

# BYTES & PIECES.

ELECTRONIC NEWSLETTER OF THE HOBART COMPUTER USERS GROUP INC.

Volume 2 - Number 35

29 June 2004

## IN THIS ISSUE

<a href="#">Worms aplenty</a>	And not from email .....	1.
<a href="#">Playing God</a>	A young virus writer's view .....	1.
<a href="#">Linux at Wimbledon</a>	Intranet now on Linux .....	2.
<a href="#">Credit card fraud</a>	A Canadian goes to gaol .....	2.
<a href="#">John James on computer security</a>	Notes from his talk at the June meeting .....	3.
<a href="#">That batch file</a>	John James' backup batch file .....	5.
<a href="#">Reference tools</a>	Start at these websites to find that information quickly .....	6.

## WORMS APLENTY

I decided to do a complete reinstallation of my operating system and software, cleaning out all the accumulated rubbish and the programs that I didn't need. I took a new hard drive, put it into my computer and began installing everything from scratch. All went well, except I made the mistake of connecting to the Internet before I had operating system patches, antivirus software and a firewall in place. Result worms invaded my computer, even though I had not set up an email account, let alone downloaded any email!

A year or two ago I would have considered a computer that was only online for a short time to not be at great risk. That is unfortunately no longer true.

With the aid of AVG, Ad-aware, Zone Alarm and Microsoft Windows patches, my system is now clean and appears to be secure, but until I reached that Nirvana-like state, I noticed that there was considerable traffic being sent from my computer. My ADSL provider, Internode, also noted the activity and emailed me a warning that I could be infected with Sasser worm and instructions what I should do to clear it up. How's that for service?

Here's a test for you: Connect to your Internet Service Provider with your browser, email client and instant message software shut down. Does your status indicator show any traffic? Open your browser. After the initial flurry caused by the page being loaded, is there any activity, especially traffic being sent? If there is you should investigate further – you may be infected with spy- or mal- ware.

<http://www.grisoft.com>  
<http://www.lavasoftusa.com>  
<http://www.zonelabs.com>  
<http://v4.windowsupdate.microsoft.com/en/default.asp>

[top](#)

## PLAYING GOD

*PC Magazine reported recently: "The future of viruses might lie in the hands of someone like BlueOwl, a 16-year-old in the Netherlands who started writing viruses when he was 14. BlueOwl isn't interested in destroying your hard drive; he just likes to experiment. A member of the Ready Rangers Liberation Front, he has written a Web site infector, a couple of genetic mass mailers, some polymorphic viruses, and a genetic polymorphic virus – some of which he posted, none of which he spread."*

What is his motivation? Here's what he said in an instant message to the magazine: *"I do it for the pleasure of creating something, seeing that it works, and making something that could really survive, spread, and hold its own in the wild. A virus is something that lives. In real life you can't make a kind of animal. You can in the computer. It's like playing God."*

According to the magazine, BlueOwl classifies virus writers into four groups: creators, who write for the thrill; students, who write for research purposes; script kiddies, writing to impress, "who think they are cool [but] their viruses suck"; and cyberterrorists, who spread viruses for the joy of not creation but destruction.

The creators, BlueOwl says, are a dying breed, quitting the virus scene out of boredom and not bringing new creators in. The students are also fading as schools get stricter about virus handling. By contrast, the number of script kiddies is growing, because "a lot of programming languages have become incredibly easy—with just a few lines these kids can make viruses that spread incredibly well, for example ILOVEYOU [the e-mail worm]. There is no real need to spend hours and hours learning how to write viruses anymore." Cyberterrorists, BlueOwl says, are steadily on the rise because of poorly protected networks and the low risk of getting caught.

Given the differing motivations of malware writers, don't expect the malware problem to go away any time soon.

[top](#)

---

## LINUX AT WIMBLEDON

The intranet for this year's Wimbledon Tennis Championships is based on a Linux-based IT infrastructure for the first time. IBM has also switched to running the Championships' internet web caching systems on Linux.

