

BUSINESS SOLUTIONS

Taking spam off the menu

Spam has increased to such a degree that it is more harmful than viruses. Steve Baxter visits a school to examine a system put in place by IT staff to try and stop the flood of junk email to teachers and pupils

THIS MONTH'S PROBLEM

This year might be remembered as the year when spam messages first outnumbered genuine emails. A report from email security firm MessageLabs says the company analysed almost one billion email messages in May and found that around 76 per cent, or over 700 million, were spam (see *Newsfile, Shopper* September 2004). The problem is out of control. Governments try to legislate against the tide but they have been unsuccessful so far.

In many ways, spam is a bigger problem than viruses. Most PCs that become infected either have no virus protection or protection that's out of date. If you are infected, excellent tools exist to remove viruses. If you're organised, you can let the virus threat fall to the back of your mind.

Spam is far more intrusive and the amount of time users waste filtering spam

from genuine email – sometimes known as 'ham' – has a significant effect on productivity. We need add-ons to our email systems that deal with spam as effectively as the software we use to fight viruses.

This is a challenge for developers because spam messages don't have the same characteristics as viruses. They tend to be non-executing, plain text messages. Distinguishing between spam and ham is a fine art; it's not as simple as cutting out messages that are sent to hundreds of users.

The more users an email system has, the bigger the problem becomes. To see how an effective shield can be built against spam we went to visit the type of organisation that suffers more than most: a school.

CASE STUDY

Bedford School is an independent school for around 1,100 boys. An IT manager in a school or college faces different problems to one in a commercial company. Whereas office workers tend to use the same computer every day, students use different computers all the time. However, they need to know that the different computers will all behave in the same way.

A school also has a different ratio of users to computers. A business may have almost equal numbers but a school will have far more users than computers.

Bob Eadie manages the senior school's fibre-connected IT network. He's responsible for running the students' computers and a smaller network of computers used by teaching and administrative staff.



THE SOLUTION

Spam started to become a serious problem for Bob Eadie last year. Up until that time, his main concern regarding email had been viruses. These were effectively countered by server-based anti-virus scanning.

The way pupils and teachers used their computers meant that the school may have been particularly prone to spam attacks. Most office workers use the internet for email and checking on leisure-related topics such as holidays. In contrast, at schools the internet is used heavily for research. All users cast their nets far and wide to websites and newsgroups, registering details extensively and making school email addresses easy to find. Eadie believes newsgroup users are hit particularly hard. It took a long time for adequate techniques to emerge to protect email addresses.

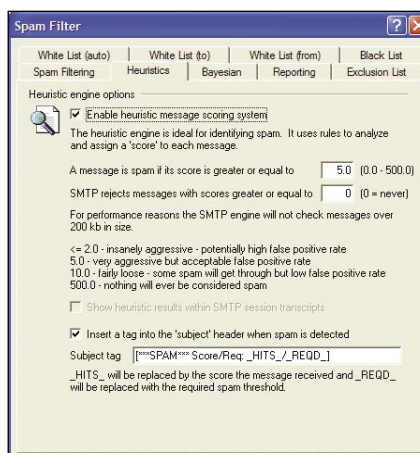
Understandably, Eadie wouldn't be drawn on whether giving internet

access to hundreds of adolescent boys generated higher than usual traffic to sites of a, shall we say, titillating nature. It's possible, though, and if you give an email address to this sort of site you can guarantee large quantities of spam daily.

THE SERVER

Bedford School uses MDAemon as its main email server. This handles messaging for the students and for most of the teaching staff. It was fortunate that just as Eadie noticed the need for a spam filter, Alt-N (www.altn.com), the server's developer, produced one. Because he has a close working relationship with the program's UK distributor, Zen Software (www.zensoftware.co.uk), he became a beta tester.

