

## MBTS TEKJOURNAL - 2004

Spring has sprung, the grass has riz, I wonder where the birdies is? That once was a favourite little poem of mine that my father used to recite to us every spring when we were kids. It really is amazing how time flies when you are having fun. I am finding it hard to believe that MicroByte TekSolutions is currently in it's seventh year. To celebrate, check out the TekSpecials at the end of this newsletter for Anniversary savings.

We have really big news this issue: My brother in law has had his first book published and I will be in Toronto on the 17<sup>th</sup> of April for the official launch. The book title is Death in the Age of Steam and you can view the cover and brief synopsis [here](#). Congratulations Mel!

## APPLICATION UPDATES

I have cleaned a lot of systems of Spyware in the last month and most of it came from the search toolbars that can be downloaded and added to enhance your Internet experience. Probably the worst I found was CoolWebSearch which installs an insidious Trojan on your system as well. Cleaning this problem takes special tools available at different sites on the Internet. Other Spyware problems came from installing peer to peer sharing software like KaZaA.

I have been asked many times what to use to accomplish these tasks without infecting a system. I have responded many times that KaZaA Lite is a good sharing program that includes no hidden surprises, but I wasn't sure about add on search toolbars. So I went searching for them and found many offerings to chose and test. But first I had to make sure I had no Spyware on my system, so I checked it with Spybot. It was clean, or so I thought. What if Spybot missed something?

So I decided to expand my testing to include Spybot, Swanksoft's SpyKiller 2004, Webroot's Spy Sweeper, and Lavasoft's Ad-Aware. The following chart identifies what each product found.

Product Used	System Checked	Infected Keys	Infected Folders	Infected Files
Spykiller 2004	PC	12	2	9
Spykiller 2004	Laptop	11	2	4
Spybot S&D	PC	0	0	0
Spybot S&D	Laptop	0	0	0
Adaware 6	PC	2	0	10
Adaware 6	Laptop	2	0	5
Spysweeper	PC	12	0	42
Spysweeper	Laptop	13	0	69

Since I have two separate systems, my wife's PC and my laptop, and I ran each product on each system without cleaning or changing any settings, I estimated that would provide me with the best possible cross section of results. As you can see from the above example, either Spybot S&D failed miserably, or the products you pay for are worth more than the free ones. [Spybot](#) and [Adaware](#) are "free" and [Spykiller 2004](#) and [Spy Sweeper](#) must be purchased.

At this time, I must confess that Lavasoft Adaware 6 appear to be a better "free" product than others available, and Webroot's SpySweeper seems to have excellent protection if you are willing to buy your protection.

My second application update this month is a comparison of both versions of Windows XP. Now that Windows 95, 98, 98Second Edition, and Millennium are no longer supported by Microsoft, the obvious upgrade path is Windows XP. But Windows XP comes in two versions: Home and Professional. Many people have chosen to use the Home version even in a business setting, I think simply to save a little money. If you are a standard home user, wants access to the Internet, plays a few games, and will never attach your computer to any network except the Internet, then the Home version is probably ideal for you. Otherwise your choice should be simple, Windows XP Professional. The following chart may help clear up some of the differences between the two products.

Feature	Home Edition	Professional Edition
Backup and Automated Recovery	No	Yes
Dynamic Hard Disk Support	No	Yes
Default File System	FAT32	NTFS
Encrypting File System Support	No	Yes
Faxing Capabilities	No	Yes
Internet Information Services (IIS 5)	No	Yes
Multiple Language Support	No	Yes
Encrypting File System Support	No	Yes
Multiple Monitor Support (DualView)	No	Yes
Processor Support	Single	Single or Dual
Remote Desktop Connection	No	Yes
Remote OS Installation	No	Yes
Task Manager Network Monitor	No	Yes
ClearType Font Rendering	Yes	Yes
DirectX 8.1 Libraries	Yes	Yes
Fast User Account Switching	Yes	Yes
Integrated CD Burning	Yes	Yes
Internet Connection Firewall	Yes	Yes
Remote Assistance	Yes	Yes
Wireless 802.11b Support	Yes	Yes

## HOW DO I ...

How do I ensure that no spyware or other parasitic code gets into my computer when I download programs and utilities from the Internet?

