Subject: All anti cheat programs can be defeated
Posted by Kanezor on Sun, 03 Apr 2005 21:19:33 GMT
View Forum Message <> Reply to Message

Firstly, the EXE is encrypted, meaning that the EXE loads up and a pre-made decryption algorithm runs on itself (actually not really itself, but for all practical purposes...). You'd have to break that first.

Once you've done that, your main goal should be to aquire the network protocol it uses (assuming you want to bypass Renguard: best way to do that would be to write your own client that emulates Renguard... but allows cheats). Easy enough once you've decrypted the EXE.
Follow the execution path of Renguard starting up (without actually starting up Renguard, as it could detect that you have debuggers not only installed and running, but running on *IT*, so you can only work with disassembly at this point). There's a number of things to watch here. You'd need to look for a few things, especially calls to Winsock. But don't just go straight to that, you really should find out what variables it loads at startup, because it will most likely be sending those variables (encrypted, of course) over the network. Things such as the hashed/encrypted version of your cd key, the name you'd be playing on (which would be the name passed to it on the command line at startup, or if none found there, then the WOL name), and the hashes of various files in your Renegade and Renegade\Data folder.

Anyways... from there, it's easy work.

Unless you know what you're doing (and have the proper tools), the hardest part would be breaking the EXE encryption, in my opinion.