



DNS Amplification and DNS Hijack Risk Mitigation

NANOG On The Road
Portland, OR - September 10, 2013

Merike Kaeo

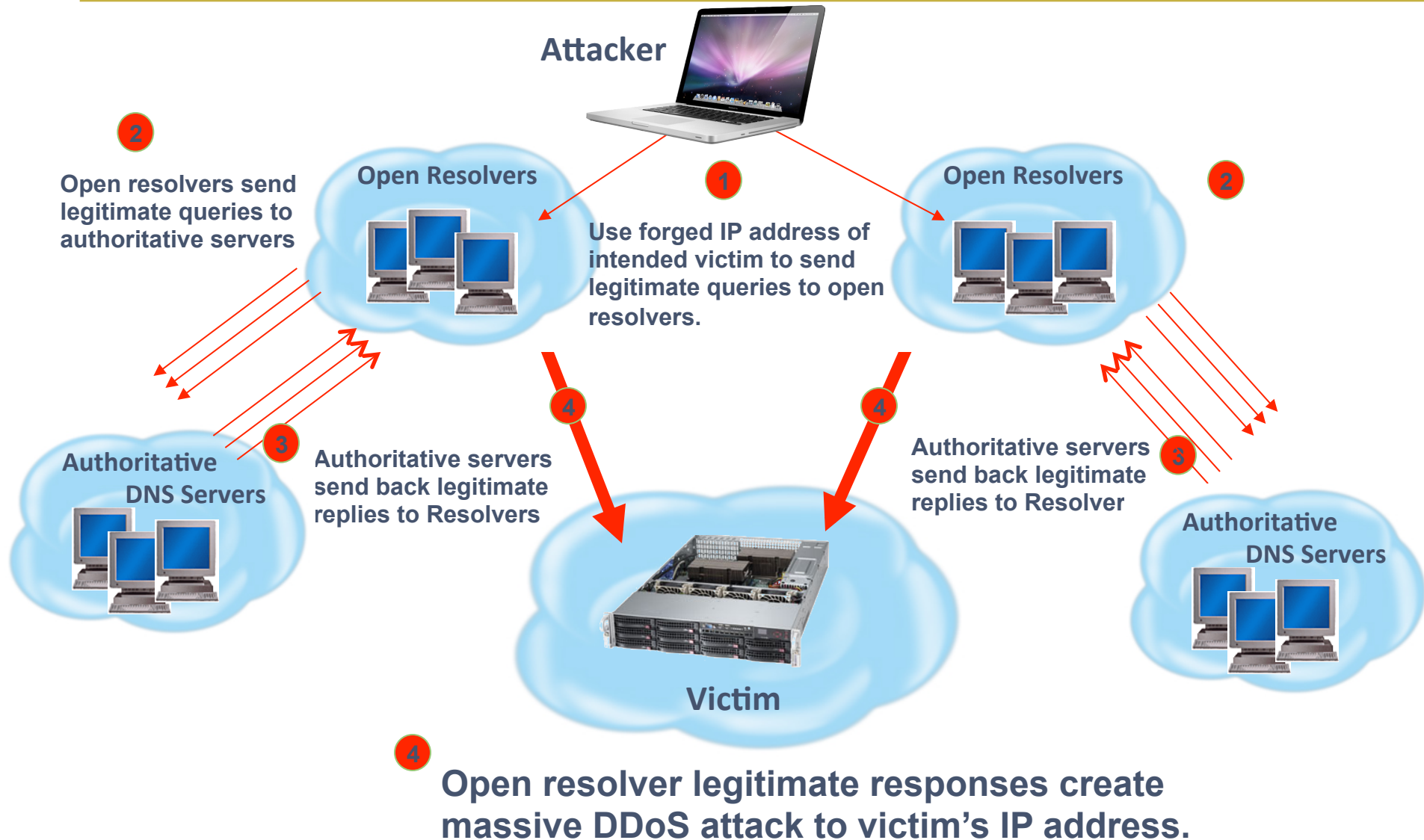
Security Evangelist, IID

merike@internetidentity.com

INTRO

- Statistics on DNS Amplification Attacks in 2012/2013
- Measurements on Open Recursive Resolvers
- How To Close Unmanaged Open Recursive Resolvers
- What Other Basic Network Hygiene Can Help?
- What About DNS Hijacks?

