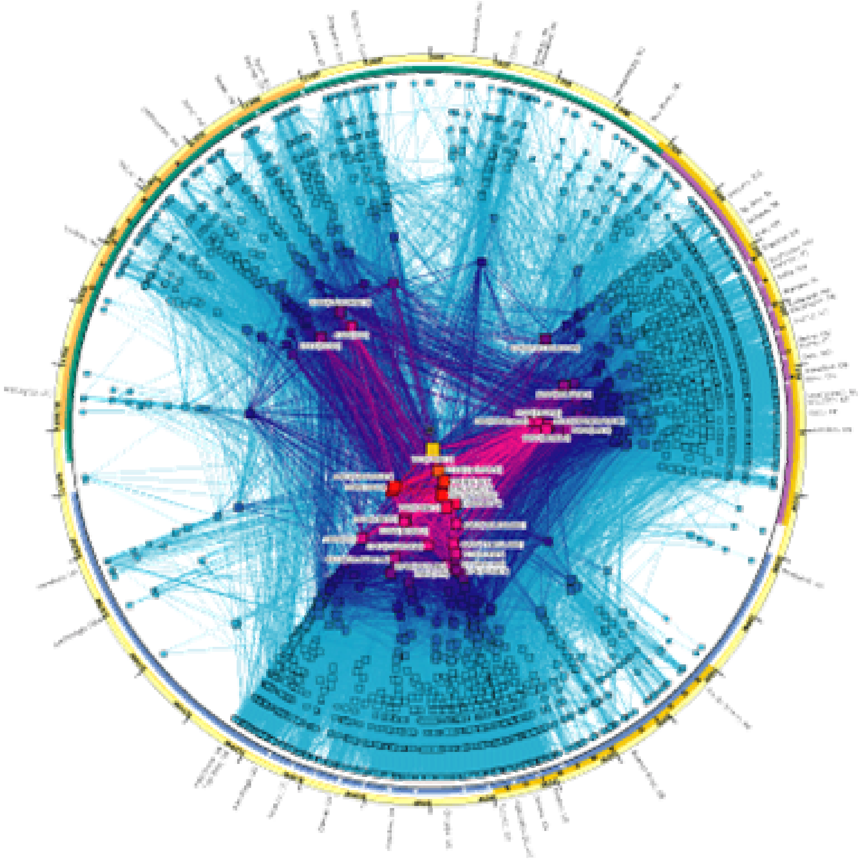
Understanding Global Internet Health



David Moore (dmoore@caida.org)

January, 2003

What CAIDA does

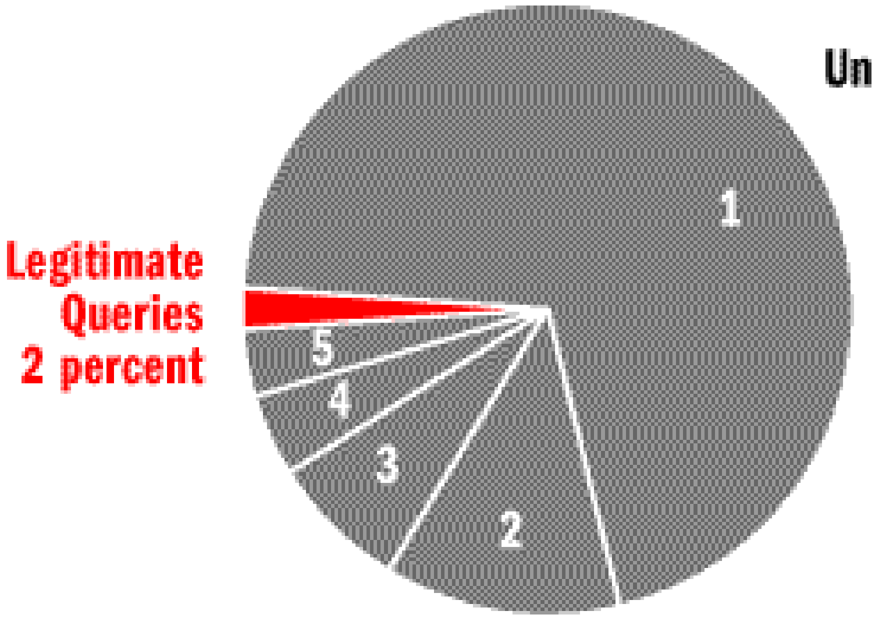
- measure and analyze the ***global*** Internet to the extent possible (macroscopic, synoptic views)
- build tools, hardware, deploy infrastructure
- visualize massive network and security datasets

