Forum:Hack Forums

Thread: Crypting DarkComet with a .net Crypter?

iRtehLeet™ - *March 30, 2013, 2:25 pm*
Does this require EOF preservation or what dude?

0xBB - *March 30, 2013, 2:55 pm*
I dont see any eof in dc stubs. And you can't load unmanaged bytes in domain.

Sc?rƒ?c3_ - *March 30, 2013, 4:03 pm*
No problem with darkcomet, i know cybergate needs eof presevation. You can use a RunPE and load the bytes....no problem with that.

Sc?rƒ?c3_ - *March 30, 2013, 4:36 pm*
No. You'll need a RunPE for unmanaged .exe, and Reflection for managed.

The-One - *March 30, 2013, 5:21 pm*
(Mar 30, 2013 04:20 PM)?Mephobia Wrote: *[CITE]* You can use .net reflection to load an unmanged exe. And both DC and CG are both unmanaged.
Lol no, managed means that it relies on a code which is already written such as .NET. Unmanaged doesn't have all those prewritten codes. So .NET reflection only works for managed code, but compiled with .NET.

salmoneus - *March 30, 2013, 6:56 pm*
You are selling a crypter. You should know this.

?Mephobia - *March 30, 2013, 7:20 pm*
I meant to say .net reflection is used with managed code. I was on my phone and didn't proofread. That's why I said DC and CG were both unmanaged.

n0$f3ratu$ - *March 30, 2013, 8:23 pm*
The answer is simple.
NO, it doesn't need EOF!!!, but either way you will crypt the server, with or without upx, it will work.
At least in my case it doesn't break it.

(Mar 30, 2013 04:36 PM)Scarfac3_ Wrote: *[CITE]* No. You'll need a RunPE for unmanaged .exe, and Reflection for managed.
Not really.
I am using runpe for both.
The only difference is when crypting .Net files i inject in it self.

0xBB - *March 30, 2013, 8:51 pm*
(Mar 30, 2013 08:23 PM)n0$f3ratu$ Wrote: *[CITE]* The answer is simple.
NO, it doesn't need EOF!!!, but either way you will crypt the server, with or without upx, it will work.
At least in my case it doesn't break it.

Not really.
I am using runpe for both.

The only difference is when crypting .Net files i inject in it self.
So what you're saying here is you currently inject managed code ? I mean for managed , don't you use a domain ? ?

n0$f3ratu$ - *March 30, 2013, 11:06 pm*
(Mar 30, 2013 08:51 PM)ibennz Wrote: [CITE] So what you're saying here is you currently inject managed code ? I mean for managed , don't you use a domain ? ?
Exactly.
I never did and as far as i am concern never will.

0xBB - *March 30, 2013, 11:37 pm*
(Mar 30, 2013 11:06 PM)n0$f3ratu$ Wrote: [CITE] Exactly.
I never did and as far as i am concern never will.
Intersting, I guess you inject into a managed process. If you don't mind, which .exe is by default in .NET that is coded in managed ? Or you drop something ?

Edit :

Nvm I found something ? ; http://msdn.microsoft.com/en-us/library/99sz37yh.aspx

Sc?rƒ?c3_ - *March 31, 2013, 2:23 am*
(Mar 30, 2013 08:23 PM)n0$f3ratu$ Wrote: [CITE] The answer is simple.
NO, it doesn't need EOF!!!, but either way you will crypt the server, with or without upx, it will work.
At least in my case it doesn't break it.

Not really.
I am using runpe for both.
The only difference is when crypting .Net files i inject in it self.
You are Correct! I actually have too a RunPE that runs managed too. But as you said inject in itself ?

iRtehLeet™ - *March 31, 2013, 1:18 pm*
I know you need two different ways to inject managed/native, but my current Native RunPE doesn't seem to run DC servers properly with no settings on the DC server.

0xBB - *April 1, 2013, 5:34 am*
(Mar 31, 2013 02:23 AM)Scarfac3_ Wrote: [CITE] You are Correct! I actually have too a RunPE that runs managed too. But as you said inject in itself ?
Yeh, and how you guys handle eof ? Copying any eof to the crypted file would trigger avira. ?

Sc?rƒ?c3_ - *April 1, 2013, 1:12 pm*
yes, if we talk about well known rat's....only cybergate needs to keep the EOF, anyway, i have my personal rat project that uses EOF only for settings (i'm currently using appendalltext) and it's clean, since the data is really really small. So...if the EOF of cybergate is not so large in size, probably would not be a problem to copy it and append to the stub, but never used cybergate. I can only say for sure that an irrilevant size of data, would probably not be a problem with avira. But for storing the entire file in your stub you can't use EOF obviously, actually i'm using cecil to add it as emebedded resource.

