

Forum:[Hack Forums](#)

Thread: [\[C++\] Hack Making \(.DLL\)](#)

The-One - September 23, 2009, 11:30 pm

Introduction to VC++

Here we will use Visual C++ 2008 Express, which is free and can be downloaded here:

<http://www.microsoft.com/express/download/> (Microsoft)

Of course you can use another program or another version, such as Visual C++ 2005 Express (if you use this you should take a look at the solved problems).

I'll be using, as I said the 2008 version.

Visual C++ is, roughly, an adaptation of C++ to Microsoft's Windows. I mean, it's not really that like, but is a little view of what it is xD (Note, we are going to program with C++)

C++ is "Case Sensitive", which means that distinguish between Mayus. and Minus.

After each C++ command you must end up with ;

Getting Ready

We start the VC++ and go to File->New->Project [Img 1]

[img][http://i40.\[censored\].com/2urs3kx.jpg](http://i40.[censored].com/2urs3kx.jpg)[/img]

Here you will see another window [Img2]. There we click on Visual C++ (left menu) -> Win32

Console Application -> We give it a name -> And click OK.

[img][http://i41.\[censored\].com/29li641.jpg](http://i41.[censored].com/29li641.jpg)[/img]

There you will see the following [Img 3], click Next >

[img][http://i39.\[censored\].com/2mzd445.jpg](http://i39.[censored].com/2mzd445.jpg)[/img]

Then [Img 4]:

Click on DLL

Click on Empty Project (Proyecto Vacio)

Click on Finish

[img][http://i40.\[censored\].com/2djxi1d.jpg](http://i40.[censored].com/2djxi1d.jpg)[/img]

Here we have our first DLL, but don't try to compile, or it will give you errors.

Now we need to create the files where the code will be written. Go to Project->Add New Item. There choose C++ File (.cpp) and write a name. I've written main, to be able to distinguish it better, but it doesn't matter.

Basic Hack!

This is the basic code of a DLL. (Note: Everything starting with // (and in the same line), means that it is a "Comment" and the compiler will ignore it, so, it's like it wasn't there. And it's the same as writing /* and then */.

First we need to add a few references to some Windows header files. This is ALWAYS done on the top of your file:

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

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

Then, we need to also put the main code of the DLL

```
Code BOOL WINAPI DllMain(HINSTANCE module, DWORD dwReason, LPVOID lpvReserved)
```

```
/*Basic Function. */
```

```
{  
    if(dwReason == DLL_PROCESS_ATTACH) /*Here is "tested" if the dll has been attached.*/
```

```

{
    /*If we get here, everything has gone well.*/
}
return TRUE;
}

```

Then we write:

```

Code void TheHacks() /* This is the "Thread" of the hacks, I'll explain it now */
{
    while(1){

        Sleep(50); /* To avoid overloading the CPU */
    }
}

```

A thread is a function that is executed "apart" from the program. Avoiding then using resources of the program.

The while(1) does that everything which is inside gets repeated every 1 milisecond.

Now we must initilize/create the thread, and it will be done only if dll has been atached, so, we will add it on the "DllMain", just below the DLL_PROCESS_ATTACH){

If you get lost, the full code is at the bottom

Add the following:

```

Code CreateThread(NULL, NULL, (LPTHREAD_START_ROUTINE)TheHacks, NULL, NULL,
NULL);

```

There's nothing to explain, we are just creating a thread.

Lets continue coding the hack. We will add a basic Stamina hack.

Actually, there are many ways to do this, but I'll explain the faster and perhaps the easier to understand. (This method may not working on all games, depending if they protect or not memory)

Inside or Thread (TheHacks):

Note: This is not the code we will be using at all. The address are NO recent.

```

Code DWORD dwPlayerPointer = *(DWORD*)0x002200;
    if(dwPlayerPointer != 0){
        *(float*)(dwPlayerPointer + 0x2A4) = 100;
    }

```

Explain it: First line: This is the Player Pointer Address. We are reading it content and saving it on dwPlayerPointer.

Second Line: We are checking that the value has been readed succefully and avoid a crash.

Third Line: First we write the value type, in this case "float". Then we write the address we want to edit, the PlayerPointer (dwPlayerPointer) plus the Offset (0x2A4). Then, following the =, it's the new value.

