# Sophos Update

June 1998

## In this issue



## Bonjour, Patrice

**Swelling the ranks of Sophos employees in Europe is Paris-based Patrice LeMounier.**

His appointment is in line with Sophos' overall strategy for international business growth, and follows the setting up of Sophos GmbH in Germany last year. The French office will provide direct hands-on sales and support for local customers. Patrice is off to a flying start, manning stand C13 at Paris's Infosec 98 on June 3-5.

*Patrice LeMounier*

# Spearheading future research

**Sophos has appointed former Technical Manager Paul Ducklin as its new Head of Research. His appointment comes in response to the increasingly diverse virus threat and draws on his decade of international experience in the virus industry. His new role will see him spearheading the company's investigative research effort.**

*Matt, Cliff, Paul and John outside the Sophos HQ*

Ducklin's strategic consultancy will be supported by the newly promoted Software Development Manager, Cliff Penton, who assumes overall control of Sophos' flagship product, Sophos Anti-Virus. At the same time, John Phelps has been made leader of the Win32 team developing the Sophos Windows NT and Windows 95/98 products, while Matt Holdcroft is promoted to Software Production Manager to add a further level of control to the already stringent QA process.

'All four promotions are a measure of Sophos' commitment to constant development and steady growth,' says Ducklin. 'The fact that these new roles are being filled from within the company indicates the massive expertise which exists in-house and explains our continued place at the forefront of the anti-virus industry'.

## The ultimate defensive line-up

**Sophos, whose SAVI interface provides a fast means for third-party applications to use the SWEEP virus engine, has joined forces with another leading player in the information security arena, Content Technologies, developer of MIMEsweeper.**


The two companies will stage *Defence beyond the firewall* a half-day seminar presenting a game plan for effective network security. Key players from both companies will discuss Web, email and FT viruses, URLs, malicious ActiveX and Java code, and junk and spoof email.

Kick off is at 9.00 am on 11 June at London's Cavendish St James Hotel. To reserve a free place call Fiona Melville on 0118 930 1300 or email seminar@mimesweeper.com.

# VB'98 fest

**Sophos is again well-represented at the prestigious *Virus Bulletin* Conference. Head of Research, Paul Ducklin, who gave last year's keynote address, and Internet Systems Administrator, Ian Whalley join other international anti-virus experts from industry and research organisations to present papers at the conference which is being held at the Munich Park Hilton on 22-23 October.**

*Munich's Christkindlmarkt*

Now in its eighth year, the two-day conference follows its highly successful format of two parallel streams providing an in-depth analysis of key corporate and technical issues. It explores the latest virus threats, new detection technologies and successful virus prevention strategies.

Throughout the conference, the world's leading anti-virus software and hardware vendors will demonstrate the latest solutions for virus prevention at the accompanying VB'98 exhibition.

For more information on VB'98 telephone +44 1235 555139 or email vb98@virusbtn.com.

## Systems 98

Sophos will also be exhibiting at Munich's Systems 98 on 19-23 October, where 1700 companies will demonstrate their latest business-to-business technologies.

For details of Sophos at Systems 98 contact Pino von Kienlin at info@de.sophos.com.

# Unrivalled research integrity

**The Sophos Virus Laboratory currently receives from 300 to 400 new viruses every month. In addition, thousands of suspect files are received which on examination turn out not to be viruses. To disassemble and analyse these thousands of samples requires a rare combination of knowledge, precision and judgement, a blend found uniquely in the international team of Sophos virus experts.**

The viruses (and non-viruses) come from three main sources: the Internet; securely encrypted exchanges with other trusted researchers; customers and non-customers worldwide. All samples are analysed according to meticulous control procedures. It is not enough simply to be able to diagnose a virus. The environments in which each operates must be determined according to rigorous scientific methods and the results must be proven and repeatable.

The virus identities created by the virus researchers are incorporated in the following month's update of Sophos Anti-Virus which is beta-built and tested before being sent out to customers. In the meantime, new identities to detect and disinfect in-the-wild viruses are placed on the Sophos website from where they can be downloaded.

The quality and rigour of the control process raises Sophos far above most of its competitors. Research laboratory access control ensures that only authorised personnel are ever allowed in. All disks that have entered the laboratory are shredded, while dedicated 'dirty' machines are used to provide the multiple test replication environments.

This stringency of control is complemented by extensive research resource; a substantial proportion of the company's profit is re-invested in research. The new high-security, 20,000 sq ft R&D facility is being built specifically for the growing R&D teams who will move there in September.

