Adaptec DirectCD Upgrade - IDA for beginners
(Software updates: 'Previous version' checks)

by Zeezee

(5 November 1997, slightly edited by fravia+)
[Picture]Courtesy of fravia's page of reverse engineering
official
IDA is an Official +HCU tool

Well, here is what zeezee wrote to me:

Here another submission of mine. I don't know exactly into what category it should fall, maybe "Most Stupid Protection"? It is somewhat similar to my 'PDFWtirer' essay of last week - you get fully functional upgrade directly from the authors for free (after some work of course).

It's a VERY IMPORTANT essay for all the readers that are 'moving' right now from wdasm to IDA (which is, btw, the 'official' +HCU disassembler 1997). It is worth downloading and cracking this target even if you most probably DO NOT HAVE a CD-recorder and therefore you could not care less for this software. Well, yes! This is the best (and most elegant) cracker attitude: we crack for the pleasure and the challenge, not for the target itself (besides, your advantage here is that you'll begin to understand how powerful IDA could be for other targets :-)

Enjoy!

Zeezee's award: Most Helpful Target for Crackers

Adaptec DirectCD Upgrade - IDA for beginners
by Zeezee, November 1997

On the Web you find many software updates which can be installed

on top of the previous version or after giving serial# of the previous version.

The goal of this essay is to give some light to previous version checks.

Our today's target will be Adaptec DirectCD Upgrade version 1.01b. For most of us the quality / functionality of the target is not important, but for them thinking of trying it, a short description follows.

You must have a UDF-capable CD-Recorder and Windoze 95 to use it.

DirectCD is a software enabling you to use your CD-Recorder just like another drive in the system. if you don't have a CD-R or CD-RW drive this software is completely useless to you (except as cracking target). Until now, CD-s were written in single- or multisession mode making practically impossible to use them as everyday backup devices. Now UDF format arrived and Adaptec started to play with it. DirectCD works under Windoze 95 only, and is of course (like all commercial stuff) full of bugs. Neverthless I'm using it, however I'm far from recommending it to anyone. Simply I've not found anything working better until now.

Back to cracking it.

Tools needed and tools not needed:

DIRECTUP.EXE from adaptec (552k): our target
IDA - of course, you may use the freeware version ida37fw.zip , but the
cracked (Quined :-) IDA37 is much better.
HIEW - no, we do cracking *without* patching here!

SoftICE - no (I have nothing against it, but this protection scheme is too

stupid for it) optionally regmon and filemon (from ntinternals) cup of coffee / cocktail / anything you like for the 'analyzing' phase of IDA (3 mins)

You must follow this lesson with IDA switched on the target, there are no

listings below!

---These steps are informational only and not necessary in the cracking process You can start the .EXE you downloaded, go until it says that previous version isn't found and exit. Simply in order to know, what the program tries to do. You can start regmon just to see what the program needs from registry.

You can start filemon just to see that what we discover later.
You can even have SoftICE up and running but i don't see any usage for it here.
---These steps end
Back to our target.
Run IDAW (or IDAX, whatever you use) DIRECTUP.EXE
Remember to click "Load Resources" on starting dialog. Do it always with

Windoze programs. Here this isn't necessary, but with most other programs

resources are needed. You may edit its cfg file to let IDA load

resources always .

Let IDA do its work. Drink what you prepared before our session and look how

wonderful IDA does it. Green READY in upper right corner? - ok, let's go on.

Menu Options/Cross-References. All checkboxes should be on, and the number of xrefs displayed should be set to 100 just to be sure you don't miss anything. I have this in my cfg.

So, first we check for some interesting strings, say "install"

Alt-B and choose "nstall" (Case sensitive checkbox on, otherwise very sloooow search).

Use "nstall", not "install": we don't know the case of 'i'.

We got 004198A4. Read this very informative message. But poor istaller did not output it to our window during install. Look at text above and below. See - all of them are referenced from the code!

Let's try. Position cursor on xref to found string, press Enter.

Yes, it's pushed and some function called. Cursor on address of this fun, Enter. OH, how many references, it must be very, very often used, let's see what's inside.

The names will be discovered by IDA37 automagically!
call wsprintf

...

call __splitpath

...

call __strupr

...

call WriteFile

It's kinda logfile, isn't it?

We found where hFile is stored, see before WriteFile there is dword_41A1D4 referenced. Go to it. Yes - once written (check it, in sub_403E40 it's written after CreateFile), several times read.

What's the file name? Try to find it or (simpler) run the installer, switch to Explorer when it's displaying one of the windows and look into \temp dir. This file will disappear after setup finishes, but we may undelete it using DOS or what you have. BTW it's very informative, however not essential for our further cracking.

We name proc at 004040D0 say, WriteLog. (press n when cursor is on address).

See how the target itself (and IDA of course) help us cracking!

Esc and we are back with our WriteLog call with "Unable to find Target Dir..."

Seems to be the last thing done in this procedure.

See what's checked in this procedure. Two PgUp-s above and we discover that
"Shellex.dll does not exist" is written to the log,
a bit above:
"DirectCD.exe does not exist",
we look upwards again finding what's written to the log.
We renamed the proc so we see immediately yellow-on-blue where it is called.

When you reach start of the proc at 401200 you may surely rename it to

"CheckPrevious" or similar. It's called from WinMain (2 times), Got it?

OK, now is the time to do detailed inspection about what setup the target expects to find on your disk... with a Little Help From Our Friends (from adaptec).

1. 00401290

In registry Soft..\Micr..\Wind..\CurVer..\UnInstall\DirectCD10 you must have UninstallString set to something. See in other appz how it should look like.

Say, you want to install in C:\DCD, so it should be like this:

UninstallString=C:\W95\uninst.exe -f"C:\DCD\DeIsL1.isu"
Of course for 'W95' substitute your own windoze dir.

2. 004013E9

In the selected dir should exist a file DIRECTCD.EXE
Contents and size of this file seem to be unimportant.
Copy anything you like to a fake file DIRECTCD.EXE in this dir.

3. 00401484

Like in 2. there should be also a SHELLEX.DLL. Copy anything to it.

You may look at the disassembled file. The more you play with IDA, the more you will like it. The whole analysis, including library calls is done. All xrefs are correct: bye bye wdasm.

Run setup again. You have DirectCD fresh and hot. Uninstall it when you don't want to use it. When you have some "unwanted" CD-Rs you may have to find the reference to "llegal" and patch what's necessary. The logfile helps you alot.

After doing it all, you may want to look at unerased logfile or check some references to WriteLog.

Exercise:

Get Easy CD Pro Update (EASY2UP.EXE), and do it again. There is one more check between the 'EXE' and the 'DLL' presence checks. Find it. Crack it.

Hint: Run it first to get EASY2CUP.EXE (with a C inside the name)- that it's the real installer.

Conclusion.

The programmers at adaptec are nice. More than nice. They simply help crackers.
We know exactly what is expected, what is wrong, simply everything. I don't want to repeat myself about IDA.
You've seen 1% of IDA power in this essayjust following it. The remaining 99% are up to you.

IDA weaknesses: just to know about them.

0 hard-to-find info in docs, but there is everything, you must just find it.
1 don't know what to do with loaded resources. They are not decoded or I don't know how to do it. Someone helps?

greets as usual

zeezee (zee_zee@hotmail.com)

You are deep inside fravia's page of reverse engineering, choose your way out:
red homepage red links red anonymity [Picture] +ORC red students' essays red academy database
red tools red cocktails red antismut CGI-scripts red search_forms red mail_fravia
red Is reverse engineering legal?