Subject: Re: Why not open source?
Posted by Kanezor on Sun, 02 Oct 2005 20:16:41 GMT
View Forum Message <> Reply to Message

howang wrote on Sun, 02 October 2005 02:22dead6re wrote on Wed, 28 September 2005 01:45
Your users need to learn some facts:

1) DJM is NOT part of BHS
2) I have never seen Crimson use bad languge, unless you calling in on the fake cheats!
3) I use ProcessGuard, it can tell you exactly whats its trying to access, so I can tell what is happening. I get no keyboard hooks or scanning cookies. Only renegade directory files.
4) The cd key is encrypted within Renegade, Im guessing MD5 as that is one way. This make it virtually impossible to crack it.
5) Open source would release the protocol and then a fake RenGuard client could be made! We don't want this to happen.

1) But BHS allow people use bad language here!
2) Take a look on the RG network ban forum, you will find some.
3) Yes, I don't think RG is spyware too, but it is really hard to let people understand this fact.
4) Don't you know that you can put the encrypted key in your registry? It is NO NEED to crack the encryption but just use the encrypted one!
5) Yes, I have think about this point before you said it.

My responses to your points:
1) BHS allowing people to swear doesn't make BHS bad. It proliferates free speech.
2) Of course people are swearing in the RenGuard network ban forum -- people are pissed that they're banned. I have never noticed Crimson swear at any particular person on these forums (whether in the Network Bans subforum or elsewhere) without major provocation. If you'd like, you could even review her posts here (Mr. Stalker!):
http://www.renegadeforums.com/index.php?t=showposts&id=8 &rid=4243
3) I *know* RenGuard is not spyware. Yes, helping people to understand that can be difficult, but that will never go away.
4) Putting an encryption key in the registry decreases security, since it's wholly easier to read a registry key than to read process memory (and to know exactly what memory to read, you must read the code to find out where that encryption key is stored)
5) Think harder. Seriously... much harder.

My own points:
1) Open-sourcing RenGuard would reveal exactly how it prevents cheats from being used. Then, people would be able to write their own program that says that they are clean, when in fact they are using cheats. Don't say that they won't, because they will.
2) Why don't you write some anti-hack software and then try to break it without the source code? Then, try again with the source code. Once you've completed both, take note how long each took.

The fact of the matter is, if you cannot understand my #1 point, then you really shouldn't be writing software and especially not criticising those that do. It doesn't take a computer scientist to realize that any executable on a user's computer can be bent to the user's (in this case, the cheater's) will, no matter what it does nor how it does it. It also doesn't take a genious to know that that

bend-to-break thing will occur in an amazingly short amount of time (hours at the very most) if the source code is available.
