Passive Monitoring of DNS Anomalies

Bojan Zdrnja[1], Nevil Brownlee[1] and Duane Wessels[2]
[1]The University of Auckland, New Zealand
[2]The Measurement Factory, Inc.

DIMVA 2007, Lucerne, Switzerland

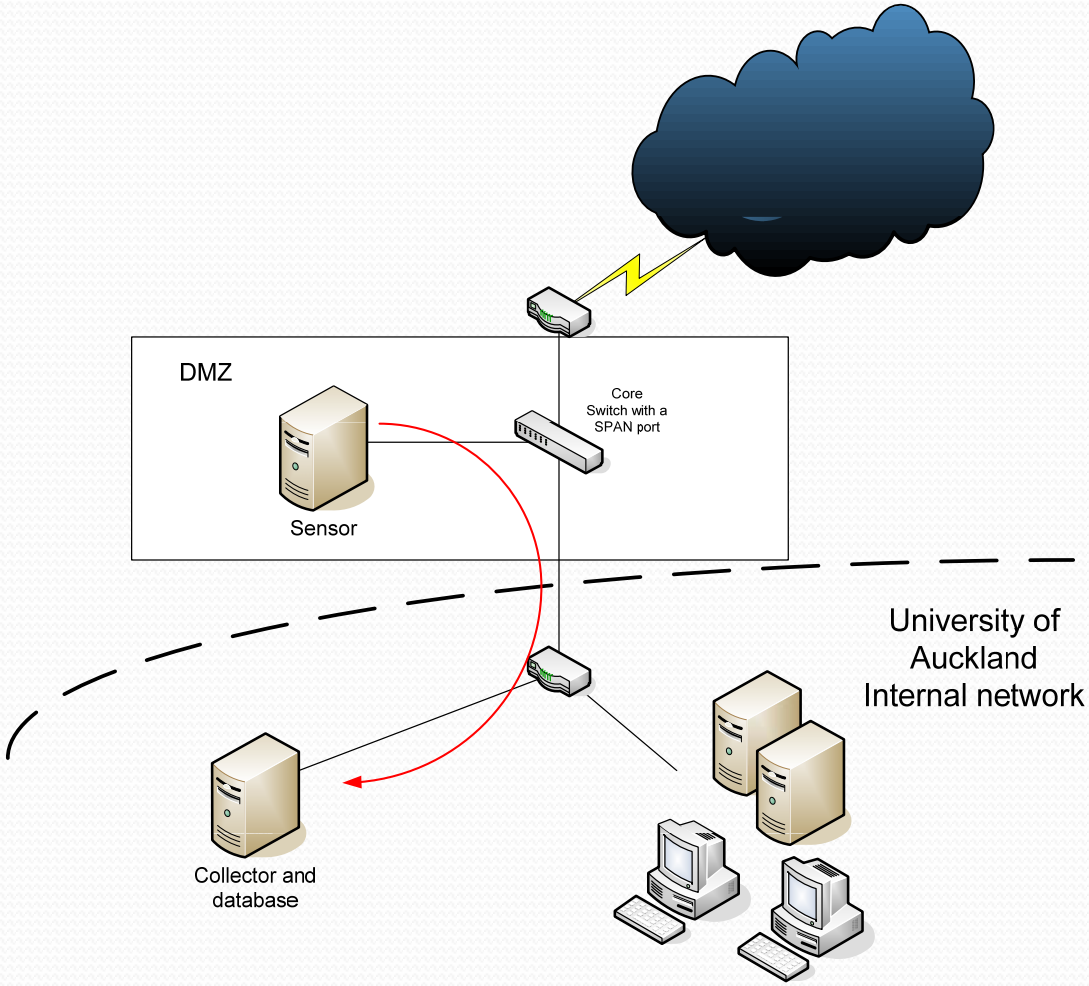
Why do we need passive replication of DNS?

- DNS is distributed
  - Each server is responsible only for its zone
  - There is no way to retrieve the whole zone from a properly configured DNS server
- DNS allows multiple mappings
  - Reverse entries almost never list all mappings
- History of domain name changes is lost
  - DNS keeps no information about previously seen domain names