The server's main spam filter works in much the same way as its competitors do. It checks the content of every message and awards it a score. The higher the score, the more



With MDAemon, each email gets a score that rates its chances of being spam

administrator can choose to delete the message before it reaches the user or flag it as probable spam and pass it to the user for a final decision. One thing Eadie particularly likes about the MDAemon spam filter is that, like the server's other features, its default settings are realistic. He found that it was possible to install it and leave it, with fine-tuning needed only at a later stage.

FINE TUNING

Early spam filters, including MDAemon's, were unintelligent beasts that

blocked messages based on where they came from instead of what they said. Such blacklisting systems still exist within MDAemon, if you want to use them, but its latest filter is far more intelligent.

likely it is to be spam. The spam filters don't stick their necks out and say that a message is definitely spam, just in case it isn't.

Depending on the score a message is given, the server

likely it is to be spam. The spam filters don't stick their necks out and say that a message is definitely spam, just in case it isn't.

Depending on the score a message is given, the server



This filter improves its accuracy through a process called Bayesian Learning, also known as Bayesian filtering. This is not based on hard and fast rules designed to find spam. Instead, it uses statistics and probabilities to assign a likelihood that a message is either spam or real. This may sound complicated but operating it is simple.

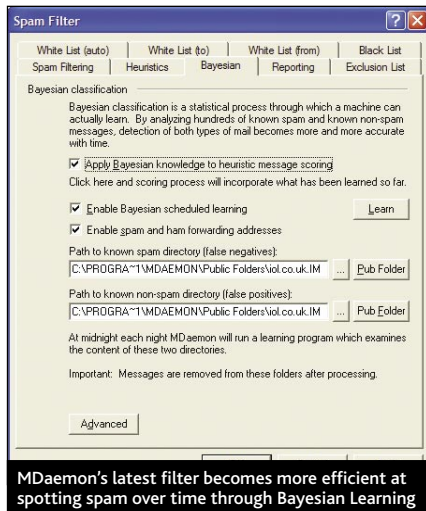
If a spam message slips through the filter, the user drops it into a Missed Spam folder. Once a stock of 200 such messages has been collected, the program uses its Bayesian wizardry to work out why it didn't recognise them correctly. For the learning process to work well, users must also feed the other side of the Bayesian brain, the side that improves its recognition of genuine messages. This side needs to be fed a steady stream of genuine emails (ham messages).

We were wondering if Eadie had found this side of the equation to cause any problems. Feeding genuine messages to a spam engine is, after all, counter-intuitive. In practice it wasn't a problem, but not because he could depend on users to feed both sides of the engine. On the contrary, he decided early on that feeding the learning engine was not a job for normal users. His concern was that people would fail to make a distinction between messages they didn't want and spam. A message isn't spam just because a user doesn't want to read it, and if that user incorrectly fed an unwanted message to the Missed Spam folder the learning process would be corrupted.

Eadie decided the best policy was to have the learning process exclusively handled by the school's IT staff and a couple of special users who'd been particularly badly blighted by spam. These users received more than enough spam and ham between them to feed the engine and make significant improvements in accuracy.

FOLDERS

Most people use a Post Office Protocol 3 (POP3) system to handle their email because it has been established longer than the main alternative, Internet Messaging Access Protocol (IMAP). The most noticeable difference between the two systems is that if you use POP3 you collect your messages from the server and store them on your workstation. IMAP users can view



MDaemon's latest filter becomes more efficient at spotting spam over time through Bayesian Learning

their messages on the server and leave them there.

MDaemon's advanced features, including its spam filtering, work best when users have IMAP mailboxes. This fitted right into Bedford School's plans. Eadie had always wanted, indeed needed, a system that would let pupils and teachers access their email regardless of which computer they were using. This was not possible with a POP3 system because messages would be downloaded and stored on whichever computer read them. This meant he had to base the school's email system on IMAP.

When MDAEMON's spam filter came along with its commitment to IMAP folders for missed spam and genuine ham, the school was able to integrate it without a hiccup. Organisations using POP3 will have a harder time.

