Passive DNS

A Tool that is Making a Different to Track Down Badness

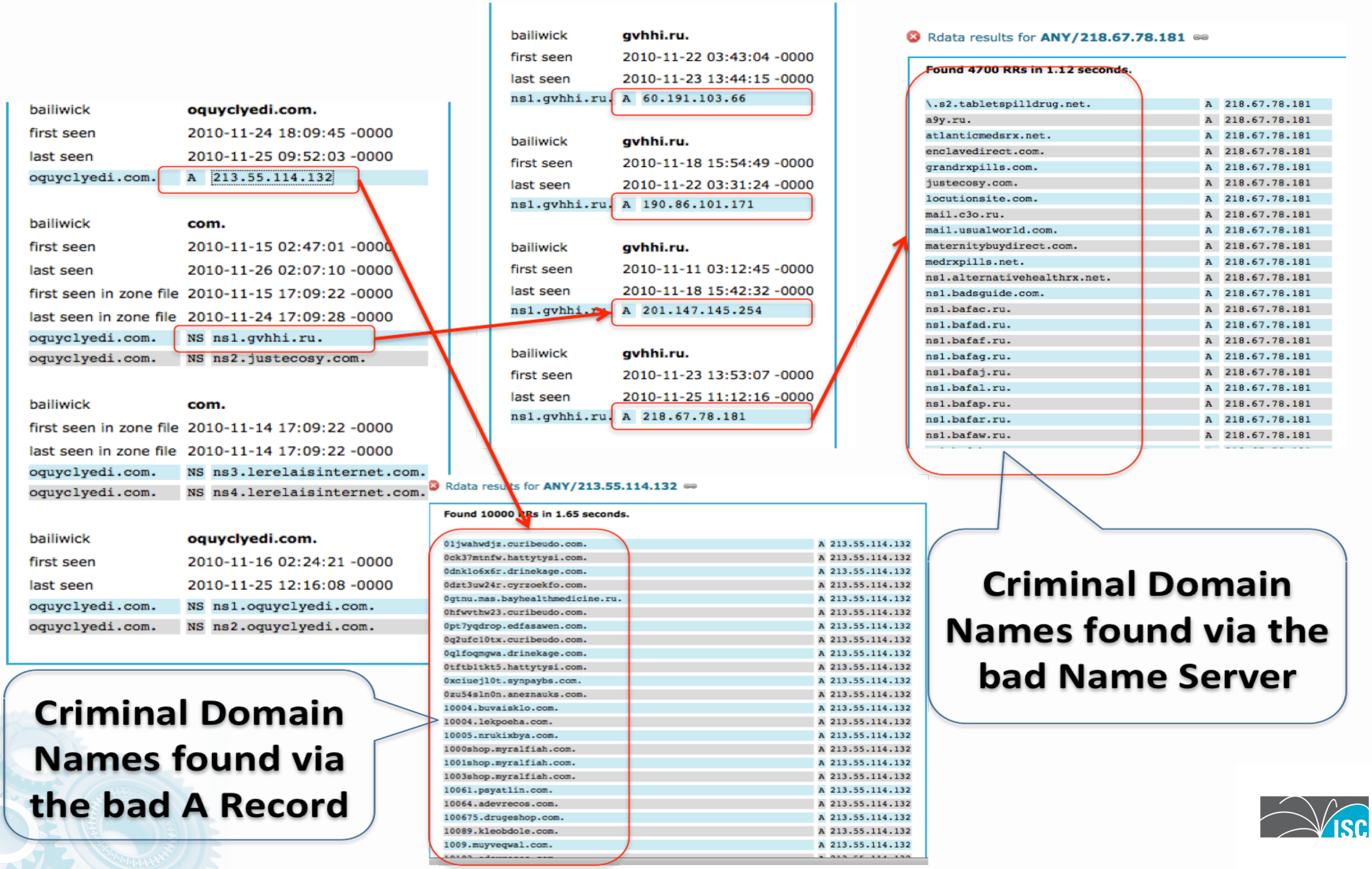
NANOG Lightening Talk in less than 10 minutes

Barry Greene
bgreene@isc.org

Please Participate

- We are looking for more providers to participate in our Passive DNS effort.
- Participation involves adding Passive DNS sensors to your DNS infrastructure.
- Participation protect the privacy of your customers.
- All data is aggregated, obscuring the source.
- Participants get access to the aggregate data for your own investigations.

