

Forum:[Hack Forums](#)

Thread: [\[TuT\] .DLL Injection \(Games\)](#)

The-One - April 12, 2010, 7:39 am

Tutorial wrote by me, I did the comments with the '//'.
NOTE:Inject it to a process, which procces is decided by the injector (<http://pastebin.com/TnCxvupB>
= Injector Source VB.net)

This has NO menu/GUI(Look down this post for a base with menu/GUI)

```
Code #include <windows.h>
#include <stdio.h>
```

```
#define ADR_SPEED 0x123819 // Not existing
```

```
/*----- Hacks Here -----*/
```

```
void SpeedHack() // When SpeedHack(); Is called
{
if(GetAsyncKeyState(VK_NUMPAD0) &1) // If GetAsyncKeyState NUMPAD 0 is pressed
{
*(float*)(ADR_SPEED) = 200; // float(used to 'float' values) to 200 (Normal value = 95)
}
}
```

```
void HackThread() // HackThread makes the hack inject
{
for(;; )
{
SpeedHack(); // This puts the hack on.
}
Sleep(200); // Protect from overload
}
```

```
BOOL WINAPI DllMain(HINSTANCE hModule, DWORD dwReason, LPVOID lpReserved) //
DllMain uses for threading
{
if(dwReason == DLL_PROCESS_ATTACH) // If its attached
{
CreateThread(0, 0, (LPTHREAD_START_ROUTINE)HackThread, 0, 0, 0); // Make thread for the
HackThread, so our hacks run when the hack is injected.
}
return TRUE;
}
EDIT:
```

Ok, im posting this now, its called inline asm, which means, using C++ to write to the asm of the .exe (I COPIED THIS FROM A SITE ILL CODE FOR)

Spoiler ([Click to View](#))

I wanted to code it a while ago, but I could manage doing it with Cpatch nor WriteASM, so I wrote an Inline ASM code.

```
Code DWORD PCross = NULL;
```

```
_declspec(naked) void PremCross()
{
    __asm
    {
        jmp PCross;
    }
}
```

The Function must write the Premiumcrosshair to the PCross.

```
Code #define ADR_PREMCROSSHAIR1      0x005E1F17
```

```
#define ADR_PREMCROSSHAIR2      0x005E1F2E
```

Example For PremiumCrosshair

```
Code If(CH_PremiumCrosshair==1)
```

```
{
    PCross = (ADR_PREMIUMCROSSHAIR2); // Let it jump to PCross
    DetourFunc((BYTE *)ADR_PREMIUMCROSSHAIR1,(BYTE *)PremCross,6); // Detour it, and make
it active
}else{
    memcpy((LPBYTE*)ADR_PREMIUMCROSSHAIR1, (BYTE*)"x0F\x84\x86\x01\x00\x00",6); //
Function will be turned off
}
```

Explanation,Read this only, if you understand more advanced C++ AND Assembly

I JUST EXPLAIN WHAT THE CODE + THE FUNCTION TOGHETHER DOES!!

Well, as we take the first Premiummaddie, and go into olly/ida (Debuggers) we see;

```
Code __:005E1F17      jz     loc_5E20A3
```

JZ means Jump if zero flag is set & if its zero, so the Inline ASM changes the JZ to JMP (JMP= Jump always). So we got:

```
Code __:005E1F17      jmp     loc_5E20A3
```

Next, we need to change the 5E20A3 (Which is normal crosshair) to the premiumcrosshair. Thats where PCross comes(In our Inline ASM code),

```
Code      jmp PCross;
```

In our function we need to place:

```
Code PCross = (ADR_PREMIUMCROSSHAIR2); // PremiumCrosshair2 = The premiumcrosshair,
PremiumCrosshair1 = the normal crosshair
```

So now it always jump to the premium crosshair! And it will always show the premium crosshair!!

So with this Inline ASM (+ The Function) code we changed:

Code ____:005E1F17 jz loc_5E20A3
to

Code ____:005E1F17 jmp loc_5E1F2E
NOTE: 5E1F2E = Premiumcrosshair2 address!

Have Fun. (Full Credits me Ofc)

My OLD Full base + menu + more advanced codes + bypass cheat detection(Full Source) =
[Download Click](#)

VTable Numbers:
[Vtable Numb3rs](#)

I hope you enjoy this thread!
[warn]

The-One - April 12, 2010, 10:17 am

22 views and a few downloads but no reply's? Feedbacks please people :)

i Slap Kidz - April 12, 2010, 11:27 am

Very nice, base is well organized, not sure what to add to the tut so A++

Weather Man - April 12, 2010, 12:11 pm

Thanks for this, I do memory editing in games and I was looking for a tutorial for using InlineASM.

