Forum:Hack Forums

Thread: read string value and replace it inside EXE file

SIM-2564555 - *September 2, 2015, 7:42 am*
Hey mates , i search for away that let me to search specific string in EXE file and replace its value to another value

all that with .net c# or vb.net

BahNahNah - *September 2, 2015, 7:46 am*
Is the exe you are trying to edit .net? You could use Mono.Cecil.

SIM-2564555 - *September 2, 2015, 8:14 am*
(Sep 2, 2015 07:46 AM)BahNahNah Wrote: *[CITE]* Is the exe you are trying to edit .net? You could use Mono.Cecil.
yes .net i coding it by c# or vb.net

nathan72389 - *September 2, 2015, 8:16 am*
you can look here:
Vb.Net FUD Builder method VIA server patching / byte replacement (Source)

the images are dead, but everything in the thread will make sense.

YunoLawliet - *September 2, 2015, 8:16 am*
(Sep 2, 2015 07:42 AM)moody2000 Wrote: *[CITE]* Hey mates , i search for away that let me to search specific string in EXE file and replace its value to another value

all that with .net c# or vb.net
Mono.Cecil is one of the .NET libraries that can do this.

DisguiserNET - *September 2, 2015, 8:50 am*
use mono.cecil or dnlib or go directly for raw writing and check the #us heap

SIM-2564555 - *September 2, 2015, 9:20 am*
(Sep 2, 2015 08:16 AM)nathan72389 Wrote: *[CITE]* you can look here:
Vb.Net FUD Builder method VIA server patching / byte replacement (Source)

the images are dead, but everything in the thread will make sense.
ok mate this metod seems good i will go to try it now ?

(Sep 2, 2015 08:16 AM)nathan72389 Wrote: *[CITE]* you can look here:
Vb.Net FUD Builder method VIA server patching / byte replacement (Source)

the images are dead, but everything in the thread will make sense.
didn't work with me , is this metod must used with same size string , beacuse i'm try to replace 1 chacracter string with huge string (Hex values for other exe)?

nathan72389 - *September 2, 2015, 10:05 am*
(Sep 2, 2015 09:20 AM)moody2000 Wrote: *[CITE]* ok mate this metod seems good i will go to try it

now ?

didn't work with me , is this metod must used with same size string , beacuse i'm try to replace 1 chacracter string with huge string (Hex values for other exe)?
maybe you did not read:
nathan72389 Wrote:ow, there are some things to remember when doing this. the new and old string MUST be the same lengthnathan72389 Wrote:I have my "Replacement String" padded with a crapload of spaces at the end, this is setting up some free space inside the server for me to add just about anything i wanted tonathan72839 Wrote:well, just think of the logic, if a (for example) gmail username can only have a max of 25 chars, then thats one string that we know the length of, so simply (like i did in the source) pad it with a few extra spaces, and use the trim function.Taserz Wrote:Like if in the stub it was STRINGGOESHERE and the string you added was string it should work if you fill in the rest of the string with blanks or make it A0.
if you cant get it to work, its your problem. there is enough spoon feeding going on, i dont need to chew it for you also.

GhostCode - *September 2, 2015, 10:11 am*
I guess the simplest way is to use dnlib, - as long as you try to modify a managed assembly.
Download the dnlib library from here : https://github.com/0xd4d/dnlib

First make sure you add these imports after you've referenced the lib:

Code using dnlib.DotNet;
using dnlib.DotNet.Emit;
Then you can lookup the string value you like to replace by iterating through the different types/methods/properties etc.
This should give you an idea of how its supposed to be done :

Not the most elegant attempt, but I guess it will suffice for your needs.
Other solutions are Mono.Cecil, System.Reflection or AsmResolver.

Edit : and as already mentioned by nathan72389 you should give us a proper error description, - otherwise
we can't help you. "Doesn't work" isn't a proper error description.

Only3 - *September 2, 2015, 10:33 am*
no need for 3d lib if its string bytes patch is very simple

VirinomTR - *September 2, 2015, 3:10 pm*
You can look Quasar's source. It uses mono cecil to write server settings.
https://hackforums.net/showthread.php?tid=4107161

GhostCode - *September 2, 2015, 3:14 pm*
(Sep 2, 2015 10:33 AM)Only3 Wrote: *[CITE]* no need for 3d lib if its string bytes patch is very simple
That will only work if the string is the same size as the replacement string.
If the new string is longer all offsets in the PE will get messed up.
I would recommend OP to use dnlib/Mono.Cecil to avoid such problems.