CSE 543 - Computer Security

Lecture 9 - Malware
September 25, 2007
URL: http://www.cse.psu.edu/~tjaeger/cse543-f07/

The Morris Worm

- Robert Morris, a 23 doctoral student from Cornell
  - Wrote a small (99 line) program
  - November 3rd, 1988
  - Simply disabled the Internet
- How it did it
  - Reads /etc/password, they tries the obvious choices and dictionary, /usr/dict words
- Used local /etc/hosts.equiv, .rhosts, .forward to identify hosts that are related
  - Tries cracked passwords at related hosts (if necessary)
  - Uses whatever services are available to compromise other hosts
- Scanned local interfaces for network information
- Covered its tracks (set is own process name to sh, prevented accurate cores, re-forked itself)

Vulnerabilities

- Network daemon vulnerabilities
  - Buffer overflows
- Insecure programs
  - Remote logins allowed
- User errors
  - Poor passwords
- Administration errors
  - Trust in other machines (hosts.equiv)
- Network information
  - Information about next likely victims (propagation)