Secure the Internet: stopping DNS reflection attacks

Kams Yeung
Akamai Technologies

ISOC NetOps Workshop, APRICOT 2014

26th Feb, 2014

Agenda

Akamai Introduction

- Akamai Intelligent Platform

Secure the Internet – stopping the DNS reflection attacks

- Open resolvers and reflection attacks

Mitigate the attacks

- Network and Servers
- Sample configuration: BIND and Windows

Akamai Introduction

The Akamai Intelligent Platform

The world's largest on-demand, distributed computing platform delivers all forms of web content and applications

The Akamai Intelligent Platform:

137,000+ Servers	2,000+ Locations	1,150+ Networks	700+ Cities	87 Countries

Typical daily traffic:

- More than **2 trillion** requests served
- Delivering over **10 Terabits/second**
- **15-30%** of all daily web traffic

Akamai
FASTER FORWARD

Secure the Internet

Open resolvers and DNS reflection attack

Open Resolvers

Why resolver exists?

- Exist to aggregate and cache queries
  - Not every computer run its own recursive resolver.
- ISPs, Large Enterprises run these
- Query through the root servers and DNS tree to resolve domains
- Cache results, and deliver cached results to clients.

Open resolvers

- Recursive lookup
- Answer recursive queries from any client

Some Public Services:

- Google DNS, OpenDNS, Level 3, etc.
- These are “special” set-ups and secured.

www.cloudflare.com

Reflection Attack

- **What is a Reflection Attack?**
  In a reflection attack, an attacker makes a request to the open resolver using a UDP packet whose source IP is the IP address of the target. The request is usually one that will result in a large response, such as a DNS ANY request or a DNSSec request, which allows the attacker to multiply up to 100x the amount of bandwidth sent to the target web server. The "multiplication" factor is what makes this particular attack dangerous, as traffic can reach up to 200- 300Gbps. The Spamhaus attack is one example of a recent reflection attack.

www.cloudflare.com

Reflection Attack

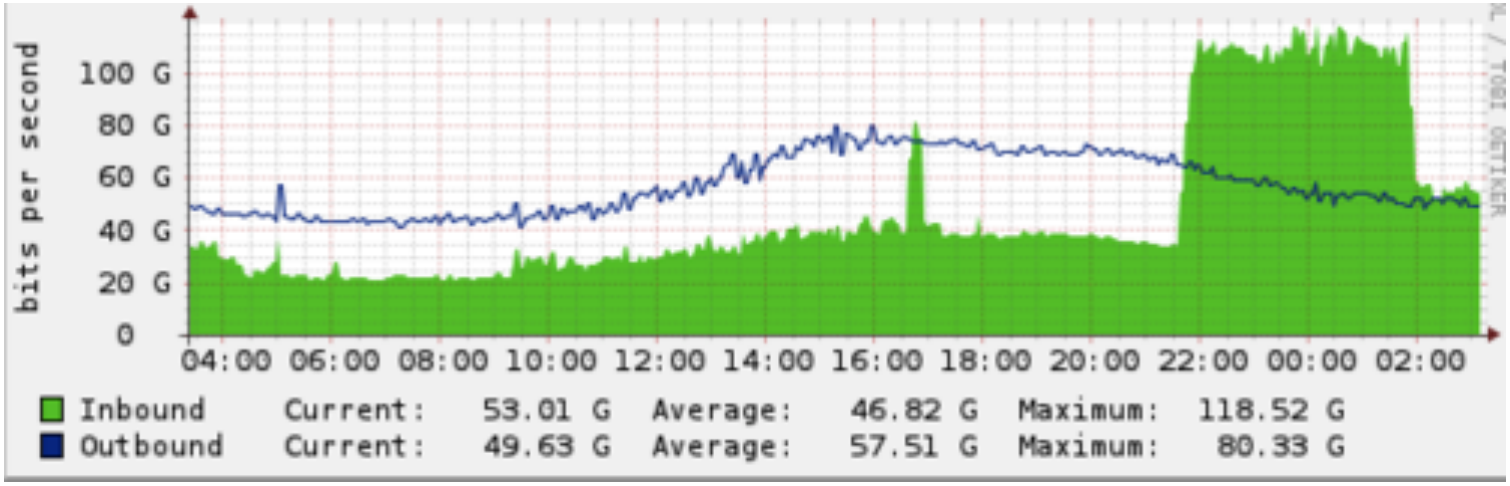
- UDP Query
- Spoofed source
  - Using the address of the person you want to attack
  - DNS Server used to attack the victim (sourced address)

- Amplification used
  - Querying domains like ripe.net or isc.org
  - ~64 byte query (from attacker)
  - ~3233 byte reply (from unsecured DNS Server)
  - 50x amplification!

