

Re: Trojan / Adware infection on Windows XP Pro computer

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-07/1204.html

From: Shenan Stanley (*newshelper_at_gmail.com*)

Date: 07/22/05

Date: Fri, 22 Jul 2005 14:27:41 -0500

Will_in_SF wrote:

- > Also, I run the computer on broadband service/ Any security
- > information that you can give me would be wonderul.
- >
- > Currently, I am downloading some programs from download.com so that I
- > can install on the infected computer so that I don't have to connect to
- > the internet while installing.
- > Will_in_SF wrote:
- >> Hi, all. I need some help. A friend of mine was working on a home
- >> computer of mine (I have 2 networked through a linksys router) and
- >> when running McAfee Virus Scan, Spybot and Adware, the computer has
- >> been infected with the following virus and adware/malware:
- >>
- >> Exploit – MhtRedir.gen
- >> Adware – Websearch
- >> Adware – DFC
- >> Adware – ISTBAR
- >> Adware – Sahagent (2)
- >> plus several PUP programs.
- >>
- >> This list goes on -- to many to mention all of them here. So, I
- >> immediately unplugged the computer from my home network and shut it
- >> down.
- >>
- >> Can someone please tell me what is the best way to take care of the
- >> situation. Since this computer was used as a second computer, there
- >> were minimal important files and quite a few personal files that I
- >> would want to keep. What tools are out there to help. Or should I
- >> restore the computer back to factory setting and start over?

Microsoft has these suggestions for Protecting your computer from the various things that could happen to you/it:

Protect your PC

<http://www.microsoft.com/security/protect/>

Although those tips are fantastic, there are many things you should know above and beyond what is there. Below I have detailed out many steps that can not only help you clean-up a problem PC but keep it clean ,secure and running at its top performance mark.

I know this text can seem intimidating – it is quite long and a lot to take in for a novice – but I assure you that one trip through this list and you will understand your computer and the options available to you for protecting your data much better – and that the next time you review these steps, the time it takes will be greatly reduced.

Let's take the cleanup of your computer step-by-step. Yes, it will take up some of your time – but consider what you use your computer for and how much you would dislike it if all of your stuff on your computer went away because you did not "feel like" performing some simple maintenance tasks – think of it like taking out your garbage, collecting and sorting your postal mail, paying your bills on time, etc.

I'll mainly work around Windows XP, as that is what the bulk of this document is about; however, here is a place for you poor souls still stuck in Windows 98/ME where you can get information on maintaining your system:

Windows 98 and 'Maintaining Your Computer':

<http://www.microsoft.com/windows98/usingwindows/maintaining/>

Windows ME Computer Health:

<http://www.microsoft.com/windowsME/using/computerhealth/articles/>

Pay close attention to the sections:

(in order)

- Clean up your hard disk
- Check for errors by running ScanDisk
- Defragment your hard disk
- Roll back the clock with System Restore

Also – now is a good time to point you to one of the easiest ways to find information on problems you may be having and solutions others have found:

Search using Google!

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

(How-to: <http://www.google.com/intl/en/help/basics.html>)

Now, let's go through some maintenance first that should only have to be done once (mostly):

Tip (1):

Locate all of the software you have installed on your computer.

(the installation media – CDs, downloaded files, etc)

Collect these CDs and files together in a central and safe

place along with their CD keys and such. Make backups of these installation media sets using your favorite copying method (CD/DVD Burner and application, Disk copier, etc.) You'll be glad to know that if you have a CD/DVD burner, you may be able to use a free application to make a duplicate copy of your CDs. One such application is ISORecorder:

ISORecorder page (with general instructions on use):

<http://isorecorder.alexfeinman.com/beta.htm>

Yes – it is BETA software – but very useful and well tested.

More full function applications (free) for CD/DVD burning would be:

DeepBurner Free

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

CDBurnerXP Pro

<http://www.cdburnerxp.se/>

Another Option would be to search the web with Pricewatch.com or Dealsites.net and find deals on Products like Ahead Nero and/or Roxio.

Tip (2):

Empty your Temporary Internet Files and shrink the size it stores to a size between 128MB and 512MB..

