Vulnerability of DNS name servers against BGP hijacking

R.H.H.G.M. Linssen (Raoul)
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
r.h.h.g.m.linssen@student.utwente.nl

ABSTRACT

The Border Gateway Protocol (BGP) is essential for the Internet to function, but remains in itself susceptible to certain types of attacks, such as a BGP hijack. In case of a BGP hijack, traffic is routed over a different transit router, making Domain Name System (DNS) queries easy to manipulate. From that point different malicious attacks could be performed, such as: many domains could be routed to an incorrect (possibly malicious) IP-address or DNS requests could simply be dropped. One solution for the BGP hijack is the Resource Public Key Infrastructure (RPKI). The deployment of RPKI has started in 2011 and is relatively new. This research performs an analysis on the vulnerability of DNS name servers in case of a BGP hijack. The research is *observational* and *cross-sectional*. A *quantitative* analysis of both protected and unprotected DNS name servers is performed.

The research looks at 11 different Top Level Domains (TLD) (including .nl,.com and .net) and the root zone, root hints and public resolvers. The research looks at the overall RPKI deployment per zone, IPv4 and IPv6 differences, country differences (in each case focusing on DNS servers).

Overall, the result is that 45% of the DNS servers reside in a protected prefix. IPv4 (71,85%) seems to be doing better than IPv6 (28,15%). 27,46% of DNS servers inside of the country of the zone itself seem to be protected. In The Netherlands about 41,48% of the domains seems to be using a DNS server located in a protected prefix.

In conclusion, to create the largest impact on the amount of RPKI protected prefixes, the research advises to look at the prefixes containing the biggest amount of DNS servers. One possible obstacle is the fact that prefixes for a zone can reside in different countries.

Keywords

BGP, BGP hijacking, DNS, DNS vulnerability and RPKI

1. INTRODUCTION

The Border Gateway Protocol (BGP) is the backbone of the Internet in terms of routing. Every packet routed over the internet will go over some network discovered by this protocol. BGP has been around since 1994 [1]. During this time security for the end user (e.g. Hypertext Transfer Protocol Secure (HTTPS)) has improved substantially. At the same time BGP has had some improvements, but these improvements are not widely used and some still have several limitations.

The impact on DNS servers in case of a BGP hijack is further explained in section 2. During a BGP hijack, DNS requests could be rerouted to a malicious DNS server or requests could simply be dropped.

The main objective of the research is to answer the following question:

How vulnerable are DNS name servers during a BGP hijack?

A quantitative analysis will address this research question. Background and related papers of the research topic are discussed in the literature review section.

Addressing the following questions will contribute to answering the main research question of this paper:

1. How many DNS name servers are located in networks that are protected with a valid Route Origin Authorization (ROA)?
2. Is there a difference between DNS name servers located in different countries?
3. How many domain names are managed by name servers that are protected with valid ROAs?
4. Do DNS servers reside in the same prefix? If so, which prefixes contains the most DNS servers?

The second question will compare different TLD's and see if the DNS servers located in the country of the TLD are ROA protected. This will give an indication on how different countries perform in the RPKI deployment area

The third question will look at all the domains in a zone and then cross reference to the DNS servers. The result could give an indication on which domains use protected or unprotected DNS servers (or partial protected).

The fourth question will tell which prefixes are responsible for a large portion of the DNS servers. This could help to increase the number of RPKI deployments by focusing on certain high impact prefixes.

2. BACKGROUND

This section will discuss some background issues of the research topic.

2.1 BGP hijacking

One of the major shortcomings of BGP is the vulnerability for a (BGP) hijack. A hijack can happen when an Autonomous System (AS) falsely announces the origin of a prefix. When this announcement is accepted by a neigh-

32^th Twente Student Conference on IT Jan. 19^nd, 2020, Enschede, The Netherlands.

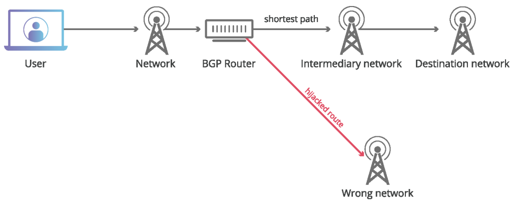

Figure 1. BGP hijacking [4]

bor, this neighbor will possibly route their packets in a different way. In the worst case scenario this will result in data being routed to a new malicious AS and is called a BGP hijack. A total overview of this phenomenon is presented in Figure 1.

