BUILDING DNS FIREWALLS WITH RESPONSE POLICY ZONES

2019-05 – Paul Vixie, Farsight

Abstract

- Throughout recorded history, criminal actors have taken by force or fraud the resources required for life and comfort. In the Internet era this force and fraud includes using the victim's own resources against them, whether in the form of botnets, credential theft, or shared infrastructure such as the Domain Name System (DNS). It is both possible and necessary to deny criminal actors the ability to use the world's shared DNS infrastructure against us. One way to do this is with DNS Firewalls which can participate in shared policy controls which enumerate in real time criminal DNS assets. Such systems must be voluntary, privately controlled, and in some cases, free for subscribers. The DNS Response Policy Zone (RPZ), invented by Schryver and Vixie in 2010, will be described as an example of a community-wide response to criminal DNS threats.

Firewalls generally

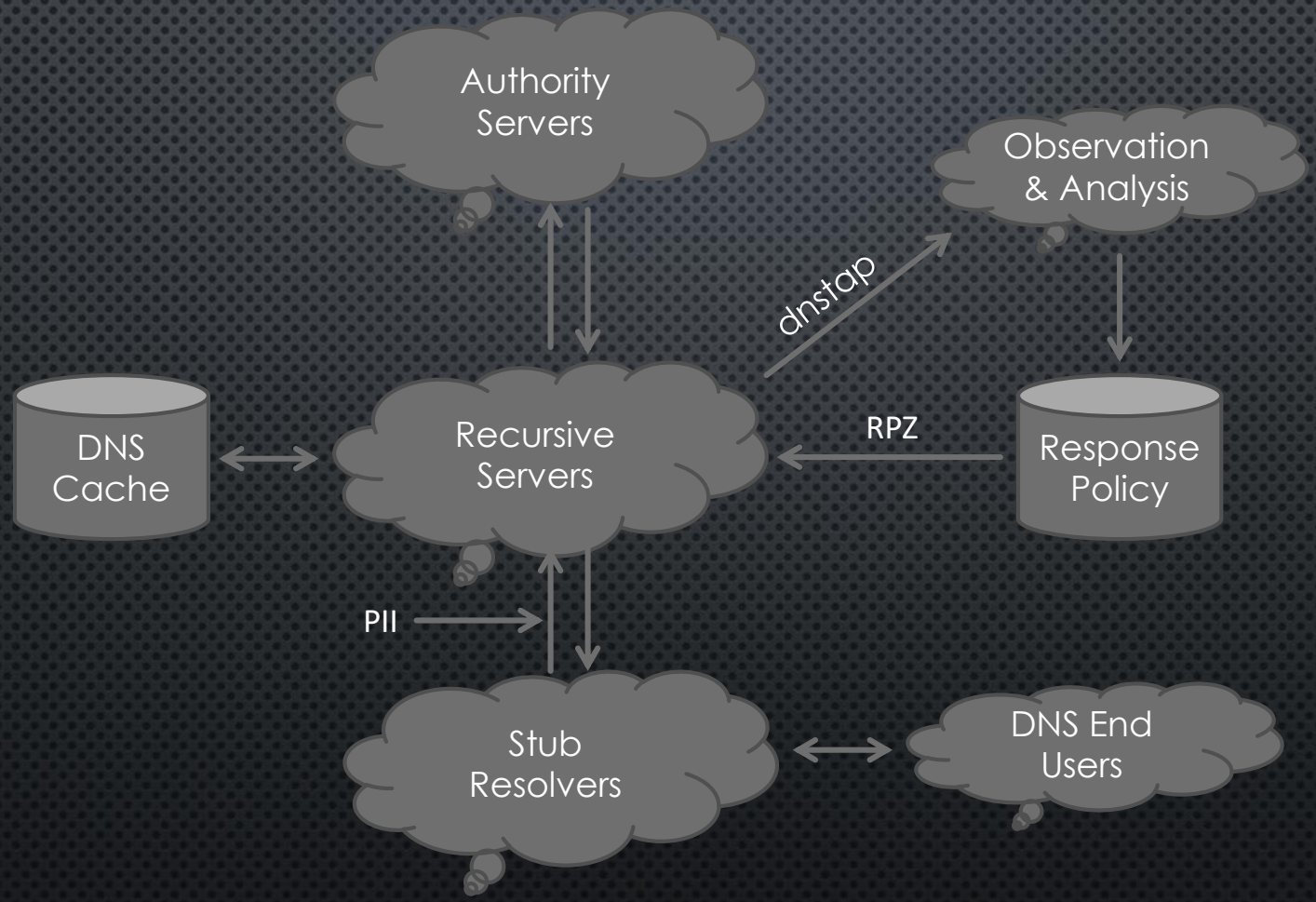
- Sits in the path of traffic
- Allows some things through, denies the rest
  - Or: denies some things, allows the rest
- Usually organized as: { *trigger* → *action* } …

