Oggi andremo ad analizzare un estratto di un malware reale e a rispondere a determinate domande su di esso:

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

.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 ; dwContent

.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

Dato questo malware, rispondiamo quindi 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

Come prima cosa, possiamo vedere che il malware ottiene persistenza facendo questa call

0040287C call esi ; RegOpenKeyExW

Questa funzione permette al malware di accedere ad una chiave di registro e di poterla modificare.

La chiamata della funzione avviene nei passaggi precedenti alla call, in modo che il malware possa avere accesso alla key prima di modificarne il valore.

Possiamo notare anche questa chiamata

004028AA call ds:RegSetValueExW

Con questa call, il malware aggiunge una nuova entry in modo da ottenere la persistenza all’avvio del pc.

Per rispondere alla seconda domanda, torniamo ad osservare il codice e andiamo ad identificare il client utilizzato dal malware per connettersi ad internet alla seguente riga:

.text:0040115A push offset szAgent ; "Internet Explorer 8.0"

.text:0040115F call ds:InternetOpenA

Possiamo osservare come ci sia nuovamente un push per avviare internet explorer e una call per inizializzare una connessione ad internet.

Per rispondere all’ultima domanda, torneremo ad analizzare il codice e noteremo le seguenti istruzioni:

.text:00401178 push offset szUrl ; "http://www.malware12com

.text:0040117D push esi ; hInternet

.text:0040117E call edi ; InternetOpenurlA

Da qui possiamo notare che c’è un push verso un url seguito da una call per inizializzare nuovamente la connessione. Il sito a cui il malware sta cercando di connettersi non è sicuramente sicuro. L’intera chiamata di funzione sarà la seguente:

.text:0040116D loc\_40116D: ; CODE XREF: StartAddress+30↓j

.text:0040116D push 0 ; dwContent

.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