

Practical Usage of Passive DNS Monitoring for E-Crime Investigations

Rod Rasmussen

President & CTO, Internet Identity

rod.rasmussen <isat> internetidentity.com

Topics

- Passive DNS overview
- Use Cases
- Challenges
- The future

Passive DNS Replication

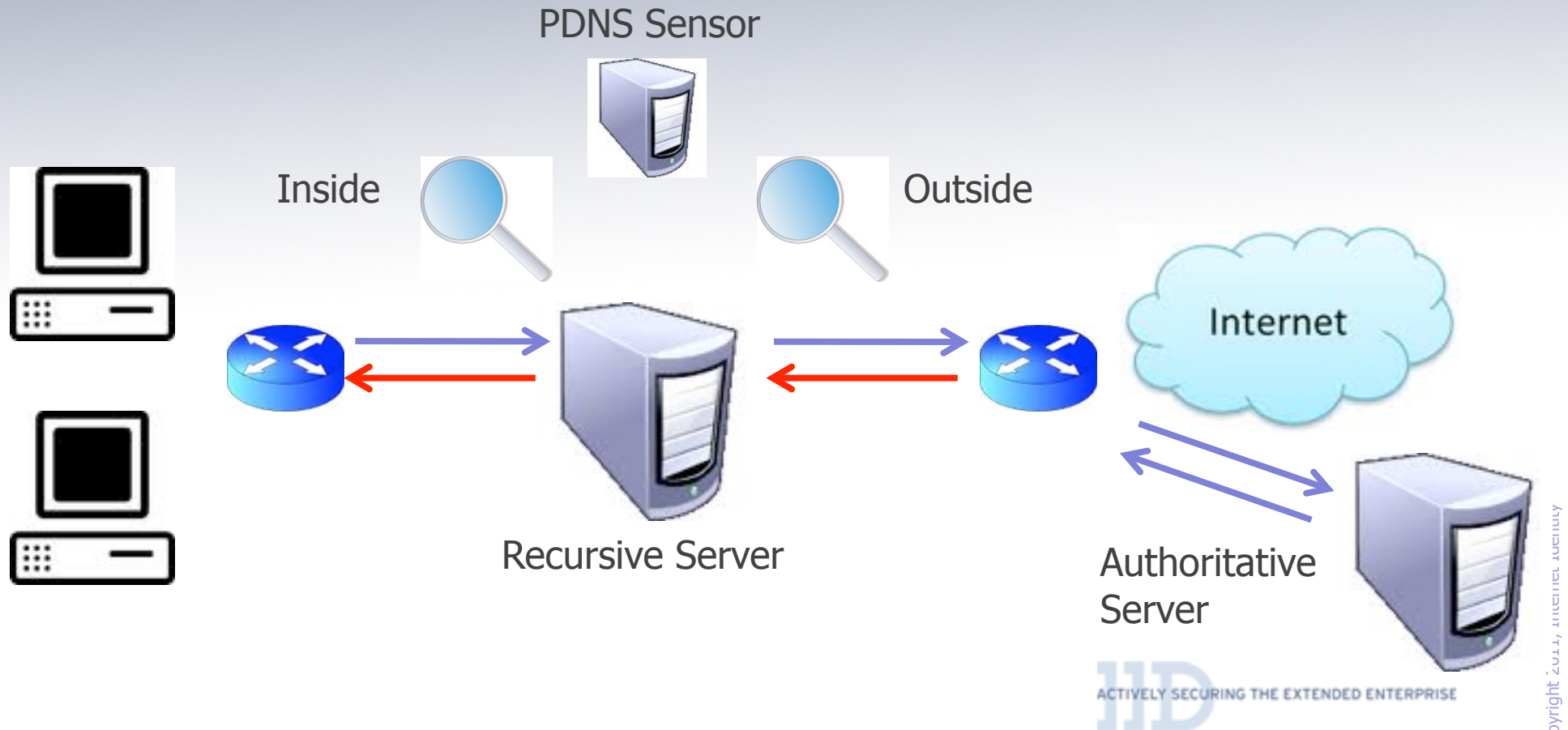
- 2004 – Florian Weimer at the University of Stuttgart
- Monitor DNS queries and responses “near” recursive servers
 - Physical network location with visibility
 - Filter down to just the DNS queries/responses
- Know what is being asked for and what the responses are being received back from authority servers
- Put it in a database
- Find out all kinds of interesting stuff!

Queryable PDNS Collections

- BFK (Florian's)
- SIE (ISC)
- DNSParse (Bojan)
- CERT-EE
- One Ring to Rule Them All?
 - passive-dns-query-tool
 - <http://code.google.com/p/passive-dns-query-tool/>

Inside vs. Outside

- Where do we monitor from?



