Cracking SalesAgent Wrapper

Written by : +Vip-Vop Published by Splatter Industries,Inc.

This tutorial deals with the software protection scheme used by major on-line software re-sellers. We will be targeting Egghead Corp.(www.egghead.com) in this lesson. You will need to download a copy of Cool3D from the graphics section of the Egghead website to begin this lesson.

Ok first when trying to register Cool 3d, you'll notice the only options for registering are over the internet and by modem. Try to register over the internet, but make sure you aren't connected. A msg box will pop up saying that you aren't connected and all that crap. Put a bpx on messagebox (not messageboxa, becuase this is a 16 bit program, not a 32-bit one). Now try to connect again, and you will pop into soft ice. Press f12, and you will see you are in rsagent code. Now assuming this is a dll, try to find it on your system. Looking in windows, windows/system, and all your other directories you won't be able to find any thing named rsa* (i used the * becuase theres a small possibility it could be an .exe, even though its most likely a .dll). Now maybe its putting it in a temporary directory. Start the install program again, but while on the first screen go to your temp directory (mine was C:\temp). You will see winsock.dll, rsagent.hlp, and a file with a random name and a .tmp ending. Now the rsagnet.hlp shows we are in the right area. So lets copy that .tmp file so it won't get deleted when the setup exe is finished. I copied it to rsa.dll. Now open up rsa.dll in W32dsm. Scroll down where all the Control ID and Dialog IDs are (near the top of the dead listing). You will will see the following:
Name: DialogID_007C, # of Controls=011, Caption:""

```
001 - ControlID:0438, Control Class:"" Control Text:"PAY THROUGH THE &INTERNET"
002 - ControlID:03E8, Control Class:"" Control Text:"PAY BY &MODEM"
003 - ControlID:03E9, Control Class:"" Control Text:"ORDER BY &PHONE"
004 - ControlID:0006, Control Class:"" Control Text:"ORDER BY U.S. MAI&L/FAX"
```

So we know the program can let us order by phone or mail, which means we can enter a serial number to unlock the program. But now we have to figure out how to make the program let us order by phone or mail. Well if you noticed that when you have to enter whatever name you want and your address etc when you were trying to register before, it saves all that information from before so you dont have to type it in every time. Now we know this is a 16 bit program so it doesnt use the registry, so it must save it all in a .ini file. Lets look in c:\windows. Looking in there you will see rsagent.ini . Open it up and look though it. Most of it is just standard things like your name and modem info. But one line is interesting and out of place.
mailStat-921=0

MailStat sounds like it might have something to do with mailing your order, so lets change it to mailStat-921=1, and restart the setup program. It works, now when you click on buy it shows some serial numbers and asks you to enter your serial number. Lets put a bpx on getdlgitemtext (not getdlgitemtexta, remember this is a 16bit program), and enter some any number for the reg number (I put 111222333). Press ok and you will pop into s-ice. Press F12 and you will see the following:

```
:0005.BF1E 9ACCBF0000          call USER.GETDLGITEMTEXT
:0005.BF23 FFB64CFD             push word ptr [bp+FD4C]
:0005.BF27 FFB64AFD             push word ptr [bp+FD4A]
:0005.BF2B 9A166C47BF            call 0003.6C16
:0005.BF30 83C404                add sp, 0004
:0005.BF33 3D0A00               cmp ax, 000A
:0005.BF36 7434                  je BF6C
```

See how right after the call it compares ax with A (10 decimal)? Well right now ax holds 9 for me, which happens to be the number of digits long my reg number was. So its checking the length of our reg number to make sure its a 10 digit number. So press ctrl-D, it will nag about your bad reg number. Now enter a 10 digit number, I put "1112223334", and press Ok again. Now you will go with the je and keep on going down. You can also clear your box getdlgitemtext now. Now as you scroll down notice there arent any conditional jumps for a little bit. So we don't have to worry about missing any important code. Now as you are pressing F10 to scroll you will see the following code coming up (but dont press F10 to go past it):

```
:0005.BFA4 8D8656FF           lea ax, [bp+FF56]
:0005.BFA8 16             push ss
:0005.BFA9 50             push ax
:0005.BFAA 9A5279D9BF          call 0003.7952
:0005.BFAF 83C408            add sp, 0008
:0005.BFB2 0BC0             or ax, ax
:0005.BFB4 7403            je BFB9
```

Continued on page 3

That je is the first jump, but it also happens to be the AreWeRegged jump. If you do a "r fl z" on that jump and then press ctrl-d you can install Cool 3D, but lets get a working serial number instead becuase creating a crack for this program would be hard as the dll is hidden inside that main exe file, and probably compressed. See the call 0003.7952 right before that je, that most likely is the call to see if we are regged. So hopefully you haven't pressed F10 to go by that lea ax line yet. As soon as you execute that "lea ax, [bp+FF56]" is executed, type "d ax" to show whats in ax. You will find the correct reg code ("HFAWPNAXEI"). So now if you want to be able to tell other people how to unlock this program, all you have to do is change the mailStat-921=0 in c:\windows\rsagent.ini to mailStat-921=1, and enter the the reg code we got earlier. You can use this method to get any reg number for any program protected with rsagent, so I suggest we start d/l everything from www.egghead.com now before they get smart and change the protection.

Cracking SalesAgent Wrapper
Written by : +Vip-Vop

Published by : Splatter Industries,Inc.

THE END