# Defeating DNS Amplification Attacks

## Ralf Weber

### Senior Infrastructure Architect

# History

- DNS amplification attacks aren't new
  - Periodically reemerge as attackers read history books ☺
- NANOG 56
  - Reports of unusual DNS traffic on *authoritative* DNS servers
- Resource Rate Limiting (RRL) proposed for nameservers
  - Subsequently implemented in BIND, NLNet NSD, Knot, more
  - NLNet paper shows effectiveness for certain attacks
- Largest DDoS ever uses open resolvers - April 2013
  - 300Gbps targeted at Spamhaus
- Providers worldwide see attacks using their DNS *resolvers*
  - Trouble for networks: load balancer failures, saturated links, server stress, operational duress
  - No media headlines but lots of targets suffer with traffic spikes

# *Quick* Introduction

Amplification attacks rely on:

- Spoofed IP source addresses
- UDP as transport
- Small DNS questions that generate large DNS answers
  - ANY queries are an old favorite, 80x amplification
  - DNSSEC-signed zones were an early favorite, but seem to have diminished
  - Other query types showing up: TXT, even A/AAAA
  - Attackers appear to be creating "purpose built" RRs

# What amplification can be achieved?

One commonly used query in the past   “ANY ripe.net"
Yields an impressively large answer  (MSG SIZE  rcvd: 2884):

```
; <<>> DiG 9.8.3-P1 <<>> ripe.net any @64.89.232.93 +edns=0 ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64292 ;; flags: qr rd ra; QUERY:
1, ANSWER: 26, AUTHORITY: 6, ADDITIONAL: 3  ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 4096 ;; QUESTION SECTION: ;ripe.net. IN ANY  ;; ANSWER SECTION: ripe.net.
197 IN RRSIG NSEC 5 2 300 20131109122844 20131010112844 2473 ripe.net. dOdaF81ic+j6DscNMdBVVAEPt7SLXpZ0bIR4Jnh+4c53RbhnM8HH46Gx jfYAB2COZKdWnkwMbW/
ifnX3c6gGcz7uRoMFWZMTHBXPtvZjyLDj/thR CrO2ntlLdP8MrM5EUyq35FiSDNIv1uyzaEo9rXNsMGjMH2bd5cQqSpbV yLU= ripe.net. 197 IN NSEC 256cns.ripe.net. A NS SOA MX AAAA RRSIG
NSEC DNSKEY ripe.net. 197 IN RRSIG MX 5 2 300 20131109122844 20131010112844 2473 ripe.net. AJfdeBOkOwdMTfybgvidmHeeQzm6ybwxLEN1qcPp2YQvoWE2VbrLmeUo
