

BYTES & PIECES

ELECTRONIC NEWSLETTER OF THE HOBART COMPUTER USERS GROUP INC.

IN THIS ISSUE

\$25 worth of software	
Equip your computer for under \$25 (Windows not included)	1
Keyboard & Mouse	
What's in the next issue and when will it be?	2
Committee Nominations	
Nominations close in a few days and we've still positions to fill	3
Rules of the Association	
Last chance to suggest changes	3
World's most affordable computer?	
Lindows.com adds another computer to its range	3
How to recognise a hoax	
Recognise hoax emails in 20 seconds flat	3
Symantec spams?	
Spams offering cheap Symantec software could be credit card frauds	4
Blasting XP	
Blasted worm is sweeping the world and making life difficult for XP users	5
Penguins at Disney	
Walt Disney's animation unit standardises on Linux	7
Buy buy	
A couple of members have items for sale	7

\$25 WORTH OF SOFTWARE

You could spend hundreds of dollars equipping your computer with an office suite, system tools, backup software, imaging software, photo editor, video editor and so on. Or you could spend less than \$25 and get dozens of quality programs.

What do you get for your money? Here's a small selection:

- Office suite- OpenOffice 1.0
- Photo editor- The Gimp
- Antivirus- AVG from Grisoft
- Video editor- VirtualDub
- System tools- MPower, PCMark, CleanDisk 2002, 4DiskCleanLite 3.0, EnZip 3.00, ZoneAlarm
- Backup and Imaging- My Own Backup, Recover My Files Drive Image 5.0
- DVD Player- Fusionsoft DVD Player
- Photocopier- Photocopier from www.niccuppen.com
- Drawing- Draw3D, ZonerDraw 3
- Internet- Mozilla, Internet Explorer 6.0 SP1, FMReader
- Email- IncrediMail, PureVoice, UltraFunk Popcom
- Downloads- FlashGet, FreshDownload, DownloadExpress
- Tweaking- FreshUI
- Chat- Trillian
- Spyware removal- AdAware
- WebCam - EasyFreeWebCam

Let's look at a few of them in more detail.

OpenOffice

This Open Source office suite is comparable to Microsoft Office Standard and includes Writer (equivalent to Word), Calc (Excel) and Presentation (Powerpoint). Shortly the developers will release version 1.1, which will include an improved installation program, improved interface, improved Microsoft filters, PDF export, Macromedia Flash (SWF) export and other improvements.

The Gimp

This photo editor has been ported from Linux and is comparable to Photoshop and similar applications.

AVG

We've been advocating this excellent antivirus software for some time now. Easy to use and with regular updates, this utility will keep your computer free of nasties and not cost you a cent.

Photocopier

As its name implies, this utility will turn your computer, scanner and printer, into a useful photocopier. If your scanner didn't come with similar software, this is what you need.

MPower

This utility will defragment and clean up memory, something which Windows 9x doesn't do very well.

DriveImage 5.0

As sold for \$150, PowerQuest's DriveImage 5.0 will clone drives and partitions. If trouble strikes, boot your computer from a floppy and roll back to the most recent image to get up and running again easily and a lot more quickly than reinstalling everything.

Recover My Files

Ever deleted files that you meant to keep? I have and I'm sure many of you have. If you act quickly, they can be retrieved. All you need is a utility like this one.

Mozilla

Developed as an Open Source browser and forming the basis of Netscape 7, Mozilla is now developing into an excellent browser in its own right. It includes pop-up killing, download manager, a webpage composer, news and email readers - in fact, all you need for your Internet activities.

FMReader

This will read web pages out loud!

IncrediMail

If you're one of those people who like to include graphics and fancy backgrounds in your email, this is the email client you need. Actually, it's an alternative interface for Outlook Express with several novel features.

Trillian

If you're into chatting on the Internet, give Trillian a try. It can connect to all the major chat services, using just the one interface.

How do you get this fabulous bargain? Nip along to one of the better newsagents and buy *Australian Personal Computer* August 2003 and *PC Utilities* Issue 36.

KEYBOARD & MOUSE

The Committee has decided to produce an issue of *Keyboard & Mouse* containing the Annual Reports and distribute it at the Annual General Meeting on 26 August 2003. After that, *K & M* will only be produced every few months to contain costs and lighten the load on the Editor. While it is up to the incoming Committee to decide, the outgoing one has agreed on only five copies per year being produced.

