

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Making an effective and undetected crypter!](#)

pr3fix - February 19, 2011, 5:30 pm

Hello everyone,

And welcome to my thread related to topic on how to lower the detection rate and make an effective crypter in Visual Basic (Remember, this is only for .NET, but some of the techniques I used can be also used in other languages as well). So you came to this thread wondering how to FUD or at least UD your crypter against the Anti-Virus scanners, well you came to the right place! This tutorial does not contain and particular/private technique that could be tagged by an Anti-Virus or anything, so mixing it with your imagination you could easily make an effective and UD crypter. So let's begin, shall we ?

STEP 1: (Encrypting Strings)

So let's say that we got our plain non-obfuscated code and it is detected, so let's say that our code looks like this:

[deleted]

As you can see, it's just a plain code, which Anti-Virus vendors could easily tag. So what we're going to do first is encrypt all possible strings. In case you don't know what is a string, a string is, essentially, a sequence of characters, and it looks like this: "Hello, I'm string! Understand?"

Note: Do not encrypt APIs just yet, because if you do you will most likely corrupt the API declaration, which would cause a more trouble, so don't do it just yet.

So to encrypt our strings, we need a encryption algorithm, which is in this case already there (XOR encryption). But in case your encryption's output is not compatible with the Editor's syntax, you can easily just encode the text with any encoding algorithm, I recommend a built-in encoding algorithm, which is Base64 which can be easily accessed within 1 line of a code.

So, this is how it should look after we encrypt our strings:

[deleted]

You may not notice a big differences, that's just because this source code has only few string declarations, but in real stub code it would've more encryptable values, of course this is just an example but you should get the point. So that's how you encrypt your strings, it is really important yet simple step which will past most of the AntiViruses, but this was just beginning don't get too excited just yet.

STEP 2: (Obfuscating Variables)

So in next part of the tutorial, I will be showing you how to obfuscate variables. You may think that this involve a usage of 3rd party application , but you're wrong. This can be done manually too , and it is much more effective than using any 3rd party application since they may corrupt your assembly or add random detections, so it's always better to do it manually since you know what you're dealing with rather than guessing what's that obfuscator doing to your code.

So, obfuscating variables is relatively easy and can be done in 2 simple steps: Select and hit your Ctrl + H

Then just simply write a new name for that variable and replace it with new one

And that's it. And it should look like something like this:
[deleted]

Note: You choose from 3 different character-set types of for your variables's names: ASCII - <http://www.robelle.com/smugbook/ascii.html>

Unicode - http://en.wikipedia.org/wiki/List_of_Unicode_characters

Numbers - (0123456789)

STEP 3: (Encrypting APIs)

For this part of tutorial, I am going to use snippet from AeonHack, but with few modifications. To get a source code of a snippet that allows you to dynamically call APIs just click on the link bellow:

His thread:

<https://hackforums.net/showthread.php?tid=652914>

OR

<http://pastebin.com/LbEDMqjX>

So once you get it, just copy/paste the code to your class/module and make delegates of your APIs, basically taking the signatures of real APIs but just without declaring a library or anything related to API which can be detected by Anti-Virus:

Real API:

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

Delegated API:

```
Code Delegate Function SizeOfResource(ByVal hModule As IntPtr, ByVal hResInfo As IntPtr) As Integer
```

Note: You can use whatever name you want for it, but make sure you remember the real Function Name & Library, in this case it was SizeOfResource as function name and kernel32 as library name (kernel32:SizeOfResource).

Once you do everything as I said, this is how it should look:
[deleted]

Now you can easily encrypt/encode and obfuscate the APIs declarations and calls by using this cool function. Which will past 90% of the detections, in case you have any other detections related to the API it is probably the usage of the APIs so I recommend you to either find different way of using the API or write own function that does whatever you're doing for you, like me in some cases. You can always find a backup APIs, since some APIs have similar or even same features, for example LoadLibrary and GetModuleHandle, they even have same usage and signature / parameters, and they do the same thing, which is retrieving the Memory Address of the libraries.