After a successful Linux pilot last year the All England Lawn Tennis Club converted its intranet from IBM's AIX Unix flavour. Linux is also used for the official website, which last year the website received 27 million hits, up 75 per cent on the year before. "We are not deploying Linux just for the sake of it," Mark McMurrugh, IBM's Wimbledon project director, told *vmunet.com*. "We considered the advantages and disadvantages of each system and decided it was appropriate to switch [the intranet]." The intranet, which now uses two IBM xSeries Intel servers, contains scores and statistics on matches and is owned by the All England Lawn Tennis Club.

Over 25 miles of cabling supporting a secure, campus-wide wireless Lan of 250 systems and 150 PDAs have been installed for the 2004 Championships. The WiFi technology will help record over 350,000 tennis strokes during the tournament, generating around 850 facts per match for pundits to ponder. More than 140 countries rely on statistical output from the Wimbledon information system, as well as around 1,000 journalists on-site at the Championships. They are deployed in the players' lounge, the press centre, and at access points around the ground.

<http://www.wimbledon.org>

[top](#)

---

## CREDIT CARD FRAUD

From the Canadian Broadcasting Corporation comes this report:

*"A 28-year-old Winnipeg man has been sentenced to more than six years in prison for a global credit card fraud.*

*Daniel Bedada-Letta was first arrested three years ago for making internet purchase orders with unauthorized credit card data.*

*The largest victim was the American Treasury Department, as Bedada-Letta filed more than 300 online orders for American savings bonds valued at more than \$250,000 US. An investigation led police to believe the credit-card data had come from victims in more than 12 countries, including Australia, Brazil, Germany, England, Switzerland, Taiwan, and the United States.*

*At first, Bedada-Letta was released on condition that he stay away from the internet. However, he was re-arrested last year after police found he had hacked into witnesses' email accounts to send emails to the RCMP providing misleading information in the case.*

*Bedada-Letta pleaded guilty earlier this week to a total of 12 charges, including unauthorized use of credit card data, obstructing justice, and fabricating evidence. He was sentenced to six years and four months in jail.”*

If using your credit card online, make sure that you only do so on secure sites. Where possible, use systems such as B-Pay and PayPal, so that you don't have to give your credit card particulars to all and sundry. And make sure your system has all necessary security measures in place.

[top](#)

---

## JOHN JAMES ON COMPUTER SECURITY

John has kindly provided the following notes from his talk at the June meeting:

### Computer Security

The following is an introduction to the type of security you should have on your computer. These programs will help keep you free of most of the nasties which invade your space and cause all sorts of problems.

### Spybot Search & Destroy - Removes Spyware. (Free). <http://www.spybot.info>

If you see new toolbars in your Internet Explorer that you didn't intentionally install, if your browser crashes, or if your browser start page has changed without your knowing, you most probably have spyware. But even if you don't see anything, you may be infected, because more and more spyware is emerging that is silently tracking your surfing behaviour to create a marketing profile of you that will be sold to advertisement companies.

Open Spybot, go to Help then to Tutorial. Briefly – Red items detected are spyware and green are “Usage Tracks” which keep a record of your activity which may be useful in that you can select from a list instead of typing in the whole filename or browsing the directory structure.

Using the Recovery icon you can undo any changes that have been made.

Immunize will set up standard immunization against bad products.

Update will search for updates for the program if you are on the net.

Now click on Search and Destroy –check for problems. Progress is noted at the bottom of the screen. If you click on the bar at the right it will provide any information that is available on what has been found. If you decide to “Fix the selected problems” the program will set up a recovery point (Windows XP) from which you can recover if something goes wrong.

One Club member on using Spybot for the first time found dozens of problems – after he fixed them his e-mail would not work but he used the recovery feature and returned to normal working. Warning - although you can recover, best to look at what you are deleting. Double click on the problem and check the information bar.

Version 1.3 is the current one, earlier versions have been abandoned – see recent e-mail from Peter Campbell.

