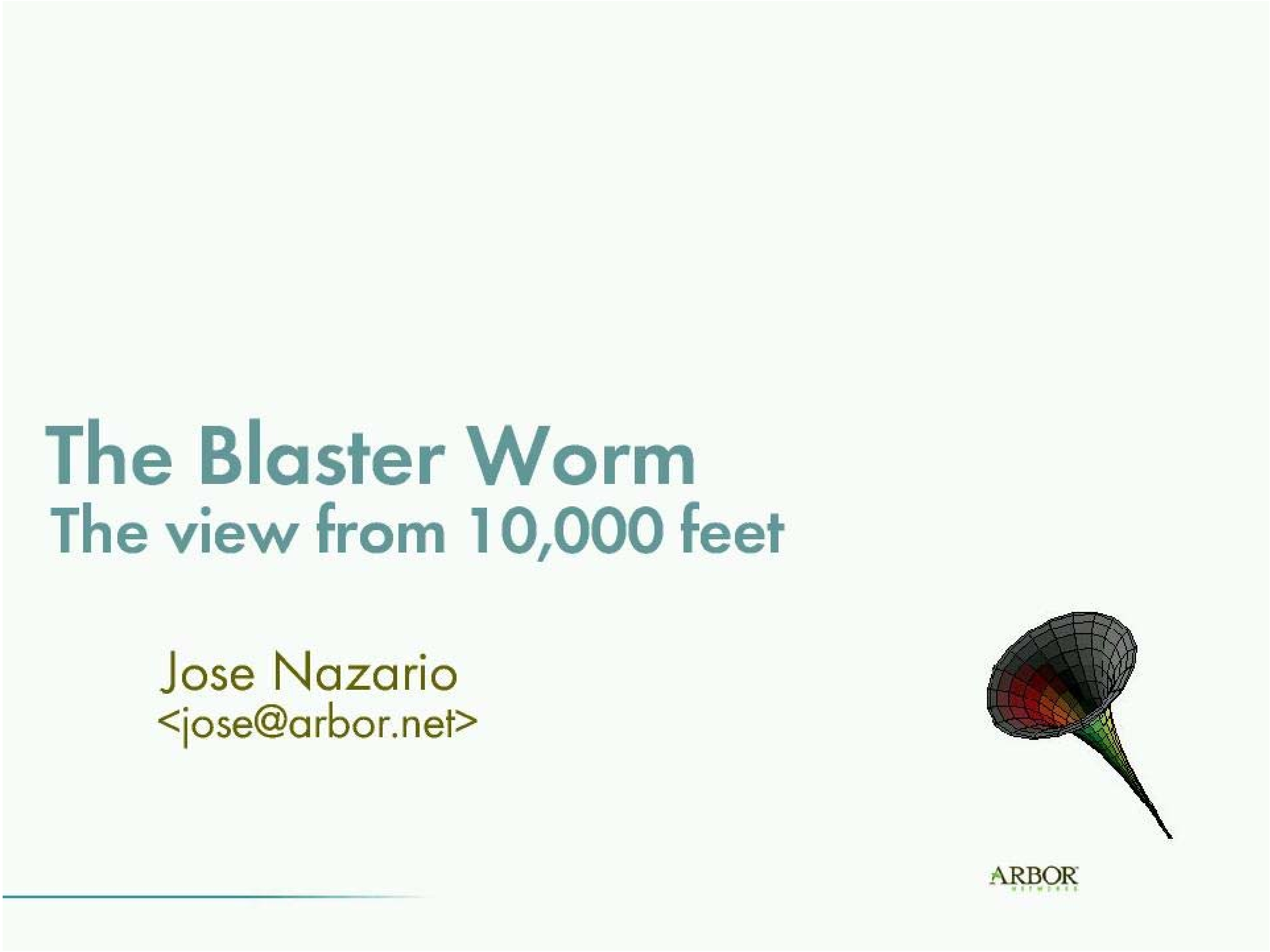
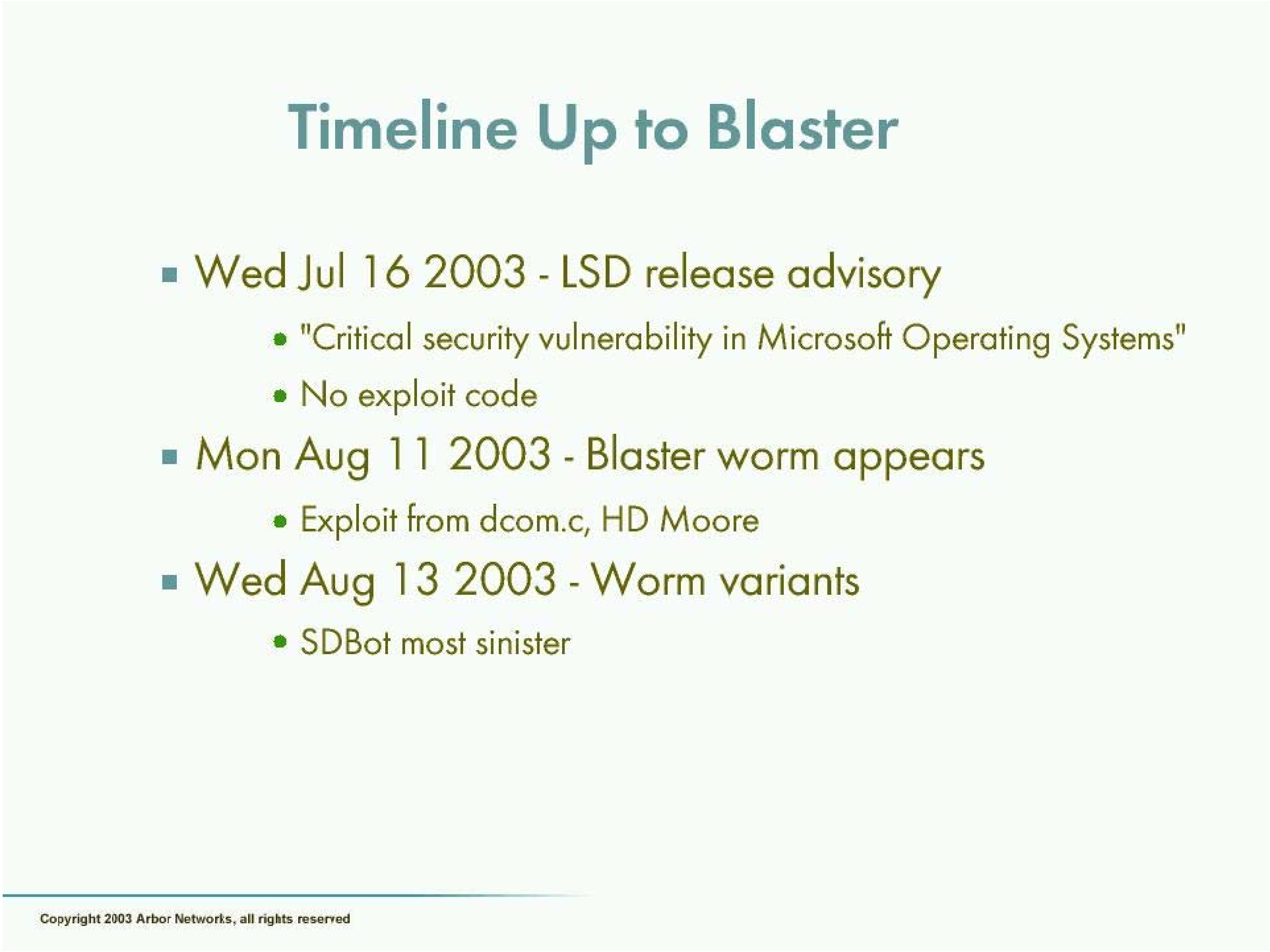


