

Backdoor.Sdbot Visus?????

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-02/2422.html

From: Euan Gamble (ewan@madprops.org)

Date: 02/21/03

From: "Euan Gamble" <ewan@madprops.org>

Date: Thu, 20 Feb 2003 21:10:10 -0800

I had the same problem.

Goto:

<http://securityresponse.symantec.com/avcenter/venc/data/backdoor.sdbot.b.html>

That has instructions at the bottom on how to remove.

Basically heres the MAIN bit:

1. Click Start, and click Run. The Run dialog box appears.
2. Type regedit and then click OK. The Registry Editor opens.
3. Navigate to the key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

4. In the right pane, delete the following value:

Configuration Loader syscfg32.exe

5. Navigate to the following key

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

6. In the right pane, delete the value

Configuration Loader syscfg32.exe

7. Exit the Registry Editor.

Good Luck. It worked for me.

>-----Original Message-----

>I have Norton Antivirus 2003 installed and i have the
>following virus

microsoft.public.windowsxp.security_admin: Backdoor.Sdbot Visus?????

>
> *Backdoor.Sdbot*
> *File Name : C:\System Volume*
> *Information : _restore{FBAB443A-41CB-4DE3-89C1-*
> *689FBE2EDD4B}\RP134\A0028752.EXE*
> *User Name : System*
>
> *Norton cannot repair or quarentine the file so i want to*
> *delete it but i cant find it. Ive searched for various*
> *strings in the name and im searching hidden files and*
> *system files but i cant find it. Does anyone know where*
> *this file is and how i get rid of it..*
>
> *Thanks.*
>
>