

Re: Beware! spyware on windows update

Source: <http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2004-11/1492.html>

From: Shenan Stanley (*news_helper_at_hushmail.com*)

Date: 11/15/04

Date: Sun, 14 Nov 2004 19:07:28 -0600

steveinicks wrote:

- > *I just downloaded a driver for my Realtek AC/97 audio control from*
- > *Microsoft Windows Update and it installed spyware on my computer.*
- >
- > *Name AlcxMonitor*
- > *Command Alcxmnr.exe*
- > *Status X*
- > *Description Realtek AC97 Audio – Event Monitor. "Sypware" file used*
- > *surreptitiously monitor one's actions. It is not a sinister one, like*
- > *remote control programs, but it is being used by Realtek to gather*
- > *data about customers*
- >
- > *Think about that next time you check the "Always trust content from*
- > *Microsoft" box.*

You download your hardware drivers from Microsoft?

Bad idea initially.

Not that it would save you in this case, as probably (if it is Realtek doing the monitoring) the driver (the proper driver) from the Realtek site would contain the same software – however, you should get the hardware driver from the original manufacturer, not Microsoft. Why wouldn't you go straight to the source – they made the product, then they likely know what it needs better than the Microsoft approved version.

WARNING This is a LONG spill, all in plain text and simplified so that even non-techs should be able to understand it. Hopefully this will assist some people in not only repairing their systems, but in making them faster and more stable tools for them to use. It contains advice on many things, many considered "common knowledge" to 'IT' people everywhere. It is split into major sections, hopefully this will make it easier to navigate. ***WARNING***

Suggestions on what you can do to secure/clean your PC. Every attempt has been made to be general and an assumption of a "Windows" operating system is made here as well – although in some ways, this could be adapted to any OS.

GENERAL UPKEEP AND CLEANUP

You should periodically defragment your hard drives as well as check them for errors. 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 one.

How to Defragment your hard drives

<http://support.microsoft.com/?kbid=314848>

How to scan your disks for errors

<http://support.microsoft.com/?kbid=315265>

How to use Disk Cleanup

<http://support.microsoft.com/?kbid=310312>

You should also empty your Internet Explorer Temporary Internet Files and make sure the maximum size for this is small enough not to cause trouble in the future. Empty your Temporary Internet Files and shrink the size it stores to a size between 10MB and 360MB..

- 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 10MB and 360MB. (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.

Uninstall any software you no longer use or cannot remember installing (ask if it is a multi-user PC) - but only if you are sure you do not need it and/or you have the installation media around to reinstall if you need to. <http://snipurl.com/8v6b> may help you accomplish this.

If things are running a bit slow 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 a bit by turning off some of the memory using 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 many 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/mess with one (or more) of the Microsoft Powertoy – TweakUI in particular:

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

You should also verify that your System Restore feature is enabled and working properly. Unfortunately, it seems to have issues on occasion, ones that can easily be avoided by turning off/on the system restore and make a manual restoration point as one of your periodic maintenance tasks. This is particularly important right before installing something major (or even minor if you are unsure what it might do to your system.) (This, of course, will erase any previous restore point you have.)

Turn off System Restore.

<http://support.microsoft.com/?kbid=310405>

Reboot.

Turn on System Restore.

<http://support.microsoft.com/?kbid=310405>

Make a Manual Restoration Point.

<http://snipurl.com/68nx>

Also, you should look into backing up your valuable files and folders.

<http://support.microsoft.com/?kbid=308422>

And keep your original installation media (CDs, disks) safe with their CD keys and such. Make backups of these installation media sets as well and always use strong 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/logon name.

UPDATES and PATCHES

** Side Note: *IF* you are about to install Service Pack 2 (SP2) for Windows XP, I suggest you clean up your system first. Uninstall any applications you do not use. Update any that you do. Download the latest drivers for your hardware devices. Defragment and run a full CHKDSK on your hard drives. Scan your system and clean it of any

Spyware/Adware/Malware and for Viruses and Trojans. Below you will find advice and links to applications that will help you do all of this. If this advice helps you, please – pass it on. Print it, email it, forward it to anyone you think it might help. A little knowledge might help prevent lots of trouble.

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.

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. For example, for Microsoft Office update, you should visit:

Microsoft Office Updates

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

(and select "downloads")

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 (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. First – how do you know what hardware you have in your computer? Invoice or if it is up and working now – take inventory:

Belarc Advisor

http://belarc.com/free_download.html

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

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>

Microsoft 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 FW 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, some helpful tips for the SP2 enabled firewall can be found

here:

<http://www.microsoft.com/technet/community/columns/cableguy/cg0204.msp>

If you read through that and look through the pages that are linked from it throughout – 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 FW, but truthfully – any of these alternatives are much better than the Windows XP FW at what they do – because that is ALL they do.

ZoneAlarm (Free and up)

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

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/>

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 gleaned from one or the other firewalls you run.

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 careless? And for the average joe-user who is careful, uses their one to three family computers carefully, never opening unknown email 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/nav/nav_9xnt/

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 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! (Free and up)

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

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)

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!

SPYWARE/ADWARE/POPUKS/HIJACKS

So you must be thinking that the above two things got your back now – you are covered, safe and secure in your little fox hole. Wrong! There are more bad guys out there. 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://mvps.org/winhelp2002/unwanted.htm>

For more updated information.

Spybot Search and Destroy (Free!)

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

Lavasoft AdAware (Free and up)

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

CWShredder (Free!)

** No longer updated as of July 29, 2004 – however, still a great product and should still be ran **

http://www.softbasket.com/download/s_8114.shtml

Hijack This! (Free)

<http://mjc1.com/mirror/hjt/>

(Tutorial: <http://hjt.wizardsofwebsites.com/>)

SpywareBlaster (Free!)

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

IE-SPYAD (Free!)

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

ToolbarCop (Free!)

<http://www.mvps.org/sramesh2k/toolbarcop.htm>

Bazooka Adware and Spyware Scanner (Free!)

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

Browser Security Tests

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

Popup Tester

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

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 and IESPYAD)

have/are immunization utilities 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. 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/>

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>

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 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. 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

microsoft.public.windowsupdate: Re: Beware! spyware on windows update

goes MUCH faster! (or if you have to go back and re-enable things..)

Task List Programs

http://www.answersthatwork.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

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", it is suggested you research for yourself before you take any advice - you are the one ultimately responsible for your actions/problems/solutions. Know what you are getting into before you jump in with both feet.