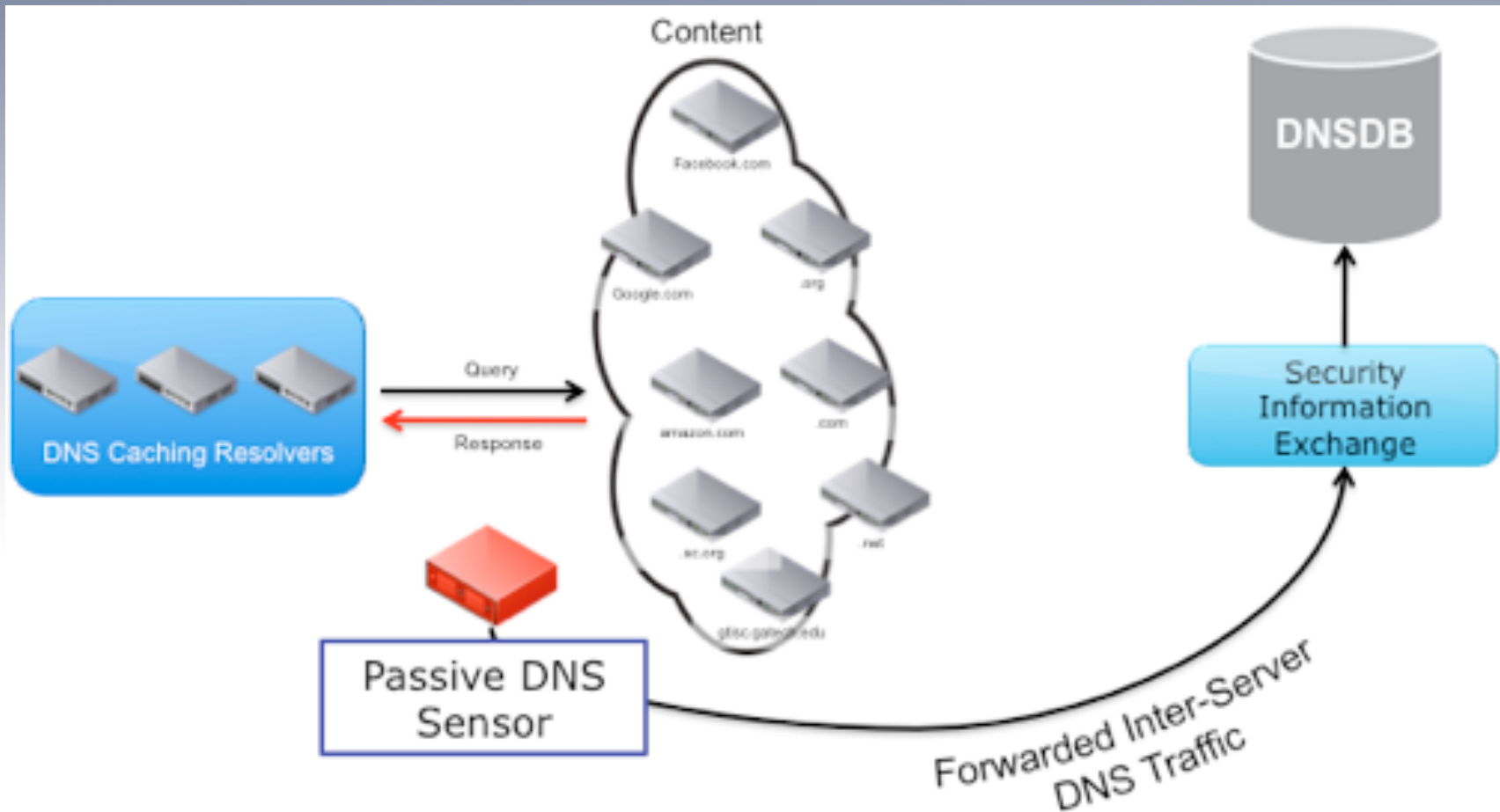
Inside Monitoring

- Get all resolution attempts (minus stub caching)
 - Good for watching for volume spikes
 - Volume can be quickly overwhelming
- Know exact machine(s) making requests
 - Can track down infections to the source
 - Privacy concerns (ISPs)

Outside Monitoring

- See aggregate numbers of resolutions for the organization, ISP etc.
 - Easier data management
 - Lose volume information to caching
- Privacy and internal security concerns largely handled

SIE Model



Source: ISC

Mapping Criminal Infrastructure

bailiwick	oquqcylyedi.com.
first seen	2010-11-24 18:09:45 -0000
last seen	2010-11-25 09:52:03 -0000
oquqcylyedi.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	2010-11-25 17:09:28 -0000
oquqcylyedi.com.	NS ns1.gvghi.ru.
oquqcylyedi.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
oquqcylyedi.com.	NS ns3.lerelaisinternet.com.
oquqcylyedi.com.	NS ns4.lerelaisinternet.com.

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

Criminal Domain Names found via the bad A Record

balliwick	gvvhi.ru.
first seen	2010-11-22 03:43:04 -0000
last seen	2010-11-23 13:44:15 -0000
ns1.gvvhi.ru.	A 60.191.103.66
balliwick	gvvhi.ru.
first seen	2010-11-18 15:54:49 -0000
last seen	2010-11-22 03:31:24 -0000
ns1.gvvhi.ru.	A 190.86.101.171
balliwick	gvvhi.ru.
first seen	2010-11-11 03:12:45 -0000
last seen	2010-11-18 15:42:32 -0000
ns1.gvvhi.ru.	A 201.147.145.254
balliwick	gvvhi.ru.
first seen	2010-11-23 13:53:07 -0000
last seen	2010-11-25 11:12:16 -0000
ns1.gvvhi.ru.	A 218.67.78.181

Found 4700 RRS in 1.12 seconds.

us2.tabletspilldrug.net.	A	218.67.78.181
sfy.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
justecostory.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
nsi.alternativehealthrx.net.	A	218.67.78.181
nsi.badsguide.com.	A	218.67.78.181
nsi.bafasc.ru.	A	218.67.78.181
nsi.bafad.ru.	A	218.67.78.181
nsi.bafaf.ru.	A	218.67.78.181
nsi.bafag.ru.	A	218.67.78.181
nsi.bafaj.ru.	A	218.67.78.181
nsi.bafal.ru.	A	218.67.78.181
nsi.bafap.ru.	A	218.67.78.181
nsi.bafar.ru.	A	218.67.78.181
nsi.bafaw.ru.	A	218.67.78.181

Criminal Domain Names found via the bad Name Server

Data results for ANY/213.55.114.132

Found 10000 hits in 1.65 seconds.

01jwahwjz.curlbeudo.com.	A 213.55.114.132
0ck37mzv.hattyspi.com.	A 213.55.114.132
0dck0x6r.driskape.com.	A 213.55.114.132
0dthow24r.cyrokofo.com.	A 213.55.114.132
0ytuu.mas.bayhealshmedicne.ru.	A 213.55.114.132
0t3vbw23.curlbeudo.com.	A 213.55.114.132
0p7ygdop.edfasesw.com.	A 213.55.114.132
0q0uf01rs.curlbeudo.com.	A 213.55.114.132
0q4fwwpdr.driskape.com.	A 213.55.114.132
0t4b0k65.hattyspi.com.	A 213.55.114.132
8wciuej0t.synpayse.com.	A 213.55.114.132
8ru34eln.amezanka.com.	A 213.55.114.132
10004.buvalialo.com.	A 213.55.114.132
10004.1expotha.com.	A 213.55.114.132
10005.ruaiabysa.com.	A 213.55.114.132
10006hop.myralfiab.com.	A 213.55.114.132
10010hop.myralfiab.com.	A 213.55.114.132
10010hop.myralfiab.com.	A 213.55.114.132
10061.payatlin.com.	A 213.55.114.132
10064.adverrecop.com.	A 213.55.114.132
100675.drugshop.com.	A 213.55.114.132
10089.kicoudu.com.	A 213.55.114.132
1009.mysqeel.com.	A 213.55.114.132

Source: ISC

Tracking Down a Spam E-mail

From: Claire Newell anarchdd@yeonil.net

Subject: Fwd:

Date: April 4, 2011 5:44:06 PM PDT



The advertisement features four items: a blue pill labeled 'VIAGRA', a pink pill labeled 'CP', an orange pill labeled 'Cialis', and a white bottle of 'LEVITRA' (Vardenafil HCl) tablets. Each item is accompanied by a description and a price. The background of the ad includes a faint watermark of 'www.pillsgy.com' and 'advocacy'.

Product	Description	Our price
Viagra	Viagra is an oral drug for male impotence, also known as erectile dysfunction. Viagra has a great safety track record and proven effects that start acting in 30 minutes to 1 hour and last for about 4 hours.	\$1.29
Female Viagra	Female Viagra (Sildenafil) is scientifically formulated to provide intense sexual satisfaction for women seeking ultimate pleasure.	\$2.36
Cialis	Cialis (Tadalafil) is used for treating erectile men's erectile dysfunction (e.g., impotence). Cialis starts working in 30 minutes and lasts for about 36 hours, while Viagra effect lasts up to 5 hours. Besides, you can take Cialis with or without food.	\$1.58
Levitra	Levitra (Vardenafil) is an oral therapy for the treatment of erectile dysfunction. Having the long-lasting effect of 4 hours, and the start time of 16 min, Levitra represents an uncontested advantage in comparison with Viagra.	\$2.81

www.pillsgy.com

Whois pillsgy.com???

