Alex Pendell

*Sendmail* is the program that proves SMTP mail service for computers connected on a TCP network across Berkley UNIX systems. A feature of *sendmail* is that instead of mailing directly to a mailbox, one could send mail to be delivered to processes. So if *sendmail* is compiled with a DEBUG flag set, it allows the sender to enter a command instead of the username of the recipient. The worm sends mail with /dev/null/ as the sender, and then continues with a String that bypasses the body of the email into the area where commands can be read. A copy of the worm is then compiled, and the computer is now infected.

The stack:

x/x $rdb:

0x20

0x50

0xb0

0xe0

0x10

0x40