Cracking 103

After days and days of doing nothing, i have decided what i should be doing. Writing another installment in the Cracking 10x series. So thats just what I'm going to do. And this one has Videos so it will be easier then ever!

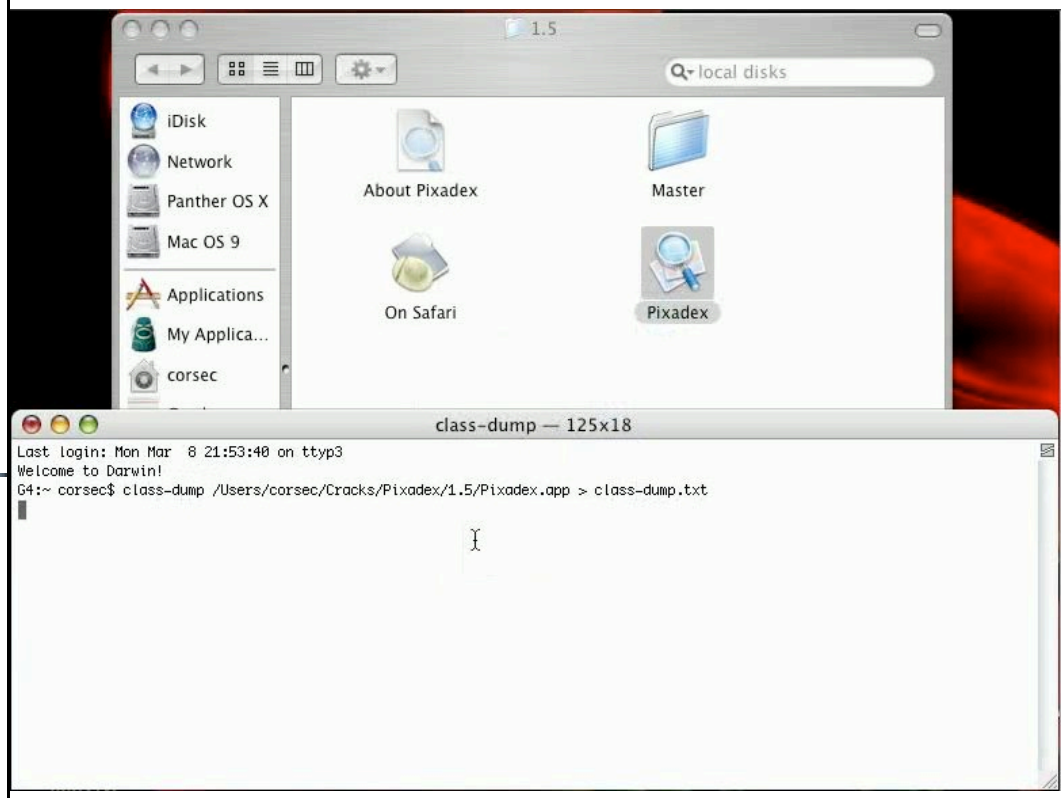
Lets start off with a little disclaimer. Please note that this is for educational purposes only. It will teach someone how to remove protections from programs, but not encourage it for illegal purposes. The idea, in the guide is to show how people add protections onto software, and how you can use your skills as a computer expert to undo those protections, etc... I am not responsible for how you use this information. Once you know this stuff, its out of my hands and i have no control what you do, weather it be to use it for illegal activities or go masturbate. Don't Crack Software, Stealing is Wrong! With that said, lets get Started :D

Todays Hit: The Nice people at The Iconfactory. All copyrights and trademarks reserved by their respective owners. Thats not me :).

They make a nice tool called "Pixadex". Heres what they say about it, because I'm not really sure what it does: Pixadex is to icons, what Apple's iPhoto is to images. Brought to you by Panic and The Iconfactory, the team who created CandyBar, Pixadex lets you import, organize and search huge numbers of icons quickly & easily. Pixadex lets you store all of your icons in a single place, organized into collections that you create. This is the program icon lovers everywhere have been waiting for.

Well, sounds cool, i want it. But 20$ seams like a little too much.

