

MBTS TEKJOURNAL - 2004

I have begun and rewritten this newsletter three times, but this time I am determined to get it done and into your mailboxes. So many things are going on right now, and people are asking about different safety issues, I keep getting sidetracked. But today, January 26th seems to be the biggest yet: Symantec is calling the **W32.Novarg.A@mm** mass mailing worm and it is a dilly. It is to be feared, and deleted immediately if not sooner. McAfee is calling it **MyDoom** and it deals a DoS or Denial of Service payload which will begin on February 1 and end on February 12 if not brought under control.

A DoS attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. In short, a very large group of computers all ping a single IP address continuously so that normal traffic cannot get through. Assume that the call waiting on your phone is not limited to one caller, but that you can interrupted an unlimited number of times. A DoS on your phone would be thousands of call interrupts per second every time you use your phone. Instead of a periodic beep beep to signify an incoming call, all you would hear when you picked up your phone is a steady beep.

Other websites are being sent to me as well by people asking if it safe for their children to be using them. Since I don't have children I can't tell anyone how to raise theirs, but I can let you know that the Internet can be very scary where scruples is merely a board game. Although certain sites will ask if the user is over 13, to be able to ask for more personal information, there is no way to verify the user really is over 13. 13 seems to be the magic age where an Internet user can legally give out personal information without recrimination from other sources. I will provide more information on this matter later.

APPLICATION UPDATES

I have received a few notes asking about the safety of an add-on for MSN Messenger called Messenger Plus. Some user's claim to be experiencing strange changes in their systems and the only thing they believe is different is this application. So, on everyone's behalf I decided to do a little checking.

I checked my system for Spyware before beginning, downloaded the application add-on and installed it. When I reran my Spyware checker again, I found no additional Spyware had been added to my system. Since the EULA (End User License Agreement) was 7 typed pages long I didn't read it carefully before installing this application. I did read it afterward and immediately uninstalled Messenger Plus.

Remember the age item above? The EULA stipulates that the person installing the software is 18 years old or older, which if your kids are installing this on your system probably aren't. Even though there are applications available which have been labeled as freeware, nothing is Free. This add-on acknowledges that your home page and search page will be changed, which means you will always be redirected somewhere else in the hopes that you will use, buy, recommend, etc. some other product or site nullifying the free aspect. It also says that a Desktop Tool bar will be installed, but I never found it. If you change the homepage from what the software sets it to, your new homepage will be sent to their servers. There are pages and pages of doublespeak but in short it sounds like you are letting them have permission to send information about you without actually telling you when they do it. The EULA also stipulates that the software will automatically deactivate any current active toolbars, so something you may have purchased to make your experience more enjoyable won't work after installation. The best part is, if anything happens to your system as a result of installing this software, their liability is limited to \$ 5.00US.

My recommendation on this product: even though it seems like it has some neat features, it probably isn't worth the possible risk. If you have installed it, you may want to rethink your decision.

HOW DO I ...

I need some help with the HOW Do I section. I have been using computers for over 30 years and specifically using Windows since 1986, so everything seems like second nature to me. I therefore have a problem identifying what isn't second nature to the everyday user. And everyone is different, so what you are thinking about while you read this will be different from someone else. I need you to send me your questions about How Do I do Relating to Windows or your computer. And remember, the only dumb question is the one you don't ask – because it never gets answered.

What are user accounts for in Windows XP?

User accounts came into use with Windows 95, but until Windows XP never seemed to have the ability to work the way they were initially supposed to. The idea of a user account is that everyone using the system should be allowed to set their own desktop, have a reserved area for their files, be able to keep track of their own email, in short – run their own personal version of Windows.

So how do we set it up? When your system was originally built it came with an Administrator account even though you may not be able to see it. You also have a Guest account which has been turned off and should be left turned off. Then you have a user account which is your account and is identified by default if you have a mass produced system or has your name if it was custom built. To see the different user accounts currently on your system: click Start | Control Panel | User Accounts. (Note – even if there is more than one user identified on your system, if that account has never logged on, no additional files will have been created for it.)

Once you have the dialog open, click on the option “Create a new account” to create additional user accounts. You will then be prompted for the name of the account, and click Next.

User accounts come in two flavours in Windows XP: Computer Administrator and Limited. A Computer Administrator has access to the full system, has the ability to add and remove programs and settings, and make system wide changes. A Limited User can change or remove their own password, change pictures, themes and other desktop settings, view files they have created, and view files and folders in the Shared Documents folder. So when you create a new account you must decide how much control you want the new user to have. Some programs may be able to be installed by a limited account, but generally a Limited User will only be able to use what is already there. Once you have decided on the level of authority, click the button “Create Account” to create the new account. If you have multiple accounts I strongly recommend setting passwords on all accounts.

Why do I want a password? Passwords limit access to whatever they are protecting. You have a secret PIN number on your bank card because you want to keep your money safe. The same logic applies to an account password: it keeps your data safe. If your account has a password and someone turns on your computer while you are not available, they require that password to gain access to the system. If they don't know the password the only available open is to Shut Down the System.