The Blaster Worm

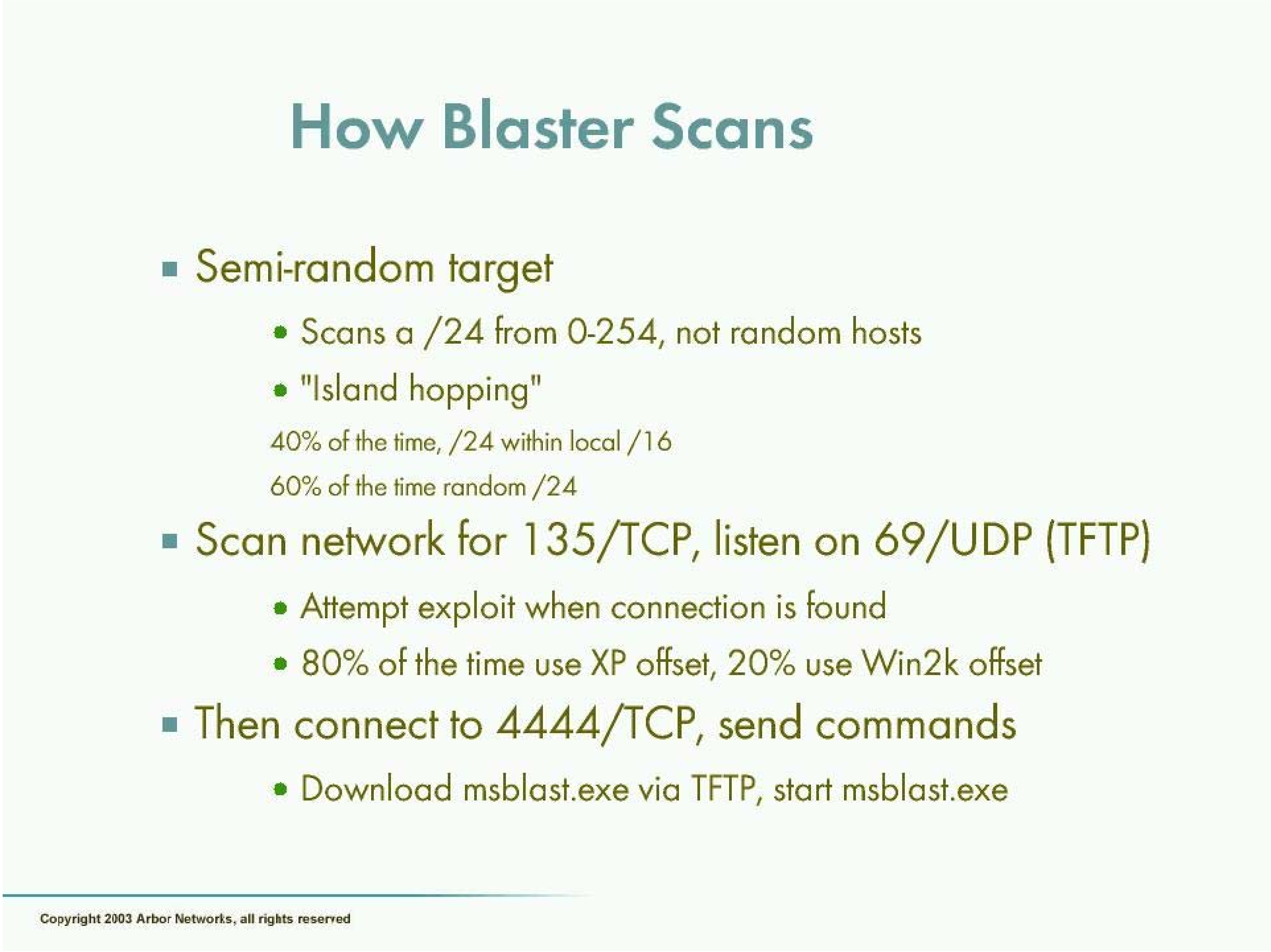
The view from 10,000 feet

Jose Nazario
<jose@arbor.net>



Timeline Up to Blaster

- Wed Jul 16 2003 - LSD release advisory
  - "Critical security vulnerability in Microsoft Operating Systems"
  - No exploit code
- Mon Aug 11 2003 - Blaster worm appears
  - Exploit from dcom.c, HD Moore
- Wed Aug 13 2003 - Worm variants
  - SDBot most sinister