Lightening the load on the Editor could, of course, be more readily achieved by more contributions. There

must be someone in the Group who uses *Word*, for example, and could explain its nuances to the rest of us. Be a change from being told about the wonders of OpenOffice and StarOffice, wouldn't it?

COMMITTEE NOMINATIONS

Just a reminder that nominations close on 16 August 2003. At the time of writing, I am aware of only five nominations being received, with no nominations yet for President, Vice-President or Secretary. So, if you want the Group to continue, it's time for you to act. Ring around your fellow members and former members and find someone who is willing to put a little time into running the Association. Nominate them, get their signature on the form, get someone to second the nomination and get the form into the Committee by the 16th. Do it now!

RULES OF THE ASSOCIATION

The final draft is now ready to go to the AGM for consideration. Hopefully, we've tidied up such matters as charging a pro-rata membership fee during the year and other obscure parts of the Rules. The motion put to the AGM will rescind all existing Rules and amendments and replace them with the draft. If you haven't read it, it is available on the website at <http://hobartpcgroup.org.au>

WORLD'S MOST AFFORDABLE COMPUTER?

Lindows.com claims that the KooBox is the world's most affordable computer. The folks at Lindows.com say it has everything you need to do all your computing for one super low price, including computer, LCD flat-panel monitor, speakers, keyboard, mouse, CD player, network card, modem, virus protection, web filtering, ISP, and applications. Selling at \$USD449 (about \$760 Australia after GST), it features a 20 GB hard disk drive, AMD 1.2GHz Duron CPU, 256MB of SDRAM and a 14.1 inch flat panel screen.

The operating system is the LindowsOS version of Linux and the software supplied includes OpenOffice, Lindows Internet Suite (Mozilla), personal accounting software, The Gimp photo editor, Acrobat Reader, RealOne, Flash etc. The "virus protection" is a three month trial of Lindows Virus Safe (the German AntiVir).

Not exactly state of the art but a nice little entry level computer nonetheless.

How did the makers, MicroTron 2000, achieve such a low price? Two ways. Firstly they used superseded components - Duron 1.2GHz CPU, motherboard to suit, SDRAM, 20 GB hard disk drive and 14 inch flat panel screen. Secondly, they didn't pay the "Microsoft tax". They used LindowsOS and free Open Source software.

HOW TO RECOGNISE A HOAX

Recently one of our members sent me an email purporting to warn about a new virus. Here's the relevant text:

```
>>>A virus has been passed to me. My address book was infected. Since you are in my address book,
>>>you will probably find it in your computer, too.
>>>
>>>The virus (called jdbg.exe) is not detected by Norton or McAfee Antivirus systems. The virus sits
>>>quietly for 14 days before damaging the system. It is sent automatically by "messenger" and by
>>>address book, whether or not you sent e-mail to your contacts.
>>>
>>>Here is how to check for the virus and how to get rid of it. Please do this!
>>>
>>>1. Go to Start, then click your find or search option.
```

>>>2. In the folder option, type the name *.jdbgmgr.exe*

>>>3. Be sure to search your C drive and all the sub folders and any other drive you may have.

>>>4. Click Find Now

>>>5. The virus has a teddy bear icon with the name *jdbgmgr.exe* Do not open it!

>>>6. Go to Edit (on the menu bar) and choose Select All to highlight the file without opening it.

>>>7. Now go to File (on the menu bar) and select delete. It will then go to the recycle bin. If you find >>>the virus you must contact all the people in your address book so that they may eradicate the virus >>>from their own address books.

>>>

>>>To do this:

>>>1. Open a new email message.

>>>2. Click the icon Address Book next to 'To'

>>>3. Highlight every name and add to "BCC"

>>>4. Copy this message and paste to e-mail

>>>5. Send e-mail

It took me all of 20 seconds to dismiss this as a hoax. Why?

1. The email was similar to the *sulfbk.exe* one that circulated a while back.
2. Address books don't get virus infections.
3. Norton, McAfee and other antivirus products examine the contents of **all** .exe files on your computer when you do a full check. If they do not report a file as infected (and you have kept your antivirus *up-to-date*), then it is because the file is not virus infected.
4. What is the probability that an anonymous email writer can detect something that hundreds of experts working around the clock cannot find?
5. The instructions attempt to get you to delete the **entire** contents of your Windows/System folder on the pretext of showing you how to delete *jdbgmgr.exe* (**Select all???**)
6. *jdbgmgr.exe* sounded suspiciously like a legitimate Java file.
7. If you could eliminate the virus by simply deleting a (named) file Norton et al could do likewise. They delete or quarantine worms and trojans all the time.
8. All hoaxes rely on you sending the email on to everyone you know, as many people as possible, everybody in your address book etc. As has been discussed at meetings and included in the newsletter from time to time, the best thing to do with email that request you send them on to all your friends is to send them to no-one.