Anyway, let's back to our topic. Next thing that you can do is encrypt and obfuscate your APIs, and

it should look like something like this:
[deleted]

STEP 4: (Optimizing & Reducing the size)

This is not really required, but it is recommended to modify & optimize your code a bit. For instance, you can edit and randomize the parameters (signatures) of your functions and subs. This won't really affect anything nor it will bypass any detections (or it may will), but it will for sure confuse the Malicious Software Analysts, of course this can be implemented (for instance) in your U.S.G (Unique Stub Generator) so each time you generate new stub code it will scramble and randomize the functions parameters.

[deleted]

Note: You can only change signatures of the your custom made functions, DO NOT change any API parameters otherwise it will corrupt that API declaration.

Also, you can reduce the size of your stub by removing or replacing some code with new one, for instance you can reduce the string's length by renaming it to the one with lower length of characters.

Next this that you can do is to remove unused references and also playing with "Compile" settings.

Remove Unused References: Double click My Project, placed at the right size of Visual Basic by default.

Click on References tab

Click on Unused References to export list and then to remove click on Remove button

[deleted]

The End

Well that's it for today folks, I hope you enjoyed my tutorial and if you did, please rate it with 5*. Also if you have any question related to this subject feel free to PM me or comment on this thread. Good luck! ?

Credits: AeonHack

ThermalSloth - February 19, 2011, 5:33 pm

Looks really good man, thanks for sharing.

Bookmarked it so I can read it while I'm not sleeping :P

Xenon - February 19, 2011, 5:33 pm

Nice tutorial. Very detailed. You should of put this into an eBook and sold it.

GyroErbin0 - February 19, 2011, 5:34 pm

Nice tut pr3fix !!! this can help many many people out !

codepoet - February 19, 2011, 5:35 pm

Very nice and detailed guide. good work.

6e756c6c - February 19, 2011, 5:37 pm

Very nice, it also demonstrates more or less how my engine outputs code so if someone ever needs an example I can point them here! :D

versx - February 19, 2011, 5:37 pm

Great tutorial pr3fix, this is just great.

DarkCore - February 19, 2011, 6:08 pm

wow, Nice job. I have seen loads of threads about re-fuding and this is the only one that isn't half assed!

RiperFish - February 20, 2011, 12:45 am

most detaile tutorial on how to make a crypter FUD, Great man :).5stars :).

TraptCode - February 20, 2011, 12:48 am

Don't forget that with API calls, you can use Alias "APIEntryPointHere", which will allow you to call upon the API with any name.

Taurine - February 20, 2011, 1:05 am

To OP, how long have you been using coding with VB?

pr3fix - February 20, 2011, 2:05 am

(Feb 20, 2011 01:48 AM)TraptCode Wrote: [\[CITE\]](#) Don't forget that with API calls, you can use Alias "APIEntryPointHere", which will allow you to call upon the API with any name.

Yeah I know that, I thought about writing about that too but that won't really do anything, I personally tried it. ?

Krox - February 20, 2011, 2:16 am

thanks a lot, very nice tutorial!! :)

hacphongthan - February 20, 2011, 2:22 am

bookmark it
thanks pr3fix
good tut

kurokitsune - February 20, 2011, 2:32 am

Nice tutorial! Thanks for sharing!

?Impossible - February 20, 2011, 5:10 am

Great tutorial pr3fix.

I'll be sure to implement these methods in my crypter.

lucien28 - February 20, 2011, 5:12 am

thanks man for this tuto :)

Axien - February 20, 2011, 5:13 am

Really nice and detailed tutorial.Thanks for sharing....

? Lollipop ? - February 20, 2011, 5:38 am

You are my personal hero pr3fix <3 I love you!

SkyWalker™ - February 20, 2011, 5:41 am

Thanks, pretty useful tutorial. Will help me for sure and other people =]

HackFox - February 20, 2011, 5:52 am

Waiting to see more crypters in the Sellers section.

My Life - February 20, 2011, 5:55 am

An amazing tutorial pr3fix . Really enjoy reading it :)

I hope not to see new crypter in few days ...

