

## Re: Totally confused

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2004-10/0799.html>

---

**From:** Mad Force (*MadForce\_at\_discussions.microsoft.com*)

**Date:** 10/14/04

Date: Thu, 14 Oct 2004 08:21:05 -0700

Webroot Spysweep is a great tool!! It blocks the spys from ever getting on your system. I use v3.0 and I paid the \$29 to get updates for free. It's worth every penny because it protects 10-12 areas of your system from ever getting spyware/adaware, etc.

I also use Ad-aware SE and Spybot Search & Destroy. It also helps to use Tracks Eraser Pro to remove all the cookies.

"Shenan Stanley" wrote:

> *Headtheball* wrote:

> > *I have just run two different spyware adware progs and one tells me*

> > *that I have 10 infections including two parasites, xxtoolbar*

> > *coolwebsearch this program is called free spywarescan and then I ran*

> > *adaware using latest reference file and it says that there is nothing*

> > *on my system. Spybot search and destroy says that I have 7 problems*

> > *associated with Download accelerator and cannot remove the problems*

> > *but it does not show the coolwebsearch or xxtoolbar. What do I make*

> > *of this?*

>

>

> *I see you are one of those that assume one program will fix everything.*

> *It won't.*

>

> *The first 5 - minimum - to clear up most unwanted parasites and prevent*

> *reinfection later. Be sure that you not only scan with Spybot Search and*

> *Destroy, but immunize with it in addition to using SpywareBlaster.*

>

> *If you don't wish to follow all of the advice immediately, just want to*

> *get rid of your current dilemma, then you are welcome to scroll down to*

> *the section titled "SPYWARE/ADWARE/POPUPS", where your problem as*

> *stated should be resolved by the applications and suggestions found in*

> *that section. If this helps solve your problem then I again HIGHLY*

> *suggest you follow the rest of the advice below (matter of fact, I*

> *suggest it either way.)*

>

> *Suggestions on what you can do to secure/clean your PC. I'm going to try*

> *and be general, I will assume a "Windows" operating system is what is*

- > *being secured here.*
- >
- >
- > **SPYWARE/ADWARE/POPUPS**
- > -----
- >
- > *There are annoyances out there you can get without*
- > *trying. Your normal web surfing, maybe a wrong click on a web page, maybe*
- > *just a momentary lack of judgment by installing some software packages*
- > *without doing the research.. And all of a sudden your screen starts filling*
- > *up with advertisements or your Internet seems much slower or your home page*
- > *won't stay what you set it and goes someplace unfamiliar to you. This is*
- > *spyware. There are a whole SLEW of software packages out there to get rid*
- > *of this crud and help prevent reinfection. Some of the products already*
- > *mentioned might even have branched out into this arena. However, there are*
- > *a few applications that seem to be the best at what they do, which is*
- > *eradicating and immunizing your system from this crap. Strangely, the best*
- > *products I have found in this category ARE generally free. That is a trend*
- > *I like. I make donations to some of them, they deserve it!*
- >
- > *Two side-notes: Never think one of these can do the whole job.*
- > *Try the first 5 before coming back and saying "That did not work!"*
- > *Also, you can always visit:*
- > *<http://myvps.org/winhelp2002/unwanted.htm>*
- > *For more updated information.*
- >
- > *Spybot Search and Destroy (Free!)*
- > *<http://www.safer-networking.net/>*
- >
- > *Lavasoft AdAware (Free and up)*
- > *<http://www.lavasoft.de>*
- >
- > *CWSShredder (Free!)*
- > *<http://www.spywareinfo.com/~merijn/downloads.html>*
- >
- > *Hijack This! (Free)*
- > *<http://mjc1.com/mirror/hjt/>*
- > *( Tutorial: <http://www.spywareinfo.com/~merijn/htlogtutorial.html> )*
- >
- > *SpywareBlaster (Free!)*
- > *<http://www.javacoolsoftware.com/>*
- >
- > *IE-SPYAD (Free!)*
- > *<http://www.staff.uiuc.edu/~ehowes/resource.htm>*
- >
- > *ToolbarCop (Free!)*
- > *<http://www.myvps.org/sramesh2k/toolbarcop.htm>*
- >
- > *Bazooka Adware and Spyware Scanner (Free!)*
- > *<http://www.kephyr.com/spywarescanner/index.html>*
- >