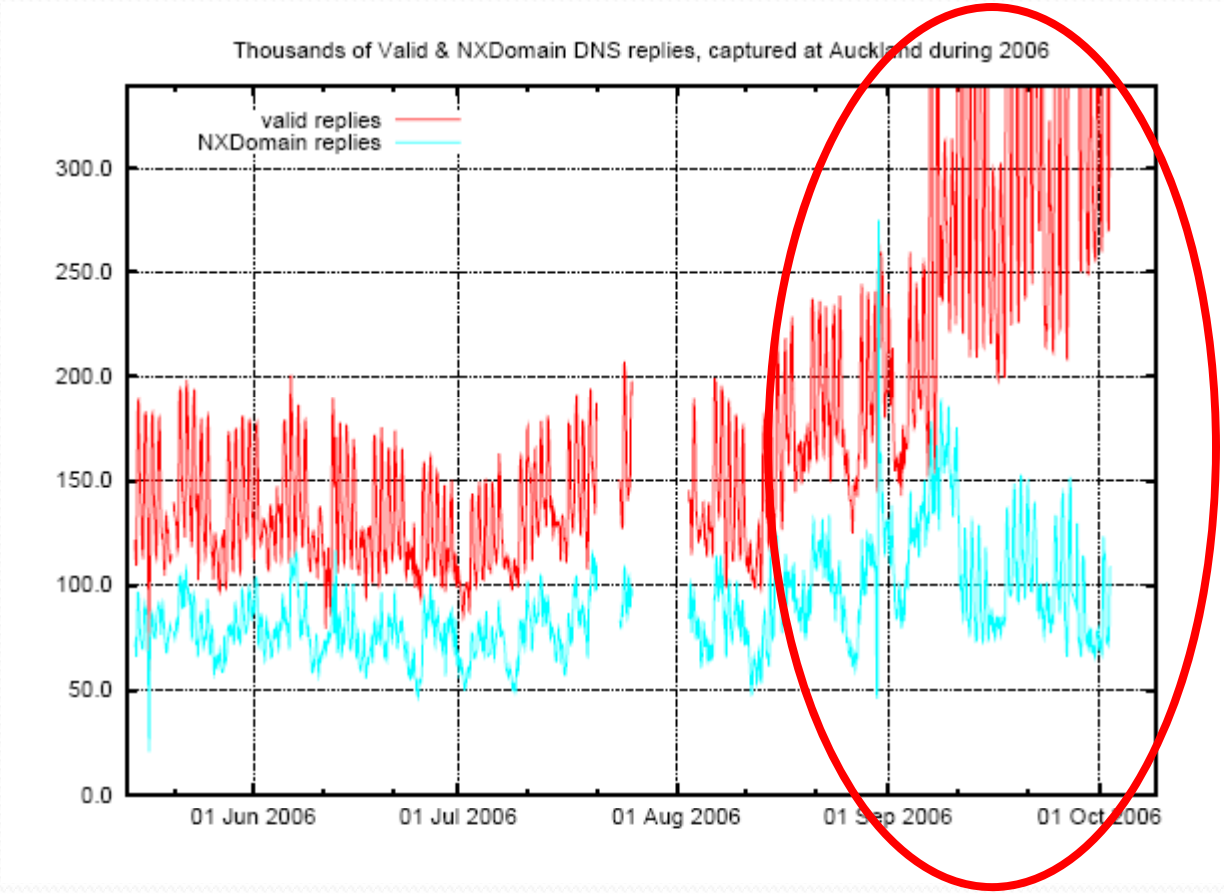
Ways to implement DNS monitoring

- Periodical polling of DNS servers
  - Intrusive, we have to know what we're looking for in advance
- Perform zone transfers
  - Have to get a consent with the DNS server's administrator
- Modify client DNS resolver
  - Impractical
- Modify server DNS resolvers
  - Affects only servers we have control over
- Passive DNS replication by capturing network traffic
  - Non-intrusive, we see all DNS traffic on a link

