

## THE LONG HOT SUMMER

Whew! We have finally had a summer to remember. It was a scorcher and we loved every minute of it, even when we were complaining it was too hot! But can you believe it, summer is almost over and the kid's will be back in school almost immediately. Unbelievable.

Winnipeg was not the only hot place this summer. The Internet was a scorcher too. We had several different viruses pop up but the end of August has probably been the worst. As of Friday there were four serious threats against our systems.

**W32.Sobig.F@mm** is a mass-mailing, network-aware worm that sends itself to all the email addresses it finds in the files that have the following extensions: .dbx, .eml, .hlp, .htm, .html, .mht, .wab, and .tx. The worm uses its own SMTP engine to propagate and attempts to create a copy of itself on accessible network shares, but fails due to bugs in the code. This worm will deactivate on September 10th, 2003 so the latest it can spread is September 9th.

**W32.Dumaru@mm** is a mass-mailing worm that drops an IRC Trojan onto the infected machine. The worm gathers email addresses from certain file types and uses its own SMTP engine to email itself. This email claims to be from Microsoft and announces a "patch" you should download. DON'T! This virus affects all file formats including NTFS.

**W32.Welchia.Worm** is a worm that exploits multiple vulnerabilities, including: The DCOM RPC vulnerability using TCP port 135. The worm specifically targets Windows XP machines using this exploit. (and) The WebDav vulnerability using TCP port 80. The worm specifically targets machines running Microsoft IIS 5.0 using this exploit.

And of course the big security problem that started most of the latest threats, the

**W32.Blaster.Worm** which is a worm that exploits the DCOM RPC vulnerability using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not have a mass-mailing functionality. Even though this particular virus only affects systems using the Windows Operating systems from NT through XP and the new Server 2003, Microsoft has issued a statement about other operating systems:

**"Note Windows 98, Windows 98 Second Edition (SE), and Windows 95** are not affected by this issue. However, these products are no longer supported. Users of these products are strongly encouraged to upgrade to later versions."

The first line of defense in securing your system is to use a quality Anti Virus product. My personal preference is Norton Anti Virus, but there are other good products as well. The second line of defense, and equally important to your system is a hardware firewall generally found in the form of a router. The router acts as a security guard on a bridge between your system and the Internet. The third line of defense is regularly accessing the Windows update site (assuming you have a supported product) for the latest security upgrades. And finally, you should also implement software to not only remove Spyware from your system, but intelligent software to Block Spyware before it gets to your system.

## SURF'S UP

Another first, (or since it only happens every many thousands of years apart so it seems like a first), was Mars getting close to the Earth. Unfortunately in Winnipeg Mother Nature picked August 27th (the day it was closest) to end the drought and provide us with a deluge. Too many clouds and

lightning made it very difficult (if not impossible) to get the full effect. We always want to think that we are not alone in the universe, and scientists say that Mars is probably the best place to start looking for other forms of life. If you are interested, there are a ton of sites with information of Mars.

Interesting page provides details of NASA's [Mars](#) bound missions.

The Mars Global Surveyor (MGS) [Mars Orbiter Camera](#) (MOC) first acquired images of Mars during its approach to the red planet in mid-1997. Hundreds of MOC images with captions describing their contents have been compiled and released by the MOC team at Malin Space Science Systems since 1997.

For those of you who often dream of space travel, you can even get the [Daily Martian Weather Report](#).

## HOW DO I... AND WINDOWS 101

It is very difficult for me, without outside help, to come up with a new thought for each of these topics on a regular basis. Sometimes I have a service call where several ideas will pop up at once, but generally I wait until I am writing the newsletter to figure out what to put here. So, until such time as I am able to stockpile ideas, I am going to combine these two topics into one.

