Windows Malware

```
)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 ; 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
```

1. Descrivere come il malware ottiene la persistenza, evidenziando la parte del codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite.

Una delle chiavi di registro usata dai malware per ottenere persistenza in un sistema operativo è **Software\\Microsoft\\Windows\\CurrentVersion\\Run**. Ci aspettiamo di trovare questo path nelle istruzioni all'inizio del codice. Nello screen che segue è evidenziato in giallo.

Dopo la specifica della rootkey istruzioni tipo **"RegOpenKeyex, RegSetValureEx, RegSetValue".** Di seguito sono sottolineati di blu.
In celeste ho evidenziato la sottocategoria del registro che contiene configurazioni della macchina "HKEY_LOCAL_MACHINE"
La prima si occupa di aprire una chiave di registro, al fine di modificarla; la seconda aggiunge un nuovo valore nel registro; la terza restituisce la tipologia e il dato del registro.

Sappiamo inoltre che i parametri della funzione verranno passati allo stack con istruzioni di tipo PUSH, che può aiutarci a trovarli.

```
)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
```

2. **Identificare il client software utilizzato dal malware per la connessione ad Internet**
   Il malware si serve delle funzioni per l'implementazione dei protocolli di rete. Troveremo:
   "**InternetOpen**", quando il malware vorrà inizializzare una connessione verso internet;
   "**InternetOpenUrl**" per effettuare una connessione a un determinato Url

```
.text:00401150 ; ╔═══════════════ S U B R O U T I N E ═══════════════════════════════════════
.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
```

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**
   L'url al quale il malware tenta di connettersi è per l'appunto **"http://www.malware12.com"**, sottolineato sopra.
   Ho sottolineato anche **"Internet Explorer 8.0"** , su cui il malware ha inizializzato una connessione

4. **Descrivere il significato e il funzionamento del comando assembly "lea"**
   Lea è il comando "load effective address" ed è utilizzato per rendere piu semplice la gestione degli array in memoria e dei pointer. E' un'opzione che avvicina assembly ad essere un linguaggio piu complesso.

Questa istruzione **copia** l'effettivo ***valore esadecimale*** a 16 bit di una ***etichetta***, passata come operando sorgente, nel ***registro di Offset*** indicato dall'operando destinazione. Il registro coinvolto per ricevere l'offset del puntatore associato all'etichetta può essere uno qualunque dei registri a 16 bit (naturalmente esclusi quelli di segmento...).