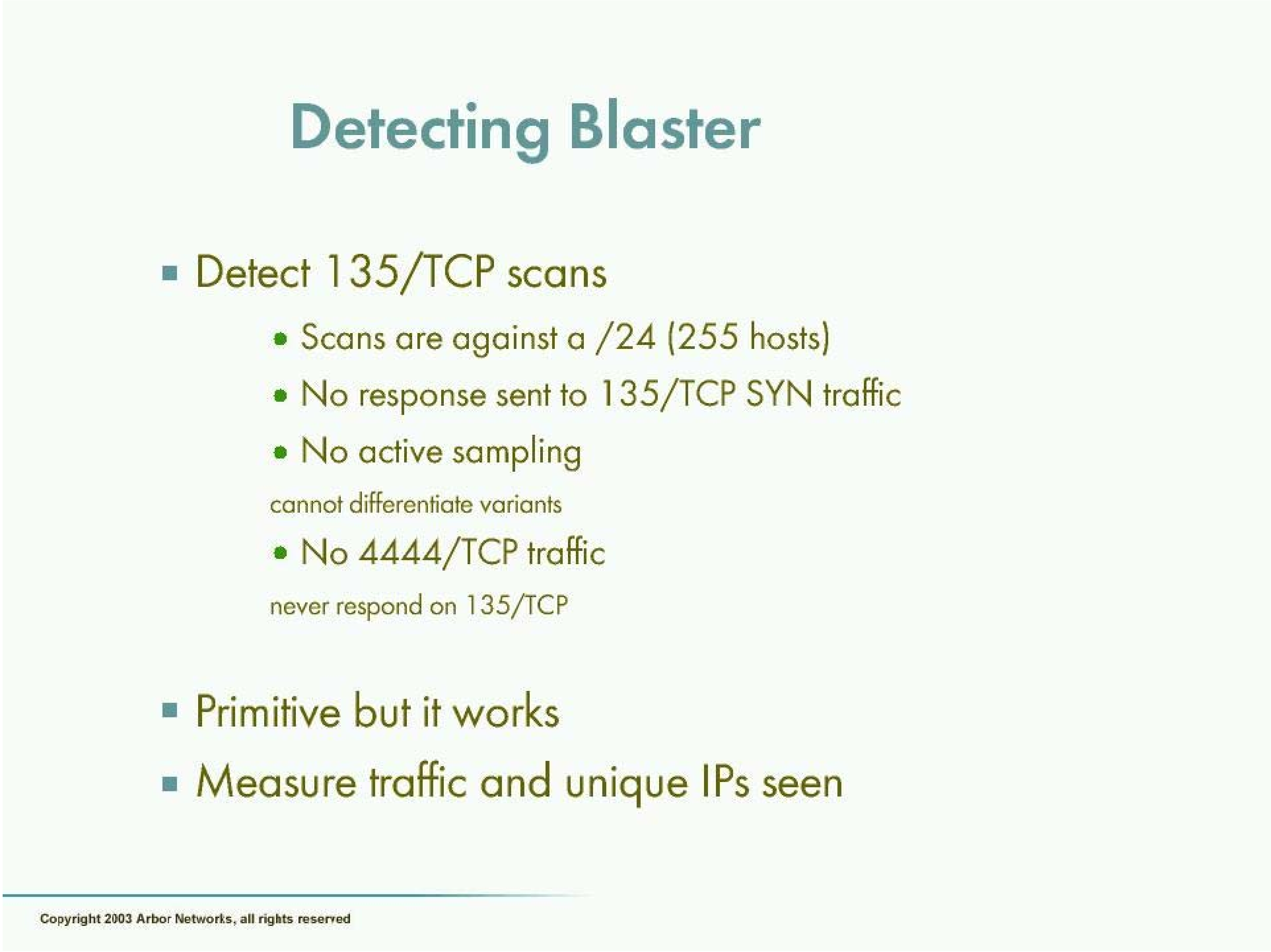


How Blaster Scans

- Semi-random target
  - Scans a /24 from 0-254, not random hosts
  - "Island hopping"

    40% of the time, /24 within local /16

    60% of the time random /24
- Scan network for 135/TCP, listen on 69/UDP (TFTP)
  - Attempt exploit when connection is found
  - 80% of the time use XP offset, 20% use Win2k offset
- Then connect to 4444/TCP, send commands
  - Download msblast.exe via TFTP, start msblast.exe



Detecting Blaster

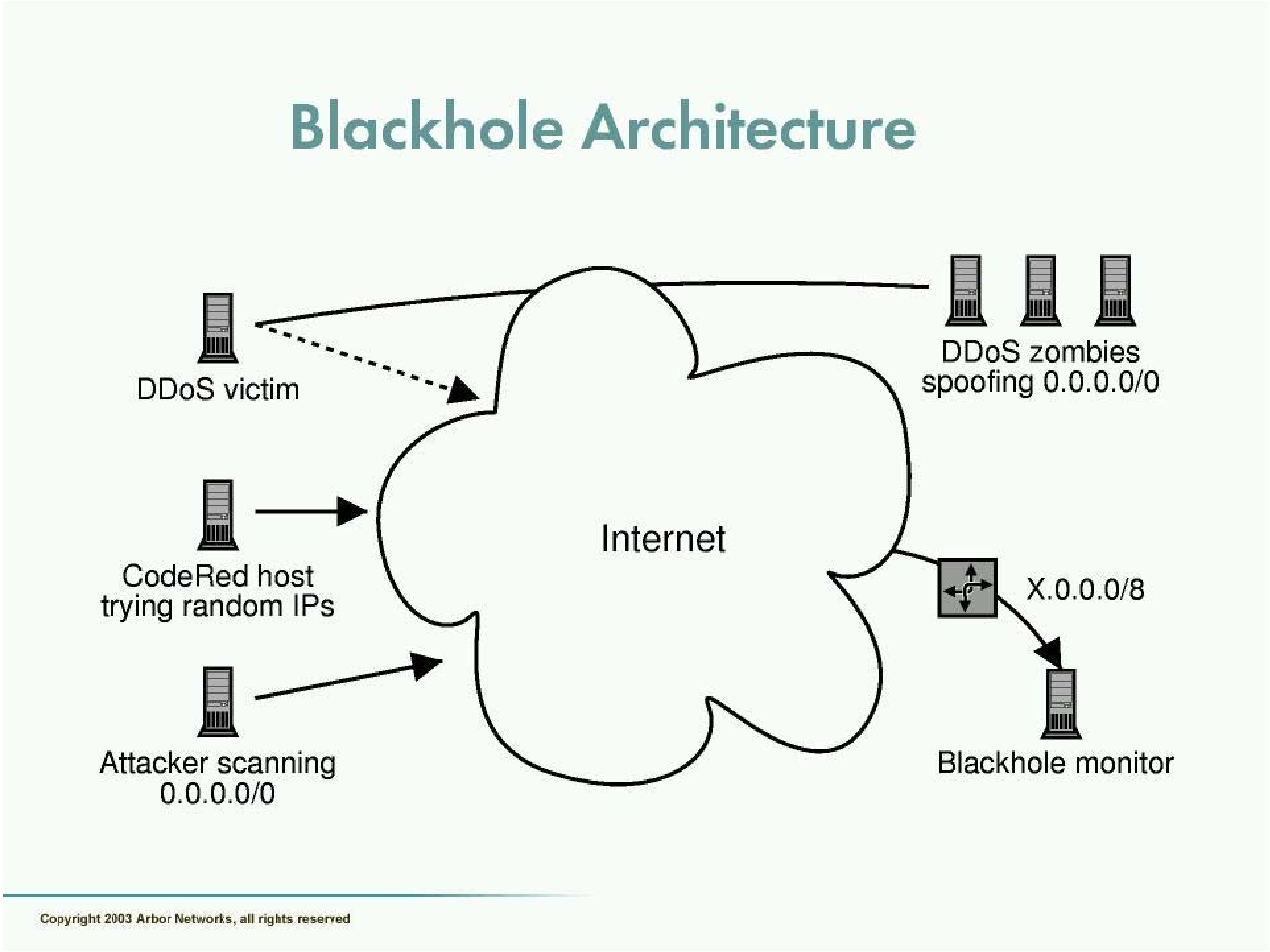
- Detect 135/TCP scans
  - Scans are against a /24 (255 hosts)
  - No response sent to 135/TCP SYN traffic
  - No active sampling

