ES Lezione 4 Settimana 10

Traccia:

La figura seguente mostra un estratto del codice di un malware.

Identificare i costrutti noti visti durante la lezione teorica.

```
.text:00401000
                                push
                                        ebp
.text:00401001
                                        ebp, esp
                                mov
.text:00401003
                               push
                                        ecx
.text:00401004
                                                         : dwReserved
                               push
.text:00401006
                                                         ; lpdwFlags
                               push
                                        ds:InternetGetConnectedState
.text:00401008
                               call
.text:0040100E
                                        [ebp+var 4], eax
                                MOV
.text:00401011
                                        [ebp+var 4], 0
                                CMD
.text:00401015
                                jz
                                        short loc 40102B
                                        offset aSuccessInterne ; "Success: Internet Connection\n"
.text:00401017
                               push
.text:0040101C
                               call
                                        sub 40105F
.text:00401021
                                        esp, 4
                                add
.text:00401024
                                        eax, 1
                                mov
                                        short loc 40103A
.text:00401029
                                jmp
.text:0040102B
.text:0040102B
```

Consegna:

- 1. Identificare i costrutti noti (es. while, for, if, switch, ecc.)
- 2. Ipotizzare la funzionalità esecuzione ad alto livello
- 3. BONUS: studiare e spiegare ogni singola riga di codice

Traccia:

La figura seguente mostra un estratto del codice di un malware.

Identificare i costrutti noti visti durante la lezione teorica.

```
.text:00401000
                               push
                                        ebp
.text:00401001
                                        ebp, esp
.text:00401003
                               push
                                        ecx
.text:00401004
                    Chiamata di Push
                                                        ; dwReserved
                     funzione
.text:00401006
                               push
                                                        ; lpdwFlags
.text:00401008
                               call
                                       ds:InternetGetConnectedState
.text:0040100E
                                        [ebp+var 4], eax
                      Ciclo IF MOV
                                       [ebp+var 4], 0
.text:00401011
                               CMP
                               jz
.text:00401015
                                        short loc_40102B
.text:00401017
                               push
                                       offset aSuccessInterne; "Success: Internet Connection\n"
                               call
                                       sub_40105F
.text:0040101C
.text:00401021
                               add
                                       esp, 4
.text:00401024
                               mov
                                        eax, 1
                              jmp
.text:00401029
                                       short loc 40103A
.text:0040102B
.text:0040102B
```

Ho ipotizzato che si tratti di un malware che tramite questo script prova a collegarsi ad internet