- > *Browser Security Tests*
- > <http://www.jasons-toolbox.com/BrowserSecurity/>
- >
- > *The Cleaner (49.95 and up)*
- > <http://www.moosoft.com/>
- >
- > *That will clean up your machine of the spyware, given that you download and*
- > *install several of them, update them regularly and scan with them when you*
- > *update. Some (like SpywareBlaster and SpyBot Search and Destroy) have*
- > *immunization features that will help you prevent your PC from being*
- > *infected. Use these features!*
- >
- > *Unfortunately, although that will lessen your popups on the Internet/while*
- > *you are online, it won't eliminate them. I have looked at a lot of options,*
- > *seen a lot of them used in production with people who seem to attract popups*
- > *like a plague, and I only have one suggestion that end up serving double*
- > *duty (search engine and popup stopper in one):*
- >
- > *The Google Toolbar (Free!)*
- > <http://toolbar.google.com/>
- >
- > *Yeah – it adds a bar to your Internet Explorer – but its a useful one. You*
- > *can search from there anytime with one of the best search engines on the*
- > *planet (IMO.) And the fact it stops most popups – wow – BONUS! If you*
- > *don't like that suggestion, then I am just going to say you go to*
- > *www.google.com and search for other options.*
- >
- > *One more suggestion, although I will suggest this in a way later, is to*
- > *disable your Windows Messenger service. This service is not used frequently*
- > *(if at all) by the normal home user and in cooperation with a good firewall,*
- > *is generally unnecessary. Microsoft has instructions on how to do this for*
- > *Windows XP here:*
- > <http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>
- >
- >
- > *UPDATES and PATCHES*
- > -----
- >
- > *This one is the most obvious. There is no perfect product and any company*
- > *worth their salt will try to meet/exceed the needs of their customers and*
- > *fix any problems they find along the way. I am not going to say Microsoft*
- > *is the best company in the world about this but they do have an option*
- > *available for you to use to keep your machine updated and patched from*
- > *the problems and vulnerabilities (as well as product improvements in some*
- > *cases) – and it's free to you.*
- >
- > *Windows Update*
- > <http://windowsupdate.microsoft.com/>
- >
- > *Go there and scan your machine for updates. Always get the critical ones as*
- > *you see them. Write down the KB##### or Q##### you see when selecting the*

- > updates and if you have trouble over the next few days, go into your control
- > panel (Add/Remove Programs), match up the latest numbers you downloaded
- > recently (since you started noticing an issue) and uninstall them. If there
- > was more than one (usually is), install them back one by one – with a few
- > hours of use in between, to see if the problem returns. Yes – the process
- > is not perfect (updating) and can cause trouble like I mentioned – but as
- > you can see, the solution isn't that bad – and is MUCH better than the
- > alternatives. (SASSER/BLASTER were SO preventable with just this step!)
- >
- > Windows is not the only product you likely have on your PC. The
- > manufacturers of the other products usually have updates as well. New
- > versions of almost everything come out all the time – some are free, some
- > are pay – some you can only download if you are registered – but it is best
- > to check. Just go to their web pages and look under their support and
- > download sections.
- >
- > You also have hardware on your machine that requires drivers to interface
- > with the operating system. You have a video card that allows you to see on
- > your screen, a sound card that allows you to hear your PCs sound output and
- > so on. Visit those manufacturer web sites for the latest downloadable
- > drivers for your hardware/operating system. Always (IMO) get the
- > manufacturers hardware driver over any Microsoft offers. On the Windows
- > Update site I mentioned earlier, I suggest NOT getting their hardware
- > drivers – no matter how tempting.
- >
- > Have I mentioned that Microsoft has some stuff to help secure your computer
- > available to the end-user for free? This seems as good of a time as any.
- > They have a CD you can order (it's free) that contain all of the Windows
- > patches through October 2003 and some trial products as well that they
- > released in February 2004. Yeah – it's a little behind now, but it's better
- > than nothing (and used in coordination with the information in this post,
- > well worth the purchase price..)
- >
- > Order the Windows Security Update CD
- > <http://www.microsoft.com/security/protect/cd/order.asp>
- >
- > They also have a bunch of suggestions, some similar to these, on how to
- > better protect your Windows system:
- >
- > Protect your PC
- > <http://www.microsoft.com/security/protect/>
- >
- >
- > FIREWALL
- > -----
- >
- > Let's say you are up-to-date on the OS (operating system) and you have
- > Windows XP.. You should at least turn on the built in firewall. That will
- > do a lot to "hide" you from the random bad things flying around the
- > Internet. Things like Sasser/Blaster enjoy just sitting out there in
- > Cyberspace looking for an unprotected Windows Operating System and jumping

