

Forum:[Hack Forums](#)

Thread: [\[Preview free release\] DexScator 2 - Native stub protector/obfuscator](#)

hgdfhsdgdgdfh - February 16, 2012, 1:47 pm

Just a preview.

May not work with all programs and have other problems.

What it does:

- Protects 32-bit .NET assembly with native stub coded in C++.
- Strips some stuff from assembly and moves it to native stub to make it harder to restore assembly

You must download ILMerge.exe and put it into same directory with all other files.

AND ALSO: when protecting, drag&drop files from same folder or it will complain about runtimestub dll missing.

Usage: Drag&drop file to protect to dexscator.console.exe.

Please tell your opinion, I'm not 100% sure if I'm going to continue developing this.

And also at the moment protected files can have false positive AV detections.

DOWNLOAD:

<https://lh.rs/Kj71cpB0gAhf>

Silicon - February 16, 2012, 1:52 pm

Any 64-bit support on the way?

Also, does the builder compile the native stub or add resources to it?

Either way, looking good - well, outstanding - from you, as always. Why can't you stop thinking of awesome ideas and give us a chance? D:

ubbelol - February 16, 2012, 1:59 pm

Awesome protection! :D You should definitely continue developing this.

Gh0st-Zer0 - February 16, 2012, 5:31 pm

False/Positives may also come from UPX packaging....

Immortal - February 16, 2012, 7:11 pm

i say stick to it :D false postives from upx looks like.

Zero?? - February 17, 2012, 3:07 am

I'm working on something similar too :)

What method are you using?

I chose to host the CLR separately, I initially thought of using C++/CLI to "bridge" the 2 worlds. ^^

CyNecx - February 17, 2012, 5:37 am

but dumping the assembly is possible or ??

hgdfhsdgdgdfh - February 17, 2012, 5:43 am

Of course its possible, and its pretty easy. But it can be made more difficult and this protector also moves some stuff from assembly to native stub. So atm if you dump the assembly, it doesnt work

without some work.

Zero:

Im using CorBindToRuntimeEx on pure C++ executable with some COM. So no C++/CLI :P

Ingenuity - February 17, 2012, 11:44 am

Categorically yes, keep on developing, this looks really, really nice!

hgdfhsdgdgdfgh - February 17, 2012, 12:03 pm

I just got encrypted methods working. They are decrypted on runtime :P
Next gonna move them from original locations.

Crackme protected with this: <https://hackforums.net/showthread.php?tid=2221170>

[img]http://img72.imageshack.us/img72/1498/tmpf983.png[/img]

But I'm still thinking whether or not release this. Scared of ppl using obfuscator to FUD malware -> AV start detecting as malware.

Immortal - February 17, 2012, 12:26 pm

I would use it for something non malware related, but it's up to you i like it. I like all your releases

hgdfhsdgdgdfgh - February 17, 2012, 3:29 pm

Ok, atm features are (not on downloadable version, its just native stub + string removal):

- Native stub
- Anti debug
- MSIL encryption, decrypt on runtime like on other obfuscators (codeveil)
- Removal of strings and ints from assembly, they are moved to native stub

Features coming/probably coming if I can figure out how to implement:

- Move MSIL bodies to different location = methods on assembly are empty
- Anti-dump
- Less CPU intensive protection
- Move primitive array initializers to native stub like strings & ints, do same also for other primitive types
- Some obfuscation on IL/.NET side like normal obfuscators
- Move resources to native stub
- Better compatibility with different assemblies, atm its a problem

If I decide to release this completely, at least those features will be included. Otherwise you can still use this preview version because it works, just with less features.

And also I have been planning of creating a licensing system based on this: licensing logic is in native loader and C# has verification class which communicates with native stub to exchange license data.

Zero?? - February 17, 2012, 10:18 pm

I haven't got the time to try yet, does it work if you try to run a 64bit .Net assembly within a 32bit native program using the COM interfaces (_AppDomain, _Assembly etc...)?

hgdfhsdgdgdfgh - February 18, 2012, 3:41 am

Havent tried that but I doubt it works. I'm pretty sure you must create a separate 64-bit loader executable for 64-bit assemblies.

li0nsar3c00l - September 3, 2012, 3:23 pm

i hate crashing your threads but all of your links are down. please reup this too

sqlvb2012 - February 6, 2013, 9:32 am

link dead please upload again or post new link

hgdfhsdgdgdfdh - February 9, 2013, 4:39 am

REUPLOAD: <https://lh.rs/Kj71cpB0gAhf>

You still need to download ILMerge and put it in same folder with other files.

Note that I haven't touched the code at all for over an year and the project is in very unstable state (not recommended for production purposes)

xaHyeG - February 9, 2013, 10:38 am

Is the ILMerge large? why you not include it yourself? I get error:

<https://gyazo.com/5660fc2a5e104336ce1e2ad683ac3b1d.png> maby the ILMerge.exe is bussy and your program not waiting for it?

hgdfhsdgdgdfdh - February 10, 2013, 2:31 am

(Feb 9, 2013 11:38 AM)dontExpectMe Wrote: [\[CITE\]](#) Is the ILMerge large? why you not include it yourself? I get error: <https://gyazo.com/5660fc2a5e104336ce1e2ad683ac3b1d.png> maby the ILMerge.exe is bussy and your program not waiting for it?

Did you try to run it many times? It might just be bugged.

The reason I'm not redistributing ILMerge has to do with ILMerge licensing (it's a Microsoft product and it wasn't so clear for me whether or not redistribution is allowed)

Meerkat.? - February 10, 2013, 4:04 am

Damn son :O

I didn't see this project yet, but it's such a nice idea. You mentioned it already, if you're going to release the real deal expect kids to use it in combination with malware, I wouldn't release the full thing to the public.

hgdfhsdgdgdfdh - July 23, 2013, 1:22 pm

(Jul 22, 2013 04:15 PM)pr0sus Wrote: [\[CITE\]](#)

i have this probleme anyone can help me ?

Do you have the file 'DexScatorNative.dll' in the same folder with the obfuscator program itself?

The file is included in the ZIP archive.

Alcatraz3222 - February 14, 2014, 7:56 am

looks awesome, Can you reupload please