SIE, PassiveDNS, and data combining

ENOG, June 2011

Eric Ziegast / Shane Kerr
<info@sie.isc.org>

Agenda

- About ISC SIE
- Passive DNS and DNSDB
- Data analysis and combining examples
- How to participate

The global leader in open source DNS

isc.org
Internet Systems Consortium

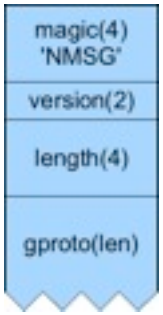
Shane Kerr

You are here

The Security Information Exchange (SIE) is ...

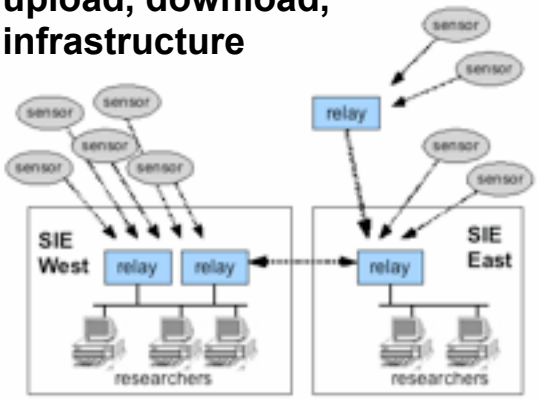
Efficient bi-lateral peering and multi-lateral sharing within a common legal/privacy framework

Common software, protocols and extensible binary data formats



NMSG

Exchange, relay, VPN, upload, download, infrastructure



Passive DNS Replication and Analysis

DNSDB

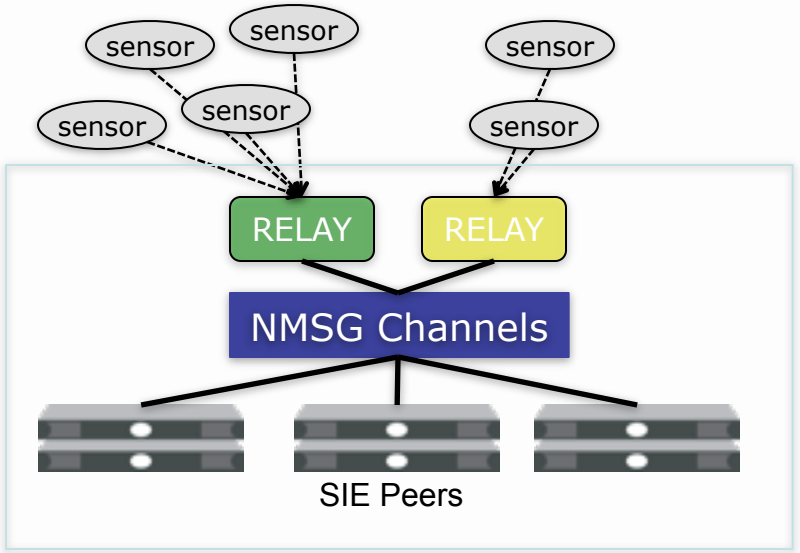
I/SDRN – Scaling security data collection within service providers

DNS RPZ – Standardizing DNS-enabled enforcement for security policy

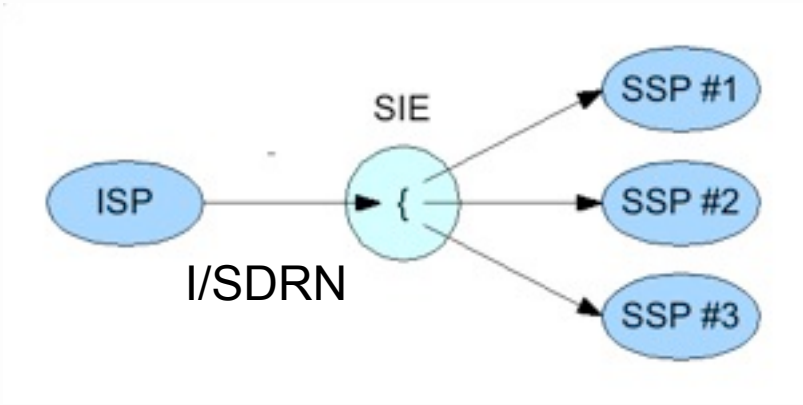
More background information on SIE & NMSG, 12/2009:
http://www.youtube.com/watch?v=f4oH7TIqFnY

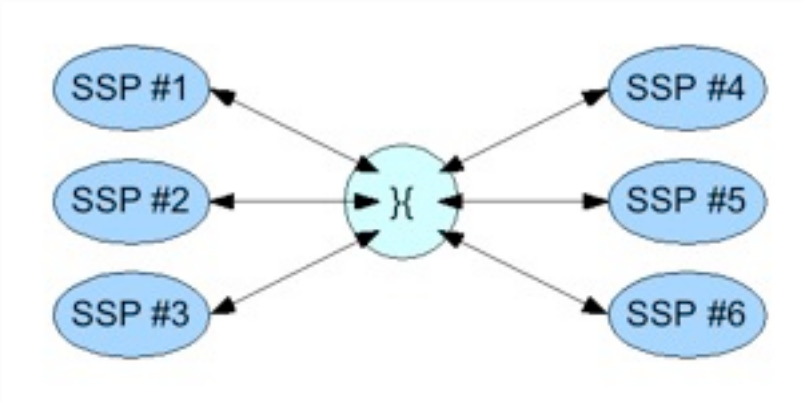
SIE "Channels"

