

PassiveDNS

João Damas
Internet Systems Consortium





The global leader in open source DNS

isc.org
Internet Systems Consortium

*We make the Internet
work better.*

BIND 10

The next
big thing
in DNS

ISC Professional Services

support development
training consulting
audit design

*Call in
the experts!*

SNS@ISC

The ultimate
insurance
policy for
your DNS

ISC is Public Benefit

F-root DHCP
SNS-PB AFTR
BIND and more

*Do what you can
to support us*

RPZ

New method for
DNS-based policy
enforcement

Taking back the DNS!

SIE

Changing how
the security
communities
productively
collaborate

You are here

RPKI

Securing BGP
from route
hijacking



Agenda

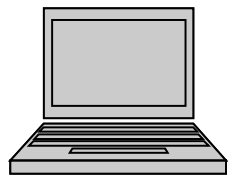
- Introduction to PassiveDNS
- How ISC does it
- Examples
- How to participate



History

- Invented by Florian Weimer in 2004
- Public efforts (RUS-CERT, BFK, DNSparse)
- Use PCAP-based tools (like tcpdump or dnscap) to capture packets, extract data, add to data base, develop query tool
- Used by security community and law enforcement to *passively* analyze associations between badness and the DNS or address resources they use.

How it works (1st client)



client 1



resolving
ns

caching
server

root ns

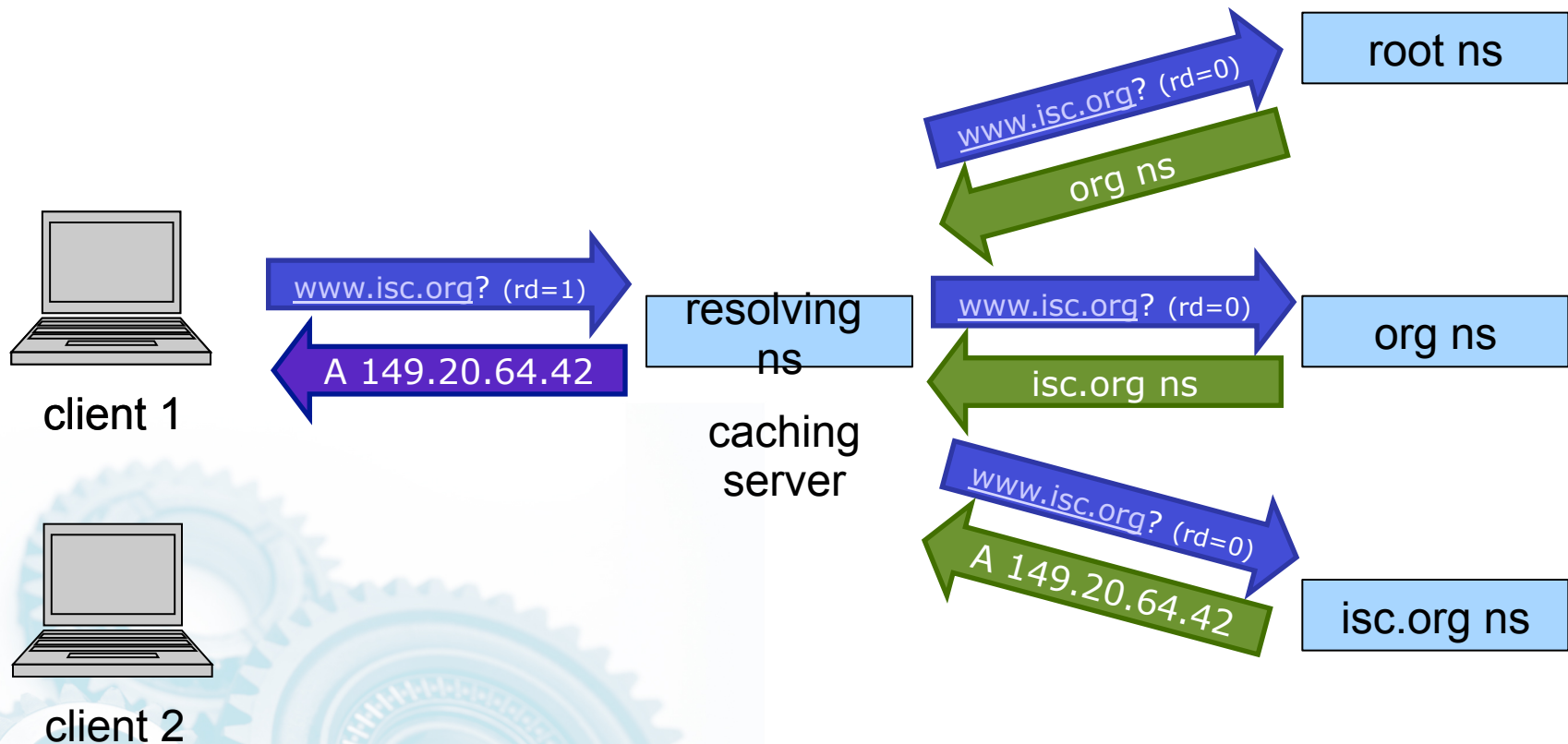
org ns

isc.org ns

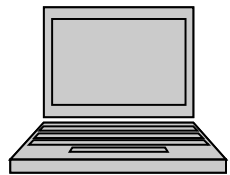


client 2

How it works (query/response)



How it works (2nd client)



client 1



client 2

resolving
ns

caching
server



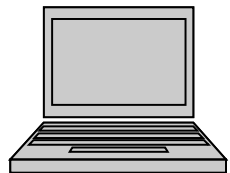
root ns

org ns

isc.org ns

Collection properties

**Personally
Identifiable
Information**

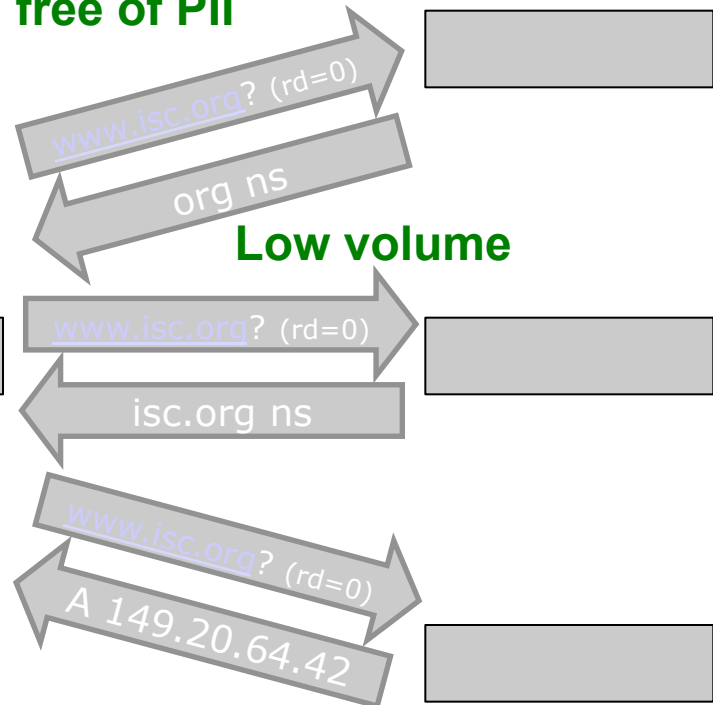


High volume



**Useful for finding
who is affected by
badness (like
infected clients)**

**Generally*
free of PII**



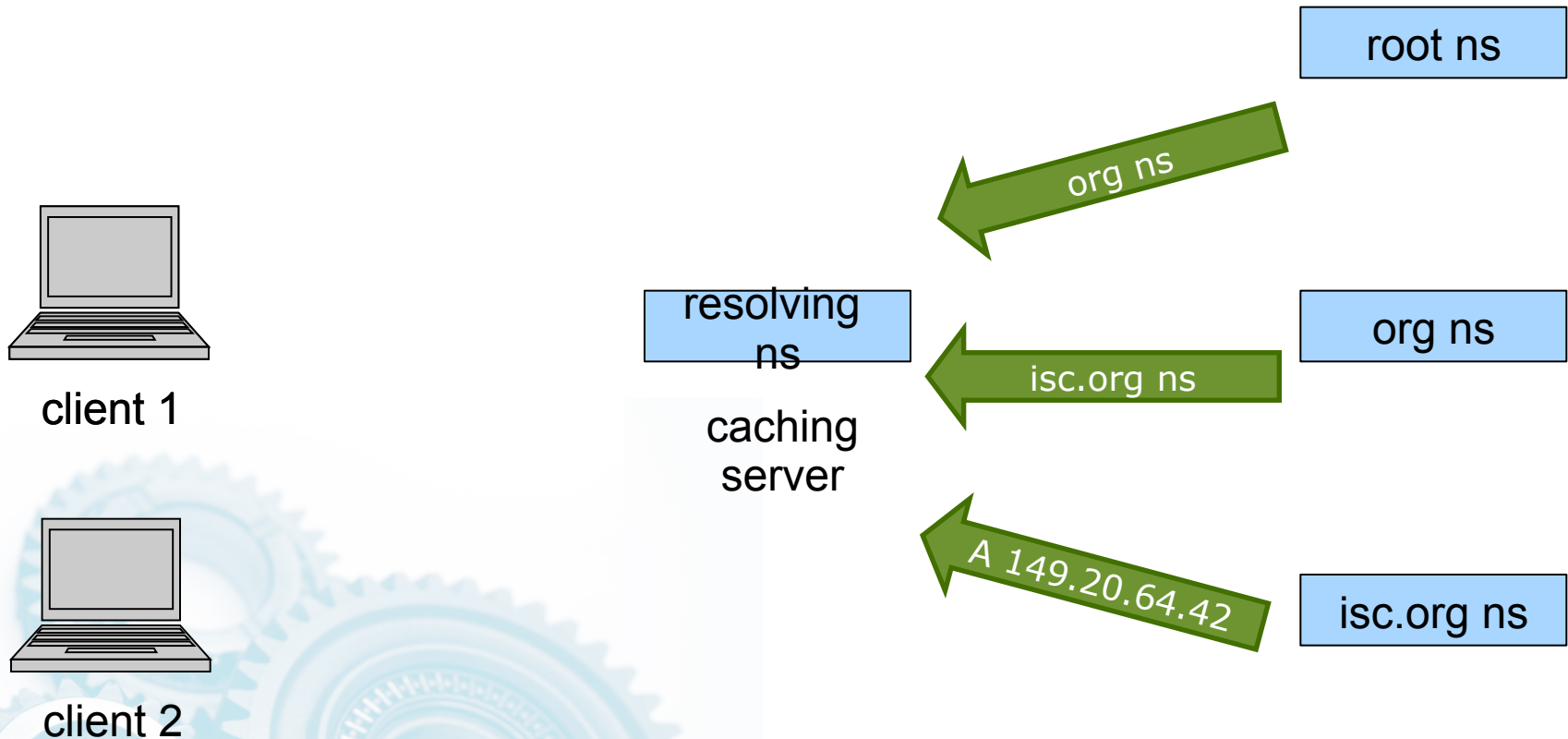
Low volume

**Useful for mapping
badness and
detecting changes**

ISC / SIE / DNSDB

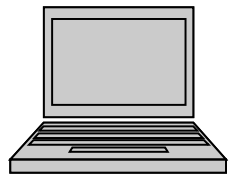
- ISC started in 2007
- Emphasis on high volume collection and near-real-time analysis
- Saw challenges in existing tools
 - Tool evolution
 - dnscap -> ncaptool -> nmsgtool
 - Scalable replication and processing
 - Data storage and access technologies

We like responses



... but that's not good enough.