JiKvecGHQlACBr1VKuguGq++bEYTXbGkragc7iG19SaisTHwWFZHLjka l3xhXL2q890pnyKpIYFGf6ZPmSYebC92BYQDGXtqnwpyvwghhLoYysQ0 ZAA= ripe.net. 197 IN MX 250 postlady.ripe.net.
ripe.net. 197 IN MX 200 postgirl.ripe.net. ripe.net. 3497 IN RRSIG NS 5 2 3600 20131109122844 20131010112844 2473 ripe.net.
RGDUw6Cu6Sh7zixsKiiJyDIIkEZEK4LagEl09s6ZnGN27GQAFHkSE9up IkAfsaJWe3Nl9fjQFWfJ/hZ5rHcgsz5LD/eK4W5VUWpZc6BX0YuikxPb LSxMoFebAkqRkIEp7TTMRUuaZyTK
+m0UadLgpp0nYX8eE6uzE8Cj2Zv0 xog= ripe.net. 197 IN RRSIG AAAA 5 2 300 20131109122844 20131010112844 2473 ripe.net. CiltCl8jysHsg2MHsU/
4bPlt7jYaFSJGZnMe0NcTACnCocAEO3+B5Y7s 9QQDWXAxVyXTPs9dtiAdEtLOH0R0TBH45I+OExxhS5CWYBJO+TWghV/r
WNyFOuUDAlFmP2KdgPpMRqfw49l7o75owbnAjefcyVZ32OtBX50LTDBe 10A= ripe.net. 197 IN AAAA 2001:67c:2e8:22::c100:68b ripe.net. 21497 IN RRSIG A 5 2 21600 20131109122844
20131010112844 2473 ripe.net. FIR1BIoGLmKUmvDHvhmDBzV6q2YXmLpZ8KpPfVw9Dw2k/O6EBSx+mXwq lvWuUdtSlBhgfYqVgB50HFKCRrDbNzUSZE9E0SQKMJR8PFu6EGckJF2P
dBveonSJowyYgqE7l+4BHB1Cx5csEO+VSCl7uiE99CcqyhvkYnGeJcY0 Ckk= ripe.net. 21497 IN A 193.0.6.139 ripe.net. 3497 IN RRSIG SOA 5 2 3600 20131109122844 20131010112844 2473
ripe.net. GKCyXEz2xtCj0czgyZ6CEPzL7BNldfK1iz7JiFaIw87UEZA1OjY2rP04 qsU1Bt9KPMHWkVY9EqJEshgSwbGRdy/1Y0LDZpYYHszvBOlkpu/JxcVR G/
NI23fvzs96Mc5iTp3ovuhLQfgS0z31oJJMd4yowcRL4dhs1jmgmeL/ nqQ= ripe.net. 3497 IN SOA pri.authdns.ripe.net. dns.ripe.net. 1381407901 3600 600 864000 300 ripe.net. 3497 IN RRSIG
DNSKEY 5 2 3600 20131109122844 20131010112844 60338 ripe.net. EbHIOgtEY/NV4DMXZpcqXFlVflCcaRD+gpXnyRnu11x4EZAFbYXl42HG
OxTZE7Z168qxHuLCeVKat0L0w7nh5ShVpfPUXhdt+fVXoDukI19aAgWy yDmaVd4zm2ZKC8E3LKkNzS9xUksx+laEC7Ff/+3GVuhi/AVL8NC/A3bP vPoxe5MRPZ/
OGwd5aQtvgm811lysdOPZWbqSJDRKTeanAyhIk8FLN2hm tRLTKJFArDakOgpmZI1GA/3dfojRlBIpuNip4c6xDI6Y9gJW+3OMj8lZ cvleUNdJ188ujS9z6fQr6zOdIwVmdZWwCYd
+rbr6dhvEzILrK8hFbJsB LjbkSg== ripe.net. 3497 IN DNSKEY 256 3 5 AwEAAX7Dm18EOseQjbKJQDhhFqkfNMjW4z2miK5/+3j33krF2KungE43 AMmUo3hgjND4A547zCLTYGV
+TchFXtVwdErJtLKs1giAfkrpvl9hYxY+ eOFSLSPFU6n8BQd7lsIqdynQ0iG9aGk6k1DAne9zWUW6x37duiBagLUB 4/yLguoT ripe.net. 3497 IN DNSKEY 256 3 5 AwEAAZYzmLhqQKDgm
