DNS-related Papers of Possible Interest

John Kristoff

jtk@ultradns.net

OARC Workshop

A Multifaceted Approach to Understanding the Botnet Phenomenon
Internet Measurement Conference 2006

- Decent analyis and survey of typical IRC botnet characteristics
- IRC c&c fingerprint and sinkholing
- Distributed DNS cache probing for existence of c&c domain names
- Malware collection and automated analysis
- Fake bot client responders

Protecting BGP Routes to Top Level DNS Servers Distributed Computing Systems 2003

- Analysis of root/TLD prefix announcement stability
- Discusses threat of route hijacks on DNS infrastructure
- Origin/path or prefix announcement filtering strategy
- Tuning route adoption delay and route verification key to acceptance
- Before widespread use of anycast, how would this change things?

The Windows of Private DNS Updates
Computer Communications Review July 2006

- Empirical study of updates for RFC 1918 addresses at AS 112 servers
- Clients often leak of system uptime and system characateristics
- Global phenomenon, widely distributed
- Rates of a few Mb/s per AS 112 were seen
- OS id by DNS payload, IP TTL and passive stack fingerprinting
- 90% of inbound packets were TCP, due to failover algorithm
- Overwhelming Windows clients, but XP/2003 better than 2000

Inferring Relative Popularity of Internet Applications by Actively Querying DNS Caches
Internet Measurement Conference 2003

- Ask local caches non-recursively for names of interest
- Poke again as the TTL expires and examine cache gaps
- Can name popularity and request interval from gap time be inferred?
- Cached entry may not stay for entire TTL time
- Server may receive a non-auth answer
- Time of delay observations in cache gap
- How to compare names with differening TTLs
- Can we infer relative client population based on this analysis

Impact of Configuration Errors on DNS Robustness SIGCOMM 2004

- Examines Lame delegations, server diversity, cyclic zone dependency
- Examine packet traces and active measurements through probes
- Followed referrals and verifies each answers correctly
- Correlate routing data to gauge diversity
- Found about 17% lame delegation rate

An Empircal Study of Spam Traffic and the Use of DNS Black Lists
Internet Measurement Conference 2004

- DNS BL queries account for 14% of all queries
- Most spam sources are in DNS BLs
- Look for A queries of the form a.b.c.d.name where name is an rbl
- Large number of SMTP connection attempts rejected, no listener
- About 80% of spam sources are listed in DNS BLs