I then took a couple of minutes to search for information on *jdbgmgr.exe* something which you should always do when warned about a new virus. After all, there may be an update or fix program that you should download to deal with it, if it really exists. The following URL gave me the complete story:

<http://securityresponse.symantec.com/avcenter/venc/data/jdbgmgr.exe.file.hoax.html>

One interesting fact I learned from this site is that the genuine Java file has a Teddy Bear icon, but the Bugbear worm, which sometimes takes advantage of this hoax does not. *jdbgmgr.exe* can be infected by other viruses, as can any .exe file, but rely on up-to-date antivirus software and/or a specific fix program from a reputable antivirus software producer to clean it up. Don't go deleting files at the behest of some unknown email writer and don't go forwarding warning emails to all and sundry.

SYMANTEC SPAMS?

Of late, I have been receiving innumerable spam messages offering me Symantec products, especially Norton Antivirus. So I went to Symantec's site with a view to complaining and asking them to do something about it. I found, to my great pleasure, that they already had set about dealing with third parties who send out spam offering Symantec products. They ask anyone who receives such mail to report them to spamwatch@symantec.com and promise to act on reports.

Thank you for taking the time to alert us about the SPAM (unsolicited e-mail) you received. Please be advised that the e-mail you forwarded to us is not affiliated with Symantec or any approved Symantec partner and has been sent without Symantec's knowledge or consent. This e-mail may vary

well be offering counterfeit and/or pirated software or may be a credit card scam. . . .

In response to these e-mails and the organizations/individuals behind them, Symantec has developed a task force to investigate the e-mails and put a stop to their proliferation, including initiating criminal and civil actions as appropriate. We ask you for your assistance in helping us put a stop to this practice by continuing to forward any similar e-mails to our task force at SpamWatch@symantec.com, so that we can investigate who is sending the e-mails and attempt to stop them. We rely on reports from individuals such as you, employees and contacts throughout the hi-tech industry about SPAMs such as this.

In short, their advice is "Don't buy or respond to these spams, report them to us so we can act on them."

BLASTING XP

Lovsan, MBlast, or Blaster it's the same nasty and, if you use XP you need to get a patch from Microsoft as a matter of urgency. Users of NT4 and Windows 2000 should also patch their systems.

To check whether you are already infected, use Windows Search (on the Start menu) and look for `msblast.exe` in the Windows System32 folder. If you find it, you are infected and, if using XP, may not be able to stay on the Internet long enough to obtain the patch and the cleanup programs that are available from major antivirus vendors. If using NT4 or 2000, then you are spreading the infection if you have `msblast.exe` on your system. Users of 95, 98, 98SE, ME, or Linux are not affected by this worm which exploits a vulnerability in the Windows NT series.

Here's Microsoft's Security Response Team has to say:

PSS Security Response Team Alert-New Worm: W32.Blaster.worm

SEVERITY: CRITICAL

DATE: August 11, 2003

PRODUCTS AFFECTED:

Windows XP, Windows 2000, Windows Server 2003, Windows NT 4.0, NT 4.0 Terminal Services Edition

WHAT IS IT?

The Microsoft Product Support Services Security Team is issuing this alert to inform customers about a new worm named W32.Blaster.Worm which is spreading in the wild. This virus is also known as: W32/Lovsan.worm (McAfee), WORM_MSBLAST.A (Trendmicro), Win32.Posa.Worm (Computer Associates). Best practices, such as applying security patch MS03-026 should prevent infection from this worm.

Customers that have previously applied the security patch MS03-026 before today are protected and no further action is required.

IMPACT OF ATTACK:

Spread through open RPC ports. Customer's machine gets rebooted or the file "`msblast.exe`" [or "`msblast.exe`"] exists on customer's system.

TECHNICAL DETAILS:

This worm scans a random IP range to look for vulnerable systems on TCP port 135. The worm attempts to exploit the DCOM RPC vulnerability patched by [MS03-026](#).

