



MBTS TEKJOURNAL

November 19, 2004

Volume 3, Number 11

In This Issue

- [Editor's Intro](#)
- [Updates](#)
- [How Do I](#)
- [Surf's Up](#)
- [Tweaks](#)
- [Viruses](#)

Category of Links

[SpySweeper Trial](#)

Download a trial version of software to help clean up your system free of Spyware

[Window Washer Trial](#)

Download a trial version of software to help clean up useless file from your system

[What is my IP](#)

A link to help you identify your IP address even behind a router

[PC PitStop](#)

A link to help you identify your bandwidth speed

[Bandwidth.com](#)

Another link to help you identify your

From the desk of MBTS

Here is a Big Thank You to our existing clients for all your referrals recently. For our new clients, Welcome to the latest edition of the MBTS TekJournal. We try to publish the MBTS TekJournal on a monthly basis and include information based on questions we receive during the course of our work, information on utilities and program you may find useful, tip, tricks, and tweaks for your system, interesting sites available on the Internet, the latest information on possible virus threats, and often a How To on some aspect of Windows.

The big buzz on currently is none other than Windows XP Service Pack 2, hereafter referred to as XP SP2. There are many different opinions being circulated varying from a great improvement to a big disappointment and everything in between. In this issue we will try to dispel some of the myths and help you figure out what is good and bad about XP SP2.

Updates

It seems that most users have adopted the approach to the Internet of a good anti virus product and a hardware firewall as being all the protection required. But is it really? Just how much security is enough?

Computers today still come with only the bare necessities and in some cases not all of the operating system installed. If your new system isn't behind a firewall while the remainder of the operating system is being installed, you are ripe for infection. The bare minimum for security today is the use of both a firewall and anti virus software. While there are still "free" versions of anti virus software available, you will probably be prompted continually to upgrade to a paid version and the old adage stands true – You get what you pay for.

The new Athlon 64 processors have an added special feature which gets turned on with XP SP2. AMD Enhanced Virus Protection enables your system to Prevent the spread of certain malicious viruses which are transported via email and instant messaging applications. You will still require additional software and hardware to be really safe, but this processor is a step in the right direction.

The firewall protection built into Windows XP should be turned on and is another line of defense in the ongoing battle for security, but more on that later.

The one area that most users seem to overlook is infection from Spyware and Adware. Since we are starting to win the war on computer viruses, this new frontier is expanding rapidly. To help keep your system even safer, we recommend the use of SpySweeper by Webroot.

SpySweeper stops Spyware from invading your system when you are surfing and controls the types of cookies that your system will allow. The latest version also blocks Common Ad Sites using the built-in Windows Hosts file.

There is a [free 30 day trial](#) of this product available from Webroot. The purchase price in most stores today range from \$ 36.99 to \$ 39.99 or you can purchase a two year option on the web

[bandwidth speed](#)

[Broadband](#)

[Reports](#)

Another link to help you identify your bandwidth speed

[Kelley's Corner](#)

A list of possible tweaks for Windows XP

[Contact Us](#)

[Visit our Website](#)

[E-Mail MBTS TekJournal](#)

at \$ 39.99 US. Given the current rate of the Canadian dollar, and the fact that all protection software must be updated annually, the two year option appears to be the best value.

How Do I...

Interpret what's new in Windows Service Pack 2 ?

Software manufacturers today seem bent on deciding for us what we should be able to do and what we shouldn't. Norton and McAfee both have Internet Security software which virtually take control of the operation of your computer system and the result is a much slower system that you had before you installed these products. XP SP2 sort of expands on this premise with a lot of it's own safeguards, and it is probably because users are demanding more security while not helping the situation. Here is a list of what's turned on is XP SP2 and whether you can turn it off.

Security Centre: This is a new feature to Windows allowing users to check the status of the Firewall, Automatic Updates, and Anti Virus software all from a single point. But the big question is "Who cares?" If the Firewall is turned on, and it is automatically with the installation of XP SP2, and Automatic Updates are turned on as they are when you answer the first recommended prompt after installing XP SP2, and you have a legal current copy of Norton or McAfee which updates automatically, why would you ever want to open the Control Panel and access the Security Centre to see if it is still set properly? Probably never, but it's there in case you want to. In my mind it is an unnecessary service and can be turned off. Here's how:

1. Open Control Panel
2. Open Administrative Tools
3. Open Services
4. Scroll down the list to Security Centre and double click on it to open it
5. Change the startup prompt to Disabled
6. Click the Stop button
7. Click OK
8. Close Services, Administrative Tools and Control Panel

