'Hoaxers ... use a form of memetic malware ('viruses of the mind') in order to reprogram system users.'

David Harley, ESET

BOTNETS OF THE MIND

'…At the very least the mind is a plausible candidate for infection by something like a computer virus…'[1]

I imagine that most readers of *Virus Bulletin* have some idea of what a botnet is, but bear with me.

A botnet is a virtual network of computers: virtual in that its members are not connected by physical cabling or other attachment to the same network segment, but by the fact that each has software installed (an 'agent' or 'bot') that allows a remote machine to access and make use of it. Not all bots are malicious, but the ones we talk about most in security circles clearly are. A bot-infected machine is often called a zombie, and one malicious use for a network of bot-infected machines is to disseminate spam[2].

A lot of money is made by some types of spam, including those advertising goods (the goods may or may not exist, but if they do exist, they seldom deliver everything the buyer is led to expect); social engineering emails that trick victims into running malicious attachments or accessing malicious URLs; and out-and-out fraudulent messages such as phishing scams and 419s.

Chain letters and hoaxes aren't always considered to meet a formal definition of spam. Nevertheless, they can create serious problems: while they may be deceptive rather than fraudulent, they are often unequivocally malicious in intent. Not all hoaxes are chain letters, of course. Come to that, not all chain letters are hoaxes, either, but it's rarely a good idea to forward chain email, even if it doesn't include any deceptive elements.

I used to say 'never' rather than 'rarely', but some situations do arise where people have an emotional need to participate actively in an issue (for instance, the identification of 2004 Tsunami victims or the search for missing children) and feel that chain emails (or more often nowadays, *Facebook* posts and *Tweets*)[3] offer them a way to do that. (Unfortunately, it's not a very efficient way, since the same message [whether true, false or in between] is broadcast again and again, long after any residual usefulness has been squeezed out.)

Fortunately, not all hoaxes pose such ethical and psychological dilemmas for email administrators, being the work of hoaxers who glorify themselves by exploiting the good intentions of others. Some hoaxes (or semi-hoaxes) arise out of genuine misunderstandings and misconceptions, or become divorced from the truth as they spread further across the Internet. However, many are started by people whose warped self esteem is boosted each time one of their victims is made to feel stupid when they realize they've been hoaxed.

Botnets, meanwhile, tend to be run by criminals exploiting bot-infected machines for various profitable activities. So what's the connection between bots and hoaxes?

Well, hoaxes and chain messages can be intended in a very general sense for personal financial gain. Causing large quantities of emails to be sent out spreading specific kinds of hoax misinformation could provide some form of fraudulent payoff for the originator, almost like a pyramid scam or BHSEO. Since there's a history in the hoax-busting business of proof-of-concept examples of possible hoaxes being plundered to form the basis of a real hoax, I won't develop that thought further here.

Hoaxers don't usually use malicious software to infect systems so that they can be used to distribute junk mail, but they do use a form of memetic malware ('viruses of the mind') in order to reprogram system users so that they send out the hoaxer's favoured brand of misinformation[4]. So before you forward any chain letters, ask yourself if you really want to be a zombie...

[1] Dawkins, R. Viruses of the Mind. In Dennett and His Critics: Demystifying Mind. Ed. Bo Dalhbom (Cambridge, Mass.: Blackwell, 1993).

[2] Harley, D.; Lee, A. Net of the Living Dead: Bots, Botnets and Zombies. http://www.welivesecurity.com/media_files/white-papers/Net_Living_Dead.pdf.

3 Harley, D. Origin of the Specious: the Evolution of Misinformation. http://go.eset.com/us/resources/white-papers/VirusHoaxes_Whitepaper.pdf.

4 Harley, D. The E-Mail of the Species: Worms, Chain-Letters, Spam and other Abuses. http://geekpeninsula.wordpress.com/2013/04/02/virus-bulletin-conference-papers-2/.