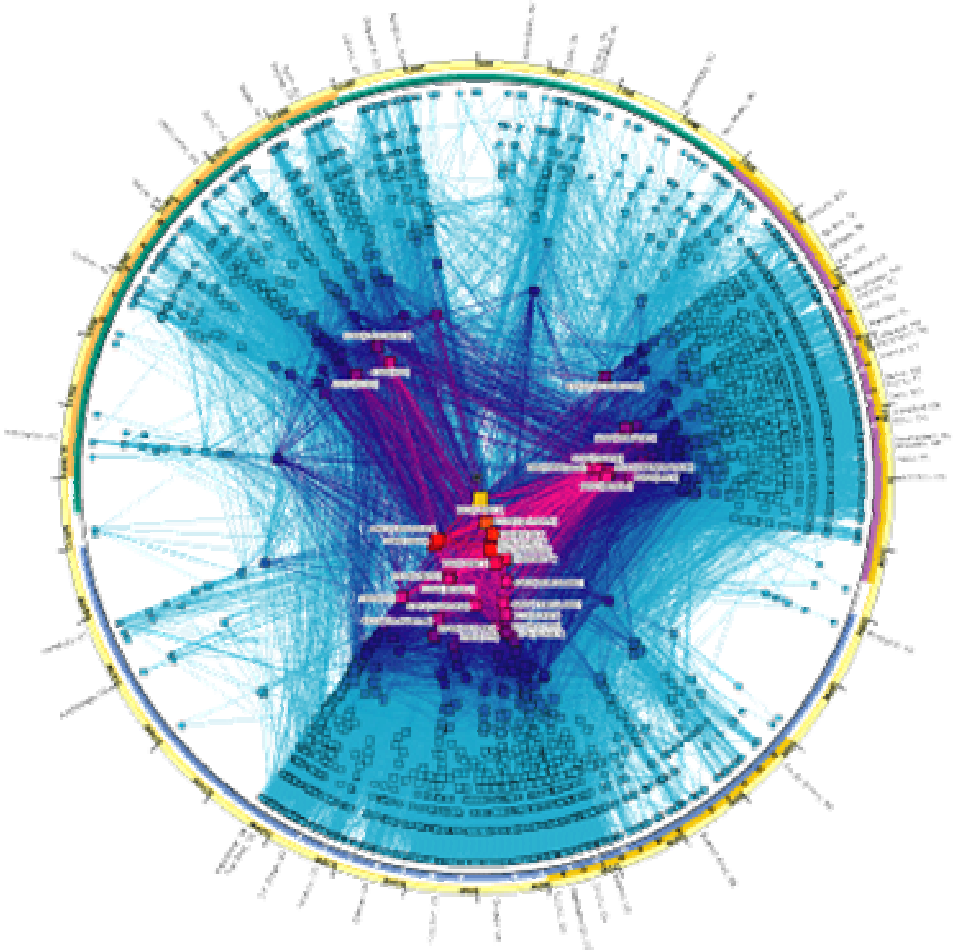
Understanding Global Internet Health



David Moore (dmoore@caida.org)

SAN DIEGO SUPERCOMPUTER CENTER

COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS

What is an Internet Worm?