Automatic Updates: This one major complaint among users has been around for a long time, and it doesn't seem to be going away. The good news is that Microsoft seems to have gotten it right this time, but the bad news is that the default setting is to do Automatic Updates at 3:00 in the morning when you are asleep. The problem with this is that most people don't leave their systems on overnight and if updates are pending when you shut down your system it will remain at the logoff screen saying that updates are in progress and you may damage your system if you interrupt the process. However, nothing will actually be done until the actual set time of 3:00 am. Luckily this can be changed:

1. Open the Control Panel
2. Open the Automatic Updates option
3. Select the day and time most agreeable to you, or select the option that says "Download updates for me but let me choose when to install them". This option puts the onus on you to check the system tray periodically to see if there are updates to be applied and then apply them.

Windows Firewall:

There is a mixed feeling about this feature as to whether it is beneficial or harmful.

If you have a hardware firewall, and there are no other computers attached to your computer

on a network, do you really need this service? Probably not, but maybe...

If you have a hardware firewall and you are connected to a local area network, you may find this feature reassuring, but the firewall accepts all traffic between computers on a local area network as being secure. So is it helpful? Again, probably not, but maybe...

If you have a hardware firewall, and you are on a local area network, are all the other computers also running anti virus software and XP SP2? If not, Yes you do want to keep this feature.

What is meant by probably not, but maybe...?

A hardware firewall lets you hide your computer from the Internet by masking the computers IP address. The IP address is what is used to identify your computer to the Internet. If you have a hardware firewall, otherwise known as a router, log into it and check the status tab. You will see the actual IP address used to identify you on the Internet. Generally just above that information is the IP address used to identify you on the Local Area Network, or LAN. These numbers will be different. Without the router, anyone could probably attach to your computer using the WAN IP Address without too much trouble. But with a router, trying to access the WAN IP Address results in an error. Try it yourself.

Here is a quick way to [Identify My IP Address](#). Write down that number. Now, open Internet Explorer, or Firefox, or Opera, or Netscape, or whatever you use to access the Internet, and enter that IP address into the address bar and press Enter. What happens? The request is routed through the Internet and back to your own computer where the router denies access because that is one of the functions of a router. To stop unauthorized access to your computer. Try it again with the private IP address from your LAN and you will probably get a login dialog box from your router. If you have the proper id and password you will be allowed entrance.

So if you have a router (hardware firewall), do you really need the Windows Firewall turned on? Probably not. The Maybe option comes next.

If you are operating a Local Area Network and not all the computers are using Windows XP or Windows 2000, or they are using Windows XP but you haven't upgraded all of them to XP SP2, then you probably want to keep the Windows Firewall operational, just in case.

According to Microsoft "When someone on the Internet or on a network tries to connect to your computer, we call that attempt an "unsolicited request." When your computer gets an unsolicited request, Windows Firewall blocks the connection. If you run a program such as an instant messaging program or a multiplayer network game that needs to receive information from the Internet or a network, the firewall asks if you want to block or unblock (allow) the connection. If you choose to unblock the connection, Windows Firewall creates an exception so that the firewall won't bother you when that program needs to receive information in the future." The blocking of "Unsolicited Requests" is a normal function of a firewall and even if you have a hardware solution (router) it doesn't mean that these "Unsolicited Requests" will always be denied. It depends on which side of the firewall they occur on. If they occur on the computer side due to some program you unknowingly downloaded, like from a shared music site, only a software firewall dedicated to catching this type of invasion will catch it. So for this reason you probably want to leave the Windows Firewall turned on.

Anti Virus Monitoring: Personally, I use Norton Anti Virus and I updated to the latest version every year. Since I started using Norton Anti Virus I have not been infected by a virus while it has been operational. I do however have CD's I have created from systems employing other anti virus solutions that appeared to be clean but that Norton has found viruses on. Therefore, I personally feel that Windows monitoring my Anti Virus product is a complete

waste of time and resources. However, that doesn't mean it shouldn't be turned on.

When I first installed XP SP2, the Security Centre always popped up and told me I had no anti virus software on my system even though I knew Norton was installed and active. It wasn't until recently that a WMI update was available via Norton's Live Update that allowed me to share the Norton status with Microsoft Windows XP. But even after installing this fix, occasionally when Windows is starting the Security Centre will display the annoying message that my anti virus software is not installed or not current and then will disappear after Norton have loaded fully.