Once the Exploit code is sent to a system, it downloads and executes the file MSBLAST.EXE from a remote system via TFTP. Once run, the worm creates the registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "windows auto update" = msblast.exe just want to say LOVE YOU SAN!! bill [A second message taunting Microsoft Chairman Bill Gates states "billy gates why do you make this possible? Stop making money and fix your software!"]

Symptoms of the virus: Some customers may not notice any symptoms at all. A typical symptom is the system is rebooting every few minutes without user input. Customers may also see:

Presence of unusual TFTP* files

Presence of the file msblast.exe in the WINDOWS SYSTEM32 directory

To detect this virus, search for msblast.exe in the WINDOWS SYSTEM32 directory or download the latest antivirus software signature from your antivirus vendor and scan your machine.

For additional detail on this worm from antivirus software vendors participating in the Microsoft Virus Information Alliance (VIA) please visit the following links:

Network Associates:

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547

Trend Micro:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html>

Computer Associates:

<http://www3.ca.com/virusinfo/virus.aspx?ID=36265>

For more information on Microsoft's Virus Information Alliance please visit this link:

<http://www.microsoft.com/technet/security/virus/via.asp>

Please contact your Antivirus Vendor for additional detail on this virus.

PREVENTION:

Turn on Internet Connection Firewall (Windows XP or Windows Server 2003) or use a third party firewall to block TCP ports 135, 139, 445 and 593; also UDP 69 (TFTP) and TCP 4444 for remote command shell. To enable the Internet Connection Firewall in Windows: <http://support.microsoft.com/?id=283673>

In Control Panel, double click Networking and Internet Connections, and then click Network Connections.

Right click the connection on which you would like to enable ICF, and then click Properties.

On the Advanced tab, click the box to select the option to Protect my computer or network.

This worm utilizes a previously announced vulnerability as part of its infection method. Because of this, customers must ensure that their computers are patched for the vulnerability that is identified in Microsoft Security Bulletin MS03-026. <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp> Install the patch MS03-026 from Windows Update <http://windowsupdate.microsoft.com>

As always, please make sure to use the latest Antivirus detection from your Antivirus vendor to detect new viruses and their variants.

RECOVERY:

Security best practices suggest that previously compromised machines be wiped and rebuilt to eliminate any undiscovered exploits that can lead to a future compromise. See Cert Advisory: [Steps for Recovering from a UNIX or NT System Compromise](http://www.cert.org/tech_tips/win/NIX-system_compromise.html) http://www.cert.org/tech_tips/win/NIX-system_compromise.html

For additional information on recovering from this attack please contact your preferred antivirus vendor.

RELATED MICROSOFT SECURITY BULLETINS:

<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>

Some antivirus vendors have cleanup programs available. Have a friend who is using Windows 9x or Linux download the patch and cleanup program and then follow Microsoft's (or your antivirus vendor's) instructions.

PENGUINS AT DISNEY

Last year when Disney's animation unit announced that it was doing its animation on a Linux-based system, there was speculation that Adobe's products would finally be ported to Linux. However, that is not what happened.

Instead Walt Disney Co. teamed with two unnamed animation companies to develop a version of CodeWeavers CrossOver that would run the Adobe products on Linux. Consideration was given to dual booting and VMWare, but performance and support issues and the need to buy Windows' licences led the team to go with the CodeWeavers Wine-based solution.

Development cost less than \$USD15,000, compared with \$USD50,000 for Windows licences and another estimated \$USD40,000 for support.

Disney's foray into Linux began in 2000 and, by 2002, digital animation had been standardised on Hewlett-Packard machines running Linux. However, there was no way to run Adobe Photoshop for the 200 animators that use it on a regular basis. Adobe declined to port it to Linux and so the idea of funding the development of CodeWeavers CrossOver for unit was conceived.

A Disney spokesman describes the successful development of CrossOver as a "win-win" situation, whereby the Open Source community got the product and Disney got what they wanted cheaper than they could have done it themselves.

Experts say the use of Wine by a corporation such as Disney to solve a technology problem gives legitimacy to the idea of running Linux on the desktop.

BUY BUY

External Zip 100 parallel port drive with three 100 MB Zip disks. Ideal for moving data from one computer to another. Simply attach to the printer port and run the software to install. Price asked: \$100.

Contact: Neil Hutton

Phone: 6248 6695 or 0400 001 701

36x and 40x CD-ROM drives (one of each). These are reasonably new and would make a good substitute for an older slower drive if you're renovating an old computer. Price asked: \$20 each on o

Contact: Charles Hunt

Phone: 6244 6943