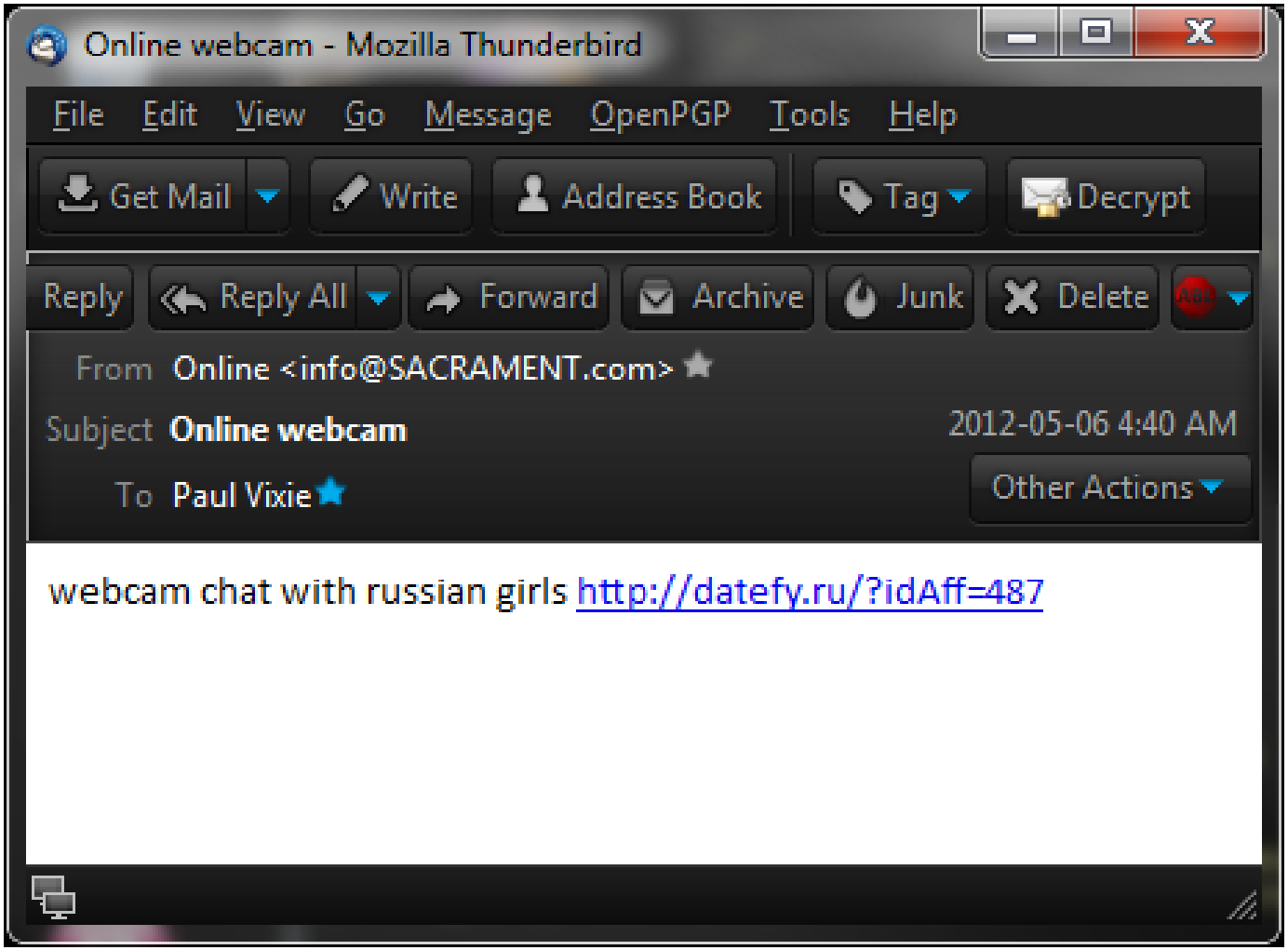
DNS RPZ In Action

Paul Vixie, ISC

DNS-OARC, Toronto

October, 2012

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: 1,\
       ADDITIONAL: 1

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

;; AUTHORITY 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";
        pid-file "/var/run/named-nsa.pid";
        query-source address 149.20.48.227 port *;
        listen-on-v6 { ::1; 2001:4f8:3:30::3; };
        listen-on { 127.0.0.1; 149.20.48.227; };
        recursion yes;
        notify yes;
        dnssec-enable yes;
        dnssec-lookaside . trust-anchor dlv.isc.org.;
        dnssec-validation 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 Patterns
  - Qname, Wildcard, RespAddr, NSName, NSAddr
- RPZ Rule Actions
  - NXDomain, Alias, NoError, Replace, or Bypass

Final Thoughts: DNS RPZ

- A Note About SOPA:
  - RPZ cannot be used to implement SOPA, since it will not interfere with DNSSEC-signed data that's being accessed by a DNSSEC-aware end user
- Further Reading:
  - http://www.circleid.com/posts/20100728_taking_back_the_dns/
  - https://deepthought.isc.org/article/AA-00525/
  - https://lists.isc.org/mailman/listinfo/dnsrpz-interest