

## Re: trojan horse downloader.winshow.v

**Source:**

<http://www.tech-archive.net/Archive/Scripting/microsoft.public.scripting.virus.discussion/2004-04/0416.html>

---

**From:** Bill Sanderson (*Bill\_Sanderson\_at\_msn.com.plugh.org*)

**Date:** 04/27/04

Date: Tue, 27 Apr 2004 13:05:06 -0400

This is another CoolWebSearch variant, which CWShredder should remove.

It sounds as though you are rather infested—and probably haven't applied critical patches to your OS which would prevent some of these issues:

The info you need to help prevent the recurrence is in the three steps here:

[www.microsoft.com/protect](http://www.microsoft.com/protect)

All three steps are important, and don't cost \$ other than connect time.

In terms of cleanup, I'd recommend the following apps:

1) CWShredder—download fresh if it has been some days since the last download:

[www.aumha.org/freeware.htm](http://www.aumha.org/freeware.htm)

2) Lavasoft's Ad-Aware and Spybot Search & destroy:

[www.lavasoftusa.com](http://www.lavasoftusa.com)

[www.safer-networking.org](http://www.safer-networking.org)

Download, install.

Run, and on the first run, update to the latest set of definitions and other updateable parts, if any.

Scan your machine with both Ad-Aware, and Spybot Search & destroy.

Remove everything Ad-aware flags.

Remove everything Spybot Search & Destroy flags in red.

If you still have this issue, the next step would be to run HijackThis from the AUMHA link above, and post your log in the Spyware forums referenced in the explanatory text about the download there. However, get cleaned up with the free apps above first.

<anonymous@discussions.microsoft.com> wrote in message  
news:4f7e01c42c72\$e28c83d0\$a501280a@phx.gbl...

>

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

>>

>>><anonymous@discussions.microsoft.com> wrote in message

>>>news:4d2f01c42c6b\$be38e8e0\$a601280a@phx.gbl...

>>>>

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

>>>>>Although the URL might seem strange at first look, I

> can

>>> vouch for the fact

>>>>that this is an appropriate, safe place to download

> this

>>> specialized

>>>>ad/spy-ware removal tool.

>>>>>

>>>>>Here's another: [www.aumha.org/freeware.htm](http://www.aumha.org/freeware.htm)

>>>>>

>>>>>This site has some explanatory text you can read before

>>> downloading.

>>>>>

>>>>>This is a specialized tool for removing the

>>> CoolWebSearch family of search

>>>>hijackers--it's been around a good long time, and is

>>> quite refined and safe

>>>>in its actions at this point.

>>>>>

>>>>>I haven't researched your bug to be certain it is

>>> covered, but this is a

>>>>safe action to take--i.e. downloading CWShredder,

>>> unzipping, and running it.

>>>>>

>>>>><anonymous@discussions.microsoft.com> wrote in message

>>>>>news:4c7701c42c5e\$d2290c70\$a401280a@phx.gbl...

>>>>>>

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

>>>>>>>Download the following file and run it.

>>>>>>>

>>>>>>>><http://209.133.47.200/~merijn/files/CWShredder.exe>

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

>>>>>>>>>my computer has this virus!!

>>>>>>>>>could anybody tell me how to fix this!???. thanks!!!

>>>>>>>>>.

>>>>>>>>>>

>>>>>>>>>>.

>>>>>>>>>>

>>>>>>>>>> What will happen when i run this file?

>>>>>>>>>> just for curiosity!?

>>>>>>>>>> ;)

>>>>>>>>>>

>>>>  
>>>>.  
>>>>  
>>> *I have already run the first file, and the problem  
> still  
>>> there!!  
>>> Do you know any other way?  
>>  
>> Say more about what is happening:  
>>  
>> My guess--you haven't said, is that AVG antivirus has  
> identified this bug as  
>> existing somewhere on your system--is this correct?  
>>  
>> Where on your system does it say it is? The pathname is  
> what is needed.  
>>  
>> When you ran CWShredder--did it state that it found and  
> removed the bug?  
>>  
>> Did the location change? Is it in a path including  
> system\_restore in the  
>> name?  
>>  
>> If the bug is now in the System\_restore folders, this  
> fix will take care of  
>> it in Windows XP:  
>>  
>> Read the message very nearly at the end of the thread  
> about how to remove  
>> the bug from the system restore storage area:  
>>  
>> [http://computercops.info/modules.php?](http://computercops.info/modules.php?name=Forums&file=viewtopic&p=149908)  
> name=Forums&file=viewtopic&p=149908  
>>  
>>  
>>  
>>.  
>> c:\winnt\winwo\winwo32.dll  
> a think the problem of that trojan is solved!!  
> but now theres another one, when i try to open IE, the  
> homepage that i choose to be my first is not appearing,  
> instead of one wich is "<http://nkvd.us>" i think this is  
> one virus who's called "trojan.bootconf"!!  
> a don't know what to do more...*