CARICERT
Caribbean Cyber Emergency Response Team

TLP WHITE

Open Resolvers Project Curaçao

Charlton Donker, MBA, BSc

Senior Security specialist @CARICERT

Bureau Telecommunicatie en Post

lacnic

CURAÇAO SAFE ONLINE

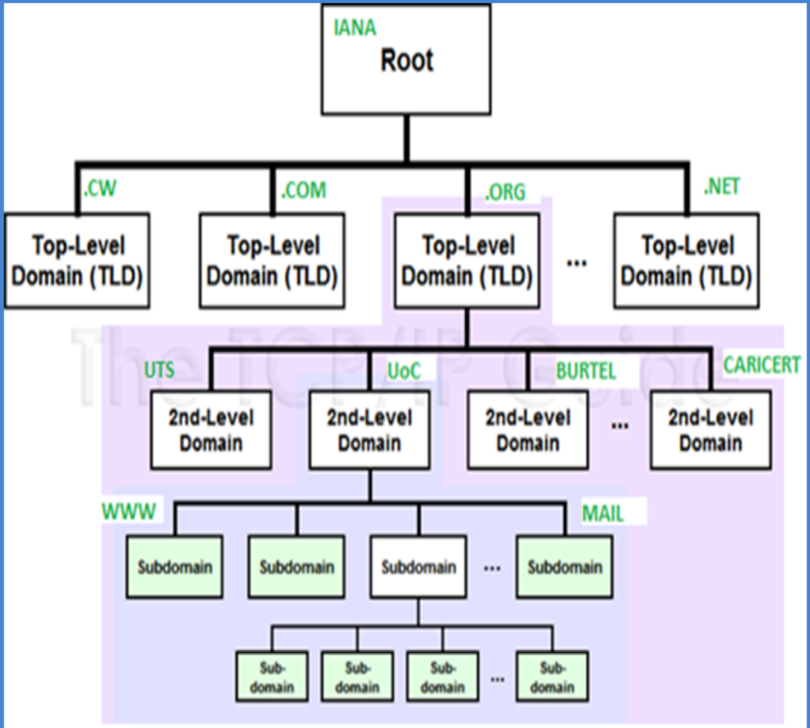
CARICERT
Caribbean Cyber Emergency Response Team

Introduction

- .CW Statistics 2018
- CARICERT identified different infected IP addresses
- CARICERT noticed a long list of DNS open resolvers
- Incentive to start with an open resolver project for our local domain