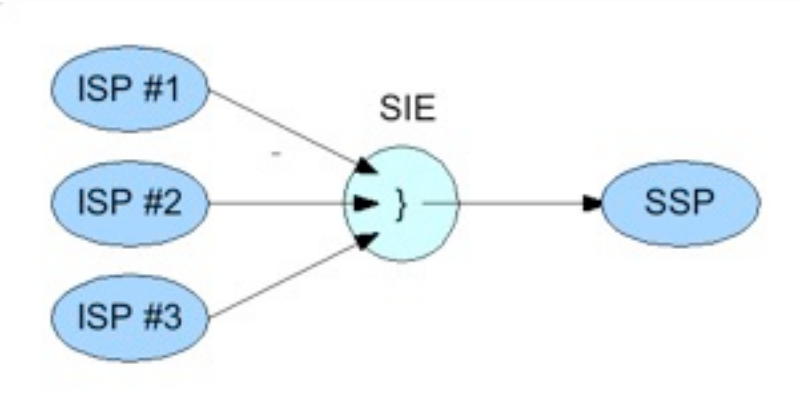
- SIE used "channels" as the term for peers who are connected to a "port" to subscribe to a data flow.
- There are several types of channels – which are all variants of "private channels":
  - **Community Channels** – multilateral peering, open to any who connect to a port (ISC channels will be converted to Multilateral Community Channels).
  - **Private Channels** – bi-lateral, multi-lateral, and commercial exchange between the SIE constituents.
  - **Incident Channels** – created to provide data during an incident – carries specific distribution rules.



