

COMMIT Chairman Peter Ashton appears to have been travelling almost as much as yours truly lately, indeed I've seen more of him on airport shuttle buses than I've seen in Riyadh. In the absence of any report from Peter I've cropped a few bits from assorted sources about a problem common to us all. I hope it doesn't worry you too much!..Ed

## MYDOOM GLOOM

MyDoom - or Shimg - has become the first major infection of 2004, and while the year is still young it will take some beating if it's not to still be the worst come year-end. Within 24 hours of it first appearing, MessageLabs had intercepted 1.2 million copies of MyDoom leading the antivirus vendor to pronounce it the fastest-spreading virus of all time.

While vendors have been quick to point out that the email itself is nothing special, its rate of spread and self-propagation has surprised many. The virus first appeared in Russia and spread overnight - following the sun as business worldwide woke up to infected inboxes.

Simon Perry, divisional vice president security strategy at Computer Associates, expressed an element of surprise that something almost retro in its design can cause such havoc.

"It's nothing unusual as far as technique - it propagates via address list. But it is doing so very effectively," he said. "It seems that we can still have your bog-standard email blaster giving us grief, even in this day of the vulnerability exploit."

However, Perry made it clear that the writer hasn't left everything to chance. The worm does have some tools in its arsenal to evade detection and aid propagation.

"The main reason it is spreading so effectively is that it is highly adaptive in the email form it takes. It spoofs origin address, alters email title, email content and attachment at random," he said.

To date the most headline grabbing element of the worm's existence has been its apparent anti-SCO mission - leading some to suggest it is the latest offensive in the newly coined 'Linux Wars' as techies air their frustrations at SCO's open-source licensing claims.

Graham Cluley, senior technology consultant for Sophos, said: "The MyDoom worm takes the Linux Wars to a new intensity. It appears that the author of MyDoom may have taken the war of words from the courtrooms and internet message boards to a new level by unleashing this worm which attacks SCO's website."

"If we ever get our hands on MyDoom's creator my guess is that he will be an open-source sympathiser. Of course, it's the last kind of assistance the open-source community would want at this time," added Cluley in a statement.



### NEW WARNING OVER 'SON OF MYDOOM' VIRUS

Computer security experts have given another warning in February 2004 of a new computer virus that is expected to attack computers which are still infected with the MyDoom virus.

The new worm, known as DoomJuice, was detected on Feb 10th and has so far infected at least 30,000 computers worldwide since it was activated on Sunday the 8th Feb.

Mikko Hypponen, director of antivirus research at F-Secure, a Finnish computer security firm, said that DoomJuice, like MyDoom, is designed to attack Microsoft's main website.

Mr Hypponen said: "Unlike Mydoom, it does not spread via e-mail. It comes through a backdoor left open by Mydoom. People won't even realise their computers are being attacked, and then they'll have both Mydoom and Doomjuice in their computers." F-Secure was one of the first to give warning of the dangers of the e-mail MyDoom worm, also known as Novarg.

Mr Hypponen believes that the authors of DoomJuice are the same people that wrote MyDoom, which infected up to one million computers worldwide in just a few days, clogged the internet and caused huge delays in the delivery of e-mails worldwide.

The main Microsoft website appears to be operational so far, but F-Secure said that it had noticed a disruption in service yesterday.

Microsoft announced last month that it was offering a reward of \$250,000 (£134,000) to anyone that helps find and prosecute the author of the MyDoom. Doomjuice's ability to spread is limited because it will only attack computers that are still infected by MyDoom, Mr Hypponen said. "And lots of them are being cleaned up already at a quick rate."

But he warned that, unlike MyDoom which is programmed to stop spreading on February 12, Doomjuice could run forever. "At least until all computers everywhere infected by both worms have been cleaned up, and that could be years," he said.

WHAT'S  
NEW IN  
THE  
COMMIT  
ARENA