

Forum:[Hack Forums](#)

Thread: [Invoking a Function from embedded resource](#)

KrypteX - April 25, 2016, 1:08 pm

Hello everyone, I've been trying to work on a few test projects of mine and I'm coming across a bit of an impass.

I'm trying to invoke a DLL/Resource that is embedded into my application, however I keep getting an error saying that the resource that I've embedded cannot be found.

Here's the entire code that I'm using for this project.

PHP Code

```
<?php
Imports System.CodeDom
Imports System.Reflection
Imports System.Reflection.Emit
Imports System.Runtime.CompilerServices
Imports System.Text
Imports Microsoft.VisualBasic.CompilerServices

Public Class Form1
    Dim isencrypted As Boolean
    Dim key As String = "ThisKey"
    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        Invoke(retrieveFile("tmp", "superhiddenstuffs"), "test.test", "eText", New Object() {TextBox1.
Text, key})
    End Sub
    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles Button2.Click

    End Sub
    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
        Dim Library = My.Resources.test
        Dim libpath As String = Application.StartupPath & "\" & "tmp.dll"
        Dim respath As String = Application.StartupPath & "\" & "tmp.resources"
        Dim libname As String = "superhiddenstuffs"
        'Clipboard.SetText(mydll)
        compile_Core(Library, libpath, Nothing, True)
        Using r As New Resources.ResourceWriter(respath)
            r.AddResource(libname, Encoding.Default.GetString(IO.File.ReadAllBytes(libpath)))
            r.Generate()
        End Using
    End Sub
    Public Shared Function Invoke(ByVal input() As Byte, ByVal cls As String, ByVal procname As String, ByVal args() As Object) As Object
        Dim handler As New DynamicMethod("", GetType(Object), New [Type]() {GetType(Byte()), GetType(String), GetType(String), GetType(Object())})
        Dim IL As ILGenerator = handler.GetILGenerator
```

```

Dim argsLoad() As Type = New [Type]() {GetType(Byte())}
Dim mthLoad As MethodInfo = GetType(Assembly).GetMethod("Load", argsLoad)

Dim argsGTYPE() As Type = New [Type]() {GetType(String)}
Dim mthGTYPE As MethodInfo = GetType(Assembly).GetMethod("GetType", argsGTYPE)

Dim argsActi() As Type = New [Type]() {GetType(Type)}
Dim mthActi As MethodInfo = GetType(Activator).GetMethod("CreateInstance", argsActi)

Dim argsGetVal() As Type = New [Type]() {GetType(Object)}
Dim mthGetVal As MethodInfo = GetType(RuntimeHelpers).GetMethod("GetObjectValue
", argsGetVal)

Dim mthCallByName As MethodInfo = GetType(Versions).GetMethod("CallByName")

IL.Emit(OpCodes.Ldarg_0)
IL.Emit(OpCodes.Call, mthLoad)
IL.Emit(OpCodes.Ldarg_1)
IL.Emit(OpCodes.Callvirt, mthGTYPE, Nothing)
IL.Emit(OpCodes.Call, mthActi)
IL.Emit(OpCodes.Call, mthGetVal)
IL.Emit(OpCodes.Ldarg_2)
IL.Emit(OpCodes.Ldc_I4_1)
IL.Emit(OpCodes.Ldarg_3)
IL.Emit(OpCodes.Call, mthCallByName)
IL.Emit(OpCodes.Ret)
Try
    Return CallByName(handler, "Invoke
", CallType.Method, New Object() {handler, New Object() {input, cls, procname, args}})
Catch ex As Exception
    MsgBox(ex.Message)
End Try
End Function
Public Shared Function retrieveFile(ByVal resName As String, ByVal libname As String) As Byte()
    Dim res_Man As New Resources.ResourceManager(resName, Reflection.Assembly.GetEntryA
ssembly)
    Try
        Return (Encoding.Default.GetBytes(res_Man.GetObject(resName)))
    Catch ex As Exception
        MsgBox(ex.Message)
    End Try
End Function
Public Shared Function compile_Core(ByVal input As String, ByVal output As String, ByVal resou
rces As String, ByVal showError As Boolean) As Boolean
    Dim provider_Args As New Dictionary(Of String, String)()
    provider_Args.Add("CompilerVersion", "v2.0")
    Dim provider As New Microsoft.VisualBasic.VBCodeProvider(provider_Args)
    Dim c_Param As New Compiler.CompilerParameters
    Dim c_Args As String = " /target:library /platform:x86 /optimize /define:_MYTYPE=\\"""""Empty\
""""""
    c_Param.GenerateExecutable = True
    c_Param.OutputAssembly = output
    c_Param.CompilerOptions = c_Args

