

## Re: Program that disables my anti-virus

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-08/0761.html>

---

**From:** Stefan Kanthak (*postmaster\_at\_1.0.0.127.in-addr.arpa*)

**Date:** 08/28/05

Date: Sun, 28 Aug 2005 19:08:51 +0200

"Patrick Dickey" <pd1ckey43@msn.com.removethis> wrote:

Your email address is wrong!

<http://www.ietf.org/rfc/rfc1855.txt> tells you netiquette.

> *C L via WinServerKB.com wrote:*

> > *Hey guys, my wife clicked a link on MSN messenger that said "hey check this*

> > *out ....blah blah blah.*

> > *She said her friend was pretty intent on her looking at it. I checked the*

> > *message history and found that she was getting this message every 2 minutes*

> > *or so. I figured that it was a virus or something so I went to do a scan*

> > *with Norton AV 2005. It turns out it was disabled. I never disable it and*

> > *my wife wouldn't know how to do it either. So I try to enable it but it*

> > *won't. So I tried to uninstall NAV and reinstall it but I keep getting an*

> > *error. Saying "internal error 2753.SAVScan.exe.3333244E....."*

> > *Also I can't visit the symantec web site or other various anti virus websites.*

> >

> > *So I downloaded McAfee ran that and it found a trojan.*

> > *I still an't visit anti virus web sites though. Any ideas?*

Read <http://www.microsoft.com/technet/community/columns/secmgmt/sm0504.msp>

The system has been compromised, installed software even damaged, so the

ONLY correct action is: flatten and rebuild!

Any other proposal is both ridiculous and risky. You can't trust your

system any more. It might be a spam bot now, or worse!

> *You need to edit your HOSTS file and remove the references to the*

> *antivirus sites. Your HOSTS file is either in C:\Windows (Windows 9x)*

> *or C:\Windows\System32\drivers\etc and you'll use Notepad to edit it.*

> *Remove ONLY the references to the antivirus sites. The one that*

> *absolutely HAS to stay is 127.0.0.1 localhost. If there are others in*

> *there, and they redirect to 127.0.0.1 ask in here before removing them*

> *(unless they are for an antivirus site).*

Snakeoil! The malware is still active! If it was able to modify the hosts file it ran with administrative rights. That's a no-no!

microsoft.public.security: Re: Program that disables my anti-virus

- > *Also, try going to*
- > *[http://housecall.antivirus.com/housecall/start\\_corp.asp](http://housecall.antivirus.com/housecall/start_corp.asp) and running that*
- > *scan. Make sure you have the Auto Clean option checked before you start.*

You can't trust the system any more. The scan results might be tampered.

- > *You may also want to check out the [public.microsoft.msn.messenger](http://public.microsoft.msn.messenger)*
- > *newsgroup and [public.microsoft.msn.discussion](http://public.microsoft.msn.discussion) newsgroup. If you're on*
- > *webnews, look for [public.microsoft.msn](http://public.microsoft.msn) and click the + by it.*

No, that's useless. If MSN messenger is insecure or the OP's wife doesn't know how to handle this program: uninstall it.

Don't trust on Norton or other anti-X-tool: it wasn't able to protect the system this time, and it won't be able the next time too!

Don't run your system as administrator, create restricted accounts!

Keep your system up-to-date.

Uninstall all programs and components you don't use, minimizing the attack surface.

Secure/configure ALL programs you use properly.

Turn off all unused services (see <http://www.ntsvcfg.de/>), minimize the attack surface.

If you can't do this yourself: let someone EXPERIENCED setup the system for you (no, not your neighbor's kid!).

Stefan