

## Forum:[Hack Forums](#)

Thread: [Vb.Net FUD Builder method VIA server patching / byte replacement \(Source\)](#)

nathan72389 - September 15, 2010, 10:09 am

wow, ok, this was a little tricky to work out, but here we go.

This is another method of passing string from a builder to a server, its FUD, and really should remain FUD because there is nothing for an AV to flag. yeah, no odd API calls, or anything crazy.

so, how is it done?

well, we will simply replace the bytes of our server with some new bytes.  
wait, a few pics might help.

first, lets check the end result.....

[img]http://i53.[censored].com/5488lg.jpg[/img]

^^^ hey! just like any other method right?

ok ok, now, we are not using any EOF / Resources / Codedom stuff for this.

ok, lets look at it in our hex editor....

[img]http://i52.[censored].com/2igf58h.jpg[/img]

^^^ O.o

so basically what we have done is setup a string inside our server, and then replaced it with a new one from the builder by reading the bytes, checking for our "Target" string, when found, simply replace it.

ok, i know its hard to describe, and your probably a little more confused than understanding.

but just so you have a better idea of whats happening, i have included a sample project for you to look and play with.

now, there are some things to remember when doing this. the new and old string MUST be the same length or else you will have to start screwing around with the PE, and thats not the point of this. If you look through the code, I have my "Replacement String" padded with a crapload of spaces at the end, this is setting up some free space inside the server for me to add just about anything i wanted to (with a length restriction). This method (as far as i know) will only work with strings, so it might not be a good idea for you crypter nuts out there.

so, uh, i think thats about it, d/l the source and check it out. im not saying that its 100% error proof, but its just another method to add under your belt.

[MediaFire Download](#)

enjoy, have fun, and leave me a bit of feedback.

**M4xlm** - September 15, 2010, 10:10 am

Wow, gonna check this out. THanks

**pr0t0typ3** - September 15, 2010, 10:12 am

As Always it looks nice but Wydle (Dunno how to write his name) already posted the same idea for vb6 ..anyway it seams nice.... But you need a very long string to store all data for a stealer or smth...

**H3x0S** - September 15, 2010, 10:16 am

Wait, Ubbelol had the same idea.

**DarkSeven46** - September 15, 2010, 10:17 am

Had this in my head a while ago, thanks for this nathan.

**Ironsides** - September 15, 2010, 10:18 am

Same as it was before Patch 16/17

**nathan72389** - September 15, 2010, 10:19 am

(Sep 15, 2010 10:12 AM)pr0t0typ3 Wrote: [\[CITE\]](#) As Always it looks nice but Wydle (Dunno how to write his name) already posted the same idea for vb6 ..anyway it seams nice.... But you need a very long string to store all data for a stealer or smth...

yeah, i know what your refering to, he sent / linked me to the same thing also, but (idk why, bad timing i guess) he always links me to stuff when im about 3/4 plowed and i end up loosing the link.

as for the string length..

well, just think of the logic, if a (for example) gmail username can only have a max of 25 chars, then thats one string that we know the length of, so simply (like i did in the source) pad it with a few extra spaces, and use the trim function.

or...

pile it all into one string, seperate it with a "|" and use a combination of the "Split" and "Trim" functions.

meh, its something else to have under your belt that may come in handy on a rainy day.

(Sep 15, 2010 10:18 AM)Barathrum Wrote: [\[CITE\]](#) Same as it was before Patch 16/17  
lol, well hell if your stuff is already detected that more your problem than it is mine.

**xCocaine** - September 15, 2010, 10:21 am

You're a fucking genius .

**The Weeknd.** - September 15, 2010, 10:21 am

Great idea, I just gave a look at the code.

Pretty easy to understand, thanks :D

**Ironsides** - September 15, 2010, 10:23 am

(Sep 15, 2010 10:18 AM)Barathrum Wrote: [\[CITE\]](#) Same as it was before Patch 16/17  
lol, well hell if your stuff is already detected that more your problem than it is mine.

[/quote]

Oh I thought this was some sort of crypt ?

So this is used to protect a source code (encrypt it)?

**pr0t0typ3** - September 15, 2010, 10:25 am

(Sep 15, 2010 10:23 AM)Barathrum Wrote: [\[CITE\]](#) Oh I thought this was some sort of crypt ?  
So this is used to protect a source code (encrypt it)  
lol you should read the hole thread before posting shit like that.. it will protect nothing .. it is used for storing

**nathan72389** - September 15, 2010, 10:28 am

(Sep 15, 2010 10:25 AM)pr0t0typ3 Wrote: [\[CITE\]](#) lol you should read the hole thread before posting shit like that.. it will protect nothing .. it is used for storing  
HAHA,,... i always enjoy a good laugh.. but really, i told exactly what it was in the 2nd sentence of the thread.

**Ironside** - September 15, 2010, 10:28 am

Yeah I noticed now, I got cunfused because I only read the word FUD and stopped reading afterwards :)  
This is good thing indeed :)

**pr0t0typ3** - September 15, 2010, 10:30 am

(Sep 15, 2010 10:28 AM)nathan72389 Wrote: [\[CITE\]](#) HAHA,,... i always enjoy a good laugh.. but really, i told exactly what it was in the 2nd sentence of the thread.I often enjoy it also but in most cases it is just annoying

**d3c0mpil3r** - September 15, 2010, 10:32 am

Very interesting, I will surely take a look!  
This is limited to strings, may be we need to think harder lol ..

