

Forum:[Hack Forums](#)

Thread: [Cleardrop Crypter | FREE | x86/32-bit | Managed/.NET | Interchangeable Stub+](#)

gigajew - February 1, 2018, 7:46 pm

Cleardrop Crypter, a project I've thrown together from some code I've wanted to experiment with. It's got built-in protection, light obfuscation (renaming), some slight USG and more. I'm not held responsible for how you use this experimental tool. It wasn't built to hack people's computers, it was built to see if it withstands public testing. I'd appreciate if you post in this thread if any errors occur, if you have any problems with anything, etc. By downloading, sharing, copying, using or otherwise modifying this software you agree to not use it for any illegal purposes. This is a software that is capable of generating malware, and it is illegal to use it, or any software produced by it on any devices or property that you do not own.

It does NOT support:EOF

64-bit based applications

Automatic startup (because it's not really meant for spreading or infecting people)

It DOES support:32-bit based assemblies

.NET and native assemblies

Features (if you didn't read above)Light obfuscation

Light anti-virtualization

Anti-emulation

Anti-debugging

Custom cryptography method

Ability to choose a custom stub (in case of updates, or alternative stubs)

It's currently 7/66 as of 02/13/2018, and I'm interested to see how the detection rate develops as more people try it out, submit samples and what not.

Download project: <https://files.catbox.moe/wb9s2b.7z> (password: gigajew)

Scanned stub:

<https://www.virustotal.com/#/file/43dd574dfd2f226fb448f025d475cc06c46d67da5c3b3fd6398540665>

Smile? - February 1, 2018, 7:58 pm

Thanks for the crypter , i will try for sure.

It's .net ?

gigajew - February 1, 2018, 8:04 pm

(Feb 1, 2018 08:58 PM)dåFu™ Wrote: [\[CITE\]](#) Thanks for the crypter , i will try for sure.

It's .net ?

The crypter and stub are .NET Framework version 4.0. I've tested both native and managed executables and they both run. Works well with Quasar actually.

Smile? - February 1, 2018, 8:09 pm

(Feb 1, 2018 09:04 PM)gigajew Wrote: [\[CITE\]](#) The crypter and stub are .NET Framework version 4.0. I've tested both native and managed executables and they both run. Works well with Quasar actually.

Possible to add 2.0 too so i try to bind them ?

Adlies - February 1, 2018, 8:10 pm

Thanks for this free cryptor, I'll give it a test now

gigajew - February 1, 2018, 8:13 pm

Delaying release, wait for more information

Vagabundo Legendario - February 1, 2018, 9:58 pm

I would like to test it thanks

Arkane21 - February 1, 2018, 10:04 pm

Hey I want to test this and scan on virus checkmate.

Thanks,

Arkane21

Takehito Morokuzu - February 2, 2018, 3:00 am

I can test this for you, is it runtime UD? Also if I get this can I spread it or just test for you?

gigajew - February 2, 2018, 2:37 pm

Released again. And to answer your question, it is illegal to spread or execute malware on any devices you do not own, or have consent from the rightful owner of. I'll leave it at that.

As for .NET 2.0 here's a legacy stub that you can use: <https://files.catbox.moe/0ohcet.7z>
(password: gigajew)

Takehito Morokuzu - February 2, 2018, 3:44 pm

(Feb 2, 2018 03:37 PM)gigajew Wrote: [\[CITE\]](#) Released again. And to answer your question, it is illegal to spread or execute malware on any devices you do not own, or have consent from the rightful owner of. I'll leave it at that.

As for .NET 2.0 here's a legacy stub that you can use: <https://files.catbox.moe/0ohcet.7z>
(password: gigajew)

Yes I already knew that. But that's what a crypter is designed for. If it's what some people say "protecting your binary" well that's not true because most crypters include malicious function and they get detected by antiviruses after a while anyway which defeats the purpose because people are going to think it's malware even if it's not.

It's not working, it says The application was unable to start correctly 0xc0000005 on the crypted file

gigajew - February 2, 2018, 4:18 pm

(Feb 2, 2018 04:44 PM)therulerofall Wrote: [\[CITE\]](#) Yes I already knew that. But that's what a crypter is designed for. If it's what some people say "protecting your binary" well that's not true because most crypters include malicious function and they get detected by antiviruses after a while anyway which defeats the purpose because people are going to think it's malware even if it's not.

