Observed Workarounds

…to the introduction of the Site Finder service in .COM/.NET

NANOG 29

Suzanne Woolf woolf@isc.org

Internet Software Consortium

Background: DNS Responses

- Normal answer
  - “Here is the data matching your question”
- Referral (or “Delegation”)
  - “Here are the servers who could answer you”
- Negative answer (or “NXDOMAIN” or “RCODE 3”)
  - “There is no such name”

Background: Why were people upset?

- Not about Site Finder as such: anyone who wants to can run a search engine
- Some political concerns expressed, out of scope for this talk
- Lost revenue for some network operators, also out of scope here
- Change to the behavior of DNS violated the Principle of Least Surprise
- Costs, particularly in time, to mitigate effects

Background: ISC's Involvement

- ISC is a not-for-profit who publishes BIND and operates "f-root" (among other things)
- Our relevance and success depends on our responsiveness to the technical community
- The technical community gave an intensely negative response to VeriSign's Site Finder
- We have no financial stake in the outcome

Workaround: Translate Address back to RCODE 3

- Unofficial patches for opensource DNSware
  - Popular programs like BIND, djbdns, others
- Look for 64.94.110.11, substitute RCODE 3
  - This is the address of the Site Finder web site
- Weakness: address could change naturally
  - For example, due to a DDoS or load balancer
- Weakness: other TLDs use other addresses
  - One BIND8 patch now has a complete list

Workaround: Require Referrals From Some TLDs

- “delegation-only” for specified domains
- Server for .FOO can only send referral (“delegation”) toward servers for SUB.FOO
- Normal answers translated to RCODE 3
- ISC released new BIND9 feature in ~40 hrs
- *This is not BIND’s default behaviour*

Workaround: Permit Non-Referrals From Some TLDs

- “root-delegation-only” applies to root and all toplevel domains except those specified
- We list some common exceptions at: http://www.isc.org/products/BIND/delegation-only.html
- This “locks out” future wildcards in TLDs
- ISC improved new BIND9 feature in 4 days
- *This is also not BIND’s default behaviour*

Workaround: Selectively Forward Queries for Some TLDs

- Many users have no analogue of BIND9's "delegation-only" or "root-delegation-only"
- Some users can *selectively forward* queries to a BIND9 server having "delegation-only"
- ISC runs such a server, open to the public at f.6to4-servers.net (via IPv4 or IPv6)
  - Traffic on "f-6to4" has been very light

Workaround: Advertise Local Instance of 64.94.110.11

- Any ISP can advertise a local Site Finder server to their own customers
- This means “typos” are handled locally, using synthetic data provided by VeriSign
- Can create a local revenue source, or at least a culturally correct page in local language
- Weakness: DNS incoherency when roaming

Workaround: Remap RCODE 3 to a Local Server

- “If VeriSign can do it why can’t we?”
- Eyeball-heavy access providers can modify DNS responses in flight
- Change “64.94.110.11” to a local address
- Also change RCODE 3 to a local address
- So: Site Finder-like behaviour for *all* otherwise non-instantiated domains
- *This is not just theory, it has been observed!*

Other Applications with Known Workarounds

- E-mail Software
  - Postfix
  - Sendmail
  - Mailtraq
  - Exim
- DNS Software
  - dbjdns/tinydns
  - PowerDNS
  - Simple DNS Plus
  - Dnsmasq

Protocol Violations?

- If the protocol is violated, then responses will be rejected by the requestor
  - VeriSign's synthesis doesn't do this
  - Nor do any of the workarounds
- Modifying data in transit, as many of the workarounds do, is a form of incoherency
- Sending unwelcome response data leads inevitably to many forms of incoherency

Numbers (through 29-SEP-2003)

- MSN distinct visitors down from 237M to 218M
- VRSN traffic rank up from #1559 to #23
- Approximately 9% of Alexa users did not see VeriSign's synthetic data due to local ISP action
- Adelphia blocked it for four days, then stopped

Summary: Strong Community Response to Site Finder

- Workarounds to “turn back the clock”
- Workarounds to keep the revenue local
- Workarounds inspired by Site Finder but which are even more ambitious
- DNS responses are less and less coherent
- So: *new instability, and maybe more to come*

Bibliography

- bcn.boulder.co.us/~neal/ietf/verisign-abuse.html
- www.imperialviolet.org/dnsfix.html
- ISC delegation-only and root-delegation only: www.isc.org/products/BIND/delegation-only.html
- Taxonomy of observed effects of Site Finder: www.packet-pushers.net/tld-wildcards/
- Web statistics from Alexa: http://www.alexa.com
- Discussion of Alexa data on Site Finder impact: cyber.law.harvard.edu/tlds/sitefinder/