EPICODE

Progetto Alessandro Moscetti 30/11

Codice

```
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
.text:00401003                push    ecx
.text:00401004                push    0               ; dwReserved
.text:00401006                push    0               ; lpdwFlags
.text:00401008                call    ds:InternetGetConnectedState
.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"
.text:0040101C                call    sub_40105F
.text:00401021                add     esp, 4
.text:00401024                mov     eax, 1
.text:00401029                jmp     short loc_40103A
.text:0040102B ; ---------------------------------------------------------------------------
.text:0040102B
```

```
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 ; "Success: Internet Connection\n"
call    sub_40105F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

Notiamo nel codice a partire dalla riga 7 un ciclo **for** dove alla variabile [ebp+var_4] viene assegnato il valore del registro eax e poi viene confrontata nella riga successiva al valore 0.
Con l'istruzione jz (rig. 9) saltiamo alla locazione loc_40102B se il Zero Flag sia 1, praticamente, se la comparazione precedente è uguale ([ebp+var_4]=0); altrimenti continuerà l'esecuzione del programma senza saltare.

Considerazione funzionalità codice

Guardando il codice ipotizzo che la sua funzionalità sia quella di verificare se ci sia una connessione internet attiva sul dispositivo, potrebbe essere una parte di un malware di tipo downloader.
La mia ipotesi si basa sulla funzione richiamata ‘InternetGetConnectedState’ e con il ciclo for presente che al raggiungimento della condizione ZF=0 chiama l’istruzione ‘push offset aSuccessInterne ; “Success: Internet Connection\n”’ abbastanza intuitiva.

Grazie per l’attenzione.