Problems



client 1



client 2

resolving
ns

caching
server

ns

TCP fragments

ns

EDNS fragments

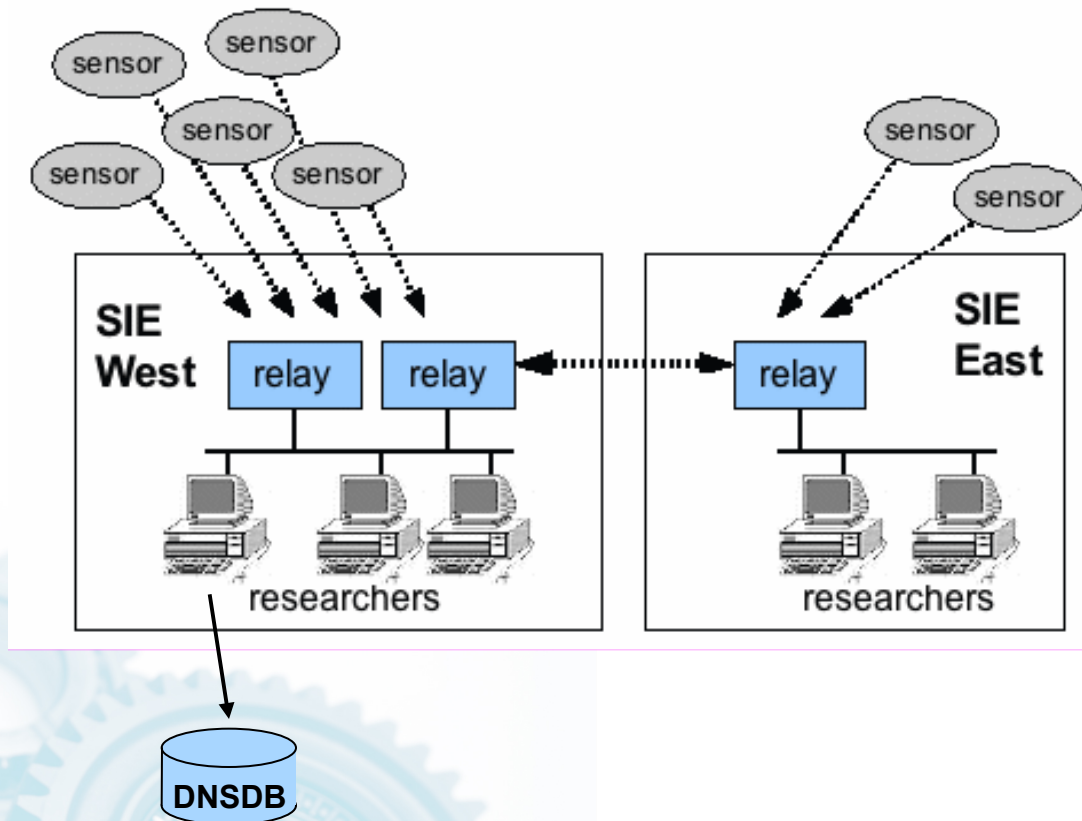
ns

incompatible
wire format

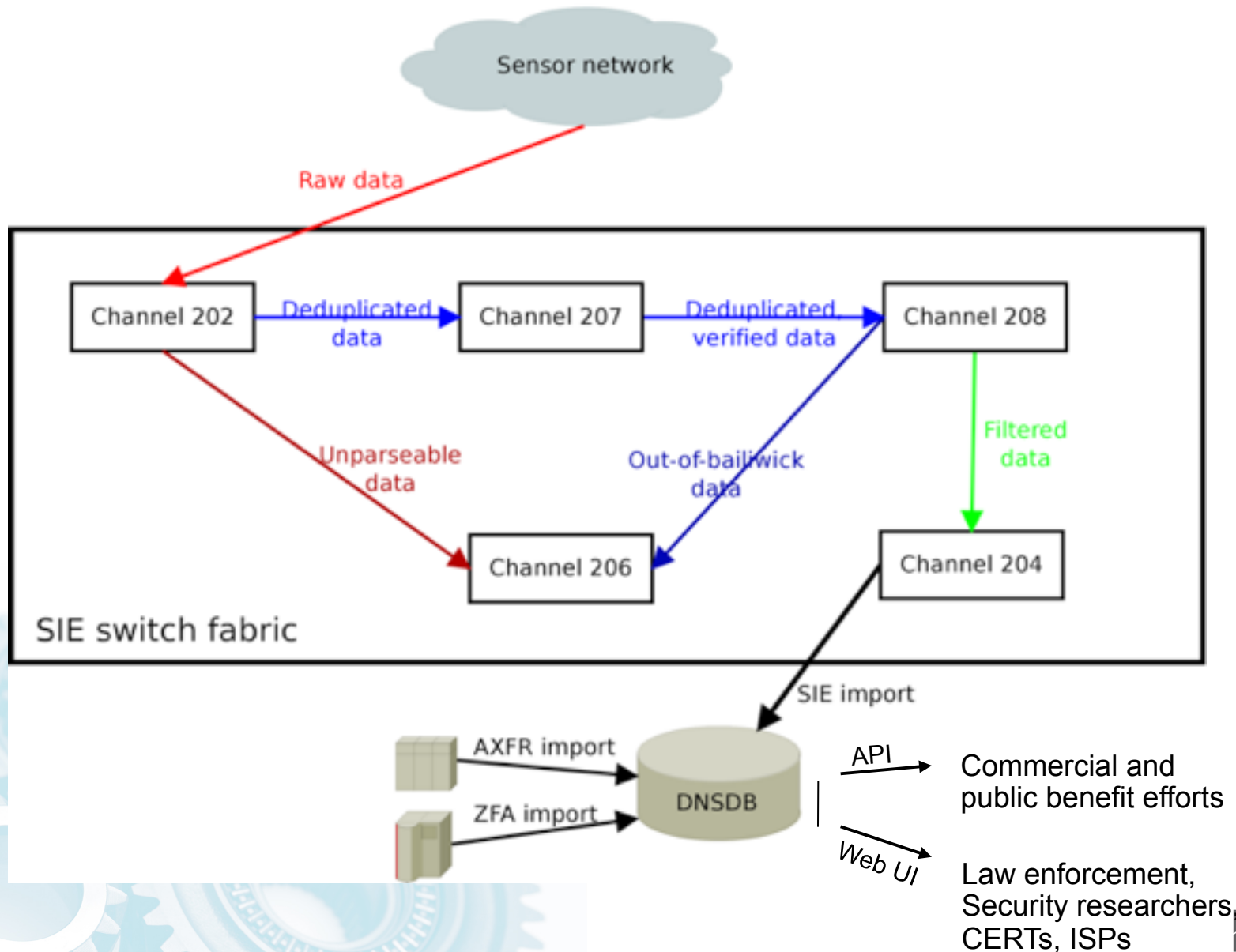
invalid or poison

bad guy

We built some infrastructure (SIE, DNSDB)



ISC Passive DNS and DNSDB architecture



More background

- Robert Edmonds, “Passive DNS Hardening”
 - Video: <http://bitly.com/IAJHVZ> (DEFCON 18, Jul 2010)
 - Slides: http://www.isc.org/files/passive_dns_hardening_handout.pdf
- ISC Webinar, “SIE & Passive DNS”
 - Video: <http://bit.ly/ilpr7k> (WebEx, Mar 2011)
 - Slides: https://www.isc.org/files/SIE&Passive%20DNS-2011-03-29_0.pdf
 - Note: Shows examples of how PassiveDNS data has been provided to and used by several research efforts.

Now some fun



Internet Systems Consortium

[ISC Main](#) [DLV@ISC](#)
[SIE@ISC](#)
[SNS@ISC](#)

[Home](#) [Login](#)

DNSDB Login

Username:
Password:

Login

© 2010-2011 Internet Systems Consortium, Inc.
Contact us by sending email to dnssdb@isc.org.



**Criminal Domain
Names found via
the bad A Record**

🔍 **Idata results for ANY/213.55.114.132** 🔍

```
Found 10000 logs in 1.63 seconds.
