DNS as a Defense Vector

Paul Vixie, Ph.D
CEO, Farsight Security

TOPIC

DNS Itself

INTERNET AS A TERRITORY

- But what **is** the internet?
  - "It's the largest equivalence class in the reflexive transitive symmetric closure of the relationship *can be reached by an IP packet from."*

    (Seth Breidbart)
- IP addresses, IP packets, underlie everything
- We overlay IP with many things, e.g., *the web*
- Most important overlay (for security) is: DNS

DNS AS A MAP

- Most everything we do on the Internet…
  - B2C Web, B2B Web, E-mail, I-M, <*your idea here*>
  - …relies on TCP/IP, and begins with a DNS lookup
- Mobile Internet is dominated by search…
  - …but search itself relies extensively upon DNS
- DNS has a rigorous internal structure
  - Things that are in fact related, *are* related in DNS
  - You can have *whois* privacy, but not DNS privacy

CRIMINAL DNS

- The Internet has been a great accelerator of human civilization
  - Inevitably, this includes human crime
- Online crime is impossible without DNS
  - Cheap throw-away domain names
  - DNS registrars and servers in bad neighborhoods
  - *Whois* privacy or simply bad *whois* data
- *Nature, to be commanded, must be obeyed*.
  - (Francis Bacon)

SO, ABOUT THAT INTERNAL STRUCTURE

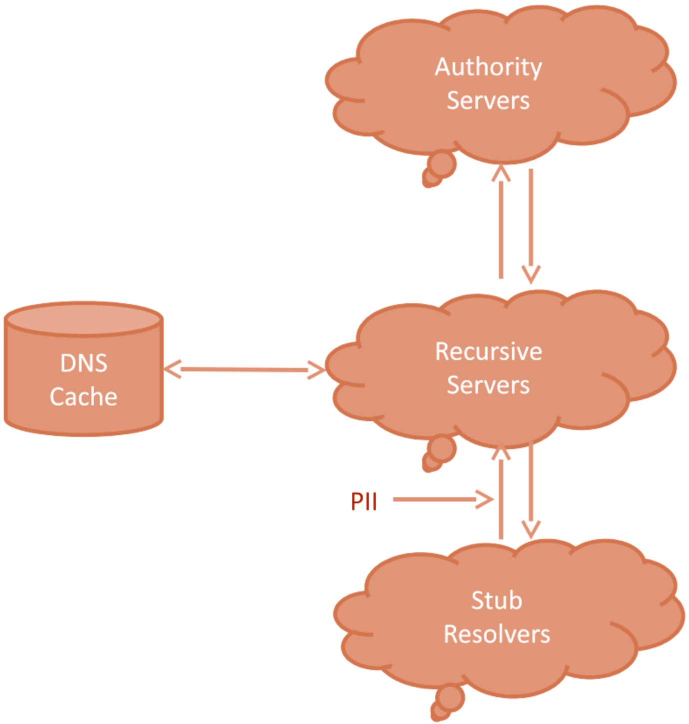
FARSIGHT SECURITY

- Domain names are grouped into *zones*
  - Like *root* zone, or “COM”, or “EXAMPLE.COM”
- A *zone* has one or more *name servers*
  - Like “COM. NS a.gtld-servers.net.”
- Each *name server* has one or more *addresses*
  - Like “a.gtld-servers.net. A 192.5.6.30”
- Other domain names also have *addresses*
  - Like “www.apnic.net. A 203.119.102.244”
- IP *addresses* are grouped into *netblocks*
  - Like “192.5.6.0/24” or “203.119.102.240/28”

DNS SECURITY FEATURES

- TSIG secures heavy weight transactions
  - Like UPDATE, IXFR/AXFR; but not QUERY
- DNSSEC secures data end-to-end
  - Zone is signed; responses contain signatures
  - Zone has keys; these are signed in parent zone
  - QUERY initiator can validate signatures
  - Requires universally trusted *root signing key*
- Use TSIG and DNSSEC: they work, they’ll help
  - But: our actual topic today lies elsewhere

