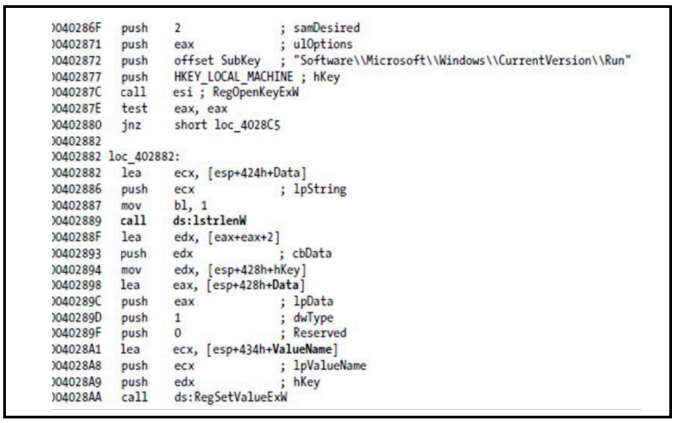
# 1. Intro e concetti di Windows avanzati

Con riferimento agli estratti di un malware, rispondere alle domande.



```
)040286F   push    2               ; samDesired
)0402871   push    eax             ; ulOptions
)0402872   push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
)040287E   test    eax, eax
)0402880   jnz     short loc_4028C5
)0402882
)0402882 loc_402882:
)0402882   lea     ecx, [esp+424h+Data]
)0402886   push    ecx             ; lpString
)0402887   mov     bl, 1
)0402889   call    ds:lstrlenW
)040288F   lea     edx, [eax+eax+2]
)0402893   push    edx             ; cbData
)0402894   mov     edx, [esp+428h+hKey]
)0402898   lea     eax, [esp+428h+Data]
)040289C   push    eax             ; lpData
)040289D   push    1               ; dwType
)040289F   push    0               ; Reserved
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

```
.text:00401150 ; ╔══════════════ S U B R O U T I N E ═══════════════════════════════════════
.text:00401150
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
.text:00401150                 push    esi
.text:00401151                 push    edi
.text:00401152                 push    0               ; dwFlags
.text:00401154                 push    0               ; lpszProxyBypass
.text:00401156                 push    0               ; lpszProxy
.text:00401158                 push    1               ; dwAccessType
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
.text:00401165                 mov     edi, ds:InternetOpenUrlA
.text:0040116B                 mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:                             ; CODE XREF: StartAddress+30↓j
.text:0040116D                 push    0               ; dwContext
.text:0040116F                 push    80000000h       ; dwFlags
.text:00401174                 push    0               ; dwHeadersLength
.text:00401176                 push    0               ; lpszHeaders
.text:00401178                 push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                 push    esi             ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
.text:00401180                 jmp     short loc_40116D
.text:00401180 StartAddress    endp
.text:00401180
```

- **Descrizione di come il malware ottiene persistenza.**

Il Malware inserisce un nuovo valore all'interno della chiave di registro **Software\\Microsoft\\Windows\\CurrentVersion\\Run** che corrisponde a tutti i programmi avviati all'accensione della macchina e del sistema operativo.

Per ottenere la persistenza utilizza due funzioni, cioè:

**RegOpenKeyEx** - Attraverso il push, i parametri sono passati allo stack per poi arrivare alla chiamata della funzione, che ci permette di aprire la chiave selezionata.

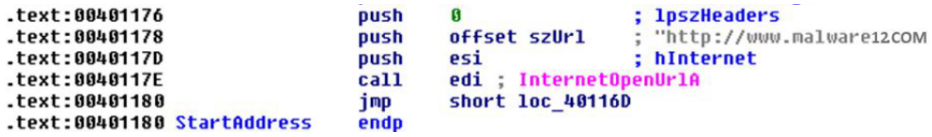
**RegSetValueEx** - Questa funzione ci permette invece di andare ad inserire un nuovo valore all'interno della chiave di registro creata.

- **Indicare client software utilizzato dal malware per connessione internet.**

```
.text:00401156                 push    0               ; lpszProxy
.text:00401158                 push    1               ; dwAccessType
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
.text:00401165                 mov     edi, ds:InternetOpenUrlA
```

Il client utilizzato per la connessione ad internet è **Internet Explorer 8.0**, come vediamo in figura.

- **Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi all'URL.**




Il malware tenta di connettersi a "**www.malware12.com**".
Possiamo inoltre notare la chiamata di funzione che permette al malware di connettersi è InternetOpenUrlA.

- **Significato e funzionamento del comando "lea".**

(Load Effective Address)
Il comando lea è un'istruzione assembly che carica l'indirizzo effettivo di un'operando nella destinazione specificata.
Il comando lea viene utilizzato nell'esempio di codice fornito per caricare l'indirizzo di una variabile in un registro.
Questo indirizzo viene poi utilizzato per specificare la posizione in cui i dati da scrivere nel registro di sistema verranno memorizzati. La funzione RegSetValueEx viene poi chiamata con questo indirizzo come parametro, in modo che i dati possano essere scritti nella posizione di memoria corretta. In altre parole, lea è un comando che permette di ottenere l'indirizzo di una variabile, che può essere utilizzato per accedere ai dati in quella variabile.