

## MBTS TEKJOURNAL - 2004

The weather outside is terrible, so I am glad I get to stay indoors today and finish the latest MBTS TekJournal. Toronto was a busy trip, but very enjoyable. I turned the big 50 while I was there, saw lots of friends and clients and had fun at my brother in laws launch of his new book Death in the Age of Steam. I have been told he will be making a trip across Canada later this year to continue the launch in many different cities, and I will let you know more details once I receive them.

There has been a lot of new virus activity with the Sasser Worm, which was originally discovered on April 30. W32.Sasser.Worm is a worm that attempts to exploit the vulnerability described in Microsoft Security Bulletin MS04-011. It spreads by scanning the randomly selected IP addresses for vulnerable systems. This worm can run on earlier versions of Windows, 98 – 98SE – Millennium, and even though it doesn't actually infect those systems it can be used to infect other systems if let on its own. The original virus creates a mutex (Mutex - Short for mutual exclusion object. In computer programming, a mutex is a program object that allows multiple program threads to share the same resource, such as file access, but not simultaneously. When a program is started, a mutex is created with a unique name. After this stage, any thread that needs the resource must lock the mutex from other threads while it is using the resource. The mutex is set to unlock when the data is no longer needed or the routine is finished.) named Jobaka31 and will exit your system if it fails. However, if successful it Adds the value:

avserve.exe="%Windir%\avserve.exe to the registry key:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run so that the worm runs when you start Windows. The execution of the worm causes LSASS.EXE to crash on some systems. The W32.Sasser.B.Worm uses a different mutex - Jobaka3, a different file avserve2.exe and creates the registry entry avserve2.exe. The W32.Sasser.C.Worm also uses a different mutex – JumpallsNlsTillt, launches 1024 threads instead of 128, but still uses and creates registry entries with avserve2.exe. The W32.Sasser.D.Worm uses yet another mutex - SkynetSasserVersionWithPingFast., a different file name - skynetave.exe, is 16,384 bytes in size uses a different port for the remote shell and does not properly execute on Windows 2000 systems. The last found variation (May 9, 2004) called W32.Sasser.E.Worm is a minor variant of W32.Sasser.Worm. It attempts to exploit the LSASS vulnerability, described in Microsoft Security Bulletin MS04-011, and spreads by scanning randomly selected IP addresses for vulnerable systems. W32.Sasser.E.Worm uses the mutex SkynetNotice and has named its file lsass.exe. The ports used are 1023 and 1022 and after running for two hours it displays a message. It will delete values from the registry originally installed by Trojan.Mitglieder, W32.Beagle.W@mm, and W32.Beagle.X@mm.

All in all the Sasser worm is really a nasty bug and reiterates the need for checking the Windows Update site regularly for security updates, employing a known anti virus program like Norton Anti Virus 2004 to check for viruses, Trojans, dialers, and other Spyware, and also using a hardware firewall. Software firewalls are good but may require constant updating to remain effective. If your system uses a hardware firewall there is no need for a software firewall and if you use a software firewall select only one.

The old adage if one is good two is better does not work with anti virus software or firewalls. Conflicts will arise from using more than one version and your system will suffer.

In this issue we have an application update on Microsoft Word. In versions of Office XP and Office 2003, Word has expanded on the use of Mail Merge and included Wizards to make its use even easier. We will show you how and then ask you to verify your information. We have tested it several times and can guarantee the information you see in your newsletter is unique to you and cannot be seen by anyone else. This section will be modified in the on line edition.

The How Do I... Section this issue will feature a lot of tweaks and settings for Windows XP that you can use to customize your own system. Surf's Up features freeware, online games, and help for some Windows utilities, and the Virus section identifies other virus to watch out for. The TekSpecials feature systems, monitors, and optical drives. We hope you enjoy reading this issue.

## APPLICATION UPDATES

In this edition of Application Updates we will show you how to use the Mail Merge feature in Word XP and Word 2003 to personalize you mass mailings.

### **Set Up**

You always start with a main document which contains the text, formatting, and other elements that will not change. You can either use an existing document, or start a new one from scratch. To start the Mail Merge process, point to Letters and Mailings on the Tools menu, and select Mail Merge. By using the hyperlinks in the task pane you can navigate through the entire process.

\*\* NOTE: in Word 2002 on the Tools Menu point to Letters and Mailings and the click Mail Merge Wizard.

### **Select the Document**

The first steps to take are selecting the type of document and then the main document you want to use. Types of documents include: Letters, emails, envelopes, labels, or a directory. The main document is the actual document that you want to send out many times, like this document you are reading for example.