Outline

- DNS Root Server Health
- Worldwide Denial-of-Service Attacks
- Code-Red Worm
- Sapphire Worm (aka Slapper, Friday’s MS-SQL worm)
- Worm Containment

DNS Root Server Health

Summary of the types of queries received on Oct. 4, 2002 by a Domain Name System (DNS) root server in California



Unnecessary Queries 98 percent

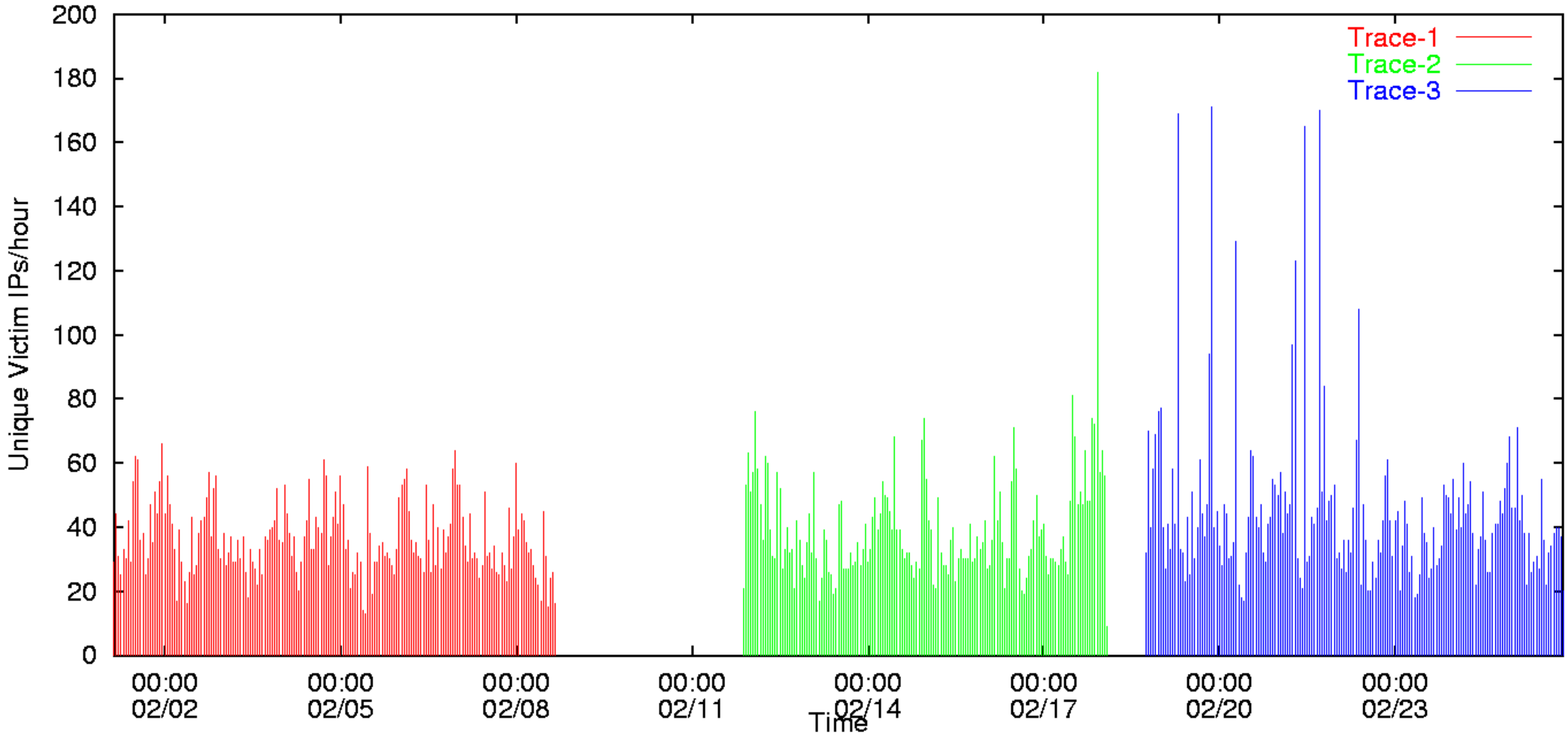
1. Repeated and identical queries* (70 percent)
2. Unknown top-level domains (13 percent)
3. Numeric IP address already in query (7 percent)
4. Referral not cached** (4 percent)
5. Other*** (4 percent)

