Pratica S11/L1

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
4. BONUS: qual è il significato e il funzionamento del comando assembly "lea"

1.Persistanza del Malware

```
00402867   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
```

Per la persistenza, il Malware aggiunge un valore all'interno della chiave di registro «**HKEY_LOCAL_MACHINE**», che contiene i record e le configurazioni della macchina, sul Path «**Software\Microsoft\Windows\CurrentVersion\Run**», ovvero il percorso delle applicazioni che vengono caricate all'avvio del sistema.
Le funzioni che il Malware utilizza sono:

- **RegOpenKeyEx:** permette di aprire una chiave di registro al fine di modificarla;
  RegSetValueEx: permette di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati.

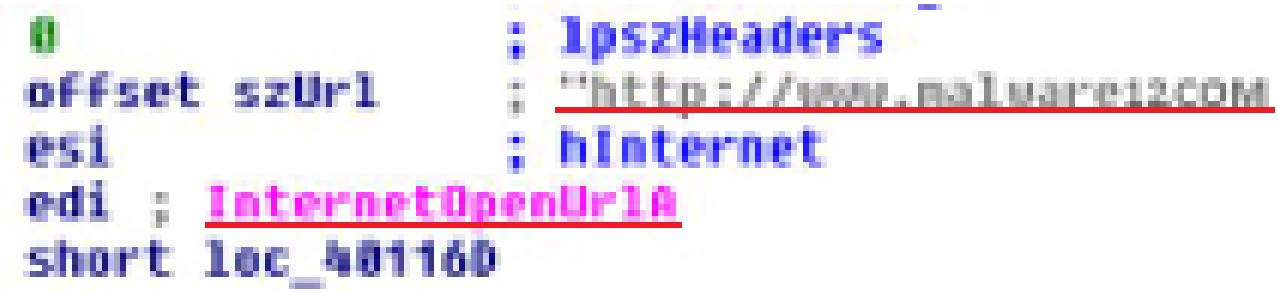
2.Client Software per connessione Internet

Il client Software utilizzato per la connessione ad Internet è «**Internet Explorer 8.0**»

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

3.Url e funzione di chiamata

L'URL a cui il malware tenta di collegarsi è «**www.malware12.com**» utilizzando la funzione «**InternetOpenUrl**», che permette di stabilire una connessione al server e poter scaricare i dati identificati dall'URL.



4.Significato e Funzionamento del comando assembly "lea"

Nel linguaggio Assembly, il comando «**lea**» è un'istruzione utilizzata per caricare l'indirizzo effettivo di una posizione di memoria in un registro, anziché caricare il valore effettivo memorizzato in quell'indirizzo di memoria.
È utile per eseguire calcoli o accedere a strutture dati in memoria.
Svolge lo stesso compito del comando «**mov**», ma oltre ad essere più compatta nella forma è anche migliore.