It's not working, it says The application was unable to start correctly 0xc0000005 on the crypted file That's a bug in the runpe, it happens because you're supposed to have a delay in a runpe at a certain part, but this one is shellcode so I wouldn't know how to add one to it. You'll see the same problem with almost all other runpes. All you can do is just start it again

Takehito Morokuzu - February 2, 2018, 4:25 pm

(Feb 2, 2018 05:18 PM)gigajew Wrote: [\[CITE\]](#) That's a bug in the runpe, it happens because you're supposed to have a delay in a runpe at a certain part, but this one is shellcode so I wouldn't know how to add one to it. You'll see the same problem with almost all other runpes. All you can do is just start it again

Ah it's working now, just didn't work the first time.

gigajew - February 2, 2018, 10:01 pm

If anyone wants to make graphics or UI for it I wouldn't mind adding it

SIM-2294117 - February 2, 2018, 10:16 pm

Love it! Detection ratio of 2/64, very well made for something that's free!

Takehito Morokuzu - February 3, 2018, 3:25 am

(Feb 2, 2018 11:16 PM)alexmicheal49 Wrote: [\[CITE\]](#) Love it! Detection ratio of 2/64, very well made for something that's free!

Don't tell me you scanned it on virustotal...

CyberStrike - February 3, 2018, 3:48 am

Would you be interested in sharing the results of length of time before mass detections, I as well am interested in this.

gigajew - February 3, 2018, 7:29 am

(Feb 3, 2018 04:48 AM)sirru5h Wrote: [\[CITE\]](#) Would you be interested in sharing the results of length of time before mass detections, I as well am interested in this.

Just keep watching and see how long it takes, my custom emulation-evasion should make sure it takes a bit of time

youhassan30 - February 3, 2018, 8:24 am

Thanks for sharing, I'll see about that

gigajew - February 3, 2018, 9:01 am

Updated Crypter and stub in original post (2/3/2018)

+ Added string encoding

- + Added renaming for properties
- + Added constant melting (thanks XenoCodeRCE)
- + Fixed application not closing if closed at license screen
- Removed string encoding from protection (caused the crash)
- Removed some unnecessary strings and calls in protection class

QuasarRAT stub crypted with Cleardrop Crypter, default icon(none), default manifest and version info(cleardrop) (2/3/2018)

NoDistribute: 0/37

VirusTotal: 5/66

cannex - February 4, 2018, 2:13 pm

is it runtime okay? and does crypter have persistence?

gigajew - February 4, 2018, 3:28 pm

(Feb 4, 2018 03:13 PM)cannex Wrote: [\[CITE\]](#) is it runtime okay? and does crypter have persistence? Runtime is okay (I believe). I haven't done any particular testing, other than Windows Defender (which it does bypass). And no, it does not feature any type of persistence. If your executable is killed, it stays that way. No tricks.

The Officer - February 5, 2018, 9:21 am

Like the design simple and easy

gigajew - February 5, 2018, 4:07 pm

Stub still seems to stand strong (0/37) as of 2/5/2018

<https://nodistribute.com/result/dtoQgEplMOCcZb2n01>

AceHardware - February 5, 2018, 5:30 pm

Wow dude thanks for sharing with the community. I bet a lot of people will find this useful. ?

VeinHellsing - February 5, 2018, 6:50 pm

Tested it using a quasargolden edition v1.4.1.0 stub, tested with both the stub.bin and the legacy one, and for some reason when stub is launched it wont connect

gigajew - February 5, 2018, 7:20 pm

(Feb 5, 2018 07:50 PM)VeinHellsing Wrote: [\[CITE\]](#) Tested it using a quasargolden edition v1.4.1.0 stub, tested with both the stub.bin and the legacy one, and for some reason when stub is launched it wont connect

The legacy stub I posted is already outdated, try the regular stub in the OP. Also I don't know what changes were made to Quasar "golden" edition but regular Quasar runs fine.

nyx322 - February 6, 2018, 9:52 am

Thanks for sharing, try this out later

suckx - February 6, 2018, 12:20 pm

If there is a source code, i would not mind looking into it.

xXGangsterXx - February 7, 2018, 3:52 am

Thanks i just Test it Working good 1/38 ? ? ? ?

VeinHellsing - February 8, 2018, 1:54 pm

its still holding up, I ran a few tests using quasar 1.3.0.0, its normal non-cryptd stub connects upon

opening, once crypted using the regular stub it needs to be launched as admin. so far thats what ive gathered. unless im doing something wrong.

gigajew - February 8, 2018, 5:27 pm

(Feb 8, 2018 02:54 PM)VeinHellsing Wrote: [\[CITE\]](#) its still holding up, I ran a few tests using quasar 1.3.0.0, its normal non-crypted stub connects upon opening, once crypted using the regular stub it needs to be launched as admin. so far thats what ive gathered. unless im doing something wrong. It shouldn't need admin privileges but I don't know

VeinHellsing - February 8, 2018, 7:05 pm

i was wondering if it works with NJrat?

gigajew - February 9, 2018, 11:17 am

(Feb 8, 2018 08:05 PM)VeinHellsing Wrote: [\[CITE\]](#) i was wondering if it works with NJrat? I don't know. Try it