First thing we need to do is a class-dump. We all remember class-dumps (It displays all the classes and functions of those classes, as well as variables in those classes. For more info see Cracking 101, Cracking 102, and search google for class-dump)



For this i just opened up the Terminal, typed "class-dump /Path/to/Pixadex.app > class-dump.txt" (make sure you have class-dump installed first or it will give you an error).

This will dump the class info into a file called class-dump.txt

Lets open this up:

```
@interface RegistrationController : NSWindowController
{
    NSDate *firstLaunch;
    NSDate *launchTime;
    NSTextField *serialNumberField;
    NSTextField *serialNameField;
}

+ (id)sharedInstance;
- (id)init;
- (void)cancelRegistration:(id)fp8;
- (void)findLostNumber:(id)fp8;
- (BOOL)isRegistered;
- (BOOL)isValidSerialNumber:(int)fp8 forName:(id)fp12;
- (void)stupidCrypt:(char *)fp8;
- (void)validateRegistration:(id)fp8;

@end
```

Oh look, there's a function called isRegistered! Thats a bad thing for them, good for us. And it returns a BOOL, True or False. Btw, in the computer worlds 0 == False, and 1 == True. So we want this function to return 1 (aka True) no matter what.

In the past we have used different tools for getting a disassembled version on the code. In this one I'm going to show you how to use GDB it self to get the disassembled code.

start up GDB by typing "gdb" in the Terminal

```
gdb-powerpc-appl — 125x18
Last login: Mon Mar  8 22:29:10 on ttyp3
Welcome to Darwin!
G4:~ corsec$ gdb
GNU gdb 5.3-20030128 (Apple version gdb-309) (Thu Dec  4 15:41:30 GMT 2003)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
(gdb)
```

Click on the Picture to watch the movie

Once GDB is started, Start up Pixadex and then type "attach Pix"
When you press tab it should fill in the rest of the word Pixadex and add a period and some number after it.

```
gdb-powerpc-appl — 125x18
Last login: Mon Mar  8 22:29:10 on ttyp3
Welcome to Darwin!
G4:~ corsec$ gdb
GNU gdb 5.3-20030128 (Apple version gdb-309) (Thu Dec  4 15:41:30 GMT 2003)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
(gdb) attach Pixadex.10256
Attaching to process 10256.
Reading symbols for shared libraries . done
Reading symbols for shared libraries ..................................................................... done
0x900075c8 in mach_msg_trap ()
(gdb)
```

Click on the Picture to watch the movie

Then type "c" for continue and Pixadex will function normally again.

```
gdb-powerpc-appl — 125x18
Last login: Mon Mar  8 22:29:10 on ttyp3
Welcome to Darwin!
G4:~ corsec$ gdb
GNU gdb 5.3-20030128 (Apple version gdb-309) (Thu Dec  4 15:41:30 GMT 2003)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
(gdb) attach Pixadex.10256
Attaching to process 10256.
Reading symbols for shared libraries . done
Reading symbols for shared libraries ..................................................................... done
0x900075c8 in mach_msg_trap ()
(gdb) c
Continuing.
```

Click on the Picture to watch the movie

Now we want to set our breakpoint. Click on the terminal window where gdb is and Press Control + C. This will bring you back to the gdb prompt.

```
gdb-powerpc-appl — 125x18
GNU gdb 5.3-20030128 (Apple version gdb-309) (Thu Dec  4 15:41:30 GMT 2003)
Copyright 2003 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "powerpc-apple-darwin".
(gdb) attach Pixadex.10256
Attaching to process 10256.
Reading symbols for shared libraries . done
Reading symbols for shared libraries ..................................................................... done
0x900075c8 in mach_msg_trap ()
(gdb) c
Continuing.
^C
Program received signal SIGINT, Interrupt.
0x900075c8 in mach_msg_trap ()
(gdb)
```

