

Forum:[Hack Forums](#)

Thread: [\[VB .NET\] Write/Read Resource! \(Bypass Avira\) - Modded](#)

pr3fix - July 19, 2010, 1:02 am

Write/Read Resource! (Bypass Avira)

Hello everyone. Well, recently some guy asked me to make an example on this how to use. So I made it, plus I modded it a bit so you can declare custom resource's name. Anyways, hope you'll like it and please post or send me PM if you have any problem. Also I want to say thanks & to regard Deathader, Aeonhack & Fenimin!

This method will easily bypass Avira. Leave a comment and rate thread. Thanks & Good luck!

Usage:

[img]http://ploader.net/files/44ad80e04617412d0bf82785eda7e6a4.gif[/img]

Download:

Code <http://uppit.com/5y8cw28s1cmh/Code.rar>

Builder Password:

Spoiler ([Click to View](#))

Code

```
+5XKDg9uAlryMHGrfi6kbgqJfoXqMgr2MfgqHg9GKtAx+oH6Slr1iGkJTyS=+iX9L4ASgy/k0HBBT4KIL
55tnkbbkLlhxLIXSLILKgj1BnyHSTGr6DIBzeiu7MG0xDf6MHoX=0i6yKmBPAkAYfg6AbxQ=TxcPMgXZ
+xnqSHTGLmA1+JQ6RlnqixQRSOQOMIXfLg0=p23sKlkVTf13SI04b5cJgfXT+tLafI0rMt1xfGrYM41s
Hh64D6ALeiwqDxXgHo5IMGJNSic6DiXsn8ASegkR0fhqAITALJ6rKf13fGqq+gQHn8L1Ti0Pi80qL5rz
fJB=Si6B0jHSMiTklX6PKHTobxHgpHX9bizIH5rzSHBUD4/rMgXzgxuGegk1D6T3RtbrnJkoDGcG+tH
XnG0kej1BM8XD+iWJLI6kplLQfGrPAkYH8AKfILR+XH5rD5haRtH=K6Q3nDgtAluGegkq+IXSfl9j+h
Q30HTxMkXNLgWrp53kMkHqAITX+yXkbgrQbHATntT3fI0z+IH0DhLOD503Slk2gx6QnirVTiueSGW
r+Jc9i8LqT5Pkb16mnj1agHLxphhZMg5t+GA7pyhfLIXKRlc2bghJSicSphX6DI6Pp5AuSoW=SxTeLyX
RKgbk0lr1T5Xof8WITiLRSGhYDyHzbj6PK5kG0mTGTjQzAlrKb5kJgiHS+kX9Lx9gbgk=SjH6MG03g
xquSHANTguOTgXffi9j+29xT4HTM8L9gJnliGc=TxW=TWG6SJAvmgXiLJWanJXoMIXTe8hgKx9gn
6TxfhBqM4KlbgBk+iHQHlhxLJXaSoAzbj/lpx9GT6Wtn8ASMGCrmthBMjHkLxJrSl6ybgrST8hYnGA4i
IL3TxXGTxXfLg6sp29B0fhym4hT+4XKpxKIDG0TMGhaKx6KH6TzOmT6MHhNMgXzgx0ynyQxMgrz
LILgK6Q30jhGpGW6SJATMIXfHInup5AJfhAyMjHTfG01fIHQgiXy0hXaLxJkKD99gHLyLmHsRJXY0i
HaSfGq0GrSfJBzbi09ShB1Di9Tn8XSnD9uSHQSMf56SJAXpGX6H2c8bqCC
```

Encryption method

TRIPO-5 (5 times) > FERON-74 (3 times) > ROT-13 > ATOM-128 (2 times)

Stub Password:

Spoiler ([Click to View](#))Code

```
e4S0RzdVY4o1XLME/4p0ntdhmKBMe+n4IEa//KhuYEph=z/Ne6amd+duQcdhVEqDe5n0VcpYU6wu
QbD18KREW0q5nKGwV+dvQ=NhX6/2nKh0UKm1/4/qS5Az/4R6/c/4dzvK/bd1=EwKUzSw8KB6U+q
hnLRhe4xn/zaQRiv1bb93W5/smpnbdBdtVEBhVa41l+7mMoaE/5Qw/Lp680aIQbdEea5oRtd=/07/X2
NYUtBze6NE80BMRCN1eY=T
```

Encryption method

ATOM-128 (3 times) > ROT-13 > Base-64 > HAZZ-15 > TRIPO-5

Tip: To decrypt, you will have to use your brain. Not only copy/paste to decrypters. Best Regards!