+OA5gfvGU6Twt9WuF2P5akXQxZxATZ79apyjW6K 1ZFeZ76Yo3L4EoGEkSBntx0m7Gacr/ry9oGmmyhK5oS9EfeitHdAV14F gkN+Qi0ROmt32rGDSFIY210fbLobwuBCCo6C
+2hYbB2CeNHF6BtYivGL arBaCt2F ripe.net. 3497 IN DNSKEY 257 3 5 AwEAAXf2xwi4s5Q1WHpQVy/kZGyY4BMyg8eJYbROOv3YyH1U8fDwmv6k BVxWZntYtYUOU0rk+Y7vZCvSN1AcYy0/
ZjL7cNlkc3Ordl2DialFHPI6 UbSQkIp3l/5fSWw5xnbnZ8KA7g3E6fkADNIEarMI4ARCWlouk8GpQHt1 1wNW1c65SWB8i958WZJ6LI0pOTNK+BIx8u98b+EVr7C08dPpr9V6Eu/7
3uiPsUqCyRqMLotRFBwK8KgvF9KO1c9MXjtmJxDT067oJoNBIK+gvSO9 QcGaRxuGEEFWvCbaTvgbK4E0OoIXRjZriJj8LXXLBEJen6N0iUzj8nqy XSCm5sNxrRk= ripe.net. 3497 IN DNSKEY 257
3 5 AwEAAYSPd7+AJXOT1k1d6eUKRCsw5cSGpzsWIjVCDjbWdNomt4mCh5of SSnf60kmNCJgeCvPYwlOWX08TPLpCHqvBh8UERkaym8oT0U2lKrOt+0W EyksYc5EnLp7HQVvH
+KaF8XiuPsemLLNbhosGofv5v0Jj2TKxJl/sgf1 n9WtkMY1bCTTaSUn5GmjKDv0XRPKkzA4RCQv8sl8pZ2pzJvIxpN0aBgx
WtRjWXXJ27mUq6+PR7+zgBvLkmSV4F1bNXOgikeN5KBlutEKBKYYcYRb fR5kDYYJ0mV/2uTsRjT7LWNXAYAJ88xuZ4WcBV01EuMzsZU21iGhRO1N Z4HFSr9jb3U= ripe.net. 86297 IN RRSIG
DS 8 2 86400 20131017044449 20131010033449 55565 net. GTgWhptNaMhw9gld4KrnVunBMQwgOwH8rSS16BCkrliSy9sOLSqTvt6l ElTrEMarfeZ3TL0NlcLkOLtddPtUl791/
Iib219s76ekGyysVeoaFkkm OBn0zcvDX9joDHleBb/UuuRA+HFiV3DnicGgZQXnaEZDkfHfUrxOyt2F JMU= ripe.net. 86297 IN DS 60338 5 2
61D99D98D0C374C1157F73282DB3E29E61E365DD9EBA435802D27A69 847C24FC ripe.net. 86297 IN DS 60338 5 1 1CB13971FC7D4DF7CB3C6EB82DF0868687FE6371 ripe.net. 3497 IN
NS ns3.nic.fr. ripe.net. 3497 IN NS pri.authdns.ripe.net. ripe.net. 3497 IN NS sec3.apnic.net. ripe.net. 3497 IN NS sns-pb.isc.org. ripe.net. 3497 IN NS tinnie.arin.net. ripe.net. 3497 IN NS
sec1.apnic.net.  ;; AUTHORITY SECTION: ripe.net. 3497 IN NS sns-pb.isc.org. ripe.net. 3497 IN NS tinnie.arin.net. ripe.net. 3497 IN NS sec3.apnic.net. ripe.net. 3497 IN NS sec1.apnic.net.
ripe.net. 3497 IN NS pri.authdns.ripe.net. ripe.net. 3497 IN NS ns3.nic.fr.  ;; ADDITIONAL SECTION: pri.authdns.ripe.net. 3497 IN A 193.0.9.5 pri.authdns.ripe.net. 3497 IN AAAA 2001:67c:e0::5  ;;
Query time: 337 msec ;; SERVER: 64.89.232.93#53(64.89.232.93) ;; WHEN: Thu Oct 10 16:34:07 2013 ;; MSG SIZE rcvd: 2884
```