DNS DATA FLOW



13 root servers,
~250 cCtld's
~15 old Gtld's
~2000 new Gtld's
~500M 2LD/etc

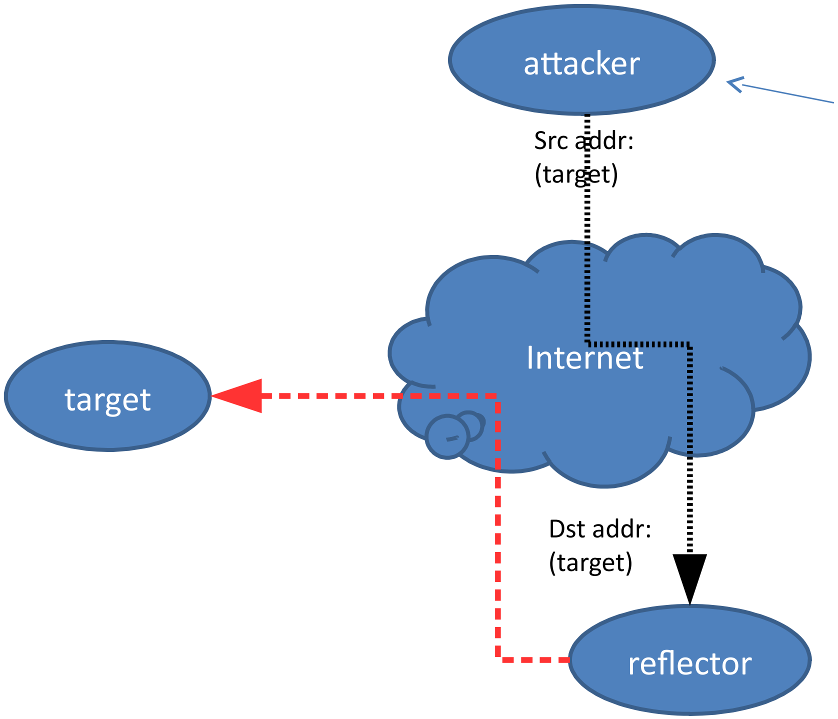
Campus,
Enterprise,
OpenDNS,
GoogleDNS

Servers, Laptops
Smartphones
Embedded devs

TOPIC

DNS as Abused

SPOOFED SOURCE ATTACK



Botted server,
in the cloud,
Gigabit speed

DNS RESPONSE RATE LIMITING (RRL)

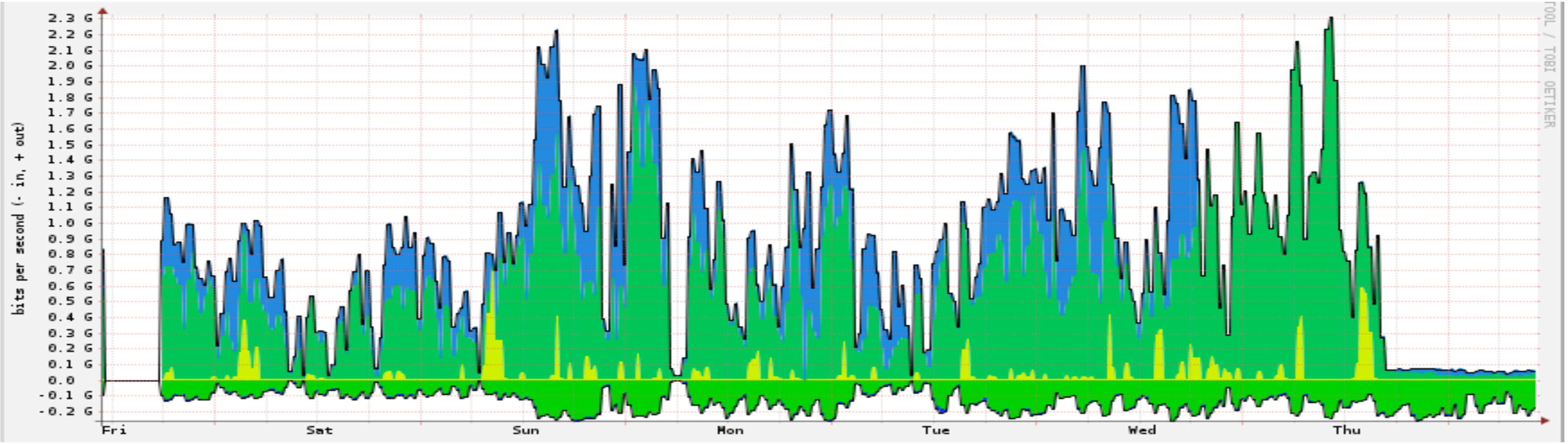
- If you run a DNS content (“authority”) server, it has to be massively overprovisioned

