



DNS and Flow

Bulk DNS Analysis

Ed Stoner



DNS and Flow

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Summary

There is a wealth of information in DNS traffic that can add another dimension to flow analysis. We will explore different techniques to analyze DNS traffic and combine that analysis with flow analysis.

DNS packet format

Message Format

Header
Question
Answer
Authority
Additional

Header

ID
QR OPCODE AA TC RD RA Z RCODE
QDCOUNT
ANCOUNT
NSCOUNT
ARCOUNT

Question

QNAME
QTYPE
QCLASS

Answer, Authority, and Additional

NAME
TYPE
CLASS
TTL
RDLENGTH
RDATA

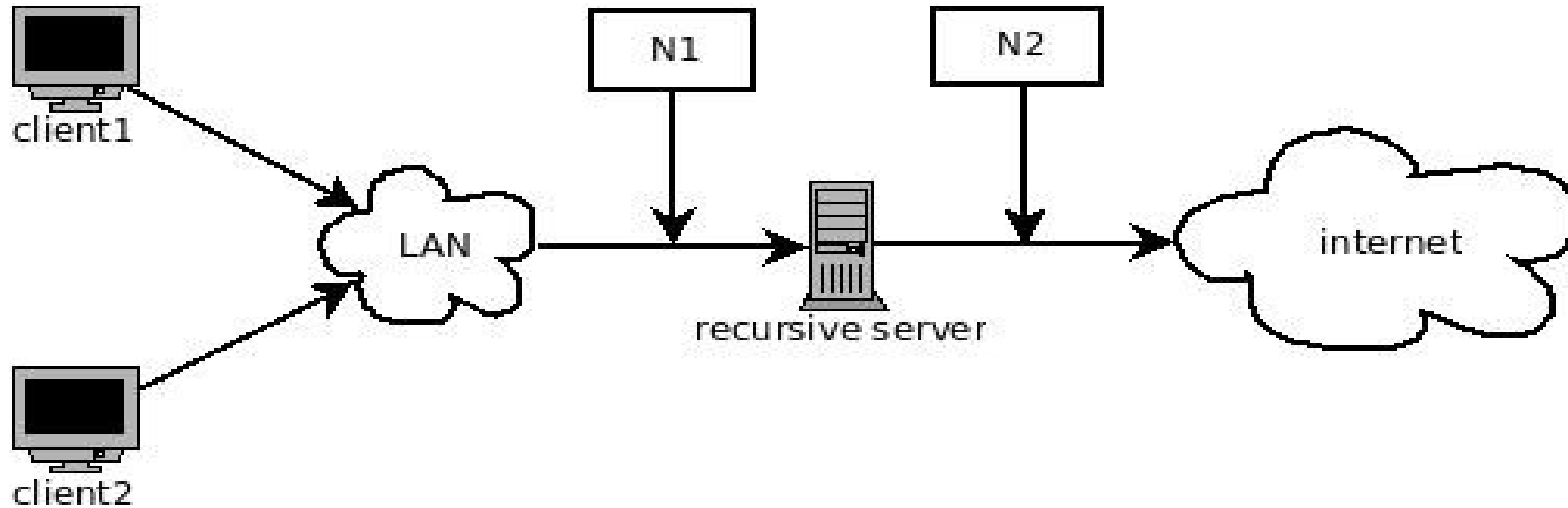
Passive DNS

Why we want to:

- No additional queries for someone to see
- You see more than you otherwise would
- Can detect things you otherwise couldn't
- You see what machines actually used ...

Passive DNS

Why we need to:



Client1: www.goodsite.com, 10.1.2.3

Client 2: www.badsite.com, 10.1.2.3

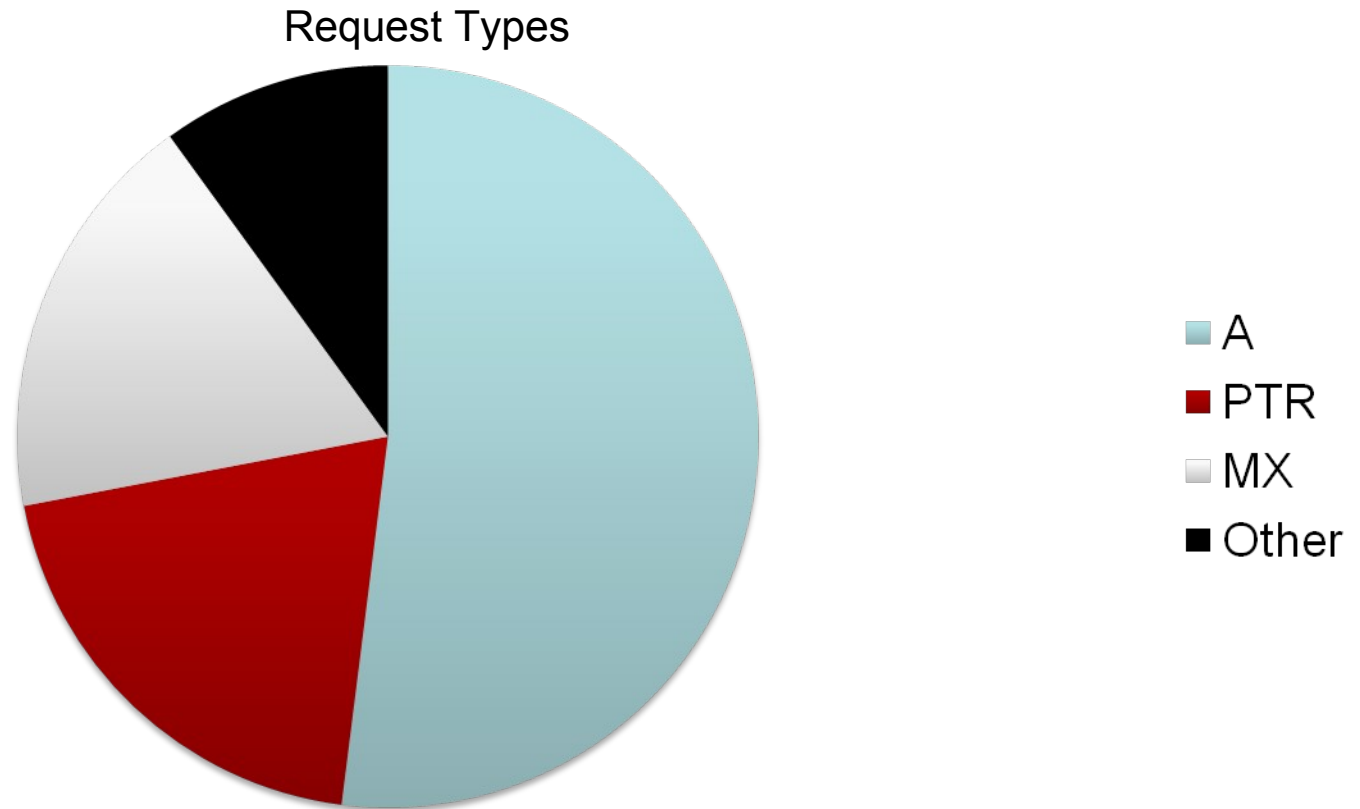
N1: one to one mapping

N2: one to one, one to many, no mapping

Our Setup

- SIE channel 5
 - ~ 260 million packets/day (3100 packets/sec)
 - Represents ~ 370 million packets (de-dup over 4 hours)
 - ~ 200 Bytes/packet
 - ~ 56 GB day raw / ~ 17 GB day with gzip
 - 200,000 msgs per file, ~ 1200 files per day
 - Typical query time between 30 min and 2 hours

Traffic Summary



RBLs account for many millions of A record request per day

For certain networks, up to 80% of lookups are to RBLs

common RBLs seen: ciphertrust.net, vcxde.com, borderware.com, sonicwall.com, fzrbl.org

Fast Flux

- Lots of IP addresses per one domain name
- Provides better uptime for bad sites
 - Load distribution
 - Hard to trace
 - Hard to takedown
- How to find
 - Iterate over message with
 - Low ttl (less than 2000 seconds)
 - Lots of A records per message (10 or more)
 - Iterate by qname of possible messages
 - Total number of uniq A records/IP addresses (25 or more)
 - Total number of ASNS (20 or more)

Fast Flux found (10/20/2009,10/23/2009)