Domain Name: PILLSGY.COM

Registrar: IPNIC, INC.

Whois Server: whois.myorderbox.com

Referral URL: <http://www.ipnic.com>

Name Server: NS1.DNSPLAC.COM

Name Server: NS2.BEZZDNS.RU

Status: clientTransferProhibited

Updated Date: 03-apr-2011

Creation Date: 18-mar-2011

Expiration Date: 18-mar-2012

Registrant:

Koshil Igor

Igor (KoshilIgor@mail.com)

Koneva str. 12-48

Koneva str. 12-48

Omsk

Omsk,644031

RU

Tel. +7.3812447211

Fax. +7.3812447211

Creation Date: 18-Mar-2011

Expiration Date: 18-Mar-2012

Domain servers in listed order:

ns1.dnsplac.com

ns2.bezzdns.ru

Administrative Contact:

Koshil Igor

Igor (KoshilIgor@mail.com)

Koneva str. 12-48

Koneva str. 12-48

Omsk

Omsk,644031

RU

Tel. +7.3812447211

Fax. +7.3812447211

Oh Goodie – V1agr4, eh.



Pharmacy Express
#1 ONLINE WORLDWIDE DRUGSTORE

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

Your cart: **GBP 0.00** (0 items)

> Free Delivery Insurance
> 7 years WorldWide Supplier
> 100% Satisfaction Guarantee
> High Quality medicaments
> 24/7/365 Support Team

Main About us F.A.Q. Our policies Track my order Your cart Contact us

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
- Anti Bacterial
- Anti Convulsants
- Anti Depressants

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



Light Pack | Save 15%

GBP 113.75 GBP 103.41

Viagra 50mg x 30
Cialis 10mg x 30

Select pack

Professional Pack | Save 15%

GBP 192.72 GBP 175.20

Viagra Professional 100mg x 30
Cialis Professional 20mg x 30

Select pack

Viagra Pack | Save 15%

GBP 155.35 GBP 141.23

Viagra 100mg x 20
Viagra Professional 100mg x 20
Viagra Super Active 100mg x 20

Select pack

Generic Viagra

GBP 0.78
special price:
GBP 0.71

Generic Cialis

GBP 0.97
special price:
GBP 0.88

Most Popular (per pill)

- Strong Pack **GBP 2.00**
- Light Pack **GBP 1.72**

Passive DNS Doesn't Look "Bad"

IP search:

Found 2 records

Host/Domain Name	First Seen	IP	ASN BGP Netblock
pillsgy.com	2011-03-25 02:43:30	122.224.6.32	4134 122.224.0.0/12
pillsgy.com	2011-03-20 02:28:22	127.0.0.1	

Nameserver search:

Found 4 records

Nameserver	First Seen
ns2.bezzdns.ru	2011-03-25 02:43:27
ns1.dnskt.com	2011-03-25 02:43:27
ns1.ezydomain.com	2011-03-20 02:28:22
ns2.ezydomain.com	2011-03-20 02:28:22

Let's Look at That IP...

inetnum: 122.224.6.0 - 122.224.6.255
netname: NINBO-LANZHONG-LTD
country: CN
descr: Ninbo Lanzhong Network Ltd
descr:
admin-c: TD209-AP
tech-c: CS64-AP
status: ASSIGNED NON-PORTABLE
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC

role: CHINANET-ZJ Shaoxing
address: No.9 Sima Road,Shaoxing,Zhejiang.
312000
country: CN
phone: +86-575-5136199
fax-no: +86-575-5114449
e-mail: anti-spam@mail.sxptt.zj.cn
trouble: send spam reports to anti-

spam@mail.sxptt.zj.cn
trouble: and abuse reports to
anti-spam@mail.sxptt.zj.cn
admin-c: CH109-AP
tech-c: CH109-AP
nic-hdl: CS64-AP
mnt-by: MAINT-CHINANET-ZJ
changed: master@dcb.hz.zj.cn 20031204
source: APNIC

person: Taichun Du
nic-hdl: TD209-AP
e-mail: anti-spam@mail.sxptt.zj.cn
address: Shaoxing,Zhejiang.Postcode:312000
phone: +86-574-88311333
country: CN
changed: auto-dbm@dcb.hz.zj.cn 20100105
mnt-by: MAINT-CN-CHINANET-ZJ-SX
source: APNIC

Jackpot!

Your query returned **438,394** records.

First Seen	Host/Domain
3/23/2011 8:59	0.2k.medicsy.com
3/23/2011 10:30	0.2l60.medicsy.com
3/23/2011 21:19	0.3.medicdm.com
3/23/2011 22:42	0.3.medicsy.com
4/4/2011 16:53	0.3.topmedicb.ru
4/4/2011 20:18	0.348t.medicsy.com
3/21/2011 0:00	0.6fj0.medicsy.com
1/27/2011 18:26	0.bsirr.doctorgco.ru
1/26/2011 15:42	0.bsirr.sodoctorg.ru
1/27/2011 8:44	0.bsirr.sudoctorg.ru
3/23/2011 8:59	0.cf7ts7.topmedicb.ru
3/23/2011 10:30	0.cf9.topmedicb.ru
3/23/2011 21:19	0.ct.medicsy.com
3/23/2011 22:42	0.cu60.medicsy.com
3/24/2011 2:52	0.d.medicsy.com

First Seen	Host/Domain
3/21/2011 10:43	candmedic.ru
3/19/2011 14:59	candoctor.ru
3/25/2011 12:14	candx.wke.asterwase.net
2/25/2011 10:58	cazht.medicinexi2.ru
3/29/2011 17:12	cazkt.extralegallow.org
1/28/2011 3:43	cazuy.pharmacyrx38.com
3/26/2011 6:16	cb.r.10yearsextrces.net
3/23/2011 8:16	cb6kf.v.topmedicb.ru
3/23/2011 9:25	cb6n8.8a.medicsy.com
3/23/2011 12:54	cb6s.gy.topmedicb.ru
3/23/2011 17:35	cb6zy.5v2rt.medicsy.com
3/23/2011 21:46	cb8.t.medicsy.com
3/24/2011 3:18	cba8g.st9al.topmedicb.ru
2/1/2011 16:36	cbaaf.rxshopds9.com

How About a Nameserver?