2.2 RPKI

One of the solutions for a BGP hijack is RPKI [2]. RPKI is a method to sign a prefix (IP-address block) and an AS together. An AS is a group of routers all announcing the same IP-address prefixes. An AS is responsible for granting access to a set of IP-addresses for the rest of the world. Any BGP router can use RPKI to validate the correctness of the route being announced. RPKI is not commonplace yet. Even the AS network responsible for the DNS server of Google do not support RPKI [3]. Every Regional Internet Registry (RIR, responsible for handing out the AS and the RPKI certificate) provides (via rsync) all public certificates to a Validator. This Validator responds to validation queries from the BGP router. Optionally, an owner of an AS can add the "maximum length" field to its certificate. When not set, the announcer can only announce the exact route as stated in the certificate. When a ROA authorises a /24 and the Maximum Length field is set to /25, a /24 or two adjacent /25 blocks can be announced.

2.3 DNS

The basic usage of DNS is to resolve a domain name to an IP address and vice versa. DNS has been introduced in 1984 [5]. Unless an extension is used a DNS resolve happens in plain text without integrity or origin verification. Since inception, DNS had a number of extensions, just like BGP. DNS Security Extensions (DNSSEC) is one of these extensions. DNSSEC validates the origin and the authenticity of the message, but does not provide any privacy on the DNS request itself.

2.4 BGP hijack of a prefix

In case of a BGP hijack Internet traffic will be routed to a different AS. When this occurs, DNS requests will be redirected to this new AS. Not every DNS server is using an extension like DNSSEC (looking at a global scale), as such making it vulnerable for the receiving AS to alter the incoming DNS requests. In that case the requesting server or PC will go to an incorrect IP address. Alternatively, all incoming packets on the new (bogus) AS could simply be dropped. This could make parts of the Internet inaccessible to the public.

2.5 Motivation

Last year RPKI has steeply increased in popularity. The most prominent cause has been the indirect DNS hack on the Amazon AWS servers [6]. After this incident, there was a substantial increase in publications on tech sites. Even RIPE (responsible for handing out BGP Autonomous System Numbers (ASN) in Europe, Middle East and Russia) created a *Deployathon* focused on RPKI and they show the increase in RPKI adoption before the incident [7]. Earlier this year [8], the *China Telecom's network* rerouted traffic meant for Europe over its own network for more than 2 hours. BPG hijacking is an everyday occurrence (2) putting the stability and the safety of the internet itself at risk.

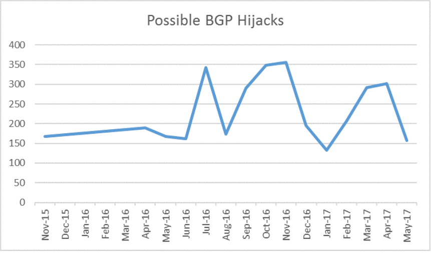

Figure 2. Number of BGP hijacks from November of 2015 to May of 2017 [10]

BGP is used by ISP's and companies, therefore this research is more relevant to those sectors. For a normal end-user it requires special software like a BGP looking glass [9] to even analyse packets transmitted by the BGP protocol.

The purpose of the research is to assess the vulnerability of DNS name servers in the case of a BGP hijacking.

3. LITERATURE REVIEW

Below, related studies to this research are briefly summarized:

RPKI is coming of age [11]: this recent research (October this year) is a longitudinal study following the deployment rate since the creation of RPKI itself. The authors mainly focused on invalid route origins, but nevertheless conclude: "RPKI is ready for the big screen, and routing security can be increased by dropping invalid announcements". Giving an indication that RPKI is ready, but not widely deployed. Therefore many DNS name servers may still be unsecured from a RPKI point of view. This only gives an indication and will be further analysed in this research. This research does not focus on DNS servers specifically, but looks at RPKI in general.

The big picture of the DNS[12]: this study looks at the current deployment of DNS and how it is used. One of the conclusions: "*roughly half of the observed traffic is handled by only 1 k authoritative name servers and by 10 AS operators*". Therefore, implementing RPKI on some key location could have major advantages.

Understanding the role of registrars in DNSSEC deployment [13]: as stated in this paper, still only 1% of the .com,.net and .org domains are properly signed. Many of the leading registrars (for these domains) simply don't support DNSSEC. The effort for most domain owners is simply to high to implement DNSSEC. Improvements in this area may be beneficial in decreasing the vulnerability of DNS in case of a BGP hijack.

RiPKI: The tragic story of RPKI deployment in the web ecosystem [14]: this paper takes a closer look at the deployment of RPKI. Top sites on Alexa are analysed. Their conclusion on why the adoption to RPKI is so slow is as follows: " *Our findings revealed that CDN hosters are the likely cause*". This indicates that CDN networks should be a focus point for increasing the RPKI deployments in a faster pace.

