

Forum:[Hack Forums](#)

Thread: [CodeDom Source Stealer \ STEAL STUB SOURCE FROM .NET CRYPTERS](#)

gigajew - May 17, 2017, 4:15 pm

Hello, this is a quick and dirty release, but none the less ingenious. It's a program that automatically steals the source (*.cs, *.vb) files of any .NET CodeDom Crypter. I wrote this because it just occurred to me that it can be done so easily, but I didn't see any tools like it.

How to use:

- Start CodeDomSourceStealer.exe
- Open your .NET (codedom) crypter
- Encrypt a dummy file (any file) just to run the process
- Any potential stub source files will be copied to program directory

Screenshots:

Virus scan:

Note: there are some false positives from using ConfuserEx

<https://virustotal.com/en/file/3f377eb70089d7386f6b837b4ddd4bbb41ac438a5c43561746b806b9ea00d4e6/analysis/1495062244/>

Download:

[Click here to download .zip from pomf.cat](#)

gringo - May 17, 2017, 5:03 pm

This is interesting, good job man I'll definitely put this to use haha.

Hopsin - May 18, 2017, 4:44 pm

(May 17, 2017 05:03 PM)gringo Wrote: [\[CITE\]](#) This is interesting, good job man I'll definitely put this to use haha.

Agreed. Quite interested indeed i should say.

@OP, Thank you.

Hypocrattes - May 18, 2017, 5:54 pm

Very interesting and quite neat. As I have developed a recent interest in cryptography, I'll be sure to use this for educational purposes. Thanks for posting, OP!

White Fox - May 18, 2017, 5:56 pm

Thanks for share!

Nice tool!

gigajew - May 18, 2017, 7:59 pm

Just want to add information; it doesn't matter if the crypter is obfuscated or not because codedom writes the source file of the stub to temp directory regardless. It supports C#, VB.NET and it also steals possible exe and dll files. Also it doesn't only work with crypters, but with any .net application

that generates assemblies using codedom. Including but not limited to keyloggers, worms, rats.

Thank you guys

HexCrypt - May 18, 2017, 8:06 pm

Lmao...

"Get in the van, source file. There's candy."

Gt403cyl - May 18, 2017, 8:09 pm

(May 18, 2017 08:06 PM)HexCrypt Wrote: [\[CITE\]](#) Lmao...

"Get in the van, source file. There's candy."

I know right!

I had a huge laugh at that.

gigajew - May 18, 2017, 10:48 pm

New version released, fixed stability and runs on more systems!

Updates:Now steals .PDB

Increased stability (way way way)

Compiled to .NET 2.0 to run on more systems

Removed goofy messages

Uses less resources

Removed obfuscation (just too lazy to do it, and since I'm not selling it anyway)

Decreased size

Screenshots:

Spoiler ([Click to View](#))

Virus scans (2/61):

Not sure where these detections come from, but if you check out the source with dnSpy you can clearly see that there isn't any malicious code

<https://virustotal.com/en/file/cca0a96923553b234a4c6b47cf79e31e4bf1f8e140b957f9de550301143b7abc/analysis/1495172677/>

Download:

<https://a.pomf.cat/dtesmk.zip> click here to download (dtesmk.zip)

Notes:

Any problems with the program (like unforeseen exceptions) let me know on this thread