- Open ONE copy of Internet Explorer.
- Select TOOLS –> Internet Options.
- Under the General tab in the "Temporary Internet Files" section, do the following:
 - Click on "Delete Cookies" (click OK)
 - Click on "Settings" and change the "Amount of disk space to use:" to something between 128MB and 512MB. (Betting it is MUCH larger right now.)
 - Click OK.
 - Click on "Delete Files" and select to "Delete all offline contents" (the checkbox) and click OK. (If you had a LOT, this could take 2–10 minutes or more.)
- Once it is done, click OK, close Internet Explorer, re–open Internet Explorer.

Tip (3):

If things are running a bit sluggish and/or you have an older system (1.5GHz or less and 256MB RAM or less) then you may want to look into tweaking the performance by turning off some of the 'resource hogging' Windows XP "prettifications". The fastest method is:

Control Panel --> System --> Advanced tab --> Performance section, Settings button. Then choose "adjust for best performance" and you now have a Windows 2000/98 look which turned off most of the annoying "prettifications" in one swift action. You can play with the last

three checkboxes to get more of an XP look without many of the other annoyances. You could also grab and install/use one (or more) of the Microsoft Powertoys – TweakUI in particular:

<http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx>

Tip (4):

Understanding what a good password might be is vital to your personal and system security. You may think you do not need to password your home computer, as you may have it in a locked area (your home) where no one else has access to it. Remember, however, you aren't always "in that locked area" when using your computer online – meaning you likely have usernames and passwords associated with web sites and the likes that you would prefer other people do not discover/use. This is why you should understand and utilize good passwords.

Good passwords are those that meet these general rules (mileage may vary):

Passwords should contain at least six characters, and the character string should contain at least three of these four character types:

- uppercase letters
- lowercase letters
- numerals
- nonalphanumeric characters (e.g., *, %, &, !, :)

Passwords should not contain your name/username.

Passwords should be unique to you and easy to remember.

One method many people are using today is to make up a phrase that describes a point in their life and then turning that phrase into their password by using only certain letters out of each word in that phrase. It's much better than using your birthday month/year or your anniversary in a pure sense. For example, let's say my phrase is:

'Moved to new home in 2004'

I could come up with this password from that:

'Mv2n3whmN04'

The password tip is in the one time section, but I highly recommend you periodically change your passwords. The suggested time varies, but I will throw out a 'once in every 3 to 6 months for every account you have.'

Tip (5):

This tip is also 'questionable' in the one time section; however – if properly setup – this one can be pretty well ignored for most people after the initial 'fiddle-with' time.

Why you should use a computer firewall..

<http://www.microsoft.com/athome/security/viruses/fwbenefits.mspx>

You should, in some way, use a firewall. Hardware (like a nice Cable Modem/DSL router) or software is up to you. Many use both of these. The simplest one to use is the hardware one, as most people don't do anything that they will need to configure their NAT device for and those who do certainly will not mind fiddling with the equipment to make things work for them. Next in the line of simplicity would have to be the built-in Windows Firewall of Windows XP. In SP2 it is turned on by default. It is not difficult to turn on in any case, however:

Enable/Disable the Internet Connection Firewall (Pre-SP2):

<http://support.microsoft.com/kb/283673>

More information on the Internet Connection Firewall (Pre-SP2):

<http://support.microsoft.com/kb/320855>

Post-SP2 Windows Firewall Information/guidance:

<http://snipurl.com/atal>

The trouble with the Windows Firewall is that it only keeps things out. For most people who maintain their system in other ways, this is MORE than sufficient. However, you may feel otherwise. If you want to know when one of your applications is trying to obtain access to the outside world so you can stop it, then you will have to install a third-party application and configure/maintain it. I have compiled a list with links of some of the better known/free firewalls you can choose from:

BlackICE PC Protection (~\$39.95 and up)

<http://blackice.iss.net/>

Jetico Personal Firewall (Free)

<http://www.jetico.com/index.htm#/jpfirewall.htm>

Kerio Personal Firewall (KPF) (Free and up)

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

Symantec's Norton Personal Firewall (~\$25 and up)

<http://www.symantec.com/sabu/nis/npf/>

ZoneAlarm (Free and up)

<http://snipurl.com/6ohg>

You should find the right firewall for your situation in that list and set it up.

