WINDOWS MALWARE – 1

- Per garantire la sua **persistenza**, il malware si inserisce nelle voci di avvio dei programmi del PC, in modo che vengano eseguiti automaticamente e in modo permanente senza richiedere l'interazione dell'utente. Spesso i malware sfruttano le funzioni per modificare i valori delle chiavi di registro, che fanno parte delle API di Windows, al fine di ottenere la persistenza e assicurarsi che vengano avviati durante le fasi iniziali di avvio del sistema operativo. La funzione utilizzata dal malware in questo caso è **RegOpenKeyEx**, che consente di aprire una chiave di registro per effettuare modifiche. Da notare il **percorso** delle chiavi di registro che viene usata dai malware per ottenere la persistenza sul sistema operativo (può cambiare in base alla versione di Windows utilizzata).

```
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
```

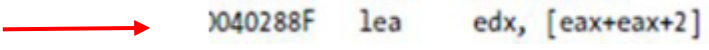
La funzione RegOpenKeyEx riceve i parametri tramite push e accede alla chiave di registro

La funzione RegOpenKeyEx riceve i parametri tramite push ecx e push edx, e modifica i valori del registro e aggiunge una nuova entry per ottenere la persistenza all'avvio

- Il malware tenta di stabilire una connessione a Internet sfruttando il software client **Internet Explorer 8.0**
- Microsoft offre una vasta gamma di API per consentire l'interazione con la rete. Oltre alle API Winsock, Microsoft fornisce anche le API WinINet per una gestione più ampia delle reti. Queste API sono incluse nella libreria Wininet.dll e offrono funzioni come HTTP e FTP. Nel nostro caso, abbiamo la funzione **InternetOpen**, utilizzata per inizializzare una connessione a Internet, e la funzione **InternetOpenUrl**, utilizzata per stabilire una connessione a un URL specificato.

```
.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
```

- Il **comando "lea" (Load Effective Address)** in assembly viene utilizzato per caricare l'indirizzo di memoria specifico in un registro. A differenza di altri comandi di caricamento non accede direttamente ai dati presenti in quella posizione di memoria, ma *calcola e carica* l'indirizzo effettivo. Questo lo rende particolarmente utile per calcolare gli indirizzi di memoria e accedervi successivamente tramite altre istruzioni.

lea destinazione, sorgente 

La "destinazione" *edx* è un registro in cui verrà memorizzato l'indirizzo effettivo calcolato, mentre la "sorgente" *[eax+eax+2]* può essere un indirizzo di memoria o una variabile.
Una volta eseguito il comando "lea", il registro di destinazione conterrà l'indirizzo di memoria calcolato, che può essere utilizzato per accedere ai dati o eseguire altre operazioni in quella specifica posizione di memoria.