There are lots of similar queries
Attackers also creating “purpose built” amplification zones (more later)

# Some Simple Math

A relatively low bandwidth home broadband connection  (~2-3 Mbps) can generate 58 Mbps at a DNS server!

18 home connections = ~ 1Gbps of traffic

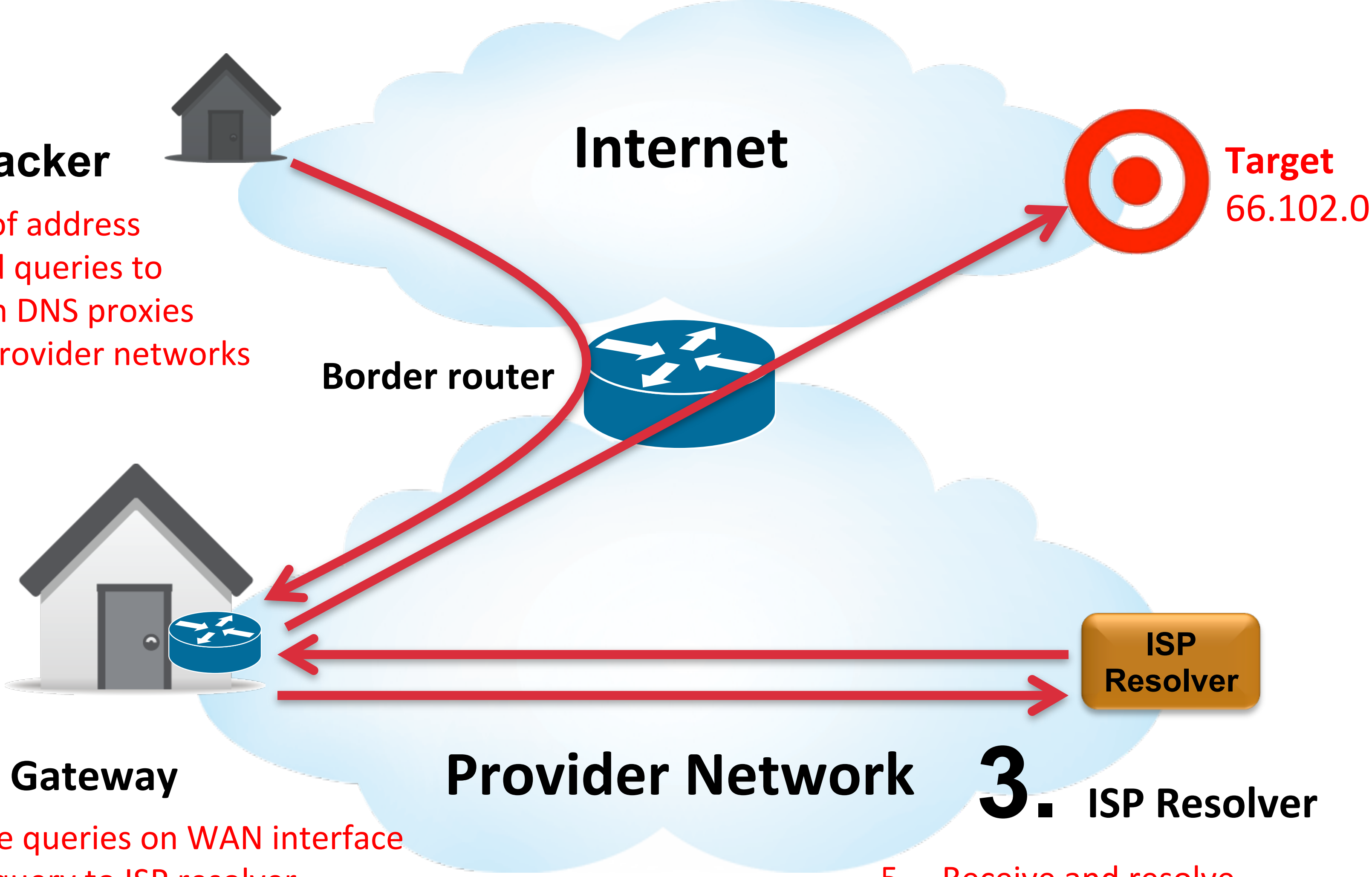
A few thousand connections = 100s of Gbps as was seen with attack on spamhaus

Mustering these kinds of resources is pretty easy

# Several Variants of Amplification Attacks

- Send queries directly to authoritative servers
  - Response Rate Limiting can help
  - But attacks can be modified to make RRL less effective, distribute, query different names etc
  - More work needed here, but *not* the topic of this presentation
- Send queries to open resolvers on the Internet
  - Works well but Best Practices will deter these attacks
    - Shut down open resolvers or limit IP ranges that can access the server  when possible
    - *Closely* monitor for attack activity
    - Not the focus of this presentation, but some techniques discussed here apply
- Send queries to ISP resolvers via home gateways
  - Huh?

# Using ISP Resolvers for DNS Amplification



**1. Attacker**

1. Spoof address
2. Send queries to open DNS proxies on provider networks

**2. Home Gateway**

3. Receive queries on WAN interface
4. Proxy query to ISP resolver
7. Forward answer to Target

**3. ISP Resolver**

5. Receive and resolve query
6. Answer the query as it’ s from a legitimate user!

# How Did We Figure this Out?

- Many reports from ISPs about attacks on their networks
  - isc.org/ripe.net in the most used domains
- Interesting work from openresolverproject.org
  - Millions of open resolvers
  - Scan with CHAOS query returns versions of resolvers
- A BIG surprise
  - *445,881* Open Vantio Resolvers What?
- We have not sold *anywhere near* 445,881 copies of Vantio
  - If we had I guess I would not be giving this talk here today
  - Someone is stealing our SW! (and they're not even using it right!)