Global Denial-of-Service Attacks

(three weeks in February 2001)

- Lots of attacks – some very large
  - **>12,000** attacks against **>5,000** targets
  - Most < **1,000** pps, but some over **600,000** pps
- Most attacks are short – some have long duration
  - a few victims were attacked continuously all weeks
- Everyone is a potential target
  - Targets not dominated by any TLD, or domain
    - Targets include large e-commerce sites, mid-sized business, ISPs, government, universities and end-users
    - Targets include routers and domain name servers

DoS Attacks over time



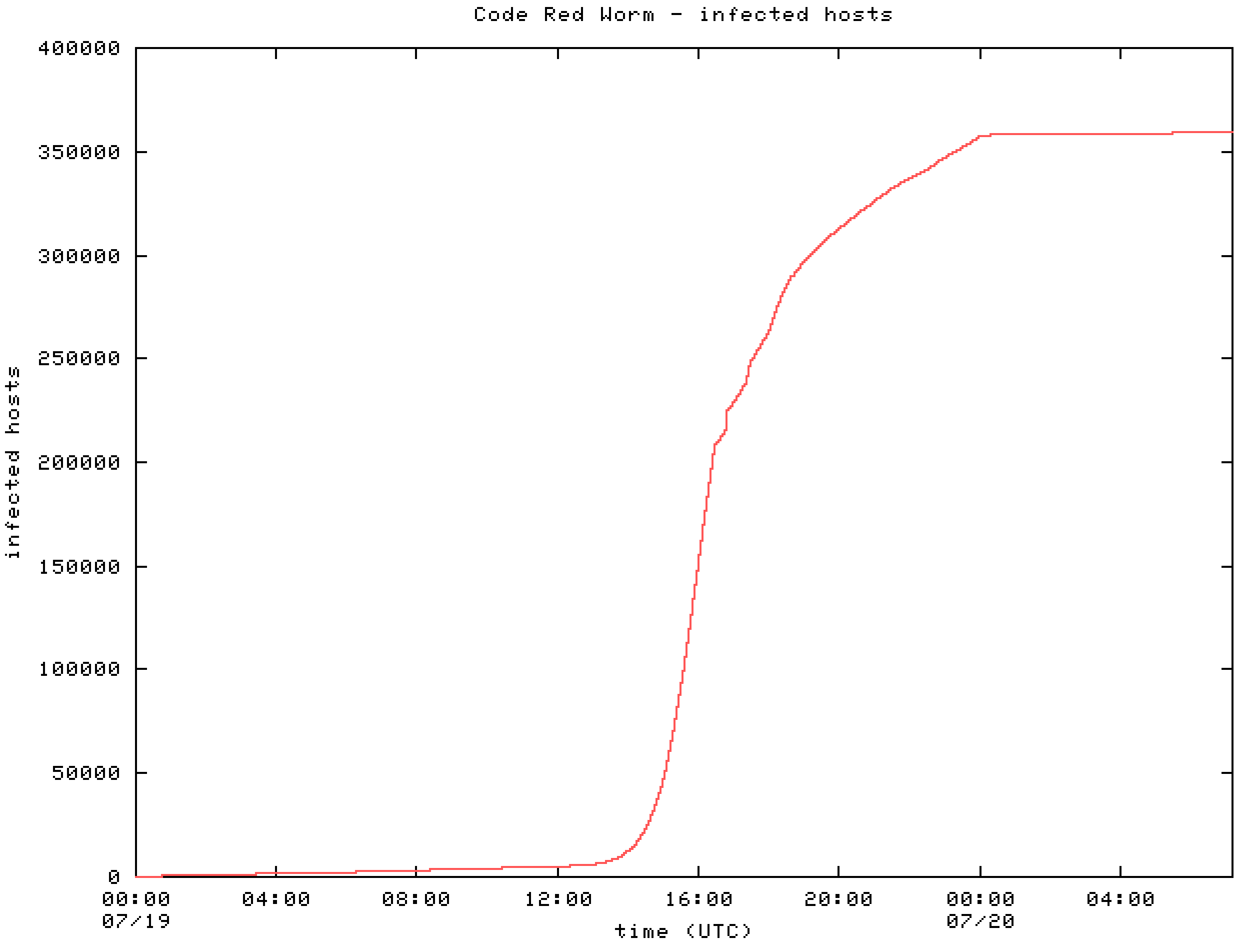
Code-Red Worm: *Background*

- July and August 2001
- Spread via Microsoft IIS web server and designed to launch DoS attack on www1.whitehouse.gov

- Measured using Network Telescope at UCSD
  - ~1 in every 256 worm probes came to our telescope

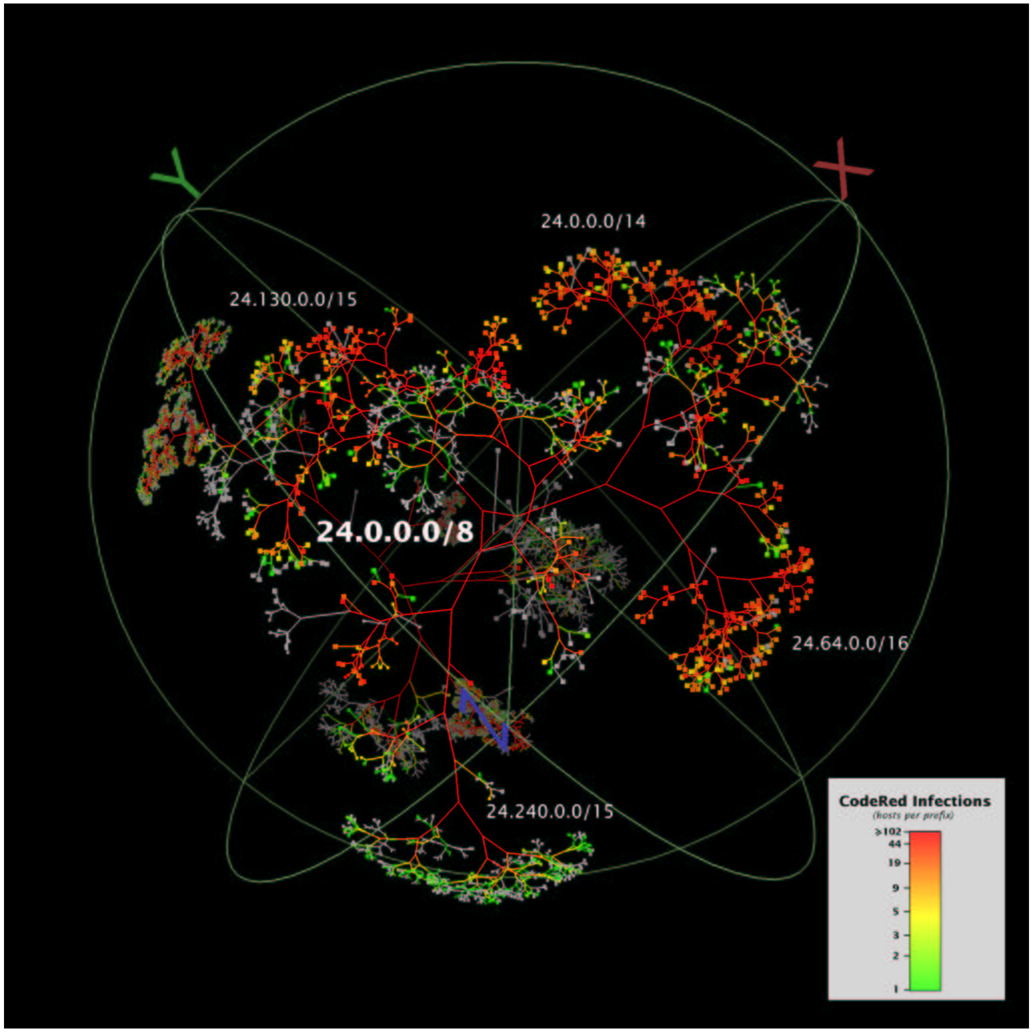
- Over 350,000 hosts infected in 24 hour period
- Between 11:00 and 16:00 UTC, the growth is exponential
- 2,000 hosts infected per minute at the peak of the infection rate (16:00 UTC)

