Taking Back the DNS with Response Policy Zones

Paul Vixie, ISC
HITB 2010

Overview

- Motivation for DNS Response Policy Zones
- Relationship to DNS RBL (DNSBL)
- RPZ Constraints and Goals
- RPZ Design Details
- RPZ Future Directions
- Conclusion

Motivation for DNS RPZ

- Most new and many existing domain names are nonuseful (infospam, malevolent, etc)
- Owners of useless domains depend on the Global (cooperative) DNS for their success
- No method exists for withholding cooperation for these domain names or their owners
- Differentiated cooperation is necessary

Relationship to MAPS RBL (DNSBL)

- In 1996, the first DNS-based SMTP reputation system was created at Vixie Enterprises
- This was published by MAPS (Vixie and Rand) and was the first Realtime Blackhole List (RBL)
- Now 15 years later, hundreds of RBL providers protect virtually all Internet SMTP servers
- With DNS RPZ, we (ISC) intend to repeat this success, but this time protecting RDNS servers

RPZ Constraints and Goals

- The goal of DNS RPZ is a global technology standard and market for publication/subscription of DNS reputation information
- Must be unencumbered by patents or licenses, and available in many RDNS implementations
- Mustn't generate new wide area DNS traffic or make RDNS more fragile / less robust / slower
- Must not directly facilitate NXDOMAIN remapping or any other form of DNS pollution

RPZ Design Details (1)

- Subscribing RDNS servers are made a stealth secondary for response policy zone(s) (RPZs)
- TSIG is used to control access and authenticity
- NOTIFY is used to ensure timeliness of updates
- IXFR is used to compress updates into deltas
- An RDNS can subscribe to more than one RPZ and if so they are searched in order, per query
- RDNS operators can use a mix of private and public RPZs, using search order for precedence

RPZ Design Details (2)

- At an RPZ apex, there is an SOA (used to control IXFR and negative cache TTL) and an NS (which is never used)
- RPZs are never queried and so need not be delegated by their parents nor have globally unique names
- Linkage from RDNS to RPZ is by configuration
  - ```
    response-policy {
            zone "dns-policy.vix.com";
            zone "rpz.deteque.com";
    };
    ```
    ```

RPZ Design Details (3)

- Policy data uses rehomed global names and some special RDATA patterns for control:
  - To force an NXDOMAIN:
    - `wide.ad.jp.@ CNAME .`
  - To force a NODATA:
    - `wide.ad.jp.@ CNAME *.`
  - To end the search early:
    - `wide.ad.jp.@ CNAME wide.ad.jp.`
  - To force a specified answer:
    - Use any normal RR, including CNAME

RPZ Design Details (4)

- Note that `wide.ad.jp.@` would match only `wide.ad.jp`, not subdomains – so maybe also add `*.wide.ad.jp.@`
- There is no way to do NXDOMAIN remapping with RPZ since processing happens before recursion

RPZ Future Directions

- RPZ can be revised by adding new patterns which are invisible to prior RDNS implementations
- Next feature will be IP4/IP6 reputation support:
  - Triggered by response data, not by query name
  - So, `27.0.150.104.24._ip4.@` would match any “A” RRset matching 24.104.150.0/27
  - Likewise `64.0.0.0.0.cb.8000.559.2001._ip6.@` would match any “AAAA” RRset in 2001:559:8000:cb::/64
  - Similarly `._ns4.@` and `._ns6.@` to match NS addresses
  - Finally, `._nsn.@` will match NS names
  - There is still (deliberately) no way to match NXDOMAIN

Conclusion

- ISC's role in RPZ is to create a new global capability for the information security market
- ISC's unique capability is to implement this in BIND, making it instantly real and viable
- ISC will not be producing any RPZ data, we will leave that to the security vendor community
- ISC expects our Security Information Exchange (SIE) to be useful to such security vendors
- Questions and comments always welcomed!

Passive DNS and ISC SIE

Paul Vixie, ISC

Passive what?

- When a “full resolver” (caching, recursive) gets a question it cannot answer from cache
  - query is forwarded to the best known authority (root, TLD, SLD, etc)
  - response is eventually received, cached for reuse, and sent back to original asker
- In “Passive DNS”, these responses from authority servers are also collected, stored, and analyzed
  - no “personally identifiable information” here

Uses for Passive DNS

- Detect security problems
  - known-bad address used under a new name
  - known-bad name has a new address
  - many other exotic possibilities
- Analyze and characterize the D. N. System
  - what is it really being used for?
  - what does it really contain?
- Reconstruct the visible parts of distant zones
  - look, ma! no zone transfers!

History

- Florian Weimar invented this concept
- Implementation in academia
  - GNU ADA, Berkeley DB
  - Sensors in European ISPs & Universities
  - Original intent: zone content recovery
- Used today by world wide LEO community
- “Inverse directory” & botnet hunting
  - what names map to “this” address?
  - when was “this” name first used and by whom?
  - who has looked up “this” botnet C&C name?

Hazards of Decentralization

- Every new passive DNS effort has to solicit sensors (instrumented recursive NS)
- Due to ops+BW costs, few sensors can feed more than one passive DNS system
- Thus, sensor population is heavily diluted
- ➔ Perhaps a central solution is warranted?

Hazards of Commercialization

- Huge datamining opportunity for spammers
- There might be some problems, though:
  - National privacy laws
  - ISP privacy policies
  - Competitors getting hold of it
- → Perhaps a trusted nonprofit could help?

Proposed Solution: ISC SIE

- PCAP-based data capture tool (NCAP)
  - similar to tcpdump and dnscap
- Lightweight relationship for sensor operators
  - get and install the free/open sensor software
  - exchange security keys
  - upload batches using SSH/SFTP
- Central collector operated by ISC
  - receives batches, rebroadcasts on a LAN
  - each passive DNS project sits on that LAN

Roles and Responsibilities

- Sensor operator – instruments a nameserver to collect incoming authoritative responses and share them via ISC SIE
- ISC Security Information Exchange – receive collected response data and share it in real time with Passive DNS projects
- Passive DNS projects – get to hear all kinds of interesting collected response data, and study/analyze it