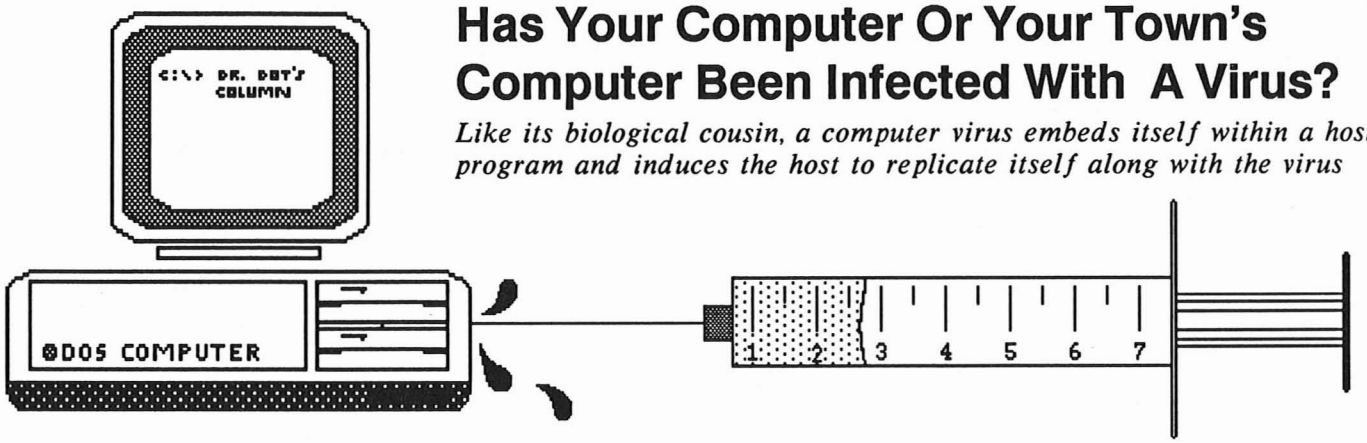

Has Your Computer Or Your Town's Computer Been Infected With A Virus?

Like its biological cousin, a computer virus embeds itself within a host program and induces the host to replicate itself along with the virus

This article was taken from Vol. 2, No. 7, April 1988 issue of PC-Transmission, a newsletter for computer users in transportation published by The University of Kansas Transportation Center.

Watch Out For Viruses
by Carl Thor

Last month, we ran a short news article about computer "viruses," which seem to be the latest trend in the realm of computer vandalism. These insidious little programs represent a significant threat to users of micro-computers, especially those who exchange public domain programs and information with other computers, either by modem or disk transfer. Let's take a closer look at what you can do to protect yourself from them.

What is a virus? Over the years, a few mischievous and malicious hackers have developed various ways of sabotaging other machines, and have released their programs into the public data stream, primarily through electronic bulletin boards.

Some of these creatures include the Trojan horse, an apparently normal program, usually a game or utility, that destroys files as its host disk is used; and the time bomb, which waits until a certain time before destroying data. Most recently, we have seen a number of cases of a new type of saboteur program - the virus.

Like its biological cousin, a computer virus embeds itself within a host to replicate itself. Viruses are often not well understood, partly because of their name association with human diseases, and partly because they inhabit the arcane world of machine language programs. Disks do not infect each other in the storage box, but rather, the virus program must take control of the computer in order to infect other disks.

Currently, the most common approach is for the virus program to be hidden within the operating system program (COMMAND.COM on PC machines). Once loaded into memory, the virus program instructs the operating system to copy itself onto any disk accessed by the computer (such as with DIR, TYPE, or COPY), if that disk already has the operating system file on it. Then, typically, after replicating itself a certain number of times, the virus proceeds to trash all the disks available to it at the time.

Actually, the virus mechanism is benign by itself. According to an article by Tom McBride and Nick Szabo in the March 1 edition of Info-Mat, "a 'pure' virus has survival as its only goal." But any kind of "payload" can be attached to the virus, enabling it to print a message on screen, improve its survivability, avoid detection, or even destroy disk data. The payload can also be benign, but destructive or obstructive payloads seem to be the rule among the viruses reported recently.

Case history Although the concept of virus programs has appeared in the literature for several years (see "Computer Recreations" in Scientific American, March 1985, for an interesting discussion), only in the last year have many actual virus outbreaks been reported. Recent accounts cite infections within several user groups, in computer networks at IBM and Hewlett-Packard, and at the computing centers of several universities.

One of the most widely publicized occurrences was at Lehigh University, where late last fall a COMMAND.COM virus infected PC's throughout the campus. The virus most likely escaped the campus and is now spreading itself around the world. Its characteristic is to copy itself four times, then trash every disk in the host system by erasing their boot records, FAT tables, and directories. Meanwhile, the virus' four children will repeat the process somewhere else as soon as they are booted into another PC.

In a memo circulated at Lehigh University, Kenneth R. van Wyk of the Computing Center stated that "all Norton's horses couldn't put it back together again," referring to the inability to recover data even with the Norton Utilities, one of the most powerful PC data repair programs available. He went on to say that both floppy and hard disks were affected, and concluded by saying "This is not a joke. A large percentage of our public site disks have been gonged by this virus in the last couple days."

What is the degree of danger? Obviously, the potential for damage by viruses (and other sabotage programs) is very serious, although there are some who argue that the whole issue may be a hoax or urban legend, the computer-age equivalent of the Kentucky Fried rat story. I doubt that anyone at Lehigh University would buy the hoax theory, but to the millions of users who have not come into contact with a virus, the whole thing certainly has a science-fiction ring to it. In fact, similar scenarios appeared in stories by several authors long before actual virus programs were created.

So far, viruses that use the operating system as a host are fairly easy to detect, and detection is the prime requirement for prevention. Szabo, who has made a hobby of designing (but not releasing) virus programs, feels that greater dangers may lie ahead. To put viruses into binary files other than the operating system is possible, he says, and would make detection much more difficult. The virus discovered last fall at Hebrew University in Jerusalem is reportedly of this type. Because of its ability to propagate itself to other disks, a virus

continued on p. 6