

Forum:[Hack Forums](#)

Thread: [Inject DLL into a defined process](#)

????? - June 8, 2016, 7:20 am

Hi, I want to create a program that downloads a dll and then injects it into a process that is already defined into the code.

I want to inject a .dll file into csgo.exe

I have found many sources for DLL injectors which require user input and I am unable to edit those to work automatically

Cecilia - June 8, 2016, 7:25 am

Depends on what type of injection you want to do (there are many).

Popular is CreateRemoteThread (CRT) and Manual Mapping (MM).

Pretty sure CRT will be detected by VAC, no idea though.

<http://www.codingvision.net/miscellaneous/c-inject-a-dll-into-a-process-w--createremotethread>

There was a library for injections on another forum somewhere. I believe Luminosity link uses it.

????? - June 8, 2016, 7:33 am

(Jun 8, 2016 07:25 AM)LaPanthere Wrote: [\[CITE\]](#) Depends on what type of injection you want to do (there are many).

Popular is CreateRemoteThread (CRT) and Manual Mapping (MM).

Pretty sure CRT will be detected by VAC, no idea though.

<http://www.codingvision.net/miscellaneous/c-inject-a-dll-into-a-process-w--createremotethread>

There was a library for injections on another forum somewhere. I believe Luminosity link uses it.
ok, thank you very much for the link though that is for C and not VB.net

Cecilia - June 8, 2016, 7:40 am

(Jun 8, 2016 07:33 AM)????? Wrote: [\[CITE\]](#) ok, thank you very much for the link though that is for C and not VB.net

C# can be easily converted to vb.net.

Learn to c#.

????? - June 8, 2016, 7:41 am

(Jun 8, 2016 07:40 AM)LaPanthere Wrote: [\[CITE\]](#) C# can be easily converted to vb.net.

Learn to c#.

Many people have told me that Vb.net is nooby and limited.

Should I just move directly to C++ (which is my main goal) or should I pass through C# ?

Cecilia - June 8, 2016, 7:43 am

(Jun 8, 2016 07:41 AM)????? Wrote: [\[CITE\]](#) Many people have told me that Vb.net is nooby and limited.

Should I just move directly to C++ (which is my main goal) or should I pass through C# ?

C# prepares you for C++ syntax.

Up to you to decide.

You asked how to inject a dll.

You're going to have to have a native dll (you can do managed, but please don't especially for csgo hacks -.-) to inject to csgo.

CRT is simple, but probably not VAC proof.

????? - June 8, 2016, 7:47 am

(Jun 8, 2016 07:43 AM)LaPanthere Wrote: [\[CITE\]](#) C# prepares you for C++ syntax.

Up to you to decide.

You asked how to inject a dll.

You're going to have to have a native dll (you can do managed, but please don't especially for csgo hacks -.-) to inject to csgo.

CRT is simple, but probably not VAC proof.

Ok, I'll go into C# at first. Kinda sucks because in school we will be taught vb.net and not C# or C++

Cecilia - June 8, 2016, 7:48 am

(Jun 8, 2016 07:47 AM)????? Wrote: [\[CITE\]](#) Ok, I'll go into C# at first. Kinda sucks because in school we will be taught vb.net and not C# or C++

There are online converters to convert C# to vb.net.

They're the same language at runtime (minus a lib or two).

????? - June 8, 2016, 7:53 am

(Jun 8, 2016 07:48 AM)LaPanthere Wrote: [\[CITE\]](#) There are online converters to convert C# to vb.net.

They're the same language at runtime (minus a lib or two).

Yeah I ran it through one of those and it gives me no errors, but I don't understand what a class is compared to Sub and why I can't call it

Cecilia - June 8, 2016, 7:57 am

(Jun 8, 2016 07:53 AM)????? Wrote: [\[CITE\]](#) Yeah I ran it through one of those and it gives me no errors, but I don't understand what a class is compared to Sub and why I can't call it

Class is a type, it's not a method.

You can call 'methods' inside of it if they are public.

Perhaps read up on OOP in .NET a bit more (especially classes and the likes).

Say I had the class foo with method bar inside.

I can call foo.bar() to get the result bar gives me.

I can't call bar if bar is not public (modifier).

????? - June 8, 2016, 8:27 am

(Jun 8, 2016 07:57 AM)LaPanthere Wrote: [\[CITE\]](#) Class is a type, it's not a method.

You can call 'methods' inside of it if they are public.

Perhaps read up on OOP in .NET a bit more (especially classes and the likes).

Say I had the class foo with method bar inside.

I can call foo.bar() to get the result bar gives me.

I can't call bar if bar is not public (modifier).

Thank you, I wrote BasicInject.Main() and it worked, now my csgo crashes when it injects but that's separate

Ninja - June 8, 2016, 8:30 am

(Jun 8, 2016 07:57 AM)LaPanthere Wrote: [\[CITE\]](#) Class is a type, it's not a method.

