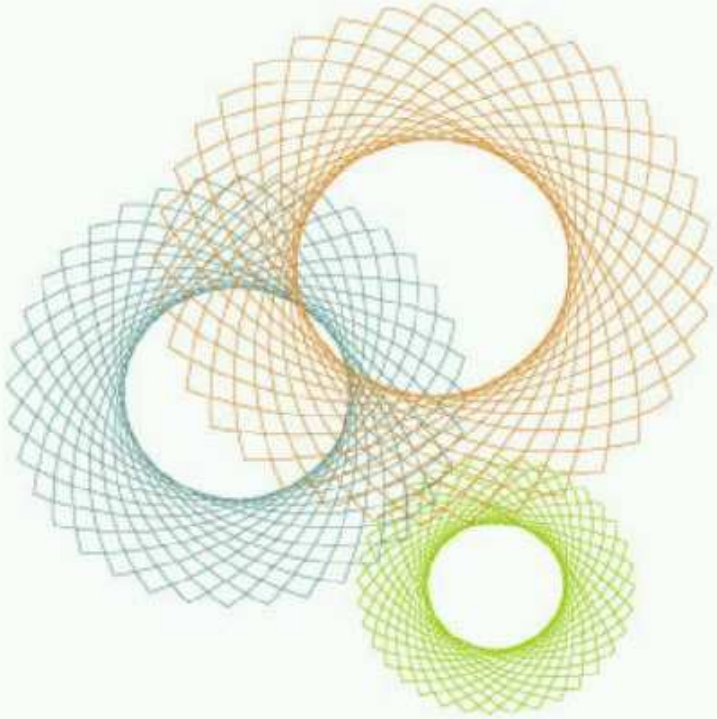
achieve peak availability

ARBOR™ NETWORKS

# Bigger and Badder: Trends in Denial of Service Attacks



Jose Nazario
<jose@arbor.net>

# Motivation

Why measure global DoS activity?

- Measure wasted bandwidth
- Observed trends

Measure what?

- Duration
- Protocol distribution
- Counts: packets, bytes
- Target distribution