01:peahedje.oculibudo.com,
00k378n2wz.hattypai.com,
0dck10wkr.driskage.com,
0dsk70wkr.syrrewhf.com,
0g1ou.maa.bayhealthmedicine.ru,
0g1herthw23.oculibudo.com,
0g17yglp3.edfesaawen.com,
0g1fuf3f54.oculibudo.com,
0g1fouqpe.driskage.com,
0g1fbi0k53.hattypai.com,
0ac1ouj10t.syrrewhf.com,
0a3k4al0n.amenacha.com,
0004.borakiahe.com,
0004.lapomha.com,
0005.trakiskpe.com,
0006hup.myrafliah.com,
000iahup.myrafliah.com,
0006hup.myrafliah.com,
0006hup.myrafliah.com,
0061.papanlin.com,
0064.adevroms.com,
00673.drupeshup.com,
0069.klaodhce.com,
0069.myrrepaal.com,
```

Criminal Domain Names found via the bad Name Server

"... due to a hack at Betfair's registrar"

RRset results for **betfair.com/NS**

Found 4 RRsets in 0.00 seconds.

bailiwick	com.
count	50182
first seen	2010-06-24 03:16:46 -0000
last seen	2011-09-05 19:24:12 -0000
first seen in zone file	2010-08-01 16:09:07 -0000
last seen in zone file	2011-09-04 16:15:51 -0000
betfair.com.	NS udns1.ultradns.net.
betfair.com.	NS udns2.ultradns.net.
bailiwick	com.
count	17
first seen	2011-09-04 20:17:34 -0000
last seen	2011-09-04 21:40:24 -0000
betfair.com.	NS ns1.yumurtakabugu.com.
betfair.com.	NS ns2.yumurtakabugu.com.