The-One - April 13, 2010, 5:43 am

(Apr 12, 2010 12:11 PM)Moterrac Wrote: [\[CITE\]](#) Thanks for this, I do memory editing in games and I was looking for a tutorial for using InlineASM.
Glad I'd helped :)

(Apr 12, 2010 11:27 AM)i Slap Kidz Wrote: [\[CITE\]](#) Very nice, base is well organized, not sure what to add to the tut so A++
Thanks :D

Weather Man - April 13, 2010, 12:11 pm

How would the Anti-Hack bypass work, would it suspend the threads with an injectable DLL?

The-One - April 14, 2010, 7:33 am

(Apr 13, 2010 12:11 PM)Moterrac Wrote: [\[CITE\]](#) How would the Anti-Hack bypass work, would it suspend the threads with an injectable DLL?
You would get the main .dll from the Anti-Cheat program, reverse(unpack) it, and find addresses. Which basically jump over the detection checks/messages and its functions.

(Apr 13, 2010 01:02 PM)dealin29a Wrote: [\[CITE\]](#) Most likely this would be detected with any anti-hack wouldn't it? but thanks!
NoMenu hacks would never be detected, although you can't use memory hacks(Which writes to assembly).

D.O.A - April 16, 2010, 5:40 am

THNX MAN I REALLY NEED THIS MAN
+k

The-One - April 17, 2010, 3:53 am

(Apr 16, 2010 05:40 AM)D.O.A Wrote: [\[CITE\]](#) THNX MAN I REALLY NEED THIS MAN
+k

No Problem hope u liked it :D

thanasis2028 - April 30, 2010, 6:01 am

Oops, posted in wrong thread. Please delete this post

The-One - April 30, 2010, 6:15 am

(Apr 30, 2010 06:01 AM)thanasis2028 Wrote: [\[CITE\]](#) Oops, posted in wrong thread. Please delete this post

Loolled, you can delete your own posts.

Physix - May 2, 2010, 11:12 am

Would this work in Counter-Strike ?

wernesgruner - May 2, 2010, 12:32 pm

Wtf this violates rules?

ztrain - May 3, 2010, 4:04 am

how would you write something that scans for a memory address like cheat engine?

we are making a game in our programing class, and the teacher is going to have a rigged character. hes going to be standing there so i cant use CE to scan for addresses, so how would i do this in code?

Justsomeguy - May 4, 2010, 5:14 am

If i could +rep you i should do it very nice organized i suck at reading topics like this but this one totally helped me out thank you dude :)

PoZHx - May 5, 2010, 10:13 am

@The One:

Code DWORD PCross = NULL;

```
_declspec(naked) void PremCross()
```

```
{  
    __asm  
    {  
        jmp PCross;  
    }  
}
```

Would not jump to an address...

Within __ASM you shouldn't know the addresses

You should really push address onto stack and ret or
move the address into register (e.g. EAX) but that way is more detectable since your leaving
modified register

You should really use some Code-Injection for your hacks instead of writting to memory with:

Code *(float*)(ADR_SPEED) = 200;

Microsoft MSDetours ? If so it leaves behind 0xE8 bytes which are detectable by Anti-Cheating
software.

Code DetourFunc

Code memcpy((LPBYTE*)ADR_PREMIUMCROSSHAIR1, (BYTE*)"\\x0F\\x84\\x86\\x01\\x00\\x00",6);
// Function will be turned off

You have direct access to memory you don't have to call this internal function.

Tip/advise: You could made a function which backup previous bytes before modifying them.. which makes it easier to toogle options.

Finally your DLL code is very messy:

e.g.

```
Code void HackThread() // HackThread makes the hack inject
```

```
{
for(;; )
{
SpeedHack(); // This puts the hack on.
}
Sleep(200); // Protect from overload
}
```

Why not just write it like:

```
Code void HackThread() // HackThread makes the hack inject
```

```
{
for(;;Sleep(200))
{
// Your hack here instead of calling a function
}
```

Your not dealing with attach/deattach thread messages in your DLL
why not disable them? save you more memory

There is alot of other things i could suggest but i hope these have being helpful :)

The-One - May 5, 2010, 11:08 am

(May 2, 2010 11:12 AM)Vibe Wrote: [\[CITE\]](#) Would this work in Counter-Strike ?Yes it would.