- Because OPN’s don’t have SAV, your server is a purpose-built DNS DDoS reflecting amplifier

- BIND, NSD, Knot now support DNS RRL, which accurately guesses what’s safe to drop

- Your authority servers need this, whereas your recursive servers need to be firewalled off

RRL IN ACTION: AFILIAS



“…TOO CHEAP TO METER”

- SpamAssassin as a teaching tool
  - For example: dotted quads in body as spamsign
- RRP and EPP: solving “the .COM problem”
  - Running a race to the bottom (cheaper; sooner)
- Quantity and fluidity having only one purpose
  - 30 seconds? Really?
- Fitting Sturgeon’s revelation
  - “90% of <thing> is crap”

TAKEDOWN: FAR-END TRICKS

- Since we can't prevent it…
  - …we'll have to evolve coping strategies
- Takedown as a Service (TaaS?)
  - Yes, you can outsource this now
- A new profit center! (.TK)
  - "Kill all you want, we'll make more!"
- Whack-a-mole as a Service (WaaS?)
  - Incrementalism breeds better criminals

FIREWALLS: NEAR-END TRICKS

- If we can’t prevent it and takedown is hard…
  - …then we’ll have to fight them at our doorstep

- We can filter IP+port, URL, and now even DNS
  - But, bad guys are endlessly adaptive
  - Ergo, so must we be

- We can’t afford manual configuration
  - So, firewall config now follows a pub-sub model

DNS FIREWALLS WITH RPZ

- Uses DNS zones to carry DNS Firewall policy
  - R-P-Z = Response Policy Zones
- Pub-sub is handled by NOTIFY/TSIG/IXFR
  - Many publishers, many subscribers, one format
- Subscribe to multiple external feeds
  - And create your own, for local policy reasons
- Simple failure or walled garden, as you choose
  - We call this “taking back the DNS”

RPZ CAPABILITIES

- Triggers (RR owners):
  - If the query name is $X
  - If the response contains an address in CIDR $X
  - If any NS name is $X
  - If any NS address is in CIDR $X
  - If the query source address is in CIDR $X

- Actions (RR data):
  - Synthesize NXDOMAIN
  - Synthesize CNAME
  - Synthesize NODATA
  - Synthesize an answer
  - Answer with the truth

WHY USE RPZ?

- Easy stuff:
  - Block access to DGA C&C’s
  - Block access to known phish/driveby
  - Block e-mail if envelope/header is spammy
- More interesting stuff:
  - Block DNS A/AAAA records in bad address space
    - E.g., import Cymru Bogons or Spamhaus DROP list
  - Block domains having some computable attribute
    - E.g., Farsight Newly Observed Domains (NOD) list