When a computer system is in a family situation you would probably like to have Administrator accounts for the parents, and Limited User accounts for the children. That way, you can see what they are doing, but they can't peek at your personal stuff. Obviously, you would only peek to make sure they are not doing anything with the computer that is contrary to your household and family values. After that, it is all a matter of trust.

Once you have created different accounts for each user, make sure you know what everyone's password is, and keep them in a safe place. Forgotten passwords can only be changed by an Administrator, so never lose that password or your system will require reinstallation. As each user logs onto the system a unique folder will be created under Documents and Settings labeled with eh users name. Inside these folders will be additional folders to keep track of their email using Outlook Express, their Favourites, their cookies, their My Documents folder, etc.

If you want to make changes to an existing account, open the User Accounts option and select Change an Account. The next screen you see will ask which account to change: Select the account by clicking on it. Then you will be able to change the User Name, Password, Picture, Account Type (if you have Administer authority) and .NET passport.

I hope this helps clarify the use and need for each user to have his or her own account on a Windows XP system, and helps you setting them up and maintaining them. If you have any questions, please write me at tekjournal@mbts.mb.ca

SURF'S UP

Over Christmas I got hooked on Harry Potter and managed to read the entire collection, all five volumes, in about two weeks. Now I can't wait to get my hands on the sixth book but no one knows when it will be delivered because a publishing date hasn't been cast. However, the Internet loves Harry Potter and there are lots of sites to prove it. The [Official Web Site](#) is sponsored by Warner Bros. and has a lot of interesting things to keep young people happy for hours. [Scholastic](#) also offers an interesting site complete with Screen Saver and a Pronunciation Guide for words and terms found in the books. If you explore, you too will find that Harry Potter isn't just a good children's story.

Since books are becoming quite expensive many people are turning to the Library to read the latest releases by their favourite authors. The following links will take you to the [Winnipeg Public Library](#), [Toronto Public Library](#), or the [Calgary Public Library](#), where you can view selections, see what new books are coming, check events, and maybe even reserve a book.

Not everybody has time to read a book so some people turn to audio books. These are the full manuscript generally read by someone important with a great voice that lets you be entertained by the book while you are driving, relaxing by the pool, or anywhere else that books aren't usually taken. Another medium is the eBook, or electronic book. One site offering free ebooks for download is [Free eBooks](#) of course. They even have a newsletter that will keep you informed of new offerings. I just downloaded 365 Daily Success Quotes. In some cases the offered link will take you to another site where the actual download can be found, as in the case of 10 Tips for Online dating safety.

The [eBook Directory](#) claims to have 20,000 free ebooks available for download. Surf through and you may find something interesting.

TIPS AND TWEAKS

NOTE: Some of the tips featured here require editing the System Registry. Always make a backup of the Registry before performing any edit procedure. MicroByte TekSolutions does not warrant nor guarantee the worthiness of your system should you decide to edit your System's Registry.

Clearing out the Prefetch

Windows XP has a new feature called the Prefetch which keeps a shortcut to recently used programs.

However, it can fill up with old and obsolete programs and may slow down your system at times. To periodically clean out the prefetch:

1. start | Run | prefetch
2. Press Ctrl+A to select and highlight all the shortcuts
3. Press the Delete key to delete them

Change Default Cache file size

The default setting in Windows XP to cache files and folder is 400. Some people using their systems a lot think this value should be higher to provide a faster access to information they readily access. Here is how to change the folder cache from the default to a higher setting.

1. start | Run | Regedit
2. Go to *HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam*
3. Change the vaule of *BagMRU* to whatever size you want (hex)
 - 1000 in hex is 3e8
 - 2000 in hex is 7d0
 - 3000 in hex is bb8
 - 4000 in hex is fa0
 - 5000 in hex is 1388

Disable Thumbnail View

Windows XP Explorer has the ability to show the contents of a folder in many different ways including Thumbnail, Tile, Icon, List, and Details. I am not sure why anyone would want to but it is possible to disable the Thumbnail view in Explorer. Here's how:

1. start | Run | Regedit
2. Go to *HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Explorer \ Advanced *
3. Change *ClassicViewState* to 1

Disable Shared Documents

If you want to disable the Shared Documents folder on your Windows XP system, here are the steps required.

1. start | Run | Regedit
2. Go to *HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer *
3. Create a new DWORD Value
4. Give it the name *NoSharedDocuments*
5. Give it a value of 1
6. Log off or reboot your system.

Removing Thumbs.db Files

Whenever you view a folder with Thumbnail view in Windows XP, a small file called thumbs.db is created. This is a cache file of every picture currently stored in that directory. Since every file stored on the hard drive adds to the overhead of the system you may want to remove these file and stop them from being created in the first place. Here's how:

1. start | All Programs | Accessories | Windows Explorer
2. Select Tools | Folder Options | View
3. In the section Files and Folders, check *Do not cache thumbnails*

4. Click Apply | OK
5. Perform a search of your system for the file thimbs.db and delete all instances

No XP Logo on Boot

If you have no need to see the Windows XP logo every time you boot your system, you can turn it off.