  cannot differentiate variants

  - No 4444/TCP traffic

  never respond on 135/TCP

- Primitive but it works
- Measure traffic and unique IPs seen



Blackhole Architecture

DDoS victim

CodeRed host
trying random IPs

Attacker scanning
0.0.0.0/0

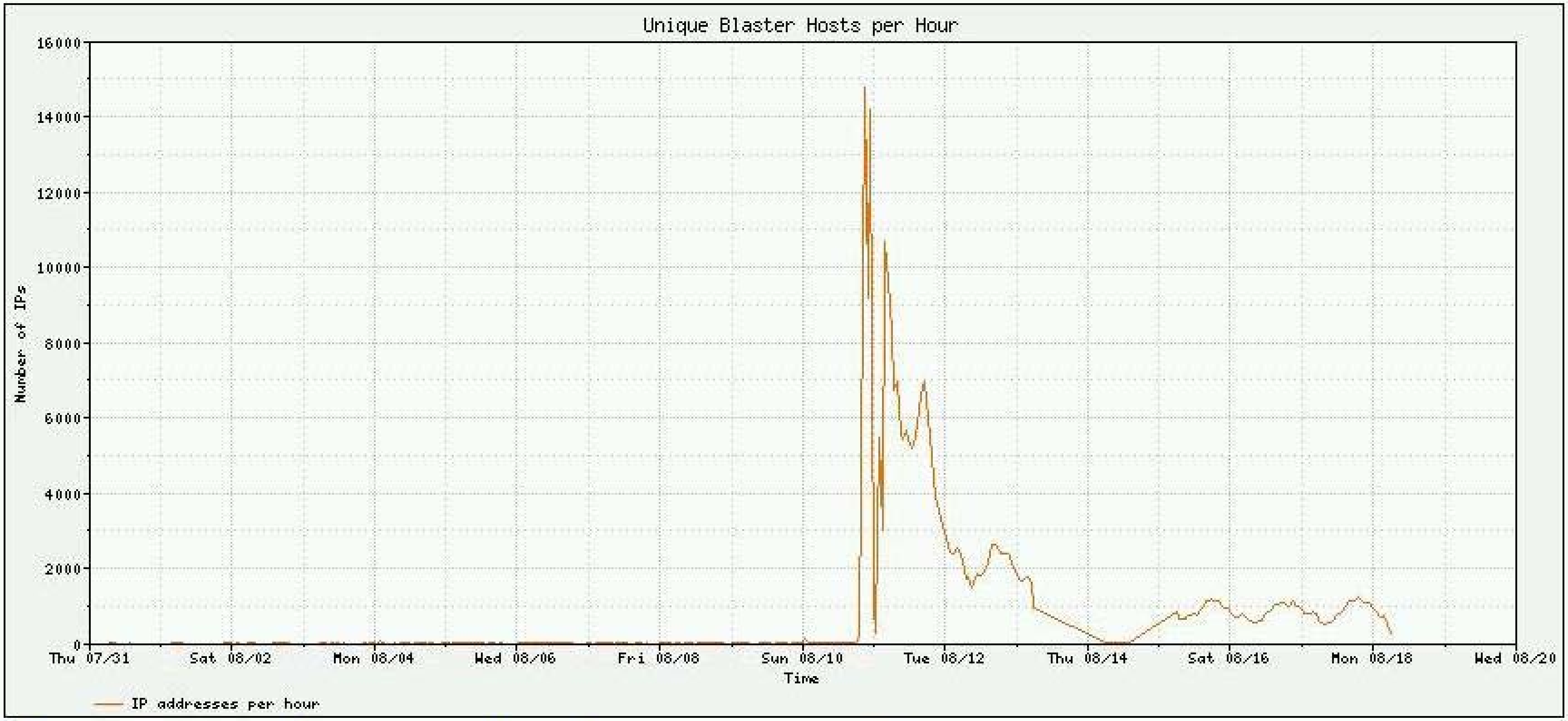