The only true way to ensure this doesn't happen to you, is abstinence. DON'T DOWNLOAD ANYTHING! Anytime you download something "free" there is bound to be a parasite product called adware, spyware, or even possibly a Trojan. If this doesn't bother you, install "free" stuff to your hearts content. If it does bother you that your system may be invaded, take the proper precautions or wait for someone to do it for you that you trust. Using the proper tools to check during and after the installation will always help, but you must install one product and check, before continuing.

The biggest want of most users of the Internet today is a good search toolbar. I have found many such "free" products and list them below. I first scanned my system for Trojans, Hijackers, Dialers, Spyware, Adware, Viruses, Remote Access and Hack Tools. Then after each installation I rescanned my system for any intrusion. Here are the Toolbars I found and what I found out about them. I used Copernic to narrow down the list of available products and then installed them in order of how they were found.

[Groowe Search Toolbar v1.2](#)- Although you can't search everything all at once, like Copernic, this toolbar does allow searching on Google toolbar, Yahoo toolbar, Teoma, MSN, AllTheWeb, HotBot, Overture, Gigablast, Altavista toolbar, PageTracer, Dogpile, About, AOL, Ask Jeeves, Kanoodle, Monster Jobs, Barnes & Noble Shopping, Tucows and Downolad.com. It also claims that the engines can be updated or changed, and that future upgrades will include more options. HOWEVER - This software adds three Adware units to your system the worst of which may be ZeroPopup. This program modifies the search page and startup page of Internet Explorer and is related to the Tellafriend Trojan which will send a message to everyone in your address book. **Recommendation** – leave it off your future install list.

[Human Nature Review](#) – Their description is "This invaluable free toolbar allows you to search resources such as PubMed, Scirus, Encarta, Encyclopedia Britannica and many other sites directly from your Internet Explorer (v. 5.01 or higher) toolbar. A term can be searched across multiple databases with a single mouse click, and the toolbar can be configured to search the sites that you use most often in your work. It is similar to the Google toolbar but is designed specifically for those involved in the natural sciences, the social sciences and philosophy." HOWEVER – It also installs a minor adware program called the Blowsearch Toolbar which seems like just another toolbar.

[Blowsearch Toolbar](#) – Like many others of its kind this bar includes a search, popup stopper, yellow and white page search, an RSS feed, etc. When I clicked on the Install button it was supposed to display a certificate dialog box saying I trusted these people. It didn't show me that but did offer a straight download and install link which I used. I should have known better... If when you uncover Spyware or Adware there are a few instances of it (10 or less) it shouldn't be doing too much harm to your system (I hope). The Human Nature Review search bar added a little over 20 instances of Adware related to Blowsearch toolbar, so I decided to add this one after removing the Human Nature. The Blowsearch Toolbar adds a whopping 154 instances of Adware in the form of Registry keys, Files, and Folders to your system. Anything that replicates that much can't be good. Recommendation – DO NOT INSTALL.

[Google Toolbar](#) – Everybody seems to love Google as a search site, and now you can install a Toolbar onto your Internet Explorer and be one of the crowd. It installed easily, but because I already had the MSN toolbar visible it didn't show up. Maybe it doesn't like the competition. Anyway, if you install additional toolbars and they don't show up, click on the View menu and select Toolbars, and make sure your new one is checked. If it is and still doesn't show up, turn off one or more of the others until it does, and then turn the others back on and see what happens. Now lets search for bad Spyware and stuff... None found.