- pr3fix

PAGMAN - July 19, 2010, 1:14 am

Wow. Surprised no one has commented yet. Good job pr3fix. This may help get stubs FUD again once WriteResource is detected .

EDIT: I just decrypted the stub password. There is an error on the last decryption cycle of ATOM-128. I got all of the password except for two non-ascii characters at the end.

pr3fix - July 19, 2010, 1:15 am

(Jul 19, 2010 01:14 AM)PAGMAN Wrote: [\[CITE\]](#) Wow. Surprised no one has commented yet. Good job pr3fix. This may help get stubs FUD again once WriteResource is detected .
Ah, it will be FUD for long time.

EOF was FUD for years, I doubt this one wont be FUD that long if you use your imagination.

Exploitations - July 19, 2010, 1:16 am

(Jul 19, 2010 01:14 AM)PAGMAN Wrote: [\[CITE\]](#) Wow. Surprised no one has commented yet. Good job pr3fix. This may help get stubs FUD again once WriteResource is detected .
Thats cause it takes forever to decrypt this.

PAGMAN - July 19, 2010, 1:24 am

(Jul 19, 2010 01:16 AM)Exploitations Wrote: [\[CITE\]](#) Thats cause it takes forever to decrypt this.
True that. Did you successfully decrypt it? I got two non-ascii characters at the end of the password for the stub.

pr3fix - July 19, 2010, 1:32 am

Guys I think I didn't wrote something right for stub's password, I'll post new one in 20 minutes. :/

Exploitations - July 19, 2010, 1:35 am

(Jul 19, 2010 01:24 AM)PAGMAN Wrote: [\[CITE\]](#) True that. Did you successfully decrypt it? I got two non-ascii characters at the end of the password for the stub.
yeah the pass doesn't work for the builder. Idk about the stub yet.

pr3fix - July 19, 2010, 1:38 am

(Jul 19, 2010 01:35 AM)Exploitations Wrote: [\[CITE\]](#) yeah the pass doesn't work for the builder. Idk about the stub yet.
Works perfect, I have just tested it.

CYSER - July 19, 2010, 2:00 am

So old :(, thats not a thanks worth if you can't modify it your own u should leave it!

pr3fix - July 19, 2010, 2:02 am

(Jul 19, 2010 02:00 AM)CYSER Wrote: [\[CITE\]](#) So old :(, thats not a thanks worth if you can't modify it your own u should leave it!
Ehm what? What do you mean, it's not old? This is one of the latest methods in VB8. I can modify, and I have modified it already.

Numair - July 19, 2010, 2:11 am

This is wonderful thanks pr3fix.

pr0t0typ3 - July 19, 2010, 4:57 am

That looks quite nice.. I also did it a while ago and had some problems with the names....

Then I found out , that I need to use numbers for them

µnKn0wn_H4CK3r - July 19, 2010, 6:16 am

Hi!

Hmm... I also got 2 non-ASCII characters for the stub password..

I use my brain but ? ...

50GTB - July 19, 2010, 6:17 am

man this is the easy think ever and their is people getting money to setup for them wtf..

Asus - July 19, 2010, 6:32 am

How does this work? You attach the stub to the builder and change strings?

pr3fix - July 19, 2010, 9:34 am

(Jul 19, 2010 06:16 AM)BabyHack Wrote: [\[CITE\]](#) Hi!

Hmm... I also got 2 non-ASCII characters for the stub password..

I use my brain but ? ...

Atm, i'm not on my PC.