Centrius - February 20, 2011, 5:57 am

Really nice detailed tutorial ! man nice work ! ;)

?Demon - February 20, 2011, 7:18 am

Awesome I must try. (: Thanks man ^.^

pr3fix - February 20, 2011, 10:41 am

Thanks guys for kind comments, glad you liked it. =]

Default Settings - February 20, 2011, 10:45 am

Good tutorial to forward kids to who ask "how do i do a crypter?".

You should combine this tutorial w/ your CodeDOM examples, so the skids can figure out how to get steps 2 & 4 done automatically on each crypt.

None the less, good tut :).

Para - February 20, 2011, 11:05 am

Okay..

What the shit? May you post me completed link of your "Undetected crypter" Because im starter at this shit, So i don't understand :|

pr0t0typ3 - February 20, 2011, 11:11 am

(Feb 20, 2011 12:05 PM)Para Wrote: [\[CITE\]](#) Okay..

What the shit? May you post me completed link of your "Undetected crypter" Because im starter at this shit, So i don't understand :|

There is no crypter you can leech. It is about learning and not using.

Default Settings - February 20, 2011, 11:11 am

(Feb 20, 2011 12:05 PM)Para Wrote: [\[CITE\]](#) Okay..

What the shit? May you post me completed link of your "Undetected crypter" Because im starter at this shit, So i don't understand :|

For the love of god, don't make a crypter as your first project in VB.

GodWall - February 20, 2011, 11:14 am

Very nice work indeed :) gr8 tut

pr3fix - February 20, 2011, 2:02 pm

Thank you guys, once I hope I helped you, even if this is a bit basic.

=]

kas - February 20, 2011, 2:20 pm

Thanks pr3fix!!!! You are very very very very big. it is very interesting. Thanks for sharing

A question, I am trying to use Dynamic api calls, but avira detects.

If i compile only this, [TR/Dropper.Gen]

```
Code Declare Function LoadLibraryA Lib "kernel32" (ByVal name As String) As IntPtr
    Declare Function GetProcAddress Lib "kernel32" (ByVal handle As IntPtr, ByVal name As String)
As IntPtr
    Function CreateAPI(Of T)(ByVal name As String) As T
        'Usage - library:funcName
        'Example - user32:MessageBoxA
        Return
        DirectCast(DirectCast(System.Runtime.InteropServices.Marshal.GetDelegateForFunctionPointer(GetProcAddress(LoadLibraryA(name.Split(":")(0)), name.Split(":")(1)), GetType(T)), Object), T)
    End Function
any idea? Thanks
```

Unreal - February 20, 2011, 2:21 pm

Hey Thanks For This TuT It Was UseFull

teddy76db - February 20, 2011, 3:37 pm

Very good tutorial detailed with pictures , thanks !

pr3fix - February 20, 2011, 3:41 pm

(Feb 20, 2011 03:20 PM)kas Wrote: [CITE](#) Thanks pr3fix!!!! You are very very very very big. it is very interesting. Thanks for sharing

A question, I am trying to use Dynamic api calls, but avira detects.

If i compile only this, [TR/Dropper.Gen]

```
Code Declare Function LoadLibraryA Lib "kernel32" (ByVal name As String) As IntPtr
    Declare Function GetProcAddress Lib "kernel32" (ByVal handle As IntPtr, ByVal name As String)
As IntPtr
    Function CreateAPI(Of T)(ByVal name As String) As T
        'Usage - library:funcName
        'Example - user32:MessageBoxA
        Return
        DirectCast(DirectCast(System.Runtime.InteropServices.Marshal.GetDelegateForFunctionPointer(GetProcAddress(LoadLibraryA(name.Split(":")(0)), name.Split(":")(1)), GetType(T)), Object), T)
    End Function
any idea? Thanks
That one detects the combination of the 2 APIs which are used to locate the memory address of an API.
```

To bypass them you will have (for example) to compile your code as windows application. There are also other methods I use, but they're private & mine. =P

Kotei - February 20, 2011, 4:05 pm

Very well done pr3fix. It looks good.

pr3fix - February 20, 2011, 4:09 pm

Hey Xypher,

Thanks for kind words. Also, I got idea from your thread actually, if it bothers you (the name) I can change it. I'm sorry if I offended you in any way also, and thanks again for posting.

