

# Forum:[Hack Forums](#)

Thread: [CLR Processes](#)

0xBB - April 3, 2013, 9:50 am

Hi everyone , today I'm gonna talk about CLR processes. What are these ?

Wikipedia :

The Common Language Runtime (CLR) is the virtual machine component of Microsoft's .NET framework and is responsible for managing the execution of .NET programs. In a process known as Just-in-time compilation, the compiled code is converted into machine instructions that, in turn, are executed by the computer's CPU. The CLR provides additional services including memory management, type safety and exception handling. All programs written for the .NET framework, regardless of programming language, are executed by the CLR. It provides exception handling, garbage collection and thread management. CLR is common to all versions of the .NET framework. The CLR is Microsoft's implementation of the Common Language Infrastructure (CLI) standard.

tl;dr :

Note : still have .NET dependencies.

Allow to run managed code as native on runtime.

Wikipedia :

[img][http://upload.wikimedia.org/wikipedia/commons/thumb/6/6f/CLR\\_diag.svg/800px-CLR\\_diag.svg.png](http://upload.wikimedia.org/wikipedia/commons/thumb/6/6f/CLR_diag.svg/800px-CLR_diag.svg.png)[/img]

Point of interest :

Since CLR process have that particularity, you can also inject any kind of bytes into the process.

Quick exemple :

[img]<http://flashgamesfactory.magix.net/public/CLR.gif>[/img]

How compile a CLR file ?

- You will need : visual C++

Create a new CLR project :

[img]<http://s10.postimg.org/ub9u17ejt/image.png>[/img]

Click on your project in solution explorer then on "add" -> "New Item".

[img]<http://s16.postimg.org/zcj7cpnn9/image.png>[/img]

Click on "UI" and "Windows Form".

[img]<http://s2.postimg.org/qudu3l6yh/image.png>[/img]

Double click on [Yourprojectname].cpp

[img]http://s18.postimg.org/h512jveu1/image.png[/img]

Add the following :

```
Quote:using namespace System;
using namespace System::Windows::Forms ;
```

```
[STAThread]
void Main (array<String^>^ args)
{
    Application::SetCompatibleTextRenderingDefault (false);
    [Yourprojectname]::MyForm form;
    Application::EnableVisualStyles();
    Application::Run(%form);
}
```

Go to your project's properties.

[img]http://s13.postimg.org/6u08uz1af/image.png[/img]

Under "Linker" > "System" , set "SubSystem" to "Windows".

[img]http://s11.postimg.org/nkdf8rn7/image.png[/img]

Under "Linker" > "Advanced" , set "Entry Point" to your main class, in this case : Main

[img]http://s17.postimg.org/l8q3cis27/image.png[/img]

And you're done ! ? You can now debug/build it.

Have fun ?

?????? - April 3, 2013, 10:39 am

No replies? Damn this is some pretty cool shit. Thank you.

\$uicidal - April 3, 2013, 10:48 am

This is the Visual Basic section.

Belongs here [Mobile Development](#)

0xBB - April 3, 2013, 11:18 am

(Apr 3, 2013 10:48 AM)shahin7777 Wrote: [\[CITE\]](#) This is the Visual Basic section.

Belongs here [Mobile Development](#)

I know its vb section , I'm just showing that you can inject managed to native process compiled under CLR.. Did you read the thread ? Actually the point of this , was that. ?

Washi - April 3, 2013, 11:18 am

(Apr 3, 2013 10:48 AM)shahin7777 Wrote: [\[CITE\]](#) This is the Visual Basic section.

Belongs here [Mobile Development](#)

This section in is not only the Visual Basic section, but also the .NET Framework section. This uses native C++, but managed C++ as well, which uses the .NET framework.

@OP: Pretty interesting stuff. keep it up!

**Percocet** - April 3, 2013, 11:39 am

Get ready to see a flood of crypters that use this in the marketplace.

inb4noobsstartcodingcrypters

**WhyWork** - April 3, 2013, 12:00 pm

pretty interesting, i won't use this, but gj OP :)

**Sc?rf?c3\_** - April 3, 2013, 4:35 pm

Really interesting..but, lets suppose i want to inject managed in this CLR process... i will need a drop first. Correct?

**C3oI** - April 3, 2013, 7:06 pm

already been posted b4 few times ... maybe for the new guys

**Coiner** - April 3, 2013, 7:26 pm

Not sure how this is interesting, since you can inject both Native, managed files in your managed process too.. It worked when i tried to inject crypted msgbox written in freebasic in-to my crypter stub.

**0xBB** - April 3, 2013, 10:17 pm

(Apr 3, 2013 04:35 PM)Scarf3\_ Wrote: [\[CITE\]](#) Really interesting..but, lets suppose i want to inject managed in this CLR process... i will need a drop first. Correct?

Sorry for late reply, Actually you don't. I read somewhere you can load this in memory and since you code it, you can set your entrypoints etc. You can probably use a dll instead tho.