

Forum:[Hack Forums](#)

Thread: [\[VB.net\] RunPE\(FUD runtime stub for crypters\)](#)

JapaBrz - October 8, 2009, 6:31 am

I think Deathrader posted something like this a while, but wasn't RunPE and wasn't runtime like this one. It was used on my crypter 2.0 but since the project is closed, here is it. Credits to me[deleted].

and BTW works with ANY unbinded executable, .net or not. But the stub requires .net after.

<http://pastebin.com/f63673e6c>

x3me - October 8, 2009, 9:19 am

I keep getting these 2 errors:

Warning 1- Variable 'pidh' is used before it has been assigned a value. A null reference exception could result at runtime. Make sure the structure or all the reference members are initialized before use

Warning 2 Variable 'Pinh' is used before it has been assigned a value. A null reference exception could result at runtime. Make sure the structure or all the reference members are initialized before use

Can you help me?

JapaBrz - October 8, 2009, 10:20 am

They aren't errors, are warnings. You can still use compile it with warnings.

CindyAngel - October 8, 2009, 10:45 am

(Oct 8, 2009 06:31 AM)JapaBrz Wrote: [\[CITE\]](#) I think Deathrader posted something like this a while, but wasn't RunPE and wasn't runtime like this one. It was used on my crypter 2.0 but since the project is closed, here is it. Credits to me and + rep if you liked it.

and BTW works with ANY unbinded executable, .net or not. But the stub requires .net after.

<http://pastebin.com/f63673e6c>

Hi JapaBrz,

Can you explain me in detail what and how to do?

Please.

Thanks.

JapaBrz - October 8, 2009, 12:57 pm

It's a crypter stub code, use it to make a crypter, if you know.

It's FUD and as I said, works with all executables that can be ran by RunPE.

Deathader - October 9, 2009, 3:53 am

I'll check this out when I get home ;)

It uses reflection, correct? Edit: Holy shit. nice work. Is this tested? :D

JapaBrz - October 9, 2009, 6:54 am

Tested and working with any executable that can be ran in RunPE

Don't use any kind of Reflection, It's all on PE reading and parsing the sections to the memory. I changed only a few steps:

[based on RunPE]

- Remove MoveMemory(don't work with .net)

- Added alot of Math to fix array segments

- added some matrix math calculation for the garbageCollection

Soul Collector - October 9, 2009, 11:29 am

So you giving free FUD RUNTIME source ??? WTF

BlueMelon - October 9, 2009, 11:56 am

(Oct 9, 2009 11:29 AM)Soul Collector Wrote: [\[CITE\]](#) So you giving free FUD RUNTIME source ??? WTF

You need to know how to use the source id Imagine. Im not at that level yet, I can only make a scan time. So Ill stay away from this for awhile :P

Soul Collector - October 9, 2009, 12:03 pm

Yea me too .. :D But okay thnx gonna study this source ..

[B]iishop - October 9, 2009, 2:38 pm

I dont get how to use it. Do we create a button or what?Put it on our crypter source? Im a little new to the whole crypting stuff. Im a beginner coder. Sorry =s

Ph?us - October 9, 2009, 3:13 pm

If you are a beginner I recommend you stay away from this. @Japabrz Nice work, I'll modify this for my own needs.

Vorfin - October 9, 2009, 3:30 pm

Already seen on LC, and as I said, WOW! This is the first time I have ever seen this done.

Ph?us - October 9, 2009, 3:31 pm

(Oct 9, 2009 03:30 PM)Vorfin Wrote: [\[CITE\]](#) Already seen on LC, and as I said, WOW! This is the first time I have ever seen this done.

I've seen a couple that work in C# but they are not compatable with .NET

Vorfin - October 9, 2009, 3:34 pm

Yeah, before this I was under the impression that runtime had not yet been done, at least not publicly. Some guys on Hack.Hound claimed they had done it using a mix of converted VB6 and C# code. However I don't think they ever provided any solid proof.

JapaBrz - October 9, 2009, 3:40 pm

I also heard that the guys on HH made it. I believe they did, but no1 has showed a fully working source yet, until this one.