- Running an unsecured DNS server helps attackers!

www.cloudflare.com

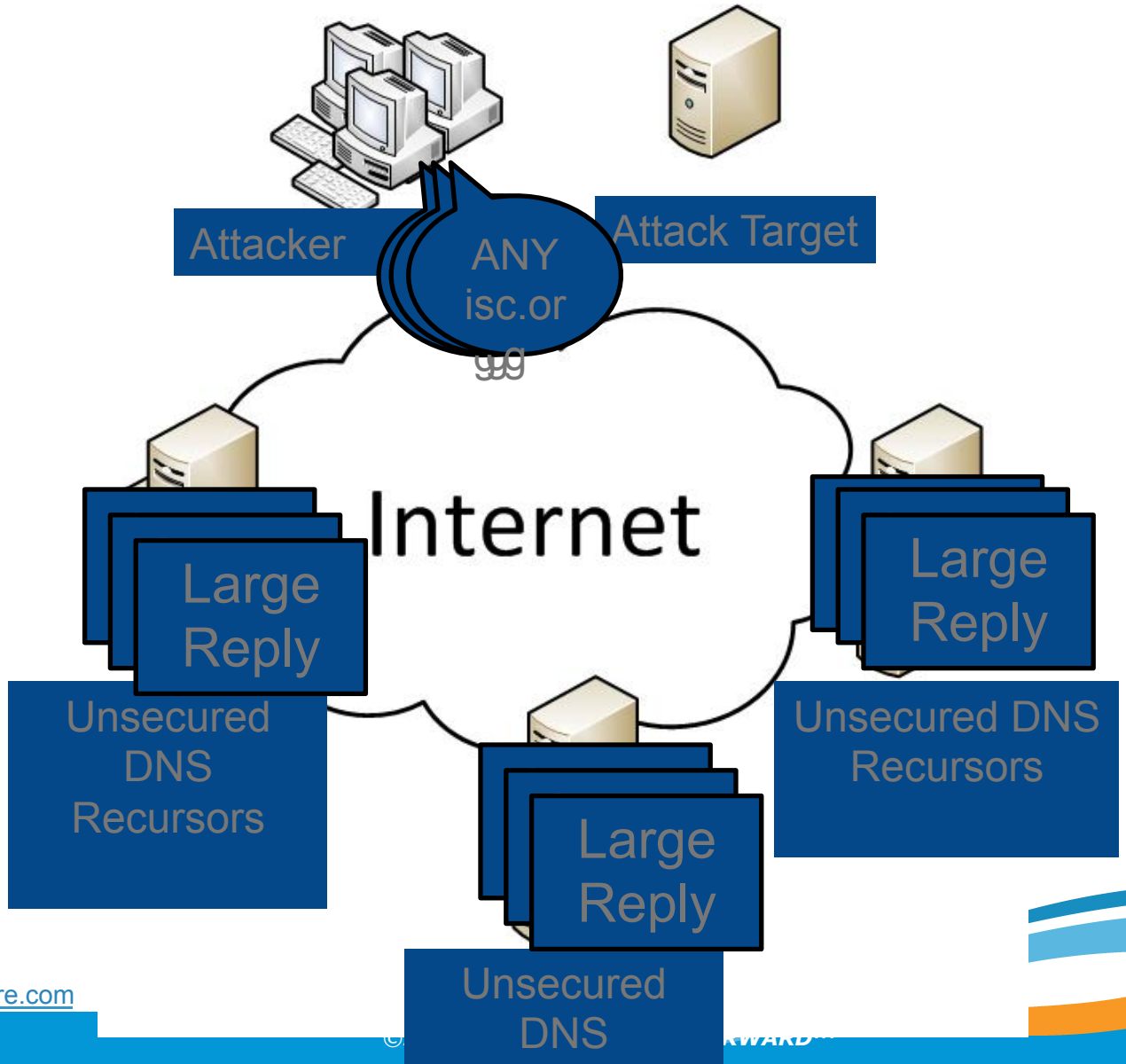
Open Resolvers – The Problem!



Example of DNS-based reflection attack exceeding 70Gbit.

- There are millions of DNS resolvers.
- Many of these are not secured.
- Non secured DNS resolvers can and will be abused
- CloudFlare has seen DNS reflection attacks hit 300Gbit/s traffic globally.

Reflection Attack



Reflection Attack

- With 50x amplification:
  - 1Gbit uplink from attacker (eg: Dedicated Servers)
  - 50Gbit attack
  - Enough to bring most services offline!