The Google Toolbar offers something I haven't seen on any other bar – an Auto Fill section. Here is

where you put in your name, email address, phone number and primary mailing address and even a credit card number, and then when this information is required on the Internet it is automatically filled in for you. Not since Gator has a program offered this (that I know of) and I would be really wary about using it.

[Alexa Toolbar](#) – This toolbar leaves me with a lot of questions. I currently have MSN Toolbar installed on my system and it has a Popup blocker on it which works very well. (see below) The Alexa product is on the fringe of known Spyware and is caught by almost every Spyware removal program available, but they claim on their website that they don't include Spyware in their products. However, the only installation method available is direct from the Internet. Click on the link and a dialog box pops up where you have to agree to the certificate before proceeding. On my system however, the MSN Toolbar blocks this dialog box as if it were an unwanted popup. It doesn't block Veritas, or MSN, or Sun, or Macromedia, or ... I wonder what it is about Alexa that it doesn't like? Considering a form of Alexa ships inside Microsoft Windows XP.

[MSN Toolbar](#) – Search the Internet, block Popups, link directly to MSN Hotmail, My MSN, or MSN Messenger, and find search terms quickly with Highlight. Click on the download and then save the program on your computer for later installation or click on the Open button to install directly. Contains no Spyware, Adware, or other ill effects.

[Dogpile](#) – I know the name is disgusting and conjures up images we would rather not imagine, but I can't exclude a product because of it's name. I can however exclude this product because it installed Spyware on my system even after I told the installer not to. Bad Product!

[Netscape Toolbar for IE](#) – I guess if you can't beat 'em, join 'em. This toolbar installs easily enough by clicking on the download button and then accepting the certificate dialog box, unlike some of the other offers listed here. It also installs no Spyware on your system whatsoever. Additional features on this bar include: an e-mail button that takes me to Netscape's version of Hotmail, a button for the Netscape News Network, the Netscape Weather Network, Horoscopes, Personals, and AOL Instant Messenger. The one addition that seems to be popping up on most toolbars is a Popup Stopper. I have a special site that I use to test these popup stoppers, and this one passes with flying colours.

Winners – MSN, Netscape and Google. All others – Beware.

## SURF'S UP

Every time I begin a new TekJournal, I wonder where on the 'Net I am going to find interesting places to send you. Who am I kidding? The Internet is a cornucopia of interesting places, and some weird ones too. Anyway, this month I had a brain freeze and didn't know where to start. So I turned to Copernic to find interesting and unique sites. I hope you enjoy them.

Did you know that Burt Reynolds once said "My movies were the kind they show in prisons and airplanes, because nobody can leave." Or that "Time is the scarcest resource and unless it is managed nothing else can be managed." was once uttered by Peter F Drucker. Don't know who Peter F Drucker is? Then this could be a neat site. [Brainy Quote](#) – Famous Quotes and Quotations may make you the hit of the next party. This site contains over 43,000 famous quotes by 10,000 authors from Aristotle to Zappa! But the best part is most all quotes have links to Biographies of the people that said them as well as life data such as Birth, Death, etc. Well worth the look.

Everybody loves free stuff and this site has a lot of links to free stuff. [Jeh's Freebies](#) has links to Recipes, Games, Screensavers, Music, Javascripts and lots more.

At [Home Improvement Sites](#) you will find many links to Arranging Rooms, Artful Furniture, Countertops, How to Clean Everything, Bob Villa, Installing Drywall and just about anything you can do to create or change your home.

In the vein of history and museums we can take you to the [Kennedy Space Centre](#) while you are still at home. There is a History section, Multimedia, Educational and media resources, the Spaceport Technology Centre and much more.

Ever wonder about your IQ? We all took tests in public school to test this value (at least us older ones did) but we were rarely if ever told how we did. Well, now you can find out at [IQ and Personality Tests](#). “Our Classic IQ Test is the most thorough and scientifically accurate IQ Test on the Web. Previously offered only to corporations, schools, and certified professionals — it's now available to you from Tickle. It's free, private and developed by PhDs.” 20 simple questions may unlock the answer to the question “What is my IQ?”