# How to find the real resolver

- No, something else must be going on
  - Customers seeing attacks restrict IP ranges ("closed” resolvers)
  - Queries have to be coming from legitimate IPs
  - What's going on?????
- Setup special domain restest.rwdns.de
- Ask unique every open resolver/proxy
  - dig 64.195.2.130.restest.rwdns.de @64.195.2.130
  - On auth server the resolver query source is seen::

```
querystore.replay duration=10m filter=((zone (true
(restest.rwdns.de))))
{
    client-address => '74.125.183.18#56355'
    local-address => '78.46.109.173#53'
    name => '64.195.2.130.restest.rwdns.de'
```

# More Tricks from Attackers
# Purpose Built Amplification Domains

- Domains purpose built for amplification are being uncovered
  - Offline analytics on DNS data sets
  - Network operators parsing log files
- Very large message sizes have been observed:  ~4096 bytes!
  - A, MX, and  Text  records
  - Dummy data
  - Some domains have real data with some record types (A, AAA) and bad with others (TXT, ANY)
  - Some admins just don't understand the effects there entries can have (dual use domains ;-)
    - 250 MX different mx entries might not be a good idea
    - Several 4096 bits DNSKEY might be more secure but…

# Advantages of This Approach (for attackers)

- ISP resolvers are a great resource
  - Lots of them out there
  - Usually high capacity
  - Reliable and available
- Best Practices won't help!
  - Spoofing protections within provider network won't work
    - Spoofed packets enter at the network border
  - Restricting resolver IP Ranges doesn't work
    - Queries appear to be sourced from internal IP ranges
- Filtering DNS queries at the border isn't an option
  - Other DNS traffic: incoming answers to recursive queries from provider resolvers, incoming queries to authoritative servers
  - Subscribers may run DNS servers
- Upgrading Home Gateways is challenging (impossible?) - lots of running room -

***So what WILL work?***

# What can be Done?
# Capture Basic Resolver Log Data

- Have DNS logging turned on all the time
  - Essential resource to identify attack activity
- Get a “dashboard” up so baseline DNS operation is always visible
  - Familiarity with "normal" makes it easier to spot changes
  - Queries per second, settable graph window
  - Top domains queried – scrollable through a few hundred domains
  - Distribution of Query Types
  - Check for domains that yield the biggest responses

# Here’s how we can detect stuff

```
statmon> querystore.top-domains filter=((response-size-ge (true
(1500)))) duration=1d
{
     type => 'querystore.top-domains'
     domain => 'isc.org'
     percentage => '69.9'
     qps => '1.655'
     count => '143036'
}
{
     domain => 'doc.gov'
     percentage => '28.9'
     qps => '0.684'
     count => '59079'
}
```

# More detection

- querystore.group-count group-by=(name query-type ) filter=((response-size-ge (true (1500)))) duration=1d

```
{
    name => '34.30.46.207.in-addr.arpa'
    query-type => 'PTR'
    count => '4'
}
{
    name => 'doc.gov'
    query-type => 'ANY'
    count => '3623'
}
{
    name => 'www.djcgrafix.netfirms.com'
    query-type => 'A'
    count => '95'
}
```

# What can be Done? Ingress Filtering of Queries

- Less work for the resolver – drop on ingress
- Filtering at the resolver less of a problem than at Authoritative server
  - Less exposure of Kaminsky style attack
    - Far less attractive targets: Individual hosts (stub) versus resolver
    - Can filter ISP resolver addresses
- Filter incoming queries by Query Type
  - Weed out simple attacks - ANY queries
- Filter incoming queries by Query Type *and* domain name
  - Finer grained filtering minimizes collateral damage

# What can be Done? Filtering Based on Reputation Lists

- Defend against purpose built or “dual use” domains
  - Need to trigger action based on a specific FQDN
  - Additional selection on query type
- What should the purposed action be?
  - Drop not as bad for a resolver as for an authoritative server, but should only be used at last resort
  - Forcing real clients to TCP seems to be a better way
  - Hopefully stub resolvers speak TCP….