Every firewall WILL require some maintenance. Essentially checking for patches or upgrades (this goes for hardware and software solutions) is the extent of this maintenance – you may also have to configure your firewall to allow some traffic depending on your needs.

** Don't stack the software firewalls! Running more than one software firewall will not make you safer – it would possibly negate some protection you gleaned from one or the other firewall you run.

Now that you have some of the more basic things down..
Let's go through some of the steps you should take periodically to maintain a healthy and stable windows computer. If you have not done some of these things in the past, they may seem tedious – however, they will become routine and some can even be automatically scheduled.

Tip (6):

The system restore feature is a new one – first appearing in Windows ME and then sticking around for Windows XP. It is a useful feature if you keep it maintained and use it to your advantage. Remember that the system restore pretty much tells you in the name what it protects which is 'system' files. Your documents, your pictures, your stuff is NOT system files – so you should also look into some backup solution.

I have seen the automatic system restore go wrong too many times not to suggest the following.. Whenever you think about it (after doing a once-over on your machine once a month or so would be optimal) – clear out your System Restore and create a manual restoration point.

'Why?'

Too many times have I seen the system restore files go corrupt or get a virus in them, meaning you could not or did not want to restore from them. By clearing it out periodically you help prevent any corruption from happening and you make sure you have at least one good "snapshot". (*This, of course, will erase any previous restore point you have.*)

- Turn off System Restore.
<http://support.microsoft.com/kb/310405>
- Reboot the Computer.
- Review the first bullet to turn on System Restore
- Make a Manual Restoration Point.
<http://snipurl.com/68nx>

That covers your system files, but doesn't do anything for the files that you are REALLY worried about – yours! For that you need to look into backups. You can either manually copy your important files, folders, documents, spreadsheets, emails, contacts, pictures, drawings and so on to an external location (CD/DVD – any disk of some sort, etc) or you can use the backup tool that comes with Windows XP:

How To Use Backup to Back Up Files and Folders on Your Computer

<http://support.microsoft.com/kb/308422>

Yes – you still need some sort of external media to store the results on, but you could schedule the backup to occur when you are not around, then burn the resultant data onto CD or DVD or something when you are (while you do other things!)

A lot of people have wondered about how to completely backup their system so that they would not have to go through the trouble of a reinstall..

I'm going to voice my opinion here and say that it would be worthless to do for MOST people. Unless you plan on periodically updating the image backup of your system (remaking it) – then by the time you use it (something goes wrong) – it will be so outdated as to be more trouble than performing a full install of the operating system and all applications.

Having said my part against it, you can clone/backup your hard drive completely using many methods – by far the simplest are using disk cloning applications:

Symantec/Norton Ghost

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

Acronis True Image

<http://www.acronis.com/homecomputing/products/trueimage>

Tip (7):

You should sometimes look through the list of applications that are installed on your computer. The list may surprise you. There are more than likely things in there you know you never use – so why have them there? There may even be things you know you did *not* install and certainly do not use (maybe don't WANT to use.)

This web site should help you get started at looking through this list:

How to Uninstall Programs

<http://snipurl.com/8v6b>

A word of warning – Do NOT uninstall anything you think you MIGHT need in the future unless you have completed Tip (1) and have the installation media and proper keys for use backed up somewhere safe!

Tip (8):

Patches and Updates!

This one cannot be stressed enough. It is SO simple, yet so neglected by many people. It is especially simple for the critical Windows patches! Microsoft put in an AUTOMATED feature for you to utilize so that you do NOT have to worry yourself about the patching of the Operating System:

How to configure and use Automatic Updates in Windows XP

<http://support.microsoft.com/kb/306525>

However, not everyone wants to be a slave to automation, and that is fine. Admittedly, I prefer this method on some of my more critical systems.

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), insure that the 'Show Updates' checkbox is checked and 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), uninstall them 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.

