



CyberGreen

*A global community to measure and improve cyberhealth*

# Risk Mitigation for Open Recursive Resolvers

# Agenda

---

1. Introduction
2. About Open Recursive Resolvers
3. Mitigation recommendations for open recursive DNS resolvers
4. Making the case for implementing mitigations and restriction access to recursive resolvers

# Introduction

---

When cyber infrastructure is insecure there is a risk to the global Internet community

DNS is of critical importance but often overlooked

- Critical network service is delegated to inexperienced and loosely supervised junior system administrators
- When configured insecurely, a DNS server can represent a risk not just to the organization that owns it, but to the broader internet community

# About CyberGreen

---

- Global non-profit and collaborative organization focused on helping improve the health of global Cyber Ecosystem
- Working to provide reliable metrics and mitigation best practice information to Cyber Security Incident Response Teams (CSIRTs), network operators, and policy makers
- Mission: help CSIRTs and others focus remediation efforts on the most important risks
  - Help understand where improvements can be made
  - How we can achieve a more sustainable, secure, and resilient cyber ecosystem

# Copyright (c) 2016, CyberGreen

---

These materials are distributed under the following license:

Permission to use, copy, modify, and/or distribute these materials for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE MATERIAL IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS MATERIAL INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS MATERIAL.



---

# About Open Recursive Resolvers

# Domain Name System (DNS)

---

Domain Name System (DNS) is a standard protocol that translates human-friendly host names like [www.cybergreen.net](http://www.cybergreen.net) into numerical, Internet Protocol (IP) addresses such as 197.222.126.114

DNS resolves name-to-address mappings when browsing web pages, or an email server sends email to another domain



# Domain Name System (DNS)

---

If your computer does not have the mapping already locally stored, your computer will query your company's or ISP's recursive DNS server

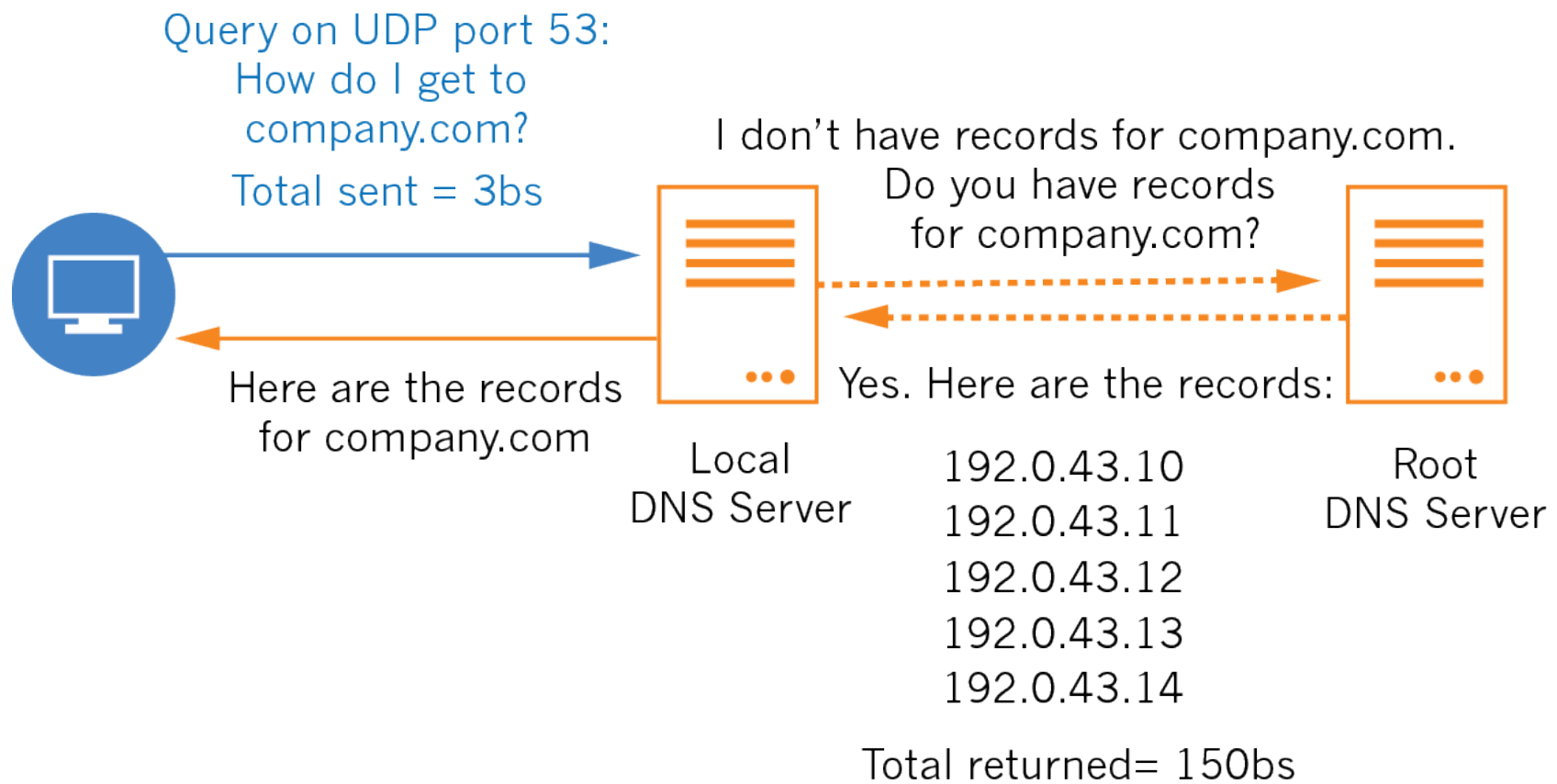
- Without this information, it will query a root name server, which acts like an operator for DNS
  - If root name server does not have answer, it will send your query to a Top-Level Domain (TLD) name server that knows which specific name server is authoritative DNS server for specific domain you seek





