Subject: All anti cheat programs can be defeated
Posted by gibberish on Fri, 25 Mar 2005 10:18:43 GMT
View Forum Message <> Reply to Message

It is only a question of how much work is necessary.

For example if someone either disassembles or gets the source to the device drivers for both their graphics card and mouse.
It would be possible to link the mouse click to a color change on a certain pixel of the graphics card.

Hence you have a basic click bot.

If the individual never released the source, binary or information about the existence of this hack it is extremely unlikely that any game or anti cheat program could detect it.

If you want to go even more extreme, do it with hardware instead.
Have a camera pointed at your monitor and have a second PC hard wired to the mouse, there is no possibility of detecting it unless the person setting it up is incompetent enough to not build in a "miss factor".

So put the issue to bed and say that there are currently no known hacks but it is possible someone has compromised RG.

PS I know this is far fetched but my point is that some people do go to extreme lengths.
And there is always the possibility someone has missed something simple.

Subject: Re: All anti cheat programs can be defeated
Posted by Blazer on Fri, 25 Mar 2005 10:46:26 GMT
View Forum Message <> Reply to Message

Its almost 4am and I'm tierd, so forgive my coyness.

captain obviousIt is only a question of how much work is necessary.

Indeed...with enough work, you could make a nuclear weapon in your garage.

gibberishFor example if someone either disassembles or gets the source to the device drivers for both their graphics card and mouse.
It would be possible to link the mouse click to a color change on a certain pixel of the graphics card.
They already have those, they are called click-bots, or color-aimbots. They work so well that nobody actually uses them. Try one out yourself if you want to see how crappy they work and how little advantage they are.

gibberishHence you have a basic click bot.

Wow you conceived of that all by yourself, and even named it the same name it was called 3 years ago :rolleyes:

gibberishIf the individual never released the source, binary or information about the existence of this hack it is extremely unlikely that any game or anti cheat program could detect it.
You are forgetting the mentality of cheaters. Despite what many people think, their goal is not to win. If this was really their goal they would use subtle cheats, just enough to give them an edge. But no, they would rather run around killing everyone, and getting their rocks off everytime someone says "wtf" or yells at them. Their main goal is to piss people off, and they always openly use and brag about their cheats, including how they work.

gibberishIf you want to go even more extreme, do it with hardware instead. Have a camera pointed at your monitor and have a second PC hard wired to the mouse, there is no possibility of detecting it unless the person setting it up is incompetent enough to not build in a "miss factor".

What about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

gibberishSo put the issue to bed and say that there are currently no known hacks but it is possible someone has compromised RG.

There are actually known hacks for RG (BHS members know how it can be done), but so far nobody has been found using that method or any reports of it. Also, this particular method will be shut down with RG 1.04

gibberishPS I know this is far fetched but my point is that some people do go to extreme lengths. And there is always the possibility someone has missed something simple.

Fortunately Renegade is a small enough community that we havn't really had to battle any "uber hackers" that are wizards at assembly language and whatnot. Even if they tried, BHS has several members with such skills, and we would easily counter any cheat that was concocted. So even IF an RG exploit is discovered, we will immediately stop it. Thats pretty much as safe as you can get.

Subject: All anti cheat programs can be defeated
Posted by zunnie on Fri, 25 Mar 2005 11:03:44 GMT
View Forum Message <> Reply to Message

Another pointless post lol

Subject: All anti cheat programs can be defeated
Posted by Dave Mason on Sun, 27 Mar 2005 18:37:42 GMT

View Forum Message <> Reply to Message

BlazerWhat about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

LMFAO!!!!!!!!!

Subject: All anti cheat programs can be defeated
Posted by csskiller on Sun, 27 Mar 2005 18:53:24 GMT
View Forum Message <> Reply to Message

Blazer
That just about sums it all up

Subject: All anti cheat programs can be defeated
Posted by Spoony_old on Sun, 27 Mar 2005 21:33:52 GMT
View Forum Message <> Reply to Message

these theoretical posts are so retarded... if you know how to bypass RG or you saw someone else do so... prove it...

