Subject: Possible virus in renegadeserver.exe
Posted by jonwil on Sat, 24 Jul 2010 07:59:11 GMT
View Forum Message <> Reply to Message

My AVG Anti-Virus reports that renegadeserver.exe from the renegade FDS is infected with a virus. Does anyone else get reports for that file?

Windows says the file is 94,208 bytes in size, does this match with what everyone else gets?

Just trying to confirm if its a genuine report or not.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Goztow on Sat, 24 Jul 2010 08:13:33 GMT
View Forum Message <> Reply to Message

jonwil wrote on Sat, 24 July 2010 09:59My AVG Anti-Virus reports that renegadeserver.exe from the renegade FDS is infected with a virus. Does anyone else get reports for that file?

Windows says the file is 94,208 bytes in size, does this match with what everyone else gets?

Just trying to confirm if its a genuine report or not.

My renegadeserver.exe is 27 KB (date: 19 Jan 2005)

Subject: Re: Possible virus in renegadeserver.exe
Posted by danpaul88 on Sat, 24 Jul 2010 08:49:30 GMT
View Forum Message <> Reply to Message

As far as I know renegadeserver.exe is just a launcher for server.dat anyway and you can just rename server.dat to server.exe and delete renegadeserver.exe.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Sladewill on Sat, 24 Jul 2010 09:18:40 GMT
View Forum Message <> Reply to Message

yes our AVG does that as well it goes as far as deleting it everytime so we have to keep putting it back on serverbox

Subject: Re: Possible virus in renegadeserver.exe
Posted by Omar007 on Sat, 24 Jul 2010 09:30:45 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Sat, 24 July 2010 10:49As far as I know renegadeserver.exe is just a launcher for server.dat anyway and you can just rename server.dat to server.exe and delete renegadeserver.exe.
You could compare the renegadeserver.exe->server.dat(exe) relation with the client's Renegade.exe that launches Game.exe

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Sat, 24 Jul 2010 09:31:02 GMT
View Forum Message <> Reply to Message

I sent the file to AVG as a "possible false positive" so they can confirm whether its a bogus report or not (and if its a bogus report, fix AVG in the next update to not report on it)

Subject: Re: Possible virus in renegadeserver.exe
Posted by Sladewill on Sat, 24 Jul 2010 21:09:12 GMT
View Forum Message <> Reply to Message

hopefully they will sort it out coz thats rlly annoying

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Tue, 03 Aug 2010 02:45:37 GMT
View Forum Message <> Reply to Message

The AVG team got back to me and said "there was virus code in those files" (both RenegadeServer.exe and Register.exe were triggering AVG) and sent the following files back as clean files:
http://www.cncmods.net/files/clean.zip

Given that others have reported this issue, it sounds like the actual FDS installer on the Westwood FTP may be infected with this virus.

If anyone has any information one way or the other (I doubt that all the people with problems actually have a virus that infected their RenegadeServer.exe files separately) please post here.
I am going to send an email to the new EA community guy explaining the situation so they can possibly look into it.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Lone0001 on Tue, 03 Aug 2010 03:12:02 GMT
View Forum Message <> Reply to Message

I'm not sure about that tbh, it sounds like a false positive to me.

Try downloading this one:
http://downloads.cncfps.com/Westwood/renegade/dedicatedserver/renegade_fds_1037. exe I copied the entire westwood ftp and got it uploaded there, while downloading things I did not get any messages from my Anti-Virus (Nod32 ftw) saying something was infected.

PS. Is it the paid or free version of AVG? If free, why even use that still when Microsoft made a free Anti-Virus that would be 5x better, imo anyways.

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Tue, 03 Aug 2010 03:34:54 GMT
View Forum Message <> Reply to Message

Its the free version.
And the MS product is NOT better than AVG, at least not on Windows XP.

Also, its not an infection in renegadefds_1037.exe, its an infection in a file inside RenegadeFDS_1037.exe (which your AV isn't likely to pick up since AVs dont generally understand that particular installer format and cant scan inside it)

I seriously doubt the AVG people would have said "those files you send do contain a virus, here are clean versions" (the clean versions ARE different to the other versions btw) unless they actually DID contain a virus.

I downloaded
http://downloads.cncfps.com/Westwood/renegade/dedicatedserver/renegade_fds_1037. exe and unpacked it with an installer unpacker and the files in that one ALSO contain the virus.

The same register.exe (the one that causes AVG to trigger) was also shipped with various builds of RA:APB and was (after I told people to scan it) tripping several AV programs.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Lone0001 on Tue, 03 Aug 2010 04:07:47 GMT
View Forum Message <> Reply to Message

I'm still not sure tbh, I scanned a few copies register.exe (and renegadeserver.exe) from a few installers from a few different sources, none of them were detected as viruses, another Nod32 user (who also didn't detect them as viruses) I know has submitted both files to ESET (makers of Nod32) so I won't know for sure until he gets response back from them.

I'm not saying it's impossible that my AV could be wrong, that is still to be seen, I'm going to try a few different AVs now tbh.