TLD	public resolvers	root hints	root zone	.com	.dk	.ee	.fi	.net	.nl	.se	.gt	.na	.ru	.co
Companies	22	-	-	-	-	-	-	-	-	-	-	-	-	-
Domains	*	13	4138	1972865	18736	12972	21333	543100	72807	45365	6777	3264	104442	96435
DNS servers	130	26	7702	2352637	26525	18988	29045	663977	91203	56208	9482	4922	121331	121798

Table 1: Used data sets (* not every company uses a domain name)

4. METHODOLOGY

Different trajectories can be followed to answer the main research question. Based on the research questions and the insights from the *Literature review* the research uses a *observational cross-sectional* analysis. The analysis will be done on data listed by OpenIntel [15]. An example of an entry in this dataset is explained in section 4.2. These lists are snapshots of one point in time. As such, this study is cross-sectional. There is no intervention on the provided data and therefore the research is observational. For the recursive resolver the list on Wikipedia is used [16]. Information about the used data is presented in table 1. The DNS servers are further divided in IPv4 and IPv6 (see figure 3).

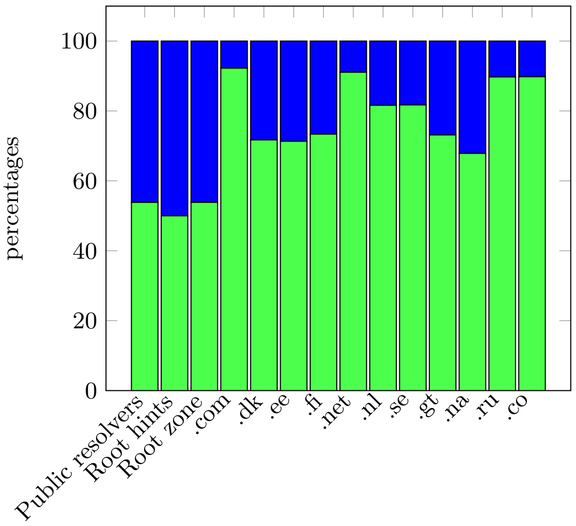

Figure 3. Division of IPv4 and IPv6 2nd level DNS servers per TLD (green= IPv4 DNS server and blue= IPv6 DNS server)

4.1 Process

The following list clarifies the main elements of the strategy. The whole procedure is put together into one program which is described in section 4.2. This section will give an overview of the most important functions of this program. The RIPE RIS API [17] is used to get results on an IP-address.

1. Program iterates over domains from data set of OpenIntel
2. Program uses the IP-address in a row to ask the RIPE database for an ASN,prefix and the validity on the provided prefix. RIPE will return: Valid (=origin AS is allowed to announce the prefix),Invalid (= the origin AS is not allowed to announce the prefix) or Unknown (=announced prefix is not covered by RPKI) for the ROA. The created software will not make a difference between *invalid* and *unknown*. In the figures presented in section 5 an *unprotected* prefixes can be both an invalid or unknown value in the RIPE database.
3. These results are stored, without any analysis on the data
4. The next step will analyse the newly written data. This part of the program will look at the resulting file from the previous step and generate a report including answers to the research questions (section 1). The output file will a .json and/or .csv file, depending on the used function.

4.2 Software

The software created for this research is called 'Brum'. It is an *RPKI deployment analysis tool.* Every result in this thesis is generated with Brum. A full guide on Brum is available in an online repository where Brum itself can be downloaded as well [18] (at the time of writing this paper, Brum is at version 0.1.4). The RIPE API is used to lookup if a valid ROA is present for a IP prefix.

4.3 Input files

Zone file: this list is not public, but is provided by OpenIntel [15]. A zone file is a *complete* list of all domains in that specific zone, in this case the .nl zone. A shorter list is used and only contains the DNS name servers for this zone. This list will be used under a NDA agreement. The data from OpenIntel looks as follows:

NS address,tot,IPv4 address,IPv6 address,country,AS

Briefly, the NS address is the domain name address of the DNS server, followed by the *tot* which is the total number of domains this DNS server is responsible for. After these two arguments, are the IP address (either IPv4 or IPv6) and the country. The last argument is the Autonomous System.

For this research the following zone files were used:

.com, .dk, .ee, .fi, .net, .nl, .se, .gt, .na, .ru and .co

To get the most comparable results all zones are from the same dates. All zones stated above are from the date 17-12-2019 and the lookup tests (discussed in section 4.5) except for .ee,.gt,.na and .co they are from 01-13-2020. The lookup tests are done as close as possible to this date in order to get more realistic results. Running the tests close to the extracted time of a zone is important to minimize the changing of any information such as a ASN or prefix.