OPEN RESOLVER AMPLIFICATION ATTACK



GROWING TRENDS

- Reflective DDoS attacks use IP addresses of legitimate users
- Combining spoofed addresses with legitimate protocol use makes mitigation extremely difficult – what do you block and where?
- Recent trends have been utilizing DNS as attack vector since it is a fundamentally used Internet technology
 - Exploit *unmanaged* open recursive resolvers
 - Exploit large response profile to some standard queries (e.g. DNSSEC)
- Utilize resources of large hosting providers for added attack bandwidth
- Many other Internet protocols also susceptible [SNMP, Chargen, etc]

HOW BAD IS THE PROBLEM?

Largest in 2012

Event Time Start: Aug 1, 2012 00:33:00 UTC

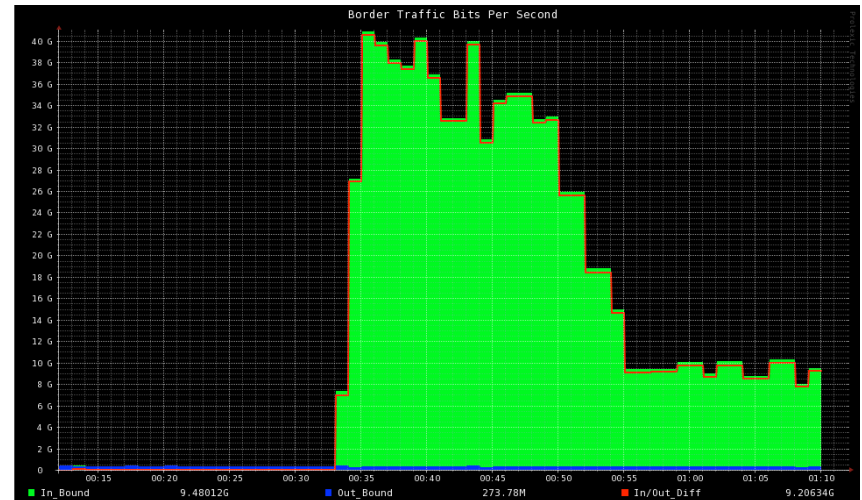
Attack Types: DNS Flood, GET Flood, UDP
Fragment Flood, ICMP Flood

Destination Ports: 80,443,53

Industry Vertical: Financial

Peak Bandwidth: **42.2 Gbps**

Peak pps: **2.1 Mpps**



Source: Prolexic

“Trending data points to an increase of DNS attacks that can be observed in the comparison of Q1 2012 (2.50 percent), Q4 2012 (4.67 percent), and Q1 2013 (6.97 percent). This represents **an increase of over 200 percent** in the last year.”

Source: Prolexic Quarterly Global DDoS Attack Report Q1 2013



WHY DOES THE DNS AMPLIFICATION WORK SO WELL?

- Victims cannot see actual originator of attack
 - Lots of DNS packets from a wide variety of 'real' DNS servers
 - Victims cannot block the BotNet making the spoofed queries
- DNS servers are answering seemingly normal requests
- Originating ISPs aren't impacted
- Originating ISPs only see small amounts of traffic
- Filtering attack traffic is difficult in practice
 - The open resolvers are themselves not infected not malicious
 - Depending on architecture, may block legitimate traffic

WHY WOULD PEOPLE RUN OPEN RESOLVERS?

- Deliberate Services
 - Google, OpenDNS, DynDNS, Amazon Route53
 - Ensure reliability and stability
- Many are not deliberate – why do they exist?
 - Evil DNS servers run by criminals on bulletproof hosts
 - Everyone else
 - Hosting companies
 - Small/medium ISPs
 - Enterprises, SMBs
 - Default device configuration

WHAT NEEDS TO BE DONE

- Ensure no *unmanaged* open recursive resolvers exist
 - Equipment vendors need ship default as CLOSED
 - BCPs should **not** show recursive resolver configurations as open
- Get everyone to participate in stopping ability to spoof IP addresses
 - ISPs need to do *ingress* filtering (BCP38/BCP84)
 - Enterprises/SMBs need to implement *egress* filters
 - Equipment vendors need to have better defaults for helping alleviate spoofing
- Sponsoring research/studies to get definitive data on where IP address spoofing is possible may help
 - MIT Spoofer Project (<http://spoofer.csail.mit.edu>)

PROJECTS THAT HELP DETERMINE OPEN RESOLVERS

- Measurement Factory
 - <http://dns.measurement-factory.com/surveys/openresolvers.html>
 - has been running tests for open recursive resolvers since 2006
 - have daily reports of open resolvers per AS number
 - send DNS query to a target IP address for a name in test.openresolver.org domain (target IP addresses tested no more than once every three days)
- The Open Resolver project
 - <http://openresolverproject.org>
 - started in March 2013
 - active scans run on a weekly basis that get some added information

THE MEASUREMENT FACTORY



DNS SURVEY: OPEN RESOLVERS

ABOUT

We have an ongoing survey that looks for open DNS resolvers. A DNS resolver is *open* if it provides recursive name resolution for clients outside of its administrative domain. Open DNS resolvers are a bad idea for a few reasons:

- They allow outsiders to consume resources that do not belong to them.
- Attackers may be able to [poison the cache](#) of an open resolver.
- Open resolvers are being used in widespread DDoS attacks with spoofed source addresses and large DNS reply messages.