0xBB - *April 1, 2013, 3:28 pm*
(Apr 1, 2013 01:12 PM)Scarfac3_ Wrote: [CITE] yes, if we talk about well known rat's....only cybergate needs to keep the EOF, anyway, i have my personal rat project that uses EOF only for

settings (i'm currently using appendalltext) and it's clean, since the data is really really small. So...if the EOF of cybergate is not so large in size, probably would not be a problem to copy it and append to the stub, but never used cybergate. I can only say for sure that an irrilevant size of data, would probably not be a problem with avira. But for storing the entire file in your stub you can't use EOF obviously, actually i'm using cecil to add it as emebedded resource.
You don't understand, Most of managed stuff use EOF. And no matters what you put here , its detected as dropper (the lenght or the way you do it doesn't really matters). I'm kinda lost on that one, I'll have to dig . Was thinking to use a CRL process to inject to and pause the execution, close the other processs, and write eof to it on runtime.. I guess the path would be the same since its injected from it. ? ..

Sc?rƒ?c3_ - *April 1, 2013, 3:42 pm*
(Apr 1, 2013 03:28 PM)ibennz Wrote: *[CITE]* You don't understand, Most of managed stuff use EOF. And no matters what you put here , its detected as dropper (the lenght or the way you do it doesn't really matters). I'm kinda lost on that one, I'll have to dig . Was thinking to use a CRL process to inject to and pause the execution, close the other processs, and write eof to it on runtime.. I guess the path would be the same since its injected from it. ? ..
http://elementscanner.com//?RE=96d1700454460a4ae6be58803e22e059
Rat server with EOF to store an XOR encrypted and splitted string (settings of the server, port, installa path, process name...and so on...) So... is not really always as you say..most times is detected in combination with other stuffs. What file are you tryng to FUD ? It's a known rat?

iRtehLeet™ - *April 1, 2013, 3:44 pm*
NyC.xXBRONX.NyC Wrote: *[CITE]* (Yesterday 04:18 PM)iRtehLeet™ Wrote: I know you need two different ways to inject managed/native, but my current Native RunPE doesn't seem to run DC servers properly with no settings on the DC server.

Because the runpe is not the issue with DC its the way you read and preserve the bytes is wrong. If your using io.readallbytes for dc it will corrupt dc servers. Pm if you need help im in class n on cell.
I have PM'ed you, I guess this is the answer because I am using this method.

0xBB - *April 1, 2013, 3:48 pm*
(Apr 1, 2013 03:42 PM)Scarfac3_ Wrote: *[CITE]*
http://elementscanner.com//?RE=96d1700454460a4ae6be58803e22e059
Rat server with EOF to store an XOR encrypted and splitted string (settings of the server, port, installa path, process name...and so on...) So... is not really always as you say..most times is detected in combination with other stuffs. What file are you tryng to FUD ? It's a known rat?
Its nothing in particular. I just use a clean PE with eof i write in (it's quite short) and on the form run I display it on a messagebox. So it need the eof to be written to the crypted output. (like some rats like clientmesh or CG)

Sc?rƒ?c3_ - *April 1, 2013, 4:00 pm*
(Apr 1, 2013 03:48 PM)ibennz Wrote: *[CITE]* Its nothing in particular. I just use a clean PE with eof i write in (it's quite short) and on the form run I display it on a messagebox. So it need the eof to be written to the crypted output. (like some rats like clientmesh or CG)
Try to add some embedded resources like some legit .dll like DirectShowLib, SharpDX.Direct3D9.dll....increasing the filesize, see what happens... my server has tons of codelines, all from scratch, and some .dlls i use for remote desktop and cam (i'm using directx) all this... seems to let Avira seeing my file legit. If you have 3 lines of code + EOF, most probably it become more suspicious. Anyway, it is possible to not be detected as dropper as i showed. I've to be honest, still cant say you why....but the more complex seems to be the source the better is the scan result

have you tryed to append something to a non encrypted file?

iRtehLeet™ - *April 4, 2013, 11:19 am*
I still have no idea to crypt DarkComet with a .net crypter unfortunately.

0xBB - *April 4, 2013, 8:29 pm*
Tend to agree , Most public runpe work with Darkcomet. Also depend where you inject, some are really unstable and doesn't work on all processes. Could take a look here ;
https://hackforums.net/showthread.php?tid=3378694

Might get some ideas ?

iRtehLeet™ - *April 5, 2013, 3:21 am*
My RunPE is running all other native files fine, unfortunately not a DarkComet server.

For those who flamed me, it's okay I understand where you are coming from.

For those that helped or tried, thank you. My RunPE is not public, was coded by Aeonhack. (not the public reflection.. that is not for native files. Please stop trying to flame me lol)

Thanks,.

ibennz Wrote: *[CITE]* Tend to agree , Most public runpe work with Darkcomet. Also depend where you inject, some are really unstable and doesn't work on all processes. Could take a look here ;
https://hackforums.net/showthread.php?tid=3378694

Might get some ideas
Thanks!

Had enough of this, going to download DC myself and test it.

I see many posts like this saying "DC doesn't work with .net crypters" -
https://hackforums.net/showthread.php?tid=2152629&pid=19492259#pid19492259