Some special cases were tested as well:

- **Root hints** These are the 13 root hints as are provided by IANA [19].
- **Root zone** This is the complete root zone as is provided by IANA [19].
- **Public resolvers** There is no complete list of all the public resolvers. Therefore, a list of 130 (most common) public resolvers is used [20].

4.4 Output files

Brum will generate a .json file as a final result containing all the information it gathered from (e.g.) a zone file. Brum will generate a lot more results than presented in this paper, but overall it will generate the following results: valid ROA in various cases, ASN information, prefix information, errors during any lookup, 10 largest (protected|unprotected|partial-protected) autonomous systems and all the previous results with a correction of duplicate domain.

4.5 Performance

Brum has three main modes (some additional modes are listed in the repository [18]). The performance of these modes is listed below. Every mode is run 5 consecutive times, the average will represent the speed of that particular mode. The tests run with the system specification presented in table 2. The time is measured with the *time* module in Python. Results are rounded to the closest integer value.

Processor	i5-4670K
Memory	8 GB
OS	Ubuntu 18.04 LTS
Internet speed	1gbit/s

Table 2: System specifications

Each mode below is measured in 'IP/s'. This is the amount of IP addresses in the input file which can be checked per second.

- **Lookup mode**
This mode is used to go through a list of rows as described in section 4.3. Every row will be looked up in the RIPE RIS database [17]. The RIPE database allows 8 concurrent connections for lookups. By default is put at 7 concurrent connections. Brum will save the existing input file with the added fields: *prefix, ASN and valid_roa.* Results of the tests are presented in table 3.

Run	1	2	3	4	5	
Result (IP/s)	5,5	5.5	5.5	6.25	4.5	5.5 (average)

Table 3: Lookup performance

- **Report mode** This mode takes a file created by the *lookup mode* and will analyse the file and generate a report as output. Usually, this only takes some seconds (<200.000 lines). Going over 1 million lines can take up to 30 seconds to minute (depending on hardware speed). Results of the tests are presented in table 4. This mode also requires a country parameter as input. This parameter will look for this country code in the file and provides results similar to table 6. For a more in depth guide on how to use this country argument see the repository [18].

Run	1	2	3	4	5	
Result (IP/s)	20000	20535	19491	15862	20000	19008 (average)

Table 4: report performance

- **Domainreport mode** This function is used to cross reference an actual domain domain and see if its DNS servers are RPKI protected. Results of the tests are presented in table 5.

Run	1	2	3	4	5	
Result (IP/s)	131	119	104	128	113	118.5 (average)

Table 5: Domainreport performance

4.6 Ziggy

At first Ziggy seemed to be the best option to lookup if a DNS server belonged to a ROA protected prefix. However, the program in combination with Ziggy was slow (in the order of weeks for the .nl zone file). Instead,RIPE is used for testing. RIPE is much faster (around 2 hours for the the shortened .nl zone file, only containing the DNS servers). RIPE is working on an improved version of checking the RPKI deployment of a prefix. This function is however in beta at the moment of writing [21], but could provide more information on RPKI deployment in the future.

5. RESULTS

This section will focus on answering the questions asked in section 1. First several sub-questions will be answered to get a solid foundation to answer the main question of this paper: *How vulnerable are DNS name servers during a BGP hijack?*

5.1 DNS servers in ROA protected networks

Every zone (as described in section 4.3) with its number of valid ROA's in percentages is presented in table 4. For a ROA to be valid only the indication *valid* in the RIPE database is accepted, both invalid and unknown (or an error) will count as invalid. The first row shows the amount of valid ROA's of the total number of DNS servers. This value is then subdivided in an IPv4 and a IPv6 row. The last row shows the number of errors (during the lookup) that were encountered. These errors are discussed in section 5.1.3.

5.1.1 Root zone, hints and public resolvers

Beside the 11 TLD's, 3 special cases are included in figure 4. Taking a look at the public resolvers, about 50% is protected. Compared to the TLD's this result is significantly higher. Both the root zone and the root hints are less protected compared to the other input files (rootzone will be further analysed in section 5.7).

Especially the root hints score badly, even though this file only contains 13 domains (26 IP addresses, one IPv4 and one IPv6 per domain, each domain has a unique letter). Only K.ROOT-SERVERS.NET has both the IPv4 and IPv6 address inside a protected prefix, both M.ROOT-SERVERS.NET and I.ROOT-SERVERS.NET have their IPv6 address in a protected prefix. In any other case the DNS server was *not* in a ROA protected prefix.

5.1.2 Overall RPKI deployment

This section aims to give an overview by combining all measurements from the 2nd level TLD's data (see table 4).

As depicted in table 6 on average just below half of the DNS-servers are located in a protected prefix. Interestingly, enough Namibia has the highest value with the .na extension. This will be further discussed in section 5.2.