KEY RPZ TAKEAWAYS

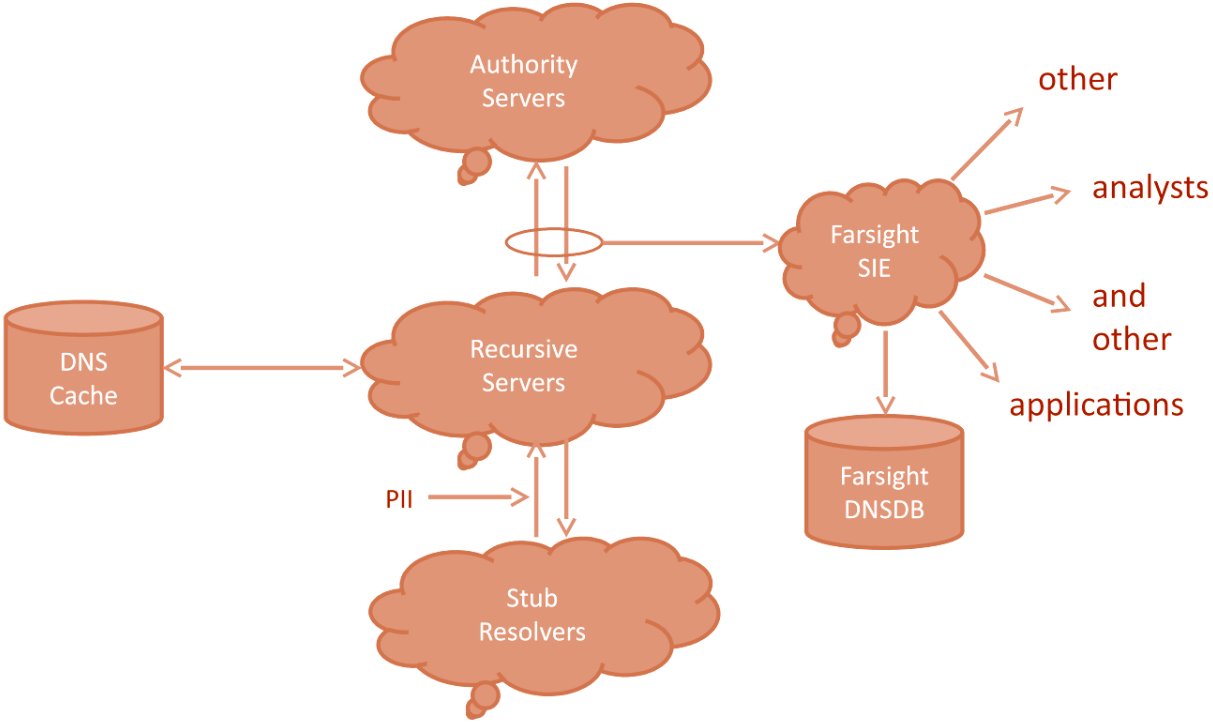
- Implications:
  - Open market for producers and consumers
  - Differentiated service at a global scale
  - Instantaneous wide area takedown

- Deployment:
  - The RPZ standard is open and unencumbered
  - So far implemented in BIND, Unbound, PowerDNS
  - BIND RPZ performance is not unreasonable (~5% QPS loss)
  - New RPZ features will be backward compatible
  - RPZ is not an IETF standard

TOPIC

DNS as Observed

PASSIVE DNS DATAFLOW



OWNER LOOKUP, SHOW HISTORY

```
$ dnsdb_query -r vix.com/ns/vix.com

;; record times: 2010-07-04 16:14:12 \
               .. 2013-05-12 00:55:59
;; count: 2221563; bailiwick: vix.com.
vix.com.  NS  ns.sql1.vix.com.
vix.com.  NS  ns1.isc-sns.net.
vix.com.  NS  ns2.isc-sns.com.
vix.com.  NS  ns3.isc-sns.info.

;; record times: 2013-10-18 06:30:10 \
               .. 2014-02-28 18:13:10
;; count: 330; bailiwick: vix.com.
vix.com.  NS  buy.internettraffic.com.
vix.com.  NS  sell.internettraffic.com.
```

OWNER WILDCARDS (LEFT OR RIGHT SIDE)

```
$ dnsdb_query -r \*.vix.com/a | fgrep 24.104.150
internal.cat.lah1.vix.com.  A  24.104.150.1
ss.vix.com.                 A  24.104.150.2
gutentag.vix.com.           A  24.104.150.3
lah1z.vix.com.              A  24.104.150.4
mm.vix.com.                 A  24.104.150.11
ww.vix.com.                 A  24.104.150.12
external.cat.lah1.vix.com.  A  24.104.150.33
wireless.cat.lah1.vix.com.  A  24.104.150.65
wireless.ss.vix.com.        A  24.104.150.66
ap-kit.lah1.vix.com.        A  24.104.150.67
cat.lah1.vix.com.           A  24.104.150.225
vix.com.                    A  24.104.150.231
deadrat.lah1.vix.com.       A  24.104.150.232
ns-maps.vix.com.            A  24.104.150.232
ns.lah1.vix.com.            A  24.104.150.234
```

