

Re: wins32.exe – virus? trojan? malware?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2005-07/0062.html>

From: Art (null_at_zilch.com)

Date: 07/05/05

Date: Tue, 05 Jul 2005 18:21:57 GMT

On Tue, 5 Jul 2005 12:11:55 -0400, "MJ" <mstanton@nospam.matrixcc.com> wrote:

*>We noticed the other day that no one could access any network shares on one
>of our W2k servers. This happened once before, and we found a
>virus/worm/trojan (whatever you want to call it) that was the culprit. So
>we ran new virus scans and spyware scans and found nothing. However, in the
>registry under HKLM/Software/Microsoft/Windows/CurrentVersion/Run – there
>was an entry for wins32.exe. Googling this filename turned up many results
>listing the file as a worm/trojan, but none of the descriptions of where to
>find it and how to get rid of it worked. In the registry the name is
>wins32.exe and the data says C:\Windows\System32\wins32.exe. When we delete
>the registry entry, it recreates itself. In the system32 folder you can
>only see it if you uncheck "Hide protected operating system files". We
>renamed it there, whacked the registry entry again, but it still returns –
>recreating itself as a hidden system32 file and in the registry. Luckily,
>this server is not critical to our day-to-day operations, so we've unplugged
>it from the network. This file does not exist in any of our other W2k
>Servers, so we're pretty sure it's a bad file. We are just at our wits end
>trying to remove it!! Any help/ideas would be greatly appreciated!!*

I suppose you tried this removal procedure?:

http://www.spywareguide.com/product_show.php?id=615

Working with just file names and no malware name is difficult since often there are several different malwares that use the same file name(s). Your best bet is to do a scan of the drive(s) using a real "heavy hitter" like KAV, assuming you haven't. Requests for help should always include the names of the av and spyware products you've already tried since their capabilities vary. Did you try Trend's Sysclean, for example?

Also, it's best to post such help requests on alt.comp.virus

Art