

Forum:[Hack Forums](#)

Thread: [\[Source\]\[Help\]My Injection wont work fully in .net 2 but works fully in .net 4, Ideas](#)

C Plus C Sharp C - November 15, 2017, 5:37 am

I am having a problem injecting into different .net exe versions of the following files

- itself
- regasm.exe
- csc.exe
- cvtres.exe
- vbc.exe
- applaunch.exe

when injecting into the .net 4 versions of these files i can inject into all of them, but when using the .net 2 exe versions i can only inject into the first 2.

I was hoping someone could shed some light why this is an issue for me?

EDIT: the following is my source code: (i am not allowed to post links, so just append github url to the front of the below

/C-Plus-C-Sharp-C/Pen-Crypter-Example

gigajew - November 15, 2017, 6:15 am

Not sure because we can't see what you're trying to inject, or what you're using to inject it to begin with. Anyway you should try to avoid using .NET 2.0 because it's incompatible with a lot of system

C Plus C Sharp C - November 15, 2017, 6:45 am

my bad the injection code i am testing with is "CMemoryExecute.cs", easy to find with google.

And i am injecting a compiled "32bit .net 2" exe, into the .net 2 version of the target exe and then

And i am injecting a compiled "32bit .net 4" exe, into the .net 4 version of the target exe

Just testing to see if it works. All work in .net 4 versions but only 2 with .net 2 versions.

cocaine_monkey - November 15, 2017, 3:00 pm

(Nov 15, 2017 07:15 AM)gigajew Wrote: [\[CITE\]](#) Not sure because we can't see what you're trying to inject, or what you're using to inject it to begin with. Anyway you should try to avoid using .NET 2.0 because it's incompatible with a lot of system
isnt 2.0 default in all windowses? or other version?

Ninja - November 15, 2017, 3:04 pm

(Nov 15, 2017 04:00 PM)cocaine_monkey Wrote: [\[CITE\]](#) isnt 2.0 default in all windowses? or other version?

<https://blogs.msdn.microsoft.com/astebner/2007/03/14/mailbag-what-version-of-the-net-framework-is-included-in-what-version-of-the-os/>

0xDEAD10CC - November 15, 2017, 4:58 pm

Have you bothered verifying the difference in .NET Runtimes of those binaries? csc.exe is also not a

managed .NET assembly for instance. Without seeing what exactly you're trying to do this can't be answered. Injection can mean many things here, and we don't even know what you're trying to inject...

gigajew - November 15, 2017, 7:54 pm

(Nov 15, 2017 04:00 PM)cocaine_monkey Wrote: [\[CITE\]](#) isnt 2.0 default in all windowses? or other version?

Not anymore it's not, the user have to manually install it on 8-10

C Plus C Sharp C - November 16, 2017, 12:30 am

(Nov 15, 2017 05:58 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Have you bothered verifying the difference in .NET Runtimes of those binaries? csc.exe is also not a managed .NET assembly for instance. Without seeing what exactly you're trying to do this can't be answered. Injection can mean many things here, and we don't even know what you're trying to inject...

How would i go about verifying the difference in .NET Runtimes of those binaries?

This is a problem i am really struggling with debugging problems, iv googled a lot and processes hollowing is hard to find detailed guides about but debuuging issues with process hollowing is totally missing in googles search results. Any advice would be greatly appreciated.

i know csc.exe is not a managed .NET assembly but it works when i inject my prog into the csc.exe in the .net 4 folder, i assume its because the needed .ddl's are in the .net 4 folder (which iv just had the idea of).

Id really like to figure out how to debug these failed injection target to see what the actual cause of the failure was, so any advice on how to do that, if its even possible would be great.