Found 26 records

First Seen	Domain
4/4/2011 1:51	bljxpills.ru
4/3/2011 23:12	brjxpills.ru
4/4/2011 13:51	caxrpills.com
4/3/2011 16:09	chxrpills.com
4/3/2011 16:33	dnsplac.com
4/3/2011 21:45	doctorje.com
4/4/2011 15:47	doctorod.com
4/3/2011 16:20	doctorrg.com
4/3/2011 16:25	doctorrl.com
4/3/2011 23:41	fajxpills.ru
4/4/2011 18:58	gejxpills.ru
4/4/2011 9:32	medicaqap.ru
4/4/2011 8:01	medicaqar.ru

First Seen	Domain
4/4/2011 17:02	medicaqch.ru
4/4/2011 10:14	medicaqci.ru
4/3/2011 22:15	medicaqee.ru
4/3/2011 22:18	medicaqen.ru
4/3/2011 22:18	midiclxia.ru
4/3/2011 22:38	midiclxic.ru
4/3/2011 22:46	midiclxme.ru
4/3/2011 22:15	midiclxnf.ru
4/3/2011 22:51	midiclxto.ru
4/4/2011 20:23	pillsin.com
4/3/2011 16:26	pillsll.com
4/4/2011 23:56	rafpills.com
4/3/2011 21:19	stpills.com

Tracking Malware C&C's

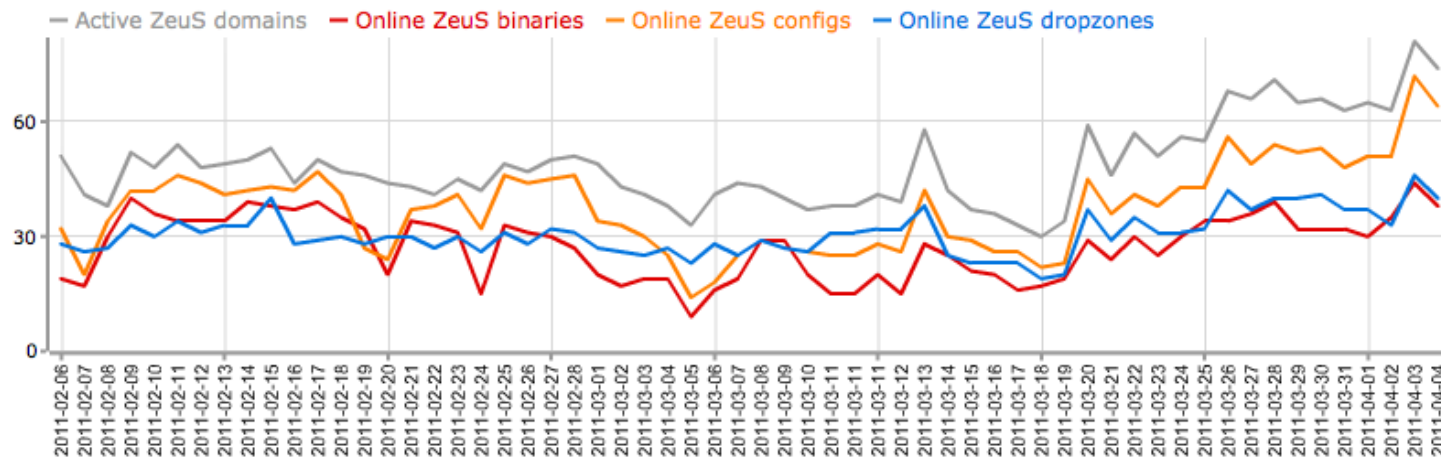
- Once you know a C&C IP, you can start tracking down probable C&C and rendezvous domains
- Zeus is a great example – typically controlled via a series of domains
- Let's take data from ZeusTracker and see if we can improve detection using PDNS

ZeusTracker

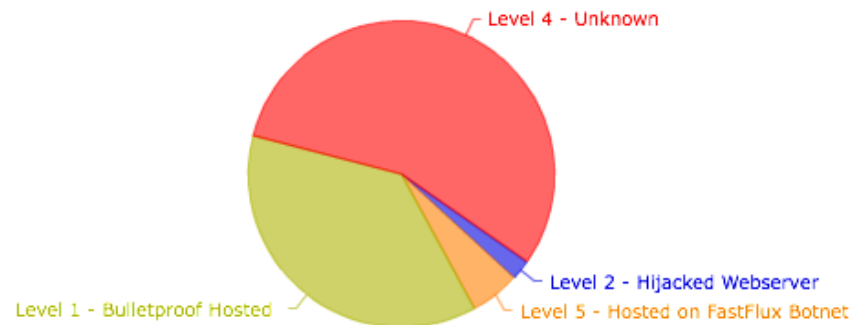
Zeus Tracker :: Statistic

Here are some statistics about the ZeusS crimeware. Note: You need the [Adobe Flash player](#) to view the statistics.

of active Zeus files (last 60 days)



Hosting Statistic (# of Hosts per Level)



<https://zeustracker.abuse.ch>

Zeus C&C IP - 94.63.244.32

- Located in Romania
- ZeusTracker has 6 domains on it

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(s)
2011-03-08	CC		bigupdate.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com
2011-03-08	CC		bigupdatings.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com
2011-03-07	CC		bigupdater.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com
2011-03-07	CC		bigupdates.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com
2011-03-07	CC		bigupdating.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com
2011-03-07	CC		bigupdaters.ru	online	0	REGTIME-REG-RIPN	ns1.nameself.com ns2.nameself.com

of Host on this IP address: **6**

Passive DNS Expands the Story

- 13 Records on 12 distinct domains – double the action for blocking and remediation

Found 13 records

IP Address	ASN	BGP Netblock	First Seen	Host/Domain
94.63.244.32	49469	94.63.244.0/24	2011-03-02 06:55:57	bigupdate.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-10 01:28:05	bigupdate1.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-05 11:14:42	bigupdater.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-04 22:31:11	bigupdaters.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-03 03:50:22	bigupdates.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-05 07:03:41	bigupdating.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-08 22:03:12	bigupdatings.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-03 07:04:40	hotupdating.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-10 23:57:28	topupdate.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-13 08:38:09	topupdater.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-15 23:38:01	topupdaters.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-11 22:47:02	topupdates.ru
94.63.244.32	49469	94.63.244.0/24	2011-03-19 07:18:06	www.bigupdater.ru

Even more to find

- Checking one of the “new” domains for this IP, we find 2 new IPs – from topupdates.ru

Found 3 records

Host/Domain Name	First Seen	IP	ASN	BGP Netblock
topupdates.ru	2011-03-28 00:35:07	94.63.149.52	42741	94.63.149.0/24
topupdates.ru	2011-03-18 01:40:39	86.55.140.204	49469	86.55.140.0/24
topupdates.ru	2011-03-11 22:47:02	94.63.244.32	49469	94.63.244.0/24

- Turns out several of the “new” domains just weren’t seen on the first IP, but were spotted later.
- PDNS would greatly improve detection speed

Fast-Flux Detection

- PDNS an excellent way to find new FFLUX domains and hosts
- Set-up traps on new (or old) domains/hosts and watch for tell-tales
 - Multiple IPs across ASNs
 - Lots and lots of hostnames (wildcarding)
- Was particularly good for ROCK/Avalanche
- Not in vogue as much these days

FFLUX Example

Suspected Avalanche Domain - platinumalbumm.com
Detected via flux behavior 31/8/2010

