Traccia:

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, 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.

1. ----------

Il malware ottiene la **persistenza** (capacità di un programma dannoso di rimanere attivo e operativo nel sistema bersaglio anche dopo che è stato eseguito o dopo un riavvio del sistema) nel sistema attraverso la *modifica del Registro di sistema di Windows*.

Utilizza la funzione **RegOpenKeyExW** per aprire la chiave di registro corrispondente alla posizione *"Software\Microsoft\Windows\CurrentVersion\Run"*, i parametri sono passati sullo stack tramite le istruzioni «push» che precedono la chiamata di funzione; e quindi imposta un valore per questa chiave usando **RegSetValueExW**. Questo valore viene utilizzato per far sì che il malware venga eseguito all'avvio del sistema:

```
push    2               ; samDesired
push    eax             ; ulOptions
push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey
call    esi ; RegOpenKeyExW
test    eax, eax
jnz     short loc_4028C5
```

```
loc_402882:
  lea     ecx, [esp+424h+Data]
  push    ecx             ; lpString
  mov     bl, 1
  call    ds:lstrlenW
  lea     edx, [eax+eax+2]
  push    edx             ; cbData
  mov     edx, [esp+428h+hKey]
  lea     eax, [esp+428h+Data]
  push    eax             ; lpData
  push    1               ; dwType
  push    0               ; Reserved
  lea     ecx, [esp+434h+ValueName]
  push    ecx             ; lpValueName
  push    edx             ; hKey
  call    ds:RegSetValueExW
```

2. ----------

Il malware utilizza **Internet Explorer 8.0** per la connessione a Internet.

Questo è evidenziato dalla stringa *"Internet Explorer 8.0"* passata come parametro alla funzione **InternetOpenA**:

```
push    0               ; lpszProxyBypass
push    0               ; lpszProxy
push    1               ; dwAccessType
push    offset szAgent  ; "Internet Explorer 8.0"
call    ds:InternetOpenA
mov     edi, ds:InternetOpenUrlA
mov     esi, eax
```

3. ----------

L'URL al quale il malware tenta di connettersi è **"http://www.malware12.COM"**.

Questo è evidenziato dalla stringa *"http://www.malware12.COM"* passata come parametro alla funzione **InternetOpenUrlA**. L'URL è passato come parametro di questa funzione sullo stack, tramite l'istruzione push: