

Forum:[Hack Forums](#)

Thread: [Open Source CodeDom Runtime Crypter - UD 2/35](#)

KrypteX - April 15, 2016, 12:09 pm

Hello everyone, I just thought I'd made a rolling release of my project.

I am new to making my own crypters and would love to learn more and continue working on this project and new projects similar to this.

Spoiler ([Click to View](#))

<https://i.gyazo.com/0feb6b9ddee25da4a6be0f0034cb0e81.png>

This project is Currently UD - 2/35

Spoiler ([Click to View](#))

<https://i.gyazo.com/a113b9641d48b82e9923c56c72840c10.png>

I am using very well known methods for Encrypting/Decrypting as well as file writing/dropping/executing the file.

This Crypter is, and will always be, open source for everyone here, feel free to contribute to the project.

Currently the biggest bug with this Crypter is that the output is compiling into the 4.0 Framework, and CodeDom is Specified to compile to v2.0.

Update: The code has been updated and now only depends on the 2.0 Framework for both the Crypter and the Output. ;)

No, I will not be providing ANY kind of bin for anyone so don't ask. If you don't know how to compile it don't use it.

No ShitCash, No Survey, Not even Adfly, No bullshit.

Password is KrypteX for the uppit link.

GitHub Here: <https://github.com/F2C-KrypteX/Scratch-Runtime-Crypter>

Download here: <http://uppit.com/oszpdcdrvax9>

I'm looking forward to, and slightly terrified of feedback.

ShittyAdvice - April 15, 2016, 1:03 pm

You should look into Github.

Github is great for sharing code. Other members can check it out without downloading anything and help you develop your code using pull requests.

If you plan on working as a developer you will most likely be required to use and / or know Github.

OT: Thanks for contributing and good luck with your crypter.

KrypteX - April 15, 2016, 1:46 pm

I've never used Git before but I used to be quite familiar with SVN.

taktaktak - April 15, 2016, 5:08 pm

I second the github motion, its just easier for everyone.

OT: this may be scantime fud, but will be fucked in runtime detection if it's a dropper.

KrypteX - April 15, 2016, 7:46 pm

It is indeed a dropper. It's my first Crypter Project. I'm not sure how I would get the bytes to run without dropping a file other than RunPE, which I'm infamiliar with. I'm also unsure if RunPE can be used with CodeDom, and if I want to actually use codedom for scantime/runtime protection.

GuRuHaX - April 16, 2016, 12:04 am

Nice share thank you verry much !

I want to learn about crypters and everything coming with that and im sure this will help a lot !

?

Cecilia - April 16, 2016, 12:29 am

(Apr 15, 2016 07:46 PM)KrypteX Wrote: [\[CITE\]](#) It is indeed a dropper. It's my first Crypter Project. I'm not sure how I would get the bytes to run without dropping a file other than RunPE, which I'm infamiliar with. I'm also unsure if RunPE can be used with CodeDom, and if I want to actually use codedom for scantime/runtime protection.

RunPE will run in a codedom app, look at some examples.

Most crypters have the runpe/settings in a different dll and build it/reference it when you are making the stub, then invoke it on runtime.

KrypteX - April 16, 2016, 1:52 am

Just finished the last major update on GitHub for the version before going for RunPE testing and such. Hope you enjoy the music XD

I've been testing allot of testing but I can't seem to get a RunPE to actually execute my server..

Slavoj Žižek - April 16, 2016, 6:22 am

adding RunPE is a headache at first but when you set up all the automated

RunPE.dll --> crypt it --> convert it to image (etc) --> then store it (prob as a icon)

its really easy to work on afterwards + it will always be FUD (the RunPE)

KrypteX - April 16, 2016, 11:40 am

(Apr 16, 2016 06:22 AM)Blezzedd Wrote: [\[CITE\]](#) adding RunPE is a headache at first but when you set up all the automated

RunPE.dll --> crypt it --> convert it to image (etc) --> then store it (prob as a icon)

its really easy to work on afterwards + it will always be FUD (the RunPE) scratches my head

You know what, that's not a bad damn idea lol. But that'd require me to.. Hmm... What if I were to include the runPE as a resource within the crypter, that'd randomize all the strings/calls before encrypting/storing it as an image and adding that resource to the codedom output somehow

Slavoj Žižek - April 16, 2016, 11:50 am

(Apr 16, 2016 11:40 AM)KrypteX Wrote: [\[CITE\]](#) *scratches my head*

You know what, that's not a bad damn idea lol. But that'd require me to.. Hmm... What if I were to include the runPE as a resource within the crypter, that'd randomize all the strings/calls before encrypting/storing it as an image and adding that resource to the codedom output somehow there is no point - its going to be stored as a png or something anyway

KrypteX - April 16, 2016, 12:31 pm

True, I've been searching around but I can't seem to find any posts here on doing string/byte() to image. The only one that I've managed to find I'm unsure of how to implement:

```
Code Public Shared Function String2Icon(ByVal input As String) As System.Drawing.Image
    Dim img As System.Drawing.Image
    Dim MS As New MemoryStream
    Dim b64 As String = input.Replace(" ", "+")
    Dim b() As Byte
    b = Convert.FromBase64String(b64)
    MS = New MemoryStream(b)
    img = System.Drawing.Image.FromStream(MS)
    Return img
End Function
```

\$lick - April 16, 2016, 2:25 pm

An open-source crypter, what a great idea, can't see how this could go wrong.

