WHOSE DNS IS IT, ANYWAY?

2017-06-21 – PAUL VIXIE, FARSDIGHT
OWNERSHIP

• Right to use and/or dispose
• E.g.: our computers, our networks, our time
INTERNET IS NOT OWNABLE

- **Internet is a cooperative asset**
- **Created by all who use it**
- **Cooperation can be withheld**
ECONOMICS OF DIGITAL DEFENSE

- Let $n$ be the number of assets to be defended
- Let $m$ be the size of a minimum effective defense team
- Let $Q$ be the benefit of a successful attack
- Let $P$ be the cost of a successful attack

- $n \times m > q - p$
INTERNET SCALE REPUTATION SYSTEMS

• Small number of analysts
• Large number of defenders

• Therefore M.A.P.S., and the R.B.L., created in 1996 or so
  • ProtecteS M.T.P. (email) servers against spammy initiators
  • Changed the game for everybody
INNOVATION ECONOMICS AND THE I.O.T.

A = time to market
D = time to first competitor
S = time to commodity
R = time to obsolescence

Area under the curve = revenue

(Credit: Tom Furlong, DEC, 1989)
LESSONS OF M.A.P.S. R.B.L.

- The economics worked, but N had to be “dozens”, not “1”
- Anti-trust law, and economics of “discovery”, were decisive
- E-mail is a dying industry, protecting only that is useless
- Selective withholding of cooperation worked and still does
SO: RESPONSE POLICY ZONES (R.P.Z.)

- SMALL NUMBER OF ANALYSTS (DOZENS OR HUNDREDS)
- LARGE NUMBER OF DEFENDERS (THE WHOLE INTERNET?)
- POLICY NOT REPUTATION
- MECHANISM NOT CONTENT
- DOMAIN NAME SYSTEM (D.N.S.) NOT E-MAIL SPECIFICALLY
R.P.Z. TRIGGERS AND ACTIONS

• On a domain name
• On an address response
• On an initiator’s address
• On a name server’s name
• On a name server’s address

• Send NXDOMAIN
• Send NODATA
• Send a CNAME
• Send replacement data
• Send truncation signal
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 DNS records in your own address space**
    • *After allowing your own domains to do so, of course*
IMPLICATIONS OF RPZ

- Controlled Balkanization
- Open market for producers and consumers
- Differentiated service at a global scale
- Instantaneous far-end takedown
R.P.Z. DEPLOYMENT STATUS

- The RPZ standard is open and unencumbered
- Implemented in BIND, Unbound, Knot, PowerDNS
- Performance is pretty reasonable (~5% of CPU)
- New features will be backward compatible
- This is not an IETF standard (yet)
A WORD ABOUT RPZ VS. SOPA
THE END (FOR NOW)

• **FURTHER READING:**
  - [https://deeptought.isc.org/article/AA-00525/](https://deeptought.isc.org/article/AA-00525/)
  - [https://lists.redbarn.org/mailman/listinfo/DNSfirewalls](https://lists.redbarn.org/mailman/listinfo/DNSfirewalls)
  - [http://dnssrpz.info/](http://dnssrpz.info/)

• **DISCUSS!**