brewers-ca.com.til1tlli.net.
brewers-ca.com.tll1tlii.com.
brewers-ca.com.tll1tlli.net.
cadtrans.net.til1tlli.com.
cpan.cpanel.net.
csajn.com.
dessaxzaa.co.uk.
diff.cpanel.net.
doubleclickr.ru.
ffffefvl.co.uk.
heiiikuv.eu.
httpupdate.cpanel.net.
layer1.cpanel.net.
layer2.cpanel.net.
mgpra.com.
okkkikla.eu.
okkkikll.eu.
rdate.cpanel.net.
rdate.darkorb.net.
rref1aaz.eu.
sclrz.com.
til1tlli.com.
til1tlli.net.
tll1tlii.com.
tll1tlli.com.
tll1tlli.net.
ttl1lil.com.
ttl1lil.net.
ttl1lll.com.
ttl1lll.net.
townternet.capitalonebank.com.f1iiti.net.
townternet.capitalonebank.com.f1iitl.com.
townternet.capitalonebank.com.f1iitl.net.
townternet.capitalonebank.com.f1liitl.com.
townternet.capitalonebank.com.ltiil1.com.
townternet.capitalonebank.com.ltiil1.net.
townternet.capitalonebank.com.ltiil1.com.
townternet.capitalonebank.com.ltiil1.net.
townternet.capitalonebank.com.ltiil1.com.
townternet.capitalonebank.com.ltiil1.net.
townternet.capitalonebank.com.ltiil1.com.
townternet.capitalonebank.com.ltiil1.net.
townternet.capitalonebank.com.racder1c.net.
townternet.capitalonebank.com.racder1x.com.
townternet.capitalonebank.com.raeder1f.net.
townternet.capitalonebank.com.rarder1g.com.
townternet.capitalonebank.com.raxsder1.com.
townternet.capitalonebank.com.raxsder1.net.
townternet.capitalonebank.com.rzasder1.com.
townternet.capitalonebank.com.t1fliil.tc.
townternet.capitalonebank.com.yyy1yyrd.co.uk.
townternet.capitalonebank.com.yyy1yyre.co.uk.
townternet.capitalonebank.com.yyy1yyrf.co.uk.
townternet.capitalonebank.com.yyy1yyrg.co.uk.
townternet.capitalonebank.com.yyy1yyrj.co.uk.
townternet.capitalonebank.com.yyy1yyrk.co.uk.
townternet.capitalonebank.com.yyy1yyrl.co.uk.
townternet.capitalonebank.com.yyy1yyrm.co.uk.
townternet.capitalonebank.com.yyy1yyro.co.uk.
townternet.capitalonebank.com.yyy1yyrq.co.uk.
townternet.capitalonebank.com.yyy1yyrr.co.uk.
townternet.capitalonebank.com.yyy1yyrs.co.uk.
townternet.capitalonebank.com.yyy1yyru.co.uk.
townternet.capitalonebank.com.yyy1yyrv.co.uk.
townternet.capitalonebank.com.yyy1yyrx.co.uk.
update.microsoft.com.bbtyak.co.uk.
update.microsoft.com.bbtyak.org.uk.
update.microsoft.com.bbtyam.co.uk.
update.microsoft.com.bbtyam.me.uk.
update.microsoft.com.bbtyap.co.uk.
update.microsoft.com.bbtyap.me.uk.
update.microsoft.com.bbtyaz.co.uk.
update.microsoft.com.bbtyaz.me.uk.
update.microsoft.com.dessaxqaa.co.uk.
update.microsoft.com.dessaxzaa.co.uk.
update.microsoft.com.dessaxzaa.me.uk.
update.microsoft.com.dessaxzaq.co.uk.
update.microsoft.com.dessaxzaq.me.uk.
update.microsoft.com.gerrasawa.eu.
update.microsoft.com.heiikok.eu.
update.microsoft.com.heiikoy.eu.
update.microsoft.com.heiikul.eu.
update.microsoft.com.heiikum.eu.
update.microsoft.com.heiikuv.eu.
update.microsoft.com.heiikuy.eu.
update.microsoft.com.n111sae.eu.
update.microsoft.com.n111sak.eu.
update.microsoft.com.n111sap.eu.
update.microsoft.com.n111saq.eu.
update.microsoft.com.n111say.eu.
update.microsoft.com.n111saz.eu.
update.microsoft.com.okkkikf.eu.
update.microsoft.com.okkkikkl.eu.
update.microsoft.com.okkkikla.eu.
update.microsoft.com.okkkiklf.eu.
update.microsoft.com.okkkikll.eu.
update.microsoft.com.okkkiklo.eu.

Malicious Domains

- Registered by bad actor – not compromised
- How to find
 - Cheat by starting with list
 - APWG
 - Maybe won't have to
 - Name has large amount of unique characters (over 20)
 - Name has tld in middle (www.yourbank.com.imbad.com)

Other

- DNS exfiltration/tunneling
 - Over 40 uniq chars in qname
- DNS amplification
 - For DDOS participation
- Outbound connections with no previous resolution
- DNS rebinding
 - www.attacker.com -> some.public.ip, ttl = 2
 - www.attacker.com -> 10.1.mydatabase.ip
- Just plain out of the ordinary
 - ns1.ziyouforever.com (zi you men – “door to freedom”)
 - 784bc3c09961b67b5f3f6f6783a54881b59f5e53680937d7ce281407.6.bnhyj.com
 - 08f0b06a25a5cf1f9df501bc39306fbc6ff7875646817b4845c17da0.6.ewsz.com

On with the flow

- How to use results with flow
- Pysilk

```
import ncap
import sdnslib
import silk
ips = silk.IPSet()
f = ncap.ncapfile('/path/to/my/file')
for msg in f:
    dnsmsg = sdnslib.message(msg.payload)
    for rr in dnsmsg.answers:
        ips.add(rr['address'])
ips.save('/path/to/my/ip.set')
```

IPs to names

```
import ncap
import sdnslib
import silk
lookup = {}
for msg in ncap.ncapfile('/path/to/my/file.ncap')
    dnsmsg = sdnslib.message(msg.payload)
    for rr in dnsmsg.answers:
        lookup[rr['name']] = rr['address']
for rec in silk.SilkFile('/path/to/my/file.rw')
    print lookup[rec.dip]
```