DNS FIREWALLS

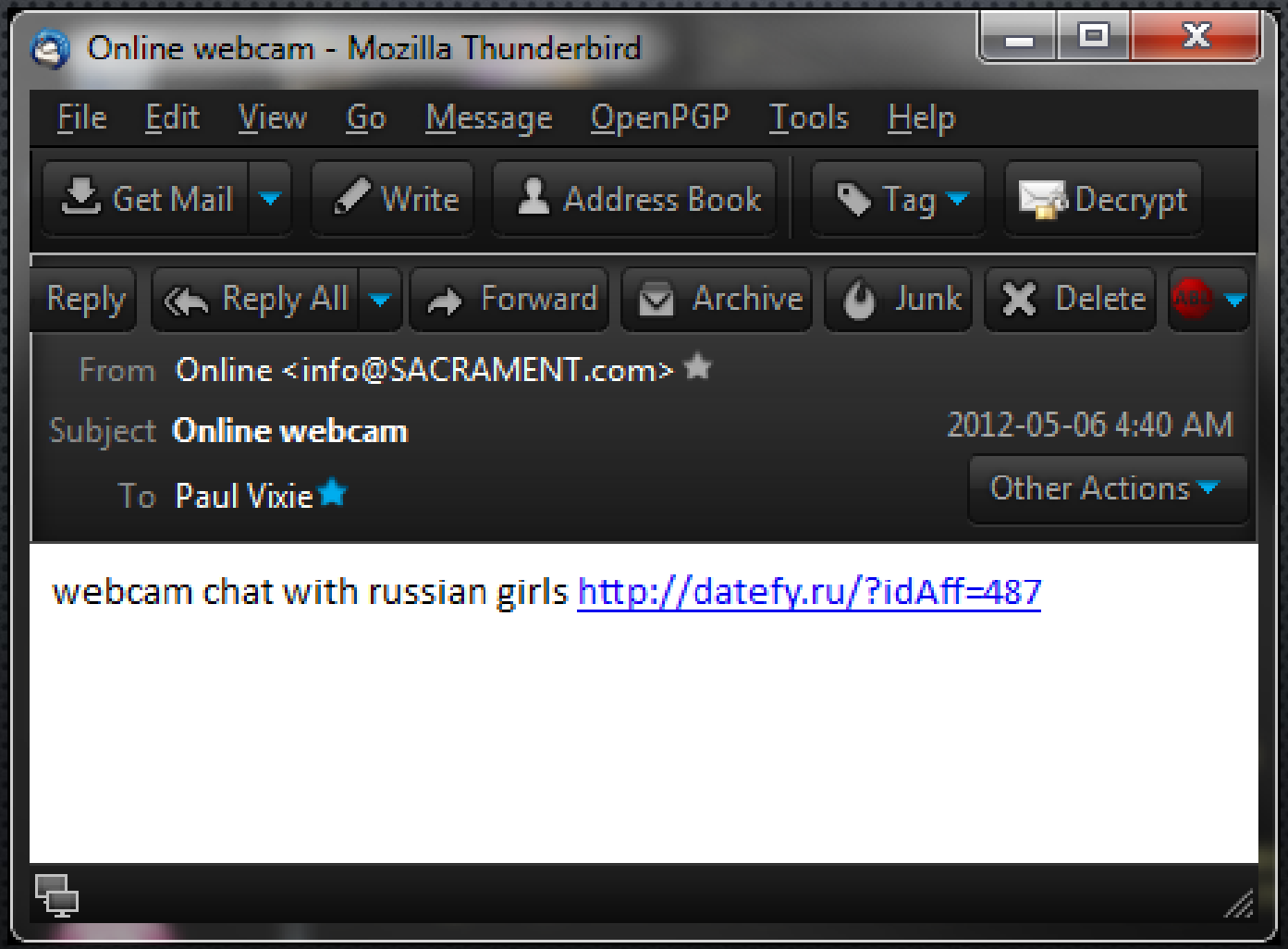
- DNS has a data path:
  - authority → recursive → stub
- We can allow or deny various kinds of traffic
- We can also replace data in real time
  - …which will redirect end users and applications

