



# DNSBLs and DULs at a major ISP

Mike O'Reirdan

Comcast Distinguished Engineer

Internet Systems Engineering, NE&TO

Comcast National Engineering & Technical Operations

**INTEROP**<sup>®</sup>

THE LEADING BUSINESS TECHNOLOGY EVENT

# Some definitions

- DNSBL
  - a third party provided list of IP addresses which are used to make inform decisions as to whether to accept mail from a third party mail sender
- DUL
  - a specialised listing of IP space which has been allocated for use as dynamically assigned addresses which is used to reject mail from those addresses

# Scale of the problem for Comcast

- Nearly a billion connections per day
- Over 90% is spam
- Over 70% discarded using DNSBLs
- DNSBLs allow us to discard the majority of incoming spam for very little system utilisation
  - Blocking based on IP (reputation and DUL space)
    - 5% of CPU cycles
    - Removes ~70% of the spam
  - Blocking based on message protocol and heuristics
    - 10% of CPU cycles
    - Removes ~15% of the spam
  - Blocking based on spammy content
    - 85% of CPU cycles
    - Remove ~10% of the spam

# Comcast deployment

- Using a dedicated DNSBL hosting platform
  - First major deployment of the product
  - Chosen based on previous experience with vendor's technology
- Hosts multiple DNSBLs
- Hosts multiple DULs
- DNS is the tool used to run the blacklists
  - Fast
  - Economic from a systems point of view
  - Easily understood

# Operational challenges

- Reliability and timeliness of the DNSBL data feeds
  - Use a limited number of lists with good records on false positives
- Direct blocked senders to the specific DNSBL that was used to block them to allow them to self remediate
- DNSBL providers decide whether to unblock listed IPs when blocked senders complain

# Reputation

- DNSBLs based on the reputation of IPs
  - Derived from sending behaviour of that IP address
  - Reports of spam received from particular IP
  - Mail from IP address caught in spam trap / honey pot
- Need to move to domain reputation
  - Some lists out there but need to be combined with domain based authentication to accurately identify the good guys
- Longer term possibility of moving to individual sender's reputation
  - Massive infrastructure challenges but not impossible

# Black vs. white lists

- Don't like white lists
- Seek to minimise their existence since hard to maintain and not scaleable
- Too many misconceptions as to ISP policy for creating a white list
- White lists have a place in personal spam prevention
  - Use your address book as a white list
  - Parental controls