Found 175 records

First Seen	IP	ASN	BGP Netblock
2010-09-02 06:03:33	125.224.87.9	3462	125.224.0.0/16
2010-09-10 17:06:36	187.18.177.80	28270	187.18.128.0/17
2010-09-11 19:53:43	217.85.219.235	3320	217.80.0.0/12
2010-09-01 01:40:41	61.63.60.123	18042	61.63.0.0/18
2010-09-06 21:30:54	69.66.112.254	7029	69.66.0.0/16
2010-09-11 16:33:28	76.168.233.98	20001	76.168.0.0/13
2010-09-06 16:13:21	78.88.220.232	29314	78.88.216.0/21
2010-09-11 11:23:17	82.61.71.66	3269	82.61.0.0/16
2010-09-07 06:41:22	87.165.115.97	3320	87.128.0.0/10
2010-09-09 07:56:47	91.82.177.158	12301	91.82.0.0/15
2010-09-13 08:39:00	95.89.168.93	31334	95.88.0.0/14
2010-09-08 22:11:47	109.184.56.252	25405	109.184.0.0/16
2010-09-11 17:53:43	178.92.69.20	6849	178.92.0.0/14

Bullet Proof Hosting

- PDNS allows you to explore entire hosting locations to tie criminal activities together
- Search CIDR blocks and correlate data
- Can't kill a pharma shop or replica knock-offs?
 - Go after them for phishing and malware hosting
 - Better chance of de-peering with nastier stuff

Monitoring Your Infrastructure

- PDNS is a great tool for alerting you of unauthorized activities with your names and your IP space
- Take-over of infrastructure – hacking/hijacking
- Compromises of machines for hosting malicious content or activities
- The latest marketing campaign you weren't told about
- Domain name expirations 😊

Finding Bots on Your Network

- Map out IP infrastructure and set-up standard scans/alerts based on new hostname mappings appearing
- Filter out “known good” domains/hosts
- Filter known anomalies
 - DNS tunneling services
 - SonicWall router responses
 - Other bizarre “chaff” that shows up
- ISPs may want to filter Dynamic DNS services – maybe not depending on hostname

Sample Network Scan

- Let's look at a large bank range (165.32.0.0/12)
- 1751 Records we've seen in past 18 months
 - Lots of standard junk
 - 918 DNS Tunneling hosts
 - b9d2183d19a87a6776d09df644df5dab898a.1.ziyouforever.com
 - 830 SonicWall hosts
 - 2.047870c52e682d850000000000000418.griddnsd.global.sonicwall.com

Three Records to Examine

- No bank hosts showing up – good, it's a non-public network space!
 - uluqwovl.info -> 165.44.178.223
 - pnncfoxrtfz.ekuxejqw.com -> 165.43.189.113
 - midvalleydental.net -> 165.38.174.232
- First one is just plain weird – no ties to anything else and not operative
- Third is odd, until you look at this:
 - Dig midvalleydental.net -> 165.38.174.232
 - Dig www.midvalleydental.net -> 65.38.174.232

pnnncfoxrtfz.ekuxejqw.com

- Whois looks bad...
 - Registrar: TODAYNIC.COM, INC.
 - Creation Date: 05-mar-2011
 - Nameservers: N588.COZVEND.BIZ, N776.COZVEND.BIZ
- On some spam lists, not working now
- Rotated IPs

IPs Moving All Over

Found 9 records

First Seen	IP	ASN	BGP Netblock
2011-03-15 00:35:03	220.146.6.136	2510	220.146.0.0/15
2011-03-14 21:25:04	150.211.25.152		
2011-03-15 00:35:02	165.43.189.113		
2011-03-15 00:35:02	180.51.204.16	4713	180.0.0.0/10
2011-03-14 21:25:03	64.120.170.101	21788	64.120.128.0/18
2011-03-14 21:25:03	18.169.198.126	3	18.0.0.0/8
2011-03-15 00:35:03	67.137.15.43	7385	67.136.0.0/14
2011-03-14 21:25:04	201.28.47.15	10429	201.28.0.0/17
2011-03-14 21:25:03	11.134.78.67		

Nameservers Look Suspicious

Found 60 records

<u>First Seen</u>	<u>Domain</u>
2011-03-07 02:48:27	adubapot.com
2011-03-14 03:23:34	afohilim.com
2011-03-14 03:23:08	afypisur.com
2011-03-14 03:19:44	ahamifej.com
2011-03-14 03:20:28	ajupymyx.com
2011-03-14 03:22:27	amqzewit.com
2011-03-14 03:21:54	apimywax.com
2011-03-07 02:57:23	arohuhuv.com
2011-03-14 03:22:44	atasyzel.com
2011-03-07 02:49:14	avqfugqv.com
2011-03-14 03:08:54	awyxufel.com
2011-03-07 02:56:33	azyjyroc.com
2011-03-14 01:55:39	ekqtagiw.com
2011-03-07 02:50:51	ekuxejqw.com
2011-03-07 02:46:49	elqvizyk.com
2011-03-14 01:59:27	epofapeb.com

First Seen

2011-03-14 01:59:48
2011-03-07 02:41:14
2011-03-07 02:37:47
2011-03-07 03:49:35
2011-03-07 03:36:02
2011-03-07 03:29:55
2011-03-14 02:23:14
2011-03-14 02:26:55
2011-03-14 02:48:34
2011-03-14 02:45:31
2011-03-14 02:49:18
2011-03-14 02:59:04
2011-03-07 03:09:20
2011-03-07 02:47:49
2011-03-07 02:49:01
2011-03-14 02:38:07
...

Domain

itipyto.com
ixohoren.com
izetqmab.com
ocesytaw.com
ofyruwqb.com
ogqhejej.com
ogycovqb.com
omizodav.com
orynypoh.com
osodigaw.com
owapupih.com
oxaxesuz.com
qdopqcqh.com
qdulyjqd.com
qfatunam.com
qgucipyl.com

pnnncfoxrtfz.ekuxejqw.com

- Google cache of this one – oops!

COMPLETE THIS SIMPLE FORM FOR YOUR **FREE LIFETIME MEMBERSHIP!**

MEMBERS BENEFITS

Unlimited Downloads
High definition Videos
Terabytes of Videos
iPod and PSP Videos
24/7 Customer Support
Free Lifetime Access

STEP 1 - VERIFY YOUR AGE

First Name:

Last Name:

Zip/Postal Code:

Email:

(Your login will be sent to this email address)

 **FREE ACCOUNT** - Credit card - \$0.00

Next 

Activate Your Membership NOW!

100% SAFE AND SECURE TRANSACTION

pnnncfoxrtfz.ekuxejqw.com

- Following that link – sure not our bank!

 **SAFE SECURE ENCRYPTED**  Constant Protection **100% SECURE**
Your personal information is safe with this form. 100% safe and secure billing.

Todays charge is \$0.00
for your free access to www.bannedfromfaceb--k.com



You must be 18 years of age or older to access this site.
Please submit your information below for **VERIFICATION**

First Name:

Last Name:

Card Number:

CVV2/CVC2 Number: [What's This?](#)

Expiration Date:

Zip/Postal Code:

Email:

* (Your login will be sent to this email address)

☒ Special Offer: Your membership today Qualifies for a FREE VIP upgrade+

By pressing **CLICK FOR FREE ACCESS**, I certify that I have read and agree to the [Terms and Conditions](#) and [Privacy Policy](#) and that the information entered above is my own and I am fully authorized to use it. I also understand that my information will be shared with third parties. Fraud will be prosecuted to the fullest extent of the law.