### Ad-aware. (Free) <http://www.lavasoftsupport.com>

Ad-aware says it is the award winning, multi-trackware detection and removal utility (designed for Windows 98 / 98SE / ME / NT40 / 2000 / XP Home / XP Pro) that will comprehensively scan your memory, registry,

hard, removable and optical drives for known Datamining, aggressive advertising, Parasites, Scumware, Keyloggers, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components, providing you with the confidence to surf the Internet knowing that your privacy will remain intact. I'll bet you didn't know there was that much gunk around.

When you run it you can make an ignore list for any item you do not want detected. You can go and get updates on the net or just "Scan Now". Then you have the choice of a "Smart System Scan", a "Custom Scan" or selected areas to scan.

Before you scan click the settings icon a "Sprocket" on the top of the dialog box and you can spend the next twenty minutes tweaking the settings if you are so minded.

Because it has so many features it is best to go to the Help icon to look at the User Manual and browse the areas "Introduction", "Getting Started" and "Option Screens and Functions".

Spybot and Adaware perform somewhat similar functions but what one might miss the other will probably get.

### **Zone Alarm. (Free) <http://www.zonelabs.com>**

Firewall protection is your front line of defense against Internet threats. Zone Labs says security software's default Zones and security levels give you immediate protection against the vast majority of threats. If you're an advanced user, custom port permissions and expert rules give you detailed control of traffic based on source, destination, port, protocol, and other factors.

When you open up Zone Alarm click on Help. There is a wealth of detail on how it operates and like Adaware you can spend lots of time trying to come to grips with it. However I think you will find that the defaults are set to provide quality protection.

Zone Alarm will not allow contact with the Net unless you have given specific permission for that particular program to do so. After giving permission for say your e-mail program to contact the Net you can set it not to warn you again when you run that program. It also keeps a record of the number of intrusions it has blocked.

Zone Alarm also incorporates some virus protection.

*[The paid version of Zone Alarm comes with integrated, automatically updating, antivirus software and costs \$USD19.95 for the first year – Ed.]*

### **AVG Anti-Virus System (Free) [www.Grisoft.com](http://www.Grisoft.com)**

This is an excellent program which when installed will remain active and detect incoming viruses. Like the other programs its default settings works well but it is capable of being tweaked. On locating a virus it will quarantine it, out of harms way, or delete it.

The "Control Centre" icon locates itself on the tray (bottom right) and allows you to customise its settings. It has an update manager which you can run when you are on the net and it is advisable to do this as soon as you go on the net. If any update is necessary it will download it and install itself automatically on your computer.

The "AVG System Status" icon is located, either on your desktop or in the Start Programs section. This will allow you to run a complete test or a removable media test at any time and there is a good Help section.

### **Backup**

This is the thing many people only think about when it is too late. Don't be amongst that group. You have been WARNED.

Windows has its own form of backup and PC Magazine disks often contain various backup programs, however all of these seem to backup your files in some coded form. The result is that when you look at your backup you cannot readily identify the files that have been backed up.

Addressing this problem, Gordon Brown and I prepared a batch file for Windows 98 which now adapted for Win2K and WinXP works very well. With one click on an icon it will back up files which have been altered in any way since the last time you backed up. It does require setting up for each individual user but I would be happy to assist if required.

Whatever form of backup you use, whether it is simply manually copying the files you have created to another hard drive a floppy disk, zip disk, CD, DVD or via some program, do it regularly.

If you have an appropriate Burner format a CD RW or a DVD RWdisk using a "Packet writing program".such as InCD, a program which formats rewritable CDs (CD-RW, DVD+RW and DVD-RW) in such a way that they can be used like hard discs or diskettes. This means that you can save files from any application onto the media and use it as you would a floppy disk. INCD is software which is bundled with the "Nero" burning program. Other burning programs have their own version of INCD.