# Sample policy

```
lvp-list.add name=dropamplify-exact element-type=name
lvp-list.add name=dropamplify-sub element-type=name

lvp-policy.add name=dropamplify action=drop selectors=(and ((qtype (ANY)) (or ((qname (dropamplify-exact exact)) (qname (dropamplify-sub subdomain ) ) ))))
lvp-binding.add view=world policy=dropamplify priority=100

lvp-node.add list=dropamplify-exact name=.
lvp-node.add list-dromamplify-sub name=ripe.net
```

# It’s All About Size

- As attacks get more subtle they'll be harder to detect
  - Purpose built domains
  - Utilize domains where admins have screwed up.
  - Multiple domains in one attack
  - Possibly less amplification per query
- How do we detect that
  - Log query response sizes
  - New metric “*top traffic domains*”
  - What names generate the most traffic?
  - What clients generate the most traffic?
- Script to generate list of top traffic generators to mitigate an attack

# Samples

- isc.org ANY
- doc.gov ANY
- irlwinning.com A or ANY
- 34.30.46.207.in-addr.arpa PTR
- outmail.zyngamail.com A
- www.djcgrafix.netfirms.com A
- ‘.’ ANY

# isc.org

```
dig isc.org any

[..]
;; ANSWER SECTION:
isc.org.      6836 IN   TXT "$Id: isc.org,v 1.1855 2013-09-26 21:27:44
bicknell Exp $"
isc.org.      6836 IN   TXT "v=spf1 a mx ip4:204.152.184.0/21
ip4:149.20.0.0/16 ip6:2001:04F8::0/32 ip6:2001:500:60::65/128 ~all"
isc.org.      6836 IN   RRSIG   TXT 5 2 7200 20131031022653 20131001022653
50012 isc.org. lgN51hBVR3EDuDL7MyfYdQ+Is3VzA2rvEZNSM2eZS4zKmwY+YlELi4Yh
BXuzFtK9Rg3N0CON6/SQJYA8TuUG78UE9OoP4/nLkOaDHLkHMTgq1yHz
8oJ0n5mzHIcNgYqphd34yRjBoldjtE9Rhrp4Q3aGVyzW21nPY6NIRlAW BNk=
[..]
;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:31:07 2013
;; MSG SIZE  rcvd: 2045
```

# doc.gov any

```
dig doc.gov any
;; Truncated, retrying in TCP mode.
[..]
;; ANSWER SECTION:
doc.gov.     25   IN   DNSKEY   256 3 8 AwEAAeBP9cEQR3eTa4u1x3WpLwnCog7rw/
l22hXgwiHZIjGAz26+l/cW
+QEHS9bAlJnRtZhmlBYN72DvfpshuEL2o6hh2yVw7wcRC4fNOTxOeury
wLrkKZQE0WC4fyaxlXJsIWRwLEb3H4YYQibGbPRWyGy1NDnapp/sj4AX
53p7RM2rHWcFc89KZ7vJMMzgmZF2v+jo96OGJU7g2Nu4vEZzj8iMJCT6 BGolQRVE/
svYmrqdWpQoIJ/SCPIp//tkZlKo5J2JNwgO4H01ZPr+Bse3
mdznrJ33FYj2waOL8d9Km2GN3h6U8UhAS9GHUMc2IsjCF1GN6OdnC0KI s8KKshwLLK0=
[..]
;; Query time: 11 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:34:09 2013
;; MSG SIZE  rcvd: 8161
```

# irlwinning.com

```
dig +trace irlwinning.com any
[..]
;; ANSWER SECTION:
irlwinning.com.      4045 IN   NS   ns1.irlwinning.com.
irlwinning.com.      4045 IN   NS   ns2.irlwinning.com.
irlwinning.com.      21578     IN   A    1.1.1.172
[..]
irlwinning.com.      21578     IN   A    1.1.1.170
irlwinning.com.      21578     IN   A    1.1.1.171
irlwinning.com.      73   IN   SOA  ns1.irlwinning.com.
packets.irlwinning.com. 2013230901 900 900 900 900

;; ADDITIONAL SECTION:
ns1.irlwinning.com.  3647 IN   A    94.102.56.150
ns2.irlwinning.com.  3647 IN   A    94.102.56.150

;; Query time: 39 msec
;; SERVER: 199.187.216.12#53(199.187.216.12)
;; WHEN: Mon Oct  7 10:45:20 2013
;; MSG SIZE  rcvd: 4011
```