# New look for Sophos on-access scanner

**Users logging into their Windows 95 workstations will soon notice that the console window has been replaced by a new splash screen. The new screen will be included as an option in August's version of SAV (v. 3.12).**

InterCheck's speed and power are unchanged and the on-access scanner remains active in the background checking every file, email attachment, document etc to make sure that it has been authorised. All this continues to be carried out behind the scenes so that it is completely user-transparent.


*The new InterCheck splash screen*

# Say goodbye to boot sector viruses

**PCs normally boot up from floppy if the floppy drive contains a diskette when the computer is switched on. They only boot from the hard drive if the floppy drive is empty. Since it is easy to leave a diskette in the drive by mistake, boot sector viruses can spread easily by this method.**

Although almost all computers are still set up to boot in this way when they are sold, the boot sequence is user-configurable. Altering the boot sequence means that the computer will always try to boot from hard disk first, even if a diskette is left in the floppy drive.

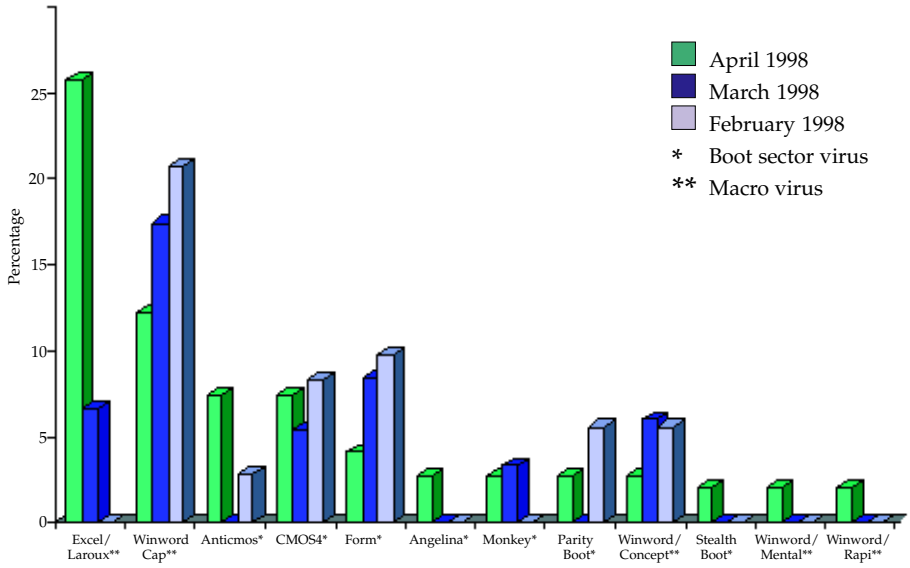
Boot sector viruses require you to boot from an infected diskette in order for your machine to catch the virus. This means it is possible to prevent them simply by changing the boot sequence of your computer. To do this usually involves pressing a particular key or group of keys shortly after switching on. The keys to use depend on the PC manufacturer, though Esc, Del, F1 and F10 are common choices. This brings up a configuration menu, in which the boot sequence can be selected.

One caveat: if you choose to disable floppy booting on your PC, you will need to readjust the boot sequence manually if in the future you decide that you really do wish to boot up from floppy, for example if you want to run SWEEP in a known, clean environment. This is done through the same configuration menu as is used to alter the original sequence. And remember, as soon as you no longer need to boot from floppy, you will need to reset the boot sequence once again.

# Top ten viruses

**The graph below shows the ten viruses reported most frequently to Sophos in April 1998. The ranking of the same viruses for March and February is also shown.**

Further details are at http://www.sophos.com/virusinfo/topten/.

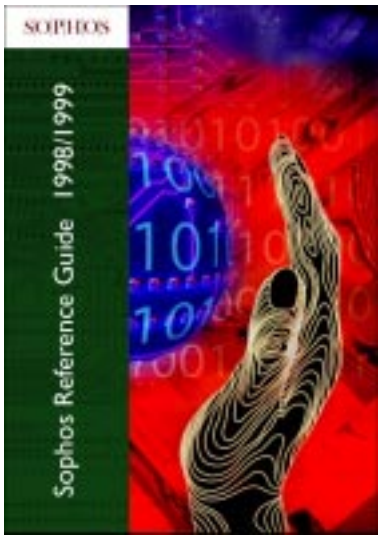



## Joke De_bug

Half the support calls received by Sophos in May relate to an email. The email contains a 'joke' Trojan attachment, JokeDe_bug, which asks a Yes/No question but will not accept 'No' as the answer. The attachment does not cause any damage. Sophos' advice: delete the attachment, delete the email, forget about it. More details can be found at www.sophos.com.