# How DNS resolvers work

## How DNS works



# What are open recursive resolvers?

---

“Open recursive resolvers” are recursive resolvers (DNS servers) that will send a reply to any IP address

- Even about domains for which that DNS server is **not** an authoritative DNS server

Recursion is often on by default when DNS servers are first set up



# Risks posed by open recursive DNS resolvers

---

Open recursive DNS resolvers can be used in reflection attacks, a type of traffic amplification attack

- **Denial of service (DoS)** – attacker tries make a victim's machine or network unavailable to its intended users
- **Amplification** – when the attacker sends a small packet to a server that will generate a large reply

In amplification distributed denial of service (DDoS) attacks, attackers simultaneous abuse multiple amplifiers such as DNS servers

- Creates highly-distributed DoS attack conducted from a single command and control host

# Open recursive resolvers in reflection attacks

---

Attacker tries to exhaust the victim's bandwidth by abusing the fact that servers using protocols such as DNS allow spoofing of sender IP addresses

Reflection attacks often exploit User Datagram Protocol (UDP) traffic

- UDP responds to requests without validation of sender identity, i.e. IP address
- UDP traffic can be spoofed (i.e. have a misleading apparent source IP address): attacker can hide true identity



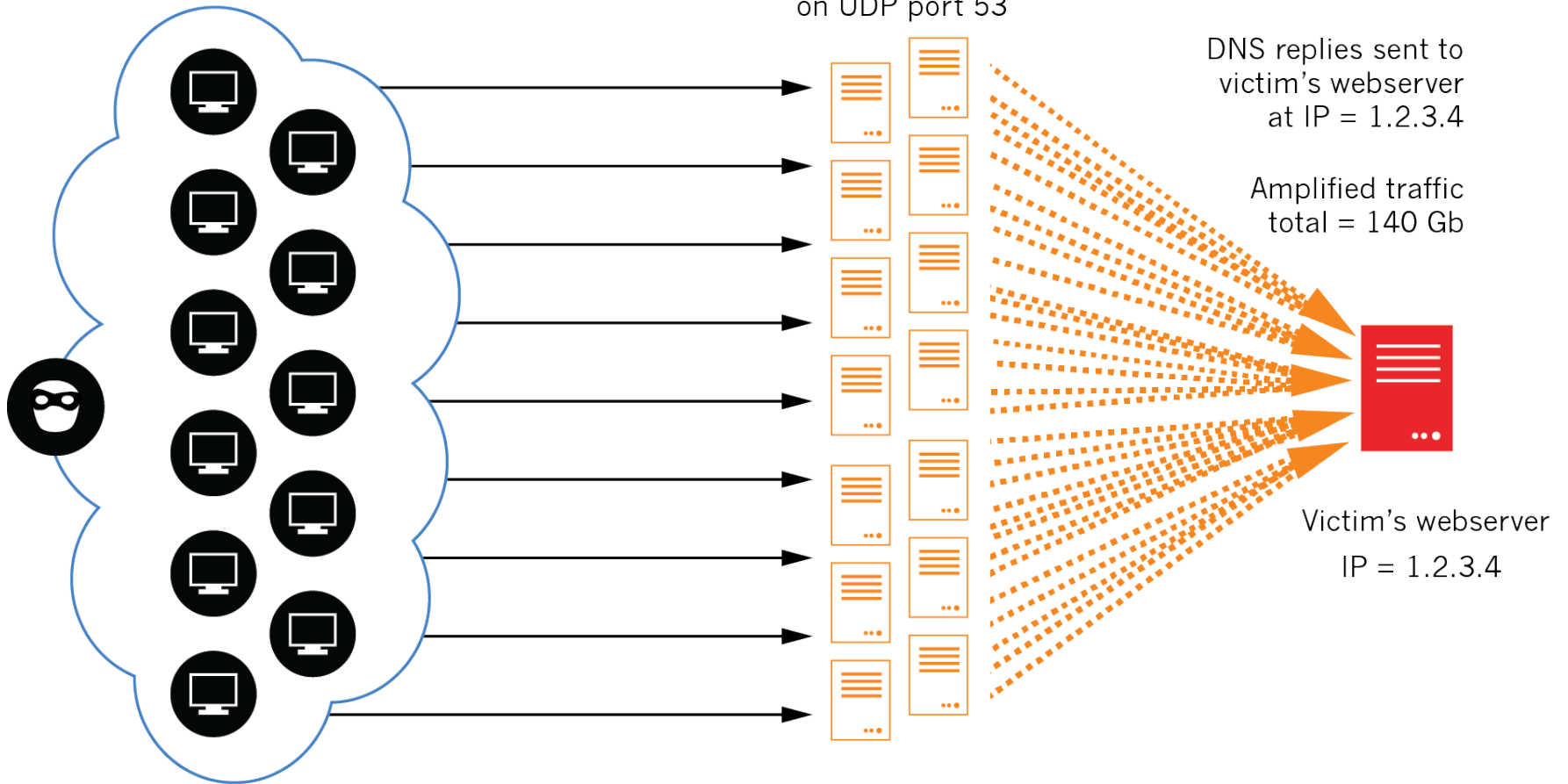
# Open Recursive Resolvers

Attacker controlled botnet targets victim's webserver with IP = 1.2.3.4

Open Recursive Resolvers on UDP port 53

DNS replies sent to victim's webserver at IP = 1.2.3.4

Amplified traffic total = 140 Gb



Botnet systems send DNS requests (UDP port 53) using spoofed source IP of victim (IP = 1.2.3.4)

Total size of all requests = 2 Gb

# DNS in reflection amplification attacks

---

DNS is generally configured as UDP, not TCP, so DNS traffic doesn't adapt to congestion

DNS traffic is almost always allowed through the network perimeter by default

DNS reflection attacks often initiated via botnets (a network of compromised devices controlled by an attacker)

- DNS reflection attacks can be scaled up to any level desired

# DNS reflection amplification attack

---

When DNS is allowed through the network perimeter, botnets can be used to overwhelm a victim with DNS response traffic