### **Select the Database**

To merge information into your document you will need a database of names and addresses of who should receive the information you are preparing. You can select the recipients from an existing list, from your contacts in Outlook, or you can create a new independent list. Microsoft Outlook is an excellent source for information assuming you

keep up to date information on those you wish to contact including full names, mailing addresses, email addresses, etc.

### **Select the Recipients**

Once you have decided on which list to use, select the names from that list by putting a check mark in the little box beside each name. This box will appear after you have selected the data source to be used. Using the data source you can sort the records by clicking on the field names above each column, you can filter out records based on different criteria, click Nonblanks to display only those records that do not contain blank information, use the command buttons to select (or de select) all records, and check or uncheck a record to include/exclude from the task. Once you have selected the records you are ready for the next step of adding fields to the main document.

### **Add the fields to your document**

Now that you have chosen the group to receive your information you must then add the pertinent fields to your document which helps to personalize it. You can start with a very formal Address Block including the recipient's name, Company Name, and Mailing address; or select a greeting line Dear ... or Dear Sir or Madam if no name is available; you can add a postal bar code if you wish, and you can also select from individual fields in the available database and add your own text. For example, since I know you are reading this newsletter here is where I will ask that you verify the information I have on file for you is correct.

Client (last name , First) : **Schultz, Justin**  
Company (if applicable) :  
Address : **26 - 100 Wickham Road**  
City : **Winnipeg** Province : **MB** Postal Code : **R2J 2L4**  
Phone Number :  
Cell Phone Nbr: **(204) 324-3201**

From the entire list you can pick and choose which fields you include in your note. Here is where I would like you to copy the above information and send me a new email telling me if your information is correct, and identifying any changes which are required. It would also be nice, but is optional, for you to tell me what you think of the TekJournal, anything that you would like to see added, removed, changed. Thanks in advance for helping me to keep my records up to date.

### **Preview, Change if required, and Send**

Once you have added all the fields you want, or think you want, the next step in the wizard is to preview what you have. Once you have seen the preview you can always go back and make changes or adjustments, you can review the recipient list and make changes to who it will be sent to, add formatting to fields like Bold, Italics, Underline,

Colour, etc. When you are completely sure you have everything the way you want it, do another preview, and then complete the merge.

## HOW DO I ...

This is the section many people have been asking for – lots of tweaks and settings for Windows XP. To put all of them in here is impossible, but we are redesigning the Help section of the website and including close to 100 new settings tweaks not including the ones listed here.

### **Remove the Recycle Bin Confirmation**

- Right-click the Recycle Bin and then click Properties.
- Clear the Display delete confirmation dialog check box, and then click OK.
- **NOTE** If you are really brave and don't want to use the Recycle Bin at all, you can select the Do not move files to the Recycle Bin prompt. Remove files immediately when deleted check box. But remember if you do this and delete something you really shouldn't have, the possibility of getting it back yourself is next to impossible.

### **Using the Windows Logo Key**

This is the key usually found between the Ctrl and Alt keys on your keyboard. In Windows XP, pressing the Logo Key is like pressing Ctrl + Esc in that the Start Menu pops up. Here are a few more uses:

- Use Windows + D to minimize or restore all windows
- Use Windows + E to display Windows Explorer
- Use Windows + F to search for files on your system
- Use Windows + Ctrl + F to Search for other computers on the network
- Use Windows + F1 to display the Help and Support Center
- Use Windows + R to display the Run dialog box
- Use Windows + break to display the System Properties dialog box
- Use Windows + M to minimize all open Windows and show the desktop
- Use Windows + shift + M to undo the minimize all windows command
- Use Windows + L to Lock your workstation
- Use Windows + U to Open Utility Manager

### **Don't Highlight Newly Installed Programs**

Whenever you install a new program in Windows XP it gets highlighted on the All Programs menu. I find this terribly annoying, after all I know what I installed and I don't need Windows to remind me. I haven't totally lost it yet. Here's how to turn off that annoying helper.

- Click Start, right-click at the top of the Start menu where your name is displayed, and then click Properties.
- In the Taskbar and Start Menu Properties dialog box, on the Start Menu tab, click Customize.

- Click the Advanced tab, and then clear the Highlight newly installed programs check box.
- Click OK, and then click OK again.

### **Only Open Menus when you actually click on them**

Windows does actually make your life easier unless you are in a hurry, then it drives you nuts. When I need some information NOW, I click on the start button and then on the All Programs button and invariably the program menu flashes before my eyes. This is because I haven't turned off the prompt to Open Submenus when I pause on them with my mouse. Here's how to turn that off.