Bureau Telecommunicatie en Post lacnic CURAÇAO SAFE ONLINE

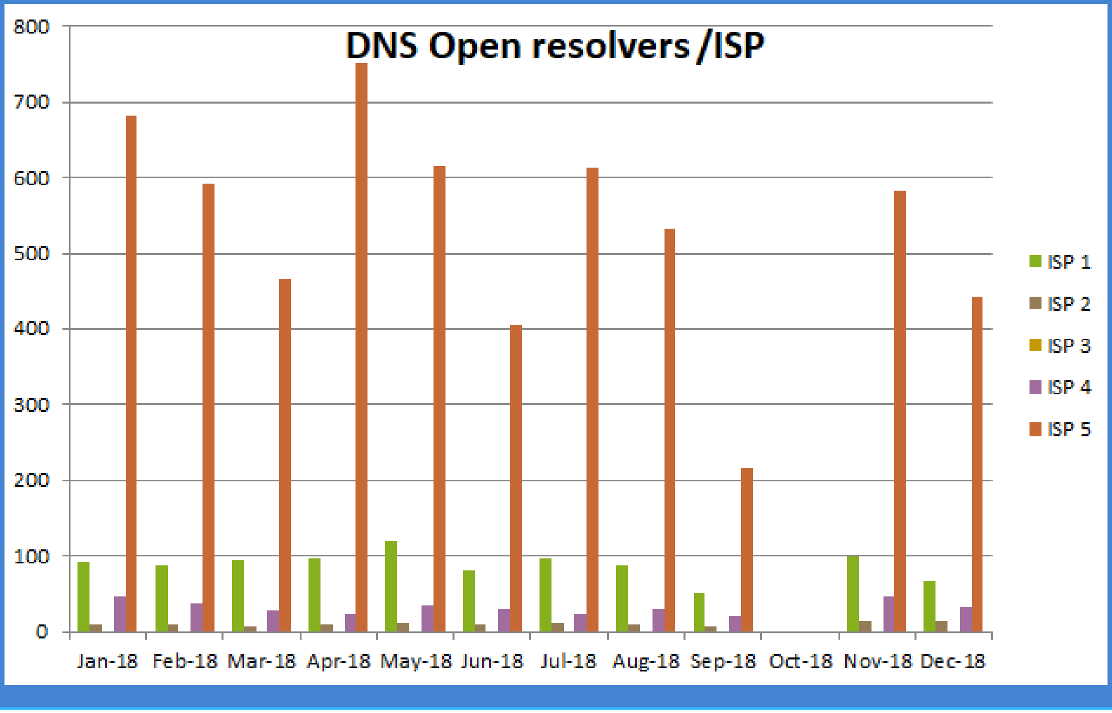
Domain Name Space tree



CARICERT
Caribbean Cyber Emergency Response Team

Open Resolvers Statistics per ISP

○



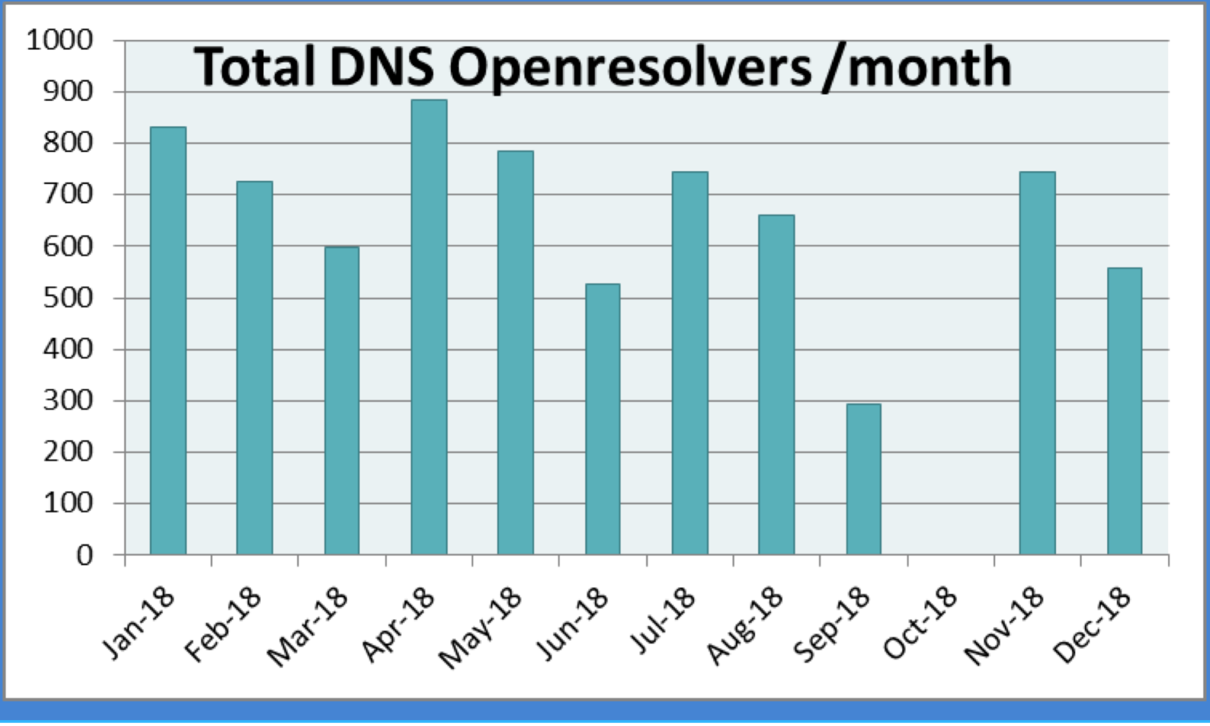
Bureau Telecommunicatie en Post

lacnic

CURAÇAO SAFE ONLINE

CARICERT
Caribbean Cyber Emergency Response Team

Total Open Resolvers Statistics



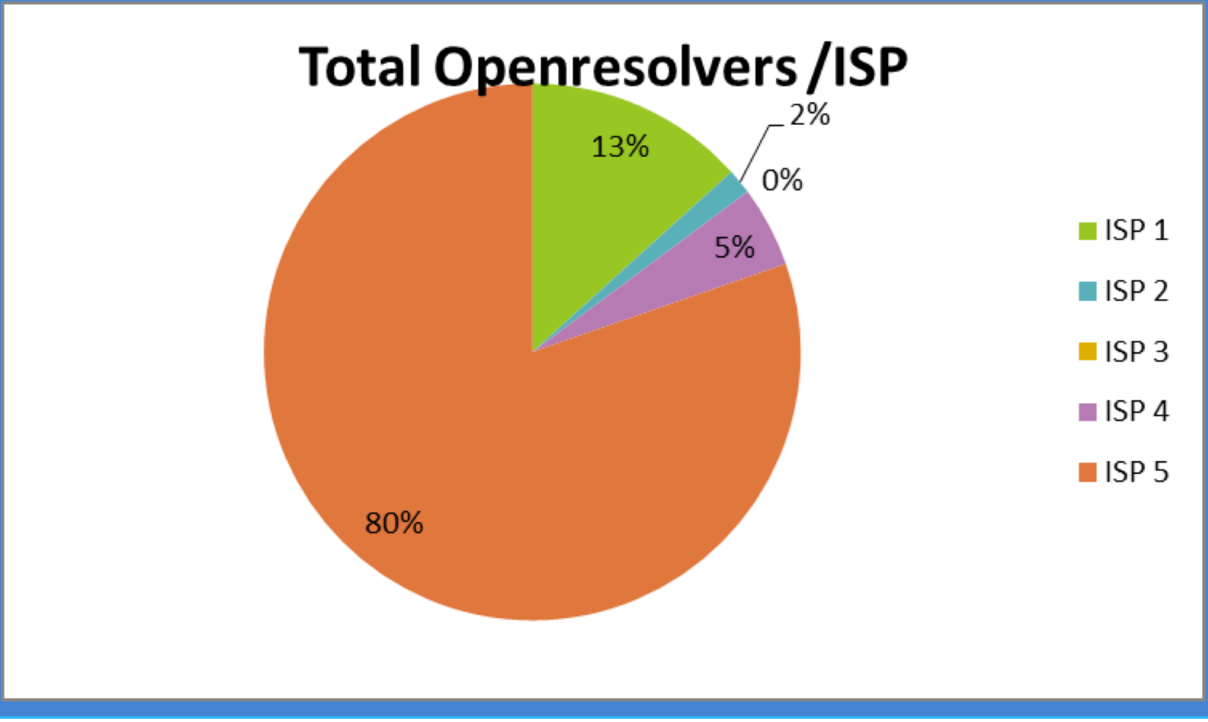