Only ***scalable and effective mitigation*** is to reduce number of servers that can be used by attackers

- As of 8/29/16, Shadowserver reported 4,324,696 unique open recursive DNS resolver; see <https://dnsscan.Shadowserver.org/stats/>

# Real life attack using open recursive DNS resolvers

---

Attack in 2009 <sup>[1]</sup> using open recursive DNS resolvers

- Generated 25Gbp/s to 30Gbp/s in traffic using 1 million open recursive resolvers
- Network was flooded and took victim offline, disrupting business

Amplification attacks have become much larger, reaching floods of 300 Gb/s and larger

- Amplification factor has been as high as 179 <sup>[2]</sup> times the original traffic

[1] <http://www.team-cymru.org/Open-Resolver-Challenge.html> (accessed 9/16)

[2] van Rijswijk-Deij, Roland (2014). "DNSSEC and its potential for DDoS attacks - a comprehensive measurement study". ACM Press.



# Potential impacts from open recursive resolvers

---

## Productivity

- Service interruption or failure of business operations relying on network connectivity, particularly for seasonal operations - *e.g. online retailers where a majority of sales happen between Thanksgiving and New Years*
- Time sensitive operations, *e.g. colleges with limited online registration periods or online wagering on sporting events, etc.*



# Other potential open recursive resolver attack impacts

---

## Brand

- Loss of reputation with customers and partners
- Becoming known as a “DoS magnet” in global community

## Technical

- Network service interrupted
- Isolation of victim network by network providers from the rest of Internet to mitigate collateral damage to other customers

## Financial

- Loss of business resulting from service interruption
- Cost of specialized DDoS mitigation services

# Indirect impacts from open recursive DNS resolver attacks

---

You may be impacted if a victim organization ***shares your upstream connectivity***

Open DNS devices on ***your network*** may be used to contribute to an attack on another organization

Potential indirect impacts include:

## Technical

- Network service degraded
- Inbound or outbound bandwidth may be reduced
- Network providers may isolate your network (or at least your insecure recursive resolver) from the rest of Internet

# Other indirect impacts

---

## **Brand**

- Loss of reputation with customers and partners due to slow or unreliable network and systems

## **Financial**

- Unexpected network usage costs
- Loss of business resulting from service degradation

# Mitigate risks from open recursive resolvers

# Mitigation options vary by environment

---

Not all mitigation best practices are appropriate for all environments

CyberGreen provides information relevant to four basic environmental profiles

Look for these icons to find mitigations for your environment

1.  Consumers
2.  Companies
3.  ISPs
4.  Policy Makers

# Mitigate risks from open recursive resolvers

---



The best way to mitigate risks from open recursive resolvers moving forward is to not purchase or deploy devices with resolvers enabled on outside interfaces


Work with your internal acquisition and procurement teams, or vendors about other options

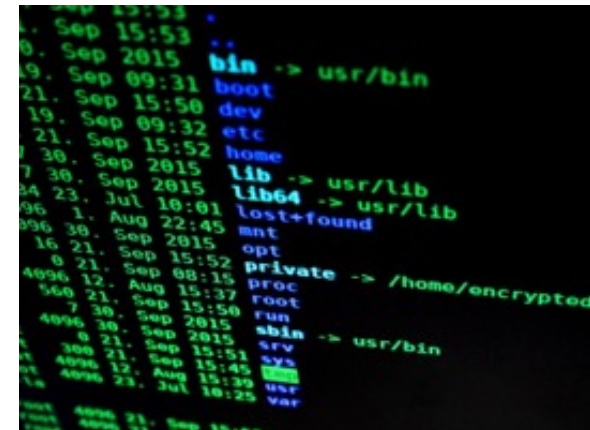


# Find hosts running open recursive DNS resolvers

---

  The simplest way to determine if you have open recursive resolvers is to use a web-based probe, such as the one at <http://openresolver.com>

 ISPs may use tools such as <http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl>





# Manually finding open recursive DNS resolvers

---



To manually identify whether or not open recursive DNS resolvers exist in your environment

Use the command:

```
dig +short @[IP]  
dnsscan.shadowserver.org
```

from a computer that does *\*not\** use the IP listed in the command as its normal recursive resolver

If the recursive resolver is open recursive, you will see the IP address of *dnsscan.shadowserver.org* returned as the result

# Manually finding open recursive DNS resolvers

---



If recursive resolver is **not** misconfigured to be open, you normally see a "query refused" or other failure message – this is GOOD!