Windows is not the only product you likely have on your PC. The manufacturers of the other products usually have updates. New versions of almost everything come out all the time – some are free, some are pay and 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. For example, for Microsoft Office you should visit:

Microsoft Office Updates

<http://office.microsoft.com/>

(and select 'Check for Updates' and/or 'Downloads' for more)

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 PC's sound output and so on. Visit those manufacturer web sites for the latest downloadable drivers for your hardware/operating system. Always 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.

How do you know what hardware you have in your computer? Break out the invoice or if it is up and working now – take inventory:

Belarc Advisor

http://belarc.com/free_download.html

EVEREST Home Edition

<http://www.lavalys.com/products/download.php?pid=1&lang=en>

Once you know what you have, what next? Go get the latest driver for your hardware/OS from the manufacturer's web page. For example, let's say you have an NVidia chipset video card or ATI video card, perhaps a Creative Labs sound card or C-Media chipset sound card...

NVidia Video Card Drivers

<http://www.nvidia.com/content/drivers/drivers.asp>

ATI Video Card Drivers

<http://www.atitech.com/support/driver.html>

Creative Labs Sound Device

<http://us.creative.com/support/downloads/>

C-Media Sound Device

http://www.cmedia.com.tw/e_download_01.htm

Then install these drivers. Updated drivers are usually more stable and may provide extra benefits/features that you really wished you had before.

As for Service Pack 2 (SP2) for Windows XP, Microsoft has made this particular patch available in a number of ways. First, there is the Windows Update web page above. Then there is a direct download site and finally, you can order the FREE CD from Microsoft.

Direct Download of Service Pack 2 (SP2) for Windows XP

<http://snipurl.com/8bqy>

Order the Free Windows XP SP2 CD

<http://snipurl.com/8umo>

If all else fails – grab the full download above and try to use that. In this case – consider yourself a 'IT professional or developer'.

Tip (9):

What about the dreaded word in the computer world, VIRUS?

Well, there are many products to choose from that will help you prevent infections from these horrid little applications. Many are FREE to the home user and which you choose is a matter of taste, really. Many people have emotional attachments or performance issues with one or another AntiVirus software. Try some out, read reviews and decide for yourself which you like more:

(Good Comparison Page for AV software: <http://www.av-comparatives.org/>)

AntiVir (Free and up)

<http://www.free-av.com/>

avast! (Free and up)

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

microsoft.public.windowsxp.security_admin: Re: Trojan / Adware infection on Windows XP Pro computer

AVG Anti-Virus System (Free and up)

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

eset NOD32 (~\$39.00 and up)

<http://www.eset.com/products/products.htm>

eTrust EZ Antivirus (~\$29.95 and up)

<http://ca.com/store/home/us/hp2/>

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

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

McAfee VirusScan (~\$11 and up)

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

Panda Antivirus Titanium (~\$39.95 and up)

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

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

RAV AntiVirus Online Virus Scan (Free!)

<http://www.ravantivirus.com/scan/>

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

http://www.symantec.com/nav/nav_9xnt/

Trend Micro (~\$49.95 and up)

<http://www.trendmicro.com/en/home/us/personal.htm>

(Free Online Scanner:

http://housecall.trendmicro.com/housecall/start_corp.asp)

Most of them have automatic update capabilities. You will have to look into the features of the one you choose. Whatever one you finally settle with – be SURE to keep it updated (I recommend at least daily) and perform a full scan periodically (yes, most protect you actively, but a full scan once a month at 4AM probably won't bother you.)

Tip (10):

The most rampant infestation at the current time concerns SPYWARE/ADWARE.

You need to eliminate it from your machine.

There is no one software that cleans and immunizes you against everything. Antivirus software – you only needed one. Firewall, you only needed one. AntiSpyware – you will need several. I have a list and I recommend you use at least the first five.

First – make sure you have NOT installed "Rogue AntiSpyware". There are people out there who created AntiSpyware products that actually install spyware of their own! You need to avoid these:

Rogue/Suspect Anti-Spyware Products & Web Sites

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Re: Trojan / Adware infection on Windows XP Pro computer

microsoft.public.windowsxp.security_admin: Re: Trojan / Adware infection on Windows XP Pro computer

Also, you can always visit this site..

<http://mvps.org/winhelp2002/unwanted.htm>

For more updated information.

Install the first five of these: (Install, Run, Update, Scan with..)