Well, perhaps ur asking yourself: <<¿But, didn't we have to freeze the stamina?>>.

Of course, but remember, our thread is being repeated every 1 milisecond!

If I'm not wrong, u would like to be able to activated and deactivate the hack, so lets code it!:

First, just below the #include(s) we add:

```

Code bool stamina=false;

```

We have just created a boolean variable. As it name says it can vary between two values, which are: false

```

true

```

As you see we've written =false;. That means that the hack is deactivated by default. Change the false to true to enable it by default.

And what is this useful for?, lets add and If statement and you will see:

We want our hack to run if the variable value is true, so:

Code `/* Note: Delete the old code and put this. DON'T put both! */`

```
if(stamina==true){
```

```
    DWORD dwPlayerPointer = *(DWORD*)0x000002;
```

```
    if(dwPlayerPointer != 0)
```

```
        *(float*)(dwPlayerPointer + 0x2A4) = 100;
```

```
}Inside of the IF we see <<stamina==true>>. There are two equals (==), and that's cus we are
```

*Comparing, not *Equaling.

Ok, nice, but now we need something to toggle it, so, we are going to add hotkeys!

On the Thread `TheHacks()`:

Code `if(GetAsyncKeyState(VK_F6) &1){ /* VK_F6 mean F6 Key*/`

```
    stamina = !stamina;
```

```
}
```

```
/*
```

Note: <<stamina = !stamina>> is the same as:

```
if (stamina==true){ stamina=false;}
```

```
else stamina=true;
```

It's explained now

`*/All the keys in C++ are VK_ and the key in mayus.`

Lets analyse it:

This <<stamina ==>> should be clear. We are changing the stamina var value.

The following: `(!stamina)`: Take a look at the exclamation mark (!). This means the contrary of the var. I mean, If stamina was true, then we would be writing this: <<stamina = !true;>>, which is the same as <<stamina = false;>>.

Ok, it works, BUT, this has a problem. We are checking up if a key is pressed every 1 MILISECOND, so, who is as fast as to press only during 1 ms a key? Noone. There are many ways to solve this, but I am not going to explain it now.

Congrats!

Lets click `Buil->Build Solution`.

We will find our DLL on the Debug folder of our project folder.

Here you have the code:

Code `#include <windows.h>`

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

```
bool stamina=false;
```

```
void TheHacks()
```

```
{
```

```
    while(1){
```

```
        if(GetAsyncKeyState(VK_F6) &1){ //F6
```

```
            stamina = !stamina;
```

```
        }
```

```
        if(stamina==true){
```

```
            DWORD dwPlayerPointer = *(DWORD*)0x002200;
```

```
            if(dwPlayerPointer != 0)
```

```
                *(float*)(dwPlayerPointer + 0x2A4) = 100;
```

```
        }
```

```
        Sleep(50);
```

```
    }
```

```
}
```

```

BOOL WINAPI DllMain(HINSTANCE module, DWORD dwReason, LPVOID lpvReserved)
{
    if(dwReason == DLL_PROCESS_ATTACH)
    {
        CreateThread(NULL, NULL, (LPTHREAD_START_ROUTINE)TheHacks, NULL, NULL, NULL);
//create the new Thread
    }
    return TRUE;
}

```

It's ALL finished, but I'll explain something more.

Appendix

Creating hacks as Zoom (no DMA (offset) and no Freeze)

It is really easy to do this:

What we did later was edit the Address value whenever the var (stamina) was true, so, if we change it value to false, it won't be edited any more. Lets do it:

Code //Below the other bool var.

```
bool zoom=false;
```

```
//On TheHacks() Thread
```

```
if(zoom){
    *(float*)(0x002200) = 0;
    zoom = false; /* We change zoom to false, so it won't be edited any more. */
}

```

There's a new concept:

As you can see we've only written `<<if(zoom){>>`, and we have omitted the `<<==true>>`, which would be `<<if(zoom==true){>>`. Ok, that's because when using a IF statement with a bool var, it's assumed that you are comparing it to true.

optimizint the hack

Have you ever though what would happen if you had like 20 address and warrock updated? Would you be searching for all of them in your code and changing them? NO, the answer it's NO!

To not to do so, we will add a new file, (Project->Add new element). BUT this time it will be a Header File (.h). Give it a name (I use to write `<<define>>` as name, but as always, it's your choice).