- > on it, doing great damage in the process and then using that Unprotected OS
- > to continue its dirty work of infecting others. If you have the Windows XP
- > ICF turned on – default configuration – then they cannot see you! Think of
- > it as Internet Stealth Mode at this point. It has other advantages, like
- > actually locking the doors you didn't even (likely) know you had. Doing
- > this is simple, the instructions you need to use your built in Windows XP
- > firewall can be found here:
- >
- > <http://support.microsoft.com/?kbid=320855>
- >
- > If you read through that and look through the pages that are linked from it
- > at the bottom of that page – I think you should have a firm grasp on the
- > basics of the Windows XP Firewall as it is today. One thing to note RIGHT
- > NOW – if you have AOL, you cannot use this nice firewall that came with
- > your system. Thank AOL, not Microsoft. You HAVE to configure another
- > one.. So we continue with our session on Firewalls...
- >
- > But let's say you DON'T have Windows XP – you have some other OS like
- > Windows 95, 98, 98SE, ME, NT, 2000. Well, you don't have the nifty built in
- > firewall. My suggestion – upgrade. My next suggestion – look through your
- > options. There are lots of free and pay firewalls out there for home users.
- > Yes – you will have to decide on your own which to get. Yes, you will have
- > to learn (oh no!) to use these firewalls and configure them so they don't
- > interfere with what you want to do while continuing to provide the security
- > you desire. It's just like anything else you want to protect – you have to
- > do something to protect it. Here are some suggested applications. A lot of
- > people tout "ZoneAlarm" as being the best alternative to just using the
- > Windows XP ICF, but truthfully – any of these alternatives are much better
- > than the Windows XP ICF at what they do – because that is ALL they do.
- >
- > ZoneAlarm (Free and up)
- > <http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp>
- >
- > Kerio Personal Firewall (KPF) (Free and up)
- > [http://www.kerio.com/kpf\\_download.html](http://www.kerio.com/kpf_download.html)
- >
- > Outpost Firewall from Agnitum (Free and up)
- > <http://www.agnitum.com/download/>
- >
- > Sygate Personal Firewall (Free and up)
- > [http://smb.sygate.com/buy/download\\_buy.htm](http://smb.sygate.com/buy/download_buy.htm)
- >
- > Symantec's Norton Personal Firewall (~\$25 and up)
- > <http://www.symantec.com/sabu/nis/npf/>
- >
- > BlackICE PC Protection (\$39.95 and up)
- > <http://blackice.iss.net/>
- >
- > Tiny Personal Firewall (~\$49.00 and up)
- > <http://www.tinysoftware.com/>
- >

> That list is not complete, but they are good firewall options, every one of  
> them. Visit the web pages, read up, ask around if you like – make a  
> decision and go with some firewall, any firewall. Also, maintain it.  
> Sometimes new holes are discovered in even the best of these products and  
> patches are released from the company to remedy this problem. However, if  
> you don't get the patches (check the manufacturer web page on occasion),  
> then you may never know you have the problem and/or are being used through  
> this weakness. Also, don't stack these things. Running more than one  
> firewall will not make you safer – it would likely (in fact) negate some  
> protection you gleamed from one or the other firewalls you ran together.

>  
>

> **ANTIVIRUS SOFTWARE**

> -----

>

> That's not all. That's one facet of a secure PC, but firewalls don't do  
> everything. I saw one person posting on a newsgroup that "they had  
> never had a virus and they never run any anti-virus software." Yep – I used  
> to believe that way too – viruses were something everyone else seemed to  
> get, were they just stupid? And for the average joe-user who is careful,  
> uses their one-three family computers carefully, never opening unknown  
> attachments, always visiting the same family safe web sites, never  
> installing anything that did not come with their computer – maybe, just  
> maybe they will never witness a virus. I, however, am a Network Systems  
> Administrator. I see that AntiVirus software is an absolute necessity given  
> how most people see their computer as a toy/tool and not something  
> they should have to maintain and upkeep. After all, they were invented to  
> make life easier, right – not add another task to your day. You  
> can be as careful as you want – will the next person be as careful? Will  
> someone send you unknowingly the email that erases all the pictures of your  
> child/childhood? Possibly – why take the chance? ALWAYS RUN ANTIVIRUS  
> SOFTWARE and KEEP IT UP TO DATE! Antivirus software comes in so many  
> flavors, it's like walking into a Jelly Belly store – which one tastes like  
> what?! Well, here are a few choices for you. Some of these are free (isn't  
> that nice?) and some are not. Is one better than the other – MAYBE.

