But is it real?
When a hoax becomes a chain letter

Ivan Trundle

Manager, communications and publishing
ivan.trundle@alia.org.au

A rash of virus warnings have prompted me to jump on one of my favourite hobby-horses this month. Rather than complain about the state of software and the ridiculous amount of effort software users have to put in to make themselves actually productive in their use of computers, I have decided that the best form of defence is to educate the unwashed masses who believe that every new virus warning should be taken seriously enough to broadcast the message to their friends.

The topic raised its ugly head the other day when I was in a meeting with some local computer consultants. We were trying to determine what the best options were to upgrade the now venerable hardware that supports all of ALIAnet's services, and to increase the available bandwidth in the process. We were trying to make choices on both hardware and software platforms, and looking to see if any real improvements had been made over the years. It is quite remarkable to observe that we have had the ALIAnet server running without a disruption of any kind (other than the very rare restart) for more than five years, and have had only two break-in attempts (viruses or otherwise) that were successful. Of the security patches available for the various systems used for internet services, a few really stand out — Microsoft-IIS/4.0 security patches lead the pack, with patches available almost daily, whilst others, such as Solaris (from Sun), are relatively secure at the other end of the scale, with patches available barely once a month, at best. This in itself indicates both the level of security, and the level of activity. Unix systems are not necessarily more secure, either — FreeBSD has a fresh collection of patches created almost as often as those for Microsoft IIS, although the reasons for the requirement of such patches may differ slightly. Check out http://www.auscert.org/ for more information, and if you want to find out what server software a site is running, go to http://www.netcraft.co.uk/whats/.

...educate yourself to be less vulnerable to such attacks by installing virus-checking software...

But back to e-mail hoaxes and viruses. In the past, I have written about the overall effect on computer systems of people sending warnings of dangerous viruses and the traffic that is generated. Whilst I can understand that some computer people are keen to keep their friends 'clean' of viruses, and to warn them of impending peril, it is generally better to ensure that education takes place in a different way. Sending warnings only exacerbates the problem in that the 'net and countless user's in-trays are clogged with warning messages instead...

Here are some e-mail tips:
First, only send such messages if you have recently been infected by the virus you are warning about, but only *after* you have cleaned your system with a commercial-grade virus-cleaner. Second, only send warnings to those who are most likely less-well educated in these things, and be very selective about who receives the message (otherwise the warning becomes the virus itself). Third, keep in touch with more-educated computer users that you trust to know the overall effect of such software, and combine this with reading alerts from the various virus-scanning sites such as Norton AntiVirus or MacAfee.

But more importantly, educate yourself to be less vulnerable to such attacks by installing virus-checking software *and* by reducing the overall effect by not allowing external software to run on your machine nor to let attachments to received e-mails slip past the gatekeeper and wreak havoc. The only way that most of these viruses can work is by the user allowing downloaded applications to run on their machine, and by letting attachments to e-mails run as scripts that can link to other software on the local machine. Unfortunately, Windows users are actively encouraged to link their applications in such a way that infection is almost guaranteed. The tide is slowly turning, though — Microsoft executives have finally been convinced that programmers who write software for Microsoft should set these so-called features off by default in newly-installed operating systems and office applications, rather than the other way around.

And last of all, keep track of those fortunate friends who use Unix systems or Macintosh systems, and who are very rarely likely to have to worry about such things at any time in their own computing environments. Respect the fact that they are less likely to warrant such warnings, and save the e-mail contact for more normal personal communications...

If you really want to find the low-down on virus hoaxes, in a very entertaining and readable form, wander over to http://www.vmyths.com (though I hesitate to recommend this site due to its cookies being a tad overdone...). ■