KrypteX - April 16, 2016, 6:15 pm

(Apr 16, 2016 02:25 PM)Nexus™ ?? Wrote: [\[CITE\]](#) An open-source crypter, what a great idea, can't see how this could go wrong.

This is not a tool to be used as a crypter per say to spread, but rather a reference of progress in development, ideas and methods on which this community can learn from.

To my knowledge, I've never seen an open source, complete with using undetection methods and updates as a better example of how everyone can learn how to do this if they are willing to.

I'm not planning on using this to spread. I'm knocking something off of my bucket list which I've long wished to accomplish, and I hope that everyone can participate and learn a bit of something themselves.

Slavoj Žižek - April 18, 2016, 7:45 am

for some reason I could not post here... it said something about i'm trying a sql attack or something I thought I might as well use my "expertise" on this subject and add something to it

here :

<http://pastebin.com/ANZQaFHV>

it uses reflection for .net files and drops the native ones...

its not as good as RunPE but it less hassle

KrypteX - April 18, 2016, 9:23 pm

I know it'd be less hassle than a runpe, but I'd really love to try to get a RunPE in there as an encrypted embedded resource, I'm just having trouble loading and invoking the encrypted DLL.

Slavoj Žižek - April 19, 2016, 10:47 am

(Apr 18, 2016 09:23 PM)KrypteX Wrote: [\[CITE\]](#) I know it'd be less hassle than a runpe, but I'd really

love to try to get a RunPE in there as an encrypted embedded resource, I'm just having trouble loading and invoking the encrypted DLL.

I had a hard time with that so here :

```
Code Dim magicType = Assembly.Load(clearPE).GetType("bobo.iscute") ' getype so project name
then class name (clearpe is your dll byte array)
        magicType.GetMethod("drugs").Invoke(Activator.CreateInstance(magicType), New
Object() {yo parahmeters}) 'getmethod so the runpe function
(this is for non-static functions)
```

?

Cecilia - April 19, 2016, 5:28 pm

(Apr 19, 2016 10:47 AM)Blezzedd Wrote: [\[CITE\]](#) I had a hard time with that so here :

```
Code Dim magicType = Assembly.Load(clearPE).GetType("bobo.iscute") ' getype so project name
then class name (clearpe is your dll byte array)
        magicType.GetMethod("drugs").Invoke(Activator.CreateInstance(magicType), New
Object() {yo parahmeters}) 'getmethod so the runpe function
(this is for non-static functions)
```

?

Not sure why it wouldn't be static though, I mean, you don't need an instance based class for a runpe that'll be accessed only once or twice.

Not sure why it is so hard to invoke a dll from resources though.

KrypteX - April 22, 2016, 10:52 am

(Apr 19, 2016 10:47 AM)Blezzedd Wrote: [\[CITE\]](#) I had a hard time with that so here :

```
Code Dim magicType = Assembly.Load(clearPE).GetType("bobo.iscute") ' getype so project name
then class name (clearpe is your dll byte array)
        magicType.GetMethod("drugs").Invoke(Activator.CreateInstance(magicType), New
Object() {yo parahmeters}) 'getmethod so the runpe function
(this is for non-static functions)
```

?

Well I made a little test project to see if I could do it right off the bat and I seem to be getting somewhere with at least loading an unencrypted DLL on Click with this

```
Code Imports System.Reflection
Public Class Form1
    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        Dim mydll = Load_Encrypted_DLL_Testing.My.Resources.test
        Dim doet = Assembly.Load(mydll).GetType("test.test")
        Dim key As String = "ThisKey"
        Dim out As String = doet.GetMethod("EncryptText").Invoke(Activator.CreateInstance(doet),
New Object() {TextBox1.Text, key})
        TextBox1.Text = out
    End Sub
End Class
Pretty damn simple, and does me a good in the learnings :)
```

Ghostenigma - April 22, 2016, 12:40 pm

(Apr 16, 2016 12:31 PM)KrypteX Wrote: [\[CITE\]](#) True, I've been searching around but I can't seem to find any posts here on doing string/byte() to image. The only one that I've managed to find I'm unsure of how to implement:

```
Code Public Shared Function String2Icon(ByVal input As String) As System.Drawing.Image
    Dim img As System.Drawing.Image
    Dim MS As New MemoryStream
    Dim b64 As String = input.Replace(" ", "+")
    Dim b() As Byte
    b = Convert.FromBase64String(b64)
    MS = New MemoryStream(b)
    img = System.Drawing.Image.FromStream(MS)
    Return img
```

End Function Maybe here on my thread :P

<https://hackforums.net/showthread.php?tid=4738210>

VisualSoft - April 23, 2016, 6:59 am

Thanks for releasing this.

Will help me in Coding my own crypter.

KrypteX - April 24, 2016, 9:57 am

No problem :) just remember to leave credits where they're due

KrypteX - April 29, 2016, 11:05 pm

big update to the source code on GitHub with stronger USG and Encryption keys + more stable.

Decay88 - May 11, 2016, 1:04 am

Thanks! Appreciate it!

Any chance of adding compressor?

Lexus™ - May 11, 2016, 2:09 am

thanks for sharing this source

no matter it is detected becuz this will help some people out!

kind regards

KrypteX - May 11, 2016, 3:52 pm

I'm actually working on a new release that won't be open source, but it will be including multiple encryption methods, startup options and better assembly cloning.

Right now it's just a skeleton:

Let me know what features you'd like to see in it and I'll give it a shot!