As with open SMTP relays, open DNS resolvers are now being abused by miscreants to further pollute the Internet.

[On main page go to 'Results' then 'DNS survey results' and finally 'Open Resolvers']



OPEN RESOLVER PROJECT

Open DNS Resolver Project

Open Recursive Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from [Smurf attacks](#) commonly seen in the late 1990s.

We have collected a list of 27,200,613 resolvers that respond to queries in some fashion. 25.2 million of these pose a significant threat (as of 07-APR-2013). [Detailed History and Breakdown](#)

Check my IP space

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /24 will be rejected):

[hilbert curve heatmap of 20130414 data heatmap archive](#)

What can I do?

If you operate a DNS server, please check the settings.

Recursive servers should be restricted to your enterprise or customer IP ranges to prevent abuse. Directions on securing BIND and Microsoft nameservers can be found on the [Team CYMRU Website](#)

Authoritative servers should not offer recursion, but can still be used in an attack. Configure your Authoritative DNS servers to use [DNS RRL](#) [\[Response Rate Limiting\]](#) Knot DNS and NLNetLabs NSD include this as a standard option now. BIND requires a patch.

Prevent spoofing on your network!

Configure BCP-38 on all CPE and Datacenter equipment edges that have fixed IP ranges. This could be as simple as setting ip verify unicast source reachable-via rx on a router interface. Any statically routed customer should receive this setting by default.

If you are in the security community:

Please contact dns-scan /at/ puck.nether.net or if you know the host owner, engage him for access to raw data.

Additional Information

[Informações em Português](#)

We can provide you a List of Open Resolvers by ASN if you e-mail dns-scan /at/ puck.nether.net

[Test your IP Now!](#)