DNSDB Search

Search mode: ☐ RRset ☒ Rdata

Record type: ☒ NS ☐

Record data:

Input mode: ☒ Name ☐ IP or network ☐ Raw hex

Search

Reset

Rdata results for **NS/ns1.yumurtakabugu.com**

Found 20 RRs in 0.02 seconds.

acer.com.	NS ns1.yumurtakabugu.com.
betfair.com.	NS ns1.yumurtakabugu.com.
cafe24.com.	NS ns1.yumurtakabugu.com.
cryjester.net.	NS ns1.yumurtakabugu.com.
dell.co.kr.	NS ns1.yumurtakabugu.com.
ec21.com.	NS ns1.yumurtakabugu.com.
filmsindirizle.com.	NS ns1.yumurtakabugu.com.
freegary.co.uk.	NS ns1.yumurtakabugu.com.
freegary.org.uk.	NS ns1.yumurtakabugu.com.
hsbc.co.kr.	NS ns1.yumurtakabugu.com.
militanz.com.	NS ns1.yumurtakabugu.com.
nationalgeographic.com.	NS ns1.yumurtakabugu.com.
ning.com.	NS ns1.yumurtakabugu.com.
seaorganization.com.	NS ns1.yumurtakabugu.com.
telegraph.co.uk.	NS ns1.yumurtakabugu.com.
theregister.co.uk.	NS ns1.yumurtakabugu.com.
ups.com.	NS ns1.yumurtakabugu.com.
vengajans.com.	NS ns1.yumurtakabugu.com.
vodafone.com.	NS ns1.yumurtakabugu.com.
yumurtakabugu.com.	NS ns1.yumurtakabugu.com.

ouch!

Zeus hunting (domains)

abuse.ch ZeuS Tracker

[Home](#) | [FAQ](#) | [ZeuS Blocklist](#) | [ZeuS Tracker](#) | [Removals](#) | [ZTDNS](#) *new!* | [Statistic](#) | [RSS F](#)

ZeuS Tracker :: IP address **173.213.76.149**

IP address: 173.213.76.149

Hostname: n/a

of ZeuS Hosts: **8**

of active files: **16**

SBL: [SBL116608](#)

AS number: [AS30693](#)

AS name: EONIX-CORPORATION-AS-PHX01-WWW-INFINITIE-NET - Eonix Corporation

Country:  [United States](#) (US)

Below is a list of all ZeuS Hosts which are currently hosted on this IP address.

Hosts on this IP address

Dateadded	CC	FU	Host	Status	Files online	Registrar	Nameserver
2011-09-05	CC		uitppyflfsnkpqid.info	online	2	Directi Internet Solutions Pvt	dns1.spi
2011-09-05	CC		jwdwlgqqgiwhxkt.com	online	2	GODADDY.COM, INC.	ns35.dor
2011-09-04	CC		vroxnpojiomtenlq.biz	online	2	NAMESECURE.COM, INC.	dns1.nar
2011-09-04	CC		jfpdsqirhsypqnn.org	online	2	NameSecure, L.L.C. (R58-LROR)	dns1.nar
2011-09-03	CC		krirfqmckkssgol.biz	online	2	NAMESECURE.COM, INC.	dns1.nar
2011-09-02	CC		aongrnernvqret.net	online	2	NAMESECURE.COM	dns1.nar
2011-09-02	CC		xqoyjkmnrhqmxyty.net	online	2	NAMESECURE.COM	dns1.nar
2011-09-02	CC		xsnnsynlsnfhklun.com	online	2	NAMESECURE.COM	dns1.nar

of Host on this IP address: **8**

DNSDB Search

Search mode: ☐ RRset ☒ Rdata

Record type: ☒ ANY ☐

Record data:

Input mode: ☐ Name ☒ IP or network ☐ Raw hex

Search

Reset

✓ ✗ Rdata results for **ANY/173.213.76.149** 

Found 13 RRs in 0.27 seconds.

aongrnernvqret.net.	A	173.213.76.149
gkoiqjyqmyjklqpv.info.	A	173.213.76.149
jfpdsqirhsypqnn.org.	A	173.213.76.149
jwdwlgqqgiwhxkt.com.	A	173.213.76.149
krirfqmckkssgol.biz.	A	173.213.76.149
llnepksnvvgllzrs.info.	A	173.213.76.149
outqrpskulndkxne.info.	A	173.213.76.149
ryqqfjhctkptirn.biz.	A	173.213.76.149
uitppyflfsnkpqid.info.	A	173.213.76.149
vroxnpojiomtenlq.biz.	A	173.213.76.149
www.jfpdsqirhsypqnn.org.	A	173.213.76.149
xqoyjkmnrhqmxyty.net.	A	173.213.76.149
xsnnsynlsnfhklun.com.	A	173.213.76.149

more domains



Zeus hunting (fast-flux)