- Prevention is the best remedy.

- In past attacks, CloudFlare seen around 80,000 open/ unsecured DNS Resolvers being used.
- At just 1Mbit each, that's 80Gbit!
  - 1Mbit of traffic may not be noticed by most operators.
  - 80Gbit at target is easily noticed!

www.cloudflare.com

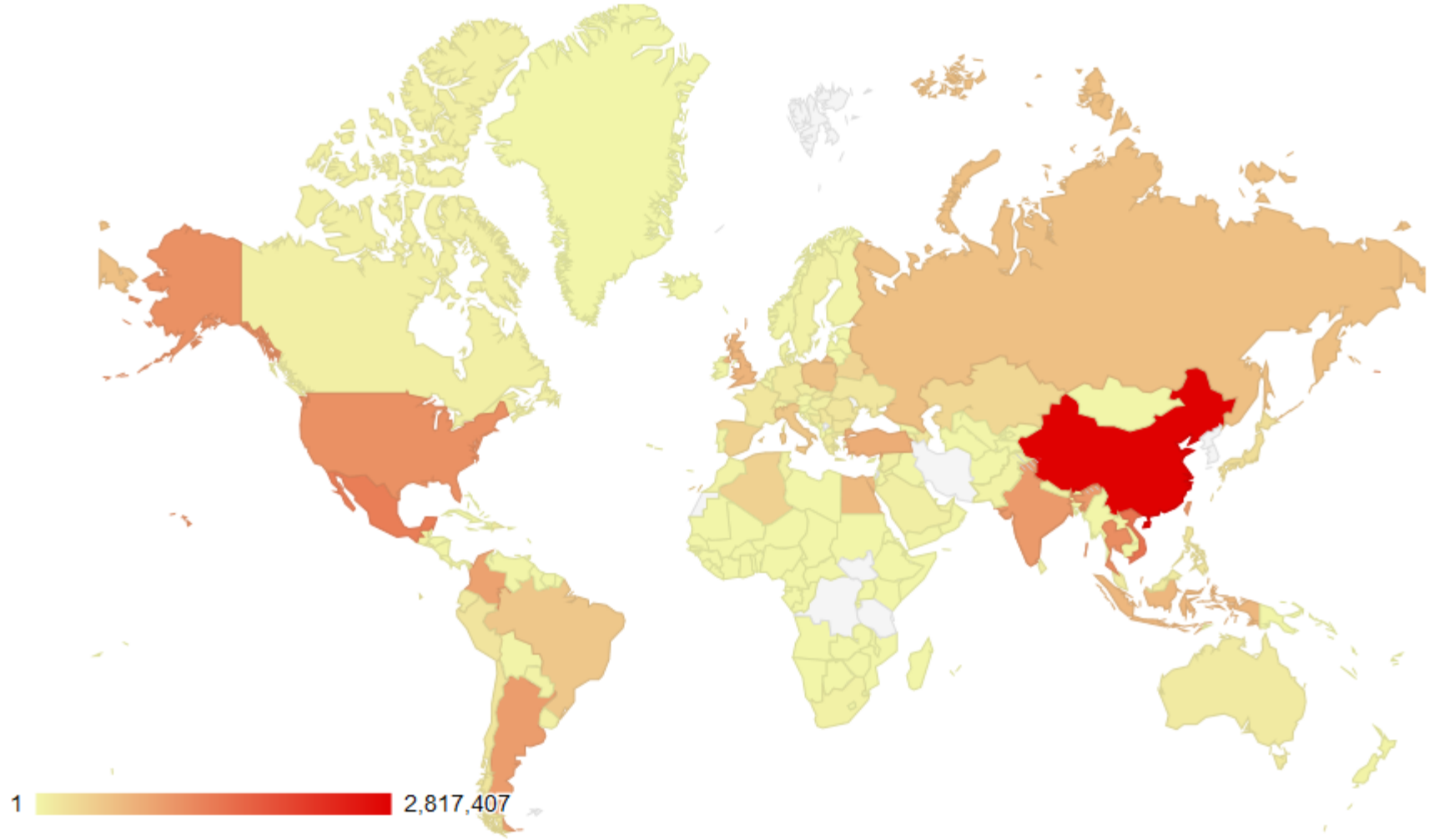
Where are the open resolvers?

- Nearly Everywhere!

- As of: 16th Feb, 2014
- Observed from Open Resolver Project:
  - 31,802,268 total responses to UDP/53 probe
  - 31,105,227 unique IPs
  - 27,432,644 responses had recursion-available bit set

Data on: 16th Feb 2014, Source: openresolverproject.org

Where are the open resolvers?



