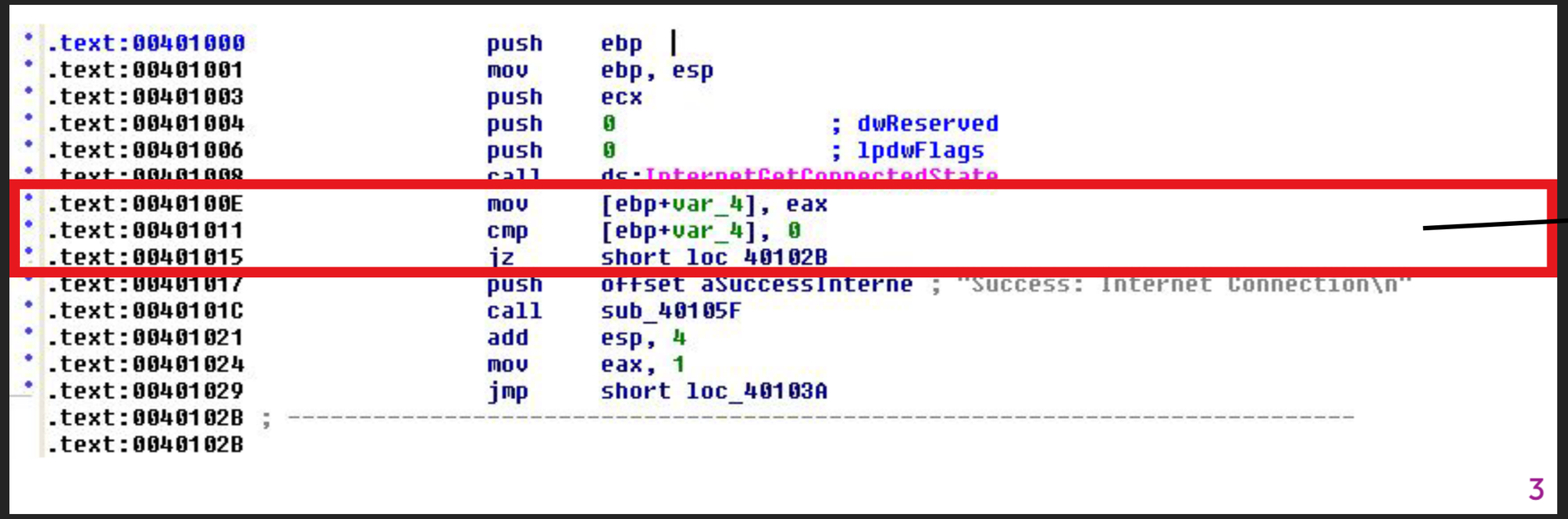
MALWARE ANALYSIS: COSTRUTTI C –ASSEMBLI 86X

Giovanni Pisapia

1. IDENTIFICARE I COSTRUTTI NOTI:

Il costrutto che ho identificato nel codice assembly è un "if" che controlla se il valore di una variabile è uguale a zero. Se la condizione è vera, deduco che la connessione sia attiva, e viene eseguito un salto all'indirizzo di memoria specificato dall'istruzione "jz short". Altrimenti, se la condizione non è verificata, l'esecuzione del codice prosegue normalmente senza effettuare il salto.



2. IPOTIZZARE FUNZIONALITA'-ESECUZIONE ALTO LIVELLO

1. Inizializzazione: Il codice inizia impostando alcune configurazioni iniziali.
2. Controllo della connessione a Internet: Viene chiamata la funzione InternetGetConnectedState per controllare lo stato della connessione a Internet. Il risultato viene salvato in una variabile.
3. Controllo dello stato: Viene controllato se lo stato della connessione è zero o diverso da zero.
4. Messaggio di successo: Se lo stato è zero (connessione attiva), viene mostrato un messaggio di successo.
5. Azioni aggiuntive: Viene chiamata una funzione (sub_40105F) per gestire il messaggio di successo e compiere ulteriori azioni.
6. Terminazione: Il programma termina.

3. SPIEGAZIONE RIGHE CODICE

1. push ebp: Salva il valore del registro ebp nello stack.
2. mov ebp, esp: Imposta il registro ebp uguale al registro esp.
3. push ecx: Salva il valore del registro ecx nello stack.
4. push 0: Mette il valore 0 nello stack.
5. push 0: Mette il valore 0 nello stack.
6. call ds: InternetGetConnectedState: Chiama la funzione InternetGetConnectedState per controllare la connessione a Internet.
7. mov [ebp+var_4], eax: Memorizza il valore di ritorno della funzione in una variabile chiamata var_4.
8. cmp [ebp+var_4], 0: Confronta il valore di var_4 con 0.
9. jz short loc_40102b: Se var_4 è uguale a 0, salta all'indirizzo loc_40102b.
10. push offset aSuccessInterne: Mette l'offset di una stringa nello stack.
11. call sub_40105F: Chiama la funzione sub_40105F.
12. add esp, 4: Ripristina lo stack rimuovendo 4 byte.
13. mov eax, 1: Assegna il valore 1 al registro eax.
14. jmp short loc_40103A: Salta incondizionatamente all'indirizzo loc_40103A.