

Forum:[Hack Forums](#)

Thread: [Assembly.LoadFile works, Assembly.Load not \(with working example\) \[C#\]](#)

RickHTW - December 26, 2017, 8:46 am

Hey Guys!

First of all (because this is my first post :O) > I loooooove this forum <3

So I try to load an assembly exe (njRAT Client in this example, without any options) as byte array, here are the working codes:

#1 Load NJ-Client (32bit) via "LoadFile" > Works

```
Code string NJ_Path = @"C:\test\NJ_Client.exe"; // 32bit assembly
```

```
Assembly Asm = Assembly.LoadFile(NJ_Path);
```

```
MethodInfo AsmMethod = Asm.EntryPoint;
```

```
AsmMethod.Invoke(null, null);
```

#2 Load DummyApp (just a 32bit testing Application) via "Load" (Byte Array) > Works

```
Code string NJ_Path = @"C:\test\DummyApp.exe"; // 32bit assembly
```

```
Assembly Asm = Assembly.Load(File.ReadAllBytes(NJ_Path));
```

```
MethodInfo AsmMethod = Asm.EntryPoint;
```

```
AsmMethod.Invoke(null, null);
```

#3 Load NJ-Client (32bit) via "Load" (Byte Array > DOES NOT WORK :(

```
Code string NJ_Path = @"C:\test\NJ_Client.exe"; // 32bit assembly
```

```
Assembly Asm = Assembly.Load(File.ReadAllBytes(NJ_Path));
```

```
MethodInfo AsmMethod = Asm.EntryPoint;
```

```
AsmMethod.Invoke(null, null);
```

So my test Application works with the LoadFile and the Load (Byte Array) method, but the NJ-Client doesn't :(

I got these exception if i try it with the Load method (hope the translation is okay):

Main Exception: A call destination has caused an exception error

InnerException 1: The type initializer for "KOWvcoR00eSSwwUq2D.l1GZeOwfWjwFGK9nAc" threw an exception

InnerException 2: Common Language Runtime detected an invalid program

I tried calling the exe without VS also (the LoadFile for example only works, if I call the exe without VS / Debugger)

If I compare the assembly object with Load and LoadFile, I see these differences:

(Load vs LoadFile)

CodeBase > "C:\test\MyCaller.exe" vs "C:\test\NJ_Client.exe"

EscapedCodeBase > "C:\test\MyCaller.exe" vs "C:\test\NJ_Client.exe" (escaped)

IsStringNameVerified > "false" vs "true"

Location > "" vs "C:\test\NJ_Client.exe"

m_handle > "0x0017cf30" vs "0x01e93698"

The NJ-Client is just an example, I just want to try all assembly applications. Because of encrypting the client, I need a funktion which loads an byte array, so Assembly.LoadFile works, but with this function I need the "native" (decrypted) file :/

I tested this also with different RunPE functions, but I never found one which runs with assembly files. Also Convert assembly files (without source code) to native files seems very hard.

Any ideas?

Have big thanks! ?

HFDone - December 26, 2017, 1:51 pm

njrat have other dlls that needed when you run it LoadFile work cuz the dlls are in his path but Load load the bytes and not the dlls

RickHTW - December 28, 2017, 6:47 am

(Dec 26, 2017 02:51 PM)HFDone Wrote: [\[CITE\]](#) njrat have other dlls that needed when you run it LoadFile work cuz the dlls are in his path but Load load the bytes and not the dlls

Ah okay, thanks! This makes sense for me :) I'm currently testing / searching for a good solution. Didn't found a working solution yet (tried the dll resolve event, but it never triggered, don't know why).

Do you have a idea how to deal with that? Or do anyone know a working RunPE method for assemblies? Or in best case for assemblies AND native exes? It could be any language (C# preferred of course), I would write a dll for it.

Thanks ?

HFDone - December 28, 2017, 8:30 am

assembly resolve event should work you can also use ilmerge to pack it with the dlls

RickHTW - December 28, 2017, 11:49 am

I guess I tried the wrong way... I tried to register the resolve event in my (caller) application. I guess I need to register the event in the loaded assembly, right? But how if I can't invoke the methods?

How could ILMerge help me? The NJ_Client.exe has no dll-files on the drive, I guess the files are embedded in the exe... What should I do? Extract (how ever) the dll-files and repack them with ILMerge? Sounds like the same way as the actual exe for me. Maybe there was a mistake, with NJ_Client.exe I mean the Builder > Client (the exe which runs on a victims pc), I know many other Tools call this "server.exe", I mean server (GUILess) side :)

RickHTW - December 30, 2017, 4:57 pm

I tried it again with the resolve event, the event was fired, but there were no missing assemblies / dlls in the ResolveEventArgs Object, so I don't know what assembly should I return.

I created a new DummyApp which calls a dll as reference (the dll file is in the exe folder) and one which has the dll as embedded resource (no dll file on the filesystem).

Both variants works, if I try to invoke (by my caller) the method which needs the dll file (so this should be the same like the NJ-Client), but why this doesn't work with the NJ-Client?

Any ideas?

Thanks!