

Re: Backdoor.Ircbot.AV infection

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-11/2283.html>

From: melvin (*anonymous_at_discussions.microsoft.com*)

Date: 11/24/03

Date: Mon, 24 Nov 2003 09:54:50 -0800

Hello David;

Thanks for the quick response. I followed your instructions up to and including "Create a New System Restore Point". This went OK. When I ran the AV package, it reported no virus infection found. However, when I look in the Test Results, of the AVG package, and click on one of the files that is highlighted in red and click Detail Info, it still states I have an infected file. Please let me know what my my next step should be, if any. Thanks in advance. I really appreciate the help.
melvin

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

>Please read the following URL:

><http://vil.nai.com/vil/SystemHelpDocs/DisableSysRestore.htm>

>

>The objective:

>-----

>- Turn off the System Restore function

>- Reboot the PC

>- Using your AV package, perform a full scan of all files on the platform and clean/delete

> infectors found

>- Turn on the System Restore function

>- Reboot the PC

>- Create a new System Restore point.

>

>If you have problems, it can be done manually....

>

>Use the WinME floppy boot disk and boot from drive "A:"

>When you get to a DOS prompt enter the following command

>

>attrib -r -s -h c:_RESTORE

>rename c:_RESTORE c:\RESTORE.old

>

>Reboot the PC.

>

>In Windows delete the folder; c:\RESTORE.old
>
>Please report back your results.
>
>Dave
>
>
>"melvin" <anonymous@discussions.microsoft.com> wrote in
message
>news:02ce01c3b224\$0fe8d5f0\$a301280a@phx.gbl...
>| Hello;
>| AVG Antivirus informed me that my machine was infected
>| with the subject virus. I suspect it got into my machine
>| because I had not updated the virus file. I am running
>| Windows ME so I did a System Restore to an earlier date
>| which seems to got rid of it. When I look in the Test
>| Results in AVG, it states I have infected files named:
>| C:_Restore\Temp\A0149115 and A0149116. Was it an OK
>| procedure to use System Restore? Should I delete the
>| infected files or just leave them alone? As far as I can
>| determine my machine runs OK. Thanks for you help in
>| advance.
>
>
>
>