If you plan on leaving the Security Centre active, and never want to see this annoying message, use the following steps:

1. Open Control Panel
2. Open Security Centre
3. Expand the virus protection banner by clicking on the down arrows at the right of the banner
4. If there is a note that says your anti virus software may not be installed properly or functioning properly, click on that notice
5. At the bottom of the displayed dialog box you will see a check box that says you will monitor the monitor the anti virus software on your own. Make sure there is a check mark in that box and you will never see the annoying popup again.

Pop Up Blocker: Something Microsoft has finally addressed and implemented successfully is a pop up blocker and Information Bar for Internet Explorer. This feature was originally available as an add-on to Internet Explorer in the form of the MSN Toolbar. If you have the MSN Toolbar you can safely uninstall it and just use the built-in version in XP SP2.

To access the pop up blocker open your Internet settings, either from the Control Panel or via the Tools option in Internet Explorer, and click on the Privacy Tab. If you click on the Settings button you will be able to identify specific sites when you want pop ups to appear. There actually are sites where this is desirable, but only you will know the ones to add.

On this screen you may also identify if you want a sound to play or the Information Bar to appear whenever a pop up is blocked. It is always a good idea to have the Information Bar appear because you may be on a site, like a registration site for software or hardware that you have just installed where they use pop ups to allow you to register. Without the Information Bar there will be no physical identification why the registration box doesn't appear.

This dialog box also allows you to determine the level of blocking you want Windows to perform. The default is Medium.

- Low: Allow Pop ups from Secure Sites
- Medium: Block most automatic pop ups
- High: Block ALL pop ups (Ctrl to override)

Or you can remove the check mark beside Popup Blocker on the Privacy screen and go back to surfing the Internet the way we have all been doing since the beginning.

System Restore: I honestly can not remember if the ability to set the monitoring of System Restore on each partition is new or existing. Here is a suggestion for all users with huge hard drives and multiple partitions on their computers.

System Restore is an option introduced in Windows Millennium which created a point in time whenever a major change happened on your computer. The reasoning was that if the software or hardware you added caused your system to malfunction in any way, you could go back (or

Restore) your system to the way it was before you made the change. Unfortunately when System Restore is activated it is activated for all partitions on your system. Since the only partition that needs restoring is the primary partition where your system files and registry are located, why should you waste resources on monitoring other partitions? You may want to turn off System Restore on all the partitions where it really isn't required and free up a little disk space and system resources.

1. Open Control Panel
2. Open the System icon
3. Click on the System Restore tab
4. If you see more than just the C drive partition being monitored and want to turn off the others, highlight the drive in question, click Settings, put a check mark in the box marked Turn off System Restore on this drive, and click OK

To make sure you are not wasting a lot of drive space on System Restore points:

1. Click start and select Help and Support
2. Click the option for Undo changes to your computer with System Restore
3. On the screen that appears offering to Restore your computer to an earlier time, click Next
4. Count the number of BOLD Dates where there are restore points you can choose from. If there are more than 30, going back over the last three months, there are probably too many and you may be wasting disk space. Click cancel to get out of this screen and then close the Help and Support Centre.
5. Go back to the System Restore tab (see above) and highlight the C drive and click on Settings
6. If your disk usage for System Restore points is greater than 5%, you are possibly dedicating too much space to this purpose and you may want to decrease it. Move the slider to the left to decrease the amount space reserved for this task and click OK. You may be prompted with a dialog box saying that there may be fewer Restore points available because of this action – if you really want to continue click OK
7. Click Ok to close the System Restore dialog box and close the Control panel

There are also new features for setting up networks and for Wireless networks, but we will leave those for another time.

Surf's Up...

Recently, it has come to our attention that some Internet providers are offering an Extreme package offering higher upload and download speeds. We covered testing your own bandwidth in an earlier newsletter, but it bears repeating here. The reason is that major blog sites are claiming the new Extreme sites to be a lot of hot air and a flash in the pan. They don't live up to their claim in every case. I personally don't know if it is true or not, but I do know how you can test it yourself. Here are three sites you can surf to and test your own bandwidth and determine for yourself if your speed is fast enough.

[PC Pit Stop](#) Click on the line that says Run Bandwidth Test

[The Bandwidth Place](#) Click on the Start button. Note: the test from this site can only be run three times in a given month at no cost to the end user.

[Broadband Reports](#) For this site you will need to have Java installed. Pick a site and the test will start. This site determines your download speed and your upload speed.

NOTE: All testing of this value is theoretical and does not display exact speeds with a claimable accuracy.