# Methodology

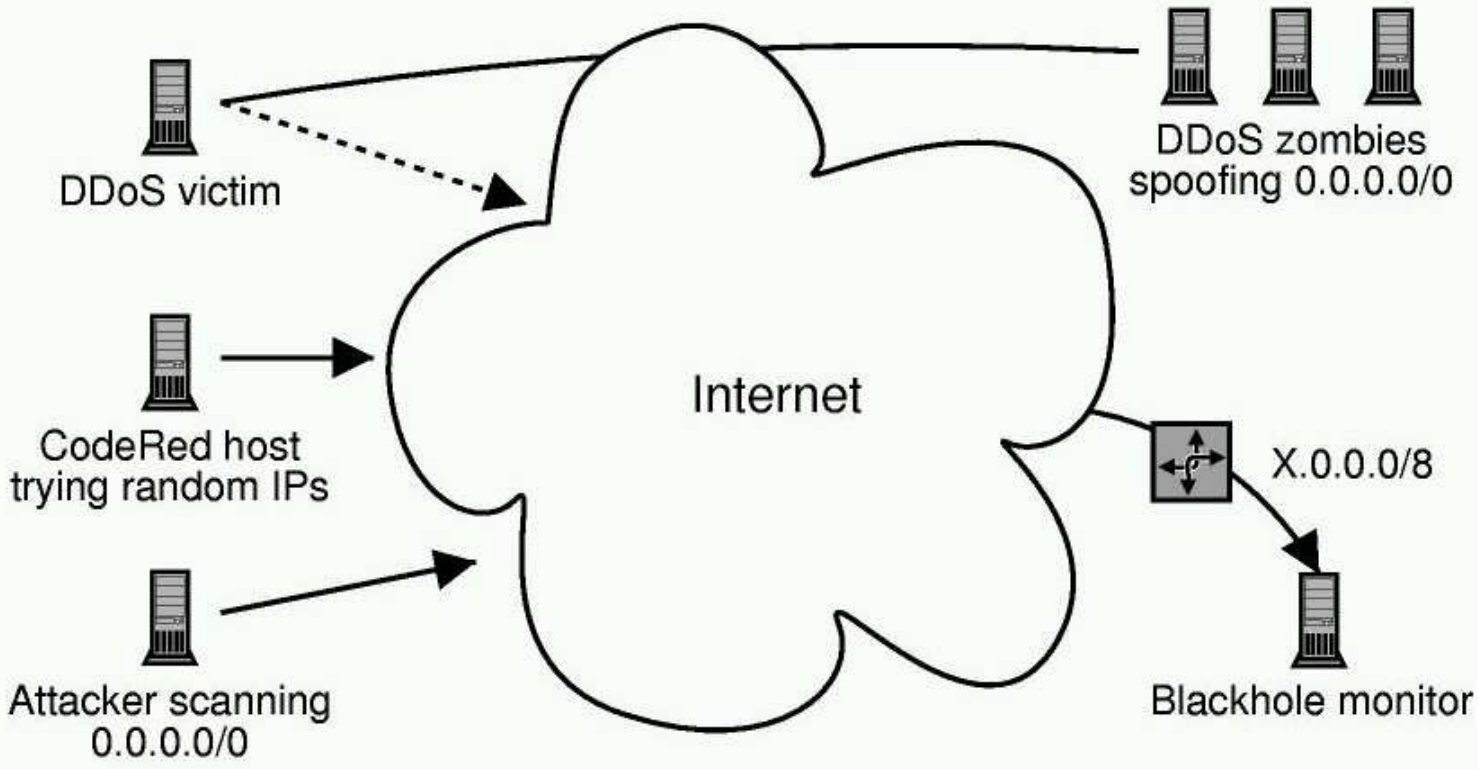
Blackhole monitoring

- Collect traffic to a globally announced, unused /8 network
  - Provided by a research partner
- Roughly 1/256 of entire Internet address space
- Collects backscatter from spoofed sources

Network monitoring

- Monitor several Tier 1, Tier 2 networks
- Sees both spoofed and not spoofed attacks

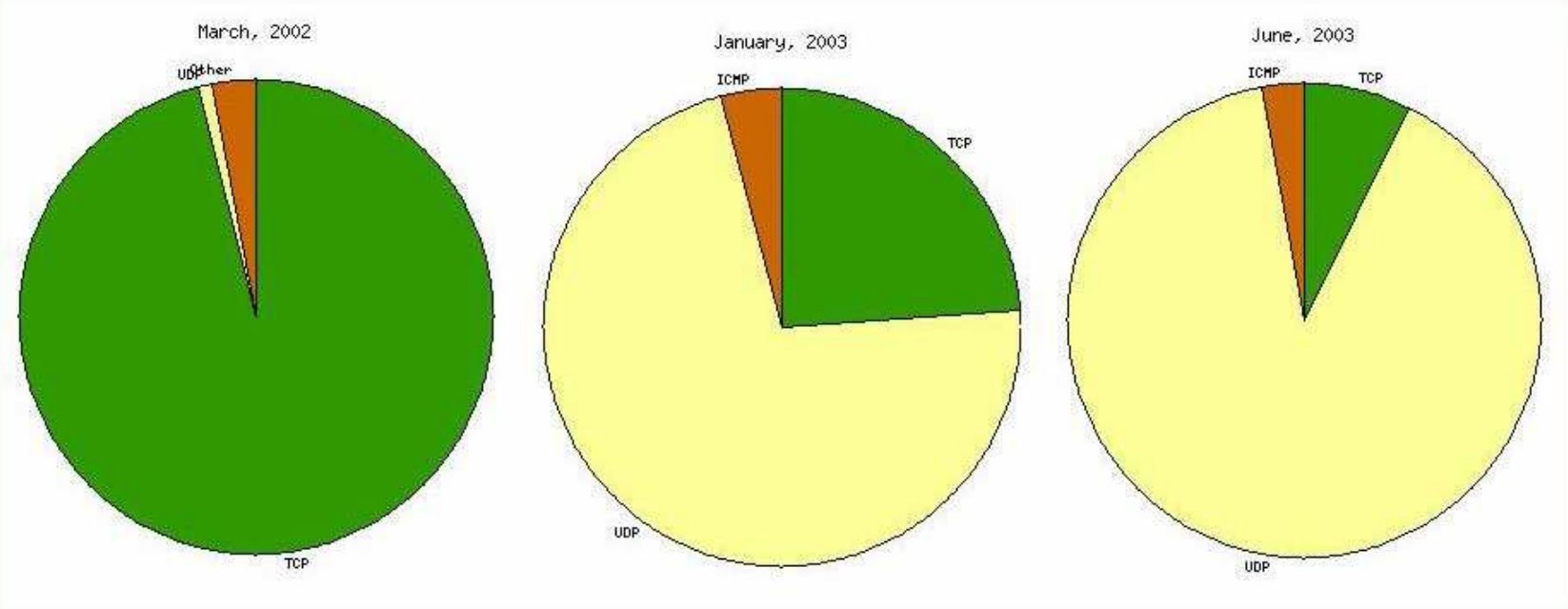
# Blackhole Architecture



# Protocol distributions

- Inverted protocol distribution
  - mid 2001: 95% TCP
  - late 2002: 75% UDP
  - current: 90% UDP
- Transition away from SYN flood to generic bandwidth attacks
  - 137/UDP, 139/UDP, 445/TCP common attack targets
  - many attacks hit random ports

# Protocol distributions (continued)



# Durations

- Most are short, but some are longer than 100 mins
- June 2003 statistics:
  - 117,000 backscatter events logged

