Windows Malware

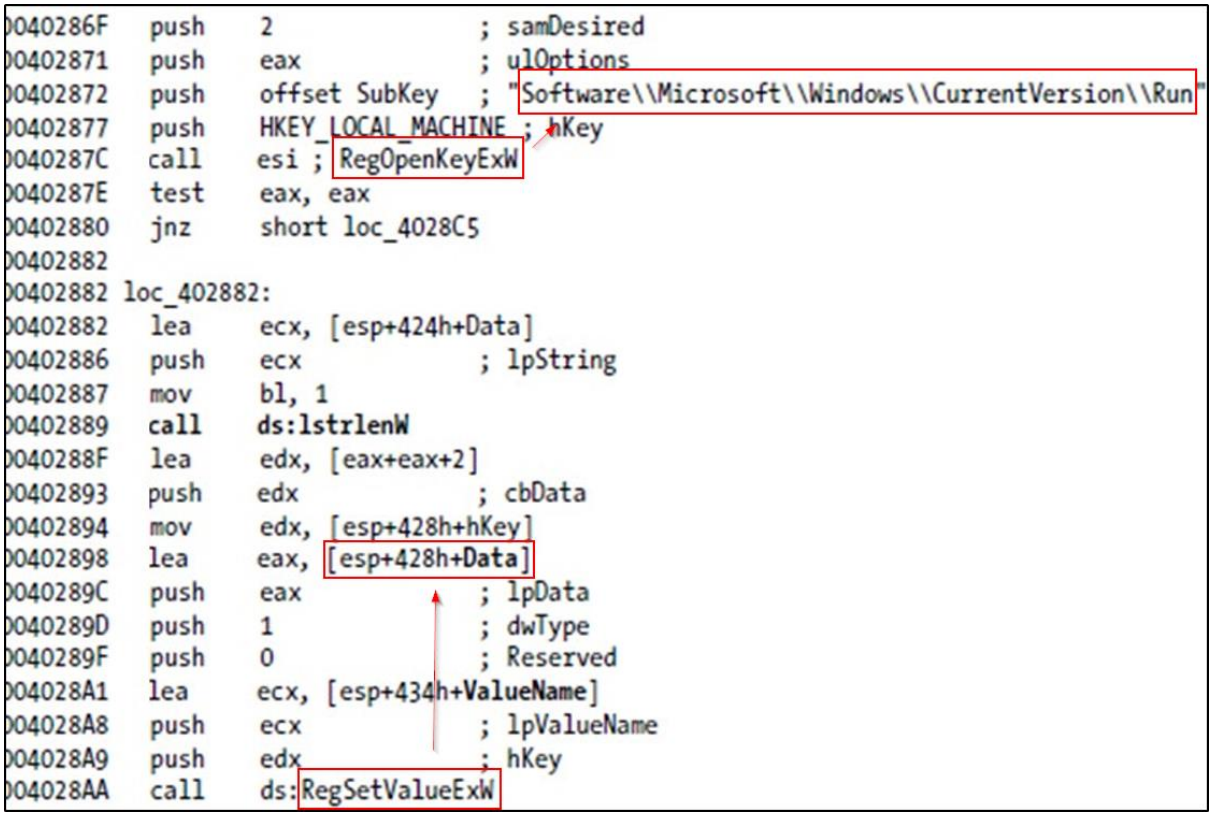
Traccia

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"

Traccia 1

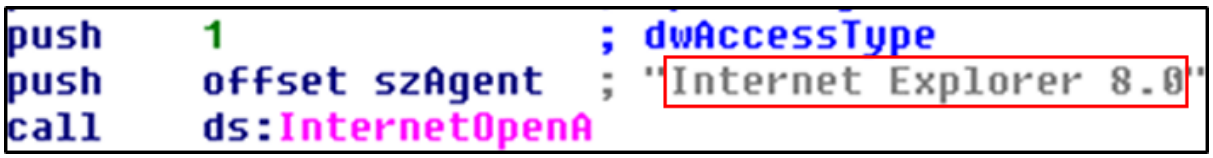
Il malware ottiene la persistenza tramite le funzioni RegOpenKey e RegSetValueEx, dove la prima apre la chiave selezionata (Software\\Microsoft\\Windows\\CurrentVersion\\Run) e la seconda setta il parametro desiderato (valore di [esp+428h+Data]).



```
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: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
```

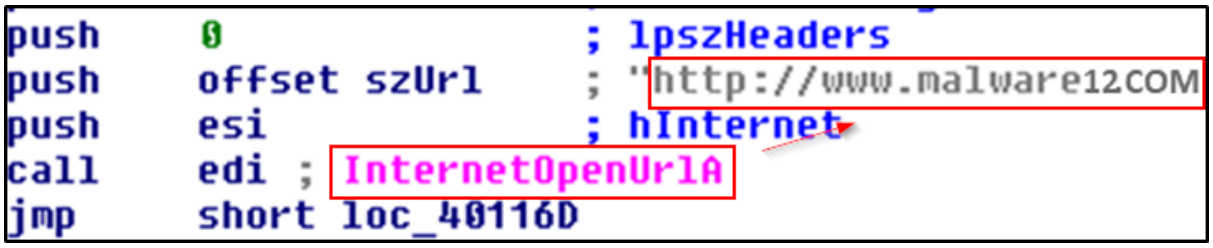
Traccia 2

Il client utilizzato dal malware per connettersi a internet è Internet Explorer 8.0.



Traccia 3

L'URL al quale il malware cerca di connettersi è http://malware12.com che viene passato come parametro alla chiamata di funzione InternetOpenUrlA.



Traccia 4

In Assembly l'istruzione lea (Load Effective Address) viene utilizzata per calcolare l'indirizzo effettivo di un operando e caricare questo indirizzo in un registro, senza accedere effettivamente alla memoria. È spesso impiegata per eseguire operazioni di indirizzamento complesse in modo efficiente senza dover manipolare direttamente i dati memorizzati in memoria.