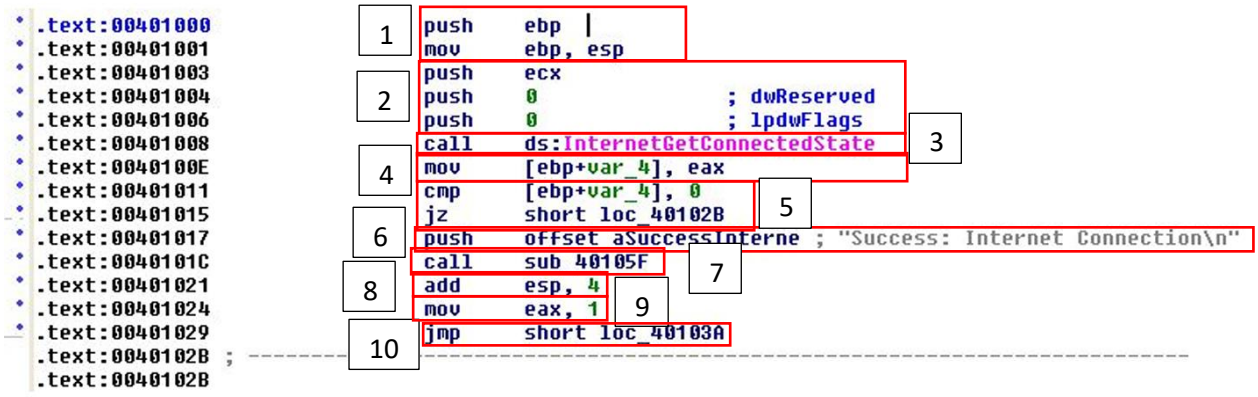
Malware analysis: Costrutti C - Assembly X86

Sommario

Traccia S10-L4

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



Analisi del codice

1. Queste istruzioni creano lo stack che verrà utilizzato dalla funzione chiamata successivamente.

-push ebp: salva il valore corrente del puntatore base dello stack

-mov ebp, esp: imposta il puntatore base dello stack per puntare alla cima dello stack

2. Queste istruzioni inseriscono dei valori nello stack da passare alla funzione:

-push ecx pusha il valore contenuto nel registro ecx nello stack

-push 0 ; dwReserved pusha il valore 0 nel valore DWORD dwReserved. Questo è un parametro riservato

-push 0 ; lpdwFlags pusha il valore 0 nel valore DWORD lpdwFlags. Questo parametro riceve informazioni aggiuntive sulla connessione internet. Se la funzione InternetGetConnectedState ritorna TRUE, allora lpdwFlags punta a un valore che specifica il tipo di connessione internet. In questo codice è 0, quindi il codice non sta cercando di ottenere queste informazioni aggiuntive.

3. Chiama la funzione **InternetGetConnectedState** che verifica se c'è una connessione internet disponibile.
4. Sposta il valore di ritorno della funzione InternetGetConnectedState (memorizzato in eax) in una variabile locale.
5. Ciclo if:

-**cmp [ebp+var_4], 0**: confronta il valore della variabile locale con zero. Se i due valori sono uguali, imposta il flag zero (ZF) a 1.

-**jz short loc_40190B**: salta a un'altra posizione nel codice (loc_40190B) se il flag zero (ZF) è impostato a 1. In pratica se non c'è connessione internet (cioè, se il valore di ritorno della funzione InternetGetConnectedState è zero), il codice salta a loc_40190B.

6. Pusha l'indirizzo di un messaggio di successo nello stack.

7. Chiama una sottoprocedura che presumibilmente stampa il messaggio di successo.

8. Pulisce lo stack aggiungendo 4 all'esp.

9. Imposta il valore del registro eax a 1.

10. Salta a un'altra posizione nel codice (loc_40103A).

Conclusioni

Il codice assembly presentato sembra essere progettato per verificare la presenza di una connessione internet sul computer in cui viene eseguito.