Response Policy Zones

- First universal standard for DNS firewall policy
  - Vixie & Schryver, 2009
- We carry DNS firewall rules inside DNS zones
  - …thus the name, RPZ
- Rules are published, subscribed, shared, by normal DNS zone transfer protocol
  - Including IXFR, NOTIFY, TSIG
  - So, propagation is timely, efficient, and authentic


Authority Servers
Observation & Analysis
dnstap
DNS Cache
Recursive Servers
RPZ
Response Policy
PII
Stub Resolvers
DNS End Users

WHAT YOU SEE


Online webcam - Mozilla Thunderbird
File Edit View Go Message OpenPGP Tools Help
Get Mail
Write
Address Book
Tag
Decrypt
Reply
Reply All
Forward
Archive
Junk
Delete
From Online <info@SACRAMENT.com>
Subject Online webcam
2012-05-06 4:40 AM
To Paul Vixie
Other Actions
webcam chat with russian girls http://datefy.ru/?idAff=487

WHAT YOU GET

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 55994
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;datefy.ru.                    IN      A

;; ADDITIONAL SECTION:
rpz.surbl.org.          180     IN      SOA     dev.null. \
        zone.surbl.org. 1337502508 180 180 604800 180

;; Query time: 1 msec
;; SERVER: 2001:4f8:3:30::3#53
```

HOW IT WORKS

```
options {
        directory "/var/local/named";
        …
        recursion yes;
        notify yes;
        …
        response-policy {
                zone "dns-policy.vix.com";
                zone "rpz.surbl.org";
                zone "rpz.spamhaus.org";
        };
};
```

WHAT IT LOOKS LIKE

```
zone "rpz.surbl.org" {
    type slave;
    masters { 94.228.131.210; 94.228.131.211; };
    also-notify { 2001:559:8000:cb::2; 24.104.150.2;    # ss
                  2001:559:8000:ca::5e; 24.104.150.42;  # mol
    };
    file "sec/rpz.surbl.org";
};

...

$ dig @nsa rpz.surbl.org axfr | grep ^datefy
datefy.ru.rpz.surbl.org. 180    IN      CNAME   .
```

How you can use it

- RPZ Feeds
  - Subscribe to one or more internal/external feeds
  - Maybe build your own feed for internal use
  - Maybe offer your feed to external subscribers
- RPZ Rule Triggers
  - QNAME, RESPADDR, NSNAME, NSADDR, CLIENTADDR
- RPZ Rule Actions
  - NXDOMAIN, ALIAS, NOERROR, REPLACE, or BYPASS

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 takedown

RPZ DEPLOYMENT STATUS

- The RPZ standard is open and unencumbered
- Implemented for BIND, Unbound, Knot, PowerDNS
- Performance is pretty reasonable (~5% of CPU)
- New features will be backward compatible
- This is not an IETF standard (yet)

Actual steps

1. Learn the syntax and capabilities; check your name server features
2. Build an introductory RPZ for yourself; make it a hidden primary
3. Add this RPZ as a secondary zone on one/more RDNS servers
4. Ensure it blocks what it should, and doesn't what it shouldn't
5. Make a change, observe propagation effects
6. Look at your log files, make sure you log RPZ events
7. Put it into production, consider offering it to others
8. Look for security producers who publish in RPZ format
9. Add external RPZ's, watch logs, delete ineffective feeds; repeat

A WORD ABOUT RPZ VS. SOPA

Final Thoughts: DNS RPZ

- Flash! Bang! Action at a distance! (It's *fun!*)
- Further Reading:
  - http://www.circleid.com/posts/20100728_taking_back_the_dns/
  - https://deepthought.isc.org/article/AA-00525/
  - https://lists.redbarn.org/mailman/listinfo/DNSfirewalls
  - http://dnsrpz.info/