(May 3, 2010 04:04 AM)ztrain Wrote: [\[CITE\]](#) how would you write something that scans for a memory address like cheat engine?

we are making a game in our programing class, and the teacher is going to have a rigged character. hes going to be standing there so i cant use CE to scan for addresses, so how would i do this in code?Use a debugger? (IDA pro/Olly DBG)

(May 4, 2010 05:14 AM)Justsomeguy Wrote: [\[CITE\]](#) If i could +rep you i should do it very nice organized i suck at reading topics like this but this one totally helped me out thank you dude :)No problem.

(May 5, 2010 10:13 AM)PoZHx Wrote: [\[CITE\]](#) @The One:
Code DWORD PCross = NULL;

```
_declspec(naked) void PremCross()
{
    __asm
    {
        jmp PCross;
    }
}
```

Would not jump to an address...

Within __ASM you shouldn't know the addresses

You should really push address onto stack and ret or move the address into register (e.g. EAX) but that way is more detectable since your leaving modified register

You should really use some Code-Injection for your hacks instead of writting to memory with:
Code `*(float*)(ADR_SPEED) = 200;`
Microsoft MSDetours ? If so it leaves behind 0xE8 bytes which are detectable by Anti-Cheating software.

Code `DetourFunc`
Code `memcpy((LPBYTE*)ADR_PREMIUMCROSSHAIR1, (BYTE*)"\\x0F\\x84\\x86\\x01\\x00\\x00",6);`
// Function will be turned off
You have direct access to memory you don't have to call this internal function.

Tip/advise: You could made a function which backup previous bytes before modifying them.. which makes it easier to toogle options.

Finally your DLL code is very messy:

e.g.

```
Code void HackThread() // HackThread makes the hack inject
{
for(;; )
{
SpeedHack(); // This puts the hack on.
}
Sleep(200); // Protect from overload
}
```

Why not just write it like:

```
Code void HackThread() // HackThread makes the hack inject
{
for(;;Sleep(200))
{
// Your hack here instead of calling a function
}
}
```

Your not dealing with attach/deattach thread messages in your DLL
why not disable them? save you more memory

There is alot of other things i could suggest but i hope these have being helpful :)
I've been using this way for a few years and it works fine for me.
I have a function with automatically gets the off bytes for a address.
Microsoft Detours will work, i'm using an bypass which bypass the whole anti cheat.

PoZHx - May 6, 2010, 10:47 am

(May 5, 2010 11:08 AM)The-One Wrote: [\[CITE\]](#) I have a function with automatically gets the off bytes for a address.

Cool since i thought your actual coding was very ineffective and messy.

(May 5, 2010 11:08 AM)The-One Wrote: [\[CITE\]](#) Microsoft Detours will work, i'm using an bypass which bypass the whole anti cheat.

Yeah it may work but still it's more easy to detect and requires you to accept Microsoft Detours Licence argeement and not very efficent as writting your own.

greed460 - May 7, 2010, 2:24 pm

Hah. I was about to write nearly the same as pozhx

The-One - May 8, 2010, 4:21 am

(May 6, 2010 10:47 AM)PoZHx Wrote: [\[CITE\]](#) Cool since i thought your actual coding was very ineffective and messy.

(May 5, 2010 11:08 AM)The-One Wrote: [\[CITE\]](#) Microsoft Detours will work, i'm using an bypass which bypass the whole anti cheat.

Yeah it may work but still it's more easy to detect and requires you to accept Microsoft Detours Licence argeement and not very efficent as writting your own. True.

(May 7, 2010 02:24 PM)greed460 Wrote: [\[CITE\]](#) Hah. I was about to write nearly the same as pozhx No problem then.

AntiH4x - May 8, 2010, 4:28 am

That isnt a universal speed hack... There is more to hooking games than what you think... Why not just learn some DirectX & go from there =D

I was coding Aimbots/Bots for a variety of games, Unreal Tournament 2003/2004/Tactical Ops/Counter-Strike 1.6 etc, almost 3-4 years ago before joining the military.. I havent touched code since & I regret it..

This site is a MUST for game development!

<http://forum.gamedeception.net>

There IRC can be located here!

irc.rizon.net

#game-deception

You will be thanking me for this later, trust me! There all game coders so literally anything/everything you will/would ever need can be covered there! The IRC is laid back too!

Haxor94 - May 8, 2010, 7:23 am

I have a hacking project but how i make it .exe so ppl can open it and shit please help me out :D?

The-One - May 8, 2010, 10:36 am

(May 8, 2010 07:23 AM)Haxor94 Wrote: [\[CITE\]](#) I have a hacking project but how i make it .exe so ppl can open it and shit please help me out :D?

You have to compile/build it.