**pr0t0typ3** - September 15, 2010, 10:34 am

(Sep 15, 2010 10:32 AM)decompiler Wrote: [\[CITE\]](#) Very interesting, I will surely take a look!  
This is limited to strings, may be we need to think harder lol ..You can easily store bytes in there as bytes can be converted the chars xD

**Taserz** - September 15, 2010, 12:01 pm

Ive known about this for a while hex editing tut i made for nubz lol. But I didn't think it could be done in vb.net but it's really basic if you think about it. I believe you can have smaller string in a larger string thats preset. Like if in the stub it was STRINGGOESHERE and the string you added was string it should work if you fill in the rest of the string with blanks or make it A0.

**pnKn0wn\_H4CK3r** - September 15, 2010, 12:11 pm

Hi!

As always, awesome...

I'll study the source tomorrow, in France, it's late and... school tomorrow ? .

**Kotei** - September 15, 2010, 1:40 pm

I'll check this out later. Looks promising.

**The-One** - September 15, 2010, 1:46 pm

Dam. I had something smiler to :P I whas still fetching bytes.  
Eh, good job.

**nathan72389** - September 16, 2010, 5:08 am

(Sep 15, 2010 12:01 PM)Taserz Wrote: [\[CITE\]](#) Ive known about this for a while hex editing tut i made

for nubz lol. But I didn't think it could be done in vb.net but it's really basic if you think about it. I believe you can have smaller string in a larger string thats preset. Like if in the stub it was STRINGGOESHERE and the string you added was string it should work if you fill in the rest of the string with blanks or make it A0.  
thats kinda the basic same thing that im doing.

if you know hex, then this will be a cakewalk for you.

**Milopeach** - September 16, 2010, 5:34 am

Wait, so a string in someone's program that they have sold and only added a Label to very it's theirs could be stolen, Am i correct? or am i correct?

Anyway, Nice tut could use Aeon's one along side this. (But i think they are the same)

**unKn0wn\_H4CK3r** - September 19, 2010, 2:25 am

The only problem is: if your constant.length is 11, ex:

Code Const EXAMPLE As String = "REPLACEME "You can't replace that with 20 chars...  
Maximum 11 ? .

**nathan72389** - September 19, 2010, 6:11 am

(Sep 19, 2010 02:25 AM)BabyHack Wrote: [\[CITE\]](#) The only problem is: if your constant.length is 11, ex:

Code Const EXAMPLE As String = "REPLACEME "You can't replace that with 20 chars...  
Maximum 11 ? .

no, its not a problem, if you look at the source (the "ServeR") i have the string padded with alot (20~30) spaces at the end of the string, then just used the trim function when i use the string,

thats just how you have to do it inorder not to screwup the files peheader and crap.

**S?Nk** - September 20, 2010, 12:26 am

Very understandable Nathan, Again another very useful piece of code to learn. Cheers!

**lilwiccseba** - September 20, 2010, 5:23 am

Not useful in this context.

Instead, try using it to let your builder edit all possible strings in your stub every time it patches a file.

Or even better, use this to dynamically recreate your stub's source code, change functions places around, before letting your builder recompile your stub. Let it do this each time you patch a file, and don't think you'll find a more unique stub. Unless you don't use one fixed method, but you store different methods for achieving the same thing in your builder, then let it randomly chose what method it wants to use.

After letting it randomly choose the method to use, let it randomize all strings in it, move functions, etc.

And there you go, a builder that can actually be called "dynamic stub" or "unique stub". Instead of all these noobs on hackforums, running around saying their builder creates "unique stubs", while it actually just pads a few bytes to the end. Ridiculous.

**lilwiccseba** - September 20, 2010, 5:24 am

Sorry, auto-double-post. Server seems to be lagging, so it double-posted.

**Threadlocks** - September 20, 2010, 6:00 am

thanks may be its of some help lol

**WhizKidz** - September 20, 2010, 6:07 am

This is really sick and good :D keep up the good work nathan

**z3pt0seC** - September 20, 2010, 7:27 am

Very nice Nathan.

Good job.

**WhizKidz** - November 16, 2010, 9:24 am

This was really awesome :P

**The 7th Sage** - November 16, 2010, 9:53 am

A friend showed similar example in vb6. But its always great to see an example in .net Well for one you've proved there are more than 2 ways to pass data to server, EOF, Res.

**xCocaine** - December 31, 2010, 8:12 am

Wait, but i can't replace more of a string? :S

**?Recovery™** - March 16, 2013, 6:53 pm

This is cool but how the hell do i use not 1 but 2 textboxes and labels????

**Antagonism** - March 16, 2013, 7:02 pm

(Mar 16, 2013 06:53 PM)?Recovery™ Wrote: [\[CITE\]](#) This is cool but how the hell do i use not 1 but 2 textboxes and labels????

Here we go, somebody has to grave dig the thread.

**k@\$f** - March 17, 2013, 3:20 am

is this method still fud ? if it is i will try it :) :)

thank you :)

**Dark Noodles** - March 17, 2013, 6:55 am

(Mar 16, 2013 06:53 PM)?Recovery™ Wrote: [\[CITE\]](#) This is cool but how the hell do i use not 1 but 2 textboxes and labels????

Are you an idiot? If you knew how to code, then you could easily do what you want with this method.