How to Crack CD Protections

Full tutorial made by to Crack CD Protections: Full tutorial made for FOR #WAREZFRANCE CREW, by **FANATIK**

Chapters:
1). About, Programs needed … etc.
2). The easy protection.
3). Finding the right file – and the right error.
4). Finding the right line number.
5). Editing the line.
6). Testing.
7). Quick order list.

Here we go (again)!

Chapter I: About, Programs needed … etc.

Hrp! This tutorial is written by FANATIK, member of the #WAREZFRANCE CREW. It is the second part of my first tutorial: RiPPing Tutorial, that explains all about RiPPing except how to crack the CD protections… so here is the other part – how to finish the RiPPing by cracking the protection. This will help you w/ the most basic system of protection, called C- dilla, that is the most usual one…
The programs we will use are 2: first, and decompiler – the files we will work with are in ExE format, and we need a program that will HeX them (transfer to 16 base, hexa, form) and locate the orders given in the code, then we will find the line we need and change it to remove the protection with... – the second program: we need a program that will *edit* the files, and fetch the right line number we got using the first program… all those action are easly done w/ the programs: Win32Dasm (the disassembler - decompiler program, added in the dir [root/Win32Dasm]), and Hiew (the editing program added in the dir [root/Hiew]). The programs are added to the tutorial, because I'm not so sure you can find then on a stable location on the net, in the dir [root/programs].

Chapter II: The easy protection.

Okay! To save you from reading this entire tutorial for nothing you're not going to use I made this chapter, because there is a good chance you won't be needing it! Some games comes w/ protection as a files in the [/Setup] dir (or root dir) called: [00000001.TMP], [CLCD16.DLL], [CLCD32.DLL] and most important [CLOKSPL.EXE]... if you see any of them delete it and the protection should disappear (Important! delete them after making a mirror of the game on your HD, using the info in the next chapter) … if you are still getting an error message just keep on reading.

Chapter III: Finding the right file – and the right error.

The files we are going to work w/ will be the main ExE of the game: you will find it on the CD, in a dir called [/Setup] or [/data], but the easy way to find it is just installing the game, and the ExE that starts the game – will be the ExE we need! ... once you've got it make some room on your HD, because we are going to copy the hole CD to it… before you do that: some games have am option, when Installing, to Install the full game to the CD (but still needing it to play), use it if possible, The files you need to copy are all the game files, in some games it is the root dir of the CD, in others it is the [root/data] dir… the worst case is when the game is inside a CAB file, then you have to use a CAB extractor (WinZip 8 should do the job), and if it is protected a different program that can compile CAB format (I'll try to put it on the tutorial as well). Once you've done all that – press the ExE, and if the game opens close it and exit the CD, then press again- you will get an error window! … usually the line goes like: "Error, please enter CD to run game" or "CD error" or "Error reading CD-ROM" .. what ever error you get – write it down and remember it, we are about to look for it in the ExE code, and change it!

Chapter IV: Finding the right line number.

Open the first program - Win32Dasm, by unzipping it and clicking on [/w32dsm89.exe], now we have to load the file we know is the main ExE of the game, so click on "Disassembler" in the main menu, then "Open File to Disassemble..." (Important! Make sure you got 50-100MB free on your HD) before then pick the file from the clone game dir you made in your HD (Important! make a backup of the ExE) … after you've success fully w8ed while the program disassembled the file, you will see *a lot * of gibberish… don't worry! You don't have to understand what is says (I don't, and I'm not so sure ne1 does… except the programs of course) … (Important! If you can't read and the font shows only numbers and bizarre letters, click on "Disassembler" in main menu, then "Font…" then "select Font" then pick Arial or something in English) … now you have to find the exact line number out of the 2 million in the file that has the error message in it, do that by clicking the "String Data references" button, from the buttons menu (under the main menu) – the second one from the right (-your right)… now you get a list of all the lines in the ExE that refers to actions, and you have narrowed the lines from 2 million – to 2 thousand… to find the error message click the first letter it started w/ (for example, if the message was "Error reading CD-ROM" click E) then search 'till you find the error line you are looking for! … once you've found it… it will mark the title, pick the first line, and it should change color to green (that means the line can be edited and is important)… to be sure you have taken the right line: if there is a line like:
":0044XBCK EB08 ….. (lots of spaces) …. Jmp 0044EBD8" or:
":0044XBCK EB08 ….. (lots of spaces) …. Call 0044EBD8" or:
":0044XBCK EB08 ….. (lots of spaces) …. Push 0044EBD8"
you at the right line, it says the command is a function, effected by the user, and probably the protection we are looking for (notice the words: Jmp = Jamp, Call = Call, Push = Push)… now that we got the right line we have to find her

number! That is done by looking at the bottom of the program window and in the line, that should look similar to this one:
“Line:*** Pg *** of *** Code Data @:0045821 @Offset 00045821h in file:***.exe“
notic the number that comes after the word „Offet“ in this line: 00045821h that is the line number! But notice the letter „h“ at the end of it – you don’t need it, and don’t forget to remove it from the number, now – the only thing left to do is changing the line and removing the protection!

Chapter V: Editing the line.

After writing down the line number you can minimize Win32Dasm, because for now we have finished using it. Open the second program: Hiew (added in the tutorial), this is an editor that will work bad for searching the right line, but will do if you know the line number and just wanna change it…
Open again the same game ExE you have processed in Win32Dasm. When you enter you see a lot of gibberish, that’s the code, and you need to change it to the decoded language… do that by pressing the F4 key and then pick the option “Decode“ .. heh! Alot better now... now click F5 key, to search the right line, you will see the line numbers at the left end of the screen is gray, enter the line number you got from Win32Dasm and it will jump you to the right loction in the file... now, this is the difficult part, not hard to do – but hard to explain, near the line number (just at the right) you will see the command in HeX form, it should be something like BC1BB3D2D1 that is in HeX code (base 16) which means a number (=byte) is represented by 2 letters/number, so that the group (BC1BB3D2D1) is made of 5 bytes: BC – 1B – B3 – D2 – D1 ... (10 numbers = 5 bytes, 8 numbers = 4 bytes and so on...), we are about to change evrey byte from D1 or BC to 90 this is done by pressing the key F3 (activates Editing option) and pressing, for every byte, the number 90 (90 is the noop number, that will disable the action)... and in our case, the command will change from BC1BB3D2D1 to 9090909090 ... once it is done click the key F10 to save the offset, and exit.

Chapter VI: Testing.

Now that you have an ExE w/out the error line, activate it from the same clone dir of the game you made to test it, if its working – congratulation! You have just cracked a CD protection! … if you are getting another error message redo the same steps you have do w/ the first error message (in chapters 3-5) to change it as well (Important! Do it on the same ExE you have edited, and backup this one as well) and then test it again. You might be needed to do it several number of times, until you are getting no error message and the game runs!

Chapter VII: Quick order list.

- Start without Cd then look at the error message and write it down.
- Search the msg in Win32Dasm referance and copy nmber w/out the H at the end!.
- Open Hiew, F4 to Decode, F5 to seach the line, and change the command – 90 for every 1 byte.
- F10 to save and then get out, don’t forget to test!

Good luck CraCKing!

FANATIK.