>

> Symantec (Norton) AntiVirus (~\$11 and up)

> <http://www.symantec.com/>

>

> Kaspersky Anti-Virus (~\$49.95 and up)

> <http://www.kaspersky.com/products.html>

>

> Panda Antivirus Titanium (~\$39.95 and up)

> <http://www.pandasoftware.com/>

> (Free Online Scanner: <http://www.pandasoftware.com/activescan/>)

>

> AVG 6.0 Anti-Virus System (Free and up)

> <http://www.grisoft.com/>

>

> McAfee VirusScan (~\$11 and up)

> <http://www.mcafee.com/>

- >
- > *AntiVir (Free and up)*
- > <http://www.free-av.com/>
- >
- > *avast! 4 (Free and up)*
- > <http://www.avast.com/>
- >
- > *Trend Micro (~\$49.95 and up)*
- > <http://www.trendmicro.com/>
- > *(Free Online Scanner:*
- > [http://housecall.trendmicro.com/housecall/start\\_corp.asp](http://housecall.trendmicro.com/housecall/start_corp.asp))
- >
- > *RAV AntiVirus Online Virus Scan (Free!)*
- > <http://www.ravantivirus.com/scan/>
- >
- > *Did I mention you have to not only install this software, but also keep it*
- > *updated? You do. Some of them (most) have automatic services to help you*
- > *do this – I mean, it's not your job to keep up with the half-dozen or more*
- > *new threats that come out daily, is it? Be sure to keep whichever one you*
- > *choose up to date!*
- >
- >
- > **SPAM EMAIL/JUNK MAIL**
- > -----
- >
- > *This one can get annoying, just like the rest. You get 50 emails in one*
- > *sitting and 2 of them you wanted. NICE! (Not.) What can you do? Well,*
- > *although there are services out there to help you, some email*
- > *servers/services that actually do lower your spam with features built into*
- > *their servers – I still like the methods that let you be the end-decision*
- > *maker on what is spam and what isn't. If these things worked perfectly, we*
- > *wouldn't need people and then there would be no spam anyway – vicious*
- > *circle, eh? Anyway – I have two products to suggest to you, look at them*
- > *and see if either of them suite your needs. Again, if they don't, Google is*
- > *free and available for your perusal.*
- >
- > *SpamBayes (Free!)*
- > <http://spambayes.sourceforge.net/>
- >
- > *Spamihilator (Free!)*
- > <http://www.spamihilator.com/>
- >
- > *As I said, those are not your only options, but are reliable ones I have*
- > *seen function for hundreds+ people.*
- >
- >
- > **DISABLE (Set to Manual) UNUSED SERVICE/STARTUP APPS**
- > -----
- >
- > *I might get arguments on putting this one here, but it's my spill. There are*
- > *lots of services on your PC that are probably turned on by default you don't*

microsoft.public.security: Re: Totally confused

- > use. Why have them on? Check out these web pages to see what all of the
- > services you might find on your computer are and set them according to your
- > personal needs. Be CAREFUL what you set to manual, and take heed and write
- > down as you change things! Also, don't expect a large performance increase
- > or anything – especially on todays 2+ GHz machines, however – I look at each
- > service you set to manual as one less service you have to worry about
- > someone exploiting. A year ago, I would have thought the Windows Messenger
- > service to be pretty safe, now I recommend (with addition of a firewall)
- > that most home users disable it! Yeah – this is another one you have to
- > work for, but your computer may speed up and/or be more secure because you
- > took the time. And if you document what you do as you do it, next time, it
- > goes MUCH faster! (or if you have to go back and re-enable things..)
- >
- > Task List Programs
- > [http://www.answerthatwork.com/Tasklist\\_pages/tasklist.htm](http://www.answerthatwork.com/Tasklist_pages/tasklist.htm)
- >
- > Black Viper's Service List and Opinions (XP)
- > <http://www.blackviper.com/WinXP/servicecfg.htm>
- >
- > Processes in Windows NT/2000/XP
- > <http://www.reger24.de/prozesse/>
- >
- > There are also applications that AREN'T services that startup when you start
- > up the computer/logon. One of the better description on how to handle these
- > I have found here:
- >
- > Startups
- > [http://www.pacs-portal.co.uk/startup\\_content.php](http://www.pacs-portal.co.uk/startup_content.php)
- >
- >
- > That's it. A small booklet on how to keep your computer secure, clean of
- > scum and more user friendly. I am SURE I missed something, almost as I am
- > sure you won't read all of it (anyone for that matter.) However, I also
- > know that someone who followed all of the advice above would also have less
- > problems with their PC, less problems with viruses, less problems with spam,
- > fewer problems with spyware and better performance than someone who didn't.
- >
- > Hope it helps.
- >
- > --
- > <- Shenan ->
- > --
- > The information is provided "as is", with no guarantees of
- > completeness, accuracy or timeliness, and without warranties of any
- > kind, express or implied. In other words, read up before you take any
- > advice – you are the one ultimately responsible for your actions.
- >
- >
- >