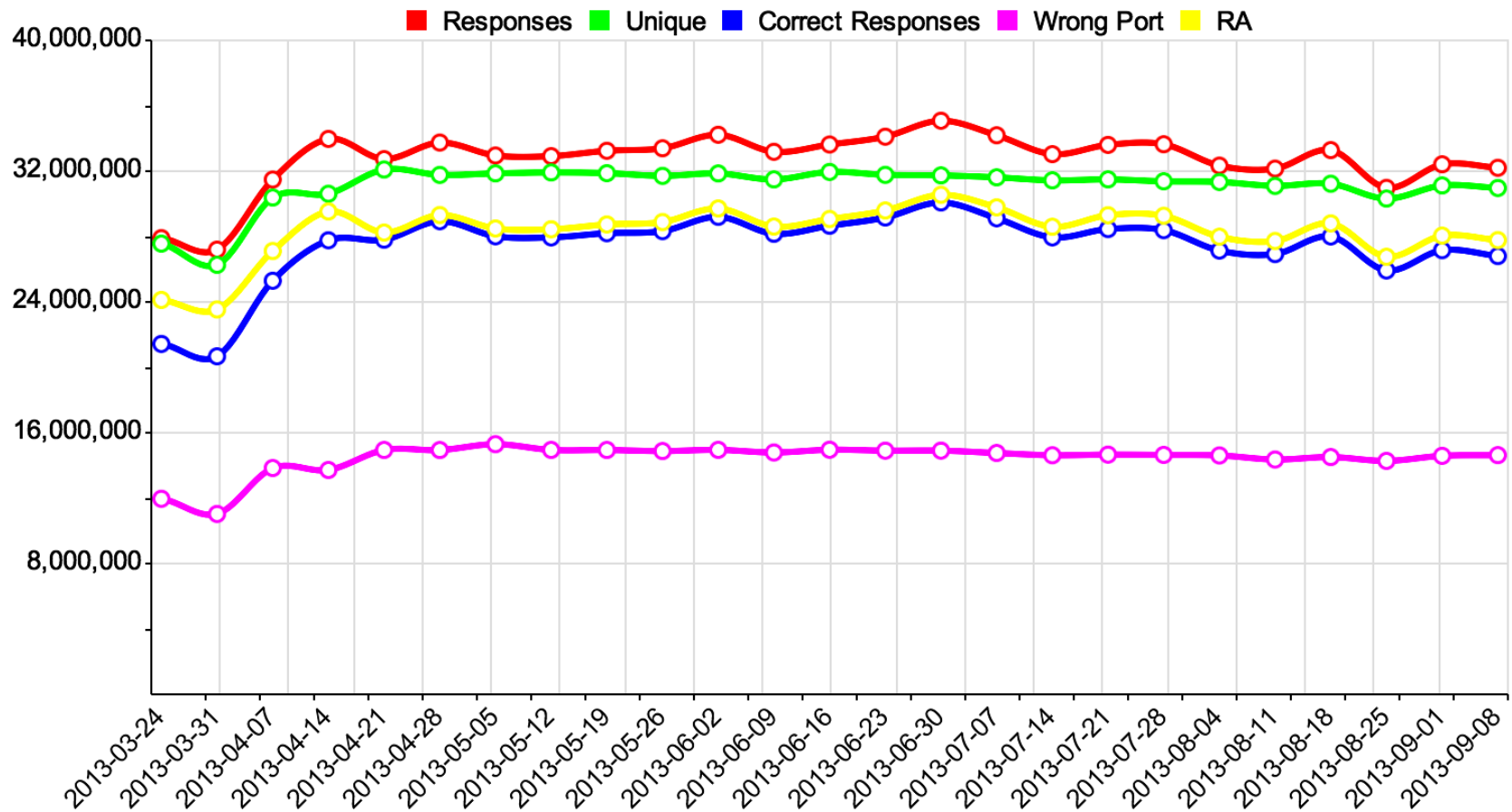
DNS DDoS and Security in the News

- 04-APR-2013 [Spamhaus DDoS was just a warning shot](#)
- 30-MAR-2013 [How the Cyberattack on Spamhaus Unfolded](#)
- 28-MAR-2013 [Is Your DNS Server part of a criminal conspiracy?](#)
- 20-MAR-2013 [75Gb/s DDoS against Cloudflare](#)

We hope to present the data at a future conference, and share it with the broader security community.

OPEN RECURSIVE RESOLVER PROJECT STATS

OpenResolverProject trends



CLOSING RECURSIVE RESOLVERS

- RFC 5358 (BCP 140): Preventing Use of Recursive Nameservers in Reflector Attacks
 - <http://www.ietf.org/rfc/rfc5358.txt>
- BIND
 - <http://www.zytrax.com/books/dns/ch9/close.html>
- Team CYMRU
 - Pointers to BIND implementations and Microsoft
 - <http://www.team-cymru.org/Services/Resolvers/instructions.html>

DNS RESPONSE RATE LIMITING (DBS RRL)



Red Barn

Blogs

Navigation

- Recent posts

User login

Username: *

Password: *

Log in

- Request new password

Home

Response Rate Limiting in the Domain Name System (DNS RRL)

This page describes DNS Response Rate Limiting (DNS RRL) which is an experimental feature for domain name servers including CZ-NIC Knot DNS, NLNetLabs NSD, and ISC BIND9.

These patches and instructions pertain to authority name servers or authoritative views. Use of this kind of rate limiting for recursive or hybrid servers or views is currently unspecified.

Note Well: This is DNS RRL, meant to be implemented in many different name servers, it is not a BIND specific feature even though BIND was the first name server for which DNS RRL was implemented. DNS RRL will eventually be submitted to the IETF for standardization work. The need for DNS RRL is immediate and pressing, and the IETF processing of this work was therefore planned to come last rather than first.

References:

- Red Hat Enterprise Linux update for RRL in BIND
- Release notes for CZ-NIC Knot DNS, available as a standard Knot feature as of Version 1.2-RC3, released 2013-03-01

