

Forum:[Hack Forums](#)

Thread: [\[vb.net\] inject .NET to non .NET Process / Updated ,, Source Code Added](#)

njq8 - February 23, 2012, 12:25 am

ok .. i will Tell you What u Need Then you Will Do it your self

what we will do is:

inject ASM to any process , And That Asm will use vbs

and vbs Code Will Load your Registered .NET

By CreateObject("Project1.Class1") ' will just invoke sub NEW

ASM code:

Code format pe gui

entry x

include 'C:\fasmw\INCLUDE\win32a.inc'

section "code import writeable readable executable

library kernel32,'kernel32',ole32,'ole32'

import

kernel32,ExitProcess,'ExitProcess',LocalAlloc,'LocalAlloc',LocalFree,'LocalFree',MultiByteToWideChar,'MultiByteToWideChar',WideCharToMultiByte,'WideCharToMultiByte'

import

ole32,CoInitialize,'CoInitialize',CoCreateInstance,'CoCreateInstance',IsEqualGUID,'IsEqualGUID'

include 'C:\fasmw\INCLUDE\vbs.inc'

x:

call @@script

vbs 'CreateObject("njin.Class1")'

invoke ExitProcess,0You Compile This Using FASM

Download IT From Here >> <http://flatassembler.net/download.php>

And you Need Download vbs.inc From Here>

<http://localhostr.com/file/YcSNsNI/VBS.INC>

put it in "C:\fasmw\INCLUDE\vbs.inc" Folder

Now Create Empty Project Name it njn

Add Class1

Code Public Class Class1

Sub New()

MsgBox(".NET!")

End Sub

End Class

Register That njn project by this command line

C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm /codebase c:\njin.exe

inject asm exe to any process And see what happen!!

[img]<http://d.localhostr.com/file/izm33r6/Untitled.png>[/img]

btw: ASM Code Not By Me

// gl ..

EDIT:

ok here is full project

i compile that asm code in resource and my program will write setting on it

you just try run it in debug and see how this program inject its self to vbc.exe

[Download](#)

no1me - February 23, 2012, 1:31 am

i didnt try it but ur threads are unique tnx

Edit - how i compile it i get error

can u make the tut more clear tnx

pr0t0typ3 - February 23, 2012, 2:59 am

Totally pointless. You did not actually inject managed code into a native process, but you injected native code which did load your managed assembly -> Nothing new at all.

njq8 - February 23, 2012, 3:19 am

(Feb 23, 2012 03:59 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Totally pointless. You did not actually inject managed code into a native process, but you injected native code which did load your managed assembly -> Nothing new at all.

every one know you cant inject managed to non managed without loader you say nothing new at all.

no1me - February 23, 2012, 3:21 am

(Feb 23, 2012 03:59 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Totally pointless. You did not actually inject managed code into a native process, but you injected native code which did load your managed assembly -> Nothing new at all.

so all is pointless even c++ inject example bcuz they load your manage ?

njq8 - February 23, 2012, 3:32 am

@no1me

Thnx For Comment ,, IF u still cant compile

make Sure your Fasm folder is here >> C:\fasmw

with 'W' at end

and download the 'vbs.inc' put it here > C:\fasmw\INCLUDE\vbs.inc

pr0t0typ3 - February 23, 2012, 3:43 am

(Feb 23, 2012 04:21 AM)no1me Wrote: [\[CITE\]](#) so all is pointless even c++ inject example bcuz they load your manage ?

Yes. In fact the only thing you could do is injecting native code which loads and invokes your managed assembly.

no1me - February 23, 2012, 4:26 am

every1 know that u cant this why we trying other ways

Edit - test the project no msgbox ? i miss something....

(i change the Framework to v2)

njq8 - February 23, 2012, 6:33 am

@no1me

yes i forget something ..

Find & Change this

p.Arguments = "/u " & Process.GetCurrentProcess.MainModule.FileName

With This

p.Arguments = "/u " & ChrW(34) & Process.GetCurrentProcess.MainModule.FileName & ChrW(34)

And Change This

p.Arguments = "/codebase " & Process.GetCurrentProcess.MainModule.FileName

With This

p.Arguments = "/codebase " & ChrW(34) & Process.GetCurrentProcess.MainModule.FileName & ChrW(34)

no1me - February 23, 2012, 6:37 am

tnx work i knew its the line but didnt know what the problem