Computers & Security, 7 (1988) 335–336

Guest Editorial

Ethical Issues in Computer Virus Distribution

When I first examined the problem of viruses, I had a severe ethical problem with publishing my results. The problem was that if I published actual viruses, I would be creating a hazard for the computing world, while if I did not publish some sort of program example, the subject would be too hard to understand to get the point across. After thinking about the issue for some time, I decided to publish "pseudo-code" which could not be used directly by an attacker against any particular system, but which would indicate to the reader the nature of the problem.

Recently, companies trying to drum up business in the anti-viral defense arena have begun the unconscionable practice of distributing viruses to potential customers. In one case, an association of companies writing defenses against viruses almost decided to distribute viruses as a policy, but owing to the efforts of two of the members, the association did not sanction the activity. Rather, the individual companies that wanted to send these viruses out continue to do so on their own. Despite their claims that they are only distributing viruses to a few "responsible" parties, one company claims that over 100 disks containing numerous viruses have been distributed to different companies, and that those distributions have been made through a bulletin board system that regularly yields to external attack.

The case for distributing viruses given by these companies consists of two basic points.

(1) To alert the potential customer to the threat.

(2) To provide a test for viral defenses.

I cannot understand how the first argument can be justified under any conditions. Surely the threat is now widely known. Even if it were not widely known, sending viruses to companies that have already expressed interest in defenses clearly does not alert anyone who is unaware of the problem.

The second argument makes even less sense. The fact that a defense works against the 29 known viruses on a distribution disk does not mean that the defense will be of any use against other viruses. Sending a particular set of viruses has a tendency to make people think that if they defend against those viruses, they will be safe. This is clearly not the case.

Let me now concentrate on why these distributions are harmful and shoud not continue. The practice

- is misleading;
- is creating a problem so you can sell a solution;
- is hazardous;
- may be illegal.

It is misleading to distribute viruses for two reasons. It gives the illusion that if a defense works against these viruses, it will work against others. This is not necessarily the case. It wrecklessly endangers hundreds of sites. Even though some of these viruses are supposedly "declawed", a program error or an operator error could cause a large number of infections.

There is no reason to distribute these viruses except to generate sales of products. In order to sell the products, some companies feel they have to scare their customers into a purchase. In a very real sense, it is like a doctor injecting patients with a disease to demonstrate the benefits of using their cure. It does not educate the customer; it only scares them into a purchase.

It has been shown time and again that even the most benign viruses can create problems because of program errors, mishandling, unexpected side effects, and malicious alteration. Program errors in the "Brain" virus have caused extensive losses of files on IBM PCs. Mishandling of viruses caused infections at Hewlett–Packard after an accidental release. Unexpected side effects of the "Cristma.exec" virus caused IBM's world-wide network to go down. Malicious altering of viruses caused the relatively benign Amiga viruses to cause widespread destruction.

In the United States, "unauthorized tampering with data files" was made illegal in 1984. The demonstration computer viruses certainly tamper with data files, and if they spread beyond the system being used to examine them, they will almost certainly violate this law. The fact that proper handling is so difficult

0167-4048/88/$3.50 © 1988, Elsevier Science Publishers Ltd.

makes this problem much more severe than the people distributing these samples may believe. For example, leaving the computer turned on and putting another disk into the system might cause undetected infection to spread throughout a company's computers, and eventually to outside organizations. With 100 copies in the hands of inexperienced users, we can be almost certain that this will eventually happen.

When we discussed these issues with one of the recipients of a sample disk (a U.S. military site), the systems administrator removed the disk and cut it in half on the spot. It is likely that any other responsible administrator would take a similar view.

In short, the practice of distributing computer viruses to demonstrate the problem is unnecessary, wreckless, and dangerous. It is being used strictly for personal gain and should be discouraged by the legitimate community. I strongly urge you, the members of this community, to take a firm stand against this type of activity.

Professor Frederick Cohen