I'm not able to give you a link. I'll have to edit main post.

pr0t0typ3 - July 19, 2010, 9:37 am

I have one question to you... I didn't download so I have to ask you : Did you store multiple strings or just one string and then splitting them ? Because a few days ago I also made smth. similar you can see here : <https://hackforums.net/showthread.php?tid=552729> and my version uses multiple stored strings and no splittings

pr3fix - July 19, 2010, 10:02 am

(Jul 19, 2010 09:37 AM)pr0t0typ3 Wrote: [\[CITE\]](#) I have one question to you... I didn't download so I have to ask you : Did you store multiple strings or just one string and then splitting them ? Because a few days ago I also made smth. similar you can see here : <https://hackforums.net/showthread.php?tid=552729> and my version uses multiple stored strings and no splittings

Well, for this example I used only one string since I only stored Text.

The-Madness - July 20, 2010, 3:40 pm

Hello, I have decrypted password for stub and builder, but they don't work :(

?LIT? \$ØLDI?R - July 20, 2010, 3:50 pm

thx this works great,keep up the good work

Neroxan - July 20, 2010, 3:57 pm

Good work I guess, but Id rather check msdn & add the support for this myself rather than messing with decryption. I understand why you decided to do it, but its still a lil fubard to do it after the original author just posted it in plain text for you to get & modify...

Oh, and if you want a REALLY secure modification to make to it. Set it up to add the data as several resources and join them back together in the stub before decrypting. Credits would be due to "sotpot" for offering that idea up though.

Su?ernatural - July 20, 2010, 5:58 pm

I'm not really sure but I think Avira detects this now :(

Neroxan - July 20, 2010, 6:08 pm

(Jul 20, 2010 05:58 PM)Supernatural® Wrote: [\[CITE\]](#) I'm not really sure but I think Avira detects this now :(

Change the resource type that you are using to check if that is whats being detected or not. If you change it and dont get more/less detections then that isnt the issue.?

revtorus - July 21, 2010, 4:52 am

Passwords don't work :/

I'm not a noob in the Builder password there is a "okay"

And in the Stub password there is a "You" =)

But both don't work

Braco Asshole - July 21, 2010, 4:56 am

Very nice. Good job pr3fix.

The-Madness - July 21, 2010, 5:01 am

Yeah Revtorus the password don't work for me too.

Hecker21 - July 21, 2010, 5:56 am

Thanks for this!

Gonna dl as soon as I can get to my Pc :3

pr3fix - July 21, 2010, 6:34 am

(Jul 20, 2010 05:58 PM)Supernatural® Wrote: [\[CITE\]](#) I'm not really sure but I think Avira detects this now :(

You are right, you aren't sure and Avira doesn't detects this.

The-Madness - July 21, 2010, 9:02 am

Hey pr3fix i send you a pm with passwords, because don't work for me.

Edit: I can't send you pm because you reached your private message quota.

Threadlocks - July 22, 2010, 6:44 pm

can some one help me with passwords ?

z3pt0seC - July 23, 2010, 2:24 am

Nice share pr3fix.

vRicks

EDIT:

Update the file's password to the currents...

?LIT? \$ØLDI?R - July 23, 2010, 3:04 am

thx

too short so i made it longer

Flork - July 23, 2010, 3:07 am

question for pr3fix. can you sell a private stub or nemesis protector 1.2 , i want buy it for you.

ps.sorry for my weak english.

z3pt0seC - July 23, 2010, 3:47 am

(Jul 23, 2010 03:04 AM)elite klr Wrote: [\[CITE\]](#) --REMOVED--Please edit your post.
vRicks

Threadlocks - July 23, 2010, 3:49 am

the password not works lol too short

pr3fix - July 23, 2010, 4:48 am

(Jul 23, 2010 03:07 AM)mateoallegro Wrote: [\[CITE\]](#) question for pr3fix. can you sell a private stub or nemesis protector 1.2 , i want buy it for you.

ps.sorry for my weak english.
I am working on private version of it.

/etc/security/access.conf - July 23, 2010, 5:32 am

Good Job Pr3fix,

But Builder Password doesn't works.
I've tested it 5times with copy/paste and without..
Hope you can tell me why :).

