DNS Operational Issues and Management Opportunities

John Kristoff
UltraDNS
jtk@ultradns.net

April 3, 2006
Introduction

Overview of UltraDNS
What I Am Doing Now

DNS Operational Issues

Open Recursive Name Service
Server Placement and Diversity
Bogus and Suspicious Queries

DNS Management Opportunities

Turn on BIND Query Logging
Software Tools
Overview of UltraDNS

- Managed DNS provider and TLD operator
- Custom-built DNS software using Oracle back-end
- Global BGP anycast for a handful of service netblocks
- Example customers:
  - .org, .info, .uk
  - Amazon, Myspace, Harley-Davidson
  - FIRST, Gentoo, www.usc.edu
What I Am Doing Now

- DNS data analysis, projects and research
- Routing analysis, projects and research
- Security analysis, projects and research
Open Recursive Name Service

- Providing answers for non-authoritative zones to the world
- Attackers may abuse this capability for reflection and amplification
- Some draw similarities with the issue to open mail relays
Numbers from an Early February Attack

- 51,000+ 4KB UDP DNS TXT RR senders to a single host
- Multi-gigabit/second packet love
- At least 50% were from *DNS proxies*
- As of March 30, 2006, all hosts were still DNS servers
- As of March 30, 2006, about 75% were still open recursive
- Our best guess so far is there are 1-2 million out there
University of Chicago

$ dig @ns1.uchicago.edu www.ultradns.com

; <<< DiG 9.2.2 <<< @ns1.uchicago.edu www.ultradns.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24127
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 8, ADDITIONAL: 8

;; QUESTION SECTION:
;www.ultradns.com. IN A

;; ANSWER SECTION:
www2.ultradns.com. 60 IN A 204.74.104.97

;; AUTHORITY SECTION:
ultradns.com. 28719 IN NS pdns1.ultradns.net.
ultradns.com. 28719 IN NS pdns2.ultradns.net.

;; MSG SIZE rcvd: 408
Northwestern University

$ dig @accuvax.northwestern.edu www.ultradns.com

; <<>> DiG 9.2.2 <<>> @accuvax.northwestern.edu www.ultradns.com
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61044
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;www.ultradns.com. IN A

;; AUTHORITY SECTION:
com. 172797 IN NS J.GTLD-SERVERS.NET.
com. 172797 IN NS K.GTLD-SERVERS.NET.
com. 172797 IN NS L.GTLD-SERVERS.NET.
com. 172797 IN NS M.GTLD-SERVERS.NET.
com. 172797 IN NS A.GTLD-SERVERS.NET.
com. 172797 IN NS B.GTLD-SERVERS.NET.
com. 172797 IN NS C.GTLD-SERVERS.NET.

;; MSG SIZE rcvd: 258
Server Placement and Diversity

- NS RRset size
- Geographic separation
- Netblock diversity
- Upstream and peer connectivity
DePaul University

ns1.depaul.edu. 86400 IN A 140.192.0.2
ns2.depaul.edu. 86400 IN A 140.192.239.2
...
$ whois -h whois.cymru.com " -p 140.192.0.0"
AS | IP | BGP Prefix | AS Name
20130 | 140.192.0.0 | 140.192.0.0/16 | DEPAUL - Depaul University
...
Route Views sees upstreams: 174 (Cogent), 6325 (ICN), 22335 (MREN)
...
  9 140.192.9.145 17.699 ms
  10 140.192.239.2 17.574 ms
  ...
  9 140.192.9.145 17.064 ms
  10 140.192.9.177 17.834 ms
  11 140.192.0.2 18.200 ms
DNS1.IT.luc.edu. 172800 IN A 147.126.1.1
DNS2.IT.luc.edu. 172800 IN A 147.126.1.2
...
$ whois -h whois.cymru.com "-p 147.126.0.0"
AS | IP | BGP Prefix | AS Name
7968 | 147.126.0.0 | 147.126.0.0/20 | LOYOLA-UNIV-CHICAGO - Loyola
...
Route Views sees upstreams: 6325 (ICN), 22335 (MREN)
...
9  147.126.95.37  17.277 ms
10 147.126.1.2  18.608 ms
11 *
...
9  147.126.95.37  17.934 ms
10 147.126.1.1  17.192 ms
11 *
Bogus and Suspicious Queries

- Obnoxious operating systems query for all sorts of junk
- Misconfigurations can result in long-lived, persistent queries
- Worms, bots and spyware often use locally configured DNS servers
$ dig @accuvax.northwestern.edu 1.0.0.10.in-addr.arpa

; <<>> DiG 9.2.2 <<>> @accuvax.northwestern.edu 1.0.0.10.in-addr.arpa
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 1181
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;1.0.0.10.in-addr.arpa. IN A

;; AUTHORITY SECTION:
10.in-addr.arpa. 10800 IN SOA prisoner.iana.org. hostmaster.root-servers.org. 1 604800 60 604800 604800

;; Query time: 25 msec
;; SERVER: 129.105.49.1#53(accuvax.northwestern.edu)
;; WHEN: Mon Apr  3 10:07:26 2006
;; MSG SIZE  rcvd: 116
### A Not Too Unusual Top Query Name List

*only non-authoritative zone queries shown*

#### Top 25 Queries

<table>
<thead>
<tr>
<th>Count</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>170549</td>
<td><a href="http://www.weather.com">www.weather.com</a></td>
</tr>
<tr>
<td>143786</td>
<td><a href="http://www.xxxposition.net.example.edu">www.xxxposition.net.example.edu</a></td>
</tr>
<tr>
<td>143786</td>
<td><a href="http://www.xxxposition.net">www.xxxposition.net</a></td>
</tr>
<tr>
<td>142213</td>
<td>cc11.kaist.ac.kr</td>
</tr>
<tr>
<td>141017</td>
<td>twx.doubleclick.net</td>
</tr>
<tr>
<td>133730</td>
<td>ad.doubleclick.net</td>
</tr>
<tr>
<td>115607</td>
<td>mail.google.com</td>
</tr>
<tr>
<td>94054</td>
<td>hoe.firststringtonesforyou.com</td>
</tr>
<tr>
<td>93978</td>
<td>hoe.firststringtonesforyou.com.example.edu</td>
</tr>
<tr>
<td>93541</td>
<td>141.136.248.143.in-addr.arpa</td>
</tr>
<tr>
<td>92310</td>
<td>255.255.255.255.in-addr.arpa</td>
</tr>
</tbody>
</table>
Turn on BIND Query Logging

- If privacy police are OK with it, turn it on, lots of good data
- With little to no effort, minimally you have an audit trail
- If you like network flows, you’ll probably like query logs
Software Tools

- dnstop and dsc from http://www.measurement-factory.com/products.html
- fpdns from http://www.rfc.se/fpdns/