# 34.30.46.207.in-addr.arpa PTR

```
dig 34.30.46.207.in-addr.arpa PTR
;; Truncated, retrying in TCP mode.
[..]
;; ANSWER SECTION:
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.gr.
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.ie.
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.in.
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.com.es.
[..]
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.com.sg.
34.30.46.207.in-addr.arpa. 3600   IN   PTR windowsmobilelive.fr.

;; Query time: 14 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:42:31 2013
;; MSG SIZE  rcvd: 12453
```

# outmail.zyngamail.com A

```
dig outmail.zyngamail.com A
[..]
;; ANSWER SECTION:
outmail.zyngamail.com.    300  IN   A    74.114.9.183
outmail.zyngamail.com.    300  IN   A    74.114.9.184
outmail.zyngamail.com.    300  IN   A    74.114.9.185
outmail.zyngamail.com.    300  IN   A    74.114.9.186
outmail.zyngamail.com.    300  IN   A    74.114.9.187
[..]
outmail.zyngamail.com.    300  IN   A    74.114.9.178
outmail.zyngamail.com.    300  IN   A    74.114.9.179
outmail.zyngamail.com.    300  IN   A    74.114.9.180
outmail.zyngamail.com.    300  IN   A    74.114.9.182

;; Query time: 19 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:45:01 2013
;; MSG SIZE  rcvd: 1778
```

# netfirms.com

```
dig www.netfirms.com
[..]
;; ANSWER SECTION:
www.netfirms.com.3600 IN  A   65.254.227.16

;; Query time: 104 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:45:47 2013
;; MSG SIZE  rcvd: 61
```

# somethingstrange.netfirms.com

```
dig somethingstrange.netfirms.com
;; Truncated, retrying in TCP mode.
[..]
;; ANSWER SECTION:
somethingstrange.netfirms.com. 3600 IN A   67.23.129.35
somethingstrange.netfirms.com. 3600 IN A   67.23.129.33
somethingstrange.netfirms.com. 3600 IN A   67.23.129.32
somethingstrange.netfirms.com. 3600 IN A   67.23.129.31
somethingstrange.netfirms.com. 3600 IN A   67.23.129.30
somethingstrange.netfirms.com. 3600 IN A   67.23.129.29

;; Query time: 8 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Oct  3 12:50:25 2013
;; MSG SIZE  rcvd: 4026
```

# '.' the root

```
dig any .
[..]
;; ANSWER SECTION:
.            42321    IN   NSEC ac. NS SOA RRSIG NSEC DNSKEY
.            42321    IN   RRSIG    NSEC 8 0 86400 20131014000000
20131006230000 59085 . Ntf5bDYSPNFwQiD
+BWYxV2dfroUhPUs3tV4q20eaM5mbDfYEHuMlwr9u lNp8wV/
uaZyzmHrqZB2XL0nKjwD3AkY1W15y+ACxEghtQAaBhbX/1xM8 L6XYr/uyfhiY/
BCnIvwWlOUoK/7m/20LIuNyiaBlYISVcloYJwwxFtYT e8s=
[..]
.            86382    IN   SOA a.root-servers.net. nstld.verisign-grs.com.
2013100701 1800 900 604800 86400
.            86382    IN   RRSIG    SOA 8 0 86400 20131014000000
20131006230000 59085 . DoGy06dHpVdSKwx9nn82m7pSZCHOg5x1/
n36+4wvKaenFLX22TSlvWYL
b0pvKZVV8dXEI4z5jqtU9XWPXurVhDw29Q2FUmb7fS87T0Ve9R4lu87x
3t0pvqYB5+uqCdxVkhO1iIRROXhrMX2q253qtmfAVhtdfCeXAvoIZxBO yqk=

;; Query time: 38 msec
;; SERVER: 199.187.216.12#53(199.187.216.12)
;; WHEN: Mon Oct  7 10:50:40 2013
;; MSG SIZE  rcvd: 1649
```

# Roadmap: More Things To Do

- Rate limiting at ingress
  - Based on name
  - Based on name AND FQDN
  - Truncated Reponses for queries that fall outside rate limits
- Automation
  - Capture purpose built amplification domains on blocklists
  - Feeds for list/zone based filtering
- For  Further Study
  - Rate limiting based on answer sizes

# Thank You