My brother in law is a real movie buff and knows just about everything on more movies than I could ever hope to watch. One of his favourite sites that he shared with me recently is [Filmwise](#). This site features movie quotes, unique text, visual quizzes, contests, and the infamous [Invisibles](#). Invisibles shows you a selected scene from a movie with all the characters made Invisible and quizzes you on what the movie is. For all previous quizzes posted the answers are also supplied. If you need a neat party game, print off the quiz and the answers and see how many your guests get right.

[Movie Mistakes](#) shows you all the overlooked bloopers that missed the cutting room floor. Believe it or not there are a whopping 265 bloopers in Pirates of the Caribbean: The Curse of the Black Pearl! There are pictures of the actual footage that shows the mistake, a list of the movies with the most mistakes, popular films of the week and much more. I will warn you that there is a cost to this site, but for a limited time you can log in as a guest for free and see most things that paid subscribers will see. Login as [guest@moviemistakes.com](mailto:guest@moviemistakes.com) with the password of guest.

## TIPS AND TWEAKS

**Windows XP Services** – Windows XP tries to do and be everything for everyone, and in the long run is probably wasting resources that could be better used elsewhere. Lucky for us that the designers thought ahead and put in the Services Control Panel so that we can turn on or off the services we want or not. Here is a short list of services that you can safely disable. To get to the Services tools, click on start | Control Panel | Administrative Tools | Services. To change a setting, right click on the service and select Properties. Change the Startup Type to Disabled and if the service is started, click the stop button.

**Automatic Updates** – Turn this off and disable it, but don't forget that Microsoft send out updates and patches to its operating systems so that the security holes can be plugged. However on several occasions since the release of Windows XP the patches have actually made things worse and in some cases caused systems to fail and required a complete restore back to factory default. Now I never install an update that hasn't been out for at least a week to 10 days.

**Fast User Switching** – If you are the only person using the computer, or you only have one user profile created, you don't need the ability to switch to anybody. Turn this off.

**Messenger** – TURN THIS OFF! This has nothing to do with Windows or MSN messenger, but it has everything to do with the ability to send messages from one computer to another through an open port without interference. Turn this off and close the security hole.

Portable Media Serial Number – This service “Retrieves the serial number of any portable media player connected to this computer. If this service is stopped, protected content might not be downloaded to the device.” If you don’t use external MP3 players to download to, this can be safely disabled and turned off.

Remote Registry – “Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.” Since the System Registry is the heart of Windows XP and knows everything about your system, why would anyone want to have someone have the ability to change it from a remote location possibly without their knowledge or permission? Unless you are a systems administrator of a large corporate network, disable and turn this off.

Secondary Logon – Allows a computer to be fooled into thinking that an Administrator is logging on during the current users session for the sole purpose of running a specific task where Administrative rights are required. Unless your system is part of a corporate network this service is also not required.

Wireless Zero Configuration – This service is turned on in every system by default. If your connection to the Internet and other computers is based on a physical Ethernet Cable being plugged into your computer, you do not need this service. It only pertains to Wireless Networks.

**Correct Time** – Windows, in keeping with trying to do everything well also has a feature that automatically synchronizes your system clock with a server on the Internet that supposedly has more accurate time than your home computer. Lately I have been wondering if mine is really accurate, so when a little program called [Rocket Time](#) crossed my Inbox, I gave it a try. My accurate system that is guaranteed by Microsoft was out by 16.7 seconds. If you want to use Rocket Time instead of the one built into Windows, turn off the one in Windows. start | Control Panel | Date & Time | Internet Time – remove the check mark for time synchronization.