Exit - February 20, 2011, 4:10 pm

This thread should be pinned, no kidding. ?

cyphax - February 20, 2011, 4:11 pm

Great Tutorial, i understand everything. 5 stars for my friend ;)

CyberKore - February 20, 2011, 4:23 pm

well i can only expect the best from prefix, and this tutorial it's the proof, Good job bro

GodWall - February 20, 2011, 4:25 pm

Wow I'm learning allot thanks again Encrypting APIs method took out NOD32 on old crypter I have :)

Zer0Fact0r - February 20, 2011, 4:40 pm

Quote:STEP 4: (Optimizing & Improving your code)

Very poorly named. You're actually making your code shittier for the sake of fooling AV and AV vendors.

pr3fix - February 20, 2011, 4:52 pm

(Feb 20, 2011 05:40 PM)Zer0Fact0r Wrote: [\[CITE\]](#) Very poorly named. You're actually making your code shittier for the sake of fooling AV and AV vendors.

Not really.

It was like 3 AM when I was finishing my tutorial, I was almost asleep so I wrote that part really quick.

I will edit it later, I am working on my Data Organizer improvement, which was requested by my friend.

.bLaZeD - February 20, 2011, 7:53 pm

Very nice tutorial, although I am waaaay to fucking lazy to type all that shit. :D

punish3r - February 20, 2011, 11:45 pm

Thanks man great tuto ?

RiperFish - February 21, 2011, 12:45 am

(Feb 20, 2011 04:41 PM)pr3fix Wrote: [\[CITE\]](#) That one detects the combination of the 2 APIs which are used to locate the memory address of an API.

To bypass them you will have (for example) to compile your code as windows application. There are also other methods I use, but they're private & mine. =P

i have bypassed avira detection by crypting the strings ..

Xflinitrix - February 21, 2011, 12:48 am

Possibly, the best tutorial on lower detection possible.

Risky - February 21, 2011, 1:04 am

this is exactly what i been lookin for thx bro

DEMó??c xO?aTâ - February 21, 2011, 8:54 am

This looks really interesting will read it carefully when I'm not sleepy ;) Gj, Pr3fix.

pr3fix - March 26, 2011, 6:38 pm

Thanks everyone, hope I helped and good luck.

=]

ziocane74 - March 27, 2011, 8:26 am

(Feb 21, 2011 01:45 AM)ThePrinCe Wrote: [\[CITE\]](#) i have bypassed avira detection by crypting the strings ..

What do you mean for "you have to compile as windows application?"

isn't it the default compile mode?

if not,how can I do it?

Avira detect the combination of Loadlibrary and getprocaddress...?

please tell me a way to bypass it...I m getting crazy...

I crypted all the strings,but it didn t bypass it!!!

Stenography - April 7, 2011, 1:13 pm

looks awesome .. What about fud a stub ?

idonotcare - April 7, 2011, 1:15 pm

(Apr 7, 2011 01:13 PM)PolarX Wrote: [\[CITE\]](#) looks awesome .. What about fud a stub ?

Its a CodeDom example, CodeDom crypters dont use stubs to crypt.

pr3fix - April 7, 2011, 1:17 pm

(Apr 7, 2011 01:15 PM)MarcelCoder ? Wrote: [\[CITE\]](#) Its a CodeDom example, CodeDom crypters dont use stubs to crypt.

LOL?

Of Course they use stubs, but they're just different to the normal ones, but more advanced.

:)

idonotcare - April 7, 2011, 1:21 pm

(Apr 7, 2011 01:17 PM)pr3fix Wrote: [\[CITE\]](#) LOL?

Of Course they use stubs, but they're just different to the normal ones, but more advanced.