```

```

c_Param.IncludeDebugInformation = False
If resources IsNot Nothing Then
    c_Param.EmbeddedResources.Add(resources)
End If
c_Param.ReferencedAssemblies.AddRange({"System.Dll", "System.Windows.Forms.Dll"})
Dim comp_Result As Compiler.CompilerResults = provider.CompileAssemblyFromSource(c_P
aram, input)
If comp_Result.Errors.Count = 0 Then
    Return True
Else
    If showError Then
        For Each _Error As Compiler.CompilerError In comp_Result.Errors
            MessageBox.Show(_Error.ToString)
        Next
        Return False
    End If
    Return False
End If
End Function
End Class

```

If anyone can help me figure out where I'm going wrong it'd be much appreciated.
 Also, I'm trying to give credit for where credit is due, not all of this is written by me, so if you see something that doesn't have credits please leave a comment or PM me and I'll put them in.

Shout out to Pr0sus as well, I'm using examples from his crypter source to call the function. I think what could be wrong is the way that the resource is being built here:

PHP Code

```
<?php
```

```

Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
    Dim Library = My.Resources.test
    Dim libpath As String = Application.StartupPath & "\" & "tmp.dll"
    Dim respath As String = Application.StartupPath & "\" & "tmp.resources"
    Dim libname As String = "superhiddenstuffs"
    'Clipboard.SetText(mydll)
    compile_Core(Library, libpath, Nothing, True)
    Using r As New Resources.ResourceWriter(respath)
        r.AddResource(libname, Encoding.Default.GetString(IO.File.ReadAllBytes(libpath)))
        r.Generate()
    End Using
End Sub

```

And on this line:

PHP Code

```
<?php
```

```
compile_Core(Library, libpath, Nothing, True)
```

VisualSoft - April 26, 2016, 2:51 am

try "Reflection.Assembly.ExecutingAssembly" in place of "Reflection.Assembly.GetEntryAssembly"

KrypteX - April 26, 2016, 11:00 am

That's what I was trying before I was using getentry, but I keep getting an exception has been

thrown by the target of an invocation which I'm not sure how to track, I wish there was more detail in these error reports to give me an idea. I've looked up on MSDN about this exception and I've tried renaming the resource a few times but it seems like it just wants to keep throwing that exception

VisualSoft - April 26, 2016, 11:27 am

yes Op is correct, if you can post more info about error, would be easy for us to help you out with it.

TRH4CK - April 26, 2016, 12:11 pm

I can't see well as I am on a tablet, however:

```
Code Dim res_Man As New Resources.ResourceManager(resName,
Reflection.Assembly.GetEntryAssembly)
Try
    Return (Encoding.Default.GetBytes(res_Man.GetObject(resName)))
Catch ex As Exception
    MsgBox(ex.Message)
End Try
```

In here you get the object from a resourcefile named the same as the object.

You should get the object named "superhiddenstuffs" from the "tmp" ressource.

godlyitnetwork - April 26, 2016, 4:26 pm

try using win32 API to access it.

KrypteX - April 27, 2016, 12:10 am

Alright, so here's the error in full that I'm getting. I've changed around a couple of things since I realize right now I'm not gonna be using the DLL as an encrypted resource, I just need the DLL to invoke the function in the embedded resource

```
PHP Code
<?php
System.Reflection.TargetInvocationException was unhandled
Message=Exception has been thrown by the target of an invocation.
Source=Microsoft.VisualBasic
StackTrace:
    at Microsoft.VisualBasic.CompilerServices.Symbols.Container.InvokeMethod(
Method TargetProcedure, Object[] Arguments, Boolean[] CopyBack, BindingFlags Flags)
    at Microsoft.VisualBasic.CompilerServices.NewLateBinding.CallMethod(
Container BaseReference, String MethodName, Object[] Arguments, String[] ArgumentNames, Type
[] TypeArguments, Boolean[] CopyBack, BindingFlags InvocationFlags, Boolean ReportErrors,
ResolutionFailure& Failure)
    at Microsoft.VisualBasic.CompilerServices.NewLateBinding.LateCall(Object Instance,
Type Type, String MemberName, Object[] Arguments, String[] ArgumentNames, Type[]
TypeArguments, Boolean[] CopyBack, Boolean IgnoreReturn)
    at Microsoft.VisualBasic.CompilerServices.Versioned.CallByName(Object Instance,
String MethodName, CallType UseCallType, Object[] Arguments)
    at Load_Encrypted_DLL_Testing.Form1.ivoke(Byte[] input, String cls, String procname, Object
[] args) in S:
\Users\W\Documents\Visual Studio 2015\Projects\Load Encrypted DLL Testing\Load Encrypted DLL
Testing\Form1.vb:line 62
    at Load_Encrypted_DLL_Testing.Form1.Button1_Click(Object sender, EventArgs e) in S:
\Users\W\Documents\Visual Studio 2015\Projects\Load Encrypted DLL Testing\Load Encrypted DLL
Testing\Form1.vb:line 12
    at System.Windows.Forms.Control.OnClick(EventArgs e)
```