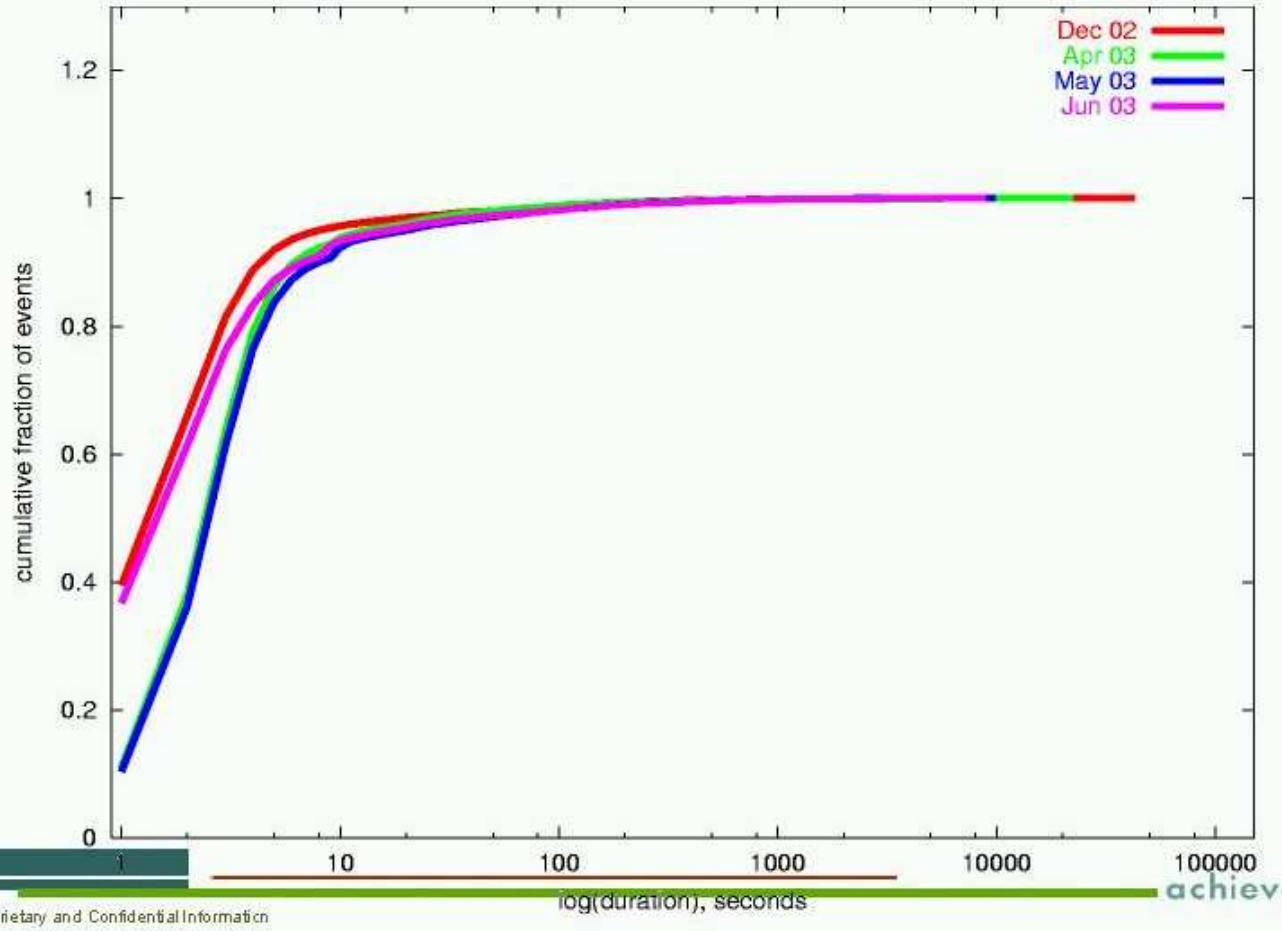
6800+ high severity

8500+ medium severity

  - 1600+ longer than 100 minutes
  - 5000+ between 10 and 100 minutes in duration

  - similar to recent months

# Durations (cont)






achieve peak availability

# Packets and Bytes

- Most are small, but several are heavy

- June 2003 statistics:
  - 500+ over 1 million packets per event
  - 2400+ over 100,000 packets per event
  - 9400+ over 100,000 bytes per event
  - 1600+ over 1 million bytes per event

  must be scaled by blackhole view (1/256)
  - 3-10 fold increase over previous months

ARBOR NETWORKS

# Target Distribution

- Targets are distributed all over the world
  - Asia-Pacific, Europe, South America, North America
- Various types of targets
  - government, network providers, universities, banks, broadband
- Most sites hit once or twice, a small handul appear commonly
  - various networks hit hundreds of times in each of the past 5 months

# Conclusions

- Cumulative effect of frequent small attacks
  - hundres of small attacks per month for top targets
  - cumulative effect of a very long lived attack
- Similar durations but larger packet and byte counts
  - individual attacks have more sources, bandwidth
  - higher packets per seconds
- What's going on?
  - rapid increase in number of tools
  - worms being ties to zombie creation - bot armies

ARBOR NETWORKS

# Acknowledgements


- Dug Song, Robert Stone, Rob Malan
- Michael Bailey, Dave Langhorst