Forum:Hack Forums

Thread: How programms copy themselves into executable file

indetectable - *January 13, 2022, 3:51 pm*
Hi, I wonder how can a program can copy himself (or just a small part of his code) into a new executable file, and how can I do it with using c#.
I know its possible

Romeos - *January 13, 2022, 4:30 pm*
"copy himself into a new executable file". I am not quite sure I understand your question tbh.

0x9F - *January 14, 2022, 12:29 am*
https://docs.microsoft.com/en-us/windows/win32/debug/pe-format

indetectable - *January 14, 2022, 6:36 am*
(Jan 13, 2022 05:30 PM)Romeos Wrote: *[CITE]* "copy himself into a new executable file". I am not quite sure I understand your question tbh.
Okay so I will take an example (not that I want to do but this is the best example I have).

I want to know how can a program (made in c#) can create an executable with some code inside, for example when we use a GUI rat, we have the builder and it can create the executable that we want to spread, so how the builder (wich is inside the program) can create a second .exe file with the code that we want inside ?

truco - *January 14, 2022, 1:02 pm*
it depends, if you simply want to create a builder you can use codedom or you can also have a stub (inside resources or w/e) and edit the necessary parts using mono.cecil or dnlib

Joseph Ducreux - *January 24, 2022, 3:13 am*
by binding data to the EOF of an executable and than patching the file image header or something to point to new breakpoint

or simply by using cmd

copy /b a.exe + b.exe = c.exe

if you use extension polygots its possable to differentiate 2 seperate exe's from 1 result if done right

indetectable - *January 24, 2022, 10:27 am*
(Jan 24, 2022 04:13 AM)Joseph Ducreux Wrote: *[CITE]* by binding data to the EOF of an executable and than patching the file image header or something to point to new breakpoint
I dont understand this

or simply by using cmd

copy /b a.exe + b.exe = c.exe

(Jan 24, 2022 04:13 AM)Joseph Ducreux Wrote: *[CITE]* if you use extension polygots its possable to

differentiate 2 seperate exe's from 1 result if done right
This isn't exaclty what I want, to infect a computer the only way I know to do it it's to download another file from web (wich is I think more spoted than just creation another .exe file from nothing (just by clicking on the main program))

Endorphins - *January 25, 2022, 3:04 am*
(Jan 24, 2022 11:27 AM)indetectable Wrote: [CITE] I dont understand this

or simply by using cmd

copy /b a.exe + b.exe = c.exe

This isn't exaclty what I want, to infect a computer the only way I know to do it it's to download another file from web (wich is I think more spoted than just creation another .exe file from nothing (just by clicking on the main program))
It is not ethical to infect another machine that you don't own or you don't have permission to access.

Regarding this quote, he is referring to append the additional information (configuration/settings/instructions in this context) to your stub (the executable you just created with the builder). Whenever the stub will get executed/launched, it will read the appended information.

xHeaven - *January 25, 2022, 6:30 am*
(Jan 25, 2022 04:04 AM)Endorphins Wrote: [CITE] It is not ethical to infect another machine that you don't own or you don't have permission to access.
Nobody cares.

0x9F - *January 25, 2022, 7:06 am*
(Jan 25, 2022 07:30 AM)xHeaven Wrote: [CITE] Nobody cares.
law enforcements do ?

xHeaven - *January 25, 2022, 7:43 am*
(Jan 25, 2022 08:06 AM)riscenjoyerx86 Wrote: [CITE] law enforcements do ?
Catch me if you can, then, bad boy.
This is still Hackforums, thinking and expecting that users will only infect PCs in their ownership is blatantly retarded and insanely naive.

Vuln - *January 25, 2022, 8:15 am*
If you're going to use C# then just access the compiler through CodeDOM, which is very noob-friendly.

mose3c - *January 26, 2022, 10:15 am*
yeb you can do it by reading self bytes and then use WriteAllBytes to write self to new directory

JoseCmanXDII - *February 4, 2022, 1:06 pm*
(Jan 25, 2022 08:43 AM)xHeaven Wrote: [CITE] Catch me if you can, then, bad boy.
This is still Hackforums, thinking and expecting that users will only infect PCs in their ownership is blatantly retarded and insanely naive.
i will catch you.

what a clown

indetectable - *February 13, 2022, 9:24 am*

(Jan 14, 2022 11:15 AM)Incog Wrote: *[CITE]* CodeDOM

https://docs.microsoft.com/en-us/dotnet/framework/reflection-and-codedom/how-to-create-a-class-using-codedom

there is microsofts explanation of it, but I preferred unams as it was easier to read, idfk why

https://github.com/UnamSanctam/UnamDownloader/blob/7fa0cf92e03e2d9f14df6650e0848342fc668cd1/UnamDownloader/Builder.cs#L30For me theses are too complex, sorry..

Code //here you would use replace on the string, and have anything inside the stub code written out like #thing# to prevent unwanted replacements
template = template.Replace("#thing#", "hello");
I dont understand this part, what should I do with #thing# and hello ??

Thanks

indetectable - *February 17, 2022, 5:12 am*

(Jan 14, 2022 11:15 AM)Incog Wrote: *[CITE]* Code //here you would use replace on the string, and have anything inside the stub code written out like #thing# to prevent unwanted replacements
template = template.Replace("#thing#", "hello");
Yes!! this is it finnaly I had to replace

template = template.Replace("#thing#", "hello");
by
template = template.Replace@"\"@"\\")
Thankkk youu!