Passive DNS – Tool to Find the Badness



```
bailiwick                oquyclyedi.com.
first seen               2010-11-24 18:09:45 -0000
last seen                2010-11-25 09:52:03 -0000
oquyclyedi.com.     A    213.55.114.132

bailiwick                com.
first seen               2010-11-15 02:47:01 -0000
last seen                2010-11-26 02:07:10 -0000
first seen in zone file  2010-11-15 17:09:22 -0000
last seen in zone file   2010-11-24 17:09:28 -0000
oquyclyedi.com.     NS   ns1.gvhhi.ru.
oquyclyedi.com.     NS   ns2.justecosy.com.

bailiwick                com.
first seen in zone file  2010-11-14 17:09:22 -0000
last seen in zone file   2010-11-14 17:09:22 -0000
oquyclyedi.com.     NS   ns3.lerelaisinternet.com.
oquyclyedi.com.     NS   ns4.lerelaisinternet.com.

bailiwick                oquyclyedi.com.
first seen               2010-11-16 02:24:21 -0000
last seen                2010-11-25 12:16:08 -0000
oquyclyedi.com.     NS   ns1.oquyclyedi.com.
oquyclyedi.com.     NS   ns2.oquyclyedi.com.
```

```
bailiwick        gvhhi.ru.
first seen       2010-11-22 03:43:04 -0000
last seen        2010-11-23 13:44:15 -0000
ns1.gvhhi.ru.  A  60.191.103.66

bailiwick        gvhhi.ru.
first seen       2010-11-18 15:54:49 -0000
last seen        2010-11-22 03:31:24 -0000
ns1.gvhhi.ru.  A  190.86.101.171

bailiwick        gvhhi.ru.
first seen       2010-11-11 03:12:45 -0000
last seen        2010-11-18 15:42:32 -0000
ns1.gvhhi.ru.  A  201.147.145.254

bailiwick        gvhhi.ru.
first seen       2010-11-23 13:53:07 -0000
last seen        2010-11-25 11:12:16 -0000
ns1.gvhhi.ru.  A  218.67.78.181
```

Rdata results for **ANY/218.67.78.181**

Found 4700 RRs in 1.12 seconds.

```
\.s2.tabletspilldrug.net.          A  218.67.78.181
a9y.ru.                            A  218.67.78.181
atlanticmedsrx.net.                A  218.67.78.181
enclavedirect.com.                 A  218.67.78.181
grandrxpills.com.                  A  218.67.78.181
justecosy.com.                     A  218.67.78.181
locutionsite.com.                  A  218.67.78.181
mail.c3o.ru.                       A  218.67.78.181
mail.usualworld.com.               A  218.67.78.181
maternitybuydirect.com.            A  218.67.78.181
medrxpills.net.                    A  218.67.78.181
ns1.alternativehealthrx.net.       A  218.67.78.181
ns1.badsguide.com.                 A  218.67.78.181
ns1.bafac.ru.                      A  218.67.78.181
ns1.bafad.ru.                      A  218.67.78.181
ns1.bafaf.ru.                      A  218.67.78.181
ns1.bafag.ru.                      A  218.67.78.181
ns1.bafaj.ru.                      A  218.67.78.181
ns1.bafal.ru.                      A  218.67.78.181
ns1.bafap.ru.                      A  218.67.78.181
ns1.bafar.ru.                      A  218.67.78.181
ns1.bafaw.ru.                      A  218.67.78.181
```

Rdata results for **ANY/213.55.114.132**

Found 10000 RRs in 1.65 seconds.

```
01jwahwdjz.curibeudo.com.              A 213.55.114.132
0ck37mtnfw.hattytysi.com.              A 213.55.114.132
0dnk1o6x6r.drinekage.com.              A 213.55.114.132
0dzt3uw24r.cyrzoekfo.com.              A 213.55.114.132
0gtnu.mas.bayhealthmedicine.ru.        A 213.55.114.132
0hfwvthw23.curibeudo.com.              A 213.55.114.132
0pt7yqdrop.edfasawen.com.              A 213.55.114.132
0q2ufc10tx.curibeudo.com.              A 213.55.114.132
0qlfoqmgwa.drinekage.com.              A 213.55.114.132
0tftb1tkt5.hattytysi.com.              A 213.55.114.132
0xciuej10t.synpaybs.com.               A 213.55.114.132
0zu54sln0n.aneznauks.com.              A 213.55.114.132
10004.buvaisklo.com.                   A 213.55.114.132
10004.lekpoeha.com.                    A 213.55.114.132
10005.nrukixbya.com.                   A 213.55.114.132
1000shop.myralfiah.com.                A 213.55.114.132
1001shop.myralfiah.com.                A 213.55.114.132
1003shop.myralfiah.com.                A 213.55.114.132
10061.psyatlin.com.                    A 213.55.114.132
10064.adevrecos.com.                   A 213.55.114.132
100675.drugeshop.com.                  A 213.55.114.132
10089.kleobdole.com.                   A 213.55.114.132
1009.muyveqwal.com.                    A 213.55.114.132
```

