

Forum:[Hack Forums](#)

Thread: [\[Preview\]\[FUD\] Vault - 95% unique output](#)

Mr. Anderson - December 4, 2011, 5:57 pm

Expect this out soon. The stub is 95% unique. Its not TRUE polymorphism, but its as close as you can get with .NET.

There is also an option to "recompile" the stub on runtime, which reassembles the code itself every-time the stub is run, so it will mutate on every run if the customer wants it to. This is a unique features that no other crypter has(to the best of my knowledge). So basically you will have mutating stub every time you run it. I'm not going to share how I do this, as its a private method I developed. Its been tested on Windows 7/Vista, on 32 bit and 64 bit operating systems, I'm also working on it for XP as well.

If anyone has any feedback or features they want added(that are not already there), then please post them. Your can see the features I have in the screenshots.

Any trolling or bashing of the .NET framework here will be reported, so don't start flaming.

Stub scan:

<http://www.prodef.net/report.php?id=dfs1i2trym22be5txanx92p5xztth7ss>

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

[img]http://www.dropmocks.com/iITLS[/img]

[img]http://www.dropmocks.com/iIKYM[/img]

[img]http://www.dropmocks.com/iIUsD[/img]

[img]http://www.dropmocks.com/iIUsJ[/img]

[img]http://www.dropmocks.com/iILIA[/img]

[img]http://www.dropmocks.com/iITyV[/img]

Orgy - December 4, 2011, 6:12 pm

If it's not "TRUE" polymorphism, why did you call it polymorphic?

Mr. Anderson - December 4, 2011, 6:14 pm

(Dec 4, 2011 07:12 PM)Orgy Wrote: [\[CITE\]](#) If it's not "TRUE" polymorphism, why did you call it polymorphic?

Because its still polymorphic. Its just not 100% polymorphic.

Lucid Walker - December 4, 2011, 6:23 pm

look nice you might have to post screen shot of file comparing

Orgy - December 4, 2011, 6:29 pm

(Dec 4, 2011 07:14 PM)Mr. Anderson Wrote: [\[CITE\]](#) Because its still polymorphic. Its just not 100% polymorphic.

oh okay. i have enough to buy this. not the TRUE amount, though. its not 100% enough.

is that ok?

moveax - December 4, 2011, 9:47 pm

inb4 codedom with string encryption

1st. Looks like copy and paste because the theme is obviously copy and pasted

2nd. Polymorphic kills the sales unless you're using it for market strategies

pr0t0typ3 - December 4, 2011, 9:50 pm

(Dec 4, 2011 07:14 PM)Mr. Anderson Wrote: [\[CITE\]](#) Because its still polymorphic. Its just not 100% polymorphic.Is your girlfriend pregnant ? Yes or No are the only answers you can give to that, exactly like in this situation. There is nothing like 90 % pregnant as well as there is nothing like 90 % polymorphic.

BreastMilk - December 4, 2011, 9:53 pm

In my opinion: Lying about Polymorphic, What else are you lying about?

Diabolic - December 4, 2011, 10:11 pm

Looks pretty decent. Vouch for an old friend when this opens ;).

Username Null - December 4, 2011, 10:24 pm

HF marketplace, where the dreams of coders (or maybe copy-pasters?) go to die.

wondernet - December 4, 2011, 11:34 pm

It says it has that option to 'generate' a new stub at every run, at least he tried to do something new (not to hard to do it with .NET), won't help him to keep it undetected but sounds nice to see that running.

I would like to see and test that kind of crypted binary.

moveax - December 5, 2011, 12:11 am

At form load

```
File = file.replace("%bluh%", GenerateRandomChar)
```

```
GenerateCode(my.resources.source, "new")
```

```
System.Process("new.exe")
```

ToXiiC - December 5, 2011, 12:28 am

Dam man, you are taking a lot of hate.... Oh well, just keep working on it and ignore people.

Probably should just junk this and just say "%95 unique output" nexttime. ?

pr0t0typ3 - December 5, 2011, 4:35 am

(Dec 5, 2011 01:28 AM)ToXiiC Wrote: [\[CITE\]](#) Dam man, you are taking a lot of hate.... Oh well, just keep working on it and ignore people. Probably should just junk this and just say "%95 unique output" nexttime. ?Exactly my suggestion. Keep the fucking Polymorphic Attribute away, as most people do not even know what it means so it will not help you with getting sales and people who know what they are talking about will flame a lot.

? Lollipop ? - December 5, 2011, 5:17 am

For some reason, when I saw the word polymorphic I knew what was going to happen.

Splodge0007 - December 5, 2011, 6:35 am

OP trying to act as if he knows what he's talking about after the fiasco in the protection thread...

95% polymorphic.. you have to be fucking kidding me.

pr3fix - December 5, 2011, 7:50 am

I don't really believe that you've achieved polymorphism. From what I've seen, at least according to your posts that you make in programming / coding section it's quite easy to conclude that you're not quite capable of such thing.

But who knows. However, I wish you good luck with whatever you're trying to do . :)

Overdose - December 5, 2011, 7:54 am

Looking pretty sexy so far.

