

microsoft.public.windowsxp.security\_admin: Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

## Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

**Source:**

[http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security\\_admin/2002-06/4317.html](http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2002-06/4317.html)

---

**From:** Patty MacDuffie ([pattymacduffie@SENDSPAMHERE.attbi.com](mailto:pattymacduffie@SENDSPAMHERE.attbi.com))

**Date:** 06/30/02

From: "Patty MacDuffie" <[pattymacduffie@SENDSPAMHERE.attbi.com](mailto:pattymacduffie@SENDSPAMHERE.attbi.com)>

Date: Sat, 29 Jun 2002 21:13:17 -0700

Remove the virus manually as follows:

Manual removal procedure for Windows 2000/XP

1. Download virus definitions

Download the definitions using the Intelligent Updater. Save the file to the Windows desktop. This is a necessary first step to make sure that you have current definitions available later in the removal process. Intelligent Updater virus definitions are available at

<http://securityresponse.symantec.com/avcenter/defs.download.html>

For detailed instructions on how to download and install the Intelligent Updater virus definitions from the Symantec Security Response Web site, read the document How to update virus definition files using the Intelligent Updater.

2. Restart the computer in Safe mode

- a. Shut down the computer and turn off the power. Wait thirty seconds. Do not skip this step.
- b. You must do this as the first step. All Windows 32-bit operating systems except Windows NT can be restarted in Safe mode. Read the document for your operating system.
  - a.. How to start Windows XP in Safe mode
  - b.. How to start Windows 2000 in Safe mode

3. Edit the registry

You must edit the key HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services and remove the wink[random characters].exe subkey after you write down the exact name of the wink file.

**CAUTION:** We strongly recommend that you back up the system registry before you make any changes. Incorrect changes to the registry could result in permanent data loss or corrupted files. Please make sure that you modify only the keys that are specified. Please see the document How to back up the Windows registry before you proceed.

- a. Click Start, and click Run. The Run dialog box appears.
- b. Type regedit and then click OK. The Registry Editor opens.
- c. Navigate to the following key:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services

Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

microsoft.public.windowsxp.security\_admin: Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

d. In the left pane, under the \Services key, look for the following subkey:

\Wink[random characters]

e. Write down the exact file name of the Wink[random characters].exe file

f. Delete the Wink[random characters] subkey.

g. Navigate to the following key:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

h. In the right pane, look for the following values, and delete them if they exist:

Wink[random characters] %System%\Wink[random characters].exe

WQK %System%\Wqk.exe

NOTE: They probably will not exist on Windows 2000/XP-based computers, but you should check for them anyway.

i. Click Registry, and click Exit.

4. Configure Windows to show all files

Do not skip these steps:

a. Start Windows Explorer.

b. Click the Tools menu, and click "Folder options."

c. Click the View tab.

d. Uncheck "Hide file extensions for known file types."

e. Uncheck "Hide protected operating system files," and under the "Hidden files" folder, click "Show hidden files and folders."

f. Click Apply, and then click OK.

5. Delete the actual Wink[random characters] file

Using Windows Explorer, open the C:\Winnt\System folder and locate the Wink[random characters].exe file. (Depending on your system settings, the .exe extension may not be displayed.)

NOTE: If you have Windows installed to a location other than C:\Windows, make the appropriate substitution.

6. Empty the Recycle Bin

Right-click the Recycle Bin on the Windows desktop, and click Empty Recycle Bin.

7. Run the Intelligent Updater

Double-click the file that you downloaded in Step 1. Click Yes or OK if you are prompted.

8. Restart the computer

Shut down the computer, and turn off the power. Wait 30 seconds, and then restart it.

CAUTION: This step is very important. Reinfection will occur if this is not followed.

Allow the computer to start normally. If any files are detected as infected by W32.Klez.H@mm or W32.Klez.gen@mm, Quarantine them. Some of the files that you may find are Luall.exe, Rescue32.exe, and Nmain.exe.

Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

microsoft.public.windowsxp.security\_admin: Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

9. Scan with Norton AntiVirus (NAV) from the command line

Because some NAV files were damaged by the worm, you must scan from the command line.

