**How To Crack A Program Using OllyDBG | Cracking A Program To Obtain Serial Key**

[1 Reply](http://wayofthecracker.wordpress.com/2012/08/31/how-to-crack-a-program-using-ollydbg-cracking-a-program-to-obtain-serial-key/#comments)

Hey dudes lets start Cracking today and lets see in the real world how Crackers phishing Serial from software.

Our target is a protected program that ask for serial Download Target bellow

<http://www.mediafire.com/?oj6982uxr8rzyrz>

The Tools that we need:  
OllyDbg , PEiD , W32dasm, HexWorkshop

The Protection:  
Serial Protection

Other Information:  
In This is a tutorial we will cover serial fishing with Olly.

Let us first get set up and ready to crack. Go to target folder in our case c:\program files\worldtv\ and make a quick backup that we can work on without fear of screwing up the file. Lets name it worldtv2.exe we will refer to it later

It has become habit to first examine a target with PEiD to determine the packer or protector. Open up PEiD and drag worldtv2.exe into it. The result: “Microsoft Visual C++ 5.0″. Surprisingly, the target is not packed or protected. That will make it all the easier to crack.

Knowing that we will not need to unpack the executable lets us do a little examination of the protection scheme. Open up worldtv. It goes directly into the nag screen letting us know that it is not registered. That is important to note because it lets us know that it is checking for a registration key (maybe a keyfile or registry key) before the program even loads. Try putting in a random key. Ahh, we get a nice little messagebox telling us “Invalid Registration Code”. Let’s write that little message down and save it. Press Okay for Exit.

Finding the Bytes:

Lets first try the easy way. We are going to patch the jump that returns the invalid registration box. Run w32dasm and use it to open up WorldTV.exe. We are opening the original WorldTV.exe file so we can work on the copy that we made. After the file has been disassembled, we will look for the string from the messagebox. To do this click on the String References button at the top of w32dasm. A new window opens up with a list of all strings found in the file. Scroll down until you find “Invalid Registration Code” and double click it.

You should now be at the following lines:

Looking at the code we see a test eax,eax followed by a jne 0041B54C

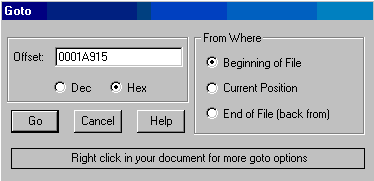
We want to change the jne (jump if not equal) to jmp (jump) that way the program will register when you use any serial. To do this we will need to find where the jne instruction is located in WorldTv.exe. That information is found at the bottom of the w32dasm window.

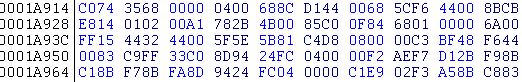
You should see:

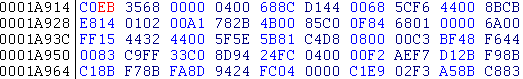
Line:52558 Pg 657 and 658 of 1734 Code Data @:0041B521 @Offset 0001A915h in File WorldTV.exe

We are interested in the Offset value of 0001A915h. Write this number down.. ignore the “h” at the end it just means that the value is hexadecimal.

Patching the Bytes:

Open up WorldTV2.exe in HexWorkshop. Next press CTRL+G to bring up the Goto dialog box, Goto can also be found under Edit. We now want to type in the offset value that we wrote down, in this case 0001A915. Make sure the Hex option is checked and the Beginning of File option is checked. When you are ready press the Go button.  


This will take us to the location of our jne 0041B54C. We know that 75 is the opcode for the instruction JNE and 74 is the opcode for instruction JE. In this case rather than jumping on bad serials we want the program to jump on ANY serial. We will replace 75 with EB which is the instruction for JMP.  


It Becomes:  


Save WorldTV2.exe, Now, find your newly patched WorldTV2.exe and run it.

It asks for a serial! give it any one you want, We will use 1234567. Press Validate Registration and… Success! Registration Code Accepted.  
Are we done? Nop.

Close WorldTV2.exe and open it back up again. It is still asking for a serial. Now, we could just put in a serial every time we use it but that is annoying. Instead, we are going to find a real serial.

Finding a Serial:

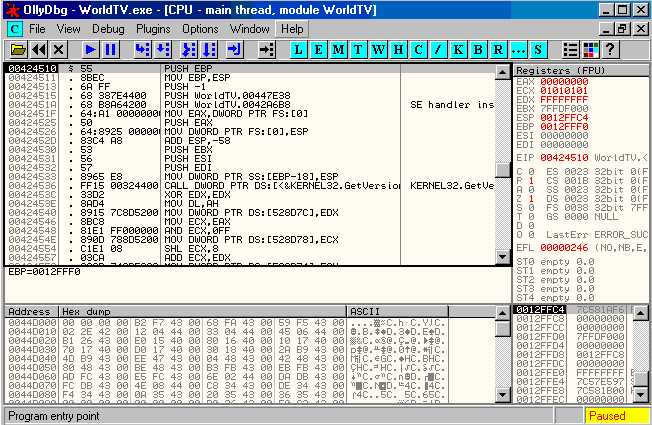
To begin, review what we know about the program so far:

1. It checks for a serial when starting up  
2. After registering with a bogus serial it is unregistered the next time you start it up