Internet

DDoS zombies
spoofing 0.0.0.0/0

X.0.0.0/8

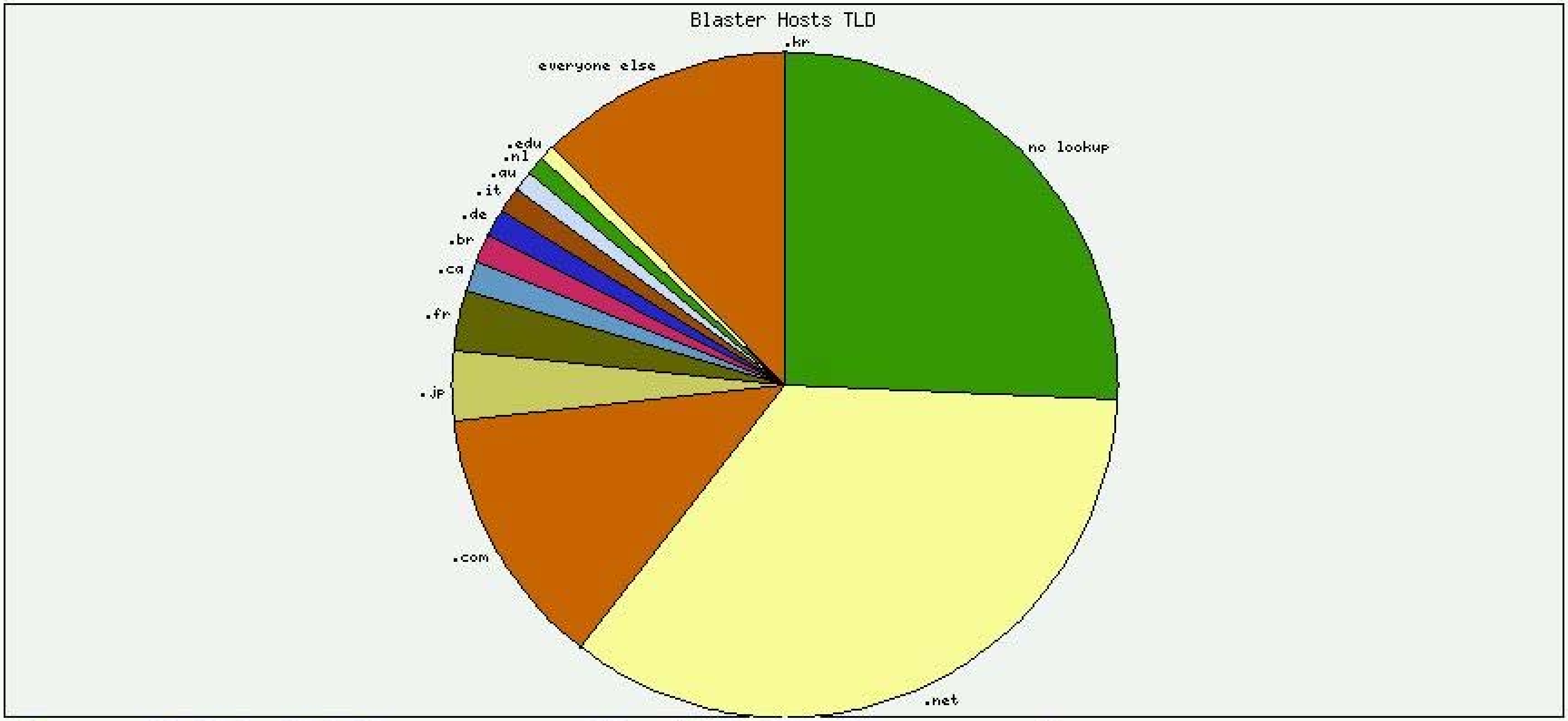
Blackhole monitor

Blaster's Traffic Patterns



3 part graph: growth, decay, persistence

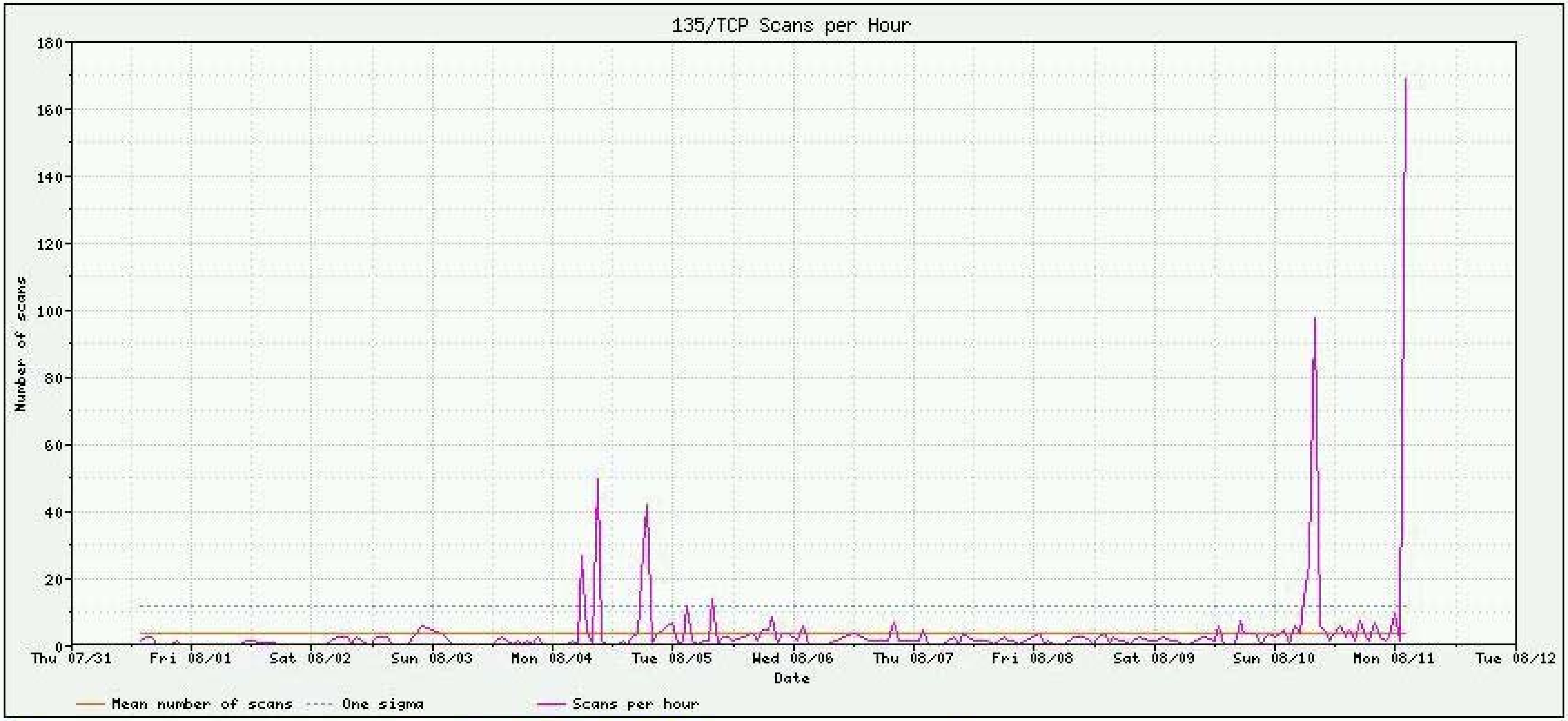
Blaster's Demographics



Over 280,000 unique IPs (10% dynamic)