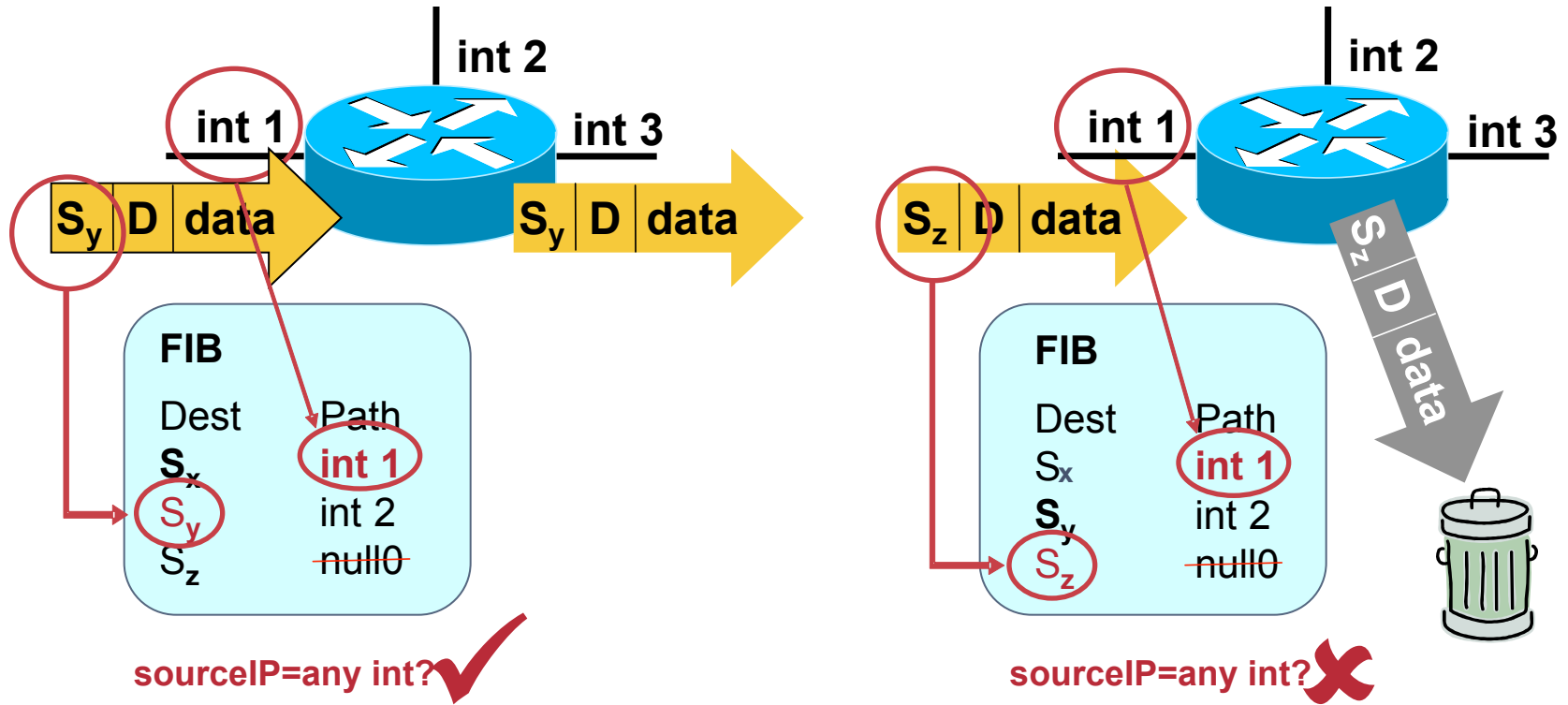
<http://www.redbarn.org/dns/ratelimits>

WHAT OTHER BASIC NETWORK HYGIENE HELPS?

- Ingress Filtering (BCP38/BCP84)
 - Using simple filters
 - Using uRPF
 - http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_unicast_rpf.html
 - http://www.juniper.net/techpubs/en_US/junos9.4/topics/concept/unicast-rpf-ex-series.html
 - <https://tools.ietf.org/html/draft-savola-bcp84-urpf-experiences-03>
- Transit Route Filters
- Peering Route Filters
- IX Specific
 - Set next-hop self on border routers
 - Do not redistribute connected routes into IGP/BGP

URFP (UNICAST REVERSE PATH FORWARDING)

