Better than Best Practices for 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
- 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 isc.org"
Yields an impressively large answer (MSG SIZE rcvd: 3223):

QUESTION SECTION: ;isc.org. IN ANY ;; ANSWER SECTION: isc.org. 4084 IN **SOA** ns-int.isc.org. hostmaster.isc.org. 2012102700 7200 3600 24796800 3600 isc.org. 4084 IN **A** 149.20.64.42 isc.org. 4084 IN **MX** 10 mx.pao1.isc.org. isc.org. 4084 IN MX 10 mx.ams1.isc.org. isc.org. 4084 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. 4084 IN **TXT** "$Id: isc.org,v 1.1724 2012-10-23 00:36:09 bind Exp $" isc.org. 4084 IN **AAAA** 2001:4f8:0:2::d isc.org. 4084 IN **NAPTR** 20 0 "S" "SIP+D2U" "" _sip._udp.isc.org. isc.org. 484 IN **NSEC** _kerberos.isc.org. A NS SOA MX TXT AAAA NAPTR RRSIG NSEC DNSKEY SPF isc.org. 4084 IN **DNSKEY** 256 3 5 BQEAAAAB2F1 v2HWzCCE9v NsKfk0K8vd4EBwizNT9KO6WYXj0oxEL4eOJ aXbax/BzPFx+3qO8B8pu8E/JjkWH0oaYz4guUyTVmT5Eelg44Vb1kssy bq8W27oQ+9qNiP8Jv 6zdOj0uC B/N0fxfVL3371xbednFqoECfSFDZa6Hw jU1qzveSsW0= isc.org. 4084 IN **DNSKEY** 257 3 5 BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hWLDMv OMRXjGr hhCeFvAZih7yJHf8Z GfW6hd38hXG/xylYCO6Krpbdo jwx8YMXL A5/kA+ u50WIL8ZR1R6KTbsYVMf/Qx5RiNbPClw+vT+U8eXEJmO20jIS1ULgqy3 47cBB1zMnnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/zZrQz Bkj0BrN/9Bexjpiks3jRhZ atEsXn3dTy47 R09Uix5WcJt+xzqZ7+ysyL KOOedS39Z7SD msn2eA0FKtQpwA6LXeG2w+jxmw3oA8lVUgEf/rzeC/bB yBNsO70aEFTd isc.org. 4084 IN **SPF** "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. 484 IN **RRSIG** NS 5 2 7200 20121125230752 20121026230752 4442 isc.org. oFeNy69Pn+/JnnltGPUZQnYzo1YGgIM hS/SZKnlgy Mbz +tT2r/2v+X1j AkUl9GRW9JAZU+x0oEj5oNAkRiQqK+D6DC+PGdM2/JHa0X41LnMIE2NX UHDAKMmbqk529fUy3MvA/ZwR9FXurcfYQ5fnpEEaawNS0bKxomw48dcp Aco= isc.org. 484 IN **RRSIG** SOA 5 2 7200 20121125230752 20121026230752 4442 isc.org. S+DLHzE/8WQbnSl70geMYoKvGIIuKARVlxmssce+MX6DO/J1xdK9xGac XCuAhRpTMKElKq2dIhKp8v nS2e+JTZLrG l4q/ bnrrmhQ9eBS7IFmrQ6s 0cKEEyuijumOPlKCCN9QX7ds4siiTIrEOGhCaamEgRJqVxqCsg1dBUrR hKk= isc.org. 484 IN **RRSIG** MX 5 2 7200 20121125230752 20121026230752 4442 isc.org. VFqFWRPyuIlT8VsIdXKMpMRJTYpdggoGgOjKJzKJs/6ZrxmbJtmAxgEu /rkwD6Q9JwsUCepNC74EYxzXFvDaNnKp/Qdmt2139h/xoZsw0JVA4Z+b zNQ3kNiDjdV6zl6 ELtCVDqj3SiWDZ hYB/ CR9pNno1FAF2joIjYSwiwbS Lcw= isc.org. 484 IN **RRSIG** TXT 5 2 7200 20121125230752 20121026230752 4442 isc.org. Ojj8YCZf3jYL9eO 8w4Tl9HjWKP3CKXQRFed8s9xeh 5TR3KI3tQTKsSeI JRQaCXkADiRwHt0j7VaJ3xUHa5LCkzetcVgJNPmhovVa1w87Hz4DU6q9 k9bbshvbYtxOF8xny/FCiR5c6NVeLmvvu4xeOqSwlpoo2zvIEfFP9deR UhA= isc.org. 484 IN **RRSIG** AAAA 5 2 7200 20121125230752 20121026230752 4442 