

Re: Need help on home network with recovery from rbot.gen virus

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2008-02/msg00023.html>

- *From:* AyeKantSpeylGud <AyeKantSpeylGud@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sat, 9 Feb 2008 01:03:01 -0800
-

Hi Denzel,

I have to admit that I can totally understand your frustration with this. I came to this page looking for the exact same thing – I had a virus, a BUNCH of them, as well as spyware and other garbage that had done a number of things to make it next to impossible to get rid of them. One of the things it did was to turn off the ability to go straight to Windows Update. (It'd also turned off Control Panel, disabled Regedit, all saying that it'd been blocked by the system administrator, even though I AM the System Administrator!)

If I am personally understanding you correctly, you are simply asking for where in the registry you can turn it back on – now that you HAVE gotten rid of the virus! I am currently stuck in the same situation. If I find the answer, I will try to post it back here for you. Who knows though, it's been a few days, perhaps you've already found the answer!

Take care and best of luck!

Heather

"denzel" wrote:

Denzel,

If you have the original file, upload it to <http://www.virustotal.com> and report the results back here.

Regards,

Leonard Agoado
agoado@xxxxxxx

<http://www.virustotal.com/analysis/eb1fcb79ea86a866a31ca76bcc285695>

Re: Need help on home network with recovery from rbot.gen virus

Antivirus Version Last Update Result

AhnLab-V3 - - -

AntiVir - - BAT/RBot.94038

Authentium - - -

Avast - - Win32:Rbot-CYW

AVG - - IRC/BackDoor.SdBot3.XGI

BitDefender - - GenPack:Generic.Sdbot.4502EEEF

CAT-QuickHeal - - Backdoor.Rbot.fwe

ClamAV - - -

DrWeb - - Win32.HLLW.MyBot.based

eSafe - - suspicious Trojan/Worm

eTrust-Vet - - Win32/Rbot!generic

Ewido - - -

FileAdvisor - - -

Fortinet - - -

F-Prot - - -

F-Secure - - Backdoor.Win32.Rbot.fwe

Ikarus - - Backdoor.Win32.Rbot.aeu

Kaspersky - - Backdoor.Win32.Rbot.fwe

McAfee - - -

Microsoft - - Backdoor:Win32/Rbot.gen

NOD32v2 - - a variant of Win32/Rbot

Norman - - W32/Spybot.CKSQ

Panda - - W32/Sdbot.LMD.worm

Prevx1 - - Backdoor.IRCBot.gen

Re: Need help on home network with recovery from rbot.gen virus

Re: Need help on home network with recovery from rbot.gen virus

Rising -- Backdoor.Win32.Rbot.GEN

Sophos -- Mal/Generic-A

Sunbelt -- Backdoor.SDBot

Symantec ---

TheHacker ---

VBA32 -- Win32.HLLW.MyBot.based

VirusBuster ---

Webwasher-Gateway -- Worm.Rbot.210944

Additional information

MD5: fc216d7b5859115a618d3adc83359349

SHA1: 18a8897baa1b1ded75e221be47cd0841d305eb6f

SHA256: 73a3f914ca5f0c2ce76186288f4c8919ea73dbc0f4c5e13fc38806ec721cc6df

SHA512: 915653b73f83b657f9ed19806d3fdbcfd3857837245d5c18836972fd32002dfe

a6362bf50a7b335ed0f03d85b371cbcd28b0a18e681a24100145610b9c0ef567