News & Comment

Worm Invades Computer Networks

Berkeley and MIT led the battle to cure a 48-hour infection in the world's most sophisticated public data exchange system; no lasting damage was found

THE MAIN COMPUTER NETWORK for researchers in the United States and overseas was disrupted for 2 days last week as managers tried to kill an electronic virus injected by a graduate student on Wednesday night, 2 November. The 60,000-machine system, some experts insisted, was not infested by a true virus but by a relatively benign "worm."

Unlike a virus, which breeds by insinuating its own logic into existing programs and making them bear its offspring, a worm remains self-contained. It lives off weaknesses in the host's logic. This particular worm did nothing but reproduce madly. A flaw in its own logic, however, caused it to breed with such foolish abandon that it was quickly discovered. "I'd be embarrassed if I'd written it," says Jeffrey Schiller of the Massachusetts Institute of Technology (MIT), a virus fighter. It was "dumb," hyperactivity gave it away.

By Thursday morning, the worm was eating processing time and causing delays at nearly all major academic centers on Internet. Internet is a global system built around a core called ARPAnet, which was created for academic users by the Defense Advanced Research Projects Agency.

The worm attacked three ways: by brute-force cracking of passwords, by penetrating a "sendmail" function, and by overpacking data into a status report function known as "finger demon" or "fingerd." The latter are parts of an overall network operating program called UNIX. Once inside a system, the worm called up the "debug" mode of sendmail, which allows a remote operator to tinker with commands. Then it gave orders for self-replication. The worm also knew precisely how to overpack the memory allocation for fingerd so that the overflow would be interpreted as a command.

Many sites were forced to disconnect temporarily to isolate themselves from repeated worm invasions while they raised a barrier. Some government centers were hit as well, notably the Lawrence Livermore National Laboratory in Livermore, California, which performs both classified and unclassified research. By Friday night, most of the islands of infestation had been cleaned up, system managers were relaxing, and the network was running at nearly full bore. As far as is known, no classified systems were invaded, no data erased, and no files altered.

After an around-the-clock battle lasting 2 days, exhausted computer wizards reflected on the events. They voiced dismay at the lost time but spoke with grudging respect of the cleverness of the attack. "This has never been done before," says Keith Bostic, a programmer at the Computer Systems Research Group at the University of California at Berkeley. He signed the first notice on the network on how to combat the worm. It went out at 3 a.m. PST on Thursday. The fight was exhilarating, and Bostic allows that, in a sense, "This guy did us a favor" by providing an unparalleled education in how to defend a computer network.

Peter Yee of NASA put out a warning: "We are currently under attack from an Internet virus."

Within hours after the worm's appearance, someone called the *New York Times* to report that his friend was its creator. Later, the *Times* identified the creator as Robert T. Morris, Jr., the 23-year-old son of the chief scientist at the National Computer Security Center. The center develops security systems for the nation's top-secret code-breaking office, the National Security Agency.

Neither the elder or younger Morris has acknowledged responsibility for the worm. But officials at Cornell University, where the son is a graduate student in computer sciences, said they found suspicious files in the son's computer account, including a list of passwords nearly identical to those used by the worm as it tried to break into networks. Much of Morris's file is encrypted, however, and the university has not deciphered it all. One feature of the worm that may come to haunt the creator is that it uses the Data Encryption Standard (DES)—a public but sensitive encoding system—to crack passwords. Because the worm went overseas over the network, it may have violated a rule against exporting DES.

The Federal Bureau of Investigation and other security offices are working on the case, and computer security experts from all over the country are planning to meet in Washington, D.C., to discuss the incident in mid-November.

According to Bostic and others who coordinated the national response, the worm appeared first in Pennsylvania at around 6 p.m. EST on Wednesday. It bounced around quietly for a time and then began to breed rapidly on the West Coast. One reason it exploded in California, suggests Russell Brand of the Livermore Computer Center, is that it infected BARnet or Bay Area Research Network, the nation's most sophisticated and fastest. BARnet is part of Internet.

Bostic says the worm "hit our system at about 8 p.m. and we started getting serious about it at 10 p.m." By 3 a.m. on Thursday he had put out over the network the first of several recommended fixes. "We were very fortunate," Bostic adds. "We had a UNIX workshop going on here with an incredible collection of talent on hand." UNIX was created at AT&T's Bell Laboratories nearly a decade ago, but most centers now use a modified version distributed by Berkeley known as BSD 4.3. The program is used chiefly on VAX computers. In addition, the worm was designed to invade equipment produced by Sun Microsystems. Its virulence was thus limited, and it could not have infected secret military systems because they use different logic. Researchers at Bell Laboratories boasted that their machines had remained entirely clean throughout the crisis; they do not use the weak elements of BSD 4.3.

Brand says he detected the worm at the Livermore Lab at about 10:30 p.m. on Wednesday. "I was working on one of the machines and noticed that over a small number of minutes it became about 1000 times slower than it should have been." He knew something was wrong. In tracing the job then on the computer back to its source, he electronically "met" people at Berkeley who were grappling with the worm.

