DNS as a Control Point for Cyber Risk

DR. PAUL VIXIE
Topics

- DNS Purpose and Role
- DNS Actions and Reactions
- DNS Control Points
Topic

DNS PURPOSE AND ROLE
The Internet as a Territory

• 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 (a layer) is: DNS
DNS As A Map

• Most everything we do on the Internet...
  – B2C Web, B2B Web, E-mail, I-M,
  – ...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
  – Sadly, the criminals came along for the ride
• Criminals can’t do Internet crime 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

- Domain names are grouped into zones
- A zone has one or more name servers
- Each name server has one or more addresses
- Other domain names also have addresses
- IP addresses are grouped into netblocks
- Domain names appear in a lot of places:
  - E-mail – somebody@domain
Traditional DNS Forensics

• DNS lets anybody look up a <domain, type>
  – You get back the current set of resource records
  – But there’s no way to see the history
  – And, your query exposes your interest

• Whois lets you check ownership of a domain
  – But it is often forged or hidden
Topic

DNS ACTIONS AND REACTIONS
...Too Cheap to Meter

• SpamAssassin as a teaching tool
  – Dotted quads as spamsign
• RRP and EPP: solving “the .COM problem”
  – Running a race to the bottom
• Fluidity having only one purpose
  – 30 seconds? Really?
• Fitting Sturgeon’s revelation
  – “90% of is crap”
Takedown: Far-End Tactics

- 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
  - Kill all you want, we’ll make more
- Whack-a-mole as a Service (WaaS?)
  - Incrementalism breeds better criminals
Firewalls: Near-End Tactics

• If we can’t prevent it and takedown is hard...
  – ...our coping strategy is, fight on the threshold
• You can filter IP+port, URL, and now even DNS
  – But you can’t keep up with the churn
  – So, another outsourceable profit center!
• And you can’t afford manual configuration
  – So, firewall config now follows a pub-sub model
  – This predates Puppet et al by a decade or more
DNS Control Points

ATTRIBUTION
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
vix.com. NS ns1.isc-sns.net.

;; record times: 2013-10-18 06:30:10 .. 2014-02-28 18:13:10
```
### Owner Wildcards, Left Hand

```bash
$ 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
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
cat.lah1.vix.com.            A 24.104.150.225
vix.com.                     A 24.104.150.231
ns.lah1.vix.com.             A 24.104.150.234
```
Owner Wildcards, Right Hand

$ dnsdb_query -r vixie./*/ns

;; zone times: 2010-08-13 16:10:10 .. 2012-12-31 17:24:50
;; count: 872; bailiwick: com.

;; zone times: 2010-04-24 16:12:21 .. 2010-08-12 16:09:01
;; count: 111; bailiwick: com.

;; zone times: 2010-10-20 20:52:43 .. 2012-03-31 20:54:04
;; count: 0; bailiwick: info.
vixie.info. NS ns31.domaincontrol.com.
vixie.info. NS ns32.domaincontrol.com.
^C
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.
toomanydatasuns.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
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}
```
DNS Control Points

DDOS RESISTANCE WITH DNS-RRL
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 and NSD 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.
Spoofed Source Attacks

attacker

Botted server, in the cloud, Gigabit speed

target

reflector

Internet

Src addr: (target)

Dst addr: (target)
RRL In Action: Afilias
DNS Control Points

DNS FIREWALLS WITH DNS-RPZ
Response Policy Zones: High Level

- 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
- Pay other publishers, or create your own
  - Or do both, plus a private white-list
- Simple failure or walled garden, as you choose
  - We call this “taking back the streets” (“the DNS”)

February 3, 2015
RPZ Capabilities

Triggers (RR owners):

– If the query name is $X
– If the response contains an address in CIDR $X
– If any name server name is $X
– If any name server 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
    o E.g., import Cymru Bogons or Spamhaus DROP list
  – Block DNS records in your own address space
    o After allowing your own domains to do so, of course
RPZ Status

• Implications:
  – Controlled Balkanization
  – Open market for producers and consumers
  – Differentiated service at a global scale
  – Instantaneous takedown

• Deployment:
  – The RPZ standard is open and unencumbered
  – So far implemented only in BIND
  – Performance is pretty reasonable
  – New features will be backward compatible
  – This is not an IETF standard
DNS Control Points

NEWLY OBSERVED DOMAINS (NOD) AN RPZ AND RHSBL FEED
Newly Observed Domains

• 60% of the spam we studied used a header or envelope domain name less than 24 hours old
• Most new domains are rapidly taken down
• Casa Vixie uses a 10 minute NXDOMAIN rule
• FSI NOD (5m, 10m, 30m, 1h, 3h, 6h, 12h, 24h) – Streams: newly active vs. newly observed – Feeds: RPZ (for DNS Firewalls) vs. RHSBL (for Spam Assassin)
Key Takeaways

• Criminals can’t do Internet crime without DNS
• DNS – including Passive DNS – provides global visibility on online criminal infrastructures
• Passive DNS is a valuable tool for security analysts – adds real-time and historical context for today’s threat feeds
• DNS RPZ and DNS RRL are examples of taking control of your own DNS server, to prevent it from becoming an accomplice to online crime.
• Learn more: New FSI whitepaper: *Passive DNS For Threat Intelligence*