

Re: Do I have TOO MANY antivirus, antispyware, etc

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-01/msg00561.html

- *From:* nursing major needs help <nursingmajorneedshelp@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 10 Jan 2006 22:02:02 -0800
-

Thanks to all of you. The info is very helpful. I will try and let you know how it goes.

"cquirke (MVP Windows shell/user)" wrote:

- > On Mon, 9 Jan 2006 01:41:02 -0800, nursing major needs help
- >
- >>I used to be internet-free. Now I have been on-line for a little over a year
- >>and I never had any anti-anything. My computer started getting retarted and I
- >>downloaded and installed the EZ anti-everything offered with my ISP. It
- >>seemed to only slow things down and didn't protect me from the Win32/sober
- >>something-or-another that sent me like 300 e-mails a day. So I went to the
- >>store and bought Norton Anti-virus, Webroot's Spy Sweeper, and installed
- >>Microsoft's Anti-spyware. I got rid of about 30 viruses and a trojan dropper
- >>and some ad stuff. Everything was working fine...for about 3 months. Now my
- >>computer is retarted again and I ran the Windows Live Safety Center Scan,
- >>which detected and deleted yet another virus. None of the others found it. I
- >>am so confused. Please tell me what I am doing wrong or what I should do.
- >
- > Your problems are:
- >
- > 1) You never formally cleaned up your system after finally getting av
- >
- > 2) You are relying on av (antivirus) to keep you safe
- >
- >
- > On (1); you are pretty much doomed as soon as you take a
- > standard-install Windows XP system online without any firewall or
- > antivirus, if the Service Pack level of XP is older than SP2.
- >
- > A "Service Pack" is basically a vast collection of bugfixes, almost
- > constituting a re-write of the Operating System (OS), and Windows XP
- > have had two of these to date.
- >
- > So once you wised up, you needed to first formally scan for and remove
- > all active malware. You didn't do this; what you did was install
- > various antivirus (av) from the infected OS and hope these would be

Re: Do I have TOO MANY antivirus, antispysware, etc

- > able to sort things out. This sometimes works, but personally I
- > wouldn't expect it to, and would be unsurprised when it doesn't.
- >
- > Once malware infects the system, it generally runs as soon as the
- > system does. So it is in a position to disable antivirus and other
- > defence apps, foil attempts to update these, and so on.
- >
- > To tackle malware that is already on the system, you should scan and
- > remove these while the infected OS is not running. This should be as
- > easy to do today as it was in the DOS days of booting a diskette and
- > then running an av on another diskette, but it isn't, because MS does
- > not provide the tools from which an av can be formally run.
- >
- > Fortunately, someone else does – in the form of Bart PE – but it's a
- > bit of a mission setting this up, and a bigger mission setting up your
- > av tools etc. to work from it. Probably best to find a tech with a
- > clue about such matters (if you hear "just re-install Windows", then
- > spit out the frog bones and keep looking!).
- >
- >
- > On (2), your firewall is the first defense, and your antivirus is the
- > "goalie of last resort". Between these, should range your other
- > defenses; patches to repair the endless stream of software defects,
- > risk management to avoid some stupid risks the OS may take "for you",
- > a smarter choice of edge-facing applications, and "safe hex", i.e. the
- > skill to know what constitutes hi-risk and to avoid such things.
- >
- > If the av unexpectedly pops up saying it "caught" something, don't
- > feel happy your av is working. Feel worried that some malware got
- > close enough to take a shot, and relieved that the av caught it...
- > this time. NO av will ever catch anything, so the fact that the av
- > caught something now, implies it may have already missed other stuff!
- >
- > The reasons an av will not catch everything, are:
- >
- > a) Some malware are not considered "viruses"
- >
- > "If it's not a 'virus', then it's not our problem", is the attitude of
- > the traditional av vendor. Such non-viral malware may include bots
- > that may be dropped from hostile web sites etc. be spammed to you via
- > email, or enter the system as downloaded "media" files via Kazaa and
- > similar file sharing applications. In particular, commercial malware
- > ("spyware") is very likely to be missed by av, although some av have
- > recently developed pretensions and ambitions in this regard.
- >
- > b) Malware may be too new to be detected
- >
- > More to the point; a malware that did not exist at the time you last
- > updated the av, is VERY likely to be missed by av. As malware can go
- > global within a few minutes, and as av vendors need time to get
- > samples, assess these, and then code, test and distribute a fix, it