# New from Sophos

**The *Sophos Reference Guide* has been completely updated and restructured by the Sophos design and documentation department and can be found in PDF format on this month's Sophos CD.**




The Guide provides an extensive overview of major data security issues, describes different types of virus and explains effective anti-virus measures. It also investigates wider issues such as security on the Internet, legislation and the millennium bug, and gives comprehensive information about the Sophos product range.

## NetWare auto-update

Sophos Anti-Virus for NetWare now allows automatic updating of NetWare networks. UNLOAD/LOAD is no longer necessary and there is no need to visit each server, or to use RCONSOLE or SWCONSOL (although these mechanisms can still be used if you prefer). To configure the automatic update feature, select 'Administration' from the main menu, followed by 'Auto-updating'.

## W98 compliance

Sophos Anti-Virus is fully compatible with Windows 98. When the new operating system arrives, Sophos Anti-Virus can be installed in exactly the same way as before from the Sophos CD.

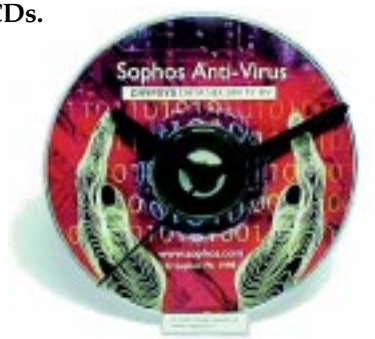
## AccessiV zeal

**A new virus, AccessiV, uses the macros and modules within the Microsoft Access 97 database and searches for other Access databases to infect.**

Of the four main components of Microsoft Office 97, only PowerPoint has not yet been a platform attackable by a virus. Identities for AccessiV and its variants are included in the Sophos Anti-Virus library on June's CD.

## Time on our hands?

**Certainly not Dutch distributor Crypsys who have found a novel use for expired Sophos Anti-Virus CDs.**




## ducks@sophos

*The only things allowed in the wild at Sophos – ducks on our wildlife pond*

## SAV for schools – £1 per PC per year

**Sophos has introduced a special Educational Site Licence offering Sophos Anti-Virus for just £1 per PC per year. The new licence is Sophos' response to the Government's plan to connect every school to the Internet by the year 2002, creating a National Grid for Learning, and will be available to all renewing and new customers in the education sector.**

*Children at home with the Internet, but their enthusiasm increases the need for robust anti-virus measures*

One of the first LEAs to take advantage of the cross-school, multi-platform protection offered by the new licence, is the country's largest, Birmingham City Council. The Council's Education IT department supports all 424 of Birmingham's state nursery, primary and secondary schools.

Andy Jackson, SIMS co-ordinator of the department explains, 'For several years now we have been using Sophos Anti-Virus in all our school sites on both stand-alone and NetWare networked systems. InterCheck has additionally provided real benefit in that it protects us against viruses interactively and thus saves us a huge amount of time. We used to have to check as a separate task each of the vast number of disks that come in and out of our offices, so we have always been really pleased with Sophos Anti-Virus. The introduction of the new Sophos Educational Site Licence makes it an even more obvious and cost-effective choice for us and our schools.'

## 1998 worldwide exhibitions

**Last month Sophos was at Network + Interop in Las Vegas and this month sees us at exhibitions in the UK, France and the US. Come and see our technical, sales and marketing staff at one of these international venues.**

| | | |
|---|---|---|
| Infosec 98 | June 3-5 | Paris, France |
| PC Expo | June 16-18 | New York, USA |
| Networks Telecom | June 23-25 | Birmingham, UK |
| Windows World Expo | July 1-4 | Tokyo, Japan |
| Windows NT | September 8-10 | San Francisco, USA |
| DECUS | September 13-17 | Paris, France |
| Systems 98 | October 19-23 | Munich, Germany |
| Networld+Interop | October 21-23 | Atlanta, USA |
| VB'98 | October 22-23 | Munich, Germany |
| Gitex 98 | Oct 29 - Nov 2 | Dubai, UAE |
| Windows NT | November 3-5 | London, UK |
| COM Japan | November 10-13 | Tokyo, Japan |

**And don't forget *Defence beyond the firewall* on 11 June in London. For further details, see the front page.**

SOPHOS
ANTI-VIRUS

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England • Tel 01235 559933 • Fax 01235 559935
Sophos Plc • 2 Place de la Défense • BP 240 • 92053 Paris la Défense • France • Tel 01 46 92 24 42 • Fax 01 46 92 24 00
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251
Email sales@sophos.com
www.sophos.com