worms and viruses use software flaws to infect computers

***worm*: no human interaction**

- CodeRed
- Nimda
- Sapphire/SQL Slammer

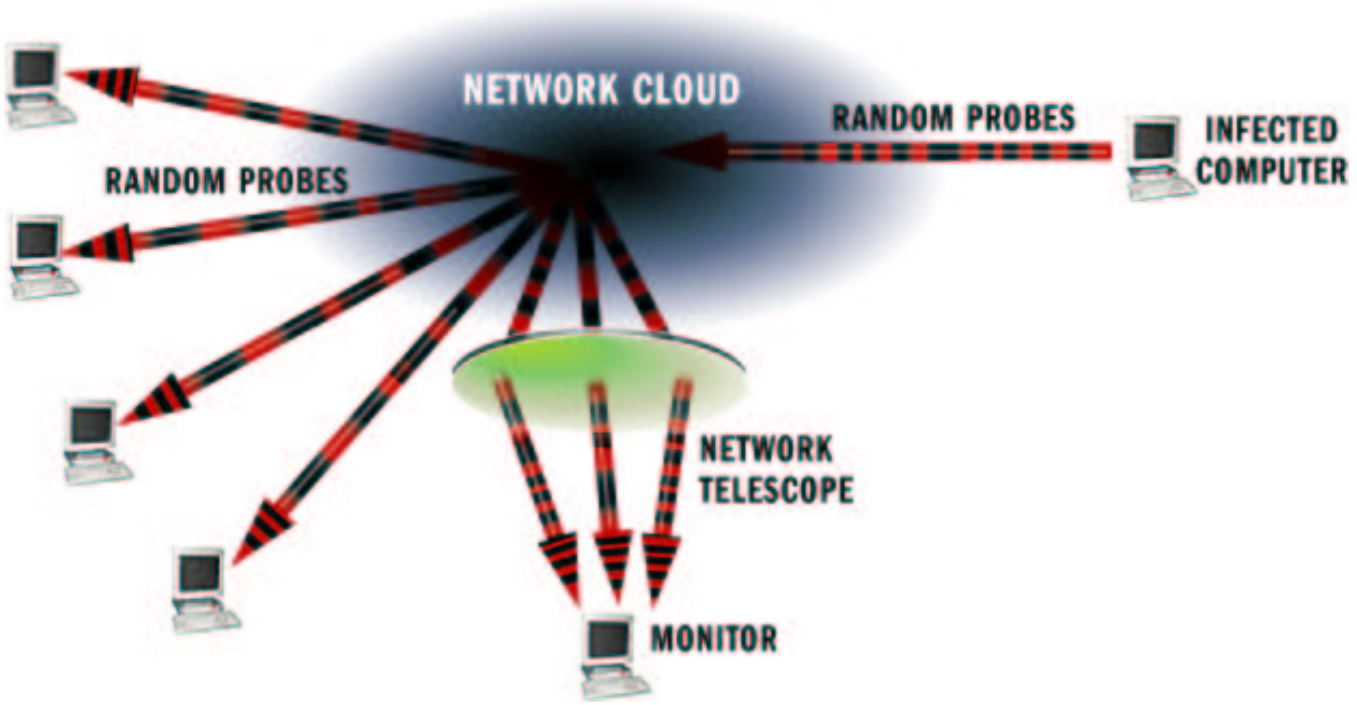
***virus*: requires human interaction**

- ILoveYou
- Melissa

Internet Addresses

- **Humans like to work with names like:**
  - www.ucop.edu www.caida.org
- **Computers like to work with numbers:**
  - 128.48.116.201 192.172.226.123
- **Over 4 billion possible IP addresses**
  - most worms use IP addresses directly to spread

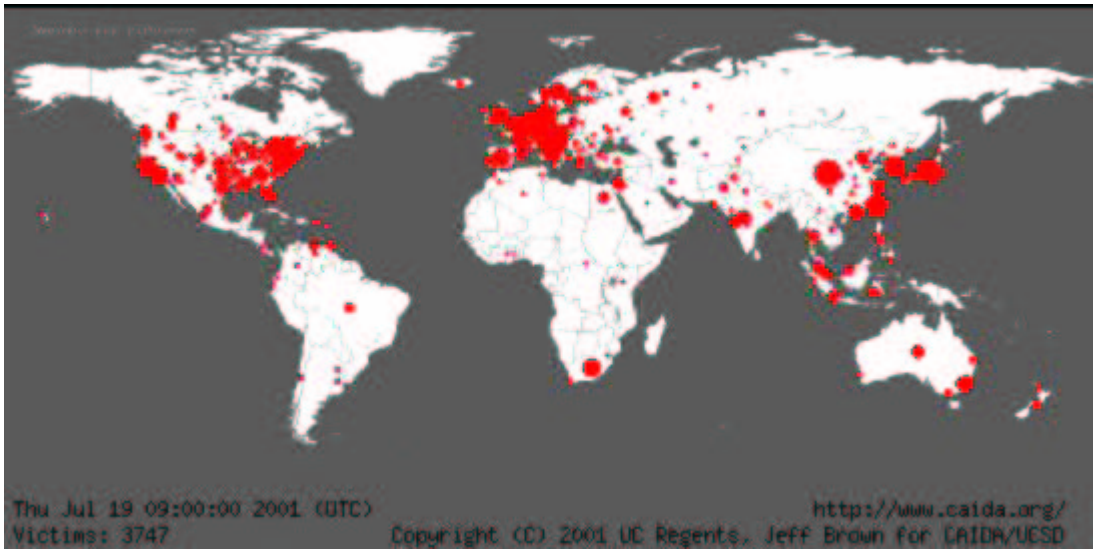
Tracking Worms with Network Telescopes



- **Recent worms spread by probing random IP addresses**
- **We monitor 16 million of all IP addresses (1/256th)**