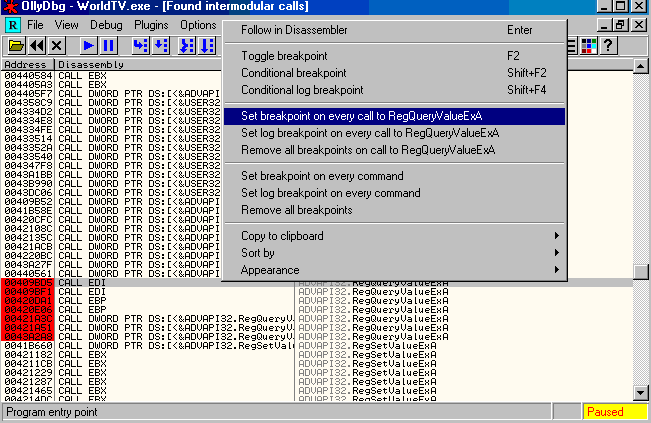
This means that before the program even completely loads it is checking for the existence of a good serial. We need to find out where that serial is being stored. There are usually two places a serial is stored! the registry and in a file. We are going to start with checking the registry. Start up WorldTV2.exe and put in 1234567 as the serial. Validate the serial and then close WorldTV.

Go to your Start menu and find the Run command. A box will open asking you to “Type the name of a program, folder, etc…”. Type in “regedit”, without the quotes, and press enter. You will now be in the regedit window and see a two pane window with a list of folders in the left pane. Click on the plus sign in front of HKEY\_CURRENT\_USER. It will open, you now have another list of folders. Click the plus sign in front of Software. Scroll down until you find WorldTV and click on the folder. Aha! In the right pane we have a key called RegCode with our bogus key: 1234567 stored in it. We now know that WorldTV checks the registry for a serial before loading.

We are going to start by opening Ollydbg. Using Ollydbg, open the original WorldTV.exe.

Resized to 93% (was 652 x 425) – Click image to enlarge

You should see something similar to the image above. Before pressing the Run key we want to set some breakpoints first. Right-click in the Code window of Olly and choose Search For, select All Intermodular Calls. This will bring up the Calls window. Sort the calls by Destination. Scroll down until you find RegQueryValueExA. Select it and Right-Click set a breakpoint on every call to RegQueryValueExA.

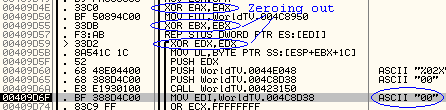
Resized to 93% (was 651 x 423) – Click image to enlarge

Now press the Run button ‘>’ You will first break at FF15 0C304400 CALL DWORD PTR DS:[<&ADVAPI32.RegQueryValueExA>]. If you look at the Register’s window on the right side of Olly, you will see EDI is holding the ASCII value “Recordings”. This is not the registry key we are looking for so press Run again. We break again on the Recordings registry key so press Run again. We will have to press Run 24 more times before we break here:

Resized to 98% (was 615 x 33) – Click image to enlargePosted Image

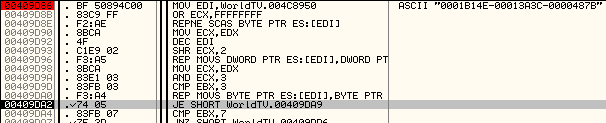
Notice the Value of EAX is ASCII “RegCode”. Press Run once more and we are now here:

Resized to 96% (was 630 x 31) – Click image to enlargePosted Image

And ECX now holds the ASCII value “RegCode”. We know we are getting close because WorldTV just looked for the registration code. We are now going to step through the code and pay attention to the Registers. After a few steps we find that ESI is holding our bogus serial 1234567 and EDI is holding 00000000-00000000-00000000-00000000. This is interesting, however I doubt that a bunch of zeros is the registration code. Stepping through some more, we see that EDI is shortened to -00000000-00000000-00000000. This still does not give us the serial. Continue to step through past where EDI is replaced by “C:\Program Files\WorldTV\Scheduler.txt.tmp”. You will find soon after that point that you come to here:  


Notice that EAX, EBX, and EDX were all zeroed out. Also we see an ASCII value moved into EDI. It is here we are going to start seeing our serial come together. After a little more stepping through we find that we are in a loop. We can see that a serial is being made and can be seen at this address: MOV EDI,WorldTV.004C8950. Rather than stepping through the code line by line we are going to set a breakpoint on MOV EDI,WorldTV.004C8950 and watch our serial come together. Select the line and press F2 to set a breakpoint. Now press the Run button a few times and we can watch our serial build itself.  
Posted Image

Paying attention to EDI earlier we know that our serial is either 4 sets of 8 characters or 3 sets of eight characters. As you get near 3 full sets slow down or you will miss the serial. When you only have 2 characters left to go stop pressing the Run button and just step through the code. When you step past the following line REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:[ESI] you will see the last two characters of your serial added on.

Resized to 100% (was 606 x 123) – Click image to enlarge

Go ahead and write this number down. Press Run again to see if there is another set of characters to be added. Nope. Pressing Run again will start you through another loop where a separate serial is calculated (for what? I am not sure because it would not register the program).

Go ahead and close Ollydbg. Open up the original WorldTV.exe and try registering with the serial we wrote down. Registration Code Accepted, we have successfully registered WorldTV with a real serial. No patching invloved!