

Re: Spyware disallows Safe Mode

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2004-06/10547.html

From: Will Denny (willdenny_at_mvps.org)

Date: 06/30/04

Date: Wed, 30 Jun 2004 05:21:42 +0100

Hi Steve

<http://202.28.24.50> resolves to Chaingmai University. Try the following programs to what spyware your system may have:

Ad-Aware – www.lavasoftusa.com

Spybot – <http://www.safer-networking.org/>

CWShredder – <http://www.spywareinfo.com/~merijn/downloads.html>

Try SpyWareBlaster to stop intrusions:

<http://www.javacoolsoftware.com/spywareblaster.html>

Also see the following links:

<http://mvps.org/winhelp2002/unwanted.htm>

<http://www.microsoft.com/security/articles/spyware.asp>

I've used AVG for years, which hasn't let me down. There is a free version available:

http://www.grisoft.com/us/us_dwnl_free.php

Failing that, there are several good online virus scanners, although they do take some time to run:

http://www.pandasoftware.com/activescan/com/activescan_principal.htm

--

Will Denny

MS-MVP Windows - Shell/User

Please reply to the News Groups

"Steve" <steve.NOMEATPLEASEthornburg@mindspeedOMITcom.NOMEATPLEASE> wrote in message news:EDA03DEE-01EE-4A82-9E47-4184A23C117F@microsoft.com...

| Hello Will,

| Thanks for your response, and for your patience. I apologize for not providing better detail in my original post.

| I am trying to boot into safe mode to see if any scanner (AV or spyware) will have better luck identifying this thing, and also hoping that it will

microsoft.public.windowsxp.help_and_support: Re: Spyware disallows Safe Mode

not keep presenting pop-ups while in safe mode. Maybe then I could sift through the registry and find something that would help. Yes, I can get into "normal" mode - that's the only mode I can get into.

| Perhaps this is not spyware, but some kind of worm or trojan or something. I have no idea how it got into my system, as I have all the latest patches and updates, and always disconnect everything when not online. I have only dial-up access, so even my IP changes whenever I connect. However, something got in, and it is proving difficult to identify and remove.

| I had already tried using msconfig; it was one of the first things I did. Still can not boot into safe mode. And there is no "restart in safe mode" on the menu. I'm not sure, but I think there was, but maybe I am thinking of a different OS.

| Here is some additional, newly discovered, information:

| While tinkering with this issue, I noticed that there was a great deal of outbound traffic as soon as I connected to the internet. So I disconnected, when over to my daughters and downloaded ZoneAlarm, and took it home to install it. What I found is that ZoneAlarm is not asking me if I want to allow it to sent traffic - it sends regardless.

| Whenever I start my browser, it now points to something at <http://202.28.24.50> (normally, my home page is set to google.com).

| So I am believing that this is some kind of worm/trojan/spyware/whatever that has messed things up. I was hoping to find out what it is, so I could report it to the various places that make AV and/or spyware scanners, but maybe I will just format the drive and re-install XP again. I have all my stuff backed up, and have all my original CDs for the few applications I have installed.

| Thanks again for your response. I hope I've answered your questions this time.

| Steve

| --

| ST

| "Will Denny" wrote:

| > Hi

| >

| > Are you trying to boot into Safe Mode because you can't boot into 'Normal'

| > Mode? If not, why are you trying to access Safe Mode. Spyware wouldn't

| > disallow access to Safe Mode. You may have some other underlying problem.

| >

| > If you can access XP - go to msconfig>boot.ini and enable the /SAFEBOOT > option.

| >

| > --

| >

| > Will Denny

| > MS-MVP Windows - Shell/User

| > Please reply to the News Groups

| >

| >

| > "Steve" <steve.NOMEATPLEASEthornburg@mindspeedOMITcom.NOMEATPLEASE>

wrote in

| > message news:247FBD3B-9C33-4C22-BE55-EE8579063EE3@microsoft.com...

| > | Hello Will,

| > |

| > | Thanks for the response. I did not say what it is because I don't know.

| > | The pop-ups only say "Click here to purchase Ad Stopper, and you will

microsoft.public.windowsxp.help_and_support: Re: Spyware disallows Safe Mode

```
never
| > see these Ads again!"
| > | But I can't tell what the URL is, right-click is disabled, and I don't
| > want to risk clicking on the darn thing.
| > | As for what is preventing getting into safe mode... there is NO safe
mode
| > entry in the menu that F8 brings up (and it used to be there!).
| > | Somehow, this software has removed it. I'm trying to find out about
| > boot.ini, to see if something in it would allow or disallow safe mode.
| > Currently, the F8 menu has only 1 choice: "Microsoft Windows XP
| > Professional"
| > | If I remember right, boot.ini can have a "safeboot" switch in it
(maybe?),
| > but I am not sure of the syntax, nor do I know how to edit the file if I
| > boot to DOS via floppy. I think I have to change the file attributes
first,
| > before I can edit it.
| > | It is not accessible from Windows. I can see it, but when I try to
open it
| > with Notepad I get a "file in use" error.
| > | --
| > | ST
| > |
| > |
| > | "Will Denny" wrote:
| > |
| > | > Hi
| > | >
| > | > You don't say what this 'awful thing' is. What is preventing you
| > accessing
| > | > Safe Mode?
| > | >
| > | > --
| > | >
| > | > Will Denny
| > | > MS-MVP Windows - Shell/User
| > | > Please reply to the News Groups
| > | >
| > | > "Steve" <steve.NOMEATPLEASEthornburg@mindspeedOMITcom.NOMEATPLEASE>
| > wrote in
| > | > message news:25BBF17B-6065-4D87-996E-F632D51E3571@microsoft.com...
| > | > | Some spyware that got into my machine keeps giving me pop-ups.
SpyBot,
| > | > Ad-Aware, The Cleaner, SpySweeper... nothing removes this awful
thing.
| > | > | When I try to boot into safe mode via F8 at startup, there is no
| > | > longer a
| > | > safe mode option! Somehow, this software has defeated the ability,
but I
| > | > don't know enough about how these things work. Is the file boot.ini
| > | > something that would control safe mode, and if so, how do I edit it
if I
| > | > boot to DOS via floppy?
| > | > | Any advice greatly appreciated.
| > | > | If you want to CC me, use
| > | > | steve.NOMEATPLEASEthornburg@mindspeedOMITcom.NOMEATPLEASE edited
| > | > | accordingly.
| > | > | Thanks!!
| > | > | --
| > | > | ST
| > | > |
```

microsoft.public.windowsxp.help_and_support: Re: Spyware disallows Safe Mode

| > | >
| >
| >