DNS: .net top in TLD queries

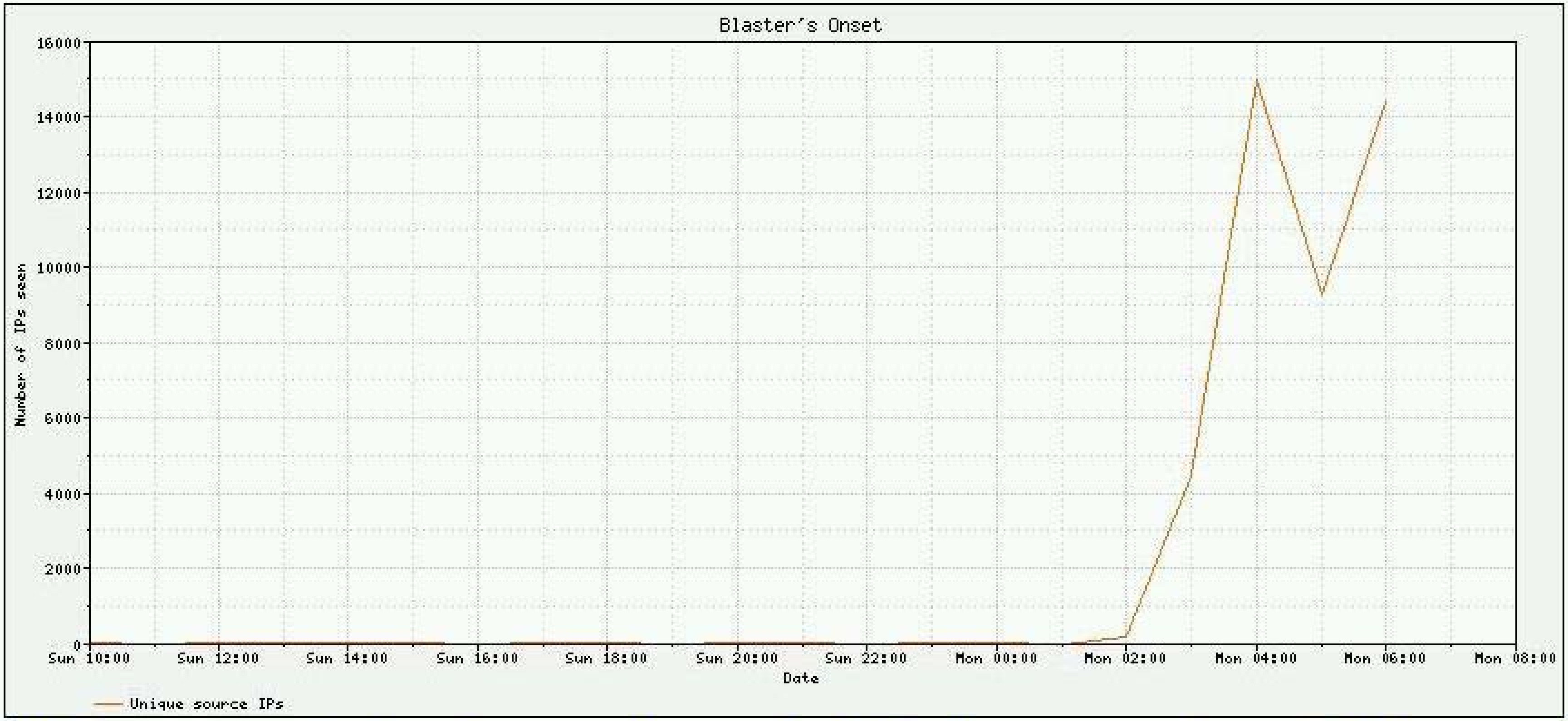
Blaster's Arrival



Strong upsurge in 135/TCP scans, unique sources

Earlier spikes from auto-rooters (k-otik)

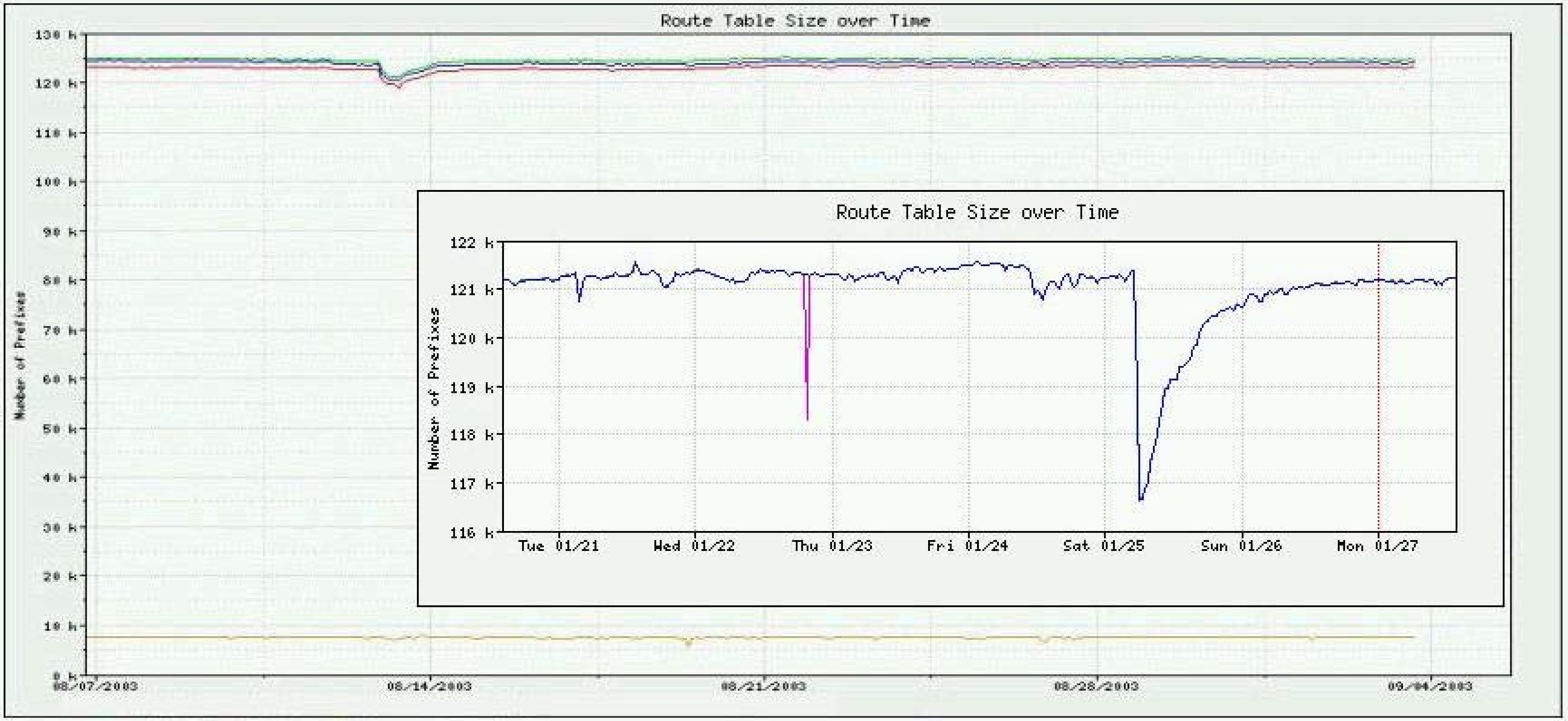
Blaster's Growth Curve



Fit to a constrained growth model (Boltzmann sigmoidal curve)

Minimum doubling time of 2.3 hours (may be overestimated)