SIE Efficiencies





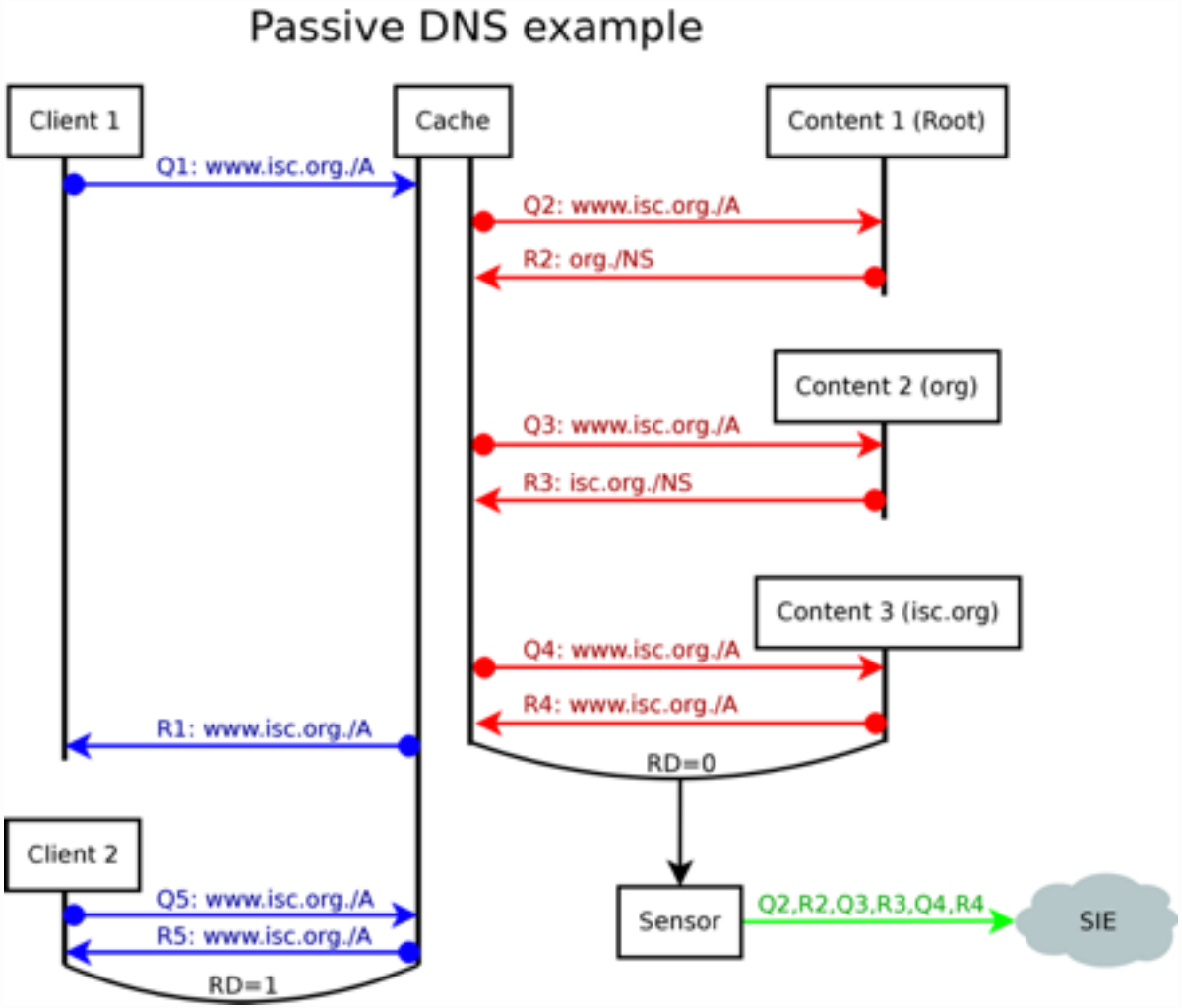


PassiveDNS

FIRST 2005, Florian Weimer

http://www.enyo.de/fw/software/dnslogger/#2

How Passive DNS works



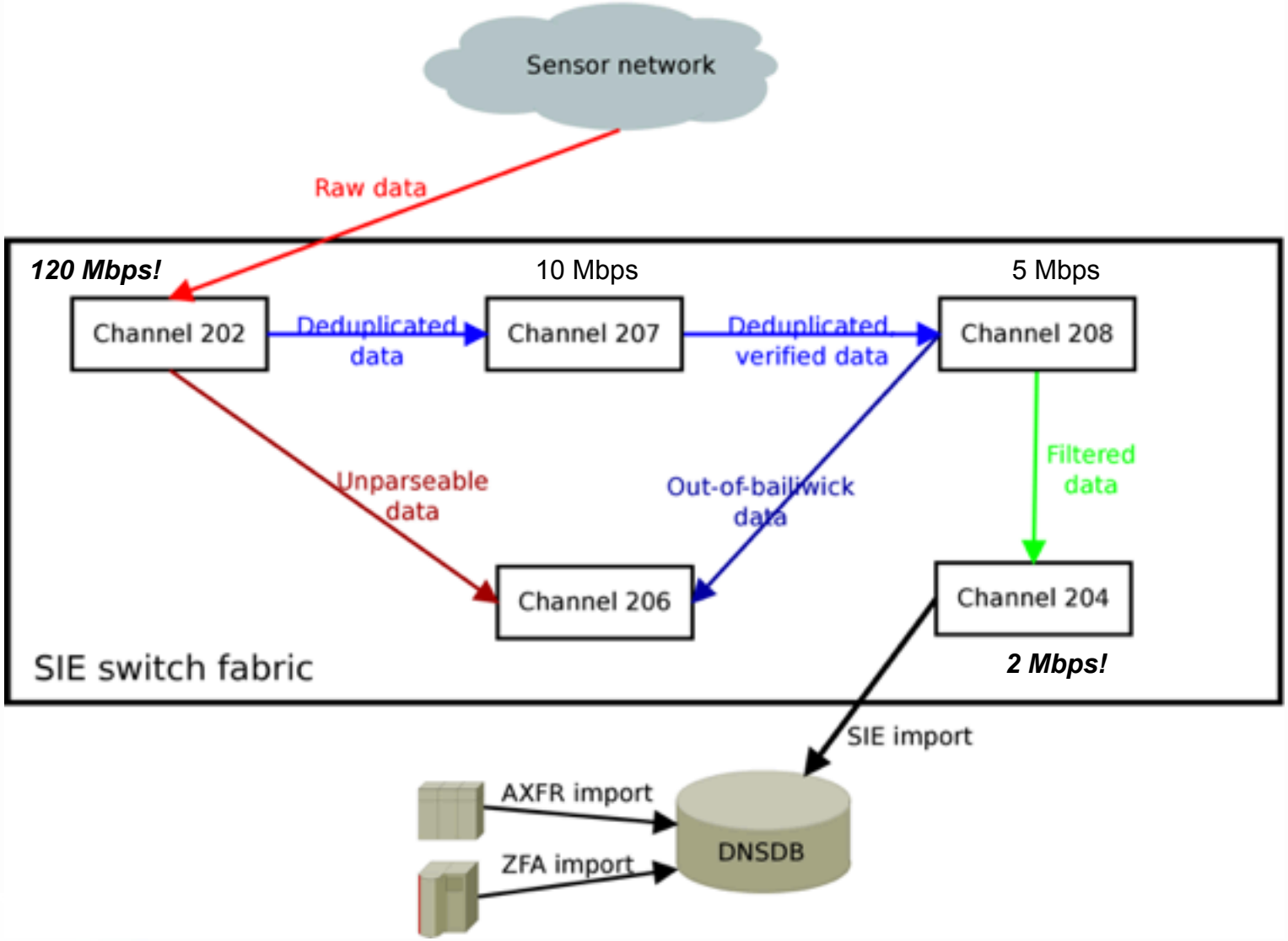
SIE Improvements

- google: sie-dns-sensor
- Advantages:
  - Platform-neutral binary format
  - Re-assembles IP and EDNS0 fragments
  - Determines bailiwick information
  - Matches queries to responses
  - Better timetamps than pcap
  - Multiple payloads per message
  - Improved payload replication capabilities
  - Defcon 18 pres: google: dc-18-archive.html#Vixie

Channel example - ch202 - dnsqr

[268] [2011-06-03 10:28:30.362351085] [1:9 ISC dnsqr] [20f58a64] [] []
type: UDP_QUERY_RESPONSE
query_ip: *A.B.C.D*
response_ip: 74.122.84.53
proto: UDP (17)
query_port: 31925
response_port: 53
id: 47504
qname: ns2.snapfish.com.
qclass: IN (1)
qtype: A (1)
rcode: NOERROR (0)
delay: 0.00133126
udp_checksum: CORRECT
query: [34 octets]
  ... omitted ...
response: [98 octets]
  ... omitted ...