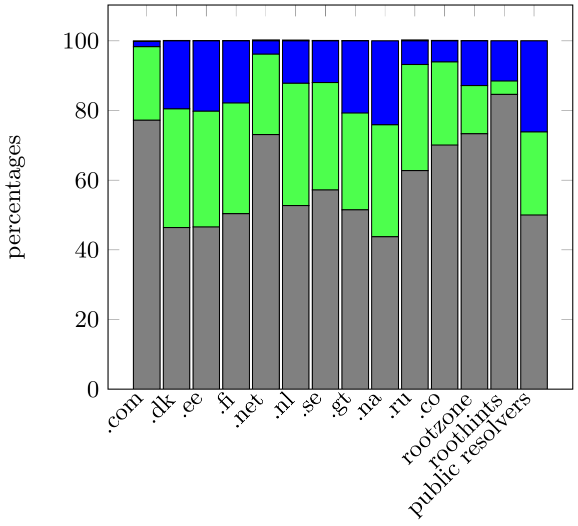

Figure 4. 2nd level DNS servers in valid ROA prefixes per TLD (Grey=Unprotected,Green=IPv4 ROA protected and Blue=IPv6 ROA protected)

TLD's (average)	45,00%

Table 6: TLD's average for 2nd level DNS servers

However, there are some differences between IPv4 and IPv6 deployments (demonstrated in figure 7).

	IPv4	IPv6
TLD's (average)	71,85%	28,15%

Table 7: Difference TLD's on IPv4 and IPv6 (2nd level DNS servers)

5.1.3 *Errors during lookup*

During the lookup for figure 4 several errors occurred. In most cases RIPE is simply unaware of the existence of this IP address. Possibly, the IP address has simply never been used before or the IP address has just been assigned and has not been picked up by a router yet.

Looking at the errors, points at another reason why RIPE is not able to verify the ROA for some of the prefixes. Some of the IP addresses are in a private IP range (e.g. 192.168.0.80, 192.168.0.7 or 192.168.0.6) or uses a loopback address:
127.0.0.1 or ::1. Figure 5 shows an overview of of the errors during the lookup. Red are errors where (in most cases) RIPE is unaware of the existence of the IP address. The green part are IPv4 loopback addresses and the blue part are IPv6 loopback addresses (both resulting in an error).

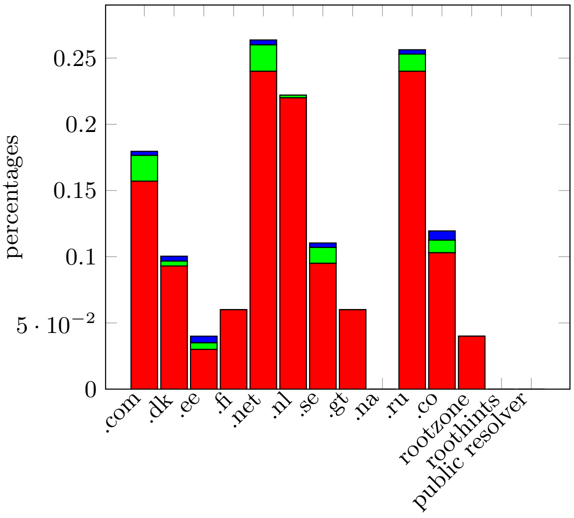

Figure 5. Errors during ROA validity check for 2nd level DNS server (red=non loopback errors, green= IPv4 loopback errors and blue= IPv6 loopback errors)

5.2 ROA protected network differences between countries

The input files (of each TLD) also provided a *country* argument, which provides the opportunity to see the difference in deployment per country (see figure 6). The country code used in the zone files comply with the 2 letter country code (for a list of country codes, see [22]). In each set of bars, on the left is the country bar dividing which part of the DNS-servers is inside the country and which part is outside the country (light blue=inside, light red= outside). The right one is the division of ROA protected DNS-servers within a country (red=unprotected,green=IPv4 protected and blue= IPv6 protected). Below each set of bars is the country code followed by the TLD. Both .com and .net are owned by VeriSign [23] and thus will be set to the US. 2nd level domains of the .com and .net TLD are widely used, but for simplicity and the fact that it is owned by VeriSign the US country code will be used.

Considering the first question one could state that the .na zone has a pretty good score (having the highest value among all of them in the second row). Having a closer look at figure 6 shows the opposite result. Just over 1.04% of the DNS-servers are actually managed within country boundaries. *None* of these servers are ROA protected. Within this table The Netherlands seems to have the best result. Whereas .co (Colombia) has a higher amount of protected prefixes it only has 0.68% of DNS-servers within country boundaries. Although, The Netherlands has 43,53% within the country with 50,65% protected prefixes. Also, in this table the number of protected IPv4 prefixes is much higher than the IPv6 prefixes (table 8). This table does not contain any error information as there are no errors. All errors as stated in table 4 are discarded. All remaining rows will have sufficient and correct information to contribute to the final result.