isc.org. hutAcro0NBMvKU/m+2lF8sgIYyIVWORTp/utIn8KsF1WOwwM2QMGa5C9 /rH/ZQBQgN46ZMmiEm4LxH6mtaKxMsBGZwgzUE dfsvVtr +fS5NUoA1rF wg92eBbInNdCvT0if8m1Sldx5/hSqKn8EAscKfg5BMQp5YDFsllsTauA 8Y4= isc.org. 484 IN **RRSIG** NAPTR 5 2 7200 20121125230752 20121026230752 4442 isc.org. ZD14qEHR7jVXn5uJUn6XR9Lvt5Pa7YTEW94hNAn9Lm3Tlnkg11AeZiOU 3woQ1pg+esCQepKCiBlplPLcag3LHlQ19OdACrHGUzzM+rnHY50Rn/H4 XQTqUWHBF2Cs0CvfqRxLv Al5AY6P2bb/ iUQ6hV8Go0OFvmMEkJOnxPPw 5i4= isc.org. 484 IN **RRSIG** NSEC 5 2 3600 20121125230752 20121026230752 4442 isc.org. rY1hqZAryM045vv3bMY0wgJ hxHJQofkXLe RLk20LaU1mVTyu7uair7jb MwDVCVhxF7gfRdgu8x7LPSvJKUl6sn731Y80CnGwszXBp6tVpgw6oOcr Pi0rsnzC6IlarXLwNBFmLZg2Aza6SSirzOPObnmK6PLQCdmaVAPrVJQs FHY= isc.org. 484 IN **RRSIG** DNSKEY 5 2 7200 20121125230126 20121026230126 4442 isc.org. i0S2MFqvHB3wOhv2IPozE/IQABM/eDDCV2D7dJ3AuOwi1A3sbYQ29XUd BK82+mxxsET2U6hv64crpbGTNJP3 OsMxNOAFA0QYphoMnt0jg3OYg+AC L2j92kx8ZdEhxKiE6pm+cFVBHLLLmXGKLDaVnffLv1GQIl5YrIyy4jiw h0A= isc.org. 484 IN **RRSIG** DNSKEY 5 2 7200 20121125230126 20121026230126 12892 isc.org. j1kgWw+wFFw01E2z2kXq+biTG1rrnG1XoP17pIOToZHElgpy7F6kEgyj fN6e2C+gvXxOAABQ+qr76o+P+ZUHrLUEI0ewtC3v4HziMEl0Z2/NE0MH qAEdmEemezKn9O1EAOC7gZ4 nU5psmuYlqxcCkUDbW0qhLd+u/8+d6L1S nlrD/vEi4R1SLI2bD5VBtaxczOz+2BEQLveUt/UusS1qhYcFjdCYbHqF JGQziTJv9ssbEDHT7COc05gG+A1Av5tNN5ag7QHWa0VE+Ux0nH7JUy0N ch1kVecPbXJVHRF97CEH5wCDEgcFKAyyhaXXh02fqBGfON8R5mIcgO/F DRdXjA== isc.org. 484 IN **RRSIG** SPF 5 2 7200 20121125230752 20121026230752 4442 isc.org. IB/bo9HPjr6aZq PRkzf9bXyK8TpBFj3HNQloqhrguMSBfcMfmJqHxKyD ZoLKZkQk9kPeztau6hj2YnyBoTd0zIVJ54442 isc.org. ViS+qg95DibkkZ5kbL8vCBpRUqI2/M9UwthPVCXl8ciglLftiMC9WUzq Ul3FBbri5CK D/ YNXqyvjxyvmZfkQLDUmffjDB+ZGqBxSpG8j1fDwK6n1 hWbKf7QSe4LuJZyEgXFEkP16CmVyZCTITUh2TNDmRgsoxrvrOqOePWhp fVSqJPuNqxwm2h9HMs140r3 9HmbnkO7Fe+L u5AD0 s6+E9qayi3wOOwunBgUkkFsC8BjiiGrRKcY8GhC kak= isc.org. 484 IN **RRSIG** A 5 2 7200 20121125230752 20121026230752 8+E= isc.org. 4084 IN **NS** ns.isc.afilias-nst.info. isc.org. 4084 IN **NS** ams.sns-pb.isc.org. isc.org. 4084 IN **NS** ord.sns-pb.isc.org. isc.org. 4084 IN NS sfba.sns-pb.isc.org. ;; AUTHORITY SECTION: isc.org. 4084 IN **NS** ns.isc.afilias-nst.info. isc.org. 4084 IN **NS** ams.sns-pb.isc.org. isc.org. 4084 IN **NS** ord.sns-pb.isc.org. isc.org. 4084 IN **NS** sfba.sns-pb.isc.org. ;; ADDITIONAL SECTION: mx.ams1.isc.org. 484 IN **A** 199.6.1.65 mx.ams1.isc.org. 484 IN **AAAA** 2001:500:60::65 mx.pao1.isc.org. 484 IN **A** 149.20.64.53 mx.pao1.isc.org. 484 IN **AAAA** 2001:4f8:0:2::2b _sip._udp.isc.org. 4084 IN **SRV** 0 1 5060 asterisk.isc.org. ;; Query time: 176 msec ;; SERVER: x.x.x.x#53(x.x.x.x) ;; WHEN: Tue Oct 30 01:14:32 2012 ;; MSG SIZE rcvd: 3223