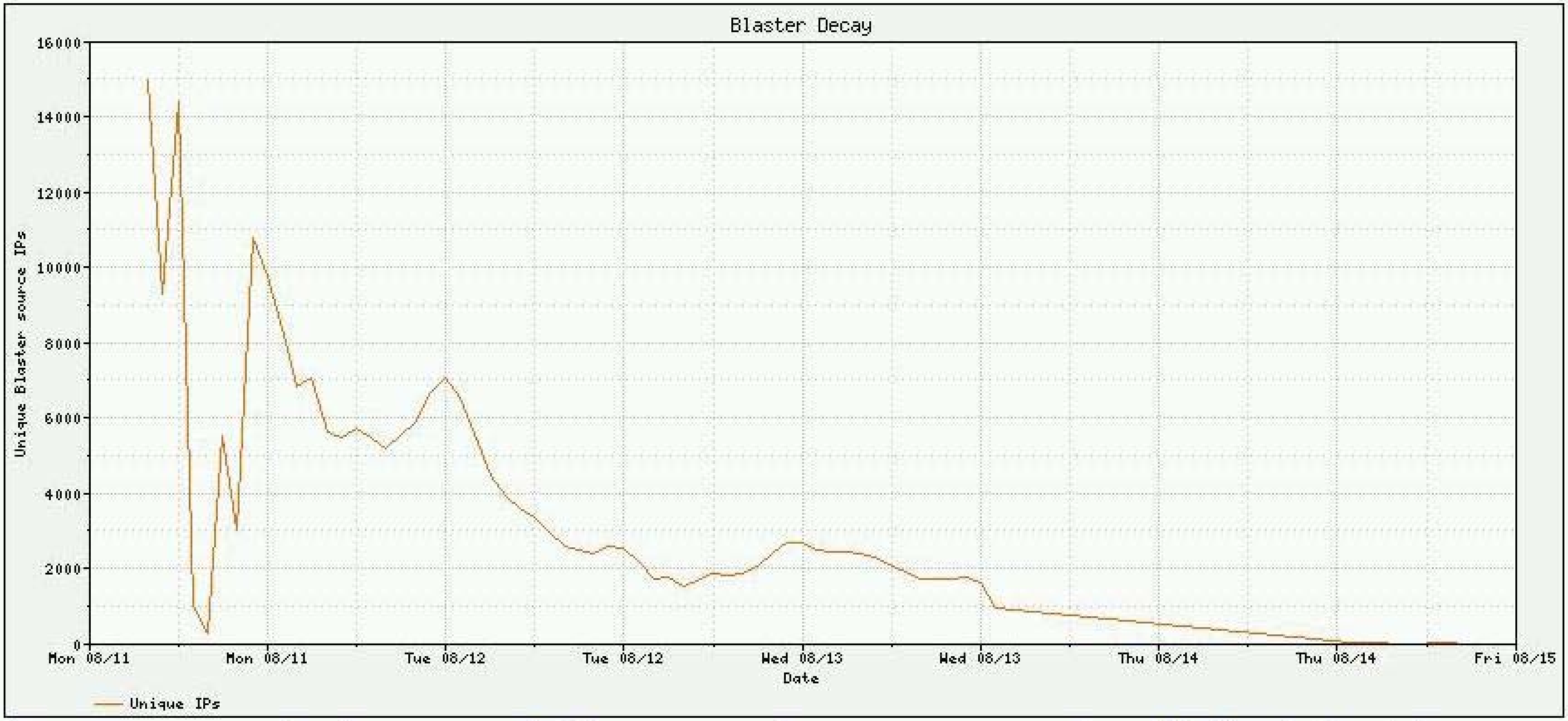
Blaster's Effect's on Routing



Only a few thousand routes dropped out

Similar effect as Sapphire or blackout

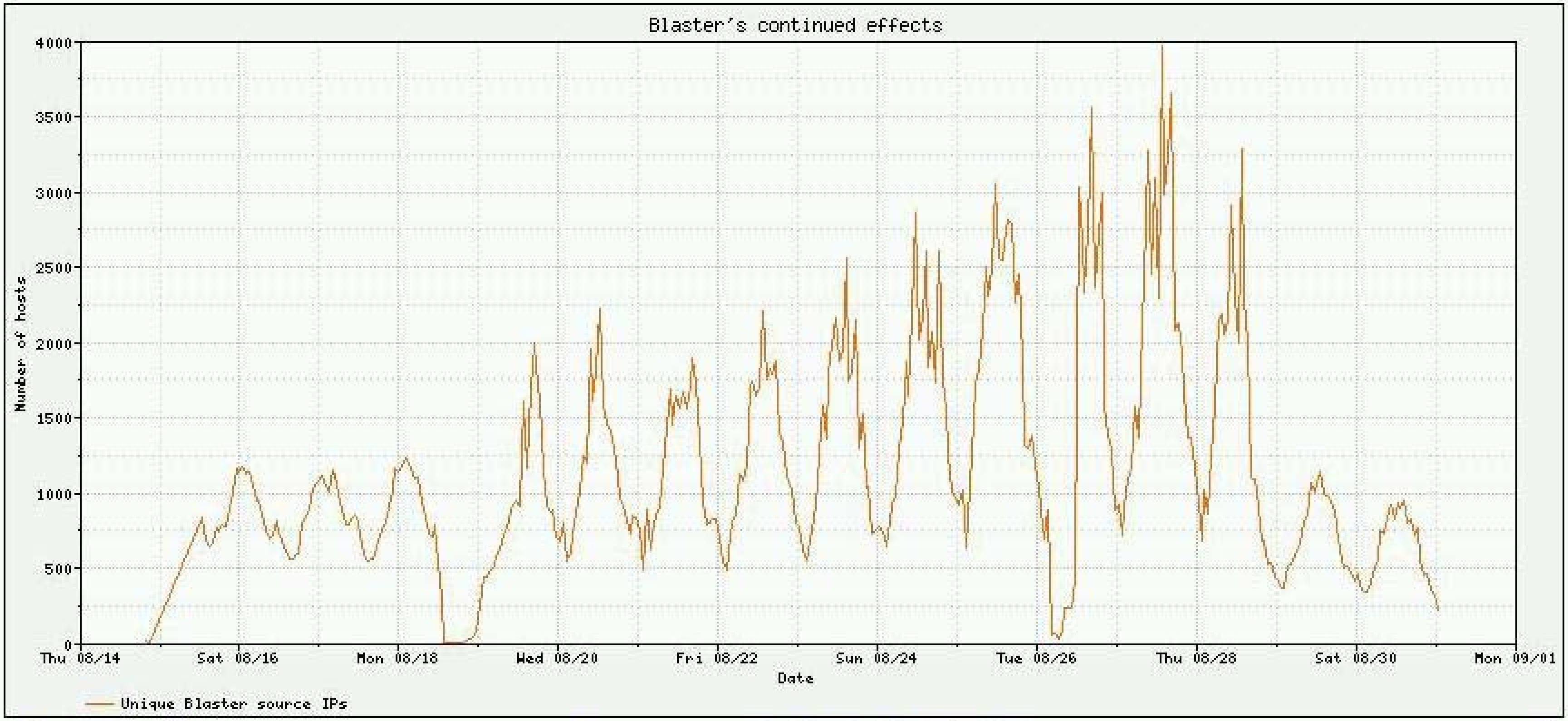
Containing Blaster



Exponential decay of Blaster observations, half-life 10.4 hours

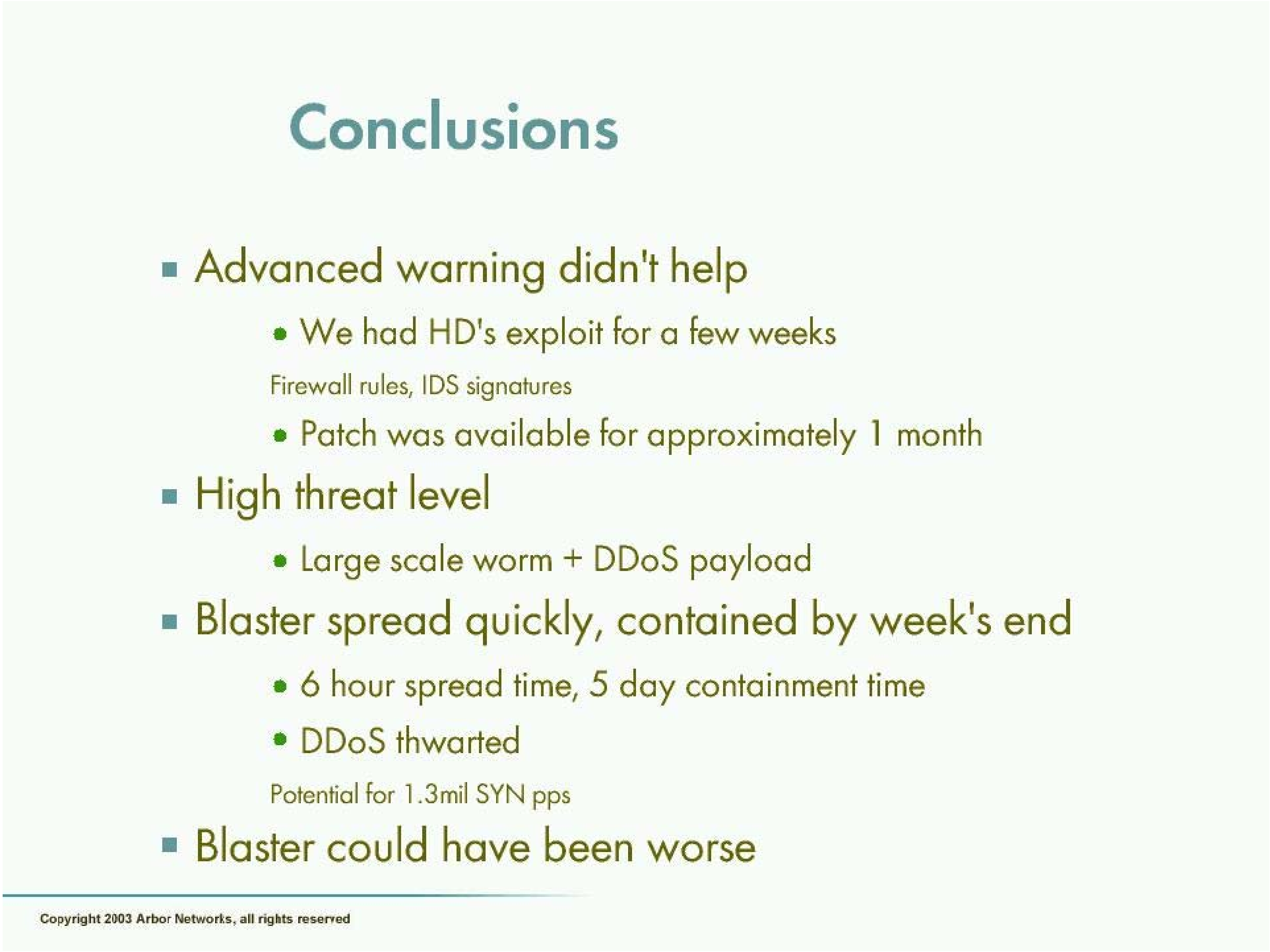
Pretty much all cleaned up in 5 days, started after about 4 hours

Blaster's Tenuous Grip



Circadian pattern, peak near 00:00 EDT, suggests power on/off

Global TLD distribution

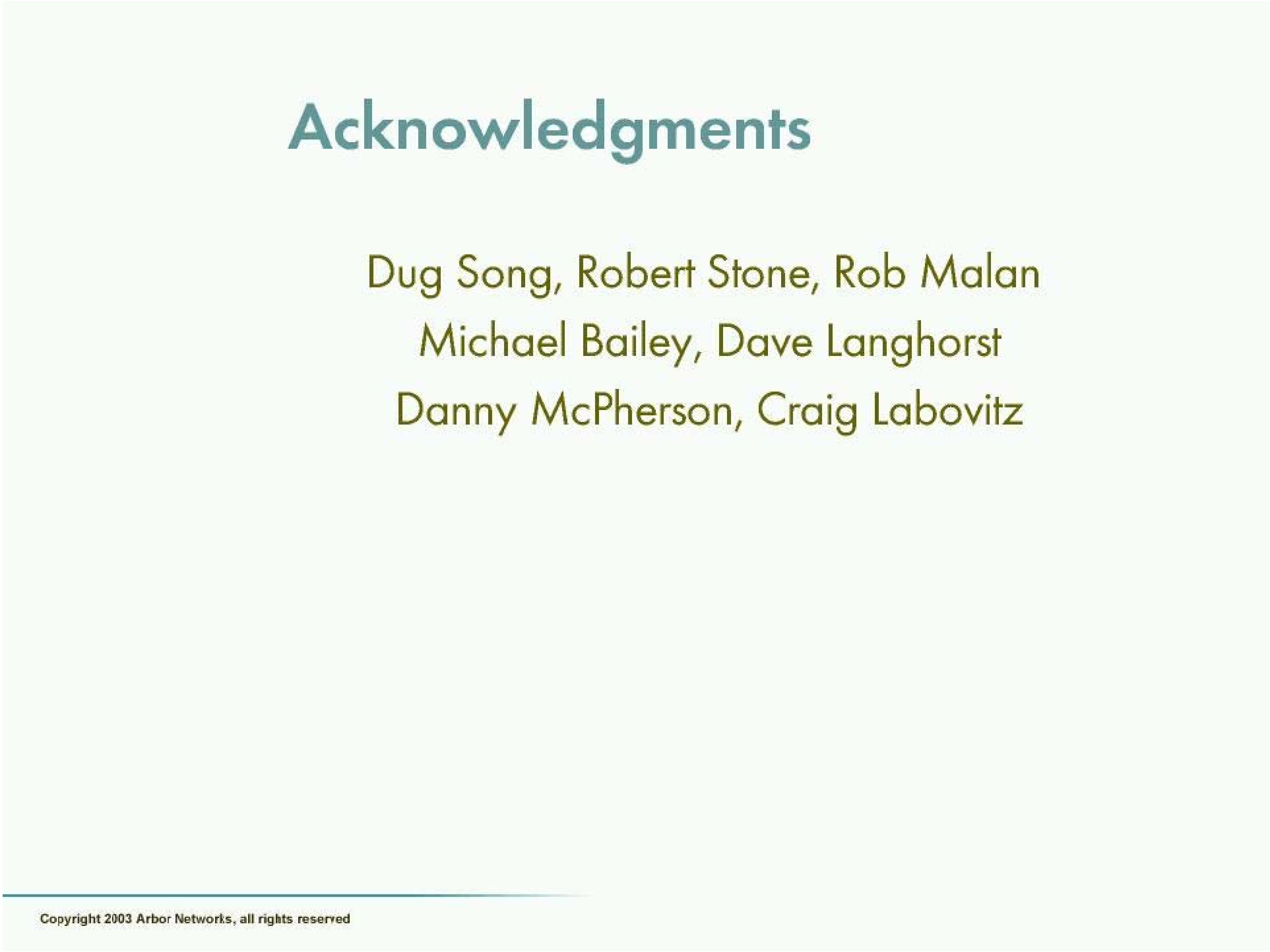


Conclusions

- Advanced warning didn't help
  - We had HD's exploit for a few weeks

    Firewall rules, IDS signatures
  - Patch was available for approximately 1 month
- High threat level
  - Large scale worm + DDoS payload
- Blaster spread quickly, contained by week's end
  - 6 hour spread time, 5 day containment time
  - DDoS thwarted

    Potential for 1.3mil SYN pps
- Blaster could have been worse



Acknowledgments

Dug Song, Robert Stone, Rob Malan
Michael Bailey, Dave Langhorst
Danny McPherson, Craig Labovitz