- Click Start, right-click at the top of the Start menu where your name is displayed, and then click Properties.
- In the Taskbar and Start Menu Properties dialog box, on the Start Menu tab, click Customize.
- Click the Advanced tab, and then clear the Open Submenus when I pause on them with my mouse check box.
- Click OK, and then click OK again.

### **The On Screen Keyboard**

Has your keyboard ever quit working? Maybe it is a hardware failure, maybe the batteries are dead, maybe the cable got pulled out by accident and it's not a USB cable so you can't plug it in without doing a shutdown first, but you need a keyboard to key something in.

- Use the Windows Logo key and R to popup the Run Dialog box
- Key in osk into the Open dialog area
- Press enter or OK

The Window On-Screen Keyboard pops up on the bottom of your screen and you can now use your mouse to type.

### **Change the Vertical space between icons**

I have never been a proponent of having icons clutter your desktop, but sometimes they may be required. However, the default spacing may be too close for you to be able to see or read them clearly.

- Right-click the desktop, and then click Properties.
- In the Display Properties dialog box, click the Appearance tab, and then click Advanced.
- In the Item box, click Icon Spacing (Vertical).
- Decrease the size, click OK, then click Apply to see the result on screen.
- When you're happy with the results, click OK.

### **Personalize your Logon name**

The pictures supplied with XP to identify different users are okay, but they lack pizzazz. I am not properly represented by a soccer ball or a yellow rubber ducky! If you have a web cam, or a digital camera or just a neat picture you really like, you can identify your logon name with something other than the standard pictures.

- Click Start, click Control Panel, and then click User Accounts.

- Click your account name, and then click Change My Picture.
- Click the picture you like, and then click Change Picture.
- To find the user's picture, click Browse for more pictures, click the picture you want to use, and then click Open.

### **Display and Use the Quick Launch Bar**

Everything that sits on your desktop gets stored in memory including the wallpaper, the icons, and the icons position. Since this memory space is limited no matter how much memory is in your system it is better to use the quick launch bar than to clutter up your desktop.

- Point anywhere on the task bar and right click your mouse
- Point to Toolbars and select Quick Launch

You will see a new group of icons appear like magic beside the Start button. To move icons from the desktop to the quick launch area, Right Click and hold the mouse button on the icon to move. Next drag the icon to the area beside the Start button. When you release the mouse button you will be presented with three options – Copy – Move - Create Shortcut, & Cancel. Select Move.

Once you have more than three icons beside the Start button you will see a small chevron at the end of the Quick Launch bar. Click on the chevron >> and the Quick Launch Menu appears. Right click anywhere on the menu and you can choose to Sort by Name to order the list alphabetically. For the three (3) icons you use most often, you can rename each icon and put a number in front of them, say 0 1 and 2. Numbers are always sorted first.

### **Change your Folder Icons**

Folders are manila in colour and boring. I have spruced mine up by selecting pictures to display rather than the boring file folder colour that comes as default. Since you can only see pictures in Thumbnail view I have included that as step one.

- Open Windows Explorer
- Click View and select Thumbnails
- Right-click a folder and then click Properties
- Click the Customize tab and then click Choose Picture.
- Select any image on your computer, click Open, and then click OK.

### **Change the default Open Folder in Windows Explorer**

I don't know about you, but I never open a document by double clicking on the document name in Windows Explorer. I use the program it is associated with. When I open Windows Explorer I want to see the drives on My Computer because I am usually looking for something on a particular drive. Here is how I changed my system to work my way.

- Click Start, point to Programs, then Accessories, then right-click Windows Explorer, and click Properties.
- Under Target field, which reads %SystemRoot%\explorer.exe, change the line so it reads %systemRoot%\explorer.exe /n, /e, /select, C:\ (better yet just copy and paste this command line over the existing one)
- Click OK.

### **Disable the Shutdown Button on the Welcome Screen**

When you start your system and you have more than one user your system always starts at the Welcome screen. In the bottom left corner is an option to Shutdown Windows which may be something you want to disable if you have small children that like clicking the mouse on the screen just to see what will happen.

- Click Start, click Control Panel, click Performance and Maintenance, and then click Administrative Tools.
- Double-click Local Security Policy.
- Expand Security Settings, then expand Local Policies, and then click Security Options.
- In the right pane, double-click the Shutdown: Allow system to be shut down without having to log on policy, click the Disabled radio button, and then click OK.

### **Speed up menu display**

- Click Start, click Control Panel, click Performance and Maintenance, and the click System.
- Click the Advanced tab, and under Performance, click the Settings button.
- Clear the Fade or slide menus into view check box, and then click OK.