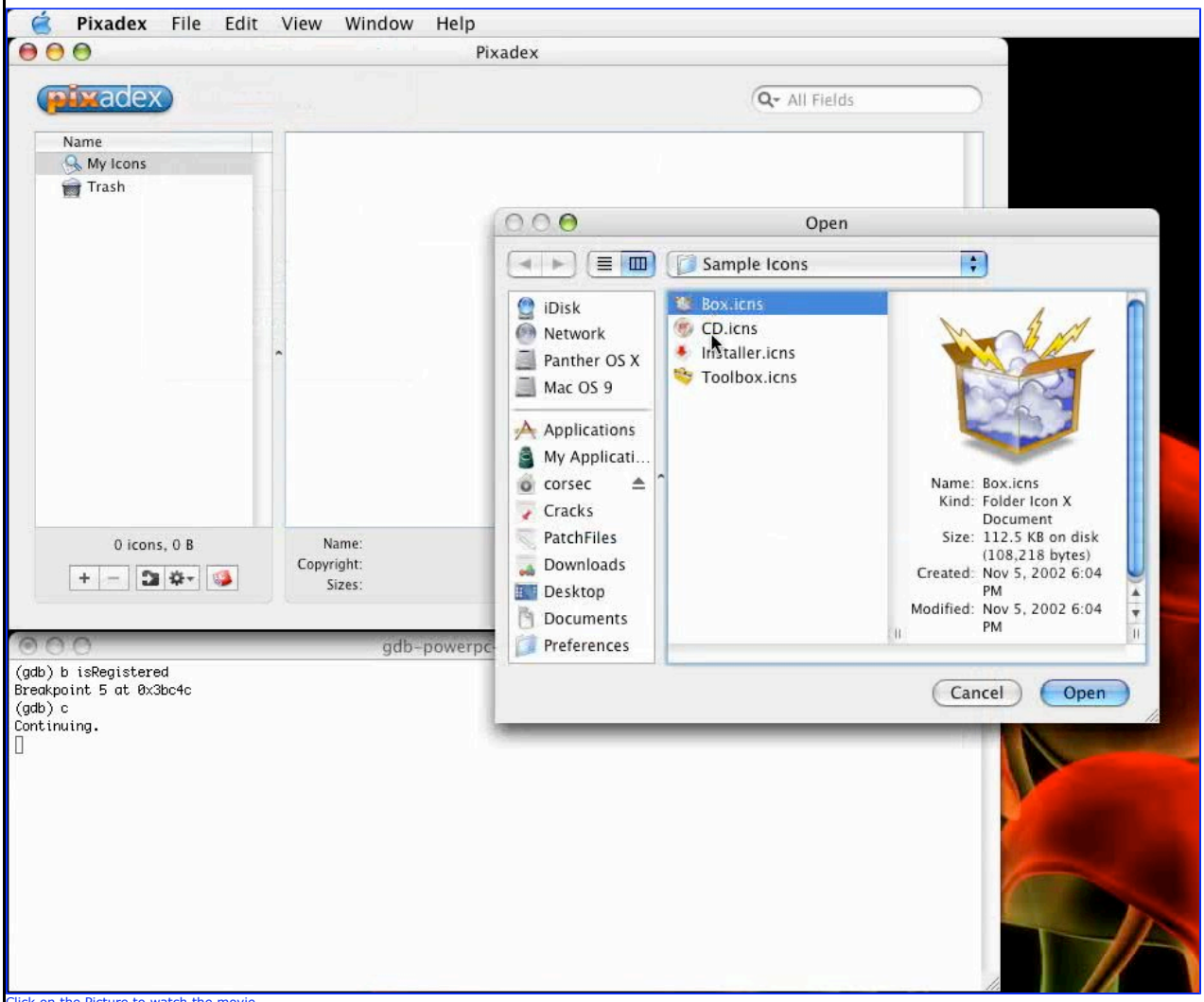
Click on the Picture to watch the movie

Then type "b isRegistered"

this will set a break point at the start of isRegistered function.

Then type "c" to let Pixadex to run normally again.

Doing a little poking around i discovered that isRegistered is called when you try and add more then one icon to the collection. So lets import more then one icon and let GDB catch isRegistered.