ISC Passive DNS and DNSDB architecture



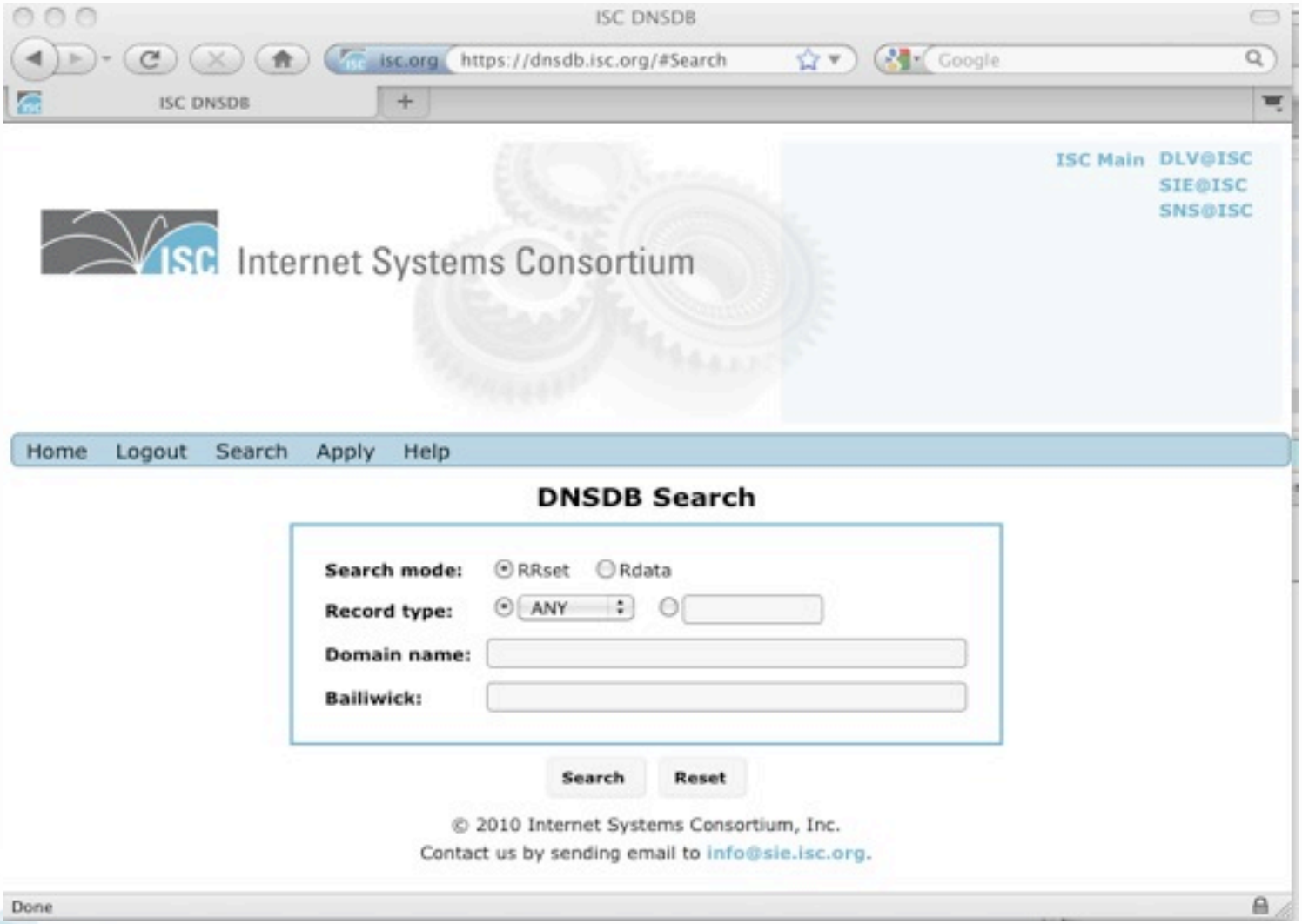
Processing notes

- Reduce and filter incoming data to a manageable level before database
- Loosely coupled multi-processor
  - Broadcast ethernet as an IPC message bus
  - Different-sized single-purpose servers working together in real time
- Database (Pgsql => DB4 => Cassandra => TokyoCabinet)
  - Write-optimized - constant updates
  - Sort & Merge - hourly, daily, monthly, yearly
  - Clustered storage /w replicas

Channel example - ch204

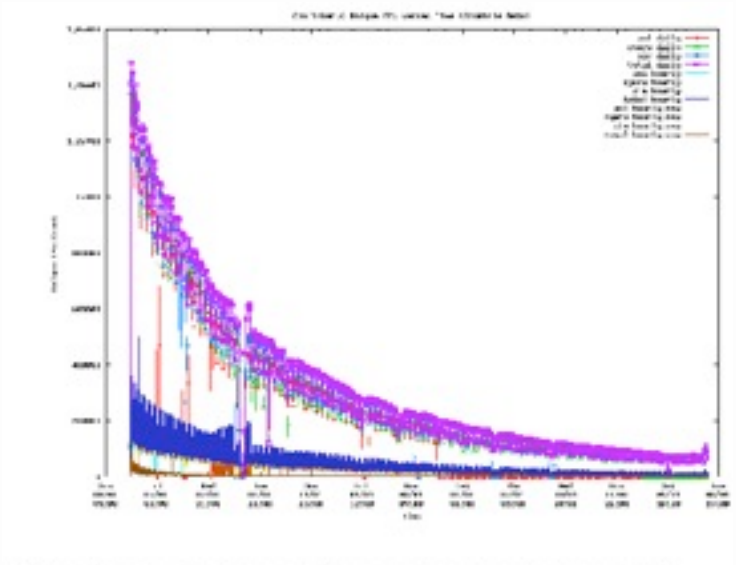
[98] [2011-06-03 09:52:31.229615386] [2:1 SIE dnsdedupe] [00000000] [] []
type: EXPIRATION
count: 100
time_first: 2011-06-02 14:52:09
time_last: 2011-06-03 06:50:16
bailiwick: gamejobs.com.
rrname: gamejobs.com.
rrclass: IN (1)
rrtype: NS (2)
rrttl: 86400
rdata: ns.rackspace.com.
rdata: ns2.rackspace.com.

DNSDB


ISC DNSDB
isc.org https://dnsdb.isc.org/#Search
Google
ISC DNSDB
ISC Main DLV@ISC
SIE@ISC
SNS@ISC
Internet Systems Consortium
Home Logout Search Apply Help
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.
Done

Channel example - sinkhole

[189] [2011-06-03 10:57:59.686034799] [1:4 ISC http] [00000000] [ISC] [ConfickerC]
type: sinkhole
srcip: 113.YY.YY.YY
srcport: 4779
dstip: XX.XX.XX.XX
dstport: 80
request:
GET / HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: XX.XX.XX.XX
Pragma: no-cache



Spam example

```
$ nmsgtool -l 10.16.25.255/8430 -c 1 -o -
[407] [2009-12-03 11:40:00.195077816] [1:2 ISC email] [0829f21a] [] []
type: spamtrap
srcip: 189.15.60.161
helo: bl15-60-161.dsl.asiatel.tl
from: REDACTED@spamtrapdomain.net
bodyurl: http://dc0ca4266.xivivxt.cn/
bodyurl: http://www.w3.org/1999/xhtml
bodyurl: http://94e433.xivivxt.cn/
bodyurl: http://60436719c5.xivivxt.cn/
bodyurl: http://4229da8a0.xivivxt.cn/
bodyurl: http://2d0a7d68.xivivxt.cn/ff24490.gif
bodyurl: http://08a6e3884b.xivivxt.cn/
bodyurl: http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd
```

