Response Policy Zones

Taking Back the DNS, V2.0

Paul Vixie
Chairman and Chief Scientist
Internet Systems Consortium

Abstract

DNS works as well for the bad guys (criminals, spammers, spies) as for respectable citizens, and the bad guys are taking better advantage of DNS's resiliency and distributed autonomy.

Something has got to be done. ISC is doing it.

RPZ 2.0 is part of BIND 9.8.0
(now at Beta 1)

Problem Statement

- DNS is a decentralized system offering complete distributed autonomy, and the relationships between operators and content owners are both tenuous and resilient.
- The split registry/registrar/registrant model insulates all parties from responsibility, so the global DNS lacks accountability – complaints are ineffective, even with provable crime/losses.
- This resiliency and unaccountability is of greater benefit to bad actors than their victims.

Historical Context

- DNS is not unique in its unaccountability. Most Internet systems (mail, blogs, I-M) are similar.
- In e-mail it's extremely common to subscribe to an DNSBL (realtime blackhole list) in order to reject messages from known-bad sources.
- Features similar to DNSBL exist for DNS in proprietary products (Nominum) and services (OpenDNS).
- RPZ (ISC Response Policy Zone) is an open standard for DNSBL-like features in the DNS.

RPZ History

- RPZ 1.0 released as patches to BIND9 in 2010:
  - Rule-based system, triggered on query name/type
  - Rule-forced outcomes:
    - Return a fake alias (CNAME), for walled gardens
    - Return a fake NXDOMAIN, to blackout the name
    - Return a fake answer of the type being queried
    - Protect the name against subsequent policy triggers
  - Subscription model: recursive name servers would become stealth servers for one or more RPZs.
  - Rules/outcomes encoded as RPZ zone content.

Lessons Learned From RPZ 1.0

- Sometimes the trigger has to be answer-based
  - E.g., if the A or AAAA RR is within a CIDR block
  - E.g., if the NS name or address is poisoned
- Sometimes the subscriber wants to import the triggers but locally specify the policy outcome
  - E.g., import a list of bad names, but decide locally whether to blackout or alias those names
- We have implemented some of these features in RPZ Format 2, released in BIND 9.8.0 (B1).

RPZ Content Examples (1)

- If rpz.net is a response policy zone and example.com is a name to be blacked out:
  - example.com.rpz.net CNAME .
- If all subdomains of example.com are to be aliased to a local walled garden:
  - *.example.com.rpz.net CNAME wg.mydom.cn
- If www.example.com/A should be redirected:
  - www.example.com A 198.168.6.66

RPZ Content Examples (2)

- If www.partner.com is to be protected from any policy action by any subsequent RPZ:
  - www.partner.com.rpz.net CNAME www.partner.com
- If www.example.com is to appear to be empty:
  - www.example.com.rpz.net CNAME *.
- If a A RRs in 192.168.1.0/24 are to be replaced with a local walled garden address:
  - 24.0.1.168.192.rpz-ip.rpz.net A 192.168.6.66

RPZ Content Examples (3)

- If AAAA RR's in 2001:500:2f::/48 ought to cause fake NXDOMAIN responses, except 2001:500:2f::f which is to be returned as normal:
  - 128.f.zz.2f.500.2001.rpz-ip.rpz.net CNAME *.
  - 48.zz.2f.500.2001.rpz-ip.rpz.net CNAME .
- Note: “zz” in this context means “::”.

Subscriber Configuration in BIND9

```
options {
    // other stuff
    response-policy {
         zone "dns-policy1.vix.com";
         zone "dns-policy2.vix.com" policy given;
         zone "dns-policy3.vix.com" policy NO-OP;
         zone "dns-policy4.vix.com" policy NXDOMAIN;
         zone "dns-policy5.vix.com" policy NODATA;
         zone "dns-policy6.vix.com" policy CNAME walled-garden.isp.net;
    };
};
zone “dns-policy1.vix.com” {
    type slave;
    masters { 192.168.1.123; };
    // note: TSIG would probably be used in a production environment
};
// and similar for the other rpz zones
```

Producer/Consumer Model in RPZ

- Producers can use RFC 2136 “UPDATE” to maintain their zone, or just periodically regenerate it and use “ixfr-from-differences” to tell BIND to compute deltas.
- Producers will use IXFR for efficient zone delta transmission, and TSIG for protection of RPZ data and authenticity of producer/consumer endpoints.
- Result: low cost, low bandwidth, low latency, and strong data protection.

Possible Good

- Specialization of labour: security experts can produce robust and targetted patterns for use by customer DNS recursive name servers.
- Competition: many security experts, many name server implementors (not just BIND!), and a global market of potential customers.
- Effect on crime: a domain or IP address used only for evil will not remain usable even if its registrant, registrar, registry, or ISP never suspends or terminates it.

Possible Harm

- Governments could use RPZ to enforce laws about censorship, since it is an open standard.
- Some RPZ data sources will inevitably be politically, racially, or religiously motivated (“all Christian web sites” or “all Muslim web sites”).
- As with all reputation systems, the systemic effect on DNS will be to make it less reliable and harder to diagnose or characterize.
- We hope these effects will be more pronounced on bad actors than on the rest of us.

Resources

- Questions and comments always welcome:
  - vixie@isc.org
- There is a mailing list for RPZ discussions:
  - dnsrpz-interest-request@lists.isc.org
- The current draft RPZ specification:
  - ftp://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt
- The blog post that started it all:
  - Google “vixie taking back the dns”