I did, wasn't hard

Subject: All anti cheat programs can be defeated
Posted by Renx on Mon, 28 Mar 2005 00:15:35 GMT
View Forum Message <> Reply to Message

Pfft, you don't have to be cheating in order for your goals to be to piss people off. Why do you think people snipe? Personally I find it hilarious when people start typing in caps with "!RG DAEPSOIN" and whatnot. But hey, that's just me...

Subject: All anti cheat programs can be defeated
Posted by Jzinsky on Mon, 28 Mar 2005 01:44:07 GMT
View Forum Message <> Reply to Message

So they DO do it to piss people off!

Subject: Lol
Posted by Uarepoo2 on Tue, 29 Mar 2005 21:06:31 GMT
View Forum Message <> Reply to Message

Blazer ... The sneakercheat ... Got me laughing like mad

Subject: All anti cheat programs can be defeated
Posted by nopic on Tue, 29 Mar 2005 22:09:50 GMT
View Forum Message <> Reply to Message

DJMBlazerWhat about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

LMFAO!!!!!!!!! x2

Subject: All anti cheat programs can be defeated
Posted by Chronojam on Tue, 29 Mar 2005 23:18:31 GMT
View Forum Message <> Reply to Message

I've used the Sneakercheat in other Westwood products before.

Subject: All anti cheat programs can be defeated
Posted by IRON FART on Tue, 29 Mar 2005 23:32:55 GMT
View Forum Message <> Reply to Message

Quote:
What about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

Well there's protection against that...
What do you think cups are for?
Wear a cup -> When someone kicks you in the nuts, pretend you are in agony -> When they are on their way back to their computer, shoot them while they are AFK.

Subject: Lol
Posted by Uarepoo2 on Wed, 30 Mar 2005 00:40:29 GMT

View Forum Message <> Reply to Message

U do realise people dont wear cups in everyday life lol ... tht wud just be odd

Subject: All anti cheat programs can be defeated
Posted by IRON FART on Wed, 30 Mar 2005 02:58:35 GMT
View Forum Message <> Reply to Message

Speak for yourself...I'm cheat-protected.

Subject: All anti cheat programs can be defeated
Posted by ododd on Thu, 31 Mar 2005 01:33:23 GMT
View Forum Message <> Reply to Message

nopicDJMBlazerWhat about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

LMFAO!!!!!!!!! x2

x3 (or is it more...)

Blazer
Indeed...with enough work, you could make a nuclear weapon in your garage.

hey i did that but CSIS caught me...
zunnie
Another pointless post lol
that was probably just as pointless (okay gibberish's post was more pointless)

Subject: All anti cheat programs can be defeated
Posted by theplague on Fri, 01 Apr 2005 00:05:12 GMT
View Forum Message <> Reply to Message

you know, he has a point, why if there is that few 'uber' asm experts out there? what if they did get into how rg works? even if it's 1/1000 people, then it's that 1 person that has the advantage and that person will discredit RG... rg hasn't been updated in a while now, i'll be waiting for the next patch...

just so you know, asm isn't hard, i did it for some helbreath servers a while back, and the stuff you need to know is minimum, it's just what tools and how you use them.

asm can do amazing stuff.. it can make flash mx 2004 work for free, westwood and ea games fall to their knees.

just don't underestimate them....

/me revises asm *although i have no intention or time to mess with rg* :S

Subject: All anti cheat programs can be defeated
Posted by ododd on Fri, 01 Apr 2005 01:32:44 GMT
View Forum Message <> Reply to Message

ya renegade is an older game and it might be easier to hack directly...

Subject: All anti cheat programs can be defeated
Posted by Blazer on Fri, 01 Apr 2005 06:54:31 GMT
View Forum Message <> Reply to Message

It would take more than just knowledge of ASM. RG uses a complex encryption...for example just because you know ASM doesnt mean you can sniff SSH, SSL, etc connections.