Also i am about to create a github account to upload my inject example too, Ill edit it in at the top if am able

Also heres the error log

Version=1
EventType=APPCRASH
EventTime=131553115767382563
ReportType=2
Consent=1
UploadTime=131553115771783019
ReportStatus=268435456
ReportIdentifier=d0bce2b2-2c51-4542-afc5-0b31b250d1d2
Wow64Host=34404
Wow64Guest=332
AppSessionGuid=00005c04-0001-0017-95dd-599edc5ed301

TargetAppId=W:0000f519feec486de87ed73cb92d3cac802400000000!00003a1814cda10fca4a53de9cc52c374ad098a937e9!csc.exe
TargetAppVer=2017//11//16:13:03:56!0!csc.exe
BootId=4294967295
TargetAsId=37513
Response.BucketId=55ccaf44ee6881cd6c63c0220a338321
Response.BucketTable=1
Response.LegacyBucketId=2045689908188906273
Response.type=4

Sig[0].Name=Application Name
Sig[0].Value=csc.exe
Sig[1].Name=Application Version
Sig[1].Value=8.0.50727.8784
Sig[2].Name=Application Timestamp
Sig[2].Value=5a0d8cbc
Sig[3].Name=Fault Module Name
Sig[3].Value=KERNELBASE.dll
Sig[4].Name=Fault Module Version
Sig[4].Value=6.2.15063.726
Sig[5].Name=Fault Module Timestamp
Sig[5].Value=32774c02
Sig[6].Name=Exception Code
Sig[6].Value=e0434f4d
Sig[7].Name=Exception Offset
Sig[7].Value=000ecbb2
DynamicSig[1].Name=OS Version
DynamicSig[1].Value=10.0.15063.2.0.0.256.48
DynamicSig[2].Name=Locale ID
DynamicSig[2].Value=2057
UI[2]=C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe
UI[3]=CryptMeAppA32N2 has stopped working
UI[4]=Windows can check online for a solution to the problem.
UI[5]=Check online for a solution and close the program
UI[6]=Check online for a solution later and close the program
UI[7]=Close the program
LoadedModule[0]=C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe
LoadedModule[1]=C:\Windows\SYSTEM32\ntdll.dll
LoadedModule[2]=C:\Windows\SYSTEM32\MSCOREE.DLL
LoadedModule[3]=C:\Windows\System32\KERNEL32.dll
LoadedModule[4]=C:\Windows\System32\KERNELBASE.dll
LoadedModule[5]=C:\Windows\SYSTEM32\apphelp.dll
LoadedModule[6]=C:\Windows\System32\ADVAPI32.dll
LoadedModule[7]=C:\Windows\System32\msvcrt.dll
LoadedModule[8]=C:\Windows\System32\sechost.dll
LoadedModule[9]=C:\Windows\System32\RPCRT4.dll
LoadedModule[10]=C:\Windows\System32\SspiCli.dll
LoadedModule[11]=C:\Windows\System32\CRYPTBASE.dll
LoadedModule[12]=C:\Windows\System32\bcryptPrimitives.dll
LoadedModule[13]=C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
LoadedModule[14]=C:\Windows\System32\SHLWAPI.dll
LoadedModule[15]=C:\Windows\System32\combase.dll
LoadedModule[16]=C:\Windows\System32\ucrtbase.dll
LoadedModule[17]=C:\Windows\System32\GDI32.dll
LoadedModule[18]=C:\Windows\System32\gdi32full.dll
LoadedModule[19]=C:\Windows\System32\msvcp_win.dll
LoadedModule[20]=C:\Windows\System32\USER32.dll
LoadedModule[21]=C:\Windows\System32\win32u.dll
LoadedModule[22]=C:\Windows\System32\IMM32.DLL
LoadedModule[23]=C:\Windows\System32\kernel.appcore.dll
LoadedModule[24]=C:\Windows\SYSTEM32\VERSION.dll
LoadedModule[25]=C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll

LoadedModule[26]=C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.9307_none_d0882a20442f72e4\MSVCR80.dll
LoadedModule[27]=C:\Windows\System32\shell32.dll
LoadedModule[28]=C:\Windows\System32\cfgmgr32.dll
LoadedModule[29]=C:\Windows\System32\shcore.dll
LoadedModule[30]=C:\Windows\System32\windows.storage.dll
LoadedModule[31]=C:\Windows\System32\powrprof.dll
LoadedModule[32]=C:\Windows\System32\profapi.dll

