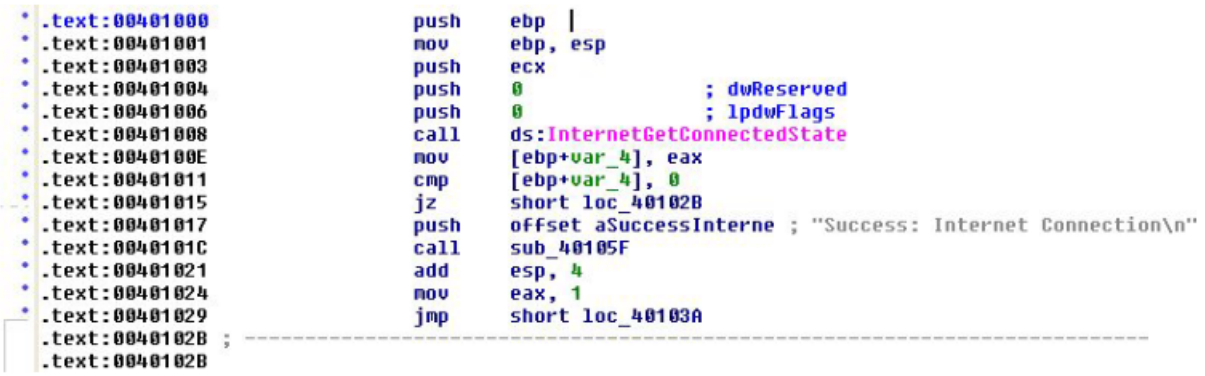
Report costrutti noti \ Assembly x86

Qui di seguito riportato un estratto di codice malware



Identifichiamone i costrutti noti, ipotizzandone funzionalità.

- text: 00401000 push ebp |
- text : 00401001 mov ebp, esp
  Si traducono nella creazione stack

- text: 00401003 push ecx
- text:00401004 push 0 ; dwReserved
- text:00401006 push 0; lpdFlags
  Si traducono nel push dei valori all'interno della funzione dello stack

- text:00401008 call ds: InternetGetconnectedState
  Call di funzione

- text:0040100E mov [ebp+var_4], eax
- text:00401011 cmp [ebp+var_4], 0
- text: 00401015 jz short loc_40102B
- text:00401017 push offset aSuccessInterne ; "Success: Internet Connection\n"
  Si traducono in comparazione, eventuale salto, printf

- text:0040101C call sub_40105F connessione avvenuta
- text:00401029 jmp short loc_40103A ritorno di processo

Viene creato lo stack della funzione, alla quale viene aggiunto a EBP iniziale, uno stack ESP, alla quale viene inserito in seguito un elemento dello stac ECX allo stack EBP.

Dopodichè vengono pushati gli elementi con valore 0.

Ipotizziamo quindi che la variabile ipdwFlags corrisponda a "connessione non avvenuta" nel caso di condizione con esito positivo e che dwREserved corrisponda

all’effettiva connessione purchè la condizione si avveri. Quindi rispettivamente ipdwFlags = 0 dwReserved=1

Valori in push pari a 0.

A questo punto abbiamo la call di verifica connessione . Venendo aggiunto a stack EBP con variabile (Var_4=0)

E comparazione tra valore sorgente 0 e la seconda variabile, sempre pari a zero.

Quindi lo ZeroFlag è 1 e il CarryFlag 0 poiché sorgente e destinazione sono uguali.

Infine si jumpa a locazione 40102B