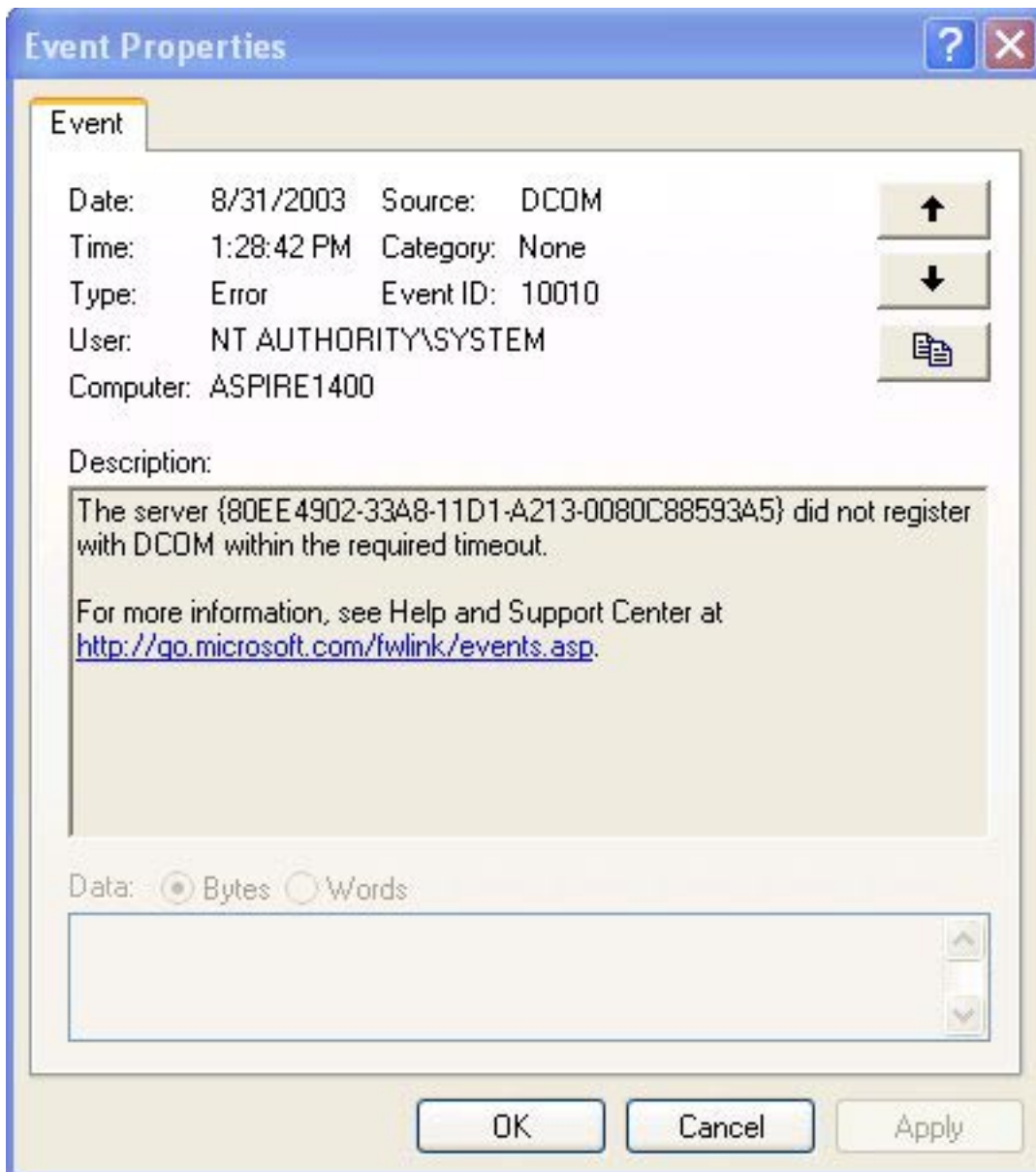
Many people are now using Windows XP and those that haven't switched should. Windows XP offers many tools for customizing the installation and fine tuning your own system. The typical place to start is in Services. To begin, click Start, then Control Panel, then Administrative Tools, and finally Services. Here you will see a list of all the services currently available in your system, and have the ability to turn off what you don't want.

It would actually take too long to identify what can be turned off, and what should be left on, and I would be reinventing the wheel that other people have already invented. The best page I have found so far for customizing Windows XP belongs to [Black Viper](#).

This page identifies all services, their links to other services, and whether they can be modified depending on the installation you are trying to achieve. Before changing anything in the services section, I highly recommend a visit to this page.

How many people running Windows XP (or any version of Windows for that matter) have come across some execution that didn't seem quite right. Was it easy to find out what happened or was happening? There is a service in XP that may just help identify what was going on, what failed, and how to fix it. Go to Administrative Tools and select Event Viewer.

The Event Viewer keeps a running log of everything that happens inside your system and separates it into Application, Security, and System processes. Opening any one of these folders and scrolling through, you will look for errors. When you double click on the error, a screen similar to the following will appear.



This screen identifies the date, time and type of error, and provide a link which may give more information about the cause, effect, and solution.

### VIRUS UPDATES

Since this summer has seen more than it's fair share of viruses and worms, refer to the opening remarks concerning viruses to be on the lookout for. Always make sure your anti virus software is current, and if you don't have anti virus software, or know of someone who needs it, refer them to us. We deliver and install to ensure your systems are protected.