Bureau Telecommunicatie en Post

lacnic

CURAÇAO SAFE ONLINE

Open Resolvers Statistics

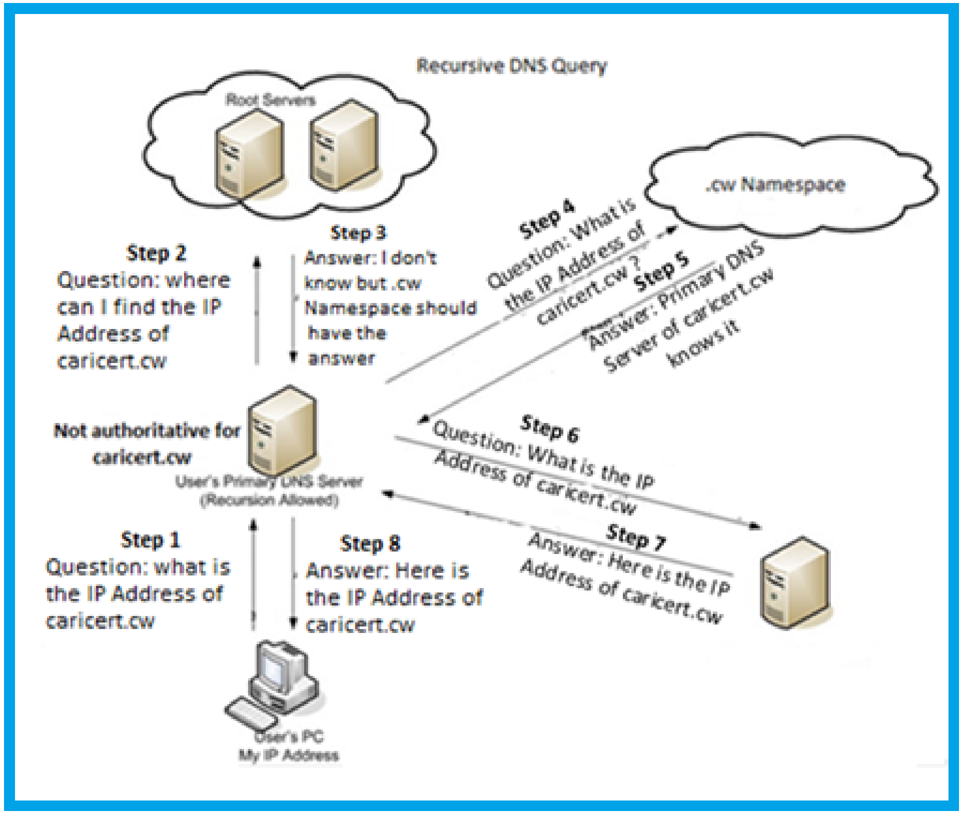
○



Problem Description

- Open Resolvers pose a significant risk to the global network infrastructure
- Open Resolvers are vulnerable for:
    - DOS attacks
    - DNS cache poisoning
    - Unauthorized use of resources
    - Root name server performance degradation

Recursive DNS Query