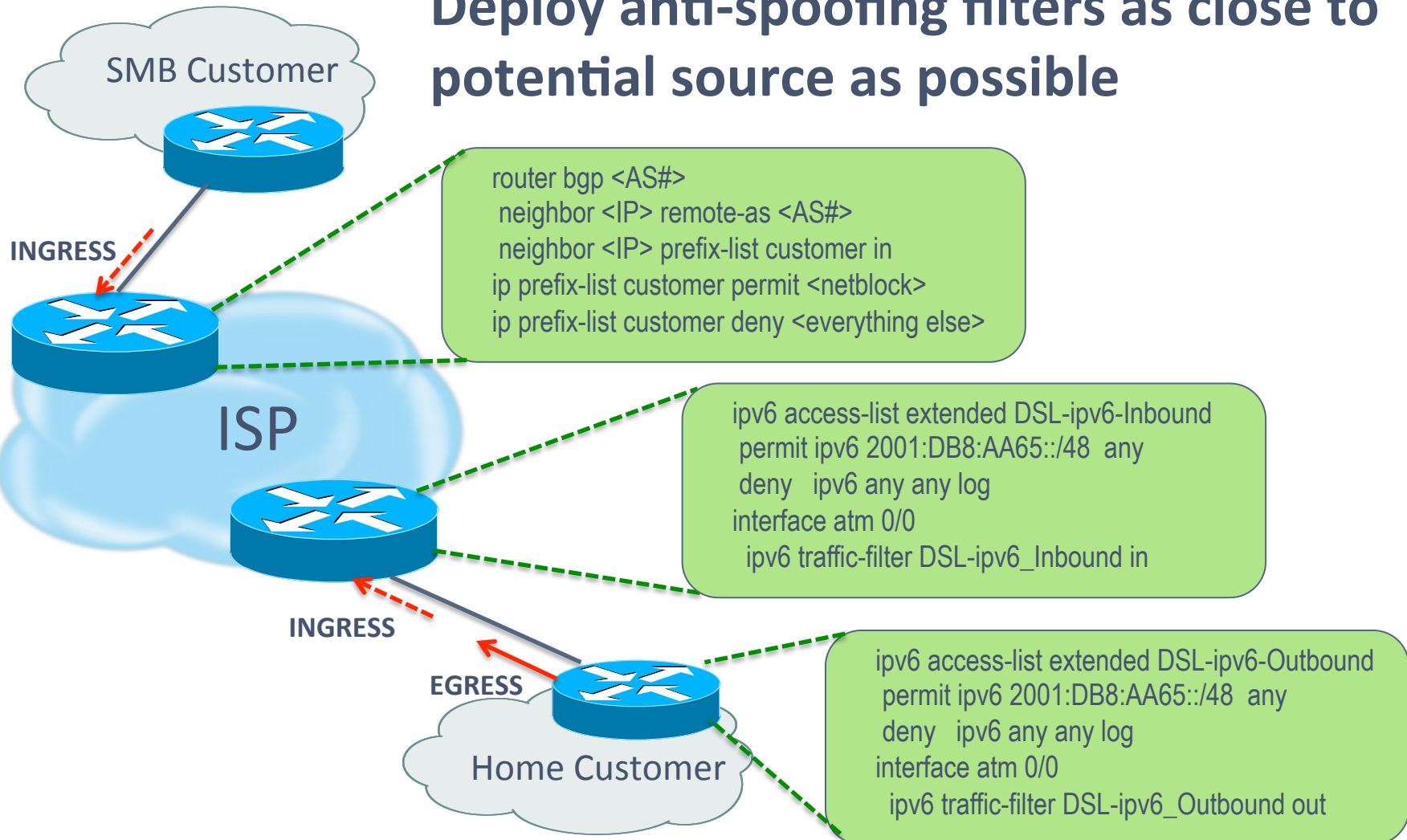
Loose Mode: Source IP has to match any interface entry in the FIB



IP verify unicast source reachable – via any

INGRESS/EGRESS FILTERS

Deploy anti-spoofing filters as close to potential source as possible



WHAT ABOUT DNS HIJACKS?




The Register

Data Center Cloud Software Networks Security Policy


The Washington Post PostTV Politics Opinions Local Sports National World Business




The Switch

Where technology and policy connect



Get 25,000 Membership Rewards® after you spend \$5,000 in the three months of Card membership

Authors Archives Follow:   

 Email  Print  Reprints

The New York Times Web site was taken down by DNS hijacking. Here's what that means.

By Timothy B. Lee, Published: August 27 at 8:34 pm [E-mail the writer](#)

Just weeks after The Washington Post had our own run-in with the Syrian Electronic Army (SEA), the New York Times is down, and the SEA is claiming responsibility. Other sites, including Twitter, have also been attacked.



SECURITY

LinkedIn DNS hijacked, site offline

Be patient ... we've dealt with hacks before says business hub

By Richard Chirgwin, 20th June 2013



1,877 followers

WHAT IS A REGISTRY LOCK?

- It is intended to mitigate against the potential for unintended changes, deletions or transfers.
- Helps protect against registry portal compromises
- Stops any of a registrar's automated systems from being able to make changes to the domain name record.
- Changes can only be made by manual intervention by staff at a registrar, and by staff at the registry.
- Additional manual security processes are usually implemented as part of this process - including needing more than one party at the holder of the domain name to authorize a change.

