

Bytes & Pieces

Electronic newsletter of the Hobart Computer Users Group Inc.

Volume 2 - Number 15

16 November 2003

IN THIS ISSUE

Worm targets PayPal users	
• Mimap variation targets PayPal users	1
Major AVG update	
• Download this update now	2
FreshDevices new application	
• FreshDevices have added FreshView to their free applications	2
Eudora users warned	
• Buffer overflow vulnerability in version 5.x	3
CNet acquires MP3.com	
• CNet plans own service	3
Turn off Windows Messenger warns FTC	
• Could let in a storm of pop-ups	3
Website still expanding	
• New hints added	4
ADSL getting cheaper	
• Netspace offer "unbeatable" flat monthly charges	4
Where was page 4?	
• No contributions so it was deleted	5
Buy, buy	
• Bargains we've noticed	5

WORM TARGETS PAYPAL USERS

If you were a PayPal user and you received an email with the headline 'YOUR PAYPAL.COM ACCOUNT EXPIRES' that claimed the company was implementing a new security policy, would you open the attachment?

Forgive me for repeating myself, but never open unexpected attachments. The attachment is called (www.paypal.com.scr) and we all know not to open attachments with double suffixes, don't we? We also know that .scr is the legitimate suffix of screen savers. Anything else is likely to be a worm. So I hope you answered "NO!" just as loudly and clearly as Marcel Marceau did in "The Silent Movie". (For those not familiar with the movie, Marcel's loud "NO!" is the only dialogue in it.)

The email is especially sneaky in that it correctly advises people not to send out credit card details by email. But when the attachment in the email is opened, the software displays a PayPal-branded window requesting all credit card information. And, of course, we know that you don't supply credit card information unless you are on a secure website (https:// or showing a padlock symbol), don't we? The worm then mails itself out to all email addresses on the infected hard drive.

Australia, New Zealand, UK and South Africa are all getting hits

Removal utilities and virus identity files are available from major antivirus companies, if you have opened the attachment. E.g. From http://www.sarc.com/avcenter/venv/data/w32_mimap.h@mm.html

MAJOR AVG UPDATE

At the same time that I received information about Mimail.H, I updated AVG and noticed that, instead of the small updates that I had been getting, it downloaded around 1800 Kb. Whether the two events are connected I don't know, but you should update your antivirus every time warnings about a new worm/virus/trojan circulate, if you haven't been doing it on a regular basis.

To force an update of AVG, right-click on the AVG icon near the time on your taskbar. Choose Run AVG Control Centre. When the Control Centre starts, click on the Update tab and then click on the Update Now! button. AVG will download the latest update or display a notice advising you that no update is needed, because you already have the latest update. Click OK when asked whether to install the update and reboot your computer after installation if AVG asks you to.

If you haven't updated to the most recent free version of AVG, you will have to download about 3 MB to install it, followed by a second download of the update.

<http://www.grisoft.com>

FRESHDEVICES NEW FREE APPLICATION

FreshDevices offer free applications to get you to go to their website, where you will see advertisements for a variety of paid applications. There is no obligation to buy, nor will you be bombarded with advertising. You will, however, receive regular email advices concerning updates to the free programs.

For some time they have offered FreshUI for tweaking Windows, FreshDownload for managing downloads and FreshDiagnose to examine your hardware. Now they have added FreshView.



FreshDevices says that *“FreshView is a multimedia browser that makes organizing your image, audio and video files much easier. It's optimized to be small and fast, with strong and rich functionality. Its intuitive user interface makes it very easy to navigate and operate.”*

FreshView offers a choice of six layouts. It displays thumbnails of your pictures and displays the original picture when the corresponding thumbnail is selected.. It can turn your pictures into slide shows. It can make

them into an HTML album for display on your website, or for burning on to a CD to send to friends and relatives. At present, only one HTML album template is included – this is, after all, only version 1.0 – but more are promised in future releases.

Thumbnail management is by database and the database can be optimised or emptied whenever you wish. FreshView not only handles pictures, but audio and video files as well. It recognises 86 file types, but currently can only save pictures as BMP or JPG.

