# Intro e concetti di Windows avanzati

#### Traccia:

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- Identificare il client software utilizzato dal malware per la connessione ad Internet
- Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL
- BONUS: qual è il significato e il funzionamento del comando assembly "lea"

#### Traccia:

```
; samDesired
0040286F
          push
                  2
                                   ; ulOptions
00402871
          push
                  eax
00402872
                  offset SubKey
                                      "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
          push
                  HKEY LOCAL MACHINE; hKey
00402877
          push
0040287C
          call
                  esi ; RegOpenKeyExW
0040287E
          test
                  eax, eax
                  short loc_4028C5
00402880
          jnz
00402882
00402882 loc_402882:
00402882
                  ecx, [esp+424h+Data]
00402886
          push
                  ecx
bl, 1
                                  ; lpString
00402887
          mov
          call
00402889
                  ds:lstrlenW
0040288F
          lea
                  edx, [eax+eax+2]
00402893
                                   ; cbData
          push
00402894
                  edx, [esp+428h+hKey]
00402898
          lea
                  eax, [esp+428h+Data]
                                   ; lpData
0040289C
          push
                  eax
0040289D
          push
                                   ; dwType
0040289F
          push
004028A1
                  ecx, [esp+434h+ValueName]
                                   ; lpValueName
004028A8
          push
                  ecx
                                     hKey
004028A9
          push
                   edx
                  ds:RegSetValueExW
004028AA
          call
```

### Traccia:

```
.text:00401150
.text:00401150
                       _stdcall StartAddress(LPV0ID)
.text:00401150
              ; DWORD
.text:00401150 StartAddress
                              proc near
                                                      ; DATA XREF: sub_401040+ECTo
                                      esi
.text:00401150
                              push
.text:00401151
                              push
                                      edi
.text:00401152
                                                      ; dwFlags
                              push
                                      0
.text:00401154
                                      0
                                                       1pszProxyBypass
                              push
.text:00401156
                              push
                                                       1pszProxy
                                                       dwAccessType
.text:00401158
                              push
.text:0040115A
                              push
                                      offset szAgent
                                                       "Internet Explorer 8.0"
.text:0040115F
                              call
                                      ds:InternetOpenA
                                      edi, ds:InternetOpenUrlA
.text:00401165
.text:0040116B
                              mov
                              mov
                                      esi, eax
.text:0040116D
.text:0040116D loc_40116D:
                                                      ; CODE XREF: StartAddress+30jj
.text:0040116D
                              push
                                                       dwContext
                                      80000000h
.text:0040116F
                              push
                                                       dwFlags
.text:00401174
                              push
                                                       dwHeadersLength
.text:00401176
                              push
                                                       lpszHeaders
"http://www.malware12com
.text:00401178
                                      offset szUrl
                              push
.text:0040117D
                              push
                                      esi
                                                      ; hInternet
.text:0040117E
                              call
                                      edi ; InternetOpenUrlA
.text:00401180
                                      short loc_40116D
.text:00401180 StartAddress
.text:00401180
```

#### 

L'istruzione <u>call</u> viene utilizzata per chiamare una funzione o un'etichetta specificata.

L'istruzione <u>lea</u> viene utilizzata per calcolare l'indirizzo effettivo di un'operando e memorizzarlo nella destinazione specificata.

L'istruzione <u>push</u> viene utilizzata per mettere un valore nello stack.

L'istruzione jnz esegue un salto condizionato se il flag è 0

1) Descrivere come il malware ottiene la **persistenza**, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite

```
00402872 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877 push HKEY_LOCAL_MACHINE ; hKey
0040287C call esi ; RegOpenKeyExW

00402889 call ds:lstrlenW
```

)04028AA call ds:RegSetValueExW

La chiave del registro viene aperta con la funzione  $\underbrace{RegOpenKeyExW}$  con chiave  $\underbrace{Software \setminus Microsoft \setminus Windows \setminus Currentversion \setminus Run}_{HKEY \ LOCAL \ MACHINE}$  nell'

Fa un test per verificare l'apertura della chiave, se <u>RegOpenKeyWxW</u> è diverso da zero, l'apertura sulla chiave non è riuscita e salta a <u>loc 4028C5</u>

Se l'apertura ha successo ne imposta il valore tramite <u>RegOpenKeyExW</u>, Calcolandone l'indirizzo, la lunghezza ed i parametri necessari per la chiamata

## 

2) Identificare il client software utilizzato dal malware per la connessione ad Internet

push offset szAgent ; "Internet Explorer 8.0" ds:InternetOpenA

Il malware per la connessione ad internet, utilizza Internet Explorer 8.0

"call offset szAgent"

3) Identificare **l'URL** al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di **connettersi** ad un **URL** 

4) BONUS: qual è il significato e il funzionamento del comando assembly "lea"

Il comando assembly "lea" (Load Effective Address) viene utilizzato per calcolare l'indirizzo di memoria dei dati ottenendo puntatori e indirizzi di variabili