at System.Windows.Forms.Button.OnMouseUp(MouseEventArgs mevent)
at System.Windows.Forms.Control.WmMouseUp(Message& m, MouseButtons button, Int32 clicks)
at System.Windows.Forms.Control.WndProc(Message& m)
at System.Windows.Forms.ButtonBase.WndProc(Message& m)
at System.Windows.Forms.Button.WndProc(Message& m)
at System.Windows.Forms.Control.ControlNativeWindow.WndProc(Message& m)
at System.Windows.Forms.NativeWindow.DebuggableCallback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)
at System.Windows.Forms.UnsafeNativeMethods.DispatchMessageW(MSG& msg)
at System.Windows.Forms.Application.ComponentManager.System.Windows.Forms.UnsafeNativeMethods.IMsoComponentManager.FPushMessageLoop(Int32 dwComponentID, Int32 reason, Int32 pvLoopData)
at System.Windows.Forms.Application.ThreadContext.RunMessageLoopInner(Int32 reason, ApplicationContext context)
at System.Windows.Forms.Application.ThreadContext.RunMessageLoop(Int32 reason, ApplicationContext context)
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.OnRun()
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.DoApplicationModel()
at Microsoft.VisualBasic.ApplicationServices.WindowsFormsApplicationBase.Run(String[] commandLine)
at Load_Encrypted_DLL_Testing.My.MyApplication.Main(String[] Args) in :line 81
at System.AppDomain._nExecuteAssembly(Assembly assembly, String[] args)
at Microsoft.VisualStudio.HostingProcess.HostProc.RunUsersAssembly()
at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
at System.Threading.ThreadHelper.ThreadStart()
InnerException:
Message=Value cannot be null.
Parameter name: type
ParamName=type
Source=mscorlib
StackTrace:
at System.Activator.CreateInstance(Type type, Boolean nonPublic)
at (Byte[] , String , String , Object[])
InnerException:

For some reason it's telling me I can't post because of an SQL injection attack..

New reply: <http://pastebin.com/SVLrmpV0>

Cecilia - April 27, 2016, 2:53 am

<https://github.com/Panthere/RuntimeExample>

Perhaps that might help you?

Invoking in such an obscure way is not needed.

HFDone - April 27, 2016, 4:24 am

the invoke function is not stable use other way

KrypteX - April 27, 2016, 8:53 pm

(Apr 27, 2016 04:24 AM)HFDone Wrote: [\[CITE\]](#) the invoke function is not stable use other way
I've heard that the most common methods are pretty much all detected by Avira though I haven't

put that to the test

Cecilia - April 27, 2016, 9:30 pm

(Apr 27, 2016 08:53 PM)KrypteX Wrote: [\[CITE\]](#) I've heard that the most common methods are pretty much all detected by Avira though I haven't put that to the test
Junk code fixes most avira detections, its quite simple.

KrypteX - April 28, 2016, 12:43 am

Alrighty I'll go about seeing if I can get it done another way :3 In the meantime I'm trying to get a RunPE working on my crypter project

Cecilia - April 28, 2016, 2:06 am

(Apr 28, 2016 12:43 AM)KrypteX Wrote: [\[CITE\]](#) Alrighty I'll go about seeing if I can get it done another way :3 In the meantime I'm trying to get a RunPE working on my crypter project
Give a look at my example I provided.
It can be used in such ways.

gigajew - April 29, 2016, 8:38 am

(Apr 27, 2016 02:53 AM)LaPanthere Wrote: [\[CITE\]](#) <https://github.com/Panthere/RuntimeExample>

Perhaps that might help you?
Invoking in such an obscure way is not needed.
This, 10 times this.

KrypteX - April 29, 2016, 11:01 am

(Apr 28, 2016 02:06 AM)LaPanthere Wrote: [\[CITE\]](#) Give a look at my example I provided.
It can be used in such ways.
I've been looking at it but I have no idea how to translate, I can understand it a little but I have next to 0 knowledge of C# and I've already tried converting to .net

Cecilia - April 29, 2016, 6:22 pm

(Apr 29, 2016 11:01 AM)KrypteX Wrote: [\[CITE\]](#) I've been looking at it but I have no idea how to translate, I can understand it a little but I have next to 0 knowledge of C# and I've already tried converting to .net
What bits are causing concern?

Use a vb.net converter.
Here's what I got: