

Here We Go Again

Once again I'm writing to warn you about a new virus that was released last weekend called the W32.Sasser.Worm. This worm attacks Windows 2000 and Windows XP machines that have not been patched for Microsoft Security Bulletin MS04-001. This update was recently added to Microsoft's list of critical updates on March 28, 2004. If you have not run the Microsoft update utility in the past two weeks you should do that right now before you finish this article.

Now that your back from updating your computer I will describe to you how this nasty little worm works. But first the good news, this particular worm doesn't seem to do any major irreversible damage to your computer. The bad news is you can't live with this particular virus. This virus has some poorly written code in it that allows your computer to shut itself off. Not all computers react the same way to this particular worm however. Some computers simply slow down to a crawl and don't actually shut down on their own.

I have already mentioned this point in a previous article, but I want to take this opportunity to reiterate it here. It is no longer safe to open e-mail from people you know without the fear of getting a virus. One such virus is called the Netsky virus which was released a month or two ago. Each infected e-mail will have a different return address originated from the address book of the infected computer. Many people will get returned e-mails stating that their system has a virus. When in reality the virus actually came from another computer system that just happened to have your e-mail address in their address book.

This newest virus however does NOT use e-mail as a distribution method. Another words you can contract this virus simply by connecting to the Internet. This worm scans the Internet looking for computers that have not been patched with the Microsoft update. Once it finds a vulnerable system it will connect to TCP port 445. Once a connection is made the virus sets a series of tasks into play that ultimately ends in transferring a copy of the virus to that computer. The copy of the virus will randomly be named using a series of four or five digits followed by "up.exe." Once your computer is infected it begins scanning the Internet looking for other vulnerable computers. The author of the virus made a mistake when writing the code. The code is designed to not allow you to be able to shut down your computer, however instead the infected computer will typically shut down uncontrollably.

If you think you have the virus you should try to get access to another computer and download the appropriate Microsoft Security Patch and the Sasser removal tool from Symantec's web site. If you are using Windows XP be sure to turn off the system restore feature. Then run the Microsoft Security Patch first and restart the computer. Once the computer restarts you should then run the Symantec removal tool. If all goes well your computer should be virus free within an hour.

If however the system continually shuts down during the repair you will probably have to take your computer to a repair shop. If you need a good computer technician to help you with your computer virus problems give Thomas or Roger a call at the Computer Depot or e-mail me at computerdepotonline@att.net.