato (impostato a 0).
- dwReserved è riservato e deve essere 0.



Bonus

3. BONUS: studiare e spiegare ogni singola riga di codice

04

La Chiamata alla Funzione InternetGetConnectedState

```
call ds:InternetGetConnectedState mov [ebp+var_4],
```

eax Chiama la funzione InternetGetConnectedState e memorizza il valore di ritorno nel registro eax.

Questo valore indica se il sistema ha una connessione a Internet attiva. Memorizza il risultato in una variabile locale (var_4) nello stack.

05

Verifica dello Stato della Connessione Internet

```
cmp [ebp+var_4], 0
```

```
jz short loc_40102B
```

- Confronta il valore memorizzato in var_4 con 0.
- Se var_4 è 0 (nessuna connessione a Internet), salta all'etichetta loc_40102B.

06

Stampa del Messaggio di Successo

```
push offset aSuccessInterne ; "Success\n"
```

```
call sub_4010fF
```

```
add esp, 4
```

- Se viene rilevata una connessione a Internet, impila l'indirizzo della stringa "Success\n" e chiama la funzione sub_40105F (presumibilmente una funzione che stampa o gestisce la stringa).
- Dopo la chiamata, regola il puntatore dello stack (esp).



Bonus

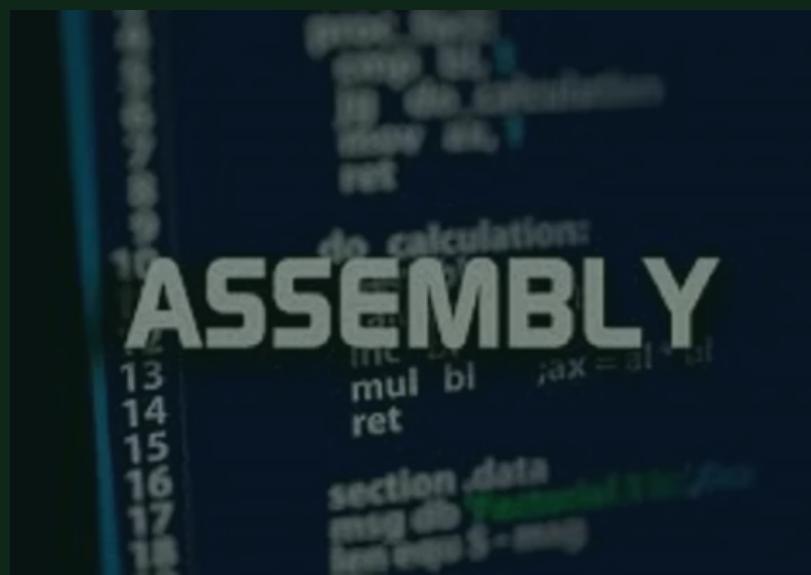
3. BONUS: studiare e spiegare ogni singola riga di codice

07

Impostazione del Valore di Ritorno e Uscita

```
mov eax, 1  
jmp short loc_40103A
```

- Imposta il valore di ritorno in eax a 1 (indicando successo) e salta all'etichetta loc_40103A per uscire dalla funzione.





TEAM ALBA



Zhongshi Liu



Mara Dello Russo



Mario Marsicano



Luca Lenzi



Giovanni Sannino



Andre Vinicius

THANK YOU
