The Scourge of Computer Viruses

Software bugs deliberately designed to replicate in computer systems have the potential to wreak havoc; protection urged for military data. Is a vaccine feasible?

"Time bombs," "Trojan horses," and "viruses" are man-made bugs that afflict computers and give nightmares to the people who run them. They can choke networks with dead-end tasks, spew out false information, erase files, and even destroy equipment.

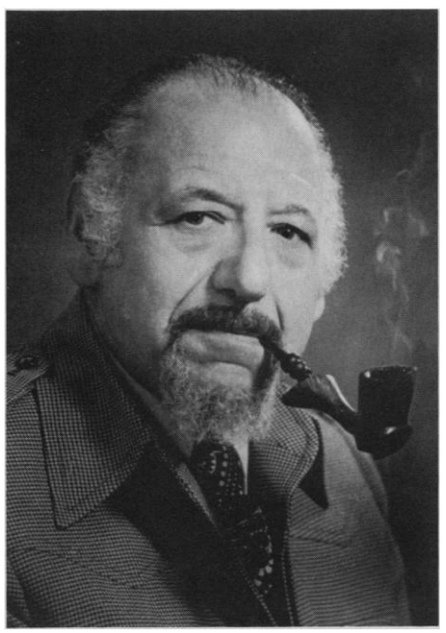
For the most part, these infestations have been confined to the world of computer hackers and electronic security squads. But occasionally, and with disturbing frequency in the last few months, they have escaped to the world at large and wreaked havoc.

Since November, there have been several outbreaks of black programs. As a result, people who have been warned about them for years are being heeded more closely now and computer operators are becoming more cautious about how they exchange data. One of the strengths of America's computer culture is that it provides a wide-open market for information and ideas. The long-term threat of the bugs is that they may force users to create islands of clean data and erect barriers around them. This spring the electronic marketplace has been flooded with a score of "vaccines" and "inoculation programs" designed to tag infestations and quarantine them.

A computer virus, according to Fred Cohen of the University of Cincinnati, is a program that infects other programs by modifying them to include a version of itself. Like real viruses, these ones carry a genetic code, recorded in this case in machine language. The code tells a "host" system to insert the virus into its main logic, usually on a hard disk. Once established, the virus silently infects every other program it can reach. For example, a floppy disk that is formatted in an infected computer will itself be infected and may carry the virus to other hosts.

Viruses are often created by vandals. But they have also been released accidentally by security experts trying to fight vandalism and by curious programmers who were engaged in experiments. Once hatched, the viruses seem to take on a life of their own.

The first viruses, according to Philip McKinney of ThumbScan, Inc., a computer security firm in Oakbrook, Illinois, were developed by software companies in the 1970s for a legitimate purpose. They were used to trace the evolution of programs that were being copied illegally. These little bugs never showed their presence; they just kept track of their parentage. Authors who knew how to read them hoped they could be used to trace the routes of piracy.



Harold Highland. *Editor of* Computers & Security *has devoted most of the April issue to viruses.*

Along with its genetic code, a computer virus may carry a benign or malicious agent. A benign agent, for example, might send a message flashing across the host's video screen. In in-house games played by one software writer against another, they may simply announce, "Gotcha!" or challenge the person at the terminal to an unwanted logical joust. A malicious agent might order the host to kill every file within reach. Usually the self-destruct command is delayed for a period during which the virus replicates, allowing for wider dispersal. The most destructive agent so far, McKinney says, turned up in a corporate network in California last year. It interfered with the scan control of two video monitors, setting one afire.

Destructive viruses are usually introduced in a Trojan horse, an attractive-looking gift program that seems useful but is in fact designed to spread the virus. Perhaps the most diabolical example is a recent Trojan horse that was attached to a program called "Flu-Shot IV." Flu-Shot was created by Ross M. Greenberg of New York as a cheap antiviral agent. He offered it for $10. Someone rose to the challenge, infected it with a virus, and distributed it on public bulletin boards. As a result, Greenberg says, he has had to redo the program and intends to release it with a new name: "Flu-Shot Plus."

A time bomb is any hidden program that keeps track of events and activates itself after a delay. Programmers sometimes leave a "back door" in their work to allow them to return later to make repairs, should the system refuse to grant them entry in the normal way. They have been known to use the back door for less noble purposes, such as to leave off a time bomb for a client who refused to pay his bill.

It is too bad that viruses and vaccines are being noticed by the press, government security experts say. They think this will stimulate copycat vandals, inspiring hackers to create tougher viruses. It would be best to give this subject as little publicity as possible, federal officials say, and they tend to play it down.

For example, the National Security Agency, parent of the Computer Security Center, has nothing to say. "This is just one of those things we don't talk about," according to a public affairs officer who asked to remain anonymous.

Stuart Katzke, chief of the computer security division at the National Bureau of Standards, says, "We have not established a technical R&D program against viruses." Although the problem is "interesting," Katzke explains, "we have got to use our resources for the best benefit of everybody," and inoculation against data diseases is low on the list of priorities. Accidents, stupid errors, floods, fires, and earthquakes are more important because they are more prevalent.

An opposing view is given by researchers who are fascinated with—and claim to be horrified by—viruses. They think better defenses are needed, and quickly. Cohen is

perhaps the most outspoken in this contingent. Another leader is Harold J. Highland, editor of the journal *Computers & Security*.* They say the subject should be openly discussed and that the federal government should invest more funds in computer security, particularly in virus research.

