

Editorial

As the number of different threats which affect businesses continues to grow, Sophos remains ahead of the game, developing and enhancing its products to keep you fully protected. EM Library is now offered as part of most licences and allows you to download the very latest protection against viruses up to 24 times a day. It therefore represents the best way of updating Sophos Anti-Virus, and so we are phasing out the monthly CD after January, as described on this page.

Among other improvements to our products, Sophos Anti-Virus will shortly be available to protect the widely used NetApp storage appliance, Sophos small business solutions have been enhanced and Sophos PureMessage for Unix uses up to 30% less memory.

The inside pages of this newsletter look at two relatively new threats – phishing and spyware – and give advice about protecting against them. There is also more general news about spam and viruses, the latest awards received by Sophos and a roundup of where you can visit Sophos in person over the coming months.

The next issue of Sophos News will be published in February 2005, so as well as “Happy reading”, I should say “Season’s greetings” and “Happy new year”!

Katherine Carr
Editor

EM Library – maximum protection against new and emerging threats



Do you know what lies around the next bend?

Sophos has responded to the changing nature of the virus threat by enhancing EM Library to update even more platforms than before. We are encouraging our enterprise customers to use this highly reliable updating mechanism, and will be phasing out the monthly Sophos Anti-Virus CD for most customers from January 2005.

The rate at which new viruses spread has continued to rise, makes frequent update of your anti-virus software imperative.

EM Library is now included in most Sophos Anti-Virus licences and is the easiest and most reliable method of keeping your protection up to date. It checks for updates every hour, pulling them down from a secure Sophos website as soon as they are published and rapidly deploying them to the servers and desktops on your network across multiple platforms. It even updates your remote users.

Because of the real advantages in using EM Library, Sophos is now recommending that all customers in environments supported by EM Library use this means to keep up to date. With EM Library keeping your network protected automatically round the clock, monthly CD updates are unnecessary. As a

result, they will be phased out, and will no longer be supplied by default to every customer. The last edition to be sent to all customers will be in January 2005. (Major upgrades will continue to be delivered on CD.)

Over the next three months we will be running a campaign to encourage all customers who aren't currently benefiting from automatic updates to start using EM Library. Where EM Library is included in your licence, we will inform you of the credentials you need to install it. If you feel that EM Library is not currently suitable for your environment, we will also be providing details of how you can opt in to continue receiving the monthly CD for the duration of your licence.

To find out more about EM Library, go to www.sophos.com/products

PRODUCT NEWS

SAV for NetApp

A new version of **Sophos Anti-Virus**, providing on-access scanning for all models of NetApp servers, will be available shortly from the Sophos website.

The software, which runs on a Windows NT/XP/2000 /2003 server connected to the same network as the NetApp machine, is configured through a Microsoft MMC snap-in. Whenever a file is written to or accessed from the protected NetApp server, it is scanned for viruses. Infected files can be quarantined or deleted.



Small Business Suite

Enhanced versions of the **Sophos small business solutions** have been released. Enhancements include improved reporting on installation in the Sophos Anti-Virus Small Business Edition and the ability to filter spam in Japanese mail streams and other multi-byte character languages in the PureMessage Small Business Edition.

PureMessage

The latest version of **Sophos PureMessage for Unix** (v 4.7) includes a number of enhancements to the anti-spam module including a reduction in memory consumption of approximately 20-30%. In addition, the delivery of spam updates is even faster.

SAV version numbering

The numbering of **Sophos Anti-Virus** versions has changed slightly. There are now two version numbers – one for the software version and one for the virus data. As before, both versions follow the structure 3.84, 3.85, 3.86 etc, with the second number continuing to increment each month. However, the software version number will now have a third digit, which will increase by one for each interim release. So, for example, in the November 2004 release, the software version number was originally set to 3.87.0.

You can find out more information about all Sophos software at www.sophos.com/products

SPAM SCAM

Don't get caught in the phishing net

Phishing is an increasingly common type of spam in which “spoofed” emails, appearing to come from a legitimate website, request personal details such as credit card numbers or online banking passwords. According to the Anti-Phishing Working Group, up to five per cent of recipients respond.

The sole purpose of phishing emails is to steal personal information from recipients' online accounts. The emails contain links to a spoofed website that looks exactly like the real site. In addition, the address is usually similar to that of the real site, such as mybankonline.com instead of mybank.com.

In order to get an immediate reaction, phishers often include false but sensational messages in the email, such as “urgent - your account details may have been stolen”.

