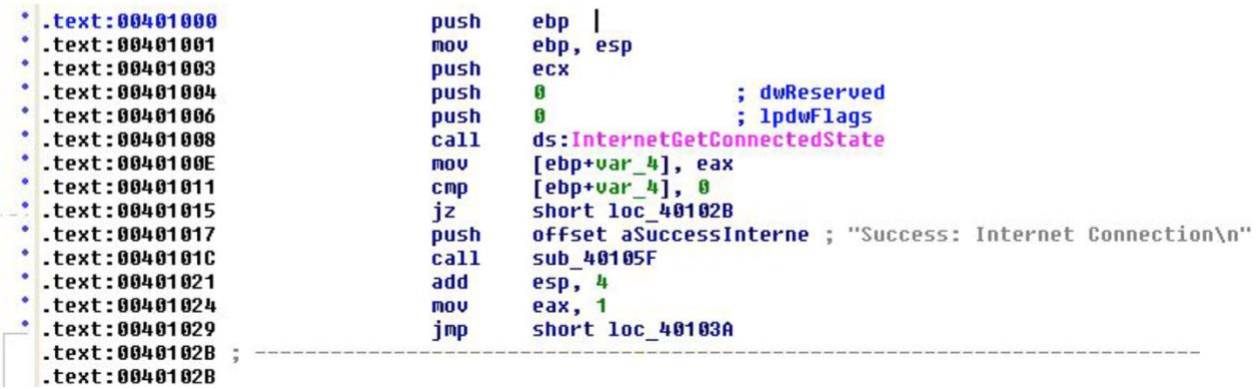
COSTRUTTI C

FRANCESCO PERSICHETTI

Traccia:

La figura seguente mostra un estratto del codice di un malware. Identificare i costrutti noti visti durante la lezione teorica.



- Identificare i costrutti noti (es. while, for, if, switch, ecc.)
- Ipotizzare la funzionalità

1)
Prendendo in considerazione il pezzo di codice sopra posso evidenziare almeno un ipotetico costruttore noto al suo interno.
“cmp [ebp+var_4], 0” e “jz short loc_40102B” posso ipotizzare sia un IF, che controlla se il risultato sia 0 in caso salta all’altro indirizzo di memoria scritto nel codice

2)
Ipotizzando la funzionalità del nostro pezzo di codice possiamo appurare che si tratti di un estratto di codice di un malware il quale partendo dall’inizio inserisce 3 nuovi parametri con l’operatore “push” per poi richiamare la funzione “ds:InternetGetConnectedState” con l’operatore “call” per controllare appunto lo stato della connessione del macchinario vittima. Una volta fatto ciò con l’IF trovato nel punto precedente, essendo la condizione esatta che il malware cercava, fa stampare “Success: Internet Connection” testimoniando così il collegamento a internet