## VIRUS UPDATES

We never seem to be too far away from being infected with viruses, but at least the latest batch seem to be no more than an annoying threat. According to Symantec here is the list of the latest Threat Level One viruses:

**Backdoor.IRC.Aimwin** is a Backdoor Trojan horse that connects to Internet Relay Chat networks. This Trojan can also spread itself through the Kazaa file-sharing network, if the attacker instructs it to do so. Discovered April 1, 2004

**Hacktool.Mailbomb** is a hack tool that allows an attacker to launch Denial of Service (DoS) attacks against email accounts. Discovered April 1, 2004.

**PWSteal.Goldpay** is a Trojan horse that steals passwords, system, and personal information. Discovered April 1, 2004.

**Trojan.Lyndkrew** is a Trojan horse that deletes critical files. Discovered April 1, 2004.

**W32.Gaobot.UM** is a variant of W32.Gaobot.gen. It attempts to spread through network shares that have weak passwords. It also allows attackers to access an infected computer through a predetermined IRC channel.

The worm uses multiple vulnerabilities to spread, including:

- The DCOM RPC vulnerability using TCP port 135.
- The RPC locator vulnerability using TCP port 445.
- The WebDav vulnerability using TCP port 80.
- The Workstation service buffer overrun vulnerability using TCP port 445.

W32.Gaobot.UM is packed with ASPack. Discovered April 2, 2004

**W32.HLLP.Philis.B** is a variant of W32.HLLP.Philis. It prepends itself to all of the .exe files that it finds. It also tries to steal passwords from the "Legend of Mir 2" online game. Discovered April 2, 2004.

These are all good reasons why your Anti Virus software should be current and kept up to date. If yours is about to expire, contact us at (204) 771 8930 or by email at [tekjournal@mbts.mb.ca](mailto:tekjournal@mbts.mb.ca) for assistance.

## TEKSPECIALS

Intel P4 3.2 GHz (800 MHz FSB) Computer system with 512MB 400MHz DDR, on board Video, Audio, 10/100 LAN, 52x24x52x CD RW & 16xDVD combo drive, Seagate 40GB 7200 rpm Hard Drive, Microsoft Wireless Desktop, Microsoft Windows XP Professional, LG Studioworks 17 in Colour Monitor – **TekJournal Anniversary Special Price \$ 1550.00** plus PST & GST delivered. (Installation extra)

Intel Celeron 2.6 GHz Computer system with 512MB PC-2700 DDR, GeForce 4 MX 64MB Video, on board Audio, 10/100 LAN, 52x24x52x CD RW & 16xDVD combo drive, Seagate 40GB 7200 rpm Hard Drive, Microsoft Wireless Desktop, Microsoft Windows XP Professional, LG Studioworks 17 in Colour Monitor – **TekJournal Anniversary Special Price \$ 1225.00** plus PST & GST delivered. (Installation extra)

LG Flatron LCD Flat Panel [Model 1715SK](#) up to 1280 x 1024 resolution, 16 ms response time, 450:1 contrast ratio - **TekJournal Anniversary Special Price \$ 700.00** plus PST & GST delivered. (Installation extra)

LG Flatron LCD Flat Panel [Model L1910S](#) thin frame design, 19 inch, brilliant TFT display with auto-synchronous support up to 1280 x 1024 @ 75Hz, an industry leading viewing angle of 176 degrees - **TekJournal Anniversary Special Price \$ 995.00** plus PST & GST delivered. (Installation extra)

AMD XP2800 2.08GHz 640k Cache Computer System with Raidmax Scorpio 668 Case w/420 watt power supply, 512MB 333MHz DDR, on board Video, Audio, 10/100 LAN, 52x24x52x CD RW & 16xDVD combo drive, Seagate 40GB 7200 rpm Hard Drive, Microsoft Wireless Desktop, Microsoft Windows XP Professional, LG Studioworks 17 in Colour Monitor – **TekJournal Anniversary Special Price \$ 1150.00** plus PST & GST delivered. (Installation extra)

Thank you for reading.

See you again soon.

Ric Jackson  
Owner  
MicroByte TekSolutions