(If you already have one or more – uninstall them and download the LATEST version from the page given!)

Lavasoft AdAware (Free and up)

<http://www.lavasoft.de/support/download/>

(How-to: <http://snipurl.com/atdn>)

Spybot Search and Destroy (Free!)

<http://www.safer-networking.net/en/download/index.html>

(How-to: <http://snipurl.com/atdk>)

Bazooka Adware and Spyware Scanner (Free!)

<http://www.kephyr.com/spywarescanner/>

(How-to: <http://snipurl.com/ate3>)

SpywareBlaster (Free!)

<http://www.javacoolsoftware.com/sbdownload.html>

(How-to: <http://snipurl.com/ate6>)

IE-SPYAD2 (Free!)

<https://netfiles.uiuc.edu/ehowes/www/resource.htm>

(How-to: <http://snipurl.com/ate7>)

CWShredder Stand-Alone (Free!)

http://www.intermute.com/spysubtract/cwshredder_download.html

Hijack This! (Free!)

<http://www.spywareinfo.com/~merijn/downloads.html>

(Log Analyzer: <http://hjt.iamnotageek.com/>)

ToolbarCop (Free!)

<http://windowsxp.mvps.org/toolbarcop.htm>

Microsoft AntiSpyware BETA (in testing stages – Free!)

<http://www.microsoft.com/athome/security/spyware/software/>

(How-to: <http://snipurl.com/fqur>)

Browser Security Tests (Free Tester)

<http://www.jasons-toolbox.com/BrowserSecurity/>

Popup Tester (Free Tester)

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

The Cleaner (~\$49.95 and up)

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

Re: Trojan / Adware infection on Windows XP Pro computer

Sometimes you need to install the application and reboot into SAFE MODE in order to thoroughly clean your computer. Many applications also have (or are) immunization applications. Spybot Search and Destroy and SpywareBlaster are two that currently do the best job at passively protecting your system from malware. None of these programs (in these editions) run in the background unless you TELL them to. The space they take up and how easy they are to use greatly makes up for any inconvenience you may be feeling.

Please notice that Windows XP SP2 does help stop popups as well.

Another option is to use an alternative Web browser. I suggest 'Mozilla Firefox', as it has some great features and is very easy to use:

Mozilla Firefox

<http://www.mozilla.org/products/firefox/>

So your machine is pretty clean and up to date now. If you use the sections above as a guide, it should stay that way as well! There are still a few more things you can do to keep your machine running in top shape.

Tip (11):

You should periodically check your hard drive(s) for errors and defragment them. Only defragment after you have cleaned up your machine of outside parasites and never defragment as a solution to a quirkiness in your system. It may help speed up your system, but it should be clean before you do this. Do these things IN ORDER...

How to use Disk Cleanup

<http://support.microsoft.com/kb/310312>

How to scan your disks for errors

<http://support.microsoft.com/kb/315265>

How to Defragment your hard drives

<http://support.microsoft.com/kb/314848>

I would personally perform the above steps at least once every three months. For most people this should be sufficient, but if the difference you notice afterwards is greater than you think it should be, lessen the time in between its schedule.. If the difference you notice is negligible, you can increase the time.

Tip (12):

SPAM! 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 is not. I have two products to suggest to

microsoft.public.windowsxp.security_admin: Re: Trojan / Adware infection on Windows XP Pro computer

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.

Tip (13):

ADVANCED TIP! Only do this once you are comfortable under the hood of your computer!

There are lots of services on your PC that are probably turned on by default you don't 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 today's 2+ GHz machines, however – I look at each service you set to manual as one less service you have to worry about someone exploiting.

Configuring Services

<http://snakefoot.fateback.com/tweak/winnt/services.html>

Task List Programs

http://www.answersthatwork.com/Tasklist_pages/tasklist.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

If you follow the advice laid out above (and do some of your own research as well, so you understand what you are doing) – your computer will stay fairly stable and secure and you will have a more trouble-free system.

--

Shenan Stanley
MS-MVP

--

How To Ask Questions The Smart Way
<http://www.catb.org/~esr/faqs/smart-questions.html>

Re: Trojan / Adware infection on Windows XP Pro computer