Passive DNS replication at the University of Auckland

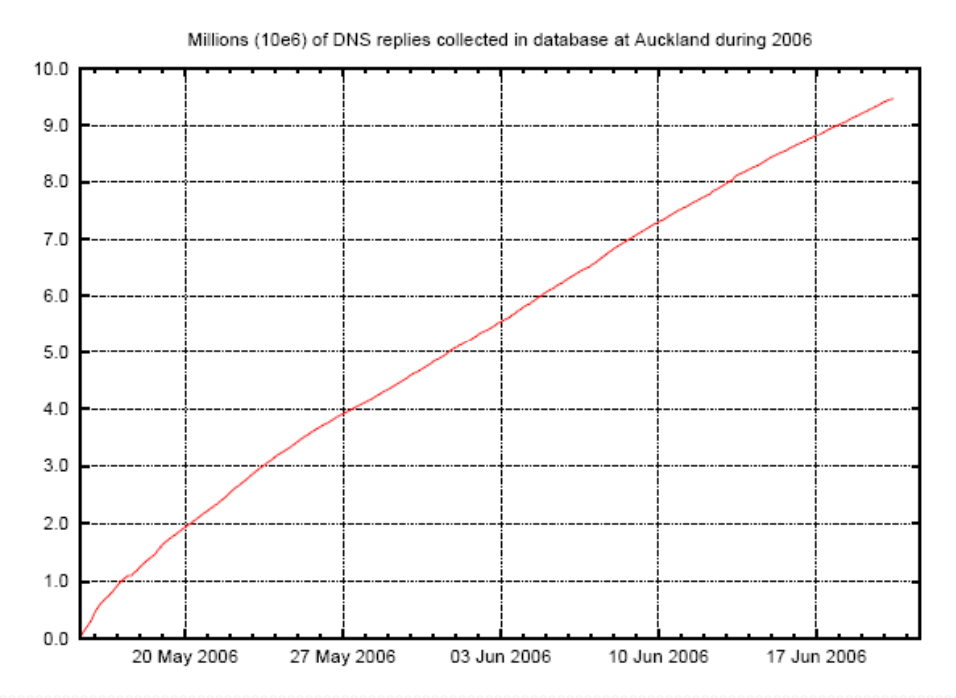


Recorded authoritative DNS replies



Database characteristics (data locality)

RR	Records	%
A	24096932	57.00%
NS	757825	1.79%
CNAME	652126	1.54%
SOA	16281	0.04%
PTR	11261024	26.64%
MX	2433120	5.76%
TXT	3047556	7.21%
AAAA	2202	0.005%
SRV	705	0.002%
Total:	**42267771**	**100%**



Typo squatter domains

- Some kind of social engineering
  - No exploits, based on users incorrectly entering URLs
- Manual inspection revealed several big sites hosting typo squatter web sites
- Most typo squatting sites host hundreds of domains

DNS query	Answer	RR type
www.gmaio.com	64.20.33.131	A
openopffice.com	64.20.33.131	A
www.eikipedia.org	64.20.33.131	A
aukland.ac.nz	64.111.218.142	A
webmail.ec.aukland.ac.nz	aukland.ac.nz	CNAME

Fast flux domains

- Domains with rapidly changing resource records
- Today typically used for command and control (C&C) servers by bot-herders
- Characteristically have low TTL records, otherwise it takes long(er) for clients to resolve the new domain
- Easy to enumerate in the database
- Example: contryloansnow.com domain

Answer	RR type	TTL	Time seen
84.105.118.33	A	5	Wed, 24 May 2006 19:31:10 UTC
84.90.205.67	A	5	Wed, 24 May 2006 21:11:55 UTC
86.203.193.193	A	5	Wed, 24 May 2006 23:21:37 UTC

Anomalous records

- Leaking RFC 1918 address space
  - Such RRs should never be resolvable outside a local network
- Not-recommended characters in domain names
  - Errors with wild card domain names (*.domain.com)
  - Phishing attempts:
    - www.paypal.com%20cgi-bin%20webscr%20cmd—secure-amp-sh-u%20%20.userid.jsp.krblrice.com
- Binary characters in names
  - moll-expert.com MX = \009mailhost.moll-expert.com

