As everyone probably knows first hand by now, we’ve all been suffering through a particularly bad period of worm infestation on the ‘Net lately. Variants of the SoBig and Blaster (aka LovSan) worms (often called “viruses” in press reports) caused major hang-ups world wide. I want to focus today on the SoBig worm and other electronic thugs that use a victim’s e-mail address book to send out lots of e-mail messages. Many of the worms use their own SMTP interface, bypassing the victim’s e-mail client program and thus leaving no obvious trace (e.g., “SENT” messages) that the user can spot early on in the infection. Worse still, modern worms often use the victim’s address book not only for targets (destination addresses) but also to forge SMTP headers using spoofed origination addresses. That is, the worms are written to make it appear that their infected traffic comes from someone whose address has been picked up from another victim’s address book.

Some antivirus programs respond to infected e-mail messages by sending a notice to the originator of the infected message. For example, you may have received message like these:

> From: postmster@somwhere.com
Sent: Thursday, September 04, 2003 22:30
To: mkabay@norwich.edu
Subject: Virus Detected by Network Associates, Inc. Webshield SMTP V4.5 MR1a

Network Associates WebShield SMTP V4.5 MR1a on mimesweeper detected virus W32/Sobig.f@MM in attachment document_all.pif from <mkabay@norwich.edu> and it was Cleaned and Quarantined.

At one time, such messages were helpful to the victims of worm and virus infections because (a) many victims lacked antivirus products; (b) the infected e-mail actually came from the indicated sender.

Unfortunately, although (a) may be true, (b) is almost certainly false. The chances that an infected message is coming from the indicated FROM address are small – they are 1/N where N is the total number of addresses in the e-mail address book of the actual victim (assuming that the victim’s own e-mail address is included in their list). So the chance that the automatic notification will go to a wrong address in a single infection is (N-1)/N. If a victim has 1,000 addresses in his or her address book then the probability that replying to an infected message will reach the wrong person is 99.9% for a single incident. What was once a courteous and helpful practice has now become an annoying contribution to the wasteful traffic generated by the worm, potentially doubling the number of spurious messages (for every one from the worm, one from the antivirus). I recommend that system administrators now disable the automatic notification to the supposed origin of infected messages. It’s just not working any more.

It’s time to cut the worm chatter.
NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.