For example:

```
$ dig @ns1.dns.ucla.edu dnsscan.shadowserver.org
; <<>> DiG 9.8.3-P1 <<>> @ns1.dns.ucla.edu
dnsscan.shadowserver.org
      (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 8798
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

[etc]
```

# Manually finding open recursive DNS resolvers

---



Some recursive resolvers may be **INTENTIONALLY OPEN**, and carefully monitored to prevent abuse

An example of this is Google's 8.8.8.8:

```
$ dig +short @8.8.8.8  
dnsscan.shadowserver.org  
184.105.143.133
```



# Mitigation: Disable recursion on authoritative nameservers

---



Many DNS servers intended to just provide authoritative name service for specified domains

- DNS resolution for internal systems provided by separate recursive resolver
- Authoritative nameserver provides DNS information only about specified domains for internal and external clients

Authoritative nameservers do not need to support recursive resolution of other domains

- Recursion should be disabled on these nameservers

# Mitigation: Disable recursion on Microsoft authoritative nameservers



## For **Microsoft DNS Server**:

1. Right-click the DNS server and click Properties
2. Click the Advanced tab
3. In Server options, select the “Disable recursion” check box, and then click OK

For details, see:

<http://technet.microsoft.com/en-us/library/cc787602.aspx>



# Mitigation: Disable recursion on BIND authoritative nameservers

---



For **BIND9**

```
options {  
    allow-query-cache { none; };  
    recursion no;  
};
```

For details, see:

<http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992>

More information about Bind and Microsoft nameservers

<http://www.team-cymru.org/Services/Resolvers/instructions.html>

# Mitigation: Disable recursion on authoritative nameservers for Microsoft

---



If you are using other DNS software, such as Unbound, please consult your documentation

You may need to set up recursive and authoritative DNS as separate, independent services to achieve the desired result of segregating recursion and authoritative DNS services

# Mitigation for consumers and small businesses

---



Consumers and small businesses typically do not maintain their own DNS servers, but should ensure their broadband routers are secure

- Clear, comprehensive explanation at <http://www.ghacks.net/2015/03/24/secure-you-wireless-router/>



Shields Up from Gibson Research Corporation (free!) can identify what services are open to the Internet:

<https://www.grc.com/x/ne.dll?rh1dkyd2>



- Select “all service ports”: screen full of little green boxes, you do not have services open to the Internet!



# Mitigation: Limit recursion to authorized clients

---



For DNS servers within an organization or Internet Service Provider: resolver should be configured to perform recursive queries on behalf of authorized clients only

These requests typically should only come from clients within the organization's network address range



# Mitigation: Limit recursion to authorized clients for BIND9

---



Add lines such as the following, changing corpnet IP ranges to your organization's actual internal IP address range(s):