Click on the Picture to watch the movie

Not that GDB has stopped Pixadex in its tracks, we would like to take a look at the code its try to run. For this we are going to use the "disassemble" command. It will disassemble the current function.

```
Breakpoint 5, 0x0003bc4c in -[RegistrationController isRegistered] ()
(gdb) disassemble
Dump of assembler code for function -[RegistrationController isRegistered]:
0x0003bc4c <-[RegistrationController isRegistered]+0>:  addis   r2,r12,1
0x0003bc50 <-[RegistrationController isRegistered]+4>:  addi    r2,r2,31864
0x0003bc54 <-[RegistrationController isRegistered]+8>:  lbz     r3,0(r2)
0x0003bc58 <-[RegistrationController isRegistered]+12>: extsb   r3,r3
0x0003bc5c <-[RegistrationController isRegistered]+16>: blr
End of assembler dump.
(gdb)
```

Click on the Picture to watch the movie

As we can see from the code as above gdb doesnt do a bad job of disassembling things

As we have learned before, the value in r3 is the value that is returned by the function. So in this case we want it to return 1. This means we want to change:

0x0003bc58 <-[RegistrationController isRegistered]+12>: extsb r3,r3

to

0x0003bc58 <-[RegistrationController isRegistered]+12>: li r3,0x1

This in it self is not such a hard thing. In GDB to find the hex value of a command we use the "p/x" command. It will print the value in hex. So type "p/x *0x0003bc58" and it will give you:
$1 = 0x7c630774

```
gdb-powerpc-appl — 125x18
(gdb) b isRegistered
Breakpoint 5 at 0x3bc4c
(gdb) c
Continuing.
[Switching to process 10256 thread 0x64b7]

Breakpoint 5, 0x0003bc4c in -[RegistrationController isRegistered] ()
(gdb) disassemble
Dump of assembler code for function -[RegistrationController isRegistered]:
0x0003bc4c <-[RegistrationController isRegistered]+0>:  addis   r2,r12,1
0x0003bc50 <-[RegistrationController isRegistered]+4>:  addi    r2,r2,31864
0x0003bc54 <-[RegistrationController isRegistered]+8>:  lbz     r3,0(r2)
0x0003bc58 <-[RegistrationController isRegistered]+12>: extsb   r3,r3
0x0003bc5c <-[RegistrationController isRegistered]+16>: blr
End of assembler dump.
(gdb) p/x *0x0003bc58
```

Click on the Picture to watch the movie

By repeating this process with 0x0003bc4c, 0x0003bc50, 0x0003bc54, 0x0003bc58 and 0x0003bc5c you end up with this:

0x3c4c0001 0x38427c78 0x88620000 0x7c630774 0x4e800020

removing the "0x" we get: 3c4c000138427c78886200007c6307744e800020

This is the hex value for the function isRegistered.

However we want to change the 7c630774 part to the value of "set r3 to 1".

Fact: The Value of li r3,0x1 (set r3 to 1) is 38600001

So, we need to search for and replace the string:

3c4c000138427c78886200007c6307744e800020

With

3c4c000138427c7888620000386000014e800020

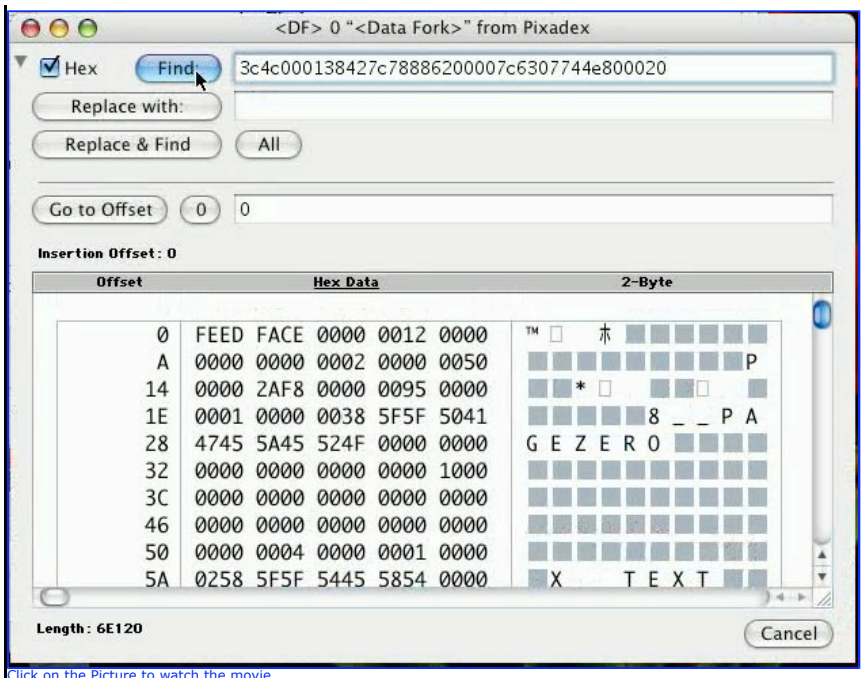
Pixadex by default doesn't allow anyone to write to the executable (this is tricky, but doesn't really stop anyone). To solve this we simply chmod the file so everyone can write to it.

```
bash — 127x19
Last login: Mon Mar  8 22:48:01 on ttyp3
Welcome to Darwin!
G4:~ corsec$ chmod a+w /Users/corsec/Cracks/Pixadex/1.5/Pixadex.app/Contents/MacOS/Pixadex
```