You can call 'methods' inside of it if they are public.

Perhaps read up on OOP in .NET a bit more (especially classes and the likes).

Say I had the class foo with method bar inside.
I can call foo.bar() to get the result bar gives me.
I can't call bar if bar is not public (modifier).
Also declare the class first unless the method is static.

Slavoj Žižek - June 8, 2016, 8:41 am

do not inject anything into csgo

work with reading the memory

no writes pls, you will get VACCED instantly

????? - June 8, 2016, 8:44 am

(Jun 8, 2016 08:41 AM)Blezzedd Wrote: [\[CITE\]](#) do not inject anything into csgo

work with reading the memory

no writes pls, you will get VACCED instantly
I have an internal dll that already works

dw about this anymore

I think i'm just going to learn some c++ and maybe recreate the screenshot tool I made in vb

AnarchyCoder - June 8, 2016, 11:15 am

(Jun 8, 2016 07:43 AM)LaPanthere Wrote: [\[CITE\]](#) C# prepares you for C++ syntax.

Up to you to decide.

You asked how to inject a dll.

You're going to have to have a native dll (you can do managed, but please don't especially for csgo hacks -.-) to inject to csgo.

CRT is simple, but probably not VAC proof.

CRT is not a valid detection vector for VAC as there is legitimate uses of it. The same principle is in use when it comes to open handles. Now I must say writing native code is preferred when the game is, any language in the .NET framework works fine though. OP seems to lack knowledge since he thinks C# will make it easier for him to reach his goal.

OP: is there any particular reason to why you want to go internal?

(Jun 8, 2016 08:41 AM)Blezzedd Wrote: [\[CITE\]](#) do not inject anything into csgo

work with reading the memory

no writes pls, you will get VACCED instantly

Why are you spreading old misinformation? Whether you read or write memory has no effect on the detection ratio, skid. 'Cant tell if troll or serious.

????? - June 8, 2016, 11:21 am

(Jun 8, 2016 11:15 AM)AnarchyCoder Wrote: [\[CITE\]](#) CRT is not a valid detection vector for VAC as there is legitimate uses of it. The same principle is in use when it comes to open handles. Now I must say writing native code is preferred when the game is, any language in the .NET framework works fine though. OP seems to lack knowledge since he thinks C# will make it easier for him to

reach his goal.

OP: is there any particular reason to why you want to go internal?

I am aware that CRT is not a real reason for VAC bans.

I am aware that .net can also be used to code cheats. I am not coding the actual cheat but rather an injector.

Yes I am lacking in knowledge but I really want to learn.

Are you saying that learning C# would not facilitate learning C++?

I want to go internal because I want to have a clickable menu but as I was writing that I realised that I can easily do this externally

AnarchyCoder - June 8, 2016, 11:34 am

(Jun 8, 2016 11:21 AM)????? Wrote: [\[CITE\]](#) I am aware that CRT is not a real reason for VAC bans.

I am aware that .net can also be used to code cheats. I am not coding the actual cheat but rather an injector.

Yes I am lacking in knowledge but I really want to learn.

Are you saying that learning C# would not facilitate learning C++?

I want to go internal because I want to have a clickable menu but as I was writing that I realised that I can easily do this externally

C# is a language within the .NET framework, whether you want to learn a new syntax or not is up to you. Honestly, I would stay in VB.NET if that's what you're comfortable with. If you're a slow learner you might want to use C# as a stepping stone but else I don't see any reason to learn it. (Unless it's some abstract language python you should easily understand it without knowing the syntax anyway)

There are multiple managed code examples to learn how injectors work, regarding the clickable menu, you can be really lazy or make an overlay ([related overlay source](#)).

????? - June 8, 2016, 11:36 am

(Jun 8, 2016 11:34 AM)AnarchyCoder Wrote: [\[CITE\]](#) C# is a language within the .NET framework, whether you want to learn a new syntax or not is up to you. Honestly, I would stay in VB.NET if that's what you're comfortable with. If you're a slow learner you might want to use C# as a stepping stone but else I don't see any reason to learn it. (Unless it's some abstract language python you should easily understand it without knowing the syntax anyway)

There are multiple managed code examples to learn how injectors work, regarding the clickable menu, you can be really lazy or make an overlay ([related overlay source](#)).

So the lazy option would be a clickable menu?

AnarchyCoder - June 8, 2016, 11:49 am

(Jun 8, 2016 11:36 AM)????? Wrote: [\[CITE\]](#) So the lazy option would be a clickable menu?

The lazy option would be to have keyboard hook and whenever for example INSERT is pressed, check whether your form or CS:GO is the active window, if csgo then form.show() & form.TopMost = True then the opposite if the form is the active window.

