

Forum:[Hack Forums](#)

Thread: [Self-Modifying Assembly](#)

DelusionalGhost - May 13, 2017, 11:33 am

Okay, so.. im working on a obfuscator called .NET Squeezer, im not exactly asking for any source code, because i like to make fresh sources, but does anyone have a concept otr an idea on how to make my program modify its own code at runtime? without saving any exe nor updating the default exe? (making it just change its own values) If you have any ideas, tell me!

Example:

I want to change this:

To this on runtime:

Heres what the obfuscated code looks like:

Itll be on my website: <http://www.delusionalprod.com/projects.html>

NuclearZombie - May 13, 2017, 12:14 pm

you cant modify a running assembly. you can however drop an application that will (when executed) modify the original application.

cawkre - May 13, 2017, 2:13 pm

Depends on what code you want to modify?

In what way would you use this?

stefsot - May 13, 2017, 3:13 pm

you probably mean you want to execute different code at runtime to make the reverse engineering process even harder

you should take a look at jit hooks and code virtualization

0xDEAD10CC - May 13, 2017, 3:58 pm

Those aren't even string's so I have no idea what you're doing or what you think you're trying to do. Obfuscation shouldn't affect the program at runtime like that so you're doing something seriously wrong... If you want to do runtime stuff creating your own VM is the way to go but it's going to degrade your program's performance at runtime which is why it's only used on PARTS of the assembly, not the entire thing.

cawkre - May 14, 2017, 12:46 am

So you want to edit the string decryption method so it decrypts to the correct string right?

Or if you simply want to change every string at runtime to the correct one I advise you not to

w4zt3d - May 14, 2017, 1:30 am

You can use reflection to deobfuscate methods and strings :)

i think you should do that with that information

EDIT: But you also should encrypt the strings before and decrypt them after ^^

EDIT2: Do you use dnlib? just askin'

ubbelol - May 14, 2017, 5:00 am

(May 13, 2017 03:58 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Obfuscation shouldn't affect the program at runtime like that so you're doing something seriously wrong...

Obfuscation may very well affect things at runtime. Not sure what OP means though.

S?pre?e - May 14, 2017, 1:11 pm

(May 14, 2017 05:00 AM)ubbelol Wrote: [\[CITE\]](#) Obfuscation may very well affect things at runtime. Not sure what OP means though.

I'm pretty sure the OP is looking for the keyword "Polymorphic code"

0xDEAD10CC - May 15, 2017, 9:16 am

(May 14, 2017 05:00 AM)ubbelol Wrote: [\[CITE\]](#) Obfuscation may very well affect things at runtime. Not sure what OP means though.

A good obfuscator should avoid drastic changes that would affect anything other than performance, and definitely not in the way OP's screenshots show with the displayed strings being entirely obfuscated, unless those strings are meant to be run through a VM that decrypts them at runtime.

Ninja - May 15, 2017, 9:50 am

(May 14, 2017 05:00 AM)ubbelol Wrote: [\[CITE\]](#) Obfuscation may very well affect things at runtime. Not sure what OP means though.

Keyword was: "should". It can affect things at runtime, but if it wasn't intended then it shouldn't.