# Spamming with BGP Spectrum Agility

Anirudh Ramachandran
Nick Feamster
Georgia Tech

# Collection

- Two domains instrumented with MailAvenger (both on same network)
  - Sinkhole domain #1
    - Continuous spam collection since Aug 2004
    - No real email addresses---sink everything
    - 10 million+ pieces of spam
  - Sinkhole domain #2
    - Recently registered domain (Nov 2005)
    - “Clean control” – domain posted at a few places
    - Not much spam yet…perhaps we are being too conservative
- Monitoring BGP route advertisements from same network
- Also capturing traceroutes, DNSBL results, passive TCP host fingerprinting *simultaneous with spam arrival*
  (results in this talk focus on BGP+spam only)

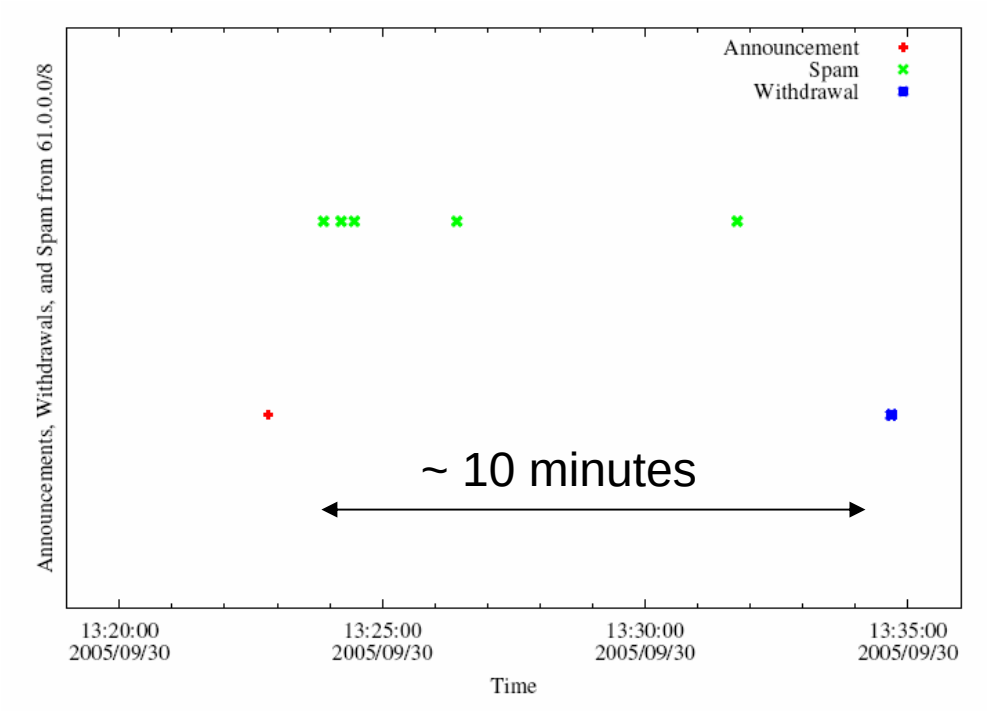
# Spamming Techniques

- Mostly botnets, of course
  - DNS hijack to get botnet topology and geography
- How we're doing this
  - Correlation with Bobax victims
    - from Georgia Tech botnet sinkhole
  - Heuristics
    - Distance in IP space of Client IP from MX record
    - Coordinated, low-bandwidth sending

**A less popular, but sometimes more effective technique: Short-lived BGP routing announcements**

# BGP Spectrum Agility

- Log IP addresses of SMTP relays
- Join with BGP route advertisements seen at network where spam trap is co-located.