????? - June 8, 2016, 11:59 am

(Jun 8, 2016 11:49 AM)AnarchyCoder Wrote: [\[CITE\]](#) The lazy option would be to have keyboard

hook and whenever for example INSERT is pressed, check whether your form or CS:GO is the active window, if csgo then form.show() & form.TopMost = True then the opposite if the form is the active window.

ok, I have 2 monitors so I don't mind about even having that check at all
But overall I can make a perfectly functional csgo cheat with vb.net?
I only intend to keep this for myself, So i don't mind the "lazy" options

AnarchyCoder - June 8, 2016, 12:12 pm

(Jun 8, 2016 11:59 AM)????? Wrote: [\[CITE\]](#) ok, I have 2 monitors so I don't mind about even having that check at all

But overall I can make a perfectly functional csgo cheat with vb.net?

I only intend to keep this for myself, So i don't mind the "lazy" options

Yes, you can make every feature in VB.NET that you can in for example C++.

If you run 2 monitors, drop the check and just have the form on the other screen so you won't have to run the game "windowed".

????? - June 8, 2016, 12:13 pm

(Jun 8, 2016 12:12 PM)AnarchyCoder Wrote: [\[CITE\]](#) Yes, you can make every feature in VB.NET that you can in for example C++.

If you run 2 monitors, drop the check and just have the form on the other screen so you won't have to run the game "windowed".

Yep I have 2 monitors so that's fine.

Thanks for the advice (I already +3 ages ago)

I'll get to messing around with this soon

Slavoj Žižek - June 8, 2016, 12:46 pm

(Jun 8, 2016 11:15 AM)AnarchyCoder Wrote: [\[CITE\]](#) CRT is not a valid detection vector for VAC as there is legitimate uses of it. The same principle is in use when it comes to open handles. Now I must say writing native code is preferred when the game is, any language in the .NET framework works fine though. OP seems to lack knowledge since he thinks C# will make it easier for him to reach his goal.

OP: is there any particular reason to why you want to go internal?

Why are you spreading old misinformation? Whether you read or write memory has no effect on the detection ratio, skid. 'Cant tell if troll or serious.

go ahead and writeprocessmemory to csgo, have fun with a vacced acc

memory reading is how menalix does it and his cheat is rarely ever detected, even with a quite large userbase

?

????? - June 8, 2016, 1:05 pm

(Jun 8, 2016 12:46 PM)Blezzedd Wrote: [\[CITE\]](#) go ahead and writeprocessmemory to csgo, have fun with a vacced acc

memory reading is how menalix does it and his cheat is rarely ever detected, even with a quite large userbase

?

Yeah I've used hexui before and watched his video about how he codes in vb.net because he knows it very well

AnarchyCoder - June 8, 2016, 1:17 pm

(Jun 8, 2016 12:46 PM)Blezzedd Wrote: [\[CITE\]](#) go ahead and writeprocessmemory to csgo, have fun with a vacced acc

memory reading is how menalix does it and his cheat is rarely ever detected, even with a quite large userbase

?

I've used writeprocessmemory with an open handle to CS:GO since closed beta in early 2012 and yet to see a ban appear. Skid, just leave the discussion, it's not the reason Menalix have stayed UD for a reasonable amount of time.

Wardow - June 9, 2016, 12:53 am

I bet it's even possible to fully disable VAC and only keep the necessary stuff used for server side verifications as it runs on Ring3 level lol

o??law - June 9, 2016, 1:27 am

(Jun 8, 2016 12:46 PM)Blezzedd Wrote: [\[CITE\]](#) go ahead and writeprocessmemory to csgo, have fun with a vacced acc

memory reading is how menalix does it and his cheat is rarely ever detected, even with a quite large userbase

?

Pretty sure that depends entirely on what you're writing to.

Scapula™ - June 9, 2016, 2:47 am

Try call the WriteProcessMemory API dynamically with this

<https://hackforums.net/showthread.php?tid=3849027>

Maybe bypass VAC...

Wardow - June 9, 2016, 4:23 am

(Jun 9, 2016 02:47 AM)Scapula™ Wrote: [\[CITE\]](#) Try call the WriteProcessMemory API dynamically with this <https://hackforums.net/showthread.php?tid=3849027>

Maybe bypass VAC...

There is nothing more stupid then that, I'm hopefull VAC does not perform IAT hooking or again hook by browsing .NET metadata (probably something could be done with that)

halearn - June 9, 2016, 6:12 am

your dll needs to be native

AnarchyCoder - June 9, 2016, 3:25 pm

(Jun 9, 2016 12:53 AM)Wardow Wrote: [\[CITE\]](#) I bet it's even possible to fully disable VAC and only keep the necessary stuff used for server side verifications as it runs on Ring3 level lol

Not really, and they do have a kernel driver however it has only ran once.