Click on the Picture to watch the movie

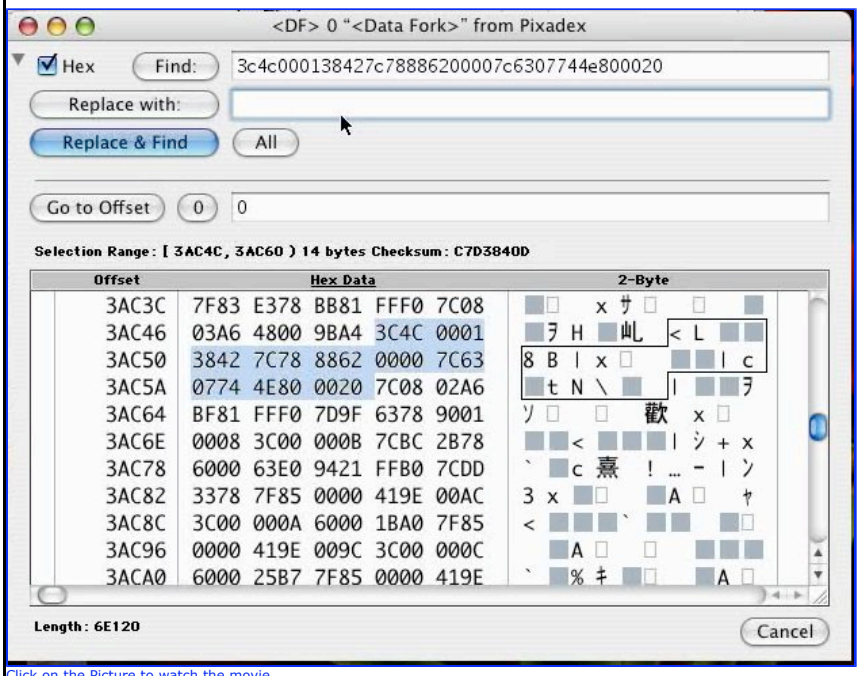
Open up Resourcer, select the Pixadex File, and open the Data Fork.

Then Search for the string we want to replace (the former). Now is the time to check if its the only occurrence of the string. Hit find again to make sure it doesn't find the string again.



Click on the Picture to watch the movie

Then Copy and past the new string into the Replace with box, and click "Replace With" and save the changes (Pixadex will need to be closed to save the changes, so in gdb type "c" and you can then quit normally).



Click on the Picture to watch the movie

Thats it, You now have a fully working copy of Pixadex that thinks its registered.

It has been noted by someone that the App will crash Unless you restore premissions back to the way they were before. So lets do that!

Type the command "chmod a-w /Full/Path/To/Pixadex.app/Contents/MacOS/Pixadex" the same way we set the permissions the first time, except changing the "+" sign for a "-" sign.
I have not looked into this at all but little things like this are sometimes added into the app by the devs just to fuck with you. So watch out.

I hope this is useful for you guys. Any feedback is welcome. I cant be contacted at http://www.CorruptFire.Com

Written By Corsec

< Get Help

Designed For CorruptFire.Com