This is too old, I made a year ago(remember my crypter?) and since I closed the project, I'm releasing some sources

Vorfin - October 9, 2009, 3:42 pm

Well you released the first working source, so you have more or less made history lol

Ph?us - October 9, 2009, 3:51 pm

Thanks Japabrz, I converted an old VB6 source to C# but it was not compatable with .NET and now I can add the math to make it work for .NET =)

JapaBrz - October 9, 2009, 6:44 pm

don't forget the creds. -_-

[B]iishop - October 9, 2009, 7:00 pm

Oh ok. lol, well thankyou anyway. I will stick to bots and stuff.lol

MC' - October 9, 2009, 7:31 pm

(Oct 9, 2009 03:40 PM)JapaBrz Wrote: [\[CITE\]](#) I also heard that the guys on HH made it. I believe they did, but no1 has showed a fully working source yet, until this one.

This is too old, I made a year ago(remember my crypter?) and since I closed the project, I'm releasing some sources

Thats pretty funny that people have been saying its 'impossible' and you had it working a year ago

I haven't programmed for a month, but I might try putting this in my binder instead of dropping.

Thanks for the contribution

JapaBrz - October 9, 2009, 8:11 pm

Yeah, true.

Anyway, forgot to say that the source code is the full RunPE module. There is verification code on the first "IF" clauses, wich you don't need to put on the stub, only on the builder. Also of course, you don't need a form.

My stub got around 10kb with assembly resizing and with no obfuscation. With obfuscation can take up to 17kb, still is a good size for .net file.

For the encryption I suggest a simple xor, simplest as possible to not increase the exe size.

Now I'm working on my obfuscator. The project isn't something expected for only one person but I like challenges.

hurmony - October 9, 2009, 9:54 pm

Interesting share.

JapaBrz - October 10, 2009, 8:13 pm

(Oct 9, 2009 03:42 PM)Vorfin Wrote: [\[CITE\]](#) Well you released the first working source, so you have more or less made history lol

Well yea, I'm in history ? .

I hope that someone in a near future writes a wiki page about me.

newbie223 - October 15, 2009, 12:01 pm

(Oct 10, 2009 08:13 PM)JapaBrz Wrote: [\[CITE\]](#) Well yea, I'm in history ? .

I hope that someone in a near future writes a wiki page about me.lol wtf?? u expect an entire wiki page for u? ??

Sikandar - October 15, 2009, 12:14 pm
cant seem to figure it out

SRexec(b)as byte, bla as string)

JapaBrz - October 15, 2009, 12:23 pm
(Oct 15, 2009 12:01 PM)newbie223 Wrote: [\[CITE\]](#) lol wtf?? u expect an entire wiki page for u? ??
You know what is a joke?

newbie223 - October 15, 2009, 8:07 pm
i noe im laughing at ur joke

ubbelol - October 15, 2009, 10:50 pm
w00t w00t!

Damn Japa! Works 100% fucking perfect :D Thanks!

ubbelol - October 22, 2009, 12:09 pm
How would i start a process with this (from my resources) with startup parameters? Like in a command line program..

cd C:\program.exe -p -a -r -a

? :]

Icy Wind - October 22, 2009, 1:10 pm
Wow, just wow. This seems awesome, too bad i dont quite understand it. Oh well, i better start learning more.

Xinapse - November 10, 2009, 12:14 pm
can anyone show me how this works? whenever i use this it doesnt run the original exe

Soul Collector - November 10, 2009, 12:28 pm
You just copy/past in stub thats all. If you want to work fully you should mod it, adding to be compleable with builder and to add to selected .exe

-C0d3ak-- - November 11, 2009, 6:09 pm
(Nov 10, 2009 01:28 PM)Soul Collector Wrote: [\[CITE\]](#) You just copy/past in stub thats all. If you want to work fully you should mod it, adding to be compleable with builder and to add to selected .exe
Copying and pasting it into your stub source can't possibly make your stub runtime..

I would really like a tutorial on runtime, scantime is just too easy =\

newbie223 - November 12, 2009, 1:01 am
hey any1 mid explaining how do we use this i dun like copy paste i wanna learn :)

D3viL - November 12, 2009, 5:51 pm
How To Call The RunPe Classes ?Cant Get It To Work
dim aj as new DD

aj(Blala)?

AzCrackZ - November 13, 2009, 5:32 pm

Try

Code Dim DD as new DD

DD.SRexec(byte_Array, Victim_Proc)

JapaBrz - November 13, 2009, 5:41 pm

yeah and remember that you can pack both array(GzipLib) and the final stub(NETz), you can get a even smaller executable size.

AzCrackZ - November 13, 2009, 6:01 pm

I keep getting "unknown executable image" got any ideas?

Bob1337 - November 15, 2009, 2:21 am

Hmmmm is this working for windows xp?

I tested it on vista and it worked but some other people said to me that there is a security error on XP.