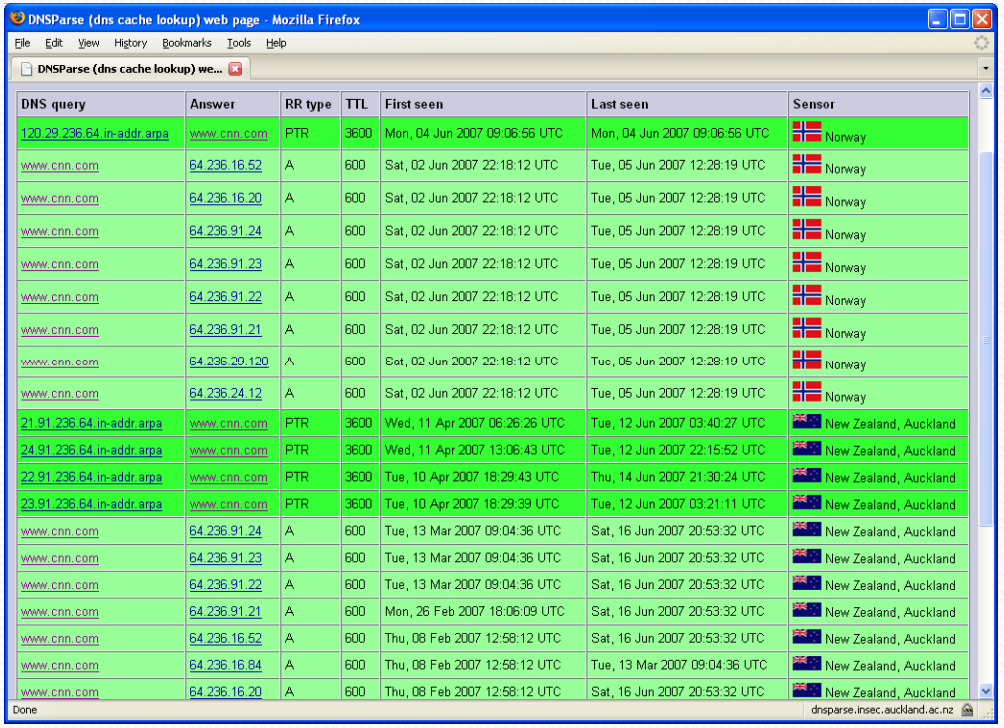
Record reputation

- Fingerprint potentially evil resource records
- Correlate domain names with associated NS or A records
  - Assign scores based on historical behavior of a record

Domain name	NS record	Time seen
mediabid97.com	dns1.ip4dns.com	Fri, 22 Dec 2006 19:22:58 UTC
loudmedia2.com	dns1.ip4dns.com	Tue, 02 Jan 2007 21:41:40 UTC
successcoffee.com	dns1.ip4dns.com	Fri, 05 Jan 2007 15:22:11 UTC
maxisolution.net	dns1.ip4dns.com	Mon, 29 Jan 2007 21:04:35 UTC
craftwireless.net	dns1.ip4dns.com	Wed, 28 Feb 2007 22:06:08 UTC
violetmatched.com	dns1.ip4dns.com	Wed, 21 Mar 2007 16:20:43 UTC
objectstatus.net	dns1.ip4dns.com	Sun, 10 Jun 2007 14:04:03 UTC

Current database

- Expanded; has about 120 million records
- Three sensors: New Zealand, Norway and Bleeding Threats
- Accessible at https://dnsparse.insec.auckland.ac.nz/dns
  - Username: caida
  - Password: dns



DNS query	Answer	RR type	TTL	First seen	Last seen	Sensor
120.29.236.64.in-addr.arpa	www.cnn.com	PTR	3600	Mon, 04 Jun 2007 09:06:56 UTC	Mon, 04 Jun 2007 09:06:56 UTC	Norway
www.cnn.com	64.236.16.52	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.16.20	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.91.24	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.91.23	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.91.22	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.91.21	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.29.120	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
www.cnn.com	64.236.24.12	A	600	Sat, 02 Jun 2007 22:18:12 UTC	Tue, 05 Jun 2007 12:28:19 UTC	Norway
21.91.236.64.in-addr.arpa	www.cnn.com	PTR	3600	Wed, 11 Apr 2007 06:26:26 UTC	Tue, 12 Jun 2007 03:40:27 UTC	New Zealand, Auckland
24.91.236.64.in-addr.arpa	www.cnn.com	PTR	3600	Wed, 11 Apr 2007 13:06:43 UTC	Tue, 12 Jun 2007 22:15:52 UTC	New Zealand, Auckland
22.91.236.64.in-addr.arpa	www.cnn.com	PTR	3600	Tue, 10 Apr 2007 18:29:43 UTC	Thu, 14 Jun 2007 21:30:24 UTC	New Zealand, Auckland
23.91.236.64.in-addr.arpa	www.cnn.com	PTR	3600	Tue, 10 Apr 2007 18:29:39 UTC	Tue, 12 Jun 2007 03:21:11 UTC	New Zealand, Auckland
www.cnn.com	64.236.91.24	A	600	Tue, 13 Mar 2007 09:04:36 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland
www.cnn.com	64.236.91.23	A	600	Tue, 13 Mar 2007 09:04:36 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland
www.cnn.com	64.236.91.22	A	600	Tue, 13 Mar 2007 09:04:36 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland
www.cnn.com	64.236.91.21	A	600	Mon, 26 Feb 2007 18:06:09 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland
www.cnn.com	64.236.16.52	A	600	Thu, 08 Feb 2007 12:58:12 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland
www.cnn.com	64.236.16.84	A	600	Thu, 08 Feb 2007 12:58:12 UTC	Tue, 13 Mar 2007 09:04:36 UTC	New Zealand, Auckland
www.cnn.com	64.236.16.20	A	600	Thu, 08 Feb 2007 12:58:12 UTC	Sat, 16 Jun 2007 20:53:32 UTC	New Zealand, Auckland

Future work

- Data mining on collected DNS replies
- Correlation between records to track malicious and spam related domain names
- Add more geographically dispersed sensors
  - Detecting where certain domain name was first used
  - Is there any data locality?
- Are you willing to participate? Please contact us:
  - b.zdrnja@auckland.ac.nz
  - nevil@auckland.ac.nz