In recent months, malicious software and hoaxsters have been increasing the level of social engineering via e-mail. This column is the first of two that will serve to alert your network users of some of the more flagrant abuses of e-mail that have been increasing lately.

* * *

The KLEZ worm has become the number-one type of malware circulating on the Net today. Now, we know that many worms have been using misleading subject lines for years; I suppose a non-misleading subject line would be “This message contains a worm” but that wouldn’t go far in helping to spread the malware, would it?

KLEZ goes one worse: it forges the SMTP header so that the message appears to come from a user other than the real victim. This social-engineering trick means that KLEZ is causing havoc among naïve users who aren’t aware of the problem. These victims assume that the infected file is coming from whichever e-mail address is listed in the FROM field and thus send helpful (or irritated, or abusive) e-mail to someone whose only connection may be that his or her e-mail address was in the address book on someone else’s infected computer. In other words, tell your users not to trust the FROM line in any e-mail message that includes an attachment. (Those of you interested in identifying forged headers can use SamSpade from <http://www.samspade.org>.) And of course, as usual, remind everyone in your network that they must absolutely not open attachments that they are not explicitly expecting for a specific reason. (OK, I know, it’s really _executable_ attachments, but that includes so many file types that it’s not worth going into with non-technical users.)

The obverse is that users should let their correspondents know in advance if they are sending an attachment OR they should use a digital signature on all their e-mail so that the authenticity of everything ostensibly from their address can be verified. There are no worms that can successfully sign an e-mail using a digital signature (yet).

One of the best descriptions of the situation that I have seen is an article by Michelle Delio in Wired <http://www.wired.com/news/technology/0,1282,52055,00.html>. You can also type “Klez worm” into a search engine for scads of other entries concerning this worm.

* * *

KLEZ is also using e-mail distribution lists as a vector. Some list managers are finding that KLEZ-infected messages have been spreading through their unmoderated lists or _appear_ to be coming from their list. Recipients of the worm then bombard the list with complaints, which sometimes get amplified out to the entire list, causing mailstorms.
Remember, if you are managing an e-mail distribution list, be sure that the REPLY-TO address on output from the list is _not_ the same as the posting address. Unfortunately, because the posting address is likely to be stored in address books, KLEZ may get access to it for its forgeries and for its destination, so even this measure won’t stop the mayhem. However, consider converting your unmoderated list into a moderated list, possibly by recruiting volunteers who can help in the task of vetting every message before it is posted to all members. At least then you’ll be able to catch the worm’s attempts to spread via your list and also stop amplification of complaints.

* * *


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 <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 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.