As well as making sure your computer is kept secure, there are

a number of other ways in which you can protect yourself:

- Never respond to emails that request personal financial information
- Visit banks' websites by typing the URL into the address bar, rather than clicking on a link in an email
- Keep a regular check on your online accounts
- Check the website you are visiting is secure, i.e. starts with https://, and not http://

There is more detailed information about phishing at www.sophos.com/spaminfo/bestpractice/phishing.html

- Sophos uses SPF (Sender Policy Framework) with its email. This is an anti-forgery solution which involves publishing a list detailing which servers are allowed to send Sophos emails. Find out more about how SPF works at spf.pobox.com



Novo Knowledge Base boosts Sophos's website support

“Through solutions such as the Novo Help Desk, Knowledge Base and Document Manager, our focus is to provide customer-driven web solutions that are robust and easy to implement and use.”

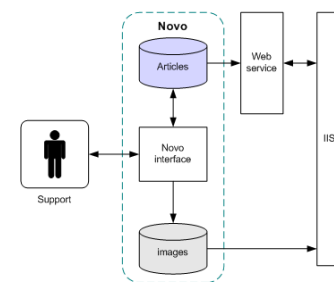
Novo Solutions

As part of a project to redesign its search engine, Sophos was looking for a cost-effective means of efficiently managing its support knowledgebase articles. After an evaluation process, Sophos decided to use the Novo Solutions Knowledge Base, part of the Novo Customer Support Suite.

The Novo application provides an MSSQL Server database and integrates with the Sophos knowledgebase interfaces on both the main Sophos website and the Sophos Partners website. The implementation is available in all Sophos's core languages.

When a search is undertaken, within the Sophos website, it is passed on to the Novo software, with the search results being seamlessly interleaved and delivered. Novo allows for a range of access privileges to be assigned to articles, so search results can be tailored to different audiences. For example, users of Sophos small business solutions can choose not to receive results that apply only to the Sophos enterprise solutions. Support articles can also be displayed as internal web pages for use only within Sophos.

Throughout the project Sophos worked with Novo's support team who provided assistance with queries and provided upgrades to meet Sophos's requirements.



Article ID: 2004 Created: 24 Sep 2004 Last updated: 28 Sep 2004

Rate this article Choose a rating Tell us

Read our search tips Contact one of our experts Suggest an improvement



You can find out more about Novo Solutions at www.novosolutions.com

22 new security flaws – are you patched?

Microsoft has released information about 22 new flaws which affect its products. Most of the advisories are labelled “critical”, Microsoft's highest severity level. In addition, “proof of concept” code that exploits a security vulnerability associated with JPEG image files has been published on the internet. Sophos is recommending that customers ensure their computers are patched and fully protected against all these vulnerabilities. To find out more, visit www.sophos.com/virusinfo/articles/criticaloct04.html and www.sophos.com/virusinfo/articles/jpegpatch.html

CASE STUDY

Coast Capital Savings

When British Columbia's Coast Capital Savings Credit Union needed a solution that could be customised to its specific requirements, it turned to Sophos PureMessage, which has given it greater control and management of email traffic at the gateway.

Coast Capital Savings is one of Canada's largest credit unions, with \$6.4 billion in assets, 300,000 members and 42 branches. In 2002 and 2003, it was recognized as one of Canada's Top 50 companies, for its business practices in the areas of leadership and strategy.

When the company experienced an influx of spam in 2002, it decided it needed to do something to protect its 2000 email users from unsolicited emails. At the same time, it wanted to prevent email-borne viruses from causing infection at the gateway.

Having investigated a

number of options, it chose Sophos PureMessage.

Scalable quarantine architecture and the

ability to customise email policies were critical elements in the decision. However, says

"We are very pleased with Sophos PureMessage. Users feel as if they have died and gone to heaven."

*Andrew Banman, Information Technology,
Coast Capital Savings Credit Union*

Andrew Banman of Coast Capital, "the spam digest was the most significant feature that influenced our decision, due to the way it diminishes the issue of false positives."

You can read the full case study at www.sophos.com/products/feedback/coastcapital.html



VIRUSES, SPAM AND HOAXES

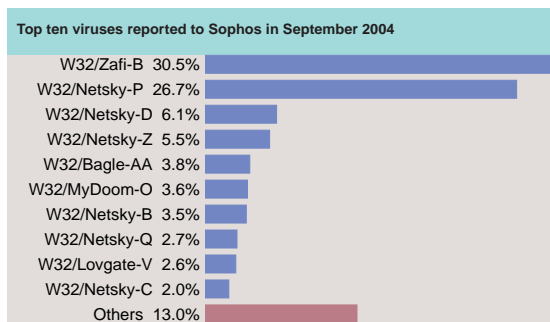
Virus top ten

The September 2004 chart of viruses reported to Sophos shows Zafi-B occupying the top slot for the fourth consecutive month, although the number of reports is beginning to drop off. Conversely, reports of Netsky-P, in the number two slot for the third consecutive month, are actually growing.