Data Exfiltration

- Same techniques can be used to spot data exfiltration from your networks
- Google found Aurora via DNS logs, PDNS works from the outside or in conjunction with inside monitoring position without the overhead of DNS log parsing
- Night Dragon case – well, not so much – didn't see the hosts in the main passive feed (we got them from a separate source)
 - Assumption is that they used the hacked company's own recursive servers for resolution to the data dump domains

RSA Breach

- Several reported domains/subdomains

AGOOGL.E.IN
ALBERTSTEIN.DDNS.US
ALVINTON.JETOS.COM
BILLGATES.ITS AOL.COM
BUFFET.BBSINDEX.COM
BUFFET80.ITS AOL.COM
DOMIKSTART.HOPTO.ORG
FOOTBALL.DYNAMICLINK.DDNS.US
FREE2.77169.NET
FTP.XMAHOME.OCRY.COM
GOOD.MINCESUR.COM
OBAMA.SERVEHTTP.COM

PRC.DYNAMICLINK.DDNS.US
SAFECHECK.ORGANICCRAP.COM
SMTP.DYNAMICLINK.DDNS.US
SUPERAROUND.NS02.BIZ
UP82673.HOPTO.ORG
WWW.ALVINTON.JETOS.COM
WWW.COMETOWAY.ORG
WWW.CZ88.NET
WWW.USGOODLUCK.COM

RSA Breach – Prelim PDNS Info

- A few of those domains appear to be outliers
- Attacks may have lasted months
- Most IPs for activities were in China, a few in South Korea and India, and at least one in the US
- We found several unreported “ftp” hostnames that point straight to possible exfiltration of data

```
;; first seen: 2010-10-18 05:46:58 -0000  
ftp.alvinton.jetos.com. IN A 114.248.86.49 CHINA
```

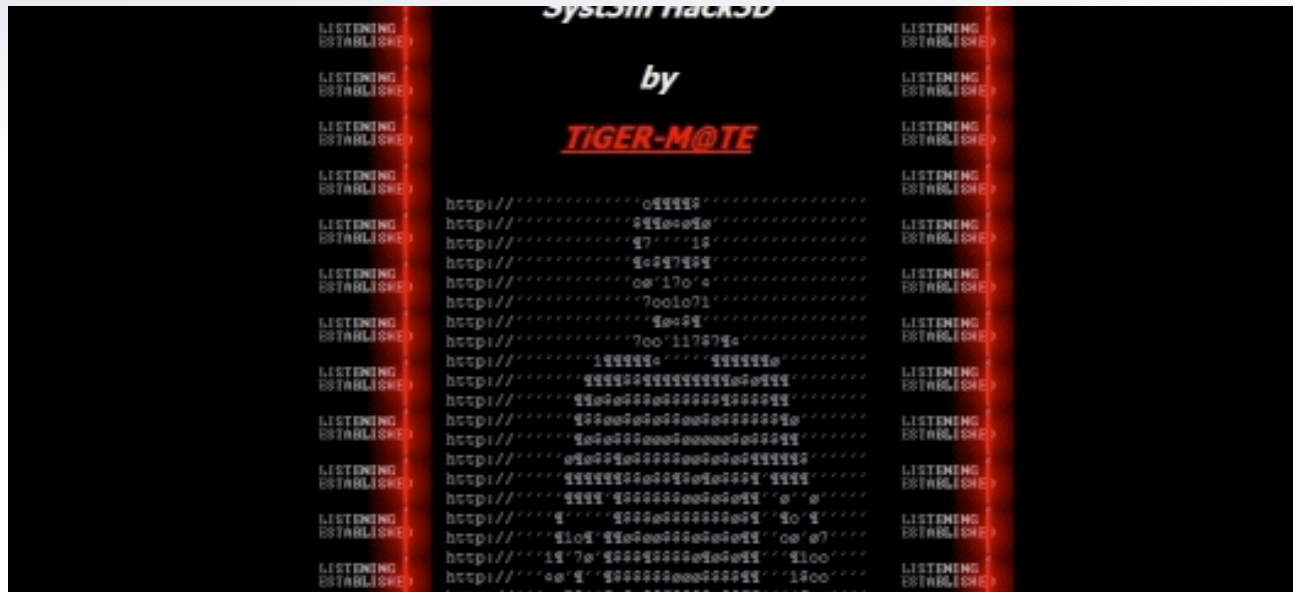
```
;; first seen: 2011-03-14 00:51:18 -0000  
ftp.alvinton.jetos.com. IN A 123.120.96.142 CHINA
```

Detecting Domain Hijacking

- Set-up watches for changes to nameservers and/or IP addresses on critical hostnames under a domain.
- Can combine with active DNS monitoring of critical assets
- Changes to ASN's used by those hosts or to known or suspicious neighborhoods can be alerted for investigation
- Can use PDNS database to determine if the event is specific or widespread (e.g. registry hack, domain account take-overs)

Bangladesh gets p0wned

- Through active DNS monitoring, we spotted microsoft.com.bd being moved onto malicious looking nameservers and an odd IP address
- Sure enough... domain name hijacking!



PDNS Tells the Bigger Story

- A lot more victims = Registry hack
- Looks like cross-site scripting attack against BD NIC

Found 4 records

Nameserver	First Seen	Host
localh0st1.avjournal.com	2011-01-08 09:51:15	google.com.bd
localh0st1.avjournal.com	2011-01-08 09:53:36	hsbc.com.bd
localh0st1.avjournal.com	2011-01-08 13:26:00	music.com.bd
localh0st1.avjournal.com	2011-01-08 16:28:19	aloashbei.com.bd

Found 3 records

Host/Domain Name	First Seen	IP	ASN	BGP Netblock
hsbc.com.bd	2010-12-03 04:38:46	203.112.92.6	9221	203.112.92.0/24
hsbc.com.bd	2011-01-08 11:32:31	173.233.68.2	40244	173.233.64.0/19
hsbc.com.bd	2010-07-01 12:49:08	203.112.92.44	9221	203.112.92.0/24

Take-over of legit DNS

- Bad guys like to use DNS but know their own domains can get blocked/shut-down
- Great leverage if you can compromise the DNS of a real site
 - Can't (or shouldn't) block/shut-down legit domain
 - Site owner may be unaware of compromise
- Can do in conjunction with site or just the DNS

Domain DNS Take-over Vectors

- Control all aspects – website/DNS/e-mail
 - Registrar/hosting combo accounts
 - Cpanel or other management tools
 - Site server looks “guilty” as evil content present
- Control the DNS
 - Registrar or DNS provider take-over
 - P0wn the nameserver
 - IPs for legit and illegitimate servers differ

Legit website



<http://townhouseflorida.com/>

Hitchhiker Site

Bank of America | Online Banking | Sign In to Online Banking

http://bankofamerica.com.townhouseflorida.com/zionbnkofamericasitykeybknofamerica22/bnkofamericasityk1eybknofamerica/bnkofamericasitykeybknofamerica/signon.php?section=signinpage&update=&cookiecheck=yes&destination=nba/signin

Most Visited ▾ Zimbra PowerShark Bugzilla Main Page Traceroute, Ping, Do... IID Twiki Domain Matching Na... VirusTotal - Free On... ThreatExpert - Auto... Internet Identity Pas... Elman's DIC Tool

Search VirusTotal Scan current site

IID - Actively securing ... Delta - Book a flight https://por...port.name= Bank of America | Onli... Welcome Internet Identity Passiv...