AzCrackZ - November 15, 2009, 8:20 am

I cant get it to inject the exe on XP. I tested in sandboxie and after it launches the original exe, it said "unknown executable image" for the process name. No actual error window pops up.

dilsin - November 16, 2009, 8:06 am

i just make it work in vb 6 on my crypter i dunno if its FUD

slow net here

and i'll try your RUN PE

:D

for my dot net crypter

AzCrackZ - November 18, 2009, 12:28 am

Has anyone made any progress implementing this?

sunnyyu - November 18, 2009, 2:06 am

Thanks. The code works great on winxp 32, vista 32, win7 32 on my test but not working in Windows vista and 7 64 bit (UAC disabled and ran as administrator). When I run it, nothing happens, no errors etc.

Is there a way to make it to work on 64 bit windows? thanks

(Oct 8, 2009 06:31 AM)JapaBrz Wrote: [\[CITE\]](#) I think Deathrader posted something like this a while, but wasn't RunPE and wasn't runtime like this one. It was used on my crypter 2.0 but since the project is closed, here is it. Credits to me and + rep if you liked it.

and BTW works with ANY unbinded executable, .net or not. But the stub requires .net after.

<http://pastebin.com/f63673e6c>

dilsin - November 18, 2009, 7:58 am

woah, i'll try it when i have the time

i hope it works :D it going to be usefull

Btw how do i convert the string data to byte() ?

in vb 6 its like strConv(data,vbFromUnicode)
Anyone knows?

sunnyyu - November 18, 2009, 10:31 am

```
Public Function GetBytesFromFile(ByVal FileName As String) As Byte()  
    Dim fs As FileStream = New FileStream(FileName, FileMode.Open)  
    Dim reader As BinaryReader = New BinaryReader(fs)  
    Dim Data As Byte() = reader.ReadBytes(DirectCast(fs.Length, Long))  
    reader.Close()  
    fs.Close()  
    Return Data  
End Function
```

(Nov 18, 2009 08:58 AM)dilsin Wrote: [\[CITE\]](#) woah, i'll try it when i have the time
i hope it works :D it going to be usefull
Btw how do i convert the string data to byte() ?
in vb 6 its like strConv(data,vbFromUnicode)
Anyone knows?

\$weet - November 20, 2009, 10:35 pm

hey i could use some help, im getting errors up the ass here

[Eprouvez] - November 21, 2009, 2:37 am

(Nov 20, 2009 11:35 PM)Coders Central Wrote: [\[CITE\]](#) hey i could use some help, im getting errors
up the ass here
What errors? And how did you paste the code into your form?

Theref - November 21, 2009, 3:16 am

Thanks for the runtime stub, still learning in it

??? Matto ??? - November 23, 2009, 2:14 pm

Is it possible to pass parameters to the program you are injecting

AzCrackZ - November 30, 2009, 11:04 pm

Can anyone help me with this? I'm still getting application errors and dumprep????

Neroxan - November 30, 2009, 11:19 pm

Id be willing to bet vorfins will be done in a week, maybe two @ tops. LOL.
Perhaps he should send it to nathan and have a contest to see who can get it working first;)

nathan72389 - December 1, 2009, 7:20 am

(Dec 1, 2009 12:19 AM)Imwyldechylde Wrote: [\[CITE\]](#) Id be willing to bet vorfins will be done in a
week, maybe two @ tops. LOL.
Perhaps he should send it to nathan and have a contest to see who can get it working first;)
this is so simple its stupid, you guys cant figure it out cuz you dont know what your doing. i have
had this working 10mins after he posted this.

but just to let you know, this is very to extreamly buggy on anything higher than win xp.

Vorfin - December 1, 2009, 10:30 am

(Dec 1, 2009 12:19 AM)Imwyldechylde Wrote: [\[CITE\]](#) Id be willing to bet vorfins will be done in a
week, maybe two @ tops. LOL.
Perhaps he should send it to nathan and have a contest to see who can get it working first;)

Not to mention Nathan is a million times the coder I am.

newbie223 - December 1, 2009, 10:39 pm

nathan will win in a landslide hey is there a place where we can learn to write own PE?
I WANNA LEARN BASIC'S

SANK - December 20, 2009, 7:54 am

(Dec 1, 2009 11:39 PM)newbie223 Wrote: [\[CITE\]](#) nathan will win in a landslide hey is there a place where we can learn to write own PE?
I WANNA LEARN BASIC'S
Lol good luck.

Might take you few hours (that is when you know what your doing).

codepoet - March 16, 2010, 4:04 pm

thank you....(*_*)....