Data on: 16th Feb 2014, Source: DNS Amplification Attacks Observer

Where are the open resolvers? (Top 30 countries)

Country	Count		Country	Count
China	2817407		Russian Federation	613661
Vietnam	1490402		Poland	585159
Mexico	1371801		Italy	536719
Thailand	1192166		Brazil	527125
United States	1151474		Spain	417102
Taiwan	1064617		Algeria	410379
India	1045396		Belarus	377028
Argentina	1013326		Kazakhstan	345597
Colombia	961150		Japan	269992
Korea Republic of	922700		Peru	191887
Turkey	830253		Philippines	189139
United Kingdom	748433		Romania	182577
Indonesia	718521		Chile	178261
Egypt	665234		Serbia	177489
Iran	644304		France	177105

Data on: 16th Feb 2014, Source: DNS Amplification Attacks Observer

Where are the open resolvers? (Top 30 ASN)

ASN	Count	ASN	Count
AS4134 Chinanet	1449655	AS36947 ALGTEL-AS	410235
AS8151 Uninet S.A. de C.V.	1252527	AS6697 Beltelecom	366259
AS3462 HiNet	982253	AS3352 TELEFONICA	357224
AS45899 VNPT Corp	901042	AS1267 WIND	352192
AS22927 Telefonica Argentina	732786	AS24560 Bharti Airtel	343274
AS17974 PT Telekom Indonesia	669395	AS9829 BSNL	342182
AS9121 Turk	632927	AS9198 Kazakhtelecom	338892
AS9737 TOT	610088	AS4812 China Telecom	333923
AS4837 CNCGROUP	540295	AS4766 Korea Telecom	324598
AS8452 TE Data	461628	AS19429 Colombia	319938
AS13285 TalkTalk	457851	AS701Verizon Business	254440
AS3816 TELECOMUNICACIONES	447406	AS17552 True Internet	230306
AS5617 Telekomunikacja Polska	432065	AS17813 MTNL	212223
AS9318 Hanaro Telecom Inc.	419709	AS7303 Telecom Argentina	195896
AS18403 FPT	418361	AS6147 Telefonica del Peru	190228

Data on: 16th Feb 2014, Source: DNS Amplification Attacks Observer

Fixing this? Preventative Measures!

- BCP-38
  - Source Filtering, you shouldn't be able to spoof addresses.
  - Needs to be done in hosting and ISP environments.
  - If the victim's IP can't be spoofed the attack will stop
  - Will also help stop other attack types
    - (eg: Spoofed Syn Flood).
- BCP-140 / RFC-5358
  - Preventing Use of Recursive Name Servers in Reflector Attacks
  - Provide recursive name lookup service to only the intended clients.

Fixing this? Preventative Measures!

- DNS Server Maintenance
  - Secure the servers!
    - Lock down recursion to your own IP addresses
  - Disable recursion
    - If the servers only purpose is authoritative DNS, disable recursion
  - Historical accidents / incorrect configuration
    - Some Packages (eg, Plesk, cPanel) have included a recursive DNS server on by default.
- Update Internet routers / modems firmware.
  - Some older firmware has security bugs
    - Allows administration from WAN (including DNS, SNMP)

www.cloudflare.com

Fixing this? Preventative Measures!

- DNS 9.x Caching

```
# example only, replace 192.0.2.0/24 a list of your CIDR blocks
acl "trusted" {
    192.0.2.0/24;
};

options {
    recursion no;
    additional-from-cache no;
    allow-query { none; };
};

view "trusted" in {
    match-clients { trusted; };
    allow-query { trusted; };
    recursion yes;
    additional-from-cache yes;
};
```

Fixing this? Preventative Measures!

- Microsoft Windows

1. Using the Windows interface
Open DNS in the console tree, right-click the applicable DNS server, then click **Properties**.

Click the **Advanced** tab.

In **Server options**, select the **Disable recursion** check box, and then click **OK**.

2. Using a command line
Open Command Prompt.

Type:
dnscmd*ServerName***/Config/NoRecursion** 1

Note: By default, recursion is enabled.

Summary

- **Akamai Intelligent Platform**
  - Highly distributed edge servers

- **Open Resolvers are harmful to the Internet community**
  - Secure your DNS server, secure the Internet
  - Stopping DNS reflection attacks

Questions?

Kams Yeung <kams@akamai.com>

More information:

DNS reflection defense:

https://blogs.akamai.com/2013/06/dns-reflection-defense.html

Open Resolver Project:

http://www.openresolverproject.org/

Acknowledgement:

Tomas Paseka tom@cloudflare.com