## **SURF'S UP**

Do you have large files that are not protected by a copyright and are not pornographic in nature that are too big to easily pass from one person to another using email? Then [Drop Load](#) is for you. Drop Load is a web site that will provide you with up to 50MB of space for you to share data, pictures, freeware, etc. with other people when email transfers just won't work. The catch, after 48 hours your space will automatically disappear. Check out the site for more information.

I have always enjoyed a good game of scrabble, but scrabble solitaire is not my idea of fun. There never seems to be any good players around when you want to play, like maybe 3 o'clock in the morning. Well, now there is. Welcome to the [Internet Scrabble Club](#). The ISC is the best place on the Internet to play Scrabble in a relaxed friendly environment. You can compete at your own level in English, French, Romanian, Italian, or Dutch while meeting new people and making friends from around the world. Registration is free.

How many people still use Outlook Express? Ever wish there was a "free" utility that would let you backup you email information so it doesn't get lost when your hard drive fails? Now there is and it is available at [OEBackup](#).

Are the standard Windows icons just not doing it for you? Do you feel the need to add a new dimension to the icons you visit every day? Then [Pixie Girl Presents](#) is a site you might want to check out. "Our award-winning site will allow you to snag the slickest

**Mac OS X, XP and Icontainer icons and desktop images** while feeding your cravings for links and tutorials!”

Do you want [Surround Sound](#) from Windows Media Player 9? This site from Microsoft shows you how to achieve it.

If you like action games and war games then [America's Army](#) may be just the game you've been looking for. America's Army: Soldiers, gives gamers a chance to role-play the Army experience, from signing up at the recruiter to handling basic training to taking their first tour of duty. Players choose the attributes, career path, and goals for their character and apply six different resources to reach each goal. We hope you have High Speed Internet and some time on your hands, the full client is a whopping 652MB. Download for free and enjoy the war games.

[Only Freeware – No Shareware](#) is a site that seems to pop into my radar from time to time. It is a great place to start looking for that utility or small program to do a special task that you don't want to pay commercial prices for. To name a few categories: Anti Virus, Compression Utilities, Email Stuff, File Managers, Graphics, Money, Organizers, registry, Search Tools, Time Clients, and much, much, more...

## VIRUS UPDATES

If we didn't scare you enough with the text on the Sasser Worm at the beginning of the newsletter, here are the latest viruses to watch for in addition to Sasser.

**W32.Gaobot.AJD**, identified on May 11, is a worm that spreads through open network shares and several Windows vulnerabilities including:

- The DCOM RPC Vulnerability using TCP port 135.
- The WebDav Vulnerability using TCP port 80.
- The Workstation Service Buffer Overrun Vulnerability using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The UPnP NOTIFY Buffer Overflow Vulnerability.
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit using UDP port 1434.
- Exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow

The worm also spreads through backdoors that the Beagle and Mydoom worms and the Optix family of backdoors install. W32.Gaobot.AJD can act as a backdoor server program and attack other systems. It attempts to kill the processes of many anti virus and security programs.

Also on May 11, the **W32.Wallon.A@mm** mass-mailing worm that sends email messages containing a hyperlink to download the worm body from certain URLs. It also harvests the email addresses on the infected machine. The worm exploits the following vulnerability: Microsoft Security Bulletin MS04-004.

Both of these threats are currently classified as Level 2 threats by Symantec. Keep your anti virus software up to date. If it has expired, or you don't currently have anti virus software installed, call us at 771 8930 for help.

## TEKSPECIALS

LG CD RE-WRITER / DVD COMBO 52x24x52 & 16 DVD \$ **98.00** plus PST & GST  
*Installed*

LG GMA-4081B 8x DVR CD-R, CDRW, DVD-RAM, DVD-R, DVD +R, DVD-RW,  
DVD +RW \$ **172.00** plus PST & GST *Installed*

LGE T710BH E-Z FLAT 17 in .25 FLAT CRT \$ **199.00** plus PST & GST *Delivered in  
Winnipeg* [View Screen Here](#)

LGE T910BU E-Z FLAT 19 in .24 FLAT CRT \$ **365.00** plus PST & GST *Delivered in  
Winnipeg* [View Screen Here](#)

LGE L1910S 19in FLAT PANEL SILVER / CHARCOAL \$ **975.00** plus PST & GST  
*Delivered in Winnipeg* [View Screen Here](#)

LGE L2320A 23" LCD with Media Station \$ **3,900.00** plus PST & GST *Delivered in  
Winnipeg* [View Screen Here](#)

Xerox Phaser 3450 Black and White 25ppm, two sided printing, Laser Printer \$ **940.00**  
plus PST & GST *Delivered in Winnipeg* [View Specifications](#)

We hope you enjoyed this issue. We will be back next month.

Ric Jackson  
Owner  
MicroByte TekSolutions