

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

1. DESCRIVERE COME IL MALWARE OTTIENE LA PERSISTENZA, EVIDENZIANDO IL CODICE ASSEMBLY DOVE LE RELATIVE ISTRUZIONI E CHIAMATE DI FUNZIONI VENGONO ESEGUITE
2. IDENTIFICARE IL CLIENT SOFTWARE UTILIZZATO DAL MALWARE PER LA CONNESSIONE AD INTERNET
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

```
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(LPVOID)
.text:00401150 StartAddress      proc near          ; DATA XREF: sub_401040+ECFo
.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:                ; 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.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) Il malware** ottiene la persistenza attraverso l'aggiunta di una voce di registro al percorso "Software\Microsoft\Windows\CurrentVersion\Run". Questo viene fatto utilizzando la funzione RegSetValueExW, evidenziata nel codice assembly, che scrive il percorso del malware come valore nella chiave di registro specificata.

- ▶ ; Aggiunta della voce di registro per ottenere la persistenza
- ▶ push offset SubKey ; "Software\Microsoft\Windows\CurrentVersion\Run"
- ▶ push HKEY\_LOCAL\_MACHINE ;
- ▶ hKeypush 0 ;
- ▶ Reservedpush 1 ;
- ▶ uloptionslea eax, [esp+10h+Data] ;
- ▶ eax punta alla stringa del percorso del malwarepush eaxlea eax, [esp+14h+ValueName] ;
- ▶ eax punta alla stringa del nome del valore nel registropush eaxpush esi ;
- ▶ esi punta alla chiave di registro (HKEY\_LOCAL\_MACHINE)call RegSetValueExW ;
- ▶ chiamata alla funzione per scrivere nel registro; Connessione a Internet utilizzando Internet Explorer 8.0 come client softwarepush offset szAgent ;
- ▶ "Internet Explorer 8.0"push 0 ;
- ▶ duHeadersLengthpush 80000000h ;
- ▶ dwFlagspush offset szUrl ;
- ▶ "http://www.malware12.com"push edi ;
- ▶ InternetOpenAcall InternetOpenUrlA ;
- ▶ chiamata alla funzione per aprire un URL utilizzando Internet Explorer



- 
- ▶ 2) Il client software utilizzato dal malware per la connessione a Internet è Internet Explorer 8.0, come indicato nel codice assembly attraverso la chiamata alla funzione InternetOpenA.
  - ▶ 3) L'URL al quale il malware tenta di connettersi è "http://www.malware12.com/", come indicato nel codice assembly attraverso la chiamata alla funzione InternetOpenUrlA, che passa questo URL come parametro per la connessione.