Recursive DNS Query

Step 1
Question: what is the IP Address of caricert.cw

Step 2
Question: where can I find the IP Address of caricert.cw

Step 3
Answer: I don't know but .cw Namespace should have the answer

Step 4
Question: What is the IP Address of caricert.cw ?

Step 5
Answer: Primary DNS Server of caricert.cw knows it

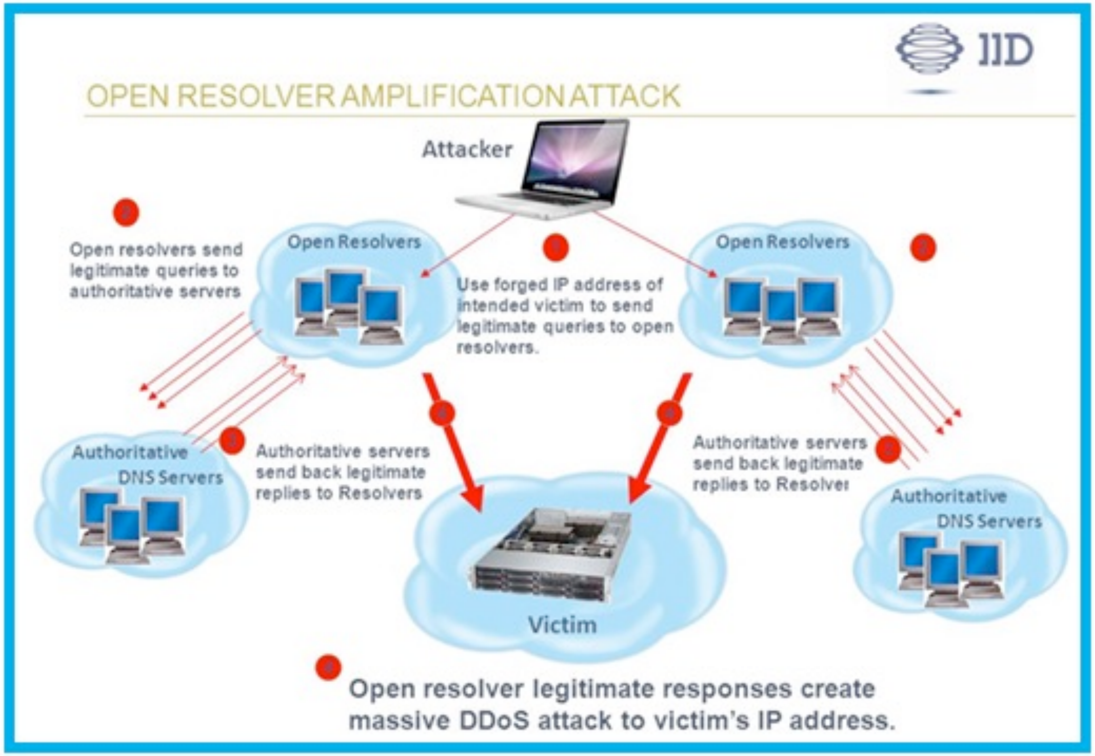
Step 6
Question: What is the IP Address of caricert.cw

