

Esercitazione WEEK 23 DI

Windows malware

Ettore Farris

Descrizione sintetica

Traccia:

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..

```
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:strlenW
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
```

```

.text:00401150 ; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPUVOID)
.text:00401150 StartAddress      proc near          ; DATA XREF: sub_401040+EC70
.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:00401168                 mov     esi, eax
.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.malware12.com
.text:0040117D                 push     esi         ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
.text:00401180                 jmp     short loc_40116D
.text:00401180 StartAddress      endp
.text:00401180

```

Svolgimento

Definizione di persistenza: capacità del malware di resistere ai reboot. Se spengo il sistema e poi lo riaccendo, questo rimane infetto.

1 - Come il malware ottiene la persistenza?

1. Chiamata di funzione *RegOpenKeyEx* per accedere alla chiave di registro da modificare

Il malware effettua due operazioni che garantiscono persistenza mediante la modifica del registro di Windows. Per prima cosa accede alla chiave di registro da modificare chiamando la funzione **RegOpenKeyEx**. Prima che ciò avvenga, passa sullo stack i parametri con delle istruzioni push.

2. Chiamata di funzione *RegValueSetEx* per impostare il valore della chiave nel registro selezionato

Il malware, dopo aver aperto la chiave di registro da modificare, chiama la funzione **RegValueSetEx** dopo aver passato i parametri richiesti sullo stack mediante delle istruzioni push.

```
X040286F push 2 ; samDesired
X0402871 push eax ; ulOptions
X0402872 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
X0402877 push HKEY_LOCAL_MACHINE ; hKey
X040287C call esi ; RegOpenKeyExW
X040287E test eax, eax
X0402880 jnz short loc_4028C5
X0402882
X0402882 loc_402882:
X0402882 lea ecx, [esp+424h+Data]
X0402886 push ecx ; lpString
X0402887 mov bl, 1
X0402889 call ds:lstrlenW
X040288F lea edx, [eax+eax+2]
X0402893 push edx ; cbData
X0402894 mov edx, [esp+428h+hKey]
X0402898 lea eax, [esp+428h+Data]
X040289C push eax ; lpData
X040289D push 1 ; dwType
X040289F push 0 ; Reserved
X04028A1 lea ecx, [esp+434h+ValueName]
X04028A8 push ecx ; lpValueName
X04028A9 push edx ; hKey
X04028AA call ds:RegSetValueExW
```

2- Client software utilizzato

Il client utilizzato per la connessione ad internet è "Internet Explorer 8.0".

L'applicazione (cioè l'User-Agent) viene lanciata mediante la chiamata della funzione *InternetOpenA* appartenente alla libreria *Wininet.dll*. L'User-Agent viene passato come parametro tramite un'istruzione *push*.

```
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress proc near ; DATA XREF: sub_401040+ECF0
.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
```

La funzione *InternetOpenA* viene utilizzata per inizializzare una connessione verso Internet

3 - URL di connessione

Il malware tenta di connettersi all'indirizzo "http://www.malware12.com" che viene passato alla funzione *InternetOpenUrlA* della libreria *Wininet.dll*. L'URL viene passato nello stack tramite un'istruzione *push*.

```
----- 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.malware12.com"
.text:0040117D push esi ; hInternet
.text:0040117E call edi ; InternetOpenUrlA
.text:00401180 jmp short loc_40116D
.text:00401180 StartAddress endp
.text:00401180
.text:0040118B -----
```

La funzione *InternetOpenUrlA* viene utilizzata per la connessione ad un URL che viene passato tra i parametri dello stack. Un'altro parametro da notare è l'*handler* alla connessione avviata in precedenza tramite *InternetOpenA*.