Internet virus of November 1998

- Reported in all the media
- Infected many, many sites
- Infected only Unix machines
- Infected only VAX and Sun3
- Virus or worm?

methods of infection

- mail
  - sendmail program has a DEBUG mode
- remote shell
  - Connect via rsh to a *trusting* system
- finger
  - Overflow finger server's buffer and changes its behavior *radically*
- remote execution (with passwords)
  - Use *discovered* user passwords to break into new machines via rexec

cost of the worm

- Network disconnection
  - Loss of service (mail)
- Time of system administrators
- End of the age of innocence
- Robert T. Morris, Jr.
- Robert T. Morris, Sr.
- Continuing (smaller) look-alike attacks
- **No file damage**

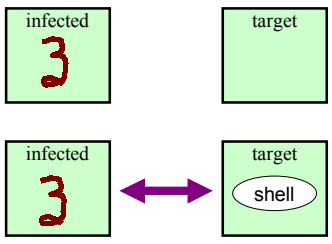
the SENDMAIL attack

- sendmail (the SMTP daemon of Unix) accepts connections of TCP port 25
- Worm transmits to sendmail:

```
debug
mail from: </dev/null>
rcpt to: <"|sed -d '1 ,/^$/'d |/bin/sh; exit 0">
data
…
```

- Shell is started at the remote site executing commands send by the worm through the TPC connection.

first subgoal of the worm



the RSH attack

- Worm simply executes:

```
/usr/ucb/rsh target
/usr/bin/rsh target
/bin/rsh target
```

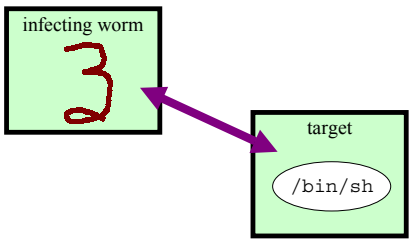
- If the infecting site is trusted by the target, that is, listed in /etc/hosts.equiv or in the .rhosts file of the worm's *user*, a shell connected to the worm will be spawned on the target machine.

the REXEC attack

- Worm gets a list of local users by reading /etc/passwd. It attempts to crack user passwords using likely guesses, such as the user's name.
- If a password is cracked, the worm attempts to connect to the rexec daemon (TCP port 512) on target machines where the user is likely to have an account. This will succeed if the same password is used at the target machine.
- Worm will use rexec to assume the identity of the owner of the cracked password on the infected machine and then pursue the rsh attack on a target machine.

first goal achieved

all else is easy



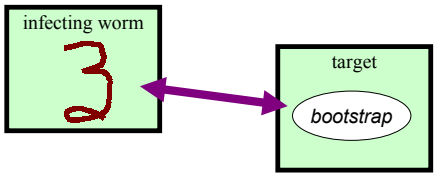
the finger attack

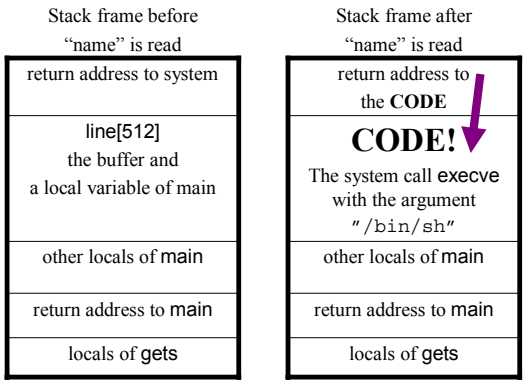
- Worm connects to the finger daemon (TCP port 79) on the target machine.
- The finger daemon expects to be sent the name of the user to be fingered. It uses the Unix library routine gets to read this name into a 512 byte butter. gets has only one argument, a pointer to the buffer.

So…

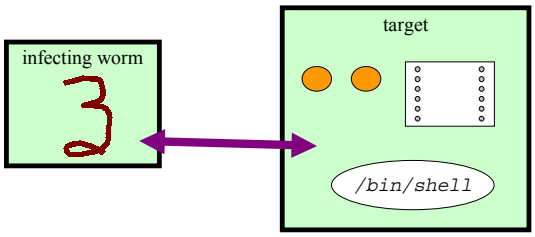
- Note: only works on VAXen.

- Worm transmits and compiles a 99-line bootstrap program.
- The bootstrap is run with the infecting worm's IP number and TCP port number as arguments.
- Bootstrap connects to the infecting worm.

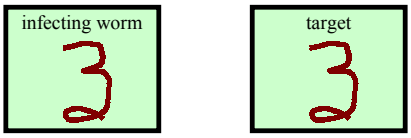




- Bootstrap receives three files:
  1) Sun 3 object for the worm;
  2) Vax object for the worm; and
  3) C code for the bootstrap.
- Bootstrap then execl's /bin/shell



- Infecting worm links, in turn, the object modules.
- The result of the link is executed with the three worm ingredients as arguments.
- If successful, a new worm is established.
- The new worms reads (and deletes) its ingredients then kills the shell.



worm population explosion

- Randomly, one of every seven worms was born immortal.
- If several worms entered machines at once, at most one can bind TCP port 23357. Others may never participate in worm-present checks.
- As system load rises, worm-to-worm communication attempts will frequently time-out.
- Consequently, the worm overwhelmed some machines in minutes and was quickly noticed.

worm procreation

- Potential sites for the next infection:
  - geteways
    `netstat -n -r`
  - local networks
    SIOCCIFCONF ioctl system call
  - equivalent hosts
    /etc/hosts.equiv
  - user-specific "equivalent" hosts
    user's .forward and .rhosts files
- Methods and sites of attack are time-shared.

worm birth control

- How can the number of worms be limited without making the worm vulnerable to *mock* worms?
  - A new worm tries to connect to local TCP port 23357. If a connection is made, the two worms exchange bytes and decide which one will *quit*.
  - Every few seconds, the non-quitter will briefly hibernate while attempting to accept connections of TCP port 23357.