

## Re: Trojan Horse = BackDoor.Agent.BA + Startpage

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-07/1593.html>

---

**From:** cafmenace (*cafmenace.19tlc3\_at\_mail.mcse.ms*)

**Date:** 07/22/04

Date: Thu, 22 Jul 2004 15:04:26 -0500

I have a very similar problem, same exact characteristics mentioned below but under a different name. I'm dealing with a virus called backdoor.trojan and I have pin pointed the file it's associated with as wdma.dll. Tried everything John posted below too but still to no avail. Please I'll really appreciate if someone could help. Thanks

John wrote:

- > *\*Hi All:*
- >
- > *Man, oh man...have I gotten nailed! Ouch! These viruses*
- > *came out of nowhere and nailed my machine. It installed*
- > *itself 6/20. I have literally spent 2 days trying*
- > *everything I know.*
- >
- > *Some background information...*
- >
- > *1. I am a fanatic about getting XP updates.*
- > *2. I have Norton AV and it doesn't even pick this one*
- > *(the backdoor.ba job) up. Norton AV found the StartPage*
- > *virus but failed to fix or delete it.*
- > *2a. This (BackDoor) was detected by AVG 6.0 (a free*
- > *download); but not by Norton AV.*
- > *2b. AdAware 6.181 will find the "bad" registry entries*
- > *related to StartPage and quarantine them...but they come*
- > *back like herpes.*
- > *3. I have tried doing all the following (to no avail).*
- >
- > *A. Disabled System Restore*
- > *B. Rebooted in Safe Mode*
- > *C. Ran "regedit" and deleted the entries made in the*
- > *registry. They are found in HKEY CURRENT USER and HKEY*
- > *LOCAL MACHINE registries.*
- > *D. I followed the instructions on Symantec's website to*
- > *kill off StartPage (like 4 times) and it has totally*
- > *failed.*

>  
> *Question #1:*  
>  
> *With regard to the StartPage issue – Is there ANYBODY who*  
> *can help? The whole family is sick and tired of seeing*  
> *the damned "about:blank" home page. So am I.*  
>  
> *Can anyone tell me what file in the system files keeps*  
> *propogating the registry entries (8 or 9 of them)?*  
>  
> *Question #2:*  
>  
> *With regard to the BackDoor.Agent.BA issue. I have*  
> *isolated the file to "winpa.dll" that seems to be the*  
> *problem. How can I delete it!?*  
>  
> *Renaming the file don't work (tried that). You still get*  
> *the AVG warning. Then I tried changing the attributes*  
> *(read only to something else)...no dice. Can't delete it*  
> *either.*  
>  
> *For now, I renamed it...but I keep getting messages that*  
> *it is infected with the backdoor.agent.BA virus.*  
>  
> *Can anybody please help?*  
>  
> *Reply offline to John\_C\_Eberle@msn.com*  
>  
> *DO NOT SEND A FILE ATTACHMENT. :-) \**

--  
cafmenace

-----  
Posted via <http://www.mcse.ms>

-----  
View this thread: <http://www.mcse.ms/message800918.html>