Good luck and happy computing,

John James  
[top](#)

---

## THAT BATCH FILE

Here's the batch file that John mentioned in the previous item. Cut and paste it into Notepad and save as MyBackup.bat. If you need help adapting it to your computer, or running it, contact John ([jamesj@southcom.com.au](mailto:jamesj@southcom.com.au)) or Gordon Brown for assistance.

```
Echo Off
Cls
echo NOTE: As MyBackup.Bat is DOS based it will only handle folder names with spaces
echo if they are subfolders and not the initial folder.
echo .
echo Backup Program Information - Backing up to E:\Backup\MyFiles .
echo This program copies any file within the C:\MyFiles folder and its sub-folders
echo which has its archive file attribute turned on. The subfolder of the copied
echo file is also copied. Having done so the program then turns the archive file
echo attributes off.
echo .
echo Files created or modified since the last backup have their
echo archive file attributes automatically turned on and therefore will
echo be the only files copied at subsequent backups.
echo .The /s switch copies directories and subdirectories unless empty
echo .The /h switch copies hidden & system files
echo .The /m switch copies files with their archives set then turns them off
echo .The /f switch displays the files being copied
echo .The /y switch suppresses prompting to overwrite an existing destination file.
Echo .
echo .           INITIAL BACKUP ONLY
echo Manually copy all the files and Folders included in the backup program below to E:\Backup\MyFiles.
echo After this the files and folders will be backed up to E:\Backup\MyFiles when you
echo run the program. Copy the files from E:\Backup\MyFiles to a formatted CD periodically for
echo additional security.
echo .
echo           RUN THE PROGRAM BY PRESSING ANY KEY.
echo If you want to stop during the backup process press 'Ctrl C'
pause
xcopy C:\Myfiles E:\Backup\MyFiles\ /s/h/m/f/y
if errorlevel 5 goto diskerr
if errorlevel 0 goto ok
: diskerr
echo A disk write error occurred.
goto exit
: ok
echo All modified files were copied.
: exit
echo The program has terminated. Close and re-run if necessary.
Pause
```

---

## REFERENCE TOOLS

We all need to look up information from time to time. Here's a short list of sites that have a multitude of links that should point you in the right direction.

### Refdesk.com

In a library, if you don't know where to look for a reference book, you go to the Librarian at the Reference Desk. This is the Internet equivalent. When you don't know where to look for answers, go to Refdesk.com. Don't be put off by the vast number of useful links on the Refdesk home page, they're really quite well organized and useful.

<http://www.refdesk.com>

### Libraryspot.com

Perhaps not as comprehensive as Refdesk, LibrarySpot is another source of convenient links to popular online almanacs, calculators, dictionaries, directories, encyclopedias, historic documents, news sources, quotations, statistics, thesauruses and more.

<http://www.libraryspot.com>

### World Factbook

Published by the United States Central Intelligence Agency, the World Factbook will give you current data on every country in the world, including maps, background, geography, people, government, economy, and military. The page on Australia was updated just last month and includes the July 2004 population estimate. Can't do much better than that!

<http://www.odci.gov/cia/publications/factbook>

### Information Please Almanac

From this website you can search dozens of almanacs all at once. Topics covered include: arts, biography, business and finance, consumer resources, entertainment, government, health, history, science, sports and weather. Accuracy of the information should be good, given the sources used to compile the information, but strangely Tasmanian (major) ports are listed as Hobart, Launceston and Devonport. The people of Burnie might disagree!

<http://infoplease.com/almanacs.html>

### State Library of Tasmania

Flip over to the State Library website and click on the Explore button and you're on your way to a wealth of information. Don't forget that you can use your membership of the Library to access several sources, such as Encyclopedia Britannica, that you would otherwise have to pay to use.

<http://www.statelibrary.tas.gov.au>

[top](#)

---

**Produced with:** OpenOffice.org 1.1. **Last changed:** 29 Jun 2004  
**Editor:** Peter Campbell, C/-Hobart Computer Users Group Inc., PO Box 563, Rosny Park Tas 7018, Australia.  
**Phone:** (03) 6234 4691 **Email:** [editor@hobartpcgroup.org.au](mailto:editor@hobartpcgroup.org.au)

*Disclaimer: Opinions expressed herein are those of the Editor or the author of the item concerned and are not necessarily endorsed by the Management Committee of the Hobart Computer Users Group Inc. While care is taken in compiling the information in this newsletter, the Hobart Computer Users Group Inc. and its officers and members cannot take responsibility for any problems arising from the use of the information.*

**Website:** This newsletter is also available from our website <http://hobartpcgroup.org.au>