	IPv4	IPv6
TLD's (average)	80.98%	9.93%

Table 8: Difference TLD's on IPv4 and IPv6 per country (looking at 2nd level DNS servers)

5.3 Protected domains

At this point, it is clear which DNS-servers are inside a

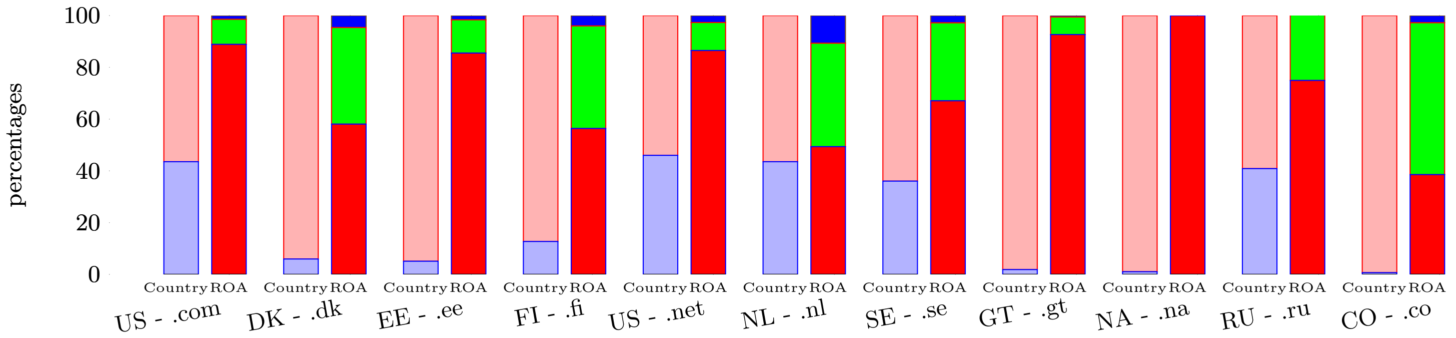

Figure 6. 2nd level DNS servers in a valid ROA prefix per country (left bar, light blue=inside country and light red=outside country, right bar, red=unprotected, green=IPv4 protected and blue=IPv6 protected)

TLD	.com	.dk	.ee	.fi	.net	.nl	.se	.gt	.na	.ru	.co
Protected	109.206.160.0/19 (7320) 2400:cb00:2049::/48 (5351) 95.216.0.0/16 (4516)	2400:cb00:2049::/48 (436) 2606:4700:50::/44 (420) 205.251.193.0/24 (267)	2606:4700:50::/44 (449) 217.160.80.0/22 (331) 2001:8d8:fe::/47 (328)	2606:4700:50::/44 (460) 2400:cb00:2049::/48 (435) 205.251.194.0/24 (273)	2a01:4f8::/29 (2722) 2400:cb00:2049::/48 (1836) 78.46.0.0/15 (1685)	37.97.128.0/17 (2536) 149.210.128.0/17 (1972) 2a01:7c8::/32 (1803)	5.133.192.0/19 (1208) 178.73.192.0/18 (778) 2606:4700:50::/44 (715)	2606:4700:50::/44 (315) 205.251.196.0/24 (170) 2600:9000:5304::/48 (169)	217.160.80.0/22 (303) 2606:4700:50::/44 (145) 173.245.59.0/24 (73)	18.194.0.0/15 (1315) 136.244.96.0/20 (1303) 2a01:4f8::/29 (970)	2606:4700:50::/44 (879) 162.159.32.0/20 (486) 217.160.80.0/22 (485)
Unprotected	162.251.82.0/24 (241279) 2001:67c:38c::/48 (88810) 218.144.0.0/13 (35110)	2604:3400:aaac::/48 (220) 2001:41d0::/32 (133) 74.208.0.0/16 (86)	162.251.82.0/24 (176) 2001:41d0::/32 (114) 217.146.64.0/20 (91)	109.69.32.0/22 (275) 2604:3400:aaac::/48 (248) 54.37.0.0/16 (182)	162.251.82.0/24 (73418) 195.149.84.0/24 (9638) 192.185.128.0/18 (4732)	212.83.192.0/18 (1218) 162.251.82.0/24 (1088) 83.172.128.0/18 (1041)	185.87.164.0/22 (2029) 192.71.125.0/24 (835) 192.36.232.0/24 (384)	192.185.0.0/18 (157) 50.87.0.0/16 (104) 192.185.64.0/18 (96)	82.223.0.0/16 (61) 2001:41d0::/32 (50) 41.185.0.0/16 (41)	162.251.82.0/24 (2465) 193.232.76.0/24 (1639) 148.251.0.0/16 (624)	162.251.82.0/24 (14523) 192.185.128.0/18 (1294) 192.185.0.0/18 (1051)