HOW TO BETTER PROTECT YOUR DOMAIN

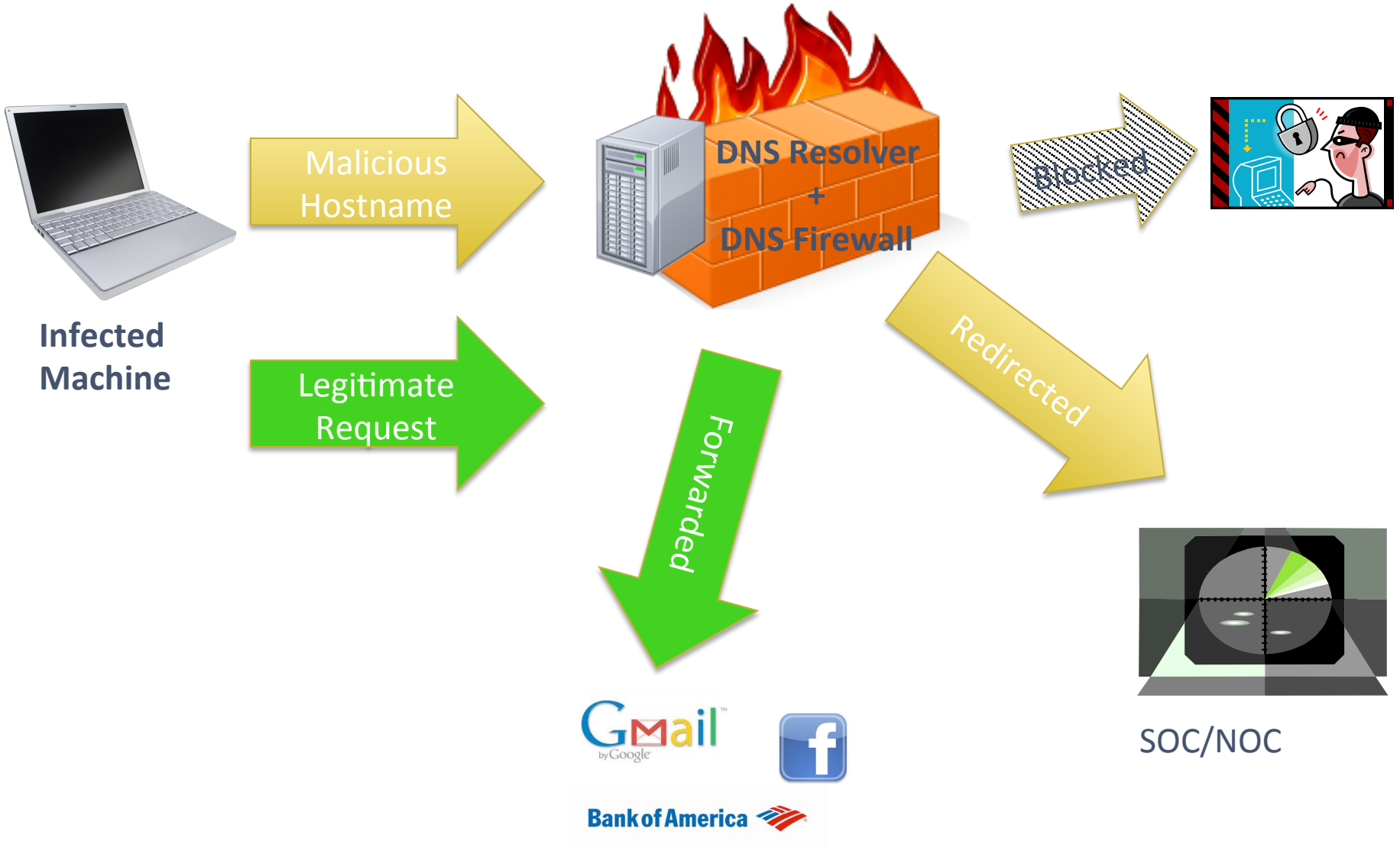
- Know the security practices of your registrar
 - How rigorous are they with access control to their internal servers?
 - Do they utilize two-factor authentication?
 - What is their process for updating / modifying any of your domain name information?
 - How are user credentials protected?
 - Do they support feature called 'registry lock'?
- Monitor your DNS records for changes

Why are you paying only \$10/month for a domain that is critical to your business????

SOMETHING TO CONSIDER - DNS FIREWALL

- How do you currently stop DNS requests to known malicious sites from going out of your network?
- Block DNS requests from your network to malicious hosts
- AKA: a secure DNS resolver or DNS filtering
- Not a new idea – just an under utilized/appreciated approach
- Key needs:
 - Infrastructure
 - Malicious host listings
 - Policies for blocking/redirection

THE DNS RESOLVER AS PRIMARY DEFENSE



DNS FIREWALL INFRASTRUCTURE

- Using current in-house DNS resolvers
 - Implement RPZ (<ftp://ftp.isc.org/isc/dnsrcpz/isc-tn-2010-1.txt>)
 - Resolvers ‘cache’ protection data and never go to Internet to resolve bad hostnames
- Using cloud-based DNS resolver servers
 - Minor change for many – already use ISP resolvers
 - Can update internal infrastructure to forward requests to “cloud” – relatively painless update
- Fairly easy to implement with no new hardware requirements and no network downtime.