CodeRed Worm – July, 2001

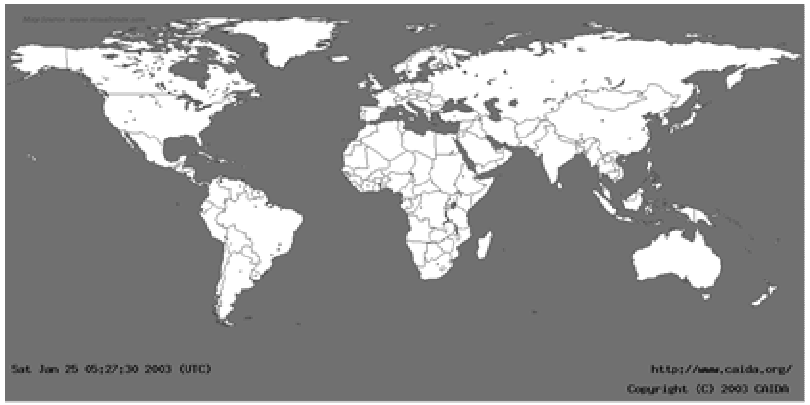
- **Over 350,000 hosts infected in 24 hour period**
- **2,000 hosts infected per minute at the peak**
- **Damage from spread rate, not inherently destructive**



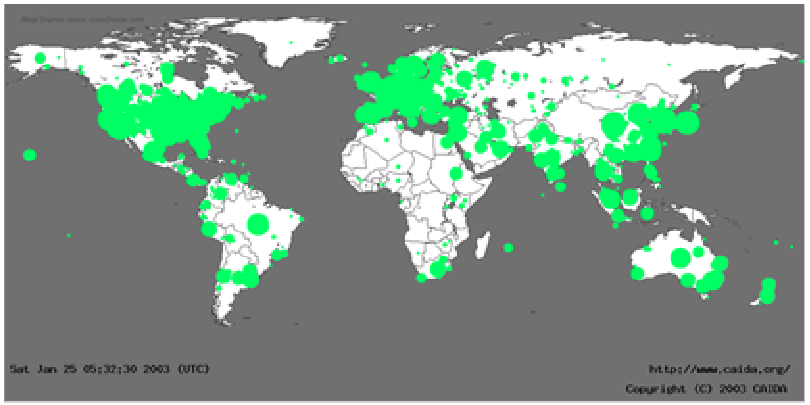
Sapphire Worm

(aka SQL Slammer) – Jan 24, 2003

- **Sent more than 55 million probes per second world wide**
- **Majority of vulnerable machines infected in under 5 min**
- **Collateral damage: Bank of America ATMs, 911 disruptions, Continental Airlines cancelled flights**
- **Clogged networks but relatively benign to hosts**



Before 9:30PM (PST)



After 9:40PM (PST)

What needs to be done

- **Proactive:**
  - Help developers produce more secure software
  - Effective, easy-to-use software updates

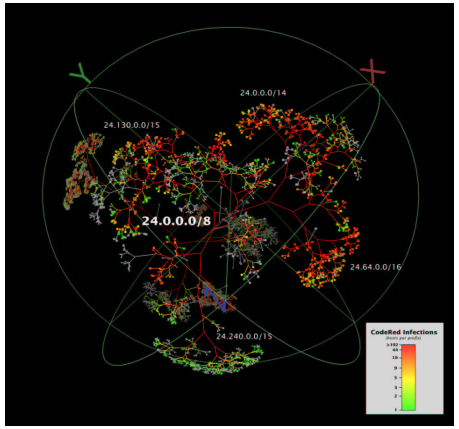
- **Reactive:**
  - Must be automated; must not be worse than the attack
  - Network Operation Center to coordinate response, cleanup

- **Support for both:**
  - Cyber CDC to track and research network attacks

The National Strategy to Secure Cyberspace

Five priorities:

- Security response system
- Threat and vulnerability reduction
- Security awareness and training
- Securing governments' cyberspace
- National and international cooperation



The University's role:

- Research rapid analysis techniques
- Form public/private partnerships
- Research design of secure systems
- Develop best practices

SDSC SAN DIEGO SUPERCOMPUTER CENTER

COOPERATIVE ASSOCIATION FOR INTERNET DATA ANALYSIS

caida