nominet

MX Scanning

Jay Daley, Taipei, February 2008

A quick explanation

nominet

- Many registries seeing large volumes of MX lookups
  - Hundreds of queries per second
  - Lasts for hours or days
  - Then finishes
- High level of NXDOMAINs in responses
- Believed to be related to spam, either:
  - Spammer trying list created for one TLD in another
  - Spammer checking list of domains to see which are can receive email
    - List is possible deliberately poisoned by anti-spam people
- Any questions?