:)

Well, thats what i meant lol

Xflinitrix - April 7, 2011, 8:00 pm

Decent tutorial nicely written out! Appreciate it! Helped me get my crypter fud ^.^

Oeno - April 7, 2011, 10:06 pm

very nice tutorial. 5* ratted

hacphongthan - April 9, 2011, 2:33 am

Method Encrypt string can't be use on codedom stub

ziocane74 - April 9, 2011, 2:34 pm

(Feb 20, 2011 04:41 PM)pr3fix Wrote: [\[CITE\]](#) That one detects the combination of the 2 APIs which are used to locate the memory address of an API.

To bypass them you will have (for example) to compile your code as windows application. There are also other methods I use, but they're private & mine. =P

What do you mean for " you have to compile your code as windows application"?... When I compile an app, isn't it compiled as windows application?

please explain this...thanks!

rapidguide - May 3, 2011, 9:11 pm

nice tutorial bro

Rated 5 star try to make good tutorials when u have time :)

Mr.TwEaK - May 3, 2011, 11:40 pm

pr3fix you are a great man, I was planing on making a crypter but couldn't find source good enough or detailed enough thank you very much I wish I could rep you man really appreciate your consideration and sharing to HF and its members thnxs (:

Binary Neuronaut - May 4, 2011, 5:08 pm

I'm going to PM you about this.

hotjohncool - May 12, 2011, 11:45 am

Thanks a lot buddy,,,,,
great share.

sas-adi - May 14, 2011, 7:14 am

Pr3fix i'm trying to make a crypter but it gives me errors always, i need the source codes to copy/paste if you want or i need you to encrypt me a istealler server. thx

Kipus - May 18, 2011, 8:53 am

Great Job, works perfectly

alekovo - May 22, 2011, 11:28 am

Thank you for the shared information, hope this thread have a long live :D

RussianFederation - May 22, 2011, 12:07 pm

Nice tutorial mate helps alot :)

Pitifoul - May 23, 2011, 2:31 am

It help me a lot and more specially the API encryptions ;) !

Thanks a lot, you're great :) !

~~((HACKER))~~ - May 23, 2011, 3:55 am

Nice Tutorial Mate....Well Explained...

neyjanbu - June 1, 2011, 2:25 pm

think you very much => it can be help me and anyone person

Fisted - June 6, 2011, 3:01 am

Damn this looks good. If only I had the motivation to read it in depth and try it myself.
Oh well, *bookmarked*, it will come someday.

Pepesi - July 13, 2011, 7:25 am

I really don't get how you encrypt api and strings >_<

eXero - July 13, 2011, 8:42 am

Dang I love this. This is a 5 star thread, and a really high quality user. I love every bit of this thread, and I saved it for future references. Thanks!

Sqlsyringe - July 13, 2011, 9:04 am

Thanks man! Thanks to your tutorial, the finishing touches are on my private crypter, and just hit 100% FUD. Time to spread some love...:p

Ghostenigma - August 14, 2011, 2:13 am

Images are down.Re upload them! It "was" a good tutorial.

~ Gogoli

Hopsin - August 14, 2011, 3:41 am

You should fix the screenshots since, it's broken. Thanks anyway.

Noribus - October 8, 2011, 3:14 pm

yeaaa, please update pictures. If u can itd be a great help . thanks pr3fix!

Gh0st-Zer0 - October 8, 2011, 3:50 pm

Quote:"1 + 8 + 16 + 32 + 256 + 1024 = ME"

You should fix your signature pr3fix you are not a l33t anymore, you are Ub3r!

stylo_asif - October 11, 2011, 9:02 am

wow Very Help Fully TUT Dear Bro Can You Update Your Pictures ... ????

Sm0k3rZz - October 11, 2011, 9:46 am

My english sucks. I only understand every other sentence. I could cry =)

ii_SNiPEzZ_xX - October 11, 2011, 1:40 pm

pictures dont work for me o.O am i the only one with this problem?

pr3fix - October 11, 2011, 3:10 pm

No, it is not only you.

The hosting that I've used to upload pictures for this tutorial is currently down. However, I believe it is still fairly easily understandable.

