Alaimo Alessandro
12/01/2023

Report Costrutti Assembly x86

Avendo il seguente codice in Assembly, le operazioni da fare sono quelle di individuare i costrutti noti, ipotizzare la funzionalità ad alto livello.

```
push   ebp
mov    ebp, esp
push   ecx
push   0                    ; dwReserved
push   0                    ;lpdwFlags
call   ds:InternetGetConnectedState
mov    [ebp+var_4], eax
cmp    [ebp+var_4], 0
jz     short loc_401102B
push   offeset aSeccessInterne ;"Success: Internet Connection\n"
call   sub_40105F
add    esp,    4
mov    eax, 1
jmp    short loc_40103A
```

Possiamo ipotizzare ciò che fa il frammento di codice. Difatti crea un nuovo stack ed inserisce 3 parametri per poi chiamare la funzione "ds:InternetGetConnectedState" per controllare se il dispositivo è connesso ad internet. Tramite un IF andiamo a stampare "Success: Internet Connection" nel caso in cui c'è la connessione ad Internet.

Iniziamo con il sottolineare che dal frammento di codice che abbiamo preso in analisi si possono individuare 2 ipotetici costrutti i quali sono:

1. "cmp [ebp+var_4], 0" e "jz short loc_401102B" possiamo dire che fanno parte di un IF, il quale controlla se il risultato è 0 ed in caso salta fino all'indirizzo di memoria scritto per continuare il codice.
2. "jmp short loc_40103A" non avendo il codice completo, non possiamo essere sicuri su ciò che è, quindi si può ipotizzare che sia un goto.