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

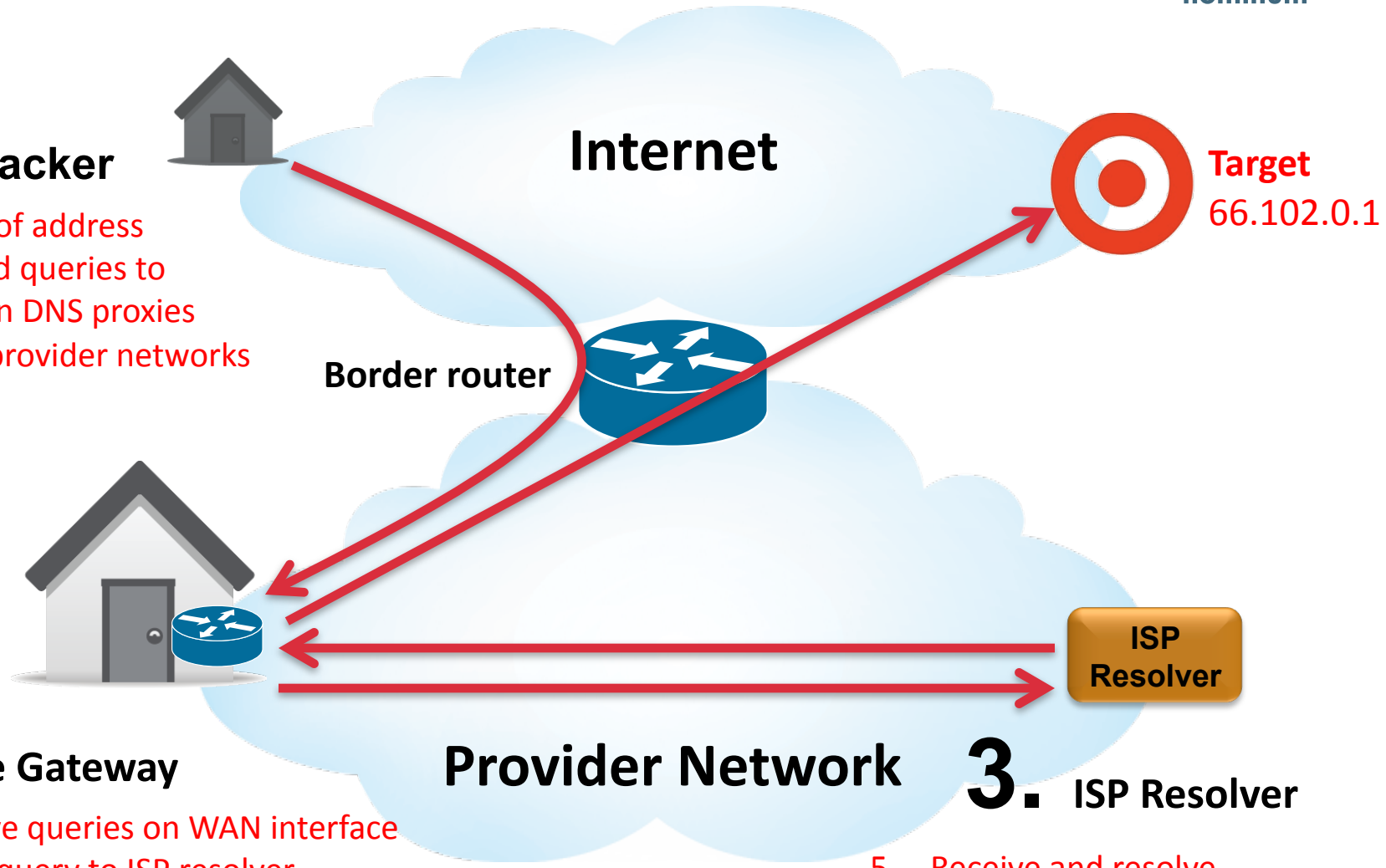
A few thousand connections = 100s of Gbps as was seen with attack on spamhaus

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
9. 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
- 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
  - Someone is stealing our SW! (and they're not even using it right!)
- 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?????

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
- irlwinning.com
- 34.30.46.207.in-addr.arpa
- www.djcgrafix.netfirms.com

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