Cheers.

pr3fix - July 23, 2010, 5:34 am

(Jul 23, 2010 05:32 AM)NoxiousHacker Wrote: [\[CITE\]](#) Good Job Pr3fix,

But Builder Password doesn't works.
I've tested it 5times with copy/paste and without..
Hope you can tell me why :).

Cheers.
I can and already have .

/etc/security/access.conf - July 23, 2010, 5:37 am

Could I PM what I got when decrypting them sir?

Thanks.

flAmingw0rm - July 23, 2010, 5:46 am

Thanks a lot. Decrypting this password now. ?

Edit: Password for builder doesn't work, I haven't test the stub yet.

This is what I get when decrypting:  unknown letter.. the latest letter of the word.

/etc/security/access.conf - July 23, 2010, 5:54 am

Yep the same..but I think we have to use our brain. This is not the real password. Something could help us to the true way...

pr3fix - July 23, 2010, 5:55 am

I'm not able to, I'm not on my main PC for another week or more. So I'm not sure..

/etc/security/access.conf - July 23, 2010, 5:59 am

Oh but don't you remember? ;(. Can't wait to get this! :D

?LIT? \$ØLDI?R - July 23, 2010, 6:09 am

password for both doesnt work in the winrar,i decrypted it,and still nothing...

pr3fix - July 23, 2010, 6:14 am

(Jul 23, 2010 06:09 AM)elite klr Wrote: [\[CITE\]](#) password for both doesnt work in the winrar,i decrypted it,and still nothing...

I do not like to insult people, but you sir are idiot.

Da Loser - July 25, 2010, 2:25 pm

decrypting the password is impossible on an iPad.

-.-

Deathader - July 25, 2010, 4:29 pm

If this uses my source, would you mind adding me to the credits / linking my thread? Thanks.

pr3fix - July 26, 2010, 1:11 am

(Jul 25, 2010 04:29 PM)Deathader Wrote: [\[CITE\]](#) If this uses my source, would you mind adding me to the credits / linking my thread? Thanks.

Well, I did already. There is credits in source and in thread. It's not same like your code, it's an modification.

Also, at the end of thread's introduction I mentioned:

"Also I want to say thanks & to regard Deathader, Aeonhack & Fenimin!"

MagicMushroom™ - July 26, 2010, 1:29 am

pass doesn't work for me

Spoiler [\(Click to View\)](#)

Too short

¶_¶ - August 10, 2010, 3:52 am

I'm using my brain and can't get the decrypted pass working!

Tasemu - October 23, 2010, 3:01 pm

Haha, i failed miserably at decrypting. O well. ^^

kas - October 23, 2010, 3:17 pm

thanks for sharing it is very interesting!

EDIT:

The password of the stub not working, i am decrypt but in then end atom-128 do ERROR

Farhan879 - October 23, 2010, 11:11 pm

The pass ain't working. There's 2 non-acsii chars on the stub pass

?eumonic - October 23, 2010, 11:32 pm

He is aware that neither password is working...

They are both corrupt in some way (at least when I decrypt them), and he is going to fix them when

he gets back to his main PC.

PongViking - October 24, 2010, 12:29 am

I decrypted passwords, but doesn't work!
What to do ?

xCocaine - October 24, 2010, 12:41 am

I decrypted successfully the password of the builder, but Pr3fix i need to put the last word after : or anything?
Because isn't working but i got the plain text.

And for stub latest 2 chars is wrong

Panagiota - November 3, 2010, 2:19 am

(Oct 23, 2010 11:11 PM)Farhan879 Wrote: [\[CITE\]](#) The pass ain't working. There's 2 non-acscii chars on the stub pass
Same thing here... God damn it.

xCocaine - November 3, 2010, 7:20 am

(Nov 3, 2010 02:19 AM)UNd3ad Wrote: [\[CITE\]](#) Same thing here... God damn it.
He said in 20 minuts will post the new password... But he said this 4-5 days ago lol.

Grieve™ - November 3, 2010, 3:00 pm

c'mon pr3fix please fix the passwords! id love to study this source! :)

kas - November 4, 2010, 12:53 pm

(Nov 3, 2010 03:00 PM)Grieve™ Wrote: [\[CITE\]](#) c'mon pr3fix please fix the passwords! id love to study this source! :)
I wait also the new password, please fix the password, this source is very interesting.