NOTE: These instructions are only for consumer versions of NAV. The file Navw32.exe is not part of Enterprise versions of NAV such as NAVCE. The NAVCE command line scanner, Vpscan.exe, will not remove the worm.

- a. Click Start, and click Run.
- b. Type—or copy and paste—the following, and then click OK:

```
NAVW32.EXE /L /VISIBLE
```

- c. Allow the scan to run. Quarantine any additional files that are detected.

10. Reinstall NAV

NOTE: If you are using NAV 2002 on Windows XP, this may not be possible on all systems. You can, however, try the following: Open the Control Panel, double-click Administrative Tools, and then double-click Services. In the list, select Windows Installer. Click Action, and then click Start.

Follow the instructions in the document How to restore Norton AntiVirus after removing a virus to reinstall NAV.

11. Restart the computer and scan again

- a. Shut down the computer, and turn off the power. Wait 30 seconds and then restart it.

CAUTION: This step is very important. Reinfection will occur if this is not followed.

- b. Run LiveUpdate and download the most current virus definitions.
- c. Start Norton AntiVirus (NAV), and make sure that NAV is configured to scan all files. For instructions on how to do this, read the document How to configure Norton AntiVirus to scan all files.
- d. Run a full system scan. Quarantine any files that are detected as infected by W32.Klez.H@mm or W32.Klez.gen@mm.

```
--
Patty MacDuffie
Windows XP MVP
"Ates" <ates1@cox.net> wrote in message news:1191601c21fba$47d896b0$37ef2ecf@TKMSFTNGXA13...
>-----Original Message-----
>
>>-----Original Message-----
>>Thanks for your reply!!!!
>>But I did read the readme and ran it! Then I watched
the
>>cleaner not being able to access a bunch of file and
>>final outcome was that i do not have it?????
>>
>>When I went into my system folder the WQK folder where
>>still there and i disabled system restore 2!!
>>
>>Nortons cleaner gets changed the moment i store it!!!
>>
>>Any other shots????
>>
>>By the way I think my regedit is tempered too! My run
```

Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

microsoft.public.windowsxp.security\_admin: Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

```
>>folder is completely empty and like i said: a lot my
>>programms seem to think i am running nt not xp!!!
>>Another folder is my downloads folder: when i open it
>it,
>>the appearance of explorer changes it seems to jump to
>>classic view and i think i am getting a snapshot view
of
>>the folder, which should be containing more files as
the
>>properties say but i only see 6 class files, which i
>>deleted and next time i check the folder it is the same
>>view!!!
>>
>>Help, Help, Help!!!!
>>>-----Original Message-----
>>>http://www.trendmicro.com/vinfo/virusencyclo/default5.a
s
>p
>>?
>>>VName=WORM_KLEZ.E Go to this page for info on how to
>>>remove. If you use the fixtool you must read
>>>the "readme"
>>>file first. I have used this tool successfully. Or if
>>>its
>>>your fancy you can try the manual procedure. Be sure
to
>>>disable System Restore (Control Panel-->System) before
>>>you
>>>attempt to remove virus. Then run Housecall to remove
>>>all
>>>infected files.
>>>>-----Original Message-----
>>>>I know i have the klez.e on my computer and i do not
>>>>know
>>>>if there is another one! Removal tools do not work
>>>>because the system fakes a different environment for
>>>>the
>>>>scanners and i think all scanners get disabled by
>this.
>>I
>>>>can not detect where it is all hidden, because I just
>>>>recently restored my hard drives and even tried to
>>>>flush
>>>>my bios by removing my battery, but it is back again!
>>My
>>>>bootssystem is supposed to be my d drive, but all my
>>>>system files have been moved to c drive again. It
also
>>>>identifies itself as Windows NT, whereas I have XP
>>>>professional. I can see in the reg files that it is
>>>>faking the current version of all programms and
>>>>updates!!!
>>>>Yesterday I tried to install the latest update and
>>>>after
>>>>downloading and starting it, it ended at the second
>>>>notch
>>>>of the progress bar and said that the update was
>>>>installed successfully! Another issue I have is that
>>>>when
>>>>i checked my directories with Norton Utilities I saw
>>>>files that I can not see with explorer expext in the
>>>>properties. This could be from the fact besides
```

Re: KLEZ.E nasty problems!! HELP PLEASE !!!!