Bank of America Online Banking

Sign In

Account in: (the state where you opened your account)

Enter Online ID:

(6 - 32 characters)

☐ Save this Online ID ([How does this work?](#))

[Sign In](#)

[Reset passcode](#)
[Forgot or need help with your ID?](#)

Not using Online Banking?
[Enroll now for Online Banking](#) >>
[Learn more about Online Banking](#) >>
[Service Agreement](#) >>

Secure Area
[Home](#) • [Locations](#) • [Contact Us](#) • [Help](#) • [Sign in](#) • [Site Map](#)
[Personal Finance](#) • [Small Business](#) • [Corporate & Institutional](#)
[About the Bank](#) • [In the Community](#) • [Finance Tools & Planning](#) • [Privacy & Security](#)

USA
Official Sponsor

Bank of America, N.A. Member FDIC. Equal Housing Lender
©2010 Bank of America Corporation. All rights reserved.

Done 85.13.194.146 off

<http://bankofamerica.com.townhouseflorida.com/zionbnkofamericasitykeybknofamerica22/bnkofamericasityk1eybknofamerica/bnkofamericasitykeybknofamerica/signon.php?section=signinpage&update=&cookiecheck=yes&destination=nba/signin>

PDNS tells a story...

Found 3 records in Passive DNS

IP Address Host/Domain	ASN	BGP Netblock	First Seen
85.13.194.146 bankofamerica.com.sitekey.securepages.infoupdate.verifyinfo.townhouseflorida.com	31708	85.13.192.0/19	2010-11-30 00:06:36
85.13.194.146 bankofamerica.com.townhouseflorida.com	31708	85.13.192.0/19	2010-07-08 20:19:20
85.13.194.146 townhouseflorida.com	31708	85.13.192.0/19	2010-07-14 05:40:30

Note that a wildcard DNS record for a domain can
Be exploited similarly if you have compromised the site.
Thanks Peter!

Disaster Scams

- Katrina, Indian Ocean Tsunami, Haiti, Japan Disaster
- Scams set-up to solicit funds
- Lots of “real” efforts too – careful analysis needed
- PDNS a great tool for finding quickly and in any ccTLD or subdomains
- Generate lists for automated and human analysis

Japan Disaster Tracking Sample

- Set-up alerts for likely string combos
 - Japan & Tsunami, Sendai & Earthquake, etc.
- Whitelists and automation to block known sites and find likely candidates
- Human Review of likely ones.

<http://tsunamireliefforjapan.net>
<http://www.disaster-relief-shelters.org>
<http://thejapanearthquakefund.com>
<http://www.japan-tsunami-relief.org>
<http://www.japanesequake2011.com>
<http://www.donatetojapan.org>
<http://www.japanrelief2011.tk>
<http://www.japanrelieffunds.weebly.com>

<http://www.ihelpjapan.org>
<http://www.helpdonatejapan.com>
<http://www.helpjapan.piczo.com>
<http://www.japanesedisasterrelief.org>
<http://helpmyjapan.com>
<http://helpfirstjapan.org>

donations-help.webs.com

DONATIONS - calm your conscience

http://donations-help.webs.com/donations.htm

Most Visited ▾ Zimbra PowerShark Bugzilla Main Page Traceroute, Ping, Do... IID Twiki Domain Matching Na... VirusTotal - Free On... ThreatExpert - Auto... Internet Identity Pas... Elman's DIC Tool

by Express-Service by JAP/JonDos by TOR FAQ Forum

Search VirusTotal Scan current site

DONATIONS - calm your conscience

calm your conscience



In This Issue:

- Home
- Information
- DONATIONS**
- Discussion Forums
- Guestbook
- Contact Us
- Videos
- Imprint

Recent Videos

-  **Radiation level**
2 views - 0 comments
-  **Explosion at**
3 views - 0 comments
-  **Japan nuclear leak**
2 views - 0 comments
-  **The earthquake and**
2 views - 0 comments

DONATION

the account data are:

Germany

Commerzbank

<u>Account Holder:</u>	<u>Andreas Rzodeczko</u>
<u>Purpose:</u>	<u>spjp</u>
<u>Account number:</u>	<u>630835701</u>
<u>Bank code:</u>	<u>36040039</u>
<u>IBAN:</u>	<u>DE86360400390630835700</u>
<u>BIC - SWIFT:</u>	<u>COBADEFF423</u>

Done

216.52.115.51 off

Same Techniques for Brands

- Search for terms, typo variants
- Group results and drill in on potential offenders
- Set-up alerts on new hits for potential nastiness

The following alerts for "google" were generated on 2010-06-30 at 23:35.
Search terms: google

ggoogle.de
goodgoogle346.cn
google-secrets.com
googlematt.com

- Build cases based on large corpus of offender data

Need a Zone File?

- If it's being used, you can get it via PDNS
- I've solved my ccTLD access problems! 😊
- Subdomain resellers aren't a major issue any more
- Can use the info to understand hostname behavior and properly categorize hosting companies, DNS providers and the like
- Would have REALLY helped ICE when they shut-down mooo.com to have done this kind of analysis (besides just looking at their homepage)

Sample Zones

- .TK – 1 million plus
- Mooo.com – 35K records
 - Just what is stuff like “0wrr6d267.mooo.com” for anyway?
- ibm.com – 947 records
- facebook.com - Just kidding! A bazillion records
- Not 100%, but pretty good coverage

Challenges/Pitfalls/Gotchas

- Not everything is perfect in PDNS land
- False-positives due to shared hosting
- People treating the DNS badly
 - DNS Tunneling
 - Facebook
- Akamai and CDN's
- Domain parking sites

The Future...



ACTIVELY SECURING THE EXTENDED ENTERPRISE

More Sensors Needed – Help!