Other data

- IDS data
- Malvertising URLs
- Darknet / Backscatter

Data combining and analysis

- Some external examples
- Some SIE examples
- General lesson for hackers:
  - conceal your access
  - infrastructure use will be detected

Fast-flux botnet detection
Malware 2008, Holz/Nazario

- What characteristics were common in Fast-Flux botnets?
- What automated heuristics could be developed to classify a new domain to badness?
  - Number of IPs/domain
  - Change frequency
  - AS distribution
  - Geographic distribution
  - domain lifetime
  - number of NS records
  - low TTL, odd SOA
- http://honeyblog.org/junkyard/paper/fastflux-malware08.pdf

CMU CERT

Malicious Domain Name Research

https://www.dns-oarc.net/files/workshop-201010/OARC-ers-20101012.pdf

uses SIE data

New Algorithm

- domains with:
  - 20 or more A recs
  - IPs are in 20 or more ASNs
  - of those domains:
    - find IP sets with more than 5 addrs in common
    - white list known CDNs

what we're finding

```
6/01/2010:
cc.allaboutc0ntrol,com.haijeihefoobeekahkohweto,net.jdhyh1230jh,
ru.mmjl3l45lkjbdb

7/15/2010:
com.drunkjeans,com.earlymale,com.hillchart,com.hugejar,com.roundstorm,
com.tightsales,ru.dealyak,ru.greedford,ru.heroguy,ru.jarpub,
ru.marketholiday,ru.pantscow,ru.problemdollars,ru.raceobject,ru.tintie

08/29/2010:
com.first-wave-aug,com.hotsku,com.iwfybfywi,com.mortalconbat,
com.qrtmpqpmlolpmu,com.uuvqvkoqrrdtli,net.instamfan,net.roundhome,
ru.adaichaepo,ru.aijohcolev,ru.dahzunaeye,ru.deilaeyeew,ru.hazelpay,
ru.iesahnaepi,ru.iveeteepew,ru.jocudaidie,ru.johgheejae,ru.kaithuushi,
ru.ohphahfech,ru.ootaivilei,ru.purplepron,ru.railuhocal
```

Damballa's NOTOS

uses SIE ch204

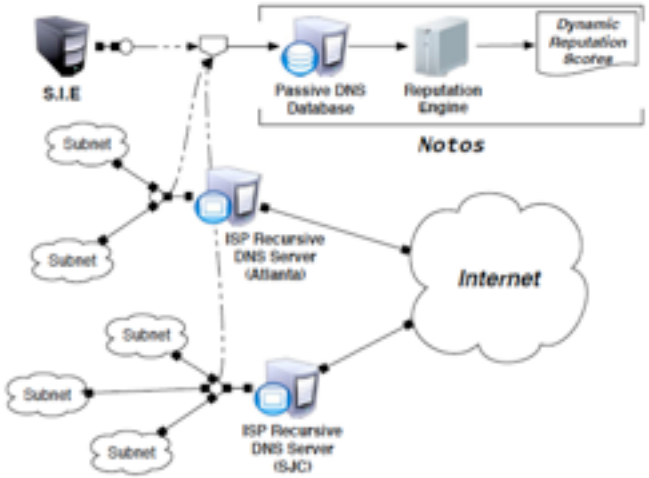


Figure 1. System overview.

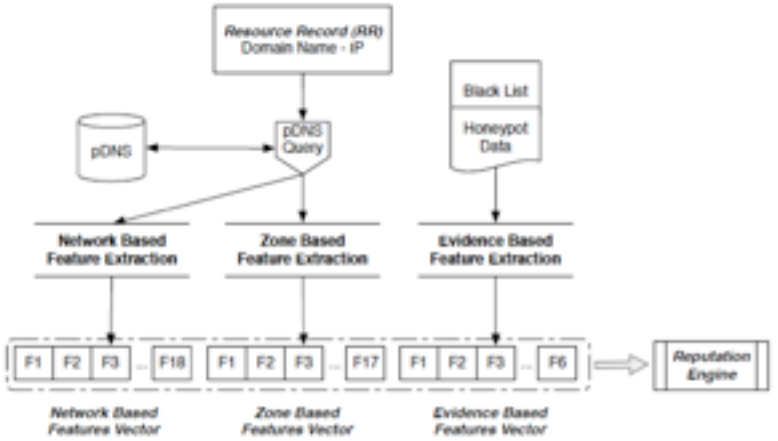


Figure 2. Computing network-based, zone-based, evidence-based features.

http://www.usenix.org/events/sec10/tech/full_papers/Antonakakis.pdf

Damballa's NOTOS

Domain Name	IP	Date
google-bot004.cn	213.182.197.229	08-15
analf.net	222.186.31.169	08-15
pro-buh.ru	89.108.67.83	08-15
ammdamm.cn	92.241.162.55	08-15
briannazfunz.com	95.205.116.55	08-15
mybank-of.com	59.125.229.73	08-15
oc00co.com	212.117.165.128	08-15
avangadershem.com	195.88.190.29	08-19
securebizccenter.cn	122.70.145.140	08-19
adobe-updating-service.cn	59.125.231.252	09-02
0md.ru	219.152.120.118	09-19
avrev.info	98.126.15.186	09-27
g00glee.cn	218.93.202.100	09-02

Table 1. Sample cases form Zeus domains detected by Notos and the corresponding days that appeared in the public BLs. All evidence information in this table were harvested from zeustracker.abuse.ch.

