

BYTES & PIECES

ELECTRONIC NEWSLETTER OF THE HOBART COMPUTER USERS GROUP INC.

IN THIS ISSUE

Antivirus software is not enough

- Don't just rely on your antivirus software, be proactive 1

New website feature

- Now you can search our website for that elusive hint 2

An interesting AGM looms

- New rules, auditor's queries, key positions to fill – it's all happening on Tuesday 2

Sobig on the loose again!

- A new strain of the virulent Sobig worm is sweeping the world 3

Buy buy

- Bargains while stocks last 4

ANTIVIRUS IS NOT ENOUGH

Antivirus software, even if you are meticulous about updating, may not protect you from the latest crop of nasties. There is always a delay before antivirus companies can distribute an update, during which period you are vulnerable. However, there are steps you can take to ensure that your computer is as protected as possible and your data is safe.

Most people call every malicious program a virus, but technically they can be classified as viruses, worms and Trojan horses. The general name used for these programs these days is “malware” and what we are seeing a lot of are what are technically known as “worms”. We are also seeing malware that combines features from different categories.

Malware first appeared in the 1980s and the first malware programs were viruses, hence the tendency to call them all “viruses”. Computer viruses are designed to attach themselves to other programs. When an infected program is run, the virus is run as well spreading the infection to other programs or the hard disk's boot sector. Today, most programs are distributed on read-only CDs, and antivirus software can protect your PC's boot sector.

A Trojan horse is malware that disguises itself as something else. Unlike viruses and worms, Trojan horses don't replicate themselves. They lurk in you computer until run, often as the result of inbuilt scheduling. They then wreak whatever havoc they have been programmed to do. In the 1980s, they were often distributed as appealing-sounding games, but today a classic Trojan is rarely seen. More commonly, you'll see blended threats distributed as email attachments whose payloads are worms or viruses. You should never double-click on an unexpected executable email attachment, even when you recognise the sender. Executable attachments have the file extensions .com, .exe, bat, or .vbs.

A worm can copy itself to other machines without your help. It does this via network security holes. For example, a worm can be implemented as a script embedded in HTML email. You don't have to double-click an attachment to get infected; you just have to view the message in an HTML-enabled email client. This is why you will sometimes find your computer being reinfected immediately after you have cleaned up a worm. Until recently, you couldn't turn off HTML email in Outlook Express. But if you're running Version 6, Service Pack 1 or later, select Tools | Options, go to the Read tab, and check the box labelled “Read all messages in plain text.” Alternatively, if you are using anti-spam software such as Spamihilator, you can preview messages in plain text and delete those about which you have any doubt. Eudora, by default, does not allow executables in HTML messages to run, so doesn't provide a way of viewing messages in plain text. However, you can tell

it not to download graphics in HTML messages by changing the Viewing Mail options.

Even with heuristic scanning, a method for detecting viruses with unknown signatures, virus checkers are basically reactive. Of course, you should install a virus checker and update its engine and virus definitions regularly – but don't stop there. You should also follow the six suggestions listed here:

1. *Microsoft are working very hard to patch holes in Windows that could be exploited by worms. Installing the resultant patches is time-consuming but worthwhile. Select Windows Update in your Start menu, or go to <http://windowsupdate.microsoft.com> and click on the Scan for updates link. A script will figure out exactly what you need and present it in a list. Just select the items you want and click on Install Now.*
2. *Worms can propagate across networks if you write-enable shared directories that contain executables or crucial system documents. Unless you have very good reason to do otherwise, only write-enable directories that contain end user documents.*
3. *Binding file sharing to TCP/IP on your Internet-connected device gives anyone on the Internet access to your hard drive. To prevent this, open the Network settings dialog, right-click on your Internet device, and choose Properties. The TCP/IP protocol will be selected. Make sure that the service File and Printer Sharing for Microsoft Networks is not selected.*
4. *Most malware is spread via e-mail attachments. A personal firewall that quarantines potentially dangerous attachments can keep your system safe and prevent viruses from spreading.*
5. *HTML scripts can run when you preview emails in your email program. Go into the options and change the layout so that emails are not previewed. In Outlook Express, go to View | Layout and untick Show preview pane. In Eudora, go to Tools | Options | Viewing Mail and untick Show message preview pane. If you receive a lot of email you should find the resultant layout even better to use than the preview mode.*
6. *Lastly, you should back up regularly. There are more than 500 new viruses discovered each month, so be prepared.*

NEW WEBSITE FEATURE

While casually browsing through a website, something you (should) do regularly, you noticed a hint that might help solve the problem you currently face. But how do you find it again?