Use of caching DNS for botnets

- 1) Victim PC is infected
- 2) Attacker registers a domain or subdomain
- 3) Attacker encodes malware binary in a set of CNAME RRs in the authoritative zone with long TTLs
- 4) Attacker queries for malware RR's using popular open recursive servers and those servers cache the responses
- 5) Attacker removes domain used from delegation
- 6) Malware on victim PC uses DNS queries to the same popular open resolvers to acquire code
- 7) Removal of authoritative doesn't mitigate threat because caches of CNAME RRs persist well beyond remediation

Paper by Rodriguez and Hidalgo - <http://goo.gl/LyTnw>

Automating Detection

- Two interesting proposals, Notos, EXPOSURE
- Notos – Dynamic Reputation System for DNS
 - Build reputation and use on new hosts
 - www.usenix.org/events/sec10/tech/full_papers/Antonakakis.pdf
- EXPOSURE – Feature Based System for PDNS
 - Use training on features to tag new hosts
 - www.iseclab.org/papers/bilge-ndss11.pdf

Notos

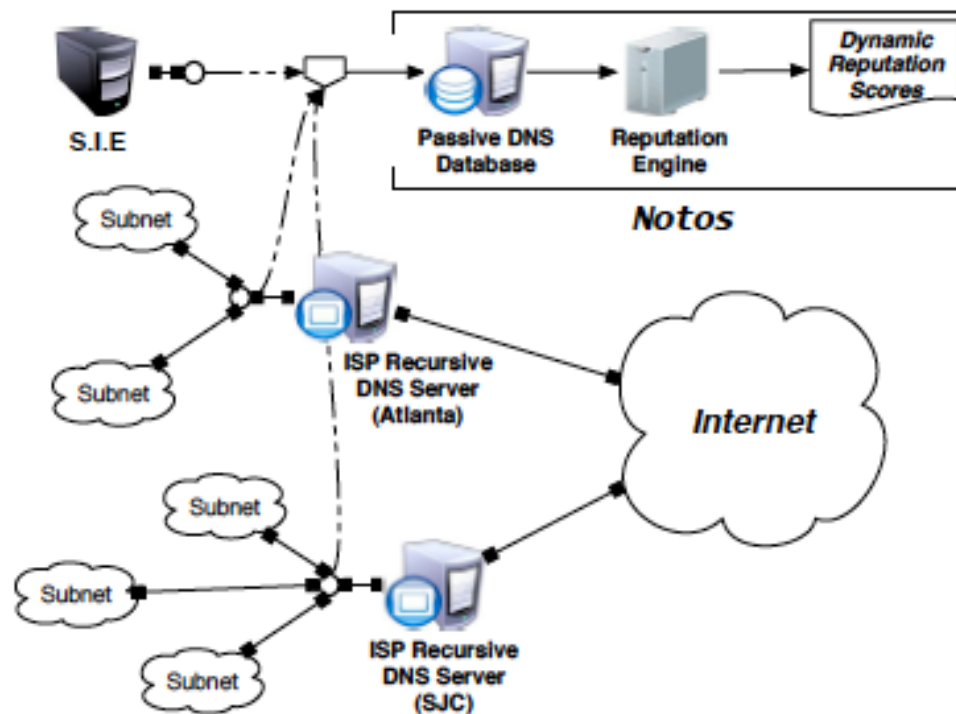


Figure 1. System overview.

Notos

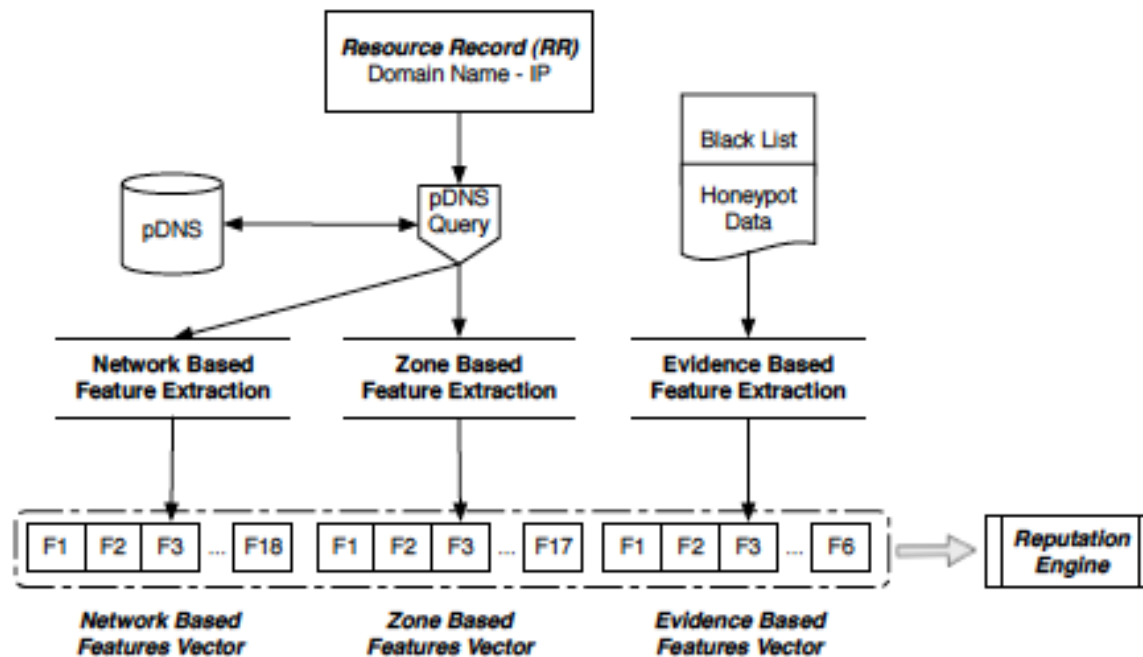


Figure 2. Computing network-based, zone-based, evidence-based features.

EXPOSURE

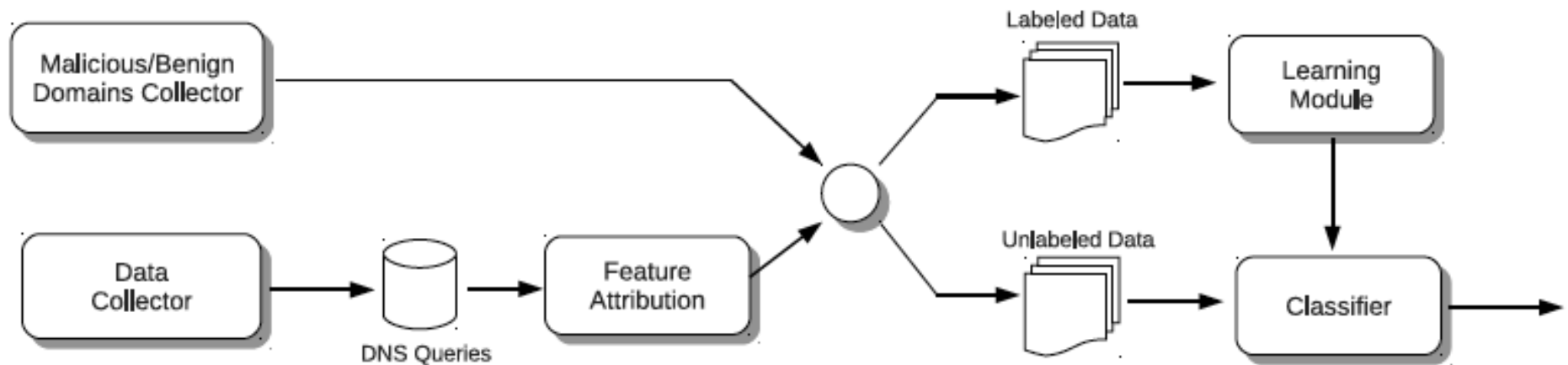


Figure 1: Overview of EXPOSURE

Questions?



ACTIVELY SECURING THE EXTENDED ENTERPRISE

Practical Usage of Passive DNS Monitoring for E-Crime Investigations

Thanks!

Rod Rasmussen

President & CTO, Internet Identity

rod.rasmussen <isat> internetidentity.com