

Re: swen virus infected friends comp

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-09/4730.html>

From: helper (*there*)

Date: 09/29/03

Date: Sun, 28 Sep 2003 23:01:17 -0400

Remember the "Safe Mode" and disable System Restore.

Follow EXACT steps from:

<http://www.symantec.com/avcenter/venc/data/w32.swen.a@mm.removal.tool.html>

Such as:

Renaming FixSwen.exe to FixSwen.cmd. etc.

Most don't read the exact steps and those are unable to clean their system.

Another tool:

<http://www.f-secure.com/v-descs/swen.shtml#disinf>

"In some cases, when Swen executable is deleted or renamed by an anti-virus program without fixing the Registry, it becomes impossible to run executable files on a computer. This happens because Windows can't find the file associated with executables (in our case - Swen's file) on a hard disk. If you have such a problem, please download the following file:

[...]

Then rename the SWENFIX.EXE file with the name of deleted Swen's executable (that Windows asks for) and copy that file to Windows folder. After that you will be able to run the SWENTOOL.COM file to disinfect your computer. "
etc...

Just follow the steps.

"Sue" <> wrote in message news:005001c38630\$b2077050\$a001280a@phx.gbl...

> *A friend of mine fell for one of the microsoft update*
> *emails and now has the Swen worm roaming around her system*
> *causing all sorts of trouble. I have been trying to help*
> *her but I am not an expert. Can someone try and tell me*
> *what to do so I can pass the info onto her. I will try to*
> *be as specific as possible but not really knowing what*
> *happened exactly is kinda hard so please bear with me.*
>
> *First off, after realizing she unleashed the worm she went*

- > to the Symantec site and tried to d/l the Swen removal
- > tool but for some reason her comp is not letting her. She
- > has tried to follow the steps at Symantec as far as
- > removing registry entries but she can't. When she opens
- > Run to enter regedit she keeps getting an error. She can't
- > even get into msconfig. She can't open command prompt in
- > safe mode and the comp will not shut down when choosing
- > restart in MS Dos mode either. Her antivirus seems to be
- > working, it picked up 3 swen viruses during her last scan
- > this afternoon and she deleted them.
- >
- > She cannot open anything in the start menu or on the
- > desktop. She can get online but she can't d/l anything at
- > all, so she can't get the Hijack This program or anything.
- > She can't open OE or messenger either. She keeps getting
- > this error message when trying to open programs, including
- > regedit..
- >
- > Program not found. Windows cannot find VGCKJDTZ.exe This
- > program is needed for opening files of this type
- > application.
- >
- > She phoned her local comp shop and they said for her to
- > bring it in and they can fix it or she can try to fix it
- > herself. She can't fix it herself if she can't even get
- > into the areas she needs to in order 'fix' it. Can someone
- > help please? I hope I've made some sense. It's kinda of
- > hard explaining a situation when I am not the one
- > experiencing it. Is there another way to get into the
- > registry to delete this virus? Is VGCKJDTZ.exe a
- > legitimate windows file or something the virus put there?
- >
- > Thanks.
- >
- > ~S~
- >