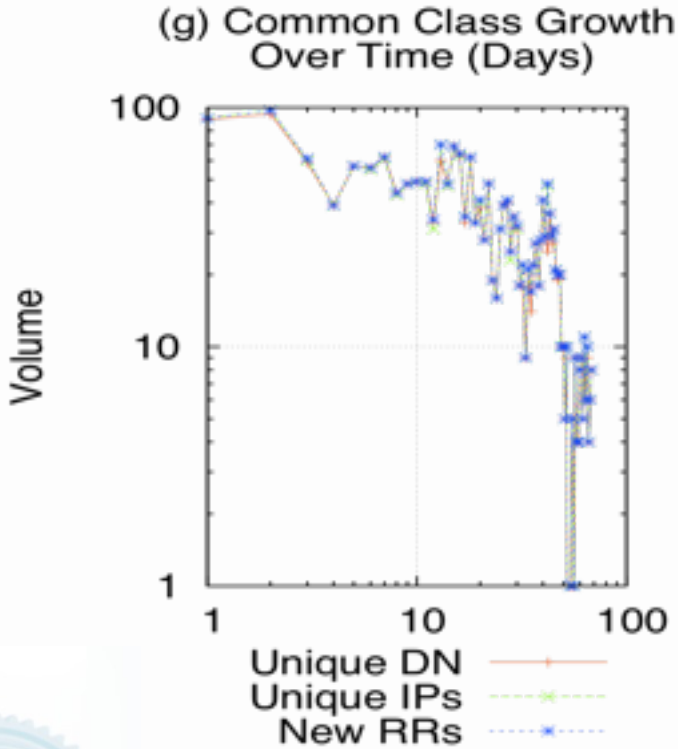
Domain Name	IP	Type	Src	Date
lzwn.in	94.23.198.97	MAL	[1]	08-26
3b9.ru	213.251.176.169	MAL	[2]	08-30
antivirprotect.com	64.40.103.249	RAV	[3]	09-05
1speed.info	212.117.163.165	CWS	[2]	09-05
spy-destroyer.com	67.211.161.44	CWS	[4]	09-05
free-spybot.com	63.243.188.110	RAV	[2]	09-05
a3l.at	89.171.115.10	MAL	[2]	09-09
gidromash.cn	211.95.79.170	BOT	[2]	09-13
iantivirus-pro.com	188.40.52.180	KBF	[5]	09-19
ericwanhouse.cn	220.196.59.19	EXP	[6]	09-22
1165651291.com	212.117.165.126	RAV	[2]	10-06

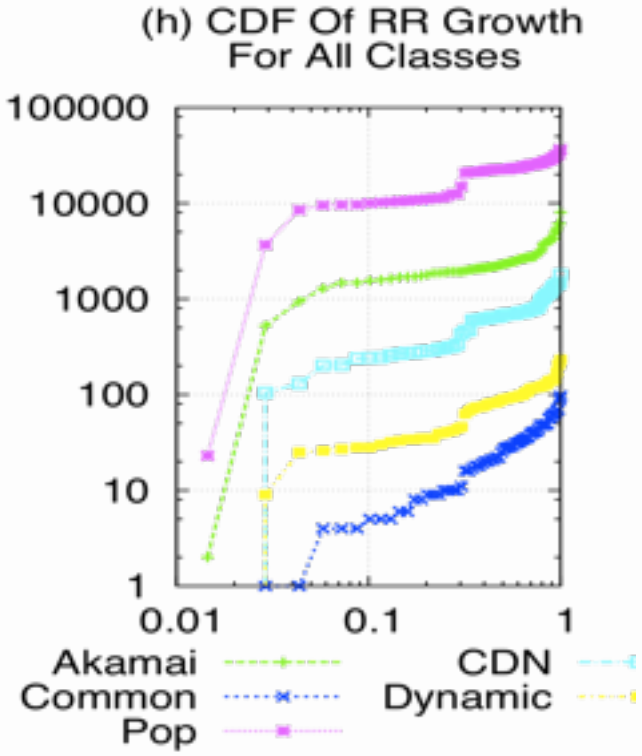
Table 2. Anecdotal cases of malicious domain names detected by Notos and the corresponding days that appeared in the public BLs .[1]: hosts-file.net, [2]: malwareurl.com, [3] siteadvisor.com, [4] virustotal.com, [5] ddanchev.blogspot.com, [6] malwaredomainlist.com

DNS cache pollution (GTISC)

M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, N. Feamster.

"Building a Dynamic Reputation System for DNS". USENIX Security Symposium 2010





ISECLAB's EXPOSURE

http://www.iseclab.org/papers/bilge-ndss11.pdf

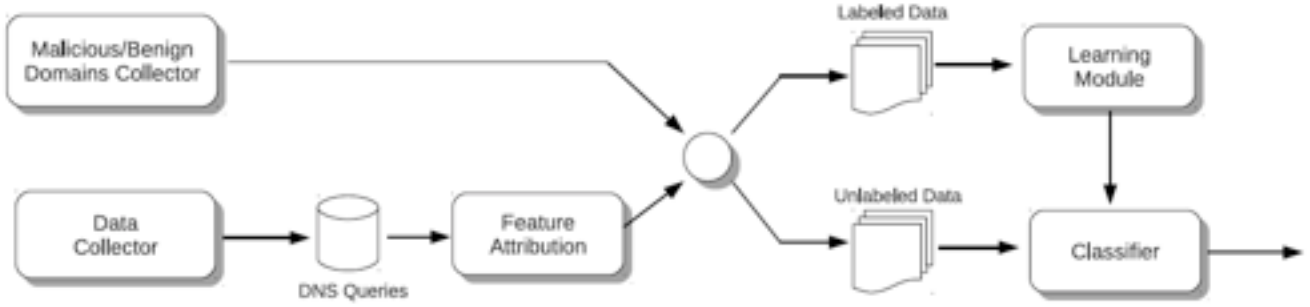


Figure 1: Overview of EXPOSURE

Feature Set	#	Feature Name
Time-Based Features	1	Short life
	2	Daily similarity
	3	Repeating patterns
	4	Access ratio
DNS Answer-Based Features	5	Number of distinct IP addresses
	6	Number of distinct countries
	7	Number of domains share the IP with
	8	Reverse DNS query results
TTL Value-Based Features	9	Average TTL
	10	Standard Deviation of TTL
	11	Number of distinct TTL values
	12	Number of TTL change
	13	Percentage usage of specific TTL ranges
Domain Name-Based Features	14	% of numerical characters
	15	% of the length of the LMS