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };  
options {  
    allow-query { any; };  
    allow-recursion { corpnets; };  
};
```

For details, see

[http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access\\_Control\\_Lists](http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists)

# Mitigation: Limit recursion to authorized clients for Microsoft

---



**For Microsoft DNS Servers, restricting recursive DNS requests to a particular IP address range is not possible at this time**

A different, caching-only name server should be set up inside the organization to provide recursive resolution

- Use firewall rule to block incoming access to the caching-only server from outside the organization's network

*Note: the authoritative name server needs to be hosted on a separate server and configured to disable recursion*

# Mitigation: Configure authoritative DNS servers to use Response Rate Limiting (RRL)

---



Response Rate Limiting (RRL) is an experimental feature, available as a set of patches for BIND9

- Allows an administrator to limit the maximum number of responses per second being sent to one client
- Should be used on only authoritative domain name servers as it will affect performance on recursive resolvers

**RRL is currently not available for Microsoft DNS Server**



# Mitigation: Configure authoritative DNS servers to use Response Rate Limiting (RRL)

---



Authoritative and recursive name servers should run on different systems

- RRL implemented on authoritative server
- Access control lists implemented on recursive server

Note: RRL may prevent legitimate hosts from receiving answers

- May increase the risk for successful DNS cache poisoning attacks
- Risk is small, particularly if you have implemented DNSSEC correctly

# Mitigation: Configure authoritative DNS servers to use Response Rate Limiting (RRL)

---



Patches 9.8/9.latest support RRL on UNIX

- Red Hat Enterprise Linux 6 updated packages in advisory RHSA-2013:0550-1

To run the RRL patches, include these lines to options block of the authoritative views:

```
rate-limit {  
    responses-per-second 5;  
    window 5;  
};
```

For details, see <http://www.redbarn.org/dns/ratelimits>

# Mitigation: Configure authoritative DNS servers to use Response Rate Limiting (RRL)

---



A TCP+ANY patch for BIND forces TYPE=ANY queries over TCP

- Prevents those queries from coming from spoofed locations

For details, see

<https://lists.dns-oarc.net/pipermail/dns-operations/2013-May/010175.html>

# Mitigations for ISPs

---



Proactively block inbound port 53 to recursive resolvers

- Use ACLs, flow-spec or other technical mechanisms



Monitor DNS between your customers and resolvers for signs of amplification attacks

- Generate abuse tickets for customers when observed
  - Take a customer's modem offline
  - Notify customer via phone call





# Mitigations for ISPs

---



Limit customer access to random third-party recursive resolvers, as detailed at:

[https://www.m3aawg.org/sites/default/files/maawg\\_dns\\_port\\_53v1.0\\_2010-06.pdf](https://www.m3aawg.org/sites/default/files/maawg_dns_port_53v1.0_2010-06.pdf)

Notify your customers of issues, even if you can't tell them how to fix them

- They may not be intentionally running a DNS server
- Traffic may be the result of malfunctioning home routers that ISP Customer Care has no idea how to reconfigure

# Other mitigations for ISPs

---



Consider rate limiting “ANY” queries

- These comprise most of what is seen in amplification attacks

Consider deploying DDOS mitigation hardware between your customers and resolver

# Spoofed Traffic Mitigation: Implement ingress filtering on networks

---



Internet Engineering Task Force (IETF) Best Current Practice (BCP) documents

Configuration changes to substantially reduce potential for source IP spoofed attacks, the most popular DDoS attack type

- How to filter network traffic on network to verify the source address of a packet
- Reject packets with source addresses that are not reachable via the actual packet's path



# IETF BCPs recommended

---



All network operators should perform network ingress filtering as described in these BCPs:

## **BCP-38 Network Ingress Filtering**

- Defeating Denial of Service Attacks which employ IP Source Address Spoofing:

<https://tools.ietf.org/html/bcp38>

## **BCP-84 Ingress Filtering for Multihomed Networks**

- <https://tools.ietf.org/html/bcp84>

# Not all devices should listen for DNS

---



Customer premises equipment (CPE) are devices like cable modems, DSL modems, broadband routers, etc.

CPE should not typically listen for DNS packets on WAN interface, includes NETWORK and BROADCAST addresses

**Consult with your provider** that source address validation is configured on

- Statically-routed CPE
- Data center equipment edges with fixed IP ranges

Command to implement on router interface:

```
ip verify unicast source reachable-via rx
```

# More info on IETF BCPs

---

Test whether your network currently follows BCP-38 using tools from the Spoofer Project:

<https://www.caida.org/projects/spoofer/>

Additional details about how to implement BCP-38:

[http://www.bcp38.info/index.php/Main\\_Page](http://www.bcp38.info/index.php/Main_Page)



# Verify your fix

---



After implementing your mitigation measures, you can verify your fix by running:

```
dig +short @[IP]  
dnsscan.shadowserver.org
```

If you are NOT vulnerable you should see query refused, as discussed in [slide 26](#)

Monitor your infrastructure to prevent re-occurrence by subscribing to free reports from Shadowserver, available at

<https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>

# Additional DNS resources

---

<https://dnsscan.shadowserver.org/>

<http://openresolverproject.org/>

<https://www.us-cert.gov/ncas/alerts/TA14-017A>

<https://www.stsauver.com/~joe/secprof10-dns/secprof10-dns.pdf>

<https://www.us-cert.gov/sites/default/files/publications/DNS-recursion033006.pdf>

<https://www.cert.be/docs/dns-amplification-attacks-and-open-dns-resolvers>

<https://www.cert.be/files/DDoS-proactive-reactive.pdf>

<https://community.infoblox.com/t5/IPv6-Center-of-Excellence/Finding-and-Fixing-Open-DNS-Resolvers/ba-p/3405>



# Making the case for implementing mitigations such as BCP 38 and restricting access to recursive resolvers

# Making the case for mitigations

---



Help everyone understand the level of effort needed to improve cyber health in their community

Why should you implement the mitigations in your environment?




1. It is the right thing to do as a good Internet neighbor
2. Your organization may be next to be attacked

***Let's join together and stop bad guys from winning!***



# Changing risk landscape

---

-    Increased need to demonstrate “due care”
- Obtaining cyber insurance
  - Complying with risk frameworks to win business with local / national governments and large corporations

If we (***you!***) don't do a better job of securing our own infrastructure and reducing cyber risk, government regulation may force additional mandates and/or penalties



# Anticipated organizational benefits

---

## **Increased productivity**

- Fewer service interruptions and failures

## **Improved network performance**

- Existing network more reliable and resilient, with greater capacity

## **Improved brand reputation**

- Technical reliability and security a selling point to customers



# More anticipated benefits

---

## **Decreased budget uncertainty**

- Fewer unanticipated usage costs for IT
- Budget can be used as planned, e.g. - upgrading technical capability / capacity, additional personnel, etc.

System admins may spend less time spent trying to deal with unexpected problems

- May improve their productivity and reduce unexpected overtime



# What do you need to implement these mitigations?

---

 Commands and configuration details for most important mitigations are publically available


- No additional software must be purchased
- Implementing mitigations does not require any special knowledge, skills, or abilities



Note: All mitigations should be carefully reviewed in light of your specific business requirements and infrastructure environment before proceeding

All organizational change management processes, including testing, should be followed

# How long will mitigations take?

---

 System administrators in smaller organizations need a few hours per domain server to investigate, implement and verify the basic mitigation of disabling recursion

  ISPs and large entities can automate administration of changes via configuration management systems with task execution (Salt, Ansible



# How long to implement BCP-38 network ingress filtering?

---



Small businesses: from a few minutes to less than an hour



Larger and more complex organizations: days to weeks

Bonus: with no real maintenance, the recurring cost is effectively zero!



# Acknowledgement

---

CyberGreen would like to thank the experts who made the creation of this document possible:

Written by:

- Laurin Buchanan, Applied Visions, Inc. – Secure Decisions Division

Contributed and Reviewed by:

- Matt Carothers, Cox Communications
- Baiba Kaskina, CERT.LV
- Moto Kawasaki, JPCERT/CC
- Art Manion, CERT/CC
- Yoshinobu Matsuzaki, IJ
- Joe St Sauver, Farsight Security
- David Watson, ShadowServer Foundation

Disclaimer: CyberGreen believes this guidance and the advice from our experts should be of benefit to anyone mitigating a risk conditions, but it is not advice specific to any reader or network. Ultimately, each reader is responsible for implementing his or her own network remediation strategy and we assume no responsibility or liability therefore.



For more information about  
risk mitigation best practices  
please contact:  
[contact@cybergreen.net](mailto:contact@cybergreen.net)