

## Forum:[Hack Forums](#)

Thread: [Builder /Stub - Fully Cryptable | NO EOF](#)

**Proton!** - November 20, 2014, 2:42 am

Hey ya'll, I remember back before I was in the struggle to find out the best way to make a builder for my RAT; How would I go on about writing settings to the stub.

Well, today I'll be showing you how to do this, and it's actually rather simple :)  
The best though; It does not involve EOF, so It's pretty much fully cryptable!

First let me explain you what we are going to be using to write to the stub;  
The UpdateResource API in the kernel32.dll

First download [this](#) class. (This is the class containing the functions to read/write resources.

So to explain the functions:

The function 'WriteResource' is a function that I made that you can simply call to write resources to the specified file with the specified resourcename. The resource written has to be byte array; whether that is a string encoded as byte array or some serialized data, thaty

It does the following: Retrieves a handle for updating resources by calling the native function "BeginUpdateResource"

Gets a pointer for the resource value that is going to be written to the resource.  
Calls the UpdateResource function to write the new resource to the file.

The function 'ReadResource' is a function that I made that you can simply call to read the resources from the specified file using the specified resourcename. The filename can be specified as Nothing, that will make it read the resources from itself (what the stub does).

It does the following:

Retrieves a handle for the found resource. Retrieves a handle for the resource when it's loaded.  
Gets the size of the resource so it can allocate the proper sized byte array for the data.  
\* Copies the data from the resource into the byte array and retrieves it.

Here is a simple builder:

In my builder I have two textboxes

The settings I use for demonstration is called 'Host' and 'Port'.

Some typical scenario for this would be in a RAT stub or something along those lines.

This is the code for the Button called "Build":

```
Code Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
    Using SFD As New SaveFileDialog()
        SFD.Title = "Save the stub..."
        SFD.Filter = "Executable (*.exe) |*.exe"
        If Not SFD.ShowDialog() = Windows.Forms.DialogResult.OK Then Return
        File.WriteAllBytes(SFD.FileName, My.Resources.Stub)
        If ResourceManager.WriteResource(SFD.FileName, "Host",
```

```

Encoding.UTF8.GetBytes(TextBox1.Text)) AndAlso _
    ResourceManager.WriteResource(SFD.FileName, "Port",
Encoding.UTF8.GetBytes(TextBox2.Text)) Then
    MessageBox.Show("The stub was successfully built!", "Success!", MessageBoxButtons.OK,
MessageBoxIcon.Information)
    Process.Start("explorer.exe", "/select, " & SFD.FileName)
    End If
    End Using
    End Sub
Pretty clean..

```

Now the stub code:

Code Module Main

```

Sub Main()
    RetrieveTheSettings()
End Sub

```

```

Sub RetrieveTheSettings()
    Dim Host As String = Encoding.UTF8.GetString(ResourceManager.ReadResource(Nothing,
"Host"))
    Dim Port As String = Encoding.UTF8.GetString(ResourceManager.ReadResource(Nothing,
"Port"))

    MessageBox.Show(String.Format("Settings Read:{0}Host:{1}{2}Port:{3}", vbCrLf, Host, vbCrLf,
Port), "Success!", MessageBoxButtons.OK, MessageBoxIcon.Information)
End Sub
End Module

```

If you want to download my solution, you may do so [here](#).

I hope you guys enjoyed this tutorial, and hopefully I explained it decently enough :)

And if you have any feedback, please leave; criticism or positive :)

~ Regards Proton!

**nathan72389** - November 20, 2014, 4:48 am

after EOF this is the next insecure way of storing stuff.  
it actually makes it easier for me to remove any info that your storing.  
think reshacker...  
you dont need a whole class for what 3,4 api calls.  
this is old school also. vb6(and lower) had been using this for a loooooong time.  
most other builder/stub applications regardless of the language still use this method.  
heck, i still use it in delphi.  
its nice to see something posted over again with 1/2 an explanation.

