



IT Counts

Conquest Wildman 

Table of Contents

Do you defrag	1
Bugbear and SoBig are the top viruses so far in 2003	2
Bugbear is back!	2
“Best Practice” for keeping your system secure	2

If you have any ideas as to what you would like to see in these newsletters, please do not hesitate to contact **Maria Alvarez**, Business Dev. Manager

Now you can afford to buy new IT equipment or upgrade your system. Our sister company, **Gregory Wildman** offer advice on various leasing options. Please contact us for further details.

When did you last check your backup properly? It may say that it is working, but is it really? The only way to be sure is to have one of your backup media externally verified. This way you can ensure that you have a tape that could be restored easily onto a replacement machine. Doing this can ensure that your business is quickly back up and running in the event of failure. We now offer a full range of backup verification services to give you and your business peace of mind. Your data can be recovered and your customers and your business will have as minimal disruption as possible.

Contact us for information on how your backup media can be verified. **01234 30 11 33.**

Do you do defrags?

Do you remember back to the good old days of DOS and check disk?

There were even some that thought Christmas had come early when the new graphical version, scandisk was released, how things have changed. At the time disk utilities seemed to be an essential part of the operating system, especially hard disk defragmenters (or DEFRAG), but now, with the user friendly graphical interfaces, and the ever increasing performance of modern computers, what once were simple essentials now seem to have taken a back seat, although still, even on modern computers, with much bigger disks, some of the potential problems these quirky little utilities addressed are even more relevant.

Disk fragmentation, for example, is a condition where pieces of an individual file on your computers hard disk are not contiguous, but instead are broken up in amongst other files and are scattered around the disk. This slows down system performance significantly, as your computer has to search around the hard disk retrieving file fragments from hundreds and possibly thousands of different places every time it accesses a file.

On a network server, where the machine is probably not only processing your request, but the requests of other users simultaneously, this can lead to severe performance degradation, and in the most serious cases, can affect the overall stability of the system.

Both on your own workstation computer and across your network, disk fragmentation can be the underlying cause of many system reliability and performance problems. Crashes, delays, even long back-

ups times can all be caused by as little as one severely fragmented file on your drive.

In Windows 2000 and XP the included Disk Defragmenter consolidates fragmented files and folders on your computer's hard disk, so that each occupies a single, contiguous space on the drive. As a result, your system can gain access to your files and folders and save new ones more efficiently. By consolidating your files and folders, Disk Defragmenter also consolidates the disks free space, making it less likely that new files will be fragmented.

This process does not run automatically though, it is an administrative task that you need to perform manually, and as

such often gets forgotten about for very long periods of time.

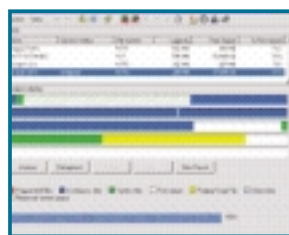
On Servers however, the machines that all of your network depend on, disk defragmentation utilities are often not included as part of the operating system as they once were. This means that the process has to be carried out using special third party software.

As this software is now widely available, and has dropped in price quite

significantly in recent years, it is now worth seriously considering having your server defragmented, especially if the server has been installed and running for some time.

For more heavily used systems, we can now even add software that will perform defragmentation automatically on a regular basis, while the system is not being used – an install and forget solution for continuous, optimal server performance.

If you think your server deserves a defrag, give us a call and we'll be pleased to help!
01234 30 11 33.



Bugbear and SoBig are the top viruses so far in 2003

A total of 3,855 new viruses were introduced in the first half of this year, this is an increase of 17.5% over the same time last year.

The growth of the internet, coupled with the wider availability of virus-writing tools, is driving the increase. Many of the virus authors appear to be operating in countries that do not have antivirus laws and more than half of the viruses tracked in 2003 appear to have emerged from Eastern Europe or the Pacific Rim.

2003 has seen its fair share of new exploits, including Bugbear and SoBig, which respectively accounted for more than 14% and 18% of the enquiries at one of the top anti-virus providers through June of this year.

Bugbear will change its appearance, which makes it hard for the antivirus software suppliers to identify it, and it also appears to target specific companies.

SoBig is a virus used primarily by the spam community. It installs a Trojan-type virus on any infected machine that could, eventually, be used as a spam relay point. The infected machine waits for the spammer to come along and connect to it and use the machine for whatever they want.

Some of the top viruses to watch out for at the moment include:

Bugbear-B, SoBig-C, Klez-H, SoBig-B, SoBig-A, Avril-B, Bugbear-A, Avril-A, Fizzer-A and Yaha-E.

"Best Practice" for keeping your system secure

Recent months have seen a sharp rise in the number of infections of Trojan viruses such as the Backdoor. Prorat, which allows the creators full unrestricted access to infected computers.

With such threats always on the increase, the chances of becoming infected with these viruses before your antivirus definitions will protect you against it seems to be increasing, so here are a few pointers from computer security experts, Norton Symantec, that help in keeping your computer as secure as possible.

Turn off and remove unneeded services. By default, many operating systems install auxiliary services that are not critical, such as an FTP server, telnet, and a Web server. These services are avenues of attack. If they are removed, blended threats have less avenues of attack and you have fewer services to maintain through patch updates.

If a blended threat exploits one or more network services, disable, or block access to, those services until a patch is applied.

Always keep your patch levels up-to-date, especially on computers that host public services and are

accessible through the firewall, such as HTTP, FTP, mail, and DNS services.

Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.

Configure your email server to block or remove email that contains file attachments that are commonly used to spread viruses, such as .vbs, .bat, .exe, .pif and .scr files.

Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media.

Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.

If you would like any further advice about computer security then please contact us. **01234 30 11 33.**

Bugbear is back!

Due to the number of submissions received from customers, Symantec Security Response has upgraded this threat to a Category 4 from a Category 3 threat.

W32.Bugbear.B@mm is a Category 4 mass-mailing, polymorphic worm that also spreads through network shares. This worm infects a select list of executable files, has keystroke-logging and backdoor capabilities and will attempt to terminate the processes of various antivirus and firewall programs.