Thanks.

Panagiota - November 5, 2010, 2:50 pm

(Nov 3, 2010 03:00 PM)Grieve™ Wrote: [\[CITE\]](#) c'mon pr3fix please fix the passwords! id love to study this source! :)
PMed him about this issue and still waiting for his response...

pr3fix - November 5, 2010, 4:13 pm

Guys, I am really busy with my new crypter.

I will post new & better example, this is detected though.

Grieve™ - November 5, 2010, 7:27 pm

Ok thankyou pr3fix!

Spoiler [\(Click to View\)](#)not too short

Panagiota - December 7, 2010, 12:32 am

Please Pr3fix, stop ignoring this, me and many other members are still waiting for this issue to be fixed.

(Nov 3, 2010 03:00 PM)Grieve™ Wrote: [\[CITE\]](#) c'mon pr3fix please fix the passwords!

(Oct 23, 2010 11:11 PM)Farhan879 Wrote: [\[CITE\]](#) The pass ain't working. There's 2 non-acscii chars

on the stub pass

(Oct 24, 2010 12:41 AM)xCocaine Wrote: [\[CITE\]](#) And for stub latest 2 chars is wrong

(Nov 3, 2010 07:20 AM)xCocaine Wrote: [\[CITE\]](#) He said in 20 minuts will post the new password...

But he said this 4-5 days ago lol.

N3oNight - December 7, 2010, 12:57 am

Hai thanks for this..

It will be really help full for people like me...

thanks man...

Sia - December 7, 2010, 2:43 am

LOL console.writeline (form2.textbox1.text) ????

don't see the big deal sorry

d3c0mpil3r - December 7, 2010, 3:36 am

(Dec 7, 2010 03:43 AM)VirtualDUDE Wrote: [\[CITE\]](#) LOL console.writeline (form2.textbox1.text) ????

don't see the big deal sorry

I think you're joking? right?

perfectiv - December 7, 2010, 3:41 am

Thank's alot for this pr3fix. Will come in handy.

san77 - June 4, 2011, 10:09 pm

(Dec 7, 2010 01:32 AM)UNd3ad Wrote: [\[CITE\]](#) Please Pr3fix, stop ignoring this, me and many other members

are still waiting for this issue to be fixed.You fucking too hard ..you post this thread useless because you post wrong password ,u konw what is the problem, but you never fixed this .This is totally disappoint our members ??

DgK - August 13, 2011, 7:35 pm

this is really good tut but fuck me i cant decrypt it :[

n0\$f3ratu\$ - August 13, 2011, 10:48 pm

I delegated all the functions and call them by api, but as soon as i did that i've got a error and my crypted file stoped working.

When i went back to original functions all was ok.

I wonder why?

Original function

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

Delegated

```
Code Delegate Function Gmh(ByVal moduleName As String) As System.IntPtr
```

Call

```
Code Dim Gmh = CreateApi(Of Gmh)("kernel32", "GetModuleHandle")
```

Am i doing something wrong?

Banks? - August 14, 2011, 1:00 am

(Aug 13, 2011 10:48 PM)n0\$f3ratu\$ Wrote: [\[CITE\]](#) I delegated all the functions and call them by api, but as soon as i did that i've got a error and my crypted file stoped working.

When i went back to original functions all was ok.

I wonder why?

Original function

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

Delegated

```
Code Delegate Function Gmh(ByVal moduleName As String) As System.IntPtr
```

Call

```
Code Dim Gmh = CreateApi(Of Gmh)("kernel32", "GetModuleHandle")
```

Am i doing something wrong?

You made a silly little mistake. ?

The API is "GetModuleHandleA", where "GetModuleHandle" was just a name to call it by in the original API.

GearCEO™ - November 24, 2011, 5:33 am

brother I love to see the source but I can't decrypt idk why?

n0\$f3ratu\$ - November 24, 2011, 10:07 am

' Wrote:You made a silly little mistake. ?

The API is "GetModuleHandleA", where "GetModuleHandle" was just a name to call it by in the original API.

Now that I've seen this old thread, i feel ashamed... ?