Don't despair, PicoSearch is here! Thanks to the free PicoSearch service, it is now possible to search our website. Try it. Go to the main page, type “Windows” into the search box at the bottom of the page, select whether to search for any word, all words, or the exact phrase, and click Search.

A new window opens and displays the results of your search. Now try the same thing with “Windows 98”, choosing exact phrase as the type of search.

Unfortunately, the PicoSearch engine doesn't search PDF files and I have yet to implement a way round that. However, I am working on it, so stay tuned.

AN “INTERESTING” AGM

“May you live in interesting times!” is an ancient Chinese curse. In the same sense this year's AGM on Tuesday could be an “interesting” one. We've revised Rules of the Association to approve; a President, Vice-President and Secretary to find; Auditor's queries to resolve; and even a proposal to increase the annual membership fee to consider.

There could be dummy spits, arguments and a move to wind up the Group, (or amalgamate it with another Group). Since I've been a member, there hasn't been an AGM like this one is shaping up to be. Don't miss it! Decisions will be taken and, if you are not there, you may find that you don't agree with them!

SOBIG IS BACK!

A while back, the malware that had many people worried was something called "Sobig". Here's what Symantec says about it:

The W32.Sobig.A@mm worm sends itself to all the addresses it finds in the .txt, .eml, .html, .htm, .dbx, and .wab files. The email message has the following characteristics:

From: big@boss.com

Subject: The subject will be one of these:

- Re: Movies
- Re: Sample
- Re: Document
- Re: Here is that sample

Attachment: The attachment will be one of these:

- Movie_0074.mpeg.pif
- Document003.pif
- Untitled1.pif
- Sample.pif

Before W32.Sobig.A@mm sends the messages, it sends a message to an address at pagers.icq.com.

The worm also attempts to copy itself to the following folders on all the open network shares:

- \Windows\All Users\Start Menu\Programs\StartUp
- Documents and Settings\All Users\Start Menu\Programs\Startup

Note: Symantec Security Response has received reports of W32.Sobig.A@mm downloading and installing the Backdoor Trojan, [Backdoor.Lala](#).

The new variant has been dubbed "Sobig.F" Here are the details:

W32.Sobig.F@mm is a mass-mailing, network-aware worm that sends itself to all the email addresses it finds in the files that have the following extensions:

- .dbx
- .eml
- .hlp
- .htm
- .html
- .mht
- .wab
- .txt

The worm uses its own SMTP engine to propagate and will attempt to create a copy of itself on accessible network shares, but fails due to bugs in the code.

Email Routine Details

The email message has the following characteristics:

From: Spoofed address (which means that the sender in the "From" field is most likely not

the real sender). The worm may also use the address admin@internet.com as the sender.

NOTES:

- The spoofed addresses and the Send To addresses are both taken from the files found on the computer. Also, the worm may use the settings of the infected computer's settings to check for an SMTP server to contact.
- The choice of the internet.com domain appears to be arbitrary and does not have any connection to the actual domain or its parent company.

Subject:

- Re: Details
- Re: Approved
- Re: Re: My details
- Re: Thank you!
- Re: That movie
- Re: Wicked screensaver
- Re: Your application
- Thank you!
- Your details

Body:

- See the attached file for details
- Please see the attached file for details.

Attachment:

- your_document.pif
- document_all.pif
- thank_you.pif
- your_details.pif
- details.pif
- document_9446.pif
- application.pif
- wicked_scr.scr
- movie0045.pif

NOTE: The worm de-activates on September 10, 2003. The last day on which the worm will spread is September 9, 2003.

BUY BUY

While stocks last, you can save big money. Contact Peter Campbell, 6234 4691, if you are interested. But be quick!

15" LG monitors

These monitors carry a 3-year warranty and are half the price of comparable ones. Just \$125 while stocks last.

17" Phillips monitors

If you would prefer a bigger monitor, try these at \$195.

HP 3500 printers

A major chain has these at \$99. For a limited period, Group members may buy them for just \$75.

Kodak 2.0 megapixel digital cameras

CX4200, 16 MB internal memory, 2X digital zoom. A good general purpose digital camera for \$225.