HOW TO CRACK ANY TYPE OF SOFTWARE PROTECTION

In this tutorial you will learn how to crack any type of software protection using W32Dasm and HIEW.

IDENTIFYING THE PROTECTION:

Run the program, game, etc., (SoftwareX) that you want to crack without the CD in the CD reader. SoftwareX will not run of course, however, when the error window pops up it will give you all of the vital information that you need to crack the program, so be sure to write down what it says.

CRACKING THE PROTECTION:

Now, run Win32Dasm. On the file menu open DISASSEMBLER > OPEN FILE TO DISASSEMBLE. Select SoftwareX's executable file in the popup window that will appear (e.g. SoftwareX.exe). W32Dasm may take several minutes to disassemble the file.

When W32Dasm finishes disassembling the file it will display unrecognizable text; this is what we want. Click on the String Data References button. Scroll through the String Data Items until you find SoftwareX's error message. When you locate it, double click the error message and then close the window to return to the Win32Dasm text. You will notice that you have been moved somewhere within the SoftwareX's check routine; this is where the error message in generated.

Now comes the difficult part, so be careful. To crack SoftwareX's protection you must know the @offset of every call and jump command. Write down every call and jump @offset number that you see (You have to be sure, that the OPBAR change its used color to green). You need the number behind the @offset without the "h."

Now open HIEW, locate SoftwareX's executable, and press the F4 key. At this point a popup window will appear with 3 options: Text, Hex, and Decode. Click on "Decode" to see a list of numbers. Now press the F5 key and enter the number that was extracted using Win32Dasm. After you have entered the number you will be taken to SoftwareX's check routine within HIEW.

To continue you must understand this paragraph. If the command that you are taken to is E92BF9BF74, for example, it means that the command equals 5 bytes. Every 2 digits equal one byte: E9-2B-F9-BF-74 => 10 digits => 5 bytes. If you understood this then you can continue.

Press F3 (Edit), this will allow you to edit the 10 digits. Replace the 5 bytes with the digits 90. In other words, E92BF9BF74 will become 9090909090 (90-90-90-90-90). After you complete this step press the F10 key to exit.

Congratulations! You just cracked SoftwareX!

Don’t panic if SoftwareX will not run after you finished cracking it. It only means that something was done incorrectly, or perhaps SoftwareX’s protection technology has been improved or created after this tutorial. Simply reinstall SoftwareX and start over. If you’re sure that you completed all steps correctly and the program still will not run, then tough nuts. Their protection was developed after the writing of this tutorial.