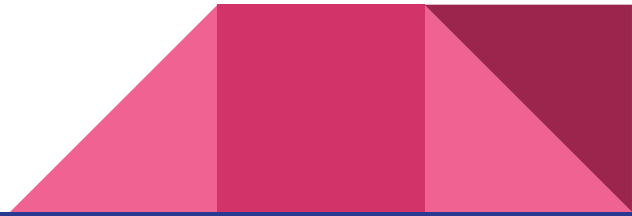
S10/L4 Epicode Cybersecurity

Costrutti C - Assembly X86

Nell’esercizio di oggi ci viene richiesto di analizzare un codice in Assembly, identificare i costrutti utilizzati ed ipotizzare quale funzionalità sia implementata.

```
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_40102B
push Offset aSuccessInterne
call sub_40105F
add esp,4
mov eax, 1
jmp short loc_40103A
```



Il codice Assembly fornitoci utilizza diversi costrutti comuni del linguaggio, quali:

- **Push e Pop**: I comandi ‘push’ e ‘pop’ vengono utilizzati per inserire e rimuovere valori dallo stack rispettivamente. In questo caso, vengono utilizzati per passare parametri alla funzione ‘InternetGetConnectedState’ e per salvare e ripristinare valori durante la gestione dello stack;
- **Mov**: L'istruzione ‘mov’ viene utilizzata per copiare dati da una posizione all'altra. In questo caso, viene utilizzata per inizializzare il registro di base ‘ebp’ e per memorizzare il risultato della funzione ‘InternetGetConnectedState’ in una variabile locale;
- **Call e Jump**: Le istruzioni ‘call’ e ‘jump’ vengono utilizzate per trasferire il controllo a un'etichetta o a una subroutine specifica. Nel codice fornito, ‘call’ viene utilizzato per chiamare la funzione ‘InternetGetConnectedState’ e per chiamare una subroutine per la stampa di un messaggio di successo. ‘jmp’ viene utilizzato per saltare a una determinata istruzione in base a una condizione (nel caso specifico, se la connessione a Internet è attiva o meno).

- **Cmp** e **Jz**: Le istruzioni ‘cmp’ e’jz’ vengono utilizzate per confrontare due valori e saltare a un'etichetta specifica se sono uguali. In questo caso, vengono utilizzati per controllare se il valore memorizzato dopo la chiamata a ‘InternetGetConnectedState’ è zero, il che potrebbe indicare che la connessione a Internet non è attiva.
- **Offset**: La parola chiave ‘Offset’ viene utilizzata per ottenere l'offset di una variabile o di un'etichetta all'interno del programma. In questo caso, viene utilizzata per ottenere l'offset di una stringa da passare come parametro alla subroutine per la stampa di un messaggio di successo.

A giudicare dal codice di cui abbiamo visione e consapevoli che esso sia parte di un malware, possiamo ipotizzare che esso possa implementare una funzionalità di avvio processi in background o accesso ad un server remoto per il download o la raccolta di dati o potrebbe trattarsi di un monitoraggio per le attività di rete.