Table 1: Features.(LMS = Longest Meaningful Substring)

uses SIE ch202

SIE Passive DNS Expansion *by April Lorenzen, ServerAuthority.net*

uses DNSDB API

Level 2
18 FQDNs

buy-pharmacy-onlines.com
buy-pharmacyonlines.com
buypharmacy-onlines.com
buypharmacyonlines.com
buy-pharmaonlines.com
buypharmaonlines.com
drugstoreonlinesites.com
greatpharmashops.com
ns2.avamegasoft.com
ns2.buysoftwaretrends.com

Level 2
15 Base Domains

avamegasoft.com
buy-pharmacy-onlines.com
buy-pharmacyonlines.com
buypharmacy-onlines.com
buypharmacyonlines.com
buy-pharmaonlines.com
buypharmaonlines.com
buysoftwaretrends.com
drugstoreonlinesites.com
greatpharmashops.com

Level 2
19 Name Servers

ns1.ao8h64tr.ru
ns1.dnsnew111.ru
ns1.freenet-dns.ru
ns1.refg436ct.ru
ns1.securepharmacyonline.net
ns1.server.com
ns2.ao8h64tr.ru
ns2.avamegasoft.com
ns2.buysoftwaretrends.com
ns2.dnsnew111.ru

Level 5
60 IPs

112.78.8.98
127.0.0.1
175.121.56.57
175.121.56.94
187.45.180.5
187.45.182.58
188.95.159.179
188.95.159.196
188.95.159.199
188.95.159.67
188.95.159.68

Level 6
32606 FQDNs

0.111.38.83.014yidmgl26f.combined.bl.rptn.ca
0.119.161.67.014yidmgl26f.combined.bl.rptn.ca
0.125.82.82.014yidmgl26f.combined.bl.rptn.ca
0.13.42.24.014yidmgl26f.combined.bl.rptn.ca
0.138.171.69.014yidmgl26f.combined.bl.rptn.ca
0.143.52.78.014yidmgl26f.combined.bl.rptn.ca
0.148.90.2.014yidmgl26f.combined.bl.rptn.ca
0.170.3.80.014yidmgl26f.combined.bl.rptn.ca
0.173.64.61.014yidmgl26f.combined.bl.rptn.ca
01njb97fx.guglielmopharm.in
01urr6d.ezekielrx.in

Level 6
4449 Base Do

115.bz
1232kxcvnk.ru
123offerte.be
127.ca
131.at
1kdfjhk.ru
1royalcasino.ru
2011-language-revol
2132kcsdcd.ru
2ksjdfh.ru
2leep.be

Master of multiple channels: spam, PassiveDNS, darknet

Spamtrap Database Query Tool

Query Type: Query – Top 250 Domains First Seen in Past Hour (slow)

Domain / String:

Submit

s	Source IP	Helo	Domain	URL
1		unet-mx2.uk.clara.net	topmedicb.ru	http://896k.rbx.topmedicb.ru/nhw
1	87.106.10.20	s15339449.onlinehome-server.info	topmedicb.ru	http://c.jeefsw.topmedicb.ru/9x
1	80.65.16.71	irc.orionnet.ru	topmedicb.ru	http://n.rq.topmedicb.ru/1hh
1	87.106.10.20	s15339449.onlinehome-server.info	topmedicb.ru	http://v7m4sn.k22vzp.topmedicb.ru/5
1	80.65.16.71	irc.orionnet.ru	topmedicb.ru	http://w0.w65h.topmedicb.ru/8zdz
1	80.65.16.71	irc.orionnet.ru	topmedicb.ru	http://e8.vvhnm.topmedicb.ru/0d
1	183.104.214.13	irc.orionnet.ru	topmedicb.ru	http://8z.q.topmedicb.ru/x4vm
1	80.65.16.71	irc.orionnet.ru	topmedicb.ru	http://hsbky.tinot7.topmedicb.ru/b
1	92.103.5.20	server2.givs.de	topmedicb.ru	http://n.or0g.topmedicb.ru/90d7

More data combining

RB-Seeker: Auto-detection of Redirection Botnets (NDSS 2009)
http://www-personal.umich.edu/~huxin/papers/xin_RBSeeker.pdf

Passive DNS + Netflow -> redirection domains
Spam URLs -> redirection domains
redirection domains + DNS queries -> actionable intel

ICSI/Berkeley/UCSD
http://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf
Similar detection methods to RB-Seeker
Add web crawling to cluster offers together
Bought products to track payment processing
Found that only a few banks processed most of the transactions
Financial system could become a choke point for spamming

uses SIE for other projects

How to Participate with SIE

How to Participate with SIE?

