

Re: beat the new worm from support@microsoft

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-05/1885.html>

From: Super_Geek (*RichardFalconer_at_thepostmaster.net*)

Date: 05/30/03

Date: Fri, 30 May 2003 10:04:27 +0100

sgopus asks a question to do with PCs, Super_Geek dives in and tries to help:

*>A better way is not open the damn attachment in the first
>place, be intelligent enough to wonder why microsoft would
>send out a non requested file with an attachment.
...and the irony of it is that it says it's a security patch.*

Sgopus (see first post,) describes a suitable method of stopping the process in a Win2k+ Os. However, if you are using Win9x, things are a little different.

The easiest method for removing most Viruses (or Virii as some say,) for which you know the file name is simple. Go to regedit and delete the key in:

[Reg directory is long and may wrap.]

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\
...that points to the file.

Then you can restart, and delete the file without getting the message 'This file is being used by Windows.'

HOWEVER, the more clever (if such a word can be used for people who cause so much damage to the ICT world,) virus authors now set the virus to re-create the reg key every few seconds. So that first method doesn't work any more.

So, boot into DOS...

The virus shouldn't run in the DOS memory, (hopefully!) because there are no start-up reg keys to call it. However, if hineman.sys or something has been infected, this method may also prove unsuccessful.

- 1) Boot do DOS, as I've said.
- 2) You'll see something like 'C:>_' if so, go to '4)'
- 3) If you see D:\, or another drive letter, type c: and hit return. If you see C:>yadda\yadda\yadaa type 'cd..' a few times.
- 4) Now type 'cd Windows' (or try 'cd Window~1' if that doesn't work,)
- 5) Type 'del x' where x is the name of the virus.
- 6) type win or exit
- 7) PC restarts, virus gone.

microsoft.public.security: Re: beat the new worm from support@microsoft

NB: You should still delete the reg key now that the virus is not there to re-create it.

Now there is one more method you can use, but it involves downloading tlist.exe and kill.exe; which are two useful DOS programs.

Unfortunately, although I have a copy, I don't have a link for you guys/gals.

If people are interested, I'll put them on my webserver.

HTH!

--

Super_Geek, 15

"If you can't beat your computer at chess, try kickboxing."