OUTLOOK AND IMAP

Outlook presents particular problems. Microsoft's excellent Personal Information Manager (PIM) may have great features for administration, organisation and collaboration but its IMAP support is weak. You can certainly access IMAP folders through Outlook but it won't work seamlessly with them. It's hard to avoid Outlook saving files to, or trying to read them from, your hard disk rather than the IMAP server. Outlook is a far worse IMAP client than Outlook Express, the free email reader that comes with all versions of Windows. If you use Outlook, be warned that you'll need extra time for configuration.

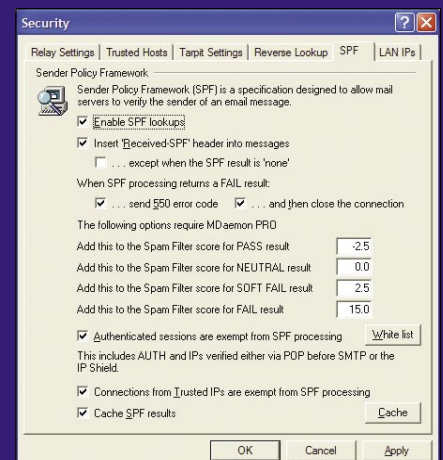
MDaemon's spam filter operates an unusual dual role. Not only does it protect MDAEMON users, it's also the first line of defence for the school's Exchange Server installation. Any email sent and received through Exchange Server has to go through the MDAEMON

STOP THE SPOOFERS

Sender Policy Framework (SPF) is a new weapon in the fight against spam. This anti-spoofing technology is now incorporated in MDAEMON.

Spoofing is a process where a spammer writes a message that claims to come from an address or server other than the one that in fact sent it. This technique keeps the spammer anonymous and stops us pushing red-hot fuse wire under his fingernails while force-feeding him raw road kill.

SPF compares a message's source address against the IP addresses that are authorised to send messages from that address. If they match the message is treated as genuine; if not it's treated as a spoofed message or spam. SPF competes against similar systems from Microsoft (Sender-ID) and Yahoo! (DomainKeys).



Foil the spammers with Sender Policy Framework, MDAEMON's new tool that combats spoofing

Server before reaching the outside world. This curious arrangement evolved because the school's administration staff needed the kind of collaborative features that are available only when using Outlook and Exchange Server.

The Exchange Server has its own spam filter, an add-on program called iHateSpam from Sunbelt Software (www.sunbelt-software.com). Impressive though MDAEMON's spam filter is, iHateSpam weeds out a few more messages. Eadie does not consider this a problem with MDAEMON but believes it's an indication that spam filtering is still an imprecise science. Just as the best protection against viruses comes from using multiple systems (such as one at the server and one on each workstation), he believes spam filtering improves when two 'minds' are applied to it.

GROUPWARE

We said that certain collaborative features are available only when you use Outlook with Exchange Server, but this is not entirely accurate. There are third-party programs available to mimic the collaborative features of Exchange Server so that you can, for example, share calendars and contacts or pass tasks from one user to another.

The best known of these utilities is called Groupware for MDAEMON.

It's an add-on to the email server Bedford School already uses. So why does Eadie still maintain the Exchange Server? We were intrigued.

Eadie's answer was simple: "If it ain't broke, don't fix it." The school bases most of its email around MDAEMON because MDAEMON was far cheaper than Exchange when it set up its own mail server. Microsoft may not do it now, but it used to calculate licences per mailbox instead of per computer. A 1,500-mailbox licence would be beyond the budget of most government ministries, let alone a modestly sized school.

The school could, however, afford a small Exchange licence so the administrative staff could work together. This system is working well and, although Eadie has run some tests with Groupware, he knows there would be disruption if he went live with it. Groupware version 2 is said to be a significant improvement and much closer to emulating Exchange. When it comes out later this year, Eadie says he will give it a thorough test.

CONTACT

STEVE BAXTER
Email Steve Baxter for IT solutions to your own business problem or objective
business@computershopper.co.uk