RRset results for [indingo.ru/A](#) @ Rdata results for [ANY/63.226.215.202](#)

abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Removals | ZTDNS

ZeuS Tracker :: C&C indingo.ru

The list below shows all ZeuS configs, ZeuS binaries, ZeuS dropzones and I

Live Information

ZeuS C&C: **indingo.ru**

Additional Note: Hosted on a FastFlux botnet - ZeuS Tracker provides

A record	TTL	Spamhaus SB
125.88.110.49	300	LISTED
60.19.30.134	300	LISTED
60.19.30.135	300	LISTED
61.197.232.43	300	Not listed
67.209.65.212	300	Not listed

Level: 5 (Hosted on a FastFlux botnet)

Sponsoring registrar: [REGRU-REG-RIPN](#)

Nameserver(s): [ns1.freetgp.net](#) | [ns2.freetgp.net](#)

Date added: 2011-09-04

Last checked: 2011-09-05

Last updated: never

BL status: This host is being published on the [ZeuS Blocklist](#)

Found 275 RRsets in 0.05 seconds.

bailiwick **indingo.ru.**

count 93

first seen 2011-09-02 01:30:37 -00

last seen 2011-09-04 03:47:38 -00

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	78.156.156.185

bailiwick **indingo.ru.**

count 15

first seen 2011-09-02 12:26:03 -00

last seen 2011-09-05 00:03:46 -00

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	113.161.87.176

bailiwick **indingo.ru.**

count 119

first seen 2011-09-02 03:26:53 -0000

last seen 2011-09-05 13:18:36 -0000

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	125.88.110.49

Found 28 RRs in 0.07 seconds.

asfun.ru.	A	63.226.215.202
coolsofa.ru.	A	63.226.215.202
qutesin.ru.	A	63.226.215.202
earlyship.ru.	A	63.226.215.202
ebaliu.com.	A	63.226.215.202
eepeohothe.ru.	A	63.226.215.202
greatjazz.ru.	A	63.226.215.202
indingo.ru.	A	63.226.215.202
itchysauce.ru.	A	63.226.215.202
jupaizeuph.ru.	A	63.226.215.202
krufop.com.	A	63.226.215.202
lamewire.ru.	A	63.226.215.202
munaeghohz.ru.	A	63.226.215.202
nahwisohch.ru.	A	63.226.215.202
one5xz7rf6fb61afyhx.com.	A	63.226.215.202
paperrain.net.	A	63.226.215.202
secondconcert.ru.	A	63.226.215.202
toplake.ru.	A	63.226.215.202

... more domains
... more IP resources

One good spam deserves another...

RRset results for [despo.pharmacyramat.ru/ANY](http://despo.pharmacyramat.ru/)

Found 1 RRsets in 0.07 seconds.

bailiwick	pharmacyramat.ru.
count	33
first seen	2011-09-01 18:24:29 -0000
last seen	2011-09-05 19:06:38 -0000
despo.pharmacyramat.ru.	A 115.239.229.196
despo.pharmacyramat.ru.	A 122.224.18.23

Rdata results for ANY/115.239.229.196

Found 10000 RRs in 10.43 seconds.

1137.pfizer.ismedic.ru.	A 115.239.229.196
14dd.pfizer.medicac.ru.	A 115.239.229.196
2867.pfizer.ismedic.ru.	A 115.239.229.196
41.pfizer.medicac.ru.	A 115.239.229.196
4623.pfizer.ismedic.ru.	A 115.239.229.196
a.aawlj.cswfex.pfizer.medicac.ru.	A 115.239.229.196
a.abub37gzyut.pfizer.ismedic.ru.	A 115.239.229.196
a.acehdd.pfizer.medicac.ru.	A 115.239.229.196
a.acjol4xusw.pfizer.medicac.ru.	A 115.239.229.196
a.acquard.pfizer.medicac.ru.	A 115.239.229.196
a.ad81yahoo.de.pfizer.ismedic.ru.	A 115.239.229.196
a.atte.viniciol2d.pfizer.medicac.ru.	A 115.239.229.196
a.ayoka9.pfizer.ismedic.ru.	A 115.239.229.196
a.bschapter.pfizer.medicac.ru.	A 115.239.229.196
a.cadet001.pfizer.ismedic.ru.	A 115.239.229.196
a.calavera35.pfizer.medicac.ru.	A 115.239.229.196
a.califjoy.pfizer.ismedic.ru.	A 115.239.229.196
a.candy1669.pfizer.ismedic.ru.	A 115.239.229.196

[162] [2011-09-06 05:31:35.#####] [1:2 ISC email]
type: spamtrap
srchost: 117.yyy.yy.yyy
bodyurl: hxxp://Despo.pharmacyramat.ru/?xxxxxxxxxxxxxxx
... redirects to "hxxp://www.medicostb.com/"

TOP SALE Viagra from USD 0.90 p...