Re: Do I have TOO MANY antivirus, antispysware, etc

- > will always lag behind the latest malware.
- >
- > MS's whole approach is to avoid getting malware in the first place.
- > They advise the following approach:
 - > – patch defects in the OS, etc. (Windows Update)
 - > – enable the built-in firewall, or install an add-on firewall
 - > – install an av and KEEP IT UP TO DATE
- >
- > That's all well and good, but it isn't really enough because you still
- > need to be smart enough not to take dumb risks, and you also need to
- > ensure the OS isn't taking dumb risks on your behalf.
- >
- > Massively and less massively dumb risks include...
- >
- > Using any pre-SP2 version of Windows XP as-is
- >
- > Out of the box, the original Windows XP and XP SP1 will be attacked
- > and infected or crashed within minutes of connecting to the Internet,
- > without you doing anything at all. This is because:
 - > – XP is designed to be a "network client"
 - > – as such, it waves services such as LSASS and RPC at the 'net
 - > – both these were defective before SP2, allowing immediate attack
 - > – XP has a firewall, but it was turned OFF by duuhfault before SP2
- >
- > Connecting to the Internet without a firewall
- >
- > See above. XP has a very competent firewall, but it doesn't work if
- > it is not enabled. It is enabled by default (i.e. without you having
- > to scratch around in network properties, Advanced etc. to turn it on)
- > in XP SP2, and SP2 also has the RPC and LSASS defects fixed. With
- > earlier SP1 and original XP "Gold", you have to download and apply
- > patches for these defects, and without a firewall on, you haven't a
- > hope of getting that right before being attacked.
- >
- > Having File and Print Sharing (F&PS) bound to the Internet
- >
- > File and Print Sharing allows any shared resource to be accessed via
- > the network it is bound to. You do NOT want to bind this to the
- > Internet, but certain configurations are likely to do this. The
- > firewall can be used to block this unwanted functionality.
- >
- > Full-sharing the whole hard drive
- >
- > If you share (allow network access to) certain locations, then malware
- > can simply drop itself into place in such a way that the next time
- > Windows starts, it will run the malware automatically. Yet Windows XP
- > uses hidden admin shares that do exactly this in XP Pro, and these may
- > be exposed if you use a non-blank account password. You may have no
- > wish to bother with a password at all, and may use a weak one just to
- > keep Tasks running. Any weak password (say, under 15 characters,
- > containing guessable words, etc.) can be brute-forced quite quickly.

Re: Do I have TOO MANY antivirus, antispysware, etc

- >
- > Clicking on every piece of junk that is sent to you
- >
- > It doesn't matter if it's "from someone you know" – if the message
- > text is non-specific and makes no specific reference to all attached
- > files, you should assume they are malware, sent by a malware running
- > on the sender's PC that acted outside that user's intent.
- >
- > Clicking on stuff without knowing what it will do
- >
- > In the old DOS days, "data" was safe to "view" (read) while "programs"
- > or "code" were not safe to run. You would look at the file name
- > extension, and if it was .EXE, .COM or .BAT, you would NOT run the
- > file because you'd know it was code. Today, there are so many file
- > types it is hard to know which are data and which are code, and due to
- > design and code defects, "data" files can get to run as code.
- > Nevertheless you should attempt to become familiar with file types, so
- > that you know what "opening" a file can do in terms of risk.
- >
- > Hiding file name extensions
- >
- > This is a duuuuhfault setting you have to manually change in Windows,
- > so that you can see the file name extensions mentioned above. Else
- > you have NO idea what will happen if you were to "open" a file – the
- > word "open" tells you absolutely NOTHING about the risk level!
- >
- > Connecting to broadband without a router
- >
- > A "router" is a device that hides your PC's address from the Internet,
- > so that you are less likely to be attacked directly. If on ADSL, you
- > want an ADSL router – not some half-assed USB "ADSL modem".
- >
- > Running without a resident antivirus
- >
- > Because it's so difficult to know what level of risk files post to the
- > system, plus there's a risk the system will automatically take risks
- > "for you", it's become mandatory for all but the geekiest of us to run
- > a resident av (antivirus) underfoot.
- >
- > Failing to keep your antivirus up to date
- >
- > It doesn't matter what av you use, and personally "Norton" would be my
- > last choice. Rather use one of several free av, such as AVG, Avast or
- > AntiVir, and crucially keep it up to date (daily updates at least).
- >
- > Failing to keep your edge-facing software updated
- >
- > Software that faces the edge includes Windows and the Internet
- > Explorer and Outlook Express components bound into this. The easiest
- > way to keep this updated is via Windows Update, preferably via the
- > Automatic Update facility – but first, you must be firewalled!

Re: Do I have TOO MANY antivirus, antispysware, etc

- >
- > If you use Firefox instead of Internet Explorer, then that has to be
- > kept updated as well (note; "as well", not "instead of" keeping
- > Windows and IE updated!). FireFox is easy to update; it's small, and
- > you just download and install the new versions as they are released,
- > which used to happen once a month – same as Windows itself.
- >
- > If you use Sun Java, then that must be updated as well, and there's a
- > wrinkle; you have to first manually uninstall the old version of Sun's
- > JRE (Java Runtime Engine) via Add/Remove Programs before installing
- > the new bug–fixed version. If you don't have Java, don't get it :-)
- >
- > Other edge–facing software include email apps, media players such as
- > Winamp, archivers such as WinZip and WinRar, file viewers such as
- > Adobe (Acrobat) Reader, etc. There have been recent defects in Adobe
- > Reader, and WinAmp gets up–versioned quite often too.
- >
- > If this all sounds like a PITA, well... it is. Most folks lose the
- > battle and get malware'd to some extent, but the more careful and
- > clueful you are, the better will be your mileage.
- >
- >
- >
- > >-----
- > Don't pay malware vendors – boycott Sony
- > >-----
- >
- .

• **References:**

- ◆ **Re: Do I have TOO MANY antivirus, antispysware, etc**
◇ From: cquirke (MVP Windows shell/user)
- Prev by Date: **Re: How to Remove .mdb files from Unsafe File List**
- Next by Date: **Logon with Administrator Account on XP Home...**
- Previous by thread: **Re: Do I have TOO MANY antivirus, antispysware, etc**
- Next by thread: **Re: MSIA TCP Port**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**