Step 7
Answer: Here is the IP Address of caricert.cw

Step 8
Answer: Here is the IP Address of caricert.cw

Not authoritative for caricert.cw

Analysis & Breakdown



OPEN RESOLVER AMPLIFICATION ATTACK

Open resolvers send legitimate queries to authoritative servers

Use forged IP address of intended victim to send legitimate queries to open resolvers.

Authoritative servers send back legitimate replies to Resolvers

Authoritative servers send back legitimate replies to Resolver

Open resolver legitimate responses create massive DDoS attack to victim's IP address.

How to detect open resolvers in your network?

1. https://www.openresolver.nl/
2. https://www.thinkbroadband.com/tools/open-dns-resolver-check/
3. https://openresolver.com/
4. http://www.openresolver.jp/en/

CARICERT

Caribbean Cyber Emergency Response Team

Mitigation & Possible Solutions

- Applying proper egress filtering on your network.
- Follow security best practices for configuring DNS
- DNSSEC

Bureau Telecommunicatie en Post

lacnic

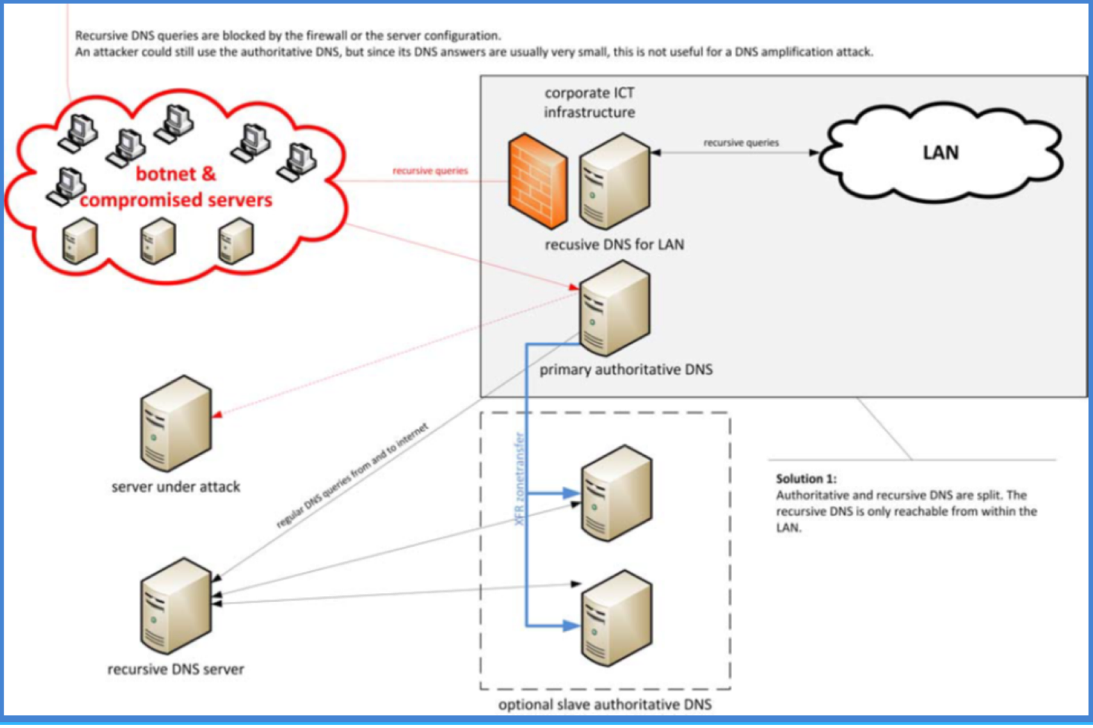
CURAÇAO SAFE ONLINE

Mitigation & Possible Solutions

- Response Rate Limiting
- Limit recursion.