Code-Red Worm: *Infection Rate*

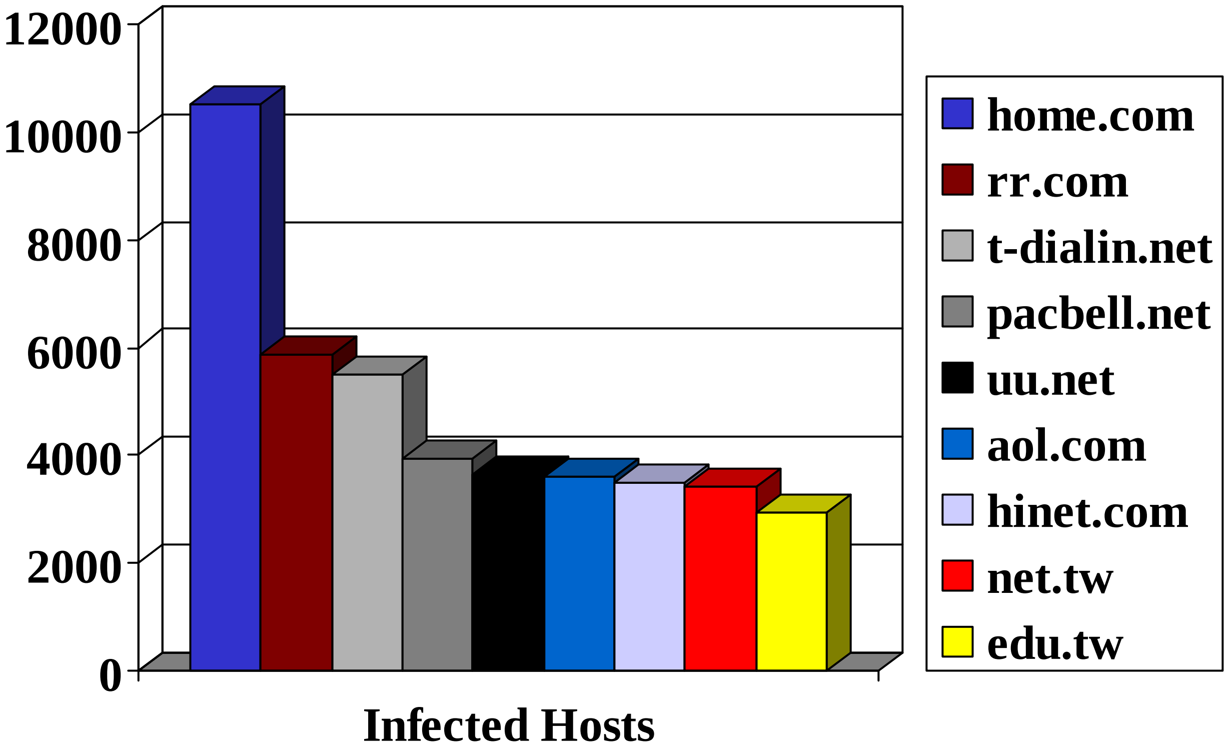


Code-Red Worm: Topology Effects

- Topological view of spread
- Some worms preferentially chose “nearby” addresses
  - e.g., CodeRedII and Nimda



Code-Red Worm: Victim Domains



- Small-business and home users were large fraction of the infected machines.

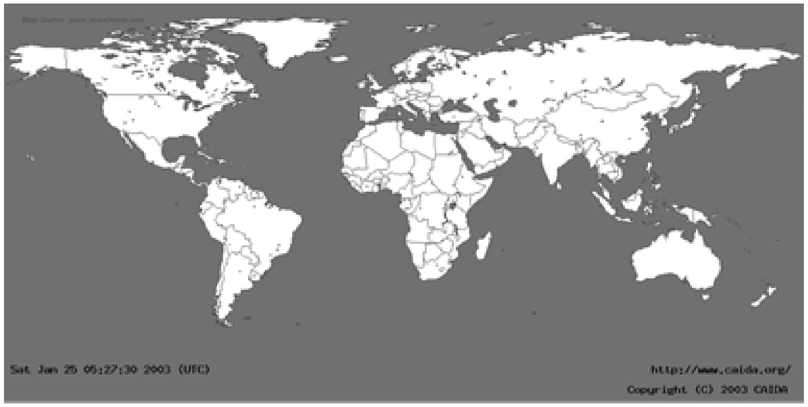
Code-Red Worm: *Geographic Spread*

🎥

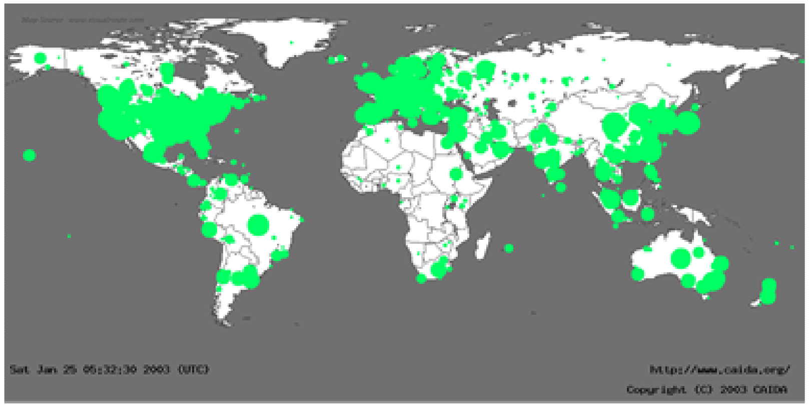
Sapphire Worm

(aka SQL Slammer)

- 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



Before 9:30PM (PST)



After 9:40PM (PST)

Worm Containment

- Code-Red: 350,000 victims in under 12 hours
- Sapphire: 60k-100k victims in a few minutes

- Sapphire probe rate was too high to be stopped by content (payload) filtering even by 100 largest ISPs, once it started.

- Proactive defenses must be used against fast worms.

Conclusions

- The US must address fundamental questions about Internet health.
  - DNS: can we reduce junk queries and only keep valid ones?
  - DoS: how can sites protect themselves? everyone?
  - Worm tracking: what techniques do hackers use to spread worms?
  - Worm containment: can we protect ourselves? everyone?

caida

Cooperative Association for Internet Data Analysis
(CAIDA)
San Diego Supercomputer Center

Dept. Computer Science & Engineering
University of California, San Diego