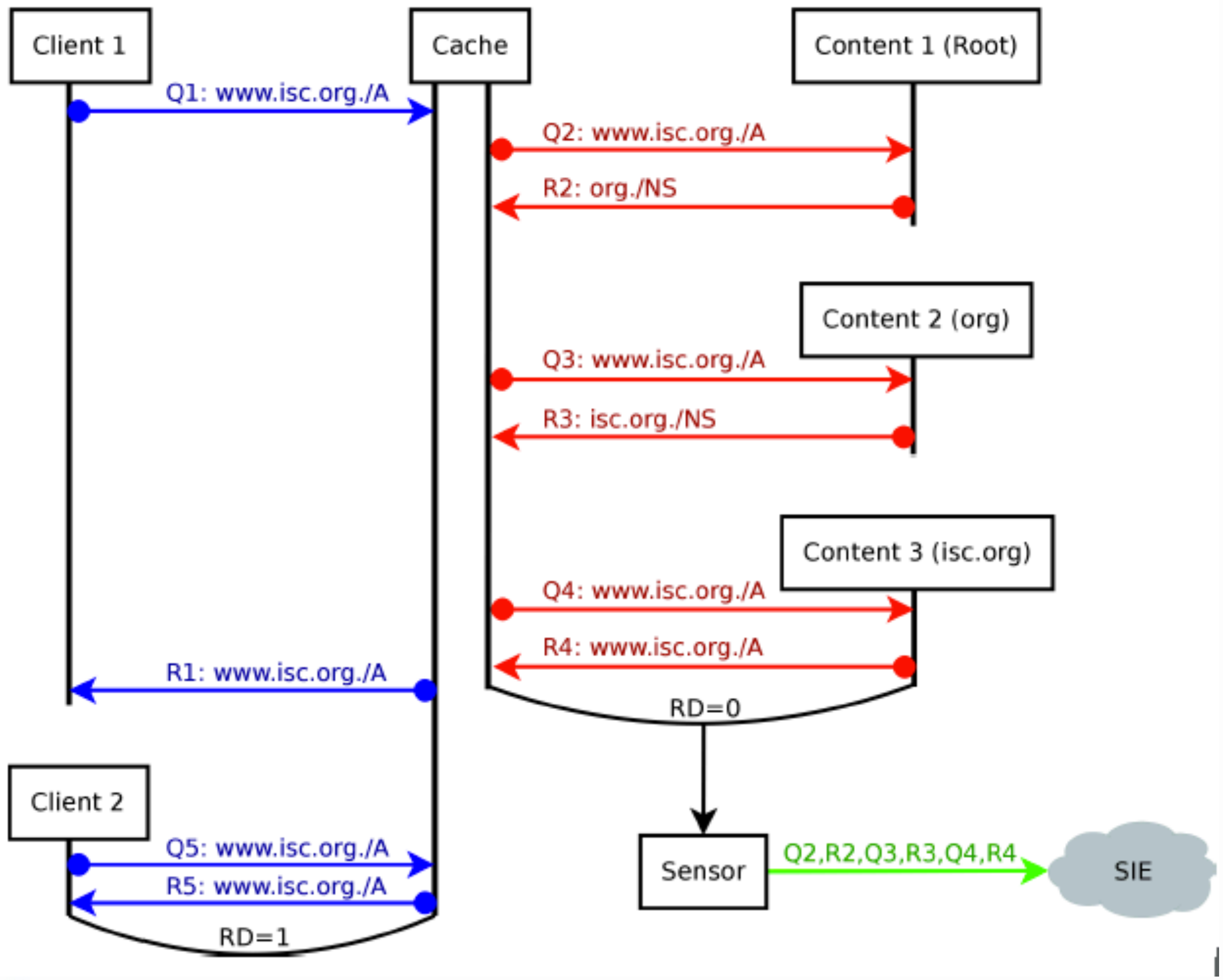
Criminal Domain Names found via the bad Name Server

