persistent queries

and phantom nameservers

- "I wonder how many systems will _still_ be trying to get to b.root-servers.net at the old address in 5 or even 10 years." - Dave Hilton; 29jan2004, NANOG

Legacy B Root

- Planning for renumbering in May 2003
- Public announcement in Jan 2004
- Renumbered 29jan2004
- Machine left on the old IP address, serving root until 01aug2006
- Honeypot placed on that IP address, collecting packets

Some Queries

- Query rates on the legacy IP address for "B" dropped from ~8000qps in 2003 to ~2000qps in 2004... and rose to ~2500qps as of 2006, when the DNS service was removed.
- Who is still using the legacy "B" address?
- What software are they using?
- Why are they trying to use this address?

Honeypot characteristics

- packet capture: "tcpdump -n -c 5000000" with a new file being written ~/every 10-15 minutes
- machine responds with "ICMP dest port unreachable" instead of just blackholing the query.
- only 4 notifications,VSGN, RIPE, CAIDA, and Rensys were still monitoring the legacy "B" address for DNS service. Were they monitoring the new address?

12 HOURS

- 02aug2006 - 11:59-23:59
- 24,000,000 queries from
- 229,283 unique IP addresses
- Queries for A, PTR, MX, TXT, NS, SOA, NAPTR, AAAA, NSAP, X25, ANY, and malformed (~5%)
- One address generated 3,147,739 queries

what about the rest?

- non-BIND... ATLAS BSRPDNSC eNom DNS incognito v2311-v4051
- MaraDNS MyDNS Nominum ANS Nominum CNS NonSequitur DNS
- OakDNS pliant DNS Posadis Power DNS 28 293 Power DNS 294 2911
- QuickDNS simple DNS plus simple DNS plus (recursive) TinyDNS 104 TinyDNS 105

- Bind 4.9.3-4.9.11 Bind 8.1R-8.2.1-t4b REC Bind 8.2.1 REC Bind 8.2.2-8.3.0-T2A
- Bind 8.2.2-8.3.0-T2A REC Bind 8.3.0RC1-8.4.3 Bind 8.3.0RC1-8.4.2 REC Bind 8 w/ RSM

- Bind 900b5 901 Bind 900b5-901 REC Bind 910 913 REC Bind 920a1 920rc3
- Bind 920a1 920rc3 REC Bind 920a1 922-P3 REC Bind 920rc7 922-P3 REC
- Bind 923rc1 940a0 Bind 923rc1 940a0 REC **** this is worrying ****
- Windows 2000 Windows 2003 Windows NT4 Windows XP

Why?

- No single conjecture works for all situations
- conjecture: still using the old hints file
  - TTL of 99999999 in early hints files and this address was the last of the original root servers
- conjecture: people are changing the source code.
- conjecture: BIND’s hint logic is broken

Futures

- How long to run the honeypot?
- Is it worth the effort to track down WHY?
    - the number of queries IS increasing over time
    - nodes continue to use the legacy address
- Is it worth the effort to do a query analysis?
- How would active probes (NMAP) be perceived?

Your Thoughts?

bill manning
03nov2006
wide/caida
bmanning@ep.net