Subject: All anti cheat programs can be defeated
Posted by Kanezor on Sun, 03 Apr 2005 05:20:49 GMT
View Forum Message <> Reply to Message

Really, if you know ASM, then it doesn't matter what type of encryption Renguard is using for network protocols. Just disassemble Renguard and learn the decrypted protocol from the program itself (eg, before it encrypts the data), instead of packet logs.

Subject: All anti cheat programs can be defeated
Posted by Dan on Sun, 03 Apr 2005 10:15:57 GMT
View Forum Message <> Reply to Message

lol.... disassemble RenGuard....

I did that to see what anti-disassembling stuff they put in, and I must say, they did a good job. I dont think anyone will be doing much by that approach ;D

But then again, I could be overlooking something because I dont know much ASM

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.

Subject: All anti cheat programs can be defeated
Posted by Kanezor on Sun, 03 Apr 2005 21:21:37 GMT
View Forum Message <> Reply to Message

oops, double post... wonder how this got here... :\

Subject: All anti cheat programs can be defeated
Posted by Scorpio9a on Mon, 04 Apr 2005 13:24:02 GMT
View Forum Message <> Reply to Message

Yes, its possible to hack RenGuard, thats something we won't deny, but it takes quiet alot of time to do so. And most simply aren't bothered or simply can't do it.

Kanesor its a bit more complex to do then you think, but the basic outline seems to be pretty good yes and you aren't far from how i would do it.

Subject: All anti cheat programs can be defeated
Posted by Dan on Mon, 04 Apr 2005 18:31:01 GMT

View Forum Message <> Reply to Message

I think we can rest assured, knowing that the people like the kind that hang around EAX barely know much more than how to press a "Download" button. Even if they did, BHS could just change the encryption, so they would have to do it aallll over again. =)

Subject: All anti cheat programs can be defeated
Posted by theplague on Tue, 05 Apr 2005 07:55:34 GMT
View Forum Message <> Reply to Message

well, someone did hack RG...
a guy with no name, or one that can change his name to any name he wants...
has all hacks under the sun, fr, bighead,wallhack...

i saw him on a server a few hours ago[/quote]

Subject: All anti cheat programs can be defeated
Posted by Crimson on Tue, 05 Apr 2005 09:20:03 GMT
View Forum Message <> Reply to Message

That's not an RG hack, and we are currently testing a fix... I also have a fix in place on my server which amsg floods an exploiter and team changes them over and over so they quite literally can't fire many shots.

Subject: All anti cheat programs can be defeated
Posted by Halo38 on Tue, 05 Apr 2005 18:33:19 GMT
View Forum Message <> Reply to Message

nopicDJMBlazerWhat about the SneakerCheat? It's where you run to the other persons house, and kick them in the balls...they take their hands off of their mouse for at least 5 mins, giving you time to run back home and headshot them while they are standing still. OMG SNEAKERCHEAT BYPASSES RENGUARD OMG ONG OMG RG SUX EVERYONE AND THEIR DOGGS ARE CHEATING! RENEGADE IS DOOOOOOMMEEED.

LMFAO!!!!!!!!! x2

(2 min later) still laughing!

Subject: All anti cheat programs can be defeated
Posted by Kanezor on Tue, 05 Apr 2005 21:22:11 GMT
View Forum Message <> Reply to Message

Scorpio9aYes, its possible to hack RenGuard, thats something we won't deny, but it takes quiet alot of time to do so. And most simply aren't bothered or simply can't do it.

Kanezor its a bit more complex to do then you think, but the basic outline seems to be pretty good yes and you aren't far from how i would do it.I know very well how complex it would be, I've done such things on old Macs several times. It was a fair bit easier for me there, because I knew where to get the information I needed, such as the PEF format (PEF is to Mac as EXE is to Windows). As such, I had written my own tools to do what I needed.

If I had the proper tools and information for Windows, I would be willing to do it, just to prove that it could be done.
I'm not saying that I would actually use an anti-anti-hack, though. I myself hate cheaters.