Watch out too for the new "Lottery winner" hoax, one of several email scams which claim that the recipient has won a substantial monetary prize. When "winners" contact the lottery company to claim their prize, they are invariably asked to pay a handling fee or disclose bank account details.

Spam producers

Sophos researchers investigating the country of origin of spam have reported that nearly a year after the introduction of the CAN-SPAM



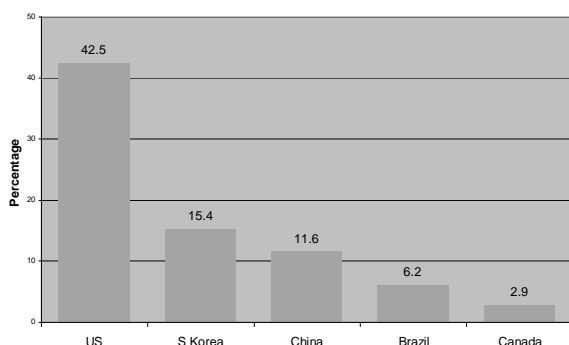
legislation, the US remains by far the worst offender, exporting 42.5% of all spam. The top five spam-producing countries are shown in the chart below. The Sophos report, produced at the end of August 2004, was based on all spam messages received at Sophos's global network of honeypots over the month. The figures show that Canada has made some progress in cutting the percentage of spam sent from the country by over half – from 6.8% to 2.9% over a six-month period.

However, the most broadband-connected country in the world, South Korea, almost tripled the percentage of spam it was responsible for in the same period.

You can find full details of the top ten and other viruses, as well as information about the latest hoaxes at www.sophos.com/virusinfo

The full article about where spam originates is at www.sophos.com/spaminfo/articles/dirtydozenaug04.html

The top five spam-producing countries



Looking at...spyware

What is spyware?

Spyware is software, usually installed without the user's consent or knowledge, that gathers information secretly from a computer and relays that information, also covertly, to someone else.



How does spyware become installed?

Spyware can be installed by a virus or Trojan, for example when a user clicks on a weblink or opens an attachment in an email.

Is business threatened by spyware?

There are several ways in which spyware can compromise business:

- **Data theft:** Spyware can steal confidential business information, such as financial data, personnel records and passwords or any other information typed into the affected computer. A damaged reputation, the loss of money or competitive advantage and an increased risk of litigation can all result from this data theft.
- **Hacking:** Backdoor Trojans can allow hackers to take control of a computer in a variety of ways, such as deleting project plans, altering stock records, downloading porn or controlling the user's mouse and keyboard.
- **Zombie attacks:** Spammers can take over a vulnerable computer or web server and force it to send out their emails for them, thus making the email appear to be from a legitimate source. Computers that have been hijacked in this way are known as "zombies". Sophos estimates that as much as 40% of spam is being sent from zombie computers without the user's knowledge.
- **Network damage:** Spyware places extra demands on networks, decreasing productivity and using up resources on finding and clearing up the problem.

How widespread a problem is spyware?

A SpyAudit report conducted by ISP Earthlink and Webroot Software performed 2.07 million scans in the first six months of 2004, finding 332,809 system monitors and 366,961 Trojan horses.*

How can I protect against spyware?

There are many basic measures which can be taken. For example, putting in place a firewall, implementing the latest security patches and educating users about best practice. However, the most effective way is to protect both the email gateway and desktop with integrated software solutions.

What protection does Sophos offer?

Sophos protects the entire enterprise, no matter what its size or complexity. Sophos Anti-Virus provides protection from spyware and viruses on desktops, servers and remote laptops. Sophos PureMessage protects the email gateway, preventing spyware, viruses and spam from entering the business network.

You can find out more about spyware and how Sophos can protect against it at www.sophos.com/virusinfo/whitepapers

*www.mediapost.com/dtls_dsp_news.cfm?newsID=262876

REVIEWS AND AWARDS

Boost for small businesses

A recent ITP Technology review of Sophos Anti-Virus Small Business Edition, part of the Sophos Small Business Suite, concluded that the product "is an excellent package for the small business. Its centralised structure is conducive to effective management on a small network".