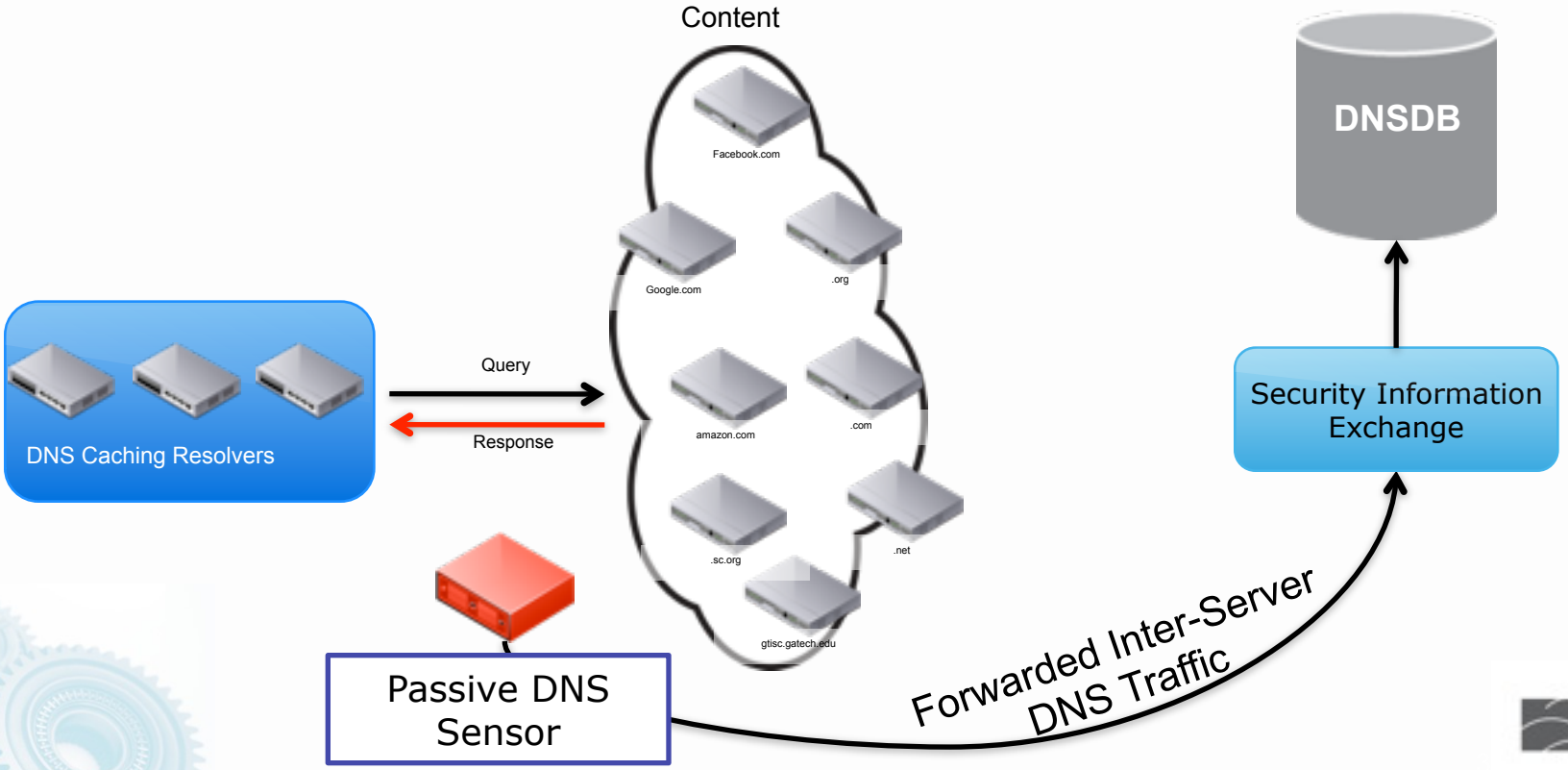
- Join the SIE Forum
- Configure a SIE Passive DNS Sensor and Contribute Passive DNS data.
  - google: join-global-passive-dns
- Submit other data (darknet, spam)
- Get a beta DNSDB UI Account
- Get a trial server

SIE Forum

- The Security Information Exchange (SIE) Forum is a new, vetted, real time "security peering" project created by Internet Systems Consortium ("ISC") organized under similar auspices as other ISC Fora (i.e BIND Forum, DHCP Forum, etc).
- The SIE Forum promotes the development of a "trusted" mechanism to exchange a variety of real time security data so to anticipate and tackle key network security issues for the protection, development, and maintenance of an operational Internet.
- SIE's measures it success by an industry ecosystem that provides law abiding Internet with the equitable means to identify and mitigate miscreant activities.
- SIE Forum membership funds the technological and operational expansion of the SIE architectural model.
- Send E-mail to info@sie.isc.org to get more information.

Submit Passive DNS Data

- Setting up a Passive DNS Sensor and submitting data is one of the best ways to start participation.
- E-mail: dnsdb@isc.org to get started.



Submit Darknet data

- Do you have any netblocks lying around? ;)
- Can capture/compress/upload with nmsgtool
- Route or cross-connect with SIE

```
router static
  address-family ipv4 unicast
    ###.###.0.0/16 10.255.10.254
arp vrf default 10.255.10.254 0202.0404.0606 ARPA
interface GigabitEthernet0/1/0/3.14
  description SIE Dark Net
  ipv4 address 10.255.10.1 255.255.255.0
  dot1g vlan 14
```

DNSDB User Interface Beta

- We have four ways to access DNSDB beta. Each are aligned with a sustainable public benefit service.
  - **Vetted Member of the Operational Security Community.**
  - **Passive DNS Contributors.**
  - **SIE Peers.**
  - **SIE Forum Members.**
- All applications should e-mail to dnsdb@isc.org
  - Please include name, e-mail, contact phone number, and public PGP key with a location of the key server used

DNSDB API Access

- The DNS API access provides a programmable access to the passive DNS data. Its allows qualified and vetted organizations to build tools that integrated directly into DNSDB.
- Access to DNSDB is limited based on a sustainability model that also vets access to mitigate potential abuse.
- Status: The DNSDB API is in BETA. The BETA is currently closed.
- But, when the DNSDB API is opened, there will be four ways to obtain access DNSDB's API:
  - **Passive DNS Contributors.**
  - **ISC Sponsored Researchers.**
  - **SIE Peers.**
  - **SIE Forum Members.**

Questions...

- Email: info@sie.isc.org
- Web: https://sie.isc.org/
- DNSDB: https://dnsdb.isc.org
- NMSG:

  ftp://ftp.isc.org/isc/nmsg

  https://lists.isc.org (nmsg-dev)