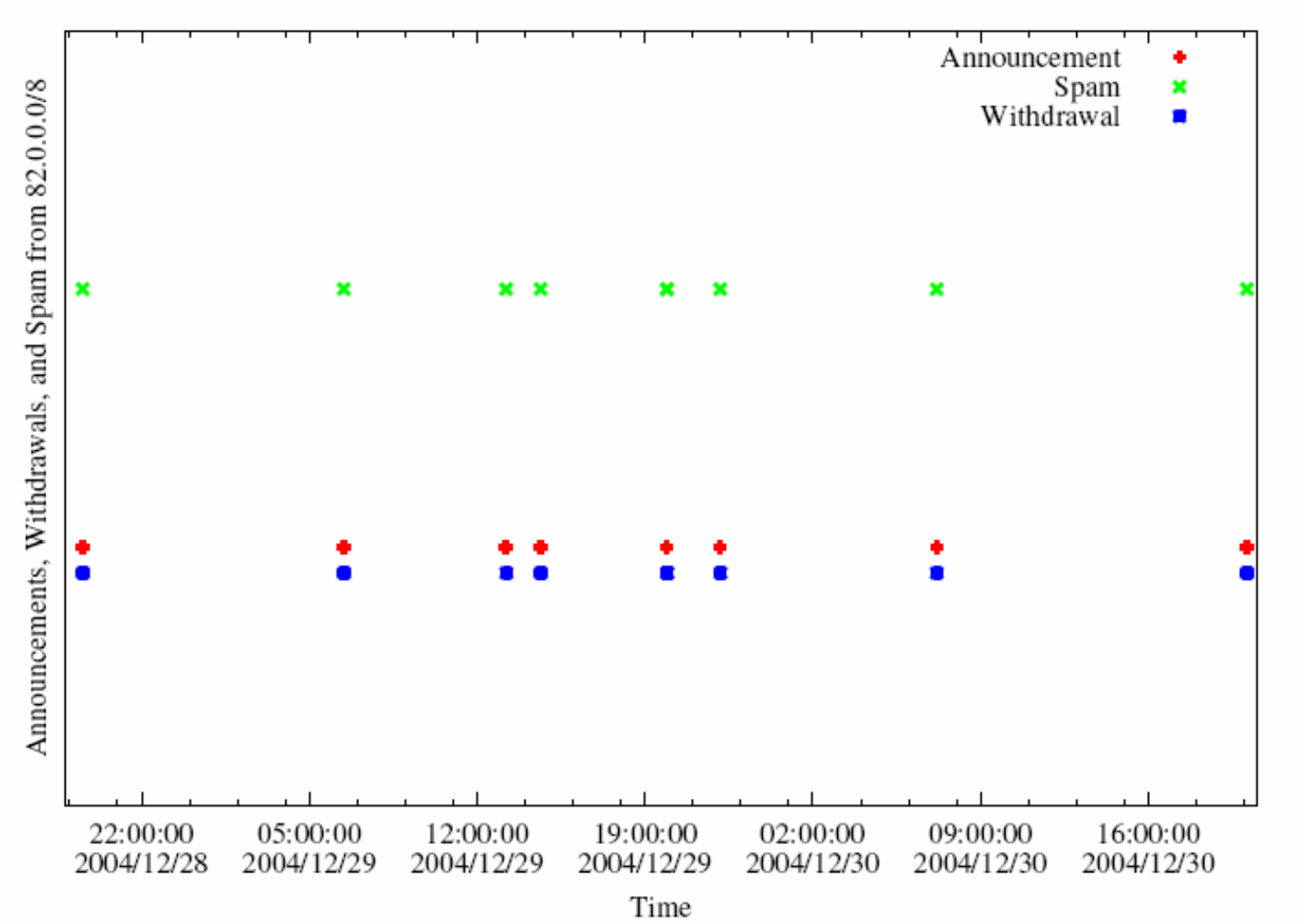

**A small club of persistent players appears to be using this technique.**

**Common short-lived prefixes and ASes**

61.0.0.0/8 4678
66.0.0.0/8 21562
82.0.0.0/8 8717

**Somewhere between 1-10% of all spam (some clearly intentional, others might be flapping)**

# A Slightly Different Pattern



# Why Such Big Prefixes?

- “Agility” (term due to Randy Bush)

- **Flexibility:** Client IPs can be scattered throughout dark space within a large /8
  - Same sender usually returns with different IP addresses

