Worming into a computer's vulnerable core

Thousands of computer users last week learned a lesson in security when a sophisticated, rogue computer program infiltrated their systems, exploiting features largely meant to facilitate certain computer functions. The program, commonly termed a "virus" but more accurately described in computer jargon as a "worm," invaded more than 6,000 computers linked by ARPANET and other data communications networks, disrupting computer operations at numerous universities and research centers.

The worm program was apparently concocted by Robert T. Morris Jr., a graduate student in computer science at Cornell University in Ithaca, N.Y. Released the night of Nov. 2, the program propagated itself rapidly using communications channels designed to permit the free flow of messages and data among researchers.

Unlike a computer virus, which usually consists of a small set of instructions that attaches itself to another program and then attempts to replicate, a worm is a self-contained computer program that enters by way of a communications channel and then generates its own commands. This particular worm, which actually consisted of a cluster of related computer programs, targeted computers that use an operating system known as Berkeley Unix 4.3.

Normally, in an electronic mail system, the sending computer opens a connection to another computer to which it wants to deliver a piece of mail, or message. Following a strict protocol, the receiving computer acknowledges the connection, approves the transfer and controls where the message goes.

The worm took advantage of a "trap door," an extra command in the protocol that provides information about how the delivery system is working and allows a user to fix any problems. The command also happens to turn off the automatic check that ensures a message is delivered to the right place.

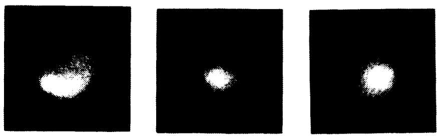
That loophole allowed the infiltrator to send a short message directly to a program called a command interpreter instead of to a "mailbox," where the message would be stored. The message, in turn, contained just enough instructions to direct the command interpreter to open a new network connection back to the invading computer, which would then pass on the other programs in the package. The command interpreter treated these programs in the same way it would handle a legitimate program, proceeding to execute the given instructions.

Those instructions were designed to rummage through the infected computer's files in search of addresses of other likely targets for infiltration. "It was actually quite smart about how it looked for such places," says Daniel Nydick, a research systems programmer at Carnegie Mellon University in Pittsburgh. For example, instead of checking the computer's lengthy main directory, it looked specifically for mail-forwarding information, going after computers on that list, or for special files listing trusted users who didn't have to use passwords. The worm could use the computer's ability to connect with a foreign machine without a password as a means of spreading the infection faster than by using the mail system. The worm included several other strategies for identifying potentially vulnerable targets and for invading other computers.

What made the infestation noticeable was that infected computers could become infected again and again, essentially slowing and clogging the computers. "We were warned that there was something going on when people noticed their machines were getting very slow and seemed to be very busy for no particular reason," Nydick says. "The machines that were hardest hit were those that were favorite places to send mail. It was very much like an automated chain letter."

The simple cure was to disconnect an infected computer from the network, shut it down and then start it up again. Because the worm was never stored permanently in a computer's memory, turning off the machine erased the invader. And because the invading program made no changes in any computer files, the computer could resume its usual operations as if nothing had happened. Programmers also had to modify the electronic mail program and the Berkeley Unix 4.3's other affected features to thwart future attacks, enabling network links to be made again. *– I. Peterson*

High expectations for Voyager 2 at Neptune


Hammel/JPL

A cloud circling Neptune, seen from Earth. What will Voyager 2 see close up?

Scientists last week reported findings with exciting implications for the Voyager 2 spacecraft's flight past Neptune next August. Though the probe's photos so far show little more than a fuzzy ball, measurements from Earth suggest Neptune has a dynamic atmosphere with details that will not be hidden by haze, and a magnetic field that might produce auroras, radiation belts and more.

"When I showed them the 6,190-angstrom images, everyone started to applaud," says Heidi B. Hammel of Jet Propulsion Laboratory in Pasadena, Calif., describing the response of members of Voyager 2's camera team. Yet the photos had been taken not from space but through the University of Hawaii's 2.24-meter telescope on Mauna Kea. The object of the excitement was a diffuse bright spot on several of the pictures – a large, cloudy feature high in the Neptunian atmosphere. The feature's detectability from Earth suggests that finer details should appear in Voyager's closeups.

The pictures, presented last week in Austin, Tex., at the meeting of the American Astronomical Society's Division for Planetary Sciences, were taken at a wavelength of 6,190 angstroms to seek brightness variations in Neptune's methane atmosphere. They excited Voyager scientists because the spacecraft has a filter to take photos at that wavelength.

Scientists can track a cloud such as Hammel photographed as it circles the planet, gaining a clue to the length of Neptune's day. A similar cloud seen in 1986 and 1987 was farther south and circling more slowly, indicating that the winds at different latitudes move at different speeds, creating wind shear that may drive a host of other visible circulation features. By comparison, Uranus – Voyager 2's previous target – kept its atmospheric details masked by haze until the spacecraft was just five days away, and even then, details appeared in images only after much computer processing.

Also reported at the meeting were measurements of Neptune's radio emissions, which Imke de Pater of the University of California, Berkeley, says provide strong evidence the planet has a magnetic field. Detected by the antennas of the Very Large Array in Socorro, N.M., the emissions proved powerful enough at a wavelength of 20 centimeters to suggest they were produced by electrons from the solar wind, trapped on the lines of a field whose strength is about 1 gauss – less than a fourth Jupiter's strength but about twice as strong as Earth's.

Such a field could mean Voyager 2 will encounter diverse electromagnetic phenomena ranging from auroras to trapped radiation akin to Earth's Van Allen belts.

Also intriguing are Neptune's possible rings, which scientists believe to be short arcs rather than whole rings because of the way they block the light of stars that pass behind them. The rings' positions are not precisely known, but several stellar occultations are expected before Voyager 2 flies past Neptune, and mission officials have readied new computer commands that can be radioed to the craft to re-aim its cameras in hopes of taking pictures of the rings as the stars pass behind the planet. *– J. Eberhart*