Subject: Re: Possible virus in renegadeserver.exe
Posted by raven on Tue, 03 Aug 2010 04:19:30 GMT
View Forum Message <> Reply to Message

How odd..

both the RenegadeServer.exe executables were detected as viruses on the Jelly box.. they have since been replaced however its weird that this all just happened recently :\

Subject: Re: Possible virus in renegadeserver.exe
Posted by Craziac on Tue, 03 Aug 2010 04:35:48 GMT
View Forum Message <> Reply to Message

I suppose they just added the definition recently. How odd.

Subject: Re: Possible virus in renegadeserver.exe
Posted by snpr1101 on Tue, 03 Aug 2010 09:01:40 GMT
View Forum Message <> Reply to Message

IT'S A CONSPIRACY!

DUN DUN DUN

On a more serious note, this is quite odd, yes.

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Tue, 03 Aug 2010 09:46:51 GMT
View Forum Message <> Reply to Message

Per (the new community guy at EA) said this
"Thank you for the heads up. I'll send it to the studio so they can make sure it gets sorted."

Subject: Re: Possible virus in renegadeserver.exe
Posted by Sladewill on Tue, 03 Aug 2010 23:15:09 GMT
View Forum Message <> Reply to Message

Talking of this avast reported it as a virus the other day, my pc then went into meltdown deleted all the exe files on my pc coz loads of temp files we're getting created. Then the computer was unusable had to reinstall windows on it.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Rocko on Wed, 04 Aug 2010 05:29:12 GMT
View Forum Message <> Reply to Message

yos'is just axd my homboi dat werk at EA clinnin the john and he da 1 who told me dat some1 put da viriz up in der fo payback about renegade 2 mel gibson style

Subject: Re: Possible virus in renegadeserver.exe
Posted by trooprm02 on Wed, 11 Aug 2010 15:10:20 GMT
View Forum Message <> Reply to Message

I think just some style of code WW used as a "hack" to launch server.dat may have been copied (just by chance) in some new kind of virus/trojan...I wouldn't ever trust AVG, instead try uploading the individual .exe's to something like www.virustotal.com where it will be scanned by 20-30 different AV's at once.

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Fri, 13 Aug 2010 12:48:03 GMT
View Forum Message <> Reply to Message

3 things here:
1.I did submit it to virus-total and a few others picked it up as well as AVG
2.Others have reported things other than AVG picking it up
and 3.The AVG team (who are presumably experts in their field) would not have sent me an email saying "the file you submitted does contain a virus, here is a cleaned file" unless it actually did contain one

Subject: Re: Possible virus in renegadeserver.exe
Posted by Rocko on Fri, 13 Aug 2010 20:04:40 GMT
View Forum Message <> Reply to Message

you should try installing it and see what it does to really confirm if it does have a virus or not

Subject: Re: Possible virus in renegadeserver.exe
Posted by cnc95fan on Thu, 26 Aug 2010 18:50:51 GMT
View Forum Message <> Reply to Message

I just did a scan there and Avast! found that the Register.exe in APB BETA, WDUMP.exe from Renegade Public Tools, Register.exe from the FDS and RenegadeServer.exe all contained the same "Injected AZ" thing.. I downloaded my FDS from Game-Maps

Subject: Re: Possible virus in renegadeserver.exe
Posted by Gen_Blacky on Fri, 27 Aug 2010 05:15:02 GMT
View Forum Message <> Reply to Message

Must be a false positive the only thing RenegadeServer.exe does is launch server.dat and if crashes RenegadeServer.exe will restart server.dat. It might read some stuff from the config file. Like danpaul said just rename server.dat to somthing.exe and it will start the fds and if you close it wont try to restart. If you run server.dat instead of the luancher I think it will have problems with xwis.

Mine is the same as jonwills 92.0 KB (94,208 bytes). Microsoft
Security Essentials dosent pick anything up.

Subject: Re: Possible virus in renegadeserver.exe
Posted by The Party on Tue, 31 Aug 2010 01:06:35 GMT
View Forum Message <> Reply to Message

TrendMicro FTW!

Subject: Re: Possible virus in renegadeserver.exe
Posted by jonwil on Tue, 31 Aug 2010 04:35:18 GMT
View Forum Message <> Reply to Message

Regardless of what different anti-virus programs pick up (or don't pick up), the AVG people (who's day job is reverse engineering and disassembling viruses) said that the files I sent them contained viruses. If these experts say they contain viruses (and have supplied files that dont contain viruses) then that's good enough for me to assume that there was SOMETHING wrong with the files.

Subject: Re: Possible virus in renegadeserver.exe
Posted by halo2pac on Mon, 04 Oct 2010 02:11:56 GMT
View Forum Message <> Reply to Message

I believe the false positive comes from the register tool and the other exe checking the register for a 'serial' key. probably sends a harvesting Trojan false positive.

Subject: Re: Possible virus in renegadeserver.exe
Posted by Jerad2142 on Mon, 04 Oct 2010 03:41:59 GMT
View Forum Message <> Reply to Message

I also got that report of a virus a couple weeks ago (Symantec Flagged it), but I installed it

anyways assuming a false positive, and beings my computer is still running I believe it is thus.