Melolz - October 14, 2011, 8:14 am

Could you link me to a C# crypter tutorial?
or give me a good reson to use vb and not C#?

algorithm2011 - October 14, 2011, 10:26 am

nice tut, thanks for sharing bro gonna have a go

Daredevil Amit - December 31, 2011, 7:23 am

Pics not working ..account suspended..
message always

saintcracker - December 31, 2011, 12:10 pm

Thanks for the tutorial man, was really worth reading :)

OwNeDI337 - January 1, 2012, 7:31 am

Great TuT but please fix the pics!
Thanks for it !

Systematic - February 20, 2012, 10:20 pm

Can you plz fix the pictures as noted above?

VB.Ex - February 21, 2012, 1:38 am

Good tutorial but please fix pictures problem as soon as

My Gran - February 21, 2012, 1:42 am

Please fix pictures and I will litterally give you bumfun xx

Systematic - February 25, 2012, 12:39 pm

Please fix the images...

Ignore these extra chars.

pr3fix - February 25, 2012, 1:26 pm

I don't have them anymore >_< But I might just re-do the tutorial later . I have much better techniques anyway now.

Systematic - February 25, 2012, 3:22 pm

(Feb 25, 2012 02:26 PM)pr3fix Wrote: [\[CITE\]](#) I don't have them anymore >_< But I might just re-do the tutorial later . I have much better techniques anyway now.

Yes please! That would be great! Could you please pm me when you do it? Thanks.

Fluxify - February 26, 2012, 7:53 am

(Feb 25, 2012 02:26 PM)pr3fix Wrote: [\[CITE\]](#) I don't have them anymore >_< But I might just re-do the tutorial later . I have much better techniques anyway now.

It would be awesome if you re-do it!

Stenography - February 26, 2012, 9:32 am

For those who don't know:

This is not Fully-Undetectable but it's pretty effective and will help you remove most of detections as well.

Thanks again.

HopeSaraiva - February 26, 2012, 11:09 am

Can someone do one topic with new methods ?

??y - March 5, 2012, 2:16 am

Just read over your tutorial, really well written :) sounds interesting, shame the images are down -

looking forward to your next one!

Gee4rce - March 5, 2012, 3:32 am

Thanks, been interested in that - very informative Dude :) !
Greetings, Gee.

Dani Corpse - June 22, 2012, 4:22 pm

I would slap a child or two for you to re-do a tutorial on this.

Wide Awake - June 22, 2012, 5:52 pm

hey i can't see the pictures can you please upload them to imgur?

Gallant - June 24, 2012, 3:01 pm

Seems to be helpful would you please re-upload the pictures :(

pr3fix - June 24, 2012, 3:18 pm

I probably won't be updating the tutorial since I don't really have time. However, the tutorial will (probably) still make sense (to most of you) if you just read it.

stevensavior - July 24, 2012, 10:25 am

Very nice tutorial
Thanks for share your knowledge ;)

BlissEsso - January 16, 2013, 3:50 am

Very nice tutorial mate, but could you re-upload the images, thanks!

iSynthesis - January 16, 2013, 3:53 am

(Jan 16, 2013 04:50 AM)welveforrs Wrote: [\[CITE\]](#) Very nice tutorial mate, but could you re-upload the images, thanks!

Dude, this thread is 2 years old,
You can't possible expect it to be relevant for today.

4RG0S - January 16, 2013, 11:24 am

Amazing Thread :) Thank you for sharing this.

SkyRider2 - January 17, 2013, 5:33 am

Thanks for going in depth, very nice tutorial bro.

Darkster - January 17, 2013, 5:40 am

Hey mate nice tutorial but your pictures are broken.

TraptCode - January 17, 2013, 5:41 am

(Jan 17, 2013 06:40 AM)Darkster Wrote: [\[CITE\]](#) Hey mate nice tutorial but your pictures are broken.
Could be because this thread is almost 2 years old.

INFA?OUS - January 17, 2013, 6:36 am

Great tut, Very detailed thanks for the share

Artisanal - February 2, 2013, 2:59 pm

The damn Pictures are down lol ?