Table 9: Big impact prefixes

protected prefix, the next question is: ”Which DNS server is responsible for which domain?”. Some DNS servers could be responsible for a large portion of the domains. This function is called the *domainreport* in Brum. It will take a zone file which is already checked and takes an input file with domain names and checks within the reference file whether or not it belongs to a protected DNS server. This test has been done for the .nl domain (the results of this test is in table 11). A domain can be configured from one to multiple DNS servers. If all the configured DNS servers lay within a ROA protected prefix than this domain is *protected*. If some are protected and some are not then the domain is *Partially protected*. If all the configured DNS servers are not within a protected prefix than the domain is *unprotected*. An error will be raised if the configured DNS server for a domain is not present in the reference file.

Protected domains	41,48%
Partially protected domains	28.84%
Unprotected domains	29,54%
Errors	0,15%

Table 11: Cross reference from domains to protected DNS-servers (.nl zone file)

An interesting observation is that almost 29% of all the domains are partially protected. This indicates that while configuring the DNS servers for these domains, checking if a DNS server is within a protected prefix was not a conscious decision (since there is a mix of protected and unprotected DNS servers configured).

5.4 "Big impact" prefixes

As stated previously, multiple DNS servers could be located inside of the same prefix. Thus signing some of these prefixes could have a rather large impact. Table 9 shows an overview of these *big impact* prefixes. One of the biggest hitters is for the .com zone file. Signing only the top three unprotected prefixes will put in total 365199 DNS servers inside of a protected prefix. Signing these prefixes would give an improvement of 15.52% for the .com TLD. The AS values, country, company and prefix of these three prefixes is summed up in table 12. .co (Colombia) would set 14523 DNS name servers in a protected prefix by signing only **one** prefix! This would give an improvement of 11.92% in the .co TLD. This prefix belongs to AS 13335 (belonging to Cloudflare).

5.4.1 Prefix analysis

Since the biggest impact prefixes are established, some of the prefixes (.com and .nl) will be looked at a little closer (see table 12 and 13). Of immediate notice is the fact that not necessarily all companies responsible for the top prefixes are in the same country (or even in the country of the zone file). Contacting these companies could complicate the process to increase the number of protected prefixes for a zone file.

Number	1	2	3
Prefix	162.251.82.0/24	2001:67c:38c::/48	218.144.0.0/13
ASN	AS13335	AS43081	AS4766
Company Name (ASN)	Cloudflare	World News PTE	KT
Company Name (prefix)	PDR	World News PTE	KT
Country	USA	Netherlands	South Korea

Table 12: Prefix analysis (.com, largest unprotected prefixes)

Number	1	2	3
Prefix	212.83.192.0/18	162.251.82.0/24	83.172.128.0/18
ASN	AS9150	AS13335	AS25459
Company Name(ASN)	ML Consultancy	Cloudflare	NedZone Internet BV
Company Name(prefix)	IML Consultancy	PDR	ISE
Country	Netherlands	USA	Netherlands

Table 13: Prefix analysis (.nl, largest unprotected prefixes)

5.5 ASN analysis

Motivating an owner of an AS could also have a big impact on the RPKI deployment overall. Table 10 shows a list of *protected* and *unprotected* AS values and the number of DNS servers between brackets (for that specific AS). Figure 7 gives an overview of how many ASN are protected. *Protected* means that all prefixes inside this AS are protected, *unprotected* means that no prefix inside this AS is protected and *partially protected* means that only some prefixes inside the AS are protected. Table 14 gives an overview of the biggest AS in the .nl TLD (protected). Herein, 1 is the largest and 3 is the smallest. For the unprotected AS values for the .nl TLD see table 15.