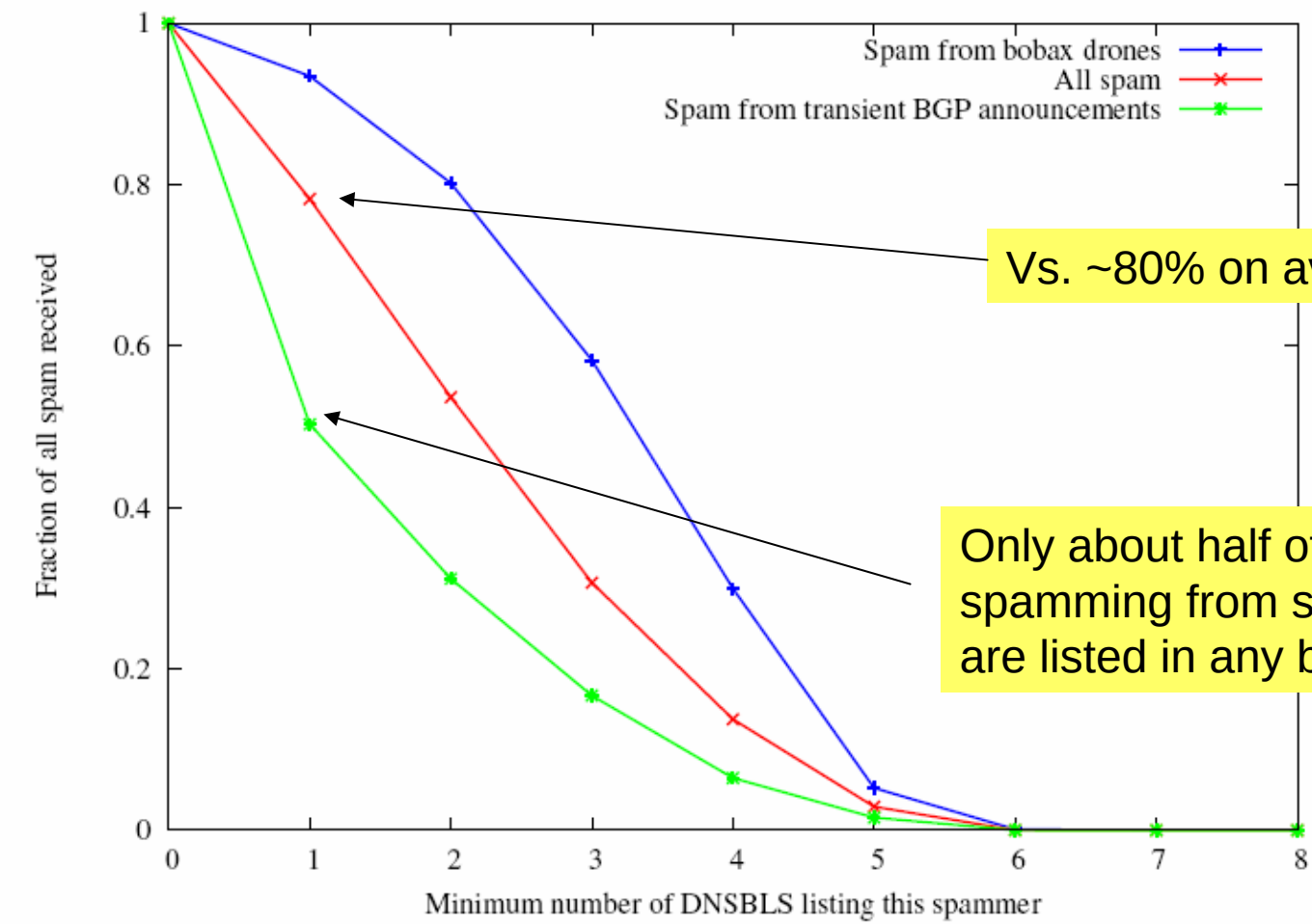
- **Visibility:** Route typically won’t be filtered (nice and short)

# Characteristics of IP-Agile Senders

- IP addresses are widely distributed across the /8 space
- IP addresses typically appear only once at our sinkhole
- Depending on which /8, 60-80% of these IP addresses were not reachable by traceroute when we spot-checked
- Some IP addresses were in *allocated*, albeing unannounced space
- Some AS paths associated with the routes contained reserved AS numbers

# Some evidence that it's working

**Spam from IP-agile senders tend to be listed in fewer blacklists**




Vs. ~80% on average

Only about half of the IPs spamming from short-lived BGP are listed in any blacklist

# Thanks

- Randy Bush
- David Mazieres

**More information:**

Anirudh Ramachandran and Nick Feamster,
*Understanding the Network-Level Behavior of Spammers*

**Send mail to Nick Feamster (username: feamster, domain: cc.gatech.edu) for a copy of the draft.**

# Length of short-lived BGP epochs