PARTING THOUGHTS

- Test to determine whether you have unmanaged open resolvers in your environment
 - <http://www.thinkbroadband.com/tools/dnscheck.html>
 - <http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl>
- Ensure that you are helping stop spoofed traffic as close to the source as possible
 - You don't need to use uRPF – simple filters work
- Who you pick as Registrar and what their security practices are is important TO YOU!
- Think about usefulness of DNS Firewall in your environment



Questions ?



Eric Zeigast

OCTOBER SECURITY UPDATE

- DDoS is not just DNS anymore
- Seeking help *before* you need it
- NANOG Tutorial Resources
- Plugging in to reporting services

DNS WAS JUST THE BEGINNING

- Latest attacks utilize open DNS or NTP servers
- Future attacks will utilize other protocols
 - Search for: NDSS 2014 amplification hell
 - Mix of protocols
- Scanning
 - Good guys *and* bad guys know what's available
- Not just servers
 - printers
 - home gateway routers
 - smart CPE / modems / wifi

InformationWeek InformationWeek CONFERENCE [REGISTER NOW!](#)

[Home](#) [News & Commentary](#) [Authors](#) [Slideshows](#) [Video](#) [Reports](#) [White Papers](#) [Events](#) [Interop](#)

[STRATEGIC CIO](#) [SOFTWARE](#) [SECURITY](#) [CLOUD](#) [MOBILE](#) [BIG DATA](#) [INFRASTRUCTURE](#)

SECURITY // [ATTACKS & BREACHES](#)

NEWS
2/11/2014
12:51 PM

DDoS Attack Hits 400 Gbit/s, Breaks Record



A distributed denial-of-service NTP reflection attack was reportedly 33% bigger than last year's attack against Spamhaus.



OPEN NTP SERVER PROJECT

OpenNTPProject.org - NTP Scanning Project

Search my IP space (eg: 192.0.2.0/24 - searches "larger" than /22 will be rejected):

If you are a member of the general public:

How can I check my server? - run the command `ntpd -n -c monlist 192.0.2.1` Or `ntpq -c rv 192.0.2.1` - If you see a response, your server may be used in attacks.

How can I fix my server, router or other device? You should upgrade to NTP-4.2.7p26 or later. You can add `disable monitor` to your `ntp.conf` and restart your NTP process if on an earlier version. Also check out the [Team Cymru Secure NTP Template](#) - Also see [NTP Bug #1532](#)

The server should also not respond to `loopinfo` Or `iostats` requests as well

We are sending one packet to every IP to test if it generates a NTP MONLIST MODE 7 response

Recent News:

2014-01-13 - [100Gb/s attacks using NTP](#)

2013-12-26 - [Christmas 2013 NTP Attacks](#)

If you are a member of the security community:

You can contact the `ntp-scan /at/ puck.nether.net` to obtain the raw data. It is available for re-use in your reporting.

About US:

OpenNTPProject.org is operated in conjunction with [Network Time Foundation](#). If this service is valuable, please consider joining or donating to NTF.

GETTING HELP BEFORE YOU NEED IT

- Know your network and services
 - Network flow analysis and graphs
 - IDS solutions (snort, suricata, commercial)
- Can your upstream ISPs help?
 - What filters or “scrubbing” can they place for you?
 - Who are their network security contacts?
- What can you deploy before the attack?
 - Anycast or agile DNS services?
 - Have you provisioned and tested a DDoS mitigation service?

NANOG TUTORIAL RESOURCES

- Check out NANOG tutorials (<http://nanog.org/resources/tutorials>):
 - The Service Provider Tool Kit (Barry Greene)
 - An Introduction to DNSSEC (Matt Larson)
 - NSP-SEC Top Ten Security Techniques (Barry Greene)
 - NetFlow to guard the Infrastructure

PLUGGING IN TO REPORTING SERVICES

- Several types of abuse are remotely detected and reported by the security community
- Automated reports about bot activity or sinkhole hits are usually given to ShadowServer and TeamCymru.



- Sign up:
 - ShadowServer: Look for “Get Reports On Your Network” on www.shadowserver.org and then email <request_report@shadowserver.org>
 - Team Cymru: www.tcconsole.com or email <outreach@cymru.com>