TLD	.com	.dk	.ee	.fi	.net	.nl	.se	.gt	.na	.ru	.co
Protected	14618 (19725) 9762 (8972) 9370 (8910)	203391 (207) 15456 (182) 20773 (166)	203391 (204) 55002 (192) 6724 (101)	203391 (424) 197595 (175) 790 (124)	14618 (8077) 203391 (4365) 8972 (2941)	6724 (1368) 203391 (502) 8315 (473)	203391 (282) 15456 (241) 50986 (230)	203391 (54) 44273 (51) 14618 (40)	26496 (126) 6724 (92) 44273 (44)	14618 (1656) 49531 (1428) 203391 (586)	14618 (780) 203391 (569) 20773 (202)
Unprotected	43081 (177620) 46606(96731) 4766 (40599)	33517 (352) 14061 (335) 397213 (334)	33517 (487) 46606 (354) 3249 (318)	46606 (590) 16552 (436) 33517 (432)	46606 (31250) 43081 (19276) 16552 (10532)	14061 (3163) 46606 (1668) 31477 (1393)	46606 (1020) 33517 (869) 14061 (683)	46606 (923) 33517 (186) 397213 (177)	397213 (123) 33517 (95) 46606 (84)	197695 (1753) 15835 (1667) 46606 (1456)	46606 (9615) 14061 (1906) 16552 (1784)

Table 10: Big impact ASN (AS followed by number of DNS servers in that AS between brackets)

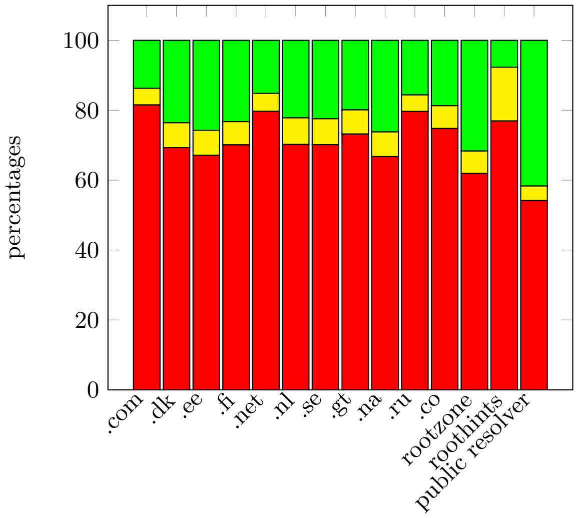

Figure 7. Protected prefixes inside an AS (red=no prefix is protected, yellow=some prefixes are protected and green=all prefixes are protected inside the AS)

Number	1	2	3
ASN	AS6724	AS203391	AS8315
Company Name	Strato	Cloud DNS Ltd	Sentia
Country	Germany	Bulgaria	Netherlands
DNS servers	1368	502	473

Table 14: AS analysis for .nl (protected)

Number	1	2	3
ASN	AS14061	AS46606	AS31477
Company Name	DigitalOcean	Unified Layer	Duocast B.V.
Country	US	US	Netherlands
DNS servers	3163	1668	1393

Table 15: AS analysis for .nl (unprotected)

5.6 DNS name server Analysis

In the dataset for each TLD, multiple DNS servers can be behind the same ns_address (or DNS name server address). In this case an IPv4 address behind a name server could be protected, but the IPv6 is not. Figure 8 gives an overview of this situation. *protected* means that all DNS servers behind the same name server address are inside of a ROA protected prefix. *Partially protected* means that only some of the DNS servers behind the same name server address are inside of a ROA protected prefix and *unprotected* means that none of the DNS servers reside inside of a protected prefix.

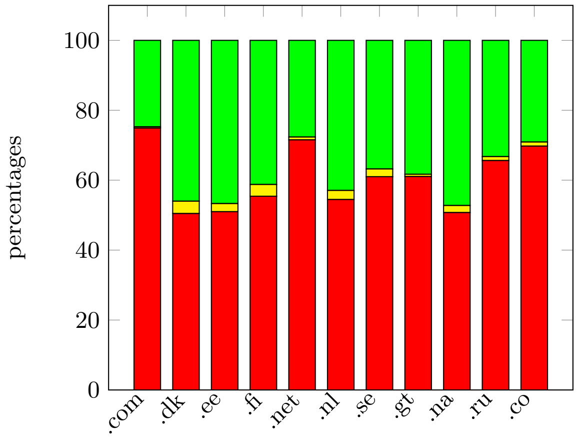

Figure 8. ROA protected 2nd level DNS name servers per TLD (red=unprotected, yellow=partially protected and green=protected)

5.7 Rootzone analysis

The rootzone can be further analysed. Root zone DNS servers can have different *types* such as: generic, country-code, sponsored, infrastructure or generic-restricted (as used by IANA [24]). Figure 9 gives the division of these types in the rootzone. Figure 10 gives an overview how many DNS servers reside in a protected prefix per type (in the root zone). Figure 11 gives an overview of the protected DNS servers for certain TLD. Interestingly, the amount of IPv4 and IPv6 protected DNS servers is in most cases equal. A possible reason could be that in most cases, a DNS server has both a IPv4 and a IPv6 address. In that case the DNS server would be in the same prefix in both cases (though, more research is required to confirm this hypothesis).

