The State of DNS Abuse

Graeme Bunton, DNS Abuse Institute

DNS ABUSE INSTITUTE

What is DNS Abuse?

- A set of online harms where
  - The DNS is integral
  - Reasonably resolved via the DNS
- Malware, botnets, pharming, phishing, and spam (where it's a vehicle for the preceding harms)

How is DNS Abuse Measured?

- ICANN's Domain Abuse Activity Reports (DAAR)
  - Technically well done, but lack transparency and detail.
- Reputation Block Lists
  - Commercial interests
  - Network protection, not mitigation
- Anti-Cybercrime Orgs
- DNSAI (Soon!)

Difficulties in Measurement

- Different definitions
- Different methodologies
- Access to data
  - Whois/RDAP
  - Rate limiting
- Detection and adaptation by criminals

Current Trends

- ~367 Million domain names
- DAAR sees ~208 Million names
  - With ~800,000 - 1,000,000 as abusive
  - 80% spam legacy / 90% new gtlds
- Good: small number in both absolute and relative terms
- Bad: it's going up, we don't know what's happening for 44% of the names on the internet.

Last Thoughts

- Abuse is increasing
- Governments, LEA, Regulators are paying attention
- Counting domains is still a terrible way to measure harms. Real impacts on real people and businesses.