Should laws be applied to disseminating functional virus code?

A January 1993 discussion in the NCSA (National Computer Security Association, later ICSA and then TruSecure) section on the CompuServe network (for which I was Chief Sysop for several years) considered the issue of forbidding publication of functional viral code. Participants drew parallels between writing down viral code and writing down instructions on creating harmful devices such as bombs. The slippery-slope argument was invoked by one prominent member of the anti-virus community, who said: “My concern is that if we can justify the suppression of information as ‘undesirable’ or ‘potentially dangerous’ is it that much further a jump to ... suppression of other ‘information?”’

Some people have suggested that publishing functional viral code is useful and necessary because everyone should understand how viruses work to be able to combat them. I disagree. No one has explained why it is useful for users and programmers to have access to detailed, working code. Generalized descriptions are fine; even fragments of code may be justifiable. But I draw the line at publishing functional code that can be typed into an assembler or a debug facility and create a working virus.

People who build antivirus products need the code but can get it through private, controlled channels. People who build computer system hardware and want to devise better anti-virus traps can also use real viruses obtained through controlled channels. So can operating-system gurus. Computer scientists and antivirus product developers wishing to publish research on specific features of viruses can share their knowledge constructively by printing portions of the code in question without making the entire functional virus available to all and sundry. As long as what is disseminated does not work if entered directly as printed or transmitted, I see no problem.

But public, unrestricted dissemination of functional viral code to, say, disturbed fifteen year olds intent on causing havoc is unnecessary and harmful and ought to be punished in the same way we place pre-emptive restrictions on other potentially harmful acts.

* * *

More in the third part of this rant.

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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 © 2004 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.