

Forum:[Hack Forums](#)

Thread: [Americrypt | Crypter foundation built on CodeDOM and TT \(text template\) stub](#)

gigajew - July 29, 2018, 1:06 pm

Here's my easy to understand codedom crypter foundation. Americrypt. Hopefully this can help some people get started with crypters. Note that this does not actually encrypt any executables, it just adds them to resources. So it is up to you to add your own algorithm.

Download: <https://files.catbox.moe/u2iy3o.zip>

int - July 30, 2018, 8:25 am

looks interesting, but looks more unclean than the normal .txt string replace crypters

Electron - July 30, 2018, 2:44 pm

Good job but dnlib would make it look better.

int - July 30, 2018, 2:54 pm

(Jul 30, 2018 02:44 PM)Noxious™ Wrote: [\[CITE\]](#) Good job but dnlib would make it look better. I would like to see an example with dnlib, I have never seen that before

Electron - July 30, 2018, 3:12 pm

(Jul 30, 2018 02:54 PM)Jukeboxhook Wrote: [\[CITE\]](#) I would like to see an example with dnlib, I have never seen that before

Well, I think there are no public examples about it at least when I made it for my crypter, there was no documentation or anything. The most of the properties, methods, opcodes and classes are named like in dnSpy which is the only thing that helps. I would like to see dnlib documentation one day because it's the best existing library. Basically, you make separate projects for your stub and loader then you add resources to them (e.g. payload), randomize Mvid, patch strings (I assume you will have settings like MessageBox) and obfuscate your file. I won't give my code but I can help anyone who needs help for it. If you organize your code you will need like 2-3 methods for adding to resources, patching strings and some basic obfuscation to randomize Mvid, rename strings and maybe some more advanced extras like Control Flow Obfuscation, etc. The only advantage over CodeDOM is that you don't have edit something blindly (without Intellisense) but instead you are working on .cs files like every project.

gigajew - July 30, 2018, 4:03 pm

What's mvid out of curiosity

josh28 - July 31, 2018, 1:11 am

(Jul 30, 2018 02:54 PM)Jukeboxhook Wrote: [\[CITE\]](#) I would like to see an example with dnlib, I have never seen that before

same here, but is it possible to make a usg function.

HFDone - July 31, 2018, 7:24 am

Module Version Id - MVID

The MVID is a Guid used to distinguish between two versions of the same module

```
var asm = Assembly.GetExecutingAssembly();  
var mvid = asm.ManifestModule.ModuleVersionID;
```

Electron - July 31, 2018, 7:30 am

(Jul 30, 2018 04:03 PM)gigajew Wrote: [\[CITE\]](#) What's mvid out of curiosity
Open an executable in dnSpy, right click on the module (purple colored) -> Edit Module, there it is.
If you don't randomize it, ESET will detect your stub easier. Same goes for Assembly Custom
Attributes (not Module). You can clear them too.

Hint:

```
Code _assembly.Modules[0].Mvid = Guid.NewGuid();  
_assembly.CustomAttributes.Clear();
```

josh28 - July 31, 2018, 8:13 am

can someone teach me how to make a runpe.

int - July 31, 2018, 8:31 am

(Jul 31, 2018 08:13 AM)josh28 Wrote: [\[CITE\]](#) can someone teach me how to make a runpe.
how about you look at the 20000 public examples there are?
you have been spamming this section for more than enough time to figure it out

josh28 - July 31, 2018, 9:00 am

(Jul 31, 2018 08:31 AM)Jukeboxhook Wrote: [\[CITE\]](#) how about you look at the 20000 public
examples there are?
you have been spamming this section for more than enough time to figure it out
cant find those public examples, just 1 working

Electron - July 31, 2018, 9:57 am

(Jul 31, 2018 09:00 AM)josh28 Wrote: [\[CITE\]](#) cant find those public examples, just 1 working
Upload one on pastebin and tell me what you don't understand.

3DES - August 3, 2018, 6:55 am

(Jul 31, 2018 08:13 AM)josh28 Wrote: [\[CITE\]](#) can someone teach me how to make a runpe.
Allocate memory in remote process, write/map PE image to the process, relocate pe, set entry point
and resume thread, better option is to use LoadPE instead of RunPE but that is your choice.

josh28 - August 4, 2018, 4:11 am

(Aug 3, 2018 06:55 AM)3DES Wrote: [\[CITE\]](#) Allocate memory in remote process, write/map PE
image to the process, relocate pe, set entry point and resume thread, better option is to use LoadPE
instead of RunPE but that is your choice.
and what does loadpe?

Electron - August 4, 2018, 4:12 am

(Aug 4, 2018 04:11 AM)josh28 Wrote: [\[CITE\]](#) and what does loadpe?
Injecting into the same process.