LoadedModule[33]=C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\8af4e275cca61579302056fbc4ac484f\mscorlib.ni.dll
LoadedModule[34]=C:\Windows\System32\ole32.dll
State[0].Key=Transport.DoneStage1
State[0].Value=1
FriendlyEventName=APPCRASH
ConsentKey=APPCRASH
AppName=CryptMeAppA32N2
AppPath=C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe
ReportDescription=Stopped working
ApplicationIdentity=00000000000000000000000000000000
MetadataHash=-1939372679

n0\$f3ratu\$ - November 17, 2017, 8:01 pm

(Nov 15, 2017 06:37 AM)C Plus C Sharp C Wrote: [\[CITE\]](#) I am having a problem injecting into different .net exe versions of the following files

- itself
- regasm.exe
- csc.exe
- cvtres.exe
- vbc.exe
- applaunch.exe

when injecting into the .net 4 versions of these files i can inject into all of them, but when using the .net 2 exe versions i can only inject into the first 2.

I was hoping someone could shed some light why this is an issue for me?

EDIT: the following is my source code: (i am not allowed to post links, so just append github url to the front of the below

/C-Plus-C-Sharp-C/Pen-Crypter-ExampleYour problem is targeted net framework.

C Plus C Sharp C - November 18, 2017, 7:16 am

(Nov 17, 2017 09:01 PM)n0\$f3ratu\$ Wrote: [\[CITE\]](#) Your problem is targeted net framework. Thanks for the reply, could you please expand on this.

My understanding is that i can inject .net exe into the .net 2 target exe's and .net 4 exe's into the .net 4 target exe's? is this right?

or did you mean something else?

subtilebestia - November 18, 2017, 8:14 am

This might be a stupid question but are you injection do you means of windows hooking or createRemoteThread technique. Because i might be able to help if u need assistance.

C Plus C Sharp C - November 18, 2017, 2:19 pm

i use windows hooking to edit the in memory COFF file, add my code in memory, replace entry point and the resume process... simplified version anyways. It would be great if you could help

subtilebestia - November 18, 2017, 9:10 pm

I will be looking into the code in like 2 hours. I'll give you my feedback. That good for you ?

kevy42 - November 19, 2017, 8:39 am

Idk why ur having this prob, but dont use 2.0 as Win 8/10 dosnt come with it by default. I use 4.5.2

C Plus C Sharp C - November 19, 2017, 9:05 am

(Nov 18, 2017 10:10 PM)subtilebestia Wrote: [\[CITE\]](#) I will be looking into the code in like 2 hours. I'll give you my feedback. That good for you ?

Looking forward to your feedback

(Nov 19, 2017 09:39 AM)WeedmasterOG Wrote: [\[CITE\]](#) Idk why ur having this prob, but dont use 2.0 as Win 8/10 dosnt come with it by default. I use 4.5.2

Thanks i know this but i like my code to work on all systems with .net 2 all the way to latest. This guarantees most targets are viable, example, my work is still on windows 7, lots of servers still run on 2003.

Covering .net 4 allows the injection software to target the majority of home users but would not allow the software to target lots of businesses.

Just to clarify i am not actually targeting anyone, this is just theory and experimentation (might sound stupid saying that but just want to be clear).

subtilebestia - November 26, 2017, 9:04 am

Hi sorry for the delay. I went through your code and even though it works for .net 4 i would still implement an injector that does not depend on whether your are embedding your code into managed or unmanaged code.

Not sure if you realised but you can inject .net 2 code in the .net csc 4 compiler.

That is to say that whenever you are trying to inject anything into an unmanaged process the embeded exebuffer is not even executed.

Do you mind if I share with you a project i have seen and took some ideas from which can greatly assist you.

C Plus C Sharp C - February 22, 2019, 5:57 am

(Nov 26, 2017 10:04 AM)subtilebestia Wrote: [\[CITE\]](#) Hi sorry for the delay. I went through your code and even though it works for .net 4 i would still implement an injector that does not depend on whether your are embedding your code into managed or unmanaged code.

Not sure if you realised but you can inject .net 2 code in the .net csc 4 compiler.

That is to say that whenever you are trying to inject anything into an unmanaged process the embeded exebuffer is not even executed.

Do you mind if I share with you a project i have seen and took some ideas from which can greatly assist you.

that would be great if you could