Windows Malware

Richiesta: Con riferimento agli estratti di un malware reale, rispondere alle seguenti domande:

• Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite.
• Identificare il client software utilizzato dal malware per la connessione ad Internet.
• 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.
• BONUS: qual è il significato e il funzionamento del comando assembly"lea".

Estratti malware:

```
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
```

```
; ||||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||

; DWORD __stdcall StartAddress(LPVOID)
StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
                push    esi
                push    edi
                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
                mov     esi, eax

loc_40116D:                             ; CODE XREF: StartAddress+30↓j
                push    0               ; dwContext
                push    80000000h       ; dwFlags
                push    0               ; dwHeadersLength
                push    0               ; lpszHeaders
                push    offset szUrl    ; "http://www.malware12COM
                push    esi             ; hInternet
                call    edi ; InternetOpenUrlA
                jmp     short loc_40116D
StartAddress    endp
```

Persistenza
Il malware riesce ad ottenere la persistenza all'interno del sistema grazie alla modifica della chiave di registro windows, aggiugendo un nuovo valore. La chiave in questione è
"Software\\Microsoft\\Windows\\CurrentVersionRun\\Run", riguarda tutti i programmi che sono eseguiti all'avvio del sistema operativo.

Le funzioni utilizzate:
RegOpenKey: Questa funzione permette di aprire la chiave desiderata, il processo avviene tramite i parametri che sono passati sullo stack tramite istruzioni push, funzioni utilizzate prima della chiamate di una funzione.

RegSetValueEx: Questa funzione permette di modificare la chiave di registro inserendo un nuovo valore, in questo caso per ottenere la persistenza.

Client Software Malware

Il client che il malware utilizza per riuscire ad effettuare una connessione ad internet è semplicemente Internet Explorer 8.0.

Parte di codice interessata:

```
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
mov     esi, eax
```

URL di destinazione

Analizzando il codice, si nota che il malware tenta di connettersi all'URL "www.malware12.com".
Per avviare la connessione con l'URL in questione, viene chiamata la funzione "InternetOpenURL". L'URL viene chiamato come parametro di questa funzione sullo stack tramite l'istruzione push.

Parte di codice interessata:

```
                push    0                   ; dwContext
                push    80000000h           ; dwFlags
                push    0                   ; dwHeadersLength
                push    0                   ; lpszHeaders
                push    offset szUrl        ; "http://www.malware12COM
                push    esi                 ; hInternet
                call    edi ; InternetOpenUrlA
                jmp     short loc_40116D
StartAddress    endp
```

Bonus comando LEA

Il comando "LEA" in Assembly sta per "Load Effective Address". Viene utilizzato per caricare l'indirizzo di una variabile, piuttosto che il suo valore, in un registro.