First we have to link the main.cpp file to this one, so, go to the first file (main.cpp) and below the others `#include(s)` write:

Code `#include "define.h"` I wrote `<<define>>`, but write the name of your new file.

Now we are going to edit the new file (define.cpp).

We will be following this pattern:

```
#define "Hack_Name" 0x"ADDRESS"
```

For example:

```
Code #define zoom_address 0x000022
```

```
#define spawn1_address 0x000032
```

You must leave a BLANK line at the bottom of this files, or some compilers may give weird errors.

And that's all? No,no...

If you remember, we first used this code:

Code `DWORD dwPlayerPointer = *(DWORD*)0x000222`; Ok, we have to change this 0x000222, which is the address, for the #define which contains the address. Lets do it:

Code //On define.h

```
#define Player_Pointer 0x000222
```

//On main.cpp, instead of the old code
DWORD dwPlayerPointer = *(DWORD*)Player_Pointer;
Now, each time warrock updates, you just have to go to define.h and edit it ^^

Solved Problems

Windows.h (No such file or directory)

This problem is because VC++ 2005 doesn't include some files.

Do the following:Go to

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=7b0b0339-613a-46e6-ab4d-080d4d4a8c4e>

You'll see a bluw box, there u must choice the VC++ which is on the SAME language as your VC++
Scroll down to Files in This Download the one which is of VC++.

Download and install

Go here:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=A55B6B43-E24F-4EA3-A93E-40C0EC4F68E5&displaylang=en> Download the one that fits with ur pcnormally the PSDK-x86.exe (1.3 MB).

Install, and then: (credits to: tamudo84.blogspot):

Step 3: Update VC++ files

Go to: Tools -> Options-> Projects and Solutions -> VC++ Directories. And then add:

Executable files: C:\Archivos de programa\Microsoft Platform SDK\Bin

Inclusive files: C:\Archivos de programa\Microsoft Platform SDK\Include

Inclusive files: C:\Archivos de programa\Microsoft Platform SDK\Include\mf

Library files: C:\Archivos de programa\Microsoft Platform SDK\Lib

Step 4: Update 'corewin_express.vsprops'

You have to edit corewin_express.vsprops. It should be found at C:\Program Files\Microsoft Visual Studio 8\VC\VCProjectDefaults. Replace this

AdditionalDependencies="kernel32.lib"

for

AdditionalDependencies="kernel32.lib user32.lib gdi32.lib winspool.lib comdlg32.lib advapi32.lib shell32.lib ole32.lib oleaut32.lib uuid.lib"

Paso 5: Enable Asistant

You have to edit 'AppSettings.htm':

C:\Program Files\Microsoft Visual Studio
8\VC\VCWizards\AppWiz\Generic\Application\html\3082\

Coment out lines 441 to 444, writing//:

```
// WIN_APP.disabled = true;  
// WIN_APP_LABEL.disabled = true;  
// DLL_APP.disabled = true;
```

```
// DLL_APP_LABEL.disabled = true;
```

Hack doesn't activate/deactivate (Hotkeys)

It can be:Incorrect Address. Can be tested by removing this

if(dwPlayerPointer != 0) and { and }.

If warrock crashes the address is incorrect (most of the times).

Perhaps the hotkeys is pressed more than during 1 ms xD

credits blipi

tomcat09 - October 7, 2009, 11:38 am

Nice Tutorial :) but I got some problem with some Adresses :(

With many I needed it works but i need to write 0x90 to some adresses and every time try to write to this addresses the game crashes :(

All I need ist to write 5 bytes to 5 addresses if I use other programm language with winapi

WriteProcessMemory or memory editor it works but with the dll it crashes and only to this addresses :(

Any Idea what this can be ?

Here my last try

Or can you show me how to use WriteProcessMemory in such an dll :) ?

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

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

```
bool stamina=false;
```

```
void TheHacks()
```

```
{
    while(1){
        if(GetAsyncKeyState(VK_F6) &1){ //F6
            stamina = !stamina;
        }
        if(stamina==true){

            *(char*)(0x005555C0) = 0x90;
        }
        Sleep(50);
    }
}
```

```
BOOL WINAPI DllMain(HINSTANCE module, DWORD dwReason, LPVOID lpvReserved)
```

```
{
    if(dwReason == DLL_PROCESS_ATTACH)
    {
        CreateThread(NULL, NULL, (LPTHREAD_START_ROUTINE)TheHacks, NULL, NULL, NULL);
//create the new Thread
    }
    return TRUE;
}
```

I hope you can help cause I just started to code in c++ some days ago ^^

n3xus - October 7, 2009, 1:29 pm

Thanks for the tut man, I've never tried making dlls before.