At different times I have wanted a hard copy printout of all the files in a particular

directory on my system. Unfortunately there isn't such a utility built into Windows but if you know where to look you can find almost anything. With a little effort I found a pretty good program called [Print Folder](#) which adds an option to the right click menu in Windows Explorer for just this purpose.

Everybody wants to have a copy of Word or Excel on their computer to do word processing or spreadsheets but they don't want to pay the high price for Microsoft Office. Luckily for us, there are companies who don't believe you should have to pay high prices for this type of software. Two such products available at NO COST are [OpenOffice](#) and [602PC Suite](#). You will have to judge for yourself which is the better of the two, however each is rated as the best depending on the site you visit or magazine you read.

I used to use Quickbooks for my accounting and really like the fact that my invoices were created in a PDF format for easy delivery by email. Simply Accounting in it's native form is not so nice when it comes to creating an invoice for email. So I made my own, but on some computers it doesn't print totals, on some it leaves out the lines, on others it just prints garbage. So I took a stroll over to [Primo PDF](#) and downloaded a utility that will let me produce any document I want in a PDF format which I can then email. This is a great utility for anyone wanting to create PDF files without having to buy Adobe Acrobat.

Tips & Tweaks

As if there wasn't enough in this issue to have you reeling, here is a site that is sure to blow you away. In searching for a few tweaks which may help your system, we found the following site with over 300 different tweaks already programmed for you. Only you can decide how much you're willing to alter your system, and only you can take full responsibility for that action. **WARNING: If you use Registry Editor incorrectly, or you run scripts created by a third party that alters your current Registry, you may cause serious problems that may require you to reinstall your operating system. MicroByte TekSolutions cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.**

The site we found with lots of tweaks is [Kelly's Corner](#)

While not exactly a tweak, we were looking for something to add a little pizzazz to our hum drum old computer. The original wallpaper that comes with Windows is new and exciting for only such a short time and then you need something new. Here are a few sites offering new wallpapers, screen savers, and sounds. Browse to your hearts content, but only download and install at your own risk.

[Widescreen XP](#) – We clicked on XP Themes to get a look at some really neat wallpaper and screen savers.

Keeping your clock accurate – Windows XP automatically synchronizes your computer's clock with an atomic clock somewhere in the world. The default is located at time.windows.com. But what do you do if suspect the Microsoft clock is wrong? Add more clocks! Here is a list of a few and how to add them:

NOTE:

1. Click start, select Run, key in regedit and press OK to start the Registry Editor
2. Navigate through the registry to
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers
3. Right click on the key area to add a new string value, and label it with the next number in sequence
4. Modify that string value by changing it from blank to the location of another clock. Samples are: clock.linuxshell.net sundial.columbia.edu timex.cs.columbia.edu and ntp.ctr.columbia.edu
5. You can change the default clock to use by editing the default parameter and changing the value to a different clock.

6. Close the registry editor when you are done for the changes to take effect.

Virus Updates

Virus problems just never seem to go away. The latest discovery on November 22nd and at Symantec's threat level 2 is **W32.Yanz.B@mm** - a mass-mailing worm that uses its own SMTP engine to send itself to the email addresses that it retrieves from the infected computer. It will display a message box that says Title: WINDOWS PANIC Message: No Windows. Yes doors and holes.

Other threat discovered recently include:

W32.Inzae.A@mm - a mass-mailing worm that uses its own SMTP engine to spread by sending itself as an email attachment. It copies itself to the system folder as svchosl.pif.

Backdoor.Sdbot.AH - a network-aware worm with backdoor capabilities that spreads via network shares and allows a remote attacker to gain unauthorized access to the infected computer. This problem copies itself to the system folder as wupdmgr32.exe and creates the value of "Windows Update Manager for NT" = "wupdmgr32.exe" in the execution part of the registry so that it will start every time Windows does. It also opens a backdoor on the infected computer by connecting to an IRC server at TCP port 4191 on the following host:

yuzuk.ath.cx

Backdoor.Jupdate - a backdoor program that allows a remote attacker to download and execute files on an infected machine. Copies itself to the system folder using a random name (makes it harder to find) and adds the value JavaUpdate0.07"="%system%\[dropped filename] to the registry key HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run so that the Trojan is executed every time Windows starts.

If your anti virus software is current and updated, and you have added the precautions of a router and Windows XP Service Pack 2, your system should be safe. If you need help cleaning a virus, spyware, or other infection, or would like to improve your systems security, call us at 771 8930 for an appointment.

Thanks for reading...

Ric Jackson

Owner

MicroByte TekSolutions