**Proton!** - November 20, 2014, 4:52 am

(Nov 20, 2014 05:48 AM)nathan72389 Wrote: [\[CITE\]](#) after EOF this is the next insecure way of storing stuff.  
it actually makes it easier for me to remove any info that your storing.  
think reshacker...  
you dont need a whole class for what 3,4 api calls.  
this is old school also. vb6(and lower) had been using this for a loooooong time.

most other builder/stub applications regardless of the language still use this method.  
heck, i still use it in delphi.

its nice to see something posted over again with 1/2 an explanation.

Best is removed; I haven't seen any proper explanation tutorial on HF regarding this method. To me this is better than codedom if you have a preobfuscated stub.

**IAmNotHere** - November 20, 2014, 4:57 am

Thanks, but uhum.

How do you make the main.vb? I keep getting an empty Form1 every time I try to run my messagebox with the values?

**Proton!** - November 20, 2014, 5:06 am

(Nov 20, 2014 05:57 AM)IAmNotHere Wrote: [\[CITE\]](#) Thanks, but uhum.

How do you make the main.vb? I keep getting an empty Form1 every time I try to run my messagebox with the values?

I simply made a windows forms project, and then I deleted Form1, and made a new module called Main.

**IAmNotHere** - November 20, 2014, 5:09 am

Going to try again, had this question while building a rat also and builded one with a form1 as stub then.

**Proton!** - November 20, 2014, 5:12 am

(Nov 20, 2014 06:09 AM)IAmNotHere Wrote: [\[CITE\]](#) Going to try again, had this question while building a rat also and builded one with a form1 as stub then.

Better not to have a Form:) I see some RAT sources using Forms that are simply hidden.

**IAmNotHere** - November 20, 2014, 5:16 am

I deleted my form1 and added a module which I named Main.vb, but now:

```
Code Error 10 'Main' is a type in 'Stub' and cannot be used as an expression.
Application.Designer.vb 35 27 Stub
```

**Proton!** - November 20, 2014, 5:21 am

(Nov 20, 2014 06:16 AM)IAmNotHere Wrote: [\[CITE\]](#) I deleted my form1 and added a module which I named Main.vb, but now:

```
Code Error 10 'Main' is a type in 'Stub' and cannot be used as an expression.
Application.Designer.vb 35 27 Stub
```

Hmm, did you go into "My Project" and disabled Application framework and set the startup object to sub main or Main?

**IAmNotHere** - November 20, 2014, 5:28 am

Proton! Dude, you made my day! The messagebox popped up as expected with the info I entered in the textboxes.

This is actually pretty cool. I have more projects where external stubs are involved and, if I want to change something I have to continuously open my visual studio for editing. I am going to see, if I can make an auto stub editor for my projects.

Positive + to Proton!  
Have a good day.

**Proton!** - November 20, 2014, 5:29 am

(Nov 20, 2014 06:28 AM)IAmNotHere Wrote: [\[CITE\]](#) Proton! Dude, you made my day!

This is actually pretty cool. I have more projects where external stubs are involved and, if I want to change something I have to continuously open my visual studio for editing. I am going to see, if I can make an auto stub editor for my projects.

Have a good day.

Sounds cool man :) - I hope u got it all working out for you now :)!

**SIM-1676753** - November 20, 2014, 7:59 pm

(Nov 20, 2014 07:29 PM)Odinz Wrote: [\[CITE\]](#) You didn't code this class.

<https://hackforums.net/showthread.php?tid=430500>

Deathader originally made this, and you just changed added created a class that combines the ResourceReader and the ResourceWriter modules, and added some minor changes.

<http://www.diffnow.com/?report=3ntzj>

I can still see that it's been modified. If it was copied, then OP should have given proper credits to the original coder along with his name in the class or something if he decided to do so.

**Proton!** - November 21, 2014, 4:16 am

(Nov 20, 2014 07:29 PM)Odinz Wrote: [\[CITE\]](#) You didn't code this class.

<https://hackforums.net/showthread.php?tid=430500>

Deathader originally made this, and you just changed added created a class that combines the ResourceReader and the ResourceWriter modules, and added some minor changes.

<http://www.diffnow.com/?report=3ntzj>

I didn't CP this, I have actually made it from scratch, which isnt that hard tbh.. as the UpdateResource API is quite easy to understand.