DATA LOOKUP, BY NAME

```
$ ./dnsdb_query -n ss.vix.su/mx
vix.su.                MX  10 ss.vix.su.
dns-ok.us.             MX   0 ss.vix.su.
mibh.com.              MX   0 ss.vix.su.
iengines.com.          MX   0 ss.vix.su.
toomanydatsuns.com.    MX   0 ss.vix.su.
farsightsecurity.com.  MX  10 ss.vix.su.
anog.net.              MX   0 ss.vix.su.
mibh.net.              MX   0 ss.vix.su.
tisf.net.              MX  10 ss.vix.su.
iengines.net.          MX   0 ss.vix.su.
al.org.                MX   0 ss.vix.su.
vixie.org.             MX   0 ss.vix.su.
redbarn.org.           MX   0 ss.vix.su.
benedelman.org.        MX   0 ss.vix.su.
```

DATA LOOKUP, BY IP ADDRESS

```
$ dnsdb_query -r ic.fbi.gov/mx
ic.fbi.gov.  MX  10 mail.ic.fbi.gov.

$ dnsdb_query -r mail.ic.fbi.gov/a
mail.ic.fbi.gov.  A  153.31.119.142

$ dnsdb_query -i 153.31.119.142
ic.fbi.gov.           A  153.31.119.142
mail.ic.fbi.gov.      A  153.31.119.142
mail.ncijtf.fbi.gov.  A  153.31.119.142
```

DATA LOOKUP, BY IP ADDRESS BLOCK

```
$ dnsdb_query -i 153.31.119.0/24 | grep -v infragard
vpn.dev2.leo.gov.           A  153.31.119.70
mail.leo.gov.               A  153.31.119.132
www.biometriccoe.gov.       A  153.31.119.135
www.leo.gov.                A  153.31.119.136
cgate.leo.gov.              A  153.31.119.136
www.infraguard.net.         A  153.31.119.138
infraguard.org.             A  153.31.119.138
www.infraguard.org.         A  153.31.119.138
mx.leo.gov.                 A  153.31.119.140
ic.fbi.gov.                 A  153.31.119.142
mail.ic.fbi.gov.            A  153.31.119.142
mail.ncijtf.fbi.gov.        A  153.31.119.142
```

TECHNICAL FORMATTING NOTES

- These slides show a DNS output conversion
  - The real output is in JSON format, i.e.:

```
$ dnsdb_query -r f.root-servers.net/a/root-servers.net
;; record times: 2010-06-24 03:10:38 .. 2014-03-05 01:22:56
;; count: 715301521; bailiwick: root-servers.net.
f.root-servers.net.  A  192.5.5.241

$ dnsdb_query -r f.root-servers.net/a/root-servers.net -j
{"count": 715301521, "time_first": 1277349038, "rrtype": "A",
"rrname": "f.root-servers.net.", "bailiwick": "root-
servers.net.", "rdata": ["192.5.5.241"], "time_last": 1393982576}
```

DNSDB DEPLOYMENT NOTES

- FSI Passive DNS sensor is open source (PCAP)
  - ‘dnstap’ is coming soon, for server embedding
- The FSI DNSDB API is open (now an IETF I-D)
  - FSI, 360.CN, NIC.AT, &others have servers
- FSI DNSDB is quasi-commercial:
  - Full grant for students (with advisor’s approval)
  - Partial grant for those who operate sensors for us
  - Commercially available for use, resale, embedding

LIMITED BIBLIOGRAPHY

https://www.farsightsecurity.com/

http://www.redbarn.org/dns/ratelimits

http://dnsrpz.info/

https://dnsdb.info/

https://dnstap.info/

DNS as a Defense Vector

Paul Vixie, Ph.D
CEO, Farsight Security