Criminal Domain Names found via the bad A Record

Passive DNS

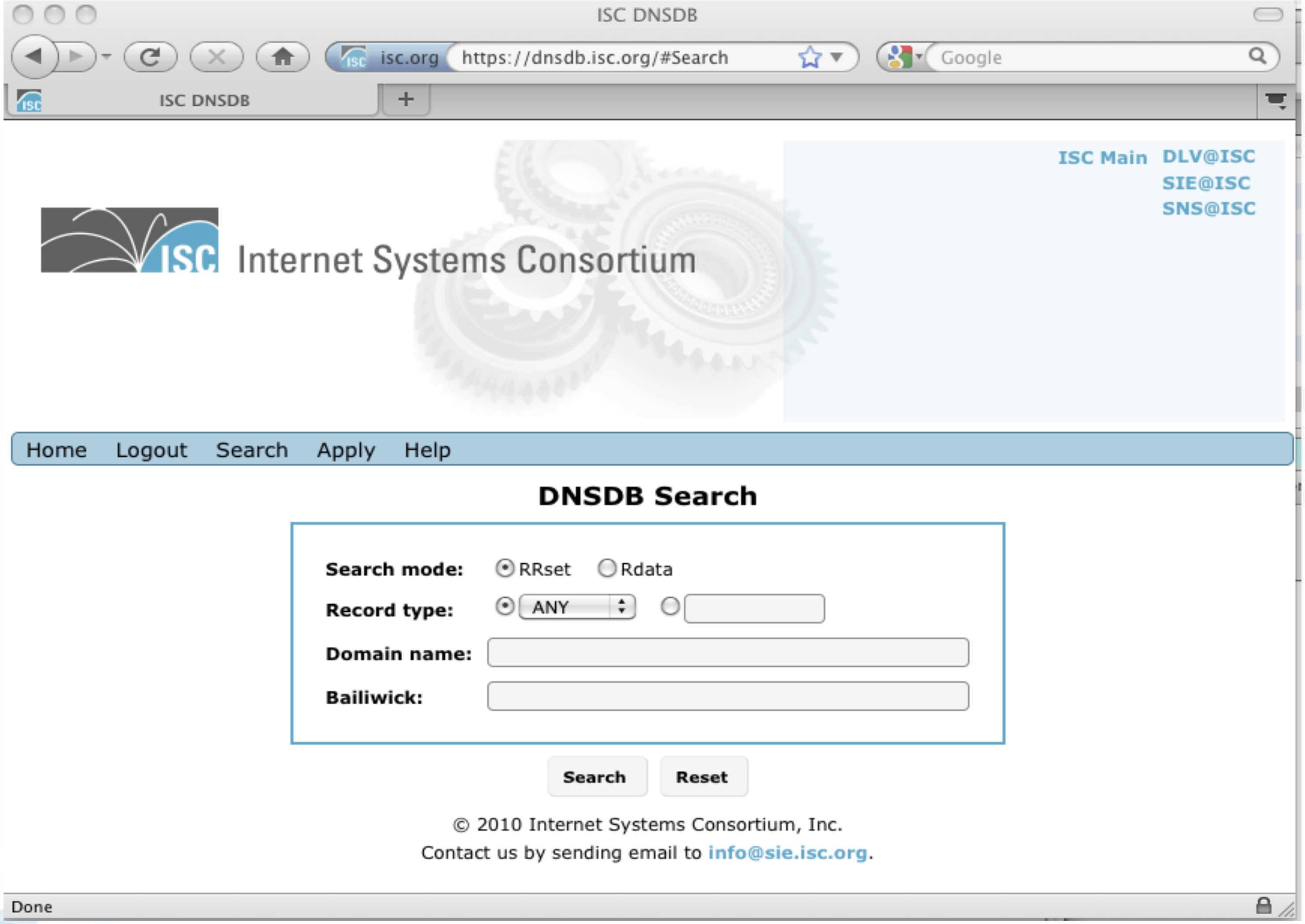
- Passive DNS replication is a technology invented in 2004 by Florian Weimer.
  - Many uses! Malware, e-crime, legitimate Internet services all use the DNS.
- Inter-server DNS messages are captured by sensors and forwarded to a collection point for analysis.
- After being processed, individual DNS records are stored in a database.

End User & Operator Privacy Protected



Not Collected **Collected**

DNS DB Demo



DNSDB Search

Search mode:	● RRset ○ Rdata
Record type:	● ANY ○
Domain name:	
Bailiwick:	

Search Reset

© 2010 Internet Systems Consortium, Inc.
Contact us by sending email to info@sie.isc.org.

Who Gets Access?

- Security Information Exchange (SIE) Peers (raw data).
- DNSDB User Interface (beta)
  - ✓ Vetted Member of the Operational Security Community
  - ✓ Passive DNS Contributors
  - ✓ SIE Peers
  - ✓ SIE Forum Members
- DNSDB API (beta)
  - ✓ Passive DNS Contributors
  - ✓ ISC Sponsored Researchers
  - ✓ SIE Peers
  - ✓ SIE Forum Members

How to Participate?

- Check out information at sie.isc.org.
  - ✓ Step 1 - Apply to contribute Passive DNS Data (Vetting)
  - ✓ Step 2 - Download SIE Passive DNS Software
  - ✓ Step 3 - Gain Credentials to allow you to submit Passive DNS Data
  - ✓ Step 4 - Configuring the SIE Passive DNS Sensor
  - ✓ Step 5 - Start feeding data into the SIE Passive DNS System
  - ✓ Step 6 - Use the benefits of Passive DNS to help with your own organization's security
- E-mail dnsdb@sie.isc.org