1. Run *MSCONFIG*
2. Click on the *BOOT.INI* tab
3. Check the box for */NOGUIBOOT*

Change the Registered Owner

Here is the vanity fix for the month. If you bought your system from a mass produced computer outlet, or by mail order, chances are really good that it was never personalized. Your user name is probably Default and it is registered to Default or some other nameless entity. To change the Registered Owner Key in the Registry:

1. start | regedit
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
3. Locate and edit the name in the Registered Owner key

VIRUS UPDATES

Aside from the obvious virus that is plaguing everyone today, the **W32.Novarg.A@mm** which is a mass-mailing worm that arrives as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr, or .zip. When a computer is infected, the worm will set up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources.

In addition, the backdoor can download and execute arbitrary files. The worm will perform a Denial of Service (DoS) starting on February 1, 2004. It also has a trigger date to stop spreading on February 12, 2004.

This threat is still rated at Symantec's level 4 which is the highest threat level available.

Also discovered on January 26th were the **W32.Mimail.Q@mm** and **W32.Dumaru.Z@mm** worms. The **W32.Dumaru.Z@mm** worm is a variation of [W32.Dumaru.Y@mm](#) which was discovered on January 23rd. All of these threats remain at Threat Level 2.

W32.Dumaru.Y@mm is a multi-threaded, mass-mailing worm that opens a backdoor, runs a keylogger, and attempts to steal personal information. It is similar to the [W32.Dumaru.M@mm](#) worm

This worm uses its own SMTP engine to spread to the email addresses it finds in the files on the infected system.

The email has the following characteristics:

From: "Elene" <F**KENSUICIDE@HOTMAIL.COM> (censored)
 Subject: Important information for you. Read it immediately !
 Message:
 Hi !

Here is my photo, that you asked for yesterday.
Attachment: Myphoto.zip

The attachment is a zip file that contains the worm executable as Myphoto.jpg <spaces> .exe. (There are 56 spaces between ".jpg" and ".exe".)

If your system has become infected with this worm, a quick service call will correct the problem.
W32.Dumaru.Z@mm, a variation of **W32.Dumaru.Y@mm**, is a multi-threaded, mass-mailing worm that downloads and runs a file, runs a keylogger, and attempts to steal personal information.

The email has the following characteristics:

From: "Elene" <F**KENSUICIDE@HOTMAIL.COM> (censored)
Subject: Important information for you. Read it immediately !
Attachment: Myphoto.zip

The attachment is a zip file that contains the worm executable as myphoto.jpg <spaces> .exe". (There are numerous spaces between ".jpg" and ".exe".)

If your system has become infected with this worm, a quick service call will correct the problem.

W32.Mimail.Q@mm is polymorphic in nature and is similar to W32.Mimail.A@mm. The worm creates a polymorphically modified version of itself as Sys32.exe and a static version of itself as Outlook.exe, which Symantec previously detected as W32.Mimail.Gen. The worm attempts to send itself by email to the email addresses found on the system. The message body and subject lines can vary.

The worm may also display a dialog box prompting you for your personal information to steal e-gold account information, and attempt to steal other system information.

W32.Novarg.A@mm is a mass-mailing worm that arrives as an attachment with the file extension .bat, .cmd, .exe, .pif, .scr, or .zip. When a computer is infected, the worm will set up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources.

In addition, the backdoor can download and execute arbitrary files.

The worm will perform a Denial of Service (DoS) starting on February 1, 2004. It also has a trigger date to stop spreading on February 12, 2004.

Norton Anti Virus is a must have for all systems today. We currently have copies in stock if you need one.

TEKSPECIALS

Microsoft Office 2003 Basic Edition, containing Word, Excel, and Outlook. \$ 300.00 plus applicable taxes.

Microsoft Windows XP Professional, \$ 350.00 plus applicable taxes. Includes backup and restore of the My Documents folder, Favourites, Outlook and/or Outlook Express, Windows Address Book.

Norton Anti Virus 2004, \$ 50.00 plus applicable taxes

LG GMA 4081B 8x DVR CD-R, CDRW, DVD-RAM, DVD-R, DVD +R, DVD-RW, DVD +RW
Optical drive, \$ 249.00 plus applicable taxes Installed.



19 inch Colour Monitor – 1600 x 1200 maximum resolution, 18 inc screen controls for H-Center, V-Center, Pincushion, Trapezoid, Pin Top Pin-Corner, Bottom Pin-Corner, Rotation, H-Linearity, V-Line Focus, Color Temperature, Color Gain/Bias, Degauss, Power Save Information, Test

Pattern Recall, 5 Multi OSD Language (Eng/Deu/Esp/Fra/Ita)

1 Only @ \$ 225.00 plus PST & GST

This concludes another issue of the MBTS TekJournal.

Ric Jackson
Owner
MicroByte TekSolutions

You are receiving this publication because you are either a client of MicroByte TekSolutions or requested addition to the mailing list. To be removed from the mailing list for this publication, please follow this link: [Remove Me](#)