Highland grumbles about the government's shortsightedness. Convinced that electronic diseases will become more important in the future, Highland has given over most of the April issue of his journal to the topic, with articles on the epidemiology, anatomy, and taxonomy of computer viruses. Speaking of the government's lack of interest, he says, "Until they get slaughtered in action, they don't do anything much."

Cohen finds that the Europeans are more interested in his work than the U.S. government. He says: "One of the NSA [National Security Agency] guys told me to my face, 'You're not going to do any research on viruses if we can help it. . .'." People dislike the subject, he thinks, because "they have a tendency not to believe something's going to happen until they get hurt. Once it happens, they react like rape victims," burying their experience.

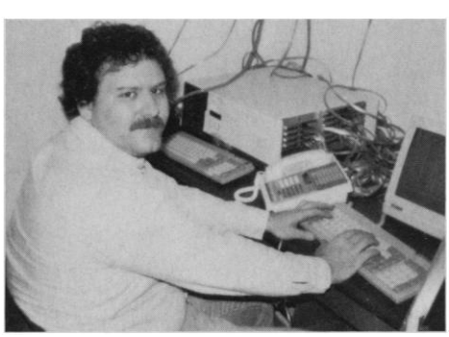
Until a few months ago, Highland says, "I didn't think anybody would talk about" viruses or Trojan horse attacks. It taints a company's image. But recently several incidents have come to light, triggering a cascade of publicity. The sellers of computer security systems have played a part in getting the word out. Many of the reports come from universities, where discussion of such matters is freer. Among the recent cases are the following:

■ The most celebrated example occurred on 11 December when a West German student naïvely sent a devastating Christmas message over a local computer network. When run, it typed out a greeting and forwarded itself to everyone on the recipient's regular outgoing mail list. Because computer mail easily moves across boundaries carrying the authorization of the sender, the message swamped the local network and moved through interconnecting links to IBM's international network, attaching to every mailing list it contacted. Within hours it swamped the IBM network. IBM officials say it was a "disruptive file" rather than a virus, and some have called it a "bacteria" because it lacked the distinctive replicating code. IBM's information officer Andrew Russell of the Armonk, New York office says, "This was the first time such an event has occurred within IBM," and the company is confident that it has plugged the loophole.

■ This winter, universities in the eastern United States and in Israel encountered a couple of nasty viruses, one of which appears to have originated in Pakistan. After replicating for several generations, the Pakistani virus, as it came to be known, destroyed every file it could reach. The number of students and faculty members affected is unknown, but may number in the hundreds. Highland claims to have identified three different strains.

■ About 2000 users of the Commodore Amiga computer have been infected by a virus, according to Highland. The company says the bug was not present in the original software, but Highland is skeptical. He claims it struck simultaneously in Australia, Britain, and parts of the United States, suggesting an infection at the source. He hopes to collect and compare the local strains to determine at what point they entered the commercial stream.

■ Another virus, disturbing in its implications, appeared in March in a program written for Macintosh computers. It seems to have originated in a Canadian software workshop, where it was being developed as an experiment. Later it made its way into a game, and a consultant visiting Canada picked up the game at a conference. The virus which was hidden in the game then infected the consultant's computer. He was working on a demonstration disk for the Aldus Corporation of Seattle, and it became infected. According to the *New York Times*, the number of customers holding the tainted product is in the "low thousands."



Fred Cohen. *The government should plan for the arrival of more insidious bugs.*

■ The Chaos Computer Club of West Germany claims it will soon trigger hidden files it planted last year in a public network maintained by the National Aeronautics and Space Administration. These vandals breached the system last year, entered computer systems based at several NASA sites in the United States, tampered with files for 5 months, and left behind at least one known Trojan horse. NASA claims to have completely closed the gaps and eliminated the bad files. Recently the French police detained the co-president of the club when he arrived in Paris to speak at a meeting on computer security.

This partial list of incidents suggests that there may be good reason to be concerned about the integrity of public networks. It also conjures up some potential nightmares for the future. Security consultants hint at the possibilities for blackmail; for sabotage of commercial rivals; for slow-moving, subtle, but devastating guerrilla warfare against data banks; ultimately, for an attack by one nation's computers on another's. The last scenario is chilling in the context of the President's plans for a Strategic Defense Initiative, for its success depends strongly on knowing that computer software will work as promised.

At present, however, the infected appear to be chiefly home users, small businesses, and particularly people who engage in adventurous transactions on the public bulletin boards. For those who feel vulnerable there are at least 16 virus detection kits available, according to Highland. Some seem designed as much for entertainment as for work. The Sophco Company of Boulder, Colorado, for example, has created a "Center for Computer Disease Control." One of its tests, a program called "Canary," chirps when healthy but dies when exposed to an infectious agent. To guard against infection, Sophco provides "Syringe," a program that can inject an antivirus virus into suspect programs and warn the operator if an infection is developing.

Highland reports that price (some of the packages cost $250 or more) is no guide to quality, and that many antiviral kits are built on faulty assumptions. They may catch one strain, but remain entirely useless for others. Electronic viruses, like the biological ones, come with many strategies and can be designed to seek out different sites in the computer.

"All of the viruses that have been detected by the public so far," Cohen says, "are so obvious that they could be detected without any mechanism." The next generation could be more sinister. In this battle, he claims, the advantage lies with the attacker. "I can prove mathematically that it's impossible to write a program that can find out in a finite amount of time whether another program is infected." He has been urging the government for 4 years to plan for the arrival of more insidious bugs, he claims, without much success.

The National Security Agency, however, does not announce its plans. But Cohen notes that "they seem more concerned now, because they've got people researching it." ■ ELIOT MARSHALL

*Published by Elsevier Science Publications, New York, NY.