No Extension spoofer?

Ludakrishna - December 5, 2011, 7:57 am

"Polymorphic .NET Crypter."

"its still polymorphic. Its just not 100% polymorphic. "

van1lle - December 5, 2011, 8:12 am

Okay this not ment as flaming, bashing .NET or trolling.

This is simply a criticism you have to deal with.

(Dec 4, 2011 06:57 PM)Mr. Anderson Wrote: [\[CITE\]](#) The stub is 95% unique. Its not TRUE polymorphism, but its as close as you can get with .NET.Why do you claim it as Polymorphic when it is not?

There is no gray zone between polymorphic or not. Since your decrypter or what else do you have to decrypt the "stub", "runPE" or anything else is not mutatis each time, it is NOT polymorphic. It is only dynamically reencrypted each time. The anti-virus system won't compare the encrypted data. It looks for something like a decrypter.

(Dec 4, 2011 06:57 PM)Mr. Anderson Wrote: [\[CITE\]](#) I'm not going to share how I do this, as its a private method I developed.Such a thing has been released for free in the .NET section and is not hard to create. I will edit this as soon as i can find the link to the thread.

What is good in my eyes:

- The GUI. It doesn't affect the functionality of the crypter though.

~van1lle

Blizzard - December 5, 2011, 8:25 am

This is reactor theme given by someone on the vbsection.

Mr. Anderson - December 5, 2011, 8:29 am

(Dec 4, 2011 10:50 PM)pr0t0typ3 Wrote: [\[CITE\]](#) Is your girlfriend pregnant ? Yes or No are the only answers you can give to that, exactly like in this situation. There is nothing like 90 % pregnant as well as there is nothing like 90 % polymorphic.

You can't apply yes-no concepts to this. Its still 95% polymorphic because most of the code is being moved and replaced, just not all of it. So you can't say its not either. But I'll edit the thread title.

?y??rion - December 5, 2011, 8:34 am

Think about it... TRUE polymorphism isn't even possible in this context because at the end of the day, the byte still has to suspend a legitimate file and inject itself into it, and this isn't possible if it's polymorphic unless you had 100's of FUD RunPE's...

Ludakrishna - December 5, 2011, 8:37 am

(Dec 5, 2011 09:34 AM)lolwtfhax Wrote: [\[CITE\]](#) Think about it... TRUE polymorphism isn't even possible in this context because at the end of the day, the byte still has to suspend a legitimate file and inject itself into it, and this isn't possible if it's polymorphic unless you had 100's of FUD RunPE's...

who even uses runpe's nowadays? its a lame ass method from 2004. ???

?y??rion - December 5, 2011, 8:41 am

(Dec 5, 2011 09:37 AM)Ludakrishna Wrote: [\[CITE\]](#) who even uses runpe's nowadays? its a lame ass method from 2004. ???

Umm, how about every single crypter on HF?

van1lle - December 5, 2011, 8:42 am

(Dec 5, 2011 09:29 AM)Mr. Anderson Wrote: [\[CITE\]](#) You can't apply yes-no concepts to this. Its still 95% polymorphic because most of the code is being moved and replaced, just not all of it. So you can't say its not either. But I'll edit the thread title.

http://en.wikipedia.org/wiki/Computer_virus#Polymorphic_code

Quote:Polymorphic code

[...] In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which remain identical between infections, making it very difficult to detect directly using signatures.

//EDIT:

Also, pr0t0typ3 is correct with is example: 95% pregnant. Either she is or she isn't!

Ludakrishna - December 5, 2011, 8:44 am

(Dec 5, 2011 09:41 AM)lolwtfhax Wrote: [\[CITE\]](#) Umm, how about every single crypter on HF? exactly, just goes to show that nobody on HF is capable of coding an alternate method. they would rather use a lame outdated method that I doubt any of these crypter coders even understand. ?

lo0oI - December 5, 2011, 8:56 am

(Nov 27, 2011 12:24 PM)lo0oI Wrote: [\[CITE\]](#) polymorphism refers to self replicating it has nothing to do with obfuscation,you will get a totally different structure,a new variant,yes some guys obfuscat a code or crypt it and then call it a "full private legit polymorfic system",wish it is not.Adding some junk code or coding a crypting program has nothing to do with coding a self-crypting program.imagine making a machine that will execute one order and only one,and making a machine that can take decisions and execute different orders. It is totally different.this is why we call it polymorphic and not monomorphic

btw,it is very hard to acheive polymophisme using hight level programming languages,your choice is assembly,and if you are too lazy then you can use C with some inline assembly.

you cant do this with VB

.net ,just forget about it

Mr. Anderson - December 5, 2011, 9:02 am

Fine, I got rid of the polymorphic part, I'll just say that each stub is 95% unique. Way to much trouble.

(Dec 5, 2011 09:25 AM)-Blizzard Wrote: [\[CITE\]](#) This is reactor theme given by someone on the vbsection.

Yes, when I start selling all credits will be given.

wacked3 - December 5, 2011, 9:16 am

Thank you.