The review praised Sophos's "neat trick" for ensuring all PCs are updated in a uniform way, stating that the central distribution and management of updates "is a great boost for small businesses that cannot afford to set aside a budget to manage security". The scores were:

- Performance: ★★★★★☆
- Feature: ★★★★★☆
- Value: ★★★★★☆
- Overall: ★★★★★☆

You can read the full review at www.itp.net.

Find out more about all the Sophos small business solutions at www.sophos.com/products

Sophos tops company lists

Sophos's continuing stable growth has been reflected in its appearance in two new listings of top companies:

- The 2004 Software 500 list, compiled by Software Magazine, has named Sophos as one of the world's largest software companies, ranking it 226th in a list of the world's foremost software and services providers.
- Sophos has been listed at position 35 in the Europe 500 list. BusinessWeek and Europe's Entrepreneurs for Growth have teamed up to create a listing of Europe's high-growth, job-creating companies.



Read more about this and other reviews at www.sophos.com/products/reviews

Newsbytes

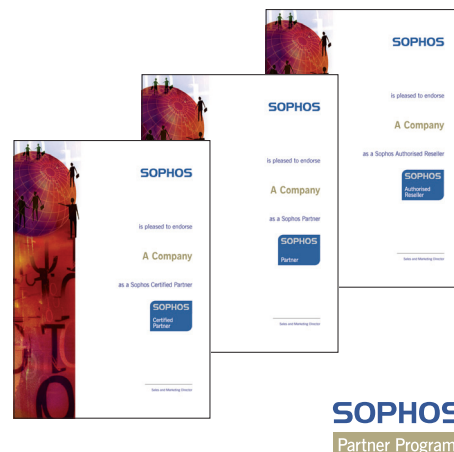
- Sven Jaschan, the teenager who has admitted responsibility for the Sasser and Netsky worms, has been hired by a German computer security firm.
- The US House of Representatives has passed the Internet Spyware Prevention Act to protect computer users from criminals who aim to spy and steal information via the internet. Under the legislation, anyone infecting a computer with spyware can be jailed for up to five years.

PARTNER NEWS

Helping them to help you

Many of you will have bought your Sophos software through a reseller or Sophos Partner. Sophos recognises that it is essential to offer not just the companies but the individuals within them guidance, training and support in order for them to continue to offer the same high levels of expertise and service.

Partners have always had the opportunity to attend Sophos training courses. Now, however, they will be given personal recognition of the training they have received in a new certification scheme. So look out for the new certificates, along with the Sophos Partner Program logo, all of which have been given a fresh new look.



EVENTS

Meet Sophos

There are many opportunities to meet Sophos at trade shows, security conferences, seminars and breakfast briefings. Below are just some of the places where you can see Sophos over the next couple of months. There are also free online seminars in which you can participate.

REGION	EVENT
North America	
14-19 Nov	Large Installation System Administration Conference, Atlanta, GA
17 Nov	CIO Executive Summit, Detroit USA
17-18 Nov	Massachusetts Computer Using Educators Conference, Sturbridge, MA
22 Nov	WestCoast Security Forum, Vancouver, BC
30 Nov	CIO Executive Summit, San Francisco, CA
30 Nov-1 Dec	Homeland Security Conference & Exhibition, Washington DC
7-9 Dec	Infosecurity USA, New York, NY
Europe	
16-18 Nov	Exponet 2004 Cologne, Germany
24-25 Nov	Infosecurity CNIT, Paris, France
Asia Pacific	
16-19 Nov	IT2004 – Evolution, Coffs Harbour, Australia
25-26 Nov	AVAR 2004, Chiba, Japan
1-3 Dec	South Pacific User Services Conference, Dunedin, New Zealand

You can find out more details of all these events at www.sophos.com/companyinfo/events

Thank you...

...to all our customers who took the time to complete our online survey – and especially to the user who rated us "100% great"! Nearly 2000 forms were received from 86 countries. As in previous years, our products and technical support received high ratings. However, we are not complacent and your feedback is very important to us in directly influencing our future product and customer service plans. Over the coming weeks we shall

be putting in place more processes to help us maintain our high standards. Look out for more details on the website.

- For the second year running, Sophos has been rated "Vendor of the Year" in the security category of Computing magazine's ImageTrak 2004 customer satisfaction survey, published on 16 September 2004.

Read more at www.sophos.com/companyinfo/news/customersat.html

If you have any comments about Sophos News or any issues you would like to see covered, please email sophosnews@sophos.com. If the person or address to whom Sophos News is being sent has changed, please email customerservice@sophos.com.