At about the same time, Peter Yee of the National Aeronautics and Space Administration's Ames Research Center, also near

San Francisco, put a warning on the network: "We are currently under attack from an Internet virus. It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames. . . . " He gave a preliminary description of its modus operandi, suggesting that "the only help" for the moment was to turn off the vulnerable services.

At Berkeley, "We felt guilty," says Bostic, because the worm was feeding on a couple of 5-year-old weaknesses in Berkeley's version of UNIX. The Berkeley team consulted with the visiting UNIX experts and summoned a computer whiz from the South Bay area for special help in decompiling the worm. As distributor of the UNIX software, Berkeley posted the official remedies, but Bostic says help came in from all over the country. He gives special credit to Jeffrey Schiller and Mark Eichin at MIT, who also decompiled the worm, and to Eugene Spafford at Purdue, who served as the central post office during the crisis.

On Thursday, Berkeley researchers discovered that deep in the worm's logic was a mysterious code linking it to a Berkeley computer called "Ernie," a popular hub in the network. Every time a worm child broke into a new computer, its code required it to send a message back to Ernie, as though Ernie was keeping track. "When we saw that," Bostic says, "We got very nervous. . . . We staked out Ernie like no tomorrow"—unobtrusively monitoring the machine's every move.

The same day, MIT researchers trapped a worm in an isolated network in Boston and dissected it. "We all had pet worms after a while," Bostic says. When the people at MIT saw Ernie's address, they delicately questioned their colleagues at Berkeley. For a time there were rumors that either a Berkeley or an MIT grad student was responsible. Everyone was relieved when the *Times* on Saturday blamed a Cornell student.

The Ernie puzzle remains unsolved, however. The surveillance at Berkeley was of no use, as it turned out, because the instructions in the worm may have been badly written. Ernie never received a message.

James Bruce, vice president for information systems at MIT, says that 200 out of the 2000 machines at his university were infected. So were machines at nearly every big university in the East. Using the MIT ratio, he figures that perhaps 6000 computers worldwide got the worm. The problem is well under control now, although 4 days after the attack Bostic said, "I just stomped on another one this morning."

Postmortems have just begun. One of the questions security experts will be asking is: How bad might it have been if the worm had not been benign? ■ ELIOT MARSHALL

NIH Delays Gene Transfer Experiment

NIH director James Wyngaarden postpones approval pending review of withheld data but asks committee to act quickly

BY A VOTE of 16 to 5, the Recombinant DNA Advisory Committee (RAC) of the National Institutes of Health said yes to a proposal for a precedent-setting experiment in gene transfer in human beings.

However, for reasons of politics and process, NIH director James B. Wyngaarden has decided to reject the RAC's advice in the hope that further review of the experimental protocol and the data that back it up will enable at least some of the five who voted no to change their minds.

Just last week the gene transfer proposal got a unanimous endorsement vote when the NIH's own Institutional Biosafety Committee met to review the data. Wyngaarden made it a point to be there himself.

No one seriously argues that the proposed experiment is particularly risky, genetically speaking. In fact, it is important to note that the experiment has little to do with gene *therapy*; rather it involves adding a marker gene to anticancer cells. As one scientific observer noted, "We add markers all the time." Initially there was a debate about whether it was appropriate to refer the proposed experiment to the RAC at all.

But the political sensitivity surrounding any human research that has to do with transferring genes is high. A full-dress review was judged the responsible thing to do. And for this reason, Wyngaarden wants the approval process to be impeccable.

Several months ago, Steven A. Rosenberg and R. Michael Blaese of the cancer institute, and W. French Anderson of the heart institute, began the lengthy process of seeking approval for a gene transfer study in people dying of cancer. First, their proposal was reviewed by the institutional review boards of the cancer and heart institutes. Then, this summer, the researchers submitted their data (most of it, anyway) to the RAC's human gene therapy subcommittee for its review prior to review by the entire RAC. That is where trouble began.

Two important pieces of data were withheld from the subcommittee during its pre-RAC review. Then, when the full RAC met, those data were presented with slides, but no hard copy was released for the committee's examination. Anderson said the critical data were withheld, in part, because of apprehension that their release at a public meeting would jeopardize subsequent publication in *Science* and *The New England Journal of Medicine* (see box). The committee was outraged. When Wyngaarden heard about the incident, he was furious. The journal editors, when later asked about their policies, declared that they would never interfere with the workings of a duly constituted government advisory body. And Anderson called the incident a regrettable case of misunderstanding. But the damage was done.

The experiment is this:

Ten desperately ill cancer patients would be the volunteer subjects in a test designed to track the course of tumor-killing white blood cells to see where they lodge in the body and how long they stay there. The plan is to use recombinant DNA technology to insert a marker gene into specially "activated" tumor infiltrating lymphocytes or TIL cells and then monitor their ability to attack and shrink massive tumors in patients who are expected to otherwise die within weeks.

Rosenberg, a pioneer in efforts to manipulate immune system cells in cancer therapy, has unpublished data (currently under review at the *New England Journal*) on 15 patients with advanced melanoma who had

Ken Heinen

James Wyngaarden: *Rejected the RAC's advice for reasons of politics and process.*