Possible DNS Configuration

○

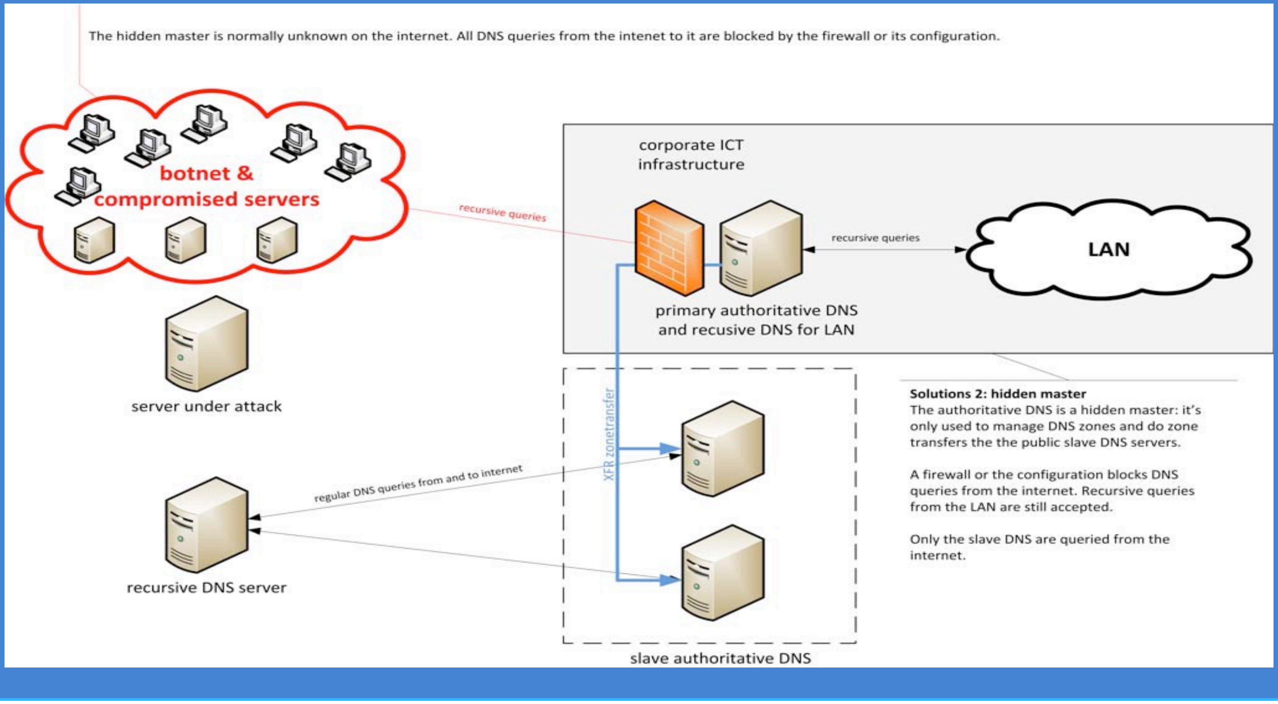


Recursive DNS queries are blocked by the firewall or the server configuration.
An attacker could still use the authoritative DNS, but since its DNS answers are usually very small, this is not useful for a DNS amplification attack.

Solution 1:
Authoritative and recursive DNS are split. The recursive DNS is only reachable from within the LAN.

Possible DNS Configuration

○



The hidden master is normally unknown on the internet. All DNS queries from the intenet to it are blocked by the firewall or its configuration.

Solutions 2: hidden master
The authoritative DNS is a hidden master: it's only used to manage DNS zones and do zone transfers the the public slave DNS servers.

A firewall or the configuration blocks DNS queries from the internet. Recursive queries from the LAN are still accepted.

Only the slave DNS are queried from the internet.

Conclusion & Recommendations

- All misconfigured DNS Servers might be an Open resolver.
- There's still a limit to the influence of the ISP’s on the behavior of their customers.
- Limit recursion to only authorized clients

Conclusion & Recommendations

- Configure Authoritative DNS servers to use DNS RRL [Response Rate Limiting].
- Apply the recommendations from IETF (BCP-38) and (BCP-84) documents.
- Update the local Cyber Security Laws

CARICERT
Caribbean Cyber Emergency Response Team

Thank You

Bureau Telecommunicatie en Post

lacnic

CURAÇAO SAFE ONLINE