Now lets start that all over again.

How did you estimate the difference? Did it include anything but your code? If so it is flawed and you shouldn't advertise it that way because essentially you are lying.

Mr. Anderson - December 5, 2011, 9:17 am

(Dec 5, 2011 07:35 AM)Splodge0007 Wrote: [\[CITE\]](#) OP trying to act as if he knows what he's talking about after the fiasco in the protection thread...

95% polymorphic.. you have to be fucking kidding me.

Whats hilarious about it? You obviously don't know what you are talking about. 95% of my code is different, 5% remains the same. Come back when you learn your coding skills.

(Dec 5, 2011 10:16 AM)wacked3 Wrote: [\[CITE\]](#) Thank you.

Now lets start that all over again.

How did you estimate the difference? Did it include anything but your code? If so it is flawed and you shouldn't advertise it that way because essentially you are lying.

I compared the code of two stubs to each other using the ubuntu utility. out of all the lines, only 3 out of the total amount were the same.

lo0ol - December 5, 2011, 9:28 am

(Dec 5, 2011 10:17 AM)Mr. Anderson Wrote: [\[CITE\]](#) 95% of my code is different, 5% remains the same.

I compared the code of two stubs to each other using the ubuntu utility. out of all the lines, only 3 out of the total amount were the same.

anti-virus companys will take the 5% as a signature

.net languages are easy to decompile just like java.

It is Like someone who provide 95% stub updates for his customers

It will be useless

Mr. Anderson - December 5, 2011, 9:32 am

(Dec 5, 2011 10:28 AM)lo0ol Wrote: [\[CITE\]](#) anti-virus companys will take the 5% as a signature .net languages are easy to decompile just like java.

It is Like someone who provide 95% stub updates for his customers

It will be uselessThe 5% is not always the same code, its still randomized. If it gets detected, I will add updated. And remember, the stub re-assembles itself every-time it is run.

van1lle - December 5, 2011, 10:52 am

(Dec 5, 2011 10:02 AM)Mr. Anderson Wrote: [\[CITE\]](#) Fine, I got rid of the polymorphic part, I'll just say that each stub is 95% unique. Way to much trouble.

Thanks Mr. Anderson for being reasonable. Now everything is fine in my eyes. ?

(Dec 5, 2011 10:32 AM)Mr. Anderson Wrote: [\[CITE\]](#) The 5% is not always the same code, its still randomized. If it gets detected, I will add updated. And remember, the stub re-assembles itself every-time it is run.

At least you don't call if polymorphic anymore.

Splodge0007 - December 5, 2011, 11:01 am

(Dec 5, 2011 10:17 AM)Mr. Anderson Wrote: [\[CITE\]](#) Whats hilarious about it? You obviously don't know what you are talking about. 95% of my code is different, 5% remains the same. Come back when you learn your coding skills.

Interesting how you had to change your thread title and remove your "Polymorphism" claims before you chose to confront me about that.

I mean, you've coded a "Polymorphic" crypter and you've only just realized it isn't "Polymorphic". That my young idiot, is the hilarious part.

Unless of course you aren't coding it yourself ? ??

lo0ol - December 5, 2011, 11:53 am

(Dec 5, 2011 10:32 AM)Mr. Anderson Wrote: [\[CITE\]](#) The 5% is not always the same code, its still randomized. (Dec 5, 2011 10:17 AM)Mr. Anderson Wrote: [\[CITE\]](#) 5% remains the same you cant be sure it is not always the same code !

(Dec 5, 2011 10:32 AM)Mr. Anderson Wrote: [\[CITE\]](#) the stub re-assembles itself every-time it is run. If you mean by this the stub will disassembles itself,changes the assembly instructions and reassembles itself,then you have a polymorphic stub witch you dont

If you mean the crypter have a number of totally different stubs,like 30 decrypters that will be generated randomly , then you have an oligomorphic engine,it could be easely realised in any language,so instead of looking for one stub an antivirus software will look for all the stubs.That will make it hard to detect your malware.

If you mean the crypter encrypt the stub randomly using a key or an algorithm to cause different encrypted stubs,then you have a simple obfuscator,and antivirus software will look for the static part in this case the key or the encryption algorithm.

why care about what techniques are used or the "95% new output" ,in a market palce such HF's,people only care about fud,it does not matter how you did that,you can code a simple PE packer and it will do the job,people who care about polymorphic and similar shit are definitely not the people who want to spend 10-100\$ on a crypter.

people here only care about dependencies and countinuous FUD

make that and you will not need to ask for "good luck/look's legit.." suport posts.people love to get what they paid for,

nothing more,nothing less

wyterzzz - April 20, 2012, 3:55 pm

You will never learn that polymorphism != polymorphic. Those who say polymorphism instead of polymorphic have no idea what they are talking about. Polymorphism is technique used in OOP -> e.g. Animal a = new Cat().

//Excuse me for b-u-m-p-ing such an old thread but I didn't see the date...

Mr. Anderson - April 20, 2012, 6:43 pm

This project is closed and not being developed since I sold the source. Don't .