Download it from <http://www.freshdevices.com> and have a look at it. I'd love to hear your views on this newcomer. Do you already use something that does a similar job? How does it compare?

EUDORA USERS WARNED

A buffer overflow vulnerability in Eudora 5.x, creates a mechanism for crackers to compromise targeted PCs. The problem stems from a failure to properly verify the "From:" and "Reply-To:" when users of vulnerable versions of Eudora select "Reply-To-All". This could allow hackers to spam users with a maliciously constructed email designed triggering this buffer overflow condition.

In practice it would be hard to trick users into selecting "Reply-To-All" in response to suspicious emails. But if they do then crackers would be able to run arbitrary code on vulnerable systems. The vulnerability was discovered in Eudora version 5.x by Japanese security researcher Hisayuki Shinmachi of Secure Net Services in January. Updating to Eudora 5.1-Jr3 (Japanese) or Eudora 6.0 (English) in order to shore up their security defences, as explained in an advisory by Secunia here.

Another hole in Eudora can allow hackers to execute code on a victim's machine through a malicious attachment, Peacefire.org Webmaster Bennett Haselton has discovered. It can be completely concealed and activated by clicking on a hyperlink. When a recipient clicks the link, the code is executed.

Eudora does not, by default, warn that such a link is about to be executed, though it does warn about links pointing to .exe, .com, and .bat files executing. Full details are available on the Peacefire Web site <http://www.peacefire.org/security/stealthattach/explanation.html>. The next version of Eudora will warn about .lnk files executing. Meantime Qualcomm recommends that users edit their Eudora.ini file and insert the following: WarnLaunchExtensions=exe|com|bat|cmd|pif|htm|do|x|reg|lnk|

Although Eudora security problems are not unprecedented, the package is far less afflicted with security issues than Microsoft's email client according to "The Register" ("Biting the hand that feeds IT").

<http://www.theregister.co.uk/content/archive/10587.html>

CNET ACQUIRES MP3.COM

CNET Networks, Inc announced on Friday that it has acquired certain assets of MP3.com, Inc.

From Tuesday, December 2, 2003 at 12:00 PM PST the MP3.com website will no longer be accessible in its current form. CNET Networks, Inc. plans to introduce a new MP3 music service in the near future. If you are an MP3.com member and want to keep up with developments, sign up at <http://mp3.cnet.com/index.html>.

TURN OFF MESSENGER WARNS FTC

People with Microsoft Windows on their PCs should turn off a little-used feature that could allow unscrupulous marketers to bombard them with unwanted "pop-up" ads, U.S. regulators said recently. Windows Messenger Service (WMS) is of no use to personal users and was designed to allow network administrators to communicate with others on their networks. If you do not shut it down, or install firewall

software, WMS can be used to send you pop-up ads that appear whenever you are online, even when you are not browsing the web. WMS is in no way related to popular Internet Messenger services.

The FTC said it had temporarily shut down one marketer, D Squared Solutions. The San Diego-based company had been selling pop-up blocking software through such pop-up ads. The FTC regarded this as extortion and is seeking to have D Squared return the money it had collected from consumers.

Microsoft advised consumers to disable Messenger last month because it could potentially serve as a conduit for Internet worms. Separately, consumer complaints prompted Time Warner's America Online to disable the feature on customer computers.

To turn WMS off:

- Click **Start**, and then click **Control Panel** (or point to **Settings**, and then click **Control Panel**).
- Double-click **Administrative Tools**.
- Double-click **Services**.
- Double-click **Messenger**.
- In the **Startup** type list, click **Disabled**.
- Click **Stop**, and then click **OK**.

If you are using Windows XP, make sure that the in-built firewall is turned on if you are not running other firewall software.

- Go to **Control Panel**, and then click **Network Connections**
- Right click on your **modem connection**
- Click on **Properties**
- Click on **Advanced**
- And make sure there is a tick in **Protect my computer...**

<http://www.ftc.gov/bcp/online/pubs/alerts/popalrt.htm>

WEBSITE STILL EXPANDING

Every week or so I add new hints to the website, as time permits. I am also looking for photos to add to the Hall of Infamy. Email them to me – they don't have to be high resolution.