We ship worldwide USD EUR CAD GBP CHF AUD JPY BRL MXN NZD
+1-800 642-1061

Pharmacy Express
#1 ONLINE WORLDWIDE DRUGSTORE

USPS Fast Delivery
Shipping to USA in 1-4 days

Free Del
> 7 year
> 100%
> Hig
> 2

Main About us F.A.Q. Our policies Track my order Yo

Search...

Browse by:

Letter

A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z

Category

ED Packs SALE -15%
Herbal ★
Most Popular ★
Allergy
Anthelmintics

New! The best and cheapest herbal pills
Herbal medications are absolutely safe and high-quality. Without any doubts you can buy Herbal products and your health problems will be solved in the right way! Herbal pills consist of 100 % natural ingredients. So, you won't be bothered by unpleasant side effects. If you decided to buy any Herbal medications we sure you won't be disappointed with its splendid and quickest results.

100% NATURAL

Cialis Pack Save 15%
USD 4.37 USD 3.71 per pill
Cialis 20mg
Cialis Professional 20mg
Cialis Super Active 20mg
Select pack
More info

Viagra + Cialis + Levitra Save 15%
USD 3.52 USD 2.99 per pill
Viagra 100mg
Cialis 20mg
Levitra 20mg
Select pack
More info

Active Pack

DNSSDB API

```
$ DNSDB_FORMAT=json isc-dnsdb-query rdata ip 192.0.32.10 | sort
{"rrtype": "A", "rrname": "example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "example.org.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mal1.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "mail2.gbs-clan.de.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "scribble.co.uk.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.com.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.edu.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.net.", "rdata": "192.0.32.10"}
{"rrtype": "A", "rrname": "www.example.org.", "rdata": "192.0.32.10"}
```

... for programmed lookups and cross-references and search.
... gets around web browser javascript limitations.

... using API with last example

```
$ dig medicostb.com ns
```

```
medicostb.com.          169386      IN      NS
```

```
    ns1.upsdns.com.ua.
```

```
medicostb.com.          169386      IN      NS
```

```
    ns2.dnsaq.ru.
```

```
$ ( for f in `isc_dnsdb_query.py -n ns1.upsdns.com.ua/NS | \
    awk '{print $1}'`; do isc_dnsdb_query.py -r $f -j | \
    egrep 'time_last": 1315[12]'; done) | awk '{print $8}' | sort -u
```

```
"healthtr.com.",
```

```
"medicacpr.ru.",
```

```
"medicannk.com.",
```

```
"mediccker.ru.",
```

```
"mediccklr.ru.",
```

```
"medicehok.com.",
```

```
"medicelcr.ru.",
```

```
"medicellk.com.",
```

```
"medicemur.ru.",
```

```
"medicheek.com.",
```

```
"medichmar.ru.",
```

```
...etc...
```

Other uses

- Look up what names are hosted on your networks (by CIDR).
- Look at what is hosted around CIDR a bulletproof hosting site.
- Look for delisted domains and watch them move around.
- Look at DNSSEC history for domains.
- Look at IPv6 utilization.
- Look at resources hosted by dynamic

Who gets access?

- Security Information Exchange Peers
- DNSDB User Interface (beta)
 - Vetted member of Operational Security community
 - Passive DNS contributors
 - SIE forum members
 - SIE peers
- DNSDB API (beta)
 - Passive DNS contributors
 - ISC Sponsored Researchers
 - SIE Peers
 - SIE Forum members

How to participate?

- Check out information at <https://sie.isc.org>
 - Apply to contribute Passive DNS data
 - Download sie-dns-sensor software
 - Gain credentials to allow you to submit PassiveDNS data
 - Configure the sensor software
 - Start feeding data
 - Use benefits of PassiveDNS to help with you own organization's security – get a UI or API account
- E-mail: dnssdb@isc.org