

Re: backdoor.afcore.bb HELL

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-02/0267.html>

From: Shewman (shewman_at_sympatico.ca)

Date: 02/03/04

Date: Mon, 2 Feb 2004 22:33:00 -0500

OK, here's how I got rid of afcore.bb:

- uninstalled the offending DLL
- got rid of the existing anti-virus program AVG and had her install Norton
- Norton found 2 offending programs, AF.EXE and audio.exe
- reboot and now everything is fine.

"Sandi - Microsoft MVP" <sandi_hardmeier@mvp.org> wrote in message news:u0WTgk%235DHA.2064@TK2MSFTNGP11.phx.gbl...

- > *The problem with some malware, is it will recreate itself (with new *.dll*
- > *names) as soon as it detects that one of its processes have been shut down*
- > *or files*
- > *have been deleted. There are two programmes, not just one.. one of which*
- > *is*
- > *the classic malware, the other is a monitoring service that restarts the*
- > *malware as soon as it detects the other is deleted, complete with new file*
- > *names.*
- >
- > *I would use MSCONFIG and select 'diagnostic startup' to run only basic*
- > *services. Then track down and nuke the malware and all associated files*
- > *that*
- > *I could find, using registry entries and MSCONFIG itself to track down as*
- > *many associated files as I could find.*
- >
- > *I note that your friend is a long way away. I really don't think this is*
- > *something that can be done remotely. If the reinfecter is missed, you're*
- > *back to square one.*

>
> --

> _____
> Sandi - Microsoft MVP since 1999 (IE/OE)
> <http://www.mvps.org/inetexplorer>

>
> "Shewman" <shewman@sympatico.ca> wrote in message
> news:_cDSb.44891\$mf4.1596318@news20.bellglobal.com...
> > Hi,

>>
>> *I've got a friend who has this trojan. I can't get rid of it. Found it*

in

> > *the registry and deleted the entries. Rebooted but the entries get added*
> > *again. Tried uninstalling the dll, ftdpwmk.dll, but I get access denied.*
> > *Everytime, I try another i.e. view processes, her PC reboots. Went into*
> > *safe*
> > *mode but I can't find the source file(s).*
> >
> > *I've tried searching google but didn't find anything. Also tried*
searching
> > *Norton and sophos*
> >
> > *Anyone have any ideas??? It's an XP PC. Unfortunately, she's a couple of*
> > *hundred miles away. But I can remote into the PC.*
> >
> > *Thanks*
> >
> >
> >
>