

WINDOWS MALWARE

- 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?

```
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:strlenW
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
```

```
.text:00401150 ; :::::::::::::: S U B R O U T I N E ::::::::::::::
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPUVOID)
.text:00401150 StartAddress    proc near      ; DATA XREF: sub_401040+ECTo
.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:0040116B             mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:           ; CODE XREF: StartAddress+304j
.text:0040116D             push    0          ; dwContext
.text:0040116F             push    80000000h ; dwFlags
.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
.text:00401180 .
```

Il malware cerca di ottenere persistenza tramite due funzioni presenti nella prima slide: RegOpenKeyExW e RegSetValueExW.

RegOpenKeyExW è usato per accedere alla chiave di registro che il malware andrà poi a modificare, nel nostro caso "Software\\Microsoft\\Windows\\CurrentVersion\\Run".

La funzione accetta alcuni parametri, posti sullo stack tramite il comando PUSH, viene poi chiamata tramite il comando CALL.

```
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
```

RegSetValueExW è la funzione usato per modificare la chiave di registro. Anch'essa accetta alcuni parametri introdotti dal comando PUSH sullo stack, in particolare il pointer lpValueName che va ad inserire il nuovo voluto dal malware.

```
004028A1 lea    ecx, [esp+434h+ValueName]
004028A8 push   ecx        ; lpValueName
004028A9 push   edx        ; hKey
004028AA call   ds:RegSetValueExW
```

Il malware utilizza il browser Internet Explorer 8.0 aprire una connessione ad internet, tramite la funzione InetrnetOpenA:

```
.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
```

Il malware cerca poi di connettersi all'indirizzo URL www.malware12.com tramite la funzione InetrnetOpenUrlA:

```
.text:00401160      push   0          ; dwContext
.text:0040116F      push   80000000h ; dwFlags
.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
```

Il comando LEA ha una funzione simile a quella di MOV, ma invece di copiare i dati, permette di caricare indirizzi di memoria in un registro.