I will +rep you as soon as the rep plugin is enabled again.

tomcat09 - October 7, 2009, 1:32 pm

I got it, it was an protected memory region -.-

MCM Domino - October 7, 2009, 11:03 pm

i don't think a noob like myself is going to fully understand why the code does what it does, it's a good post, just sayin ppl will just copy/paste and not learn anything not because they are lazy but because they don't know the technical names yet

i reconize some of it, but i myself am still learning

ByteReaper - October 8, 2009, 1:27 am

Sweet, I've wanted to learn DLLs for ages. Thanks for the info ?

Kingdutch - October 8, 2009, 6:26 am

Nice tutorial, but if you'd want to edit this for other games. How'd you find out what the memory address is (for say stamina, or whatever you wish to edit) and if it's protected yes or no.

Thanks for posting :D

PoZHx - October 8, 2009, 2:48 pm

(Oct 7, 2009 01:32 PM)tomcat09 Wrote: [\[CITE\]](#) I got it, it was an protected memory region -.-
<http://msdn.microsoft.com/en-us/library/aa366898%28VS.85%29.aspx>
Sorted.

(Oct 8, 2009 06:26 AM)Kingdutch Wrote: [\[CITE\]](#) Nice tutorial, but if you'd want to edit this for other games. How'd you find out what the memory address is (for say stamina, or whatever you wish to edit) and if it's protected yes or no.

Thanks for posting :D

When you attempt to change the value of the address it wil fail

Use CheatEngine to scan for addresses follow tutorial and get better understanding before you asked questions

Work on none protected games such as minesweeper before you move onto actual games

Check following websites out:

www.gamehacking.com great website for new hackers

<https://forum.gamedeception.net> great website for adv. hackers (dont ask noob questions or you will be banned no questions asked)

www.feagaming.info new gamehacking very little resources atm

www.aimbots.net inbetween check out tutorials etc

If you dont have good understanding of debugging / asm / coding language of your choice i recommend you go learn

If you do really want to dedicate yourself to learning gamehacking send me via private msg your MSN.. But before you decide it wont be thing you can learn in few weeks

TheHackingIdiot - October 8, 2009, 7:40 pm

In Soviet Russia, computers program YOU!

Agelast - October 28, 2009, 8:47 pm

thats pretty good!...

tomcat09 - November 22, 2009, 4:01 pm

Hi i tried this:

```
DWORD *thefirst = (DWORD*)(*(DWORD*)0x0040014F + 0x1378);
DWORD *thesecond = (DWORD*)(*(DWORD*)thefirst + 0x18);
DWORD *thethird = (DWORD*)(*(DWORD*)thesecond + 0x974);
DWORD *thefourth = (DWORD*)(*(DWORD*)thethird + 0x34);
```

but now i have one problem. How can i prevent a crash when I try to read an adress that does not exists?

I have 3th level Pointer and the last adress does only exist sometimes ^^

Can anyone help me with example how to solve this problem ?

PoZHx - November 22, 2009, 4:05 pm

(Nov 22, 2009 05:01 PM)tomcat09 Wrote: [\[CITE\]](#) Hi i tried this:

```
DWORD *thefirst = (DWORD*)(*(DWORD*)0x0040014F + 0x1378);
DWORD *thesecond = (DWORD*)(*(DWORD*)thefirst + 0x18);
DWORD *thethird = (DWORD*)(*(DWORD*)thesecond + 0x974);
DWORD *thefourth = (DWORD*)(*(DWORD*)thethird + 0x34);
```

but now i have one problem. How can i prevent a crash when I try to read an adress that does not exists?

I have 3th level Pointer and the last adress does only exist sometimes ^^

Can anyone help me with example how to solve this problem ?

You dont add offsets like that lol xd

Use ReadProcessMemory() read 0x040014F then add offset to the buffer
etc etc

Also extra note: 0x0040014F must be invalid because an EP starts at 0x0400000 in typical x86 application