Corrections have been made to the layout so that the meeting details are now readily accessed from the Home Page and, when this newsletter is uploaded, there will be a printable and a viewable (on screen) version of *Bytes & Pieces*.

Suggestions for further improvements are welcome.

ADSL GETS CHEAPER

Telstra's Bigpond ADSL for home users generously offers 500 MB usage (combined upload and download traffic) for \$59.95 per month, provided you preselect Telstra for your phone calls. If not, it is \$76.45. They slug you 15.9c a megabyte if you exceed the quota, the speed is 256/64 and people wonder why ADSL has not grown as quickly in Australia as it has in other countries.

Well, now it may be set to take off in metropolitan areas. Netspace have made an almost irresistible offer. For \$49.95 per month you get 2 GB of download, uploads for free, 256/64 speed, no preselection of phone company required, and no excess usage charge – instead your speed is “shaped” to 56k for the remainder of the month. If you absolutely must have the greater speed, you can purchase a 1GB data block for \$25 (about 158 MB of Telstra overusage) or a 5 GB data block for \$50. However, this must be used in the month of purchase. For \$59.95 a month, you can have 3 MB of download at peak periods plus a further 3 MB at defined off-peak periods on the terms listed already mentioned.

In addition to the above monthly charges, both Telstra and NetSpace require an upfront payment. This varies with the length of the contract and can, with NetSpace, be as little as \$0 if you already have an ADSL modem. Minimum upfront payment with Telstra is \$129.

There are many other ADSL deals on offer and it will pay you to shop around, compare what is offered and examine the fine print. However, NetSpace are confident that, when you have done that, you will find that the deals they are offering are the best available.

To sweeten the deal further, they are offering free rapid transfer from your existing ADSL provider. However, before you take up that offer, your contract with your present provider will need to have been fulfilled, or you may be up for a hefty early termination fee.

Broadband is only available in some areas. You generally need to be within 3.5 km of a suitable telephone exchange (as measured over the wires – not radially) and the service is incompatible with pair-gain and RIM technologies, as well as the Fax Duet service.

When assessing the monthly cost, remember that you don't pay for local calls to connect to the Internet or to get your email so add the amount you are presently paying for those calls to the monthly amount you pay for Internet access to get your present cost. If you use a separate line for your modem, add that cost in too. You will probably find that you can have a lot of extra speed for only a little extra cost, if you are currently on an unlimited hours/downloads contract.

<http://home.netSPACE.net.au/broadband>

WHERE WAS PAGE 4?

Last week, some people received or downloaded a PDF file that said it had four pages when it only had three. Where was the fourth page? Well, it was reserved for **your** contributions and when they weren't received, the extra page was deleted, because it was blank.

Actually, what happened was that the OpenOffice file contained a fourth blank page. Had I deleted it then, before turning the newsletter into a PDF file, the numbering would have been corrected automatically. Instead I deleted the excess page from the PDF file and the numbering didn't correct. Sorry about that. The PDF file was corrected later and the corrected version is the one currently on the website.

BUY BUY

If you need some paper for your inkjet, trot along to BigW at Eastlands – less than \$4.50 per ream for Alco brand from China. I also found AA Dorey Ashflash alkaline batteries at 12 for \$4.48. If you are into printing your own photos, you'll need a paper trimmer so that you can print two or three on the one page and then separate them neatly. Try the Alco guillotine-style one that BigW have for less than \$25. Note: These BigW prices are everyday prices, not specials.

Surely I'm not the only one that notices good buys around the town. If you notice something cheap, how about sharing the information with everybody. Email me so that I can include the details in the next issue, or, if it is urgent, send the details out directly to the HCUG-List by sending an email to hcug-list@lists.southcom.com.au.

Produced with OpenOffice.org 1.1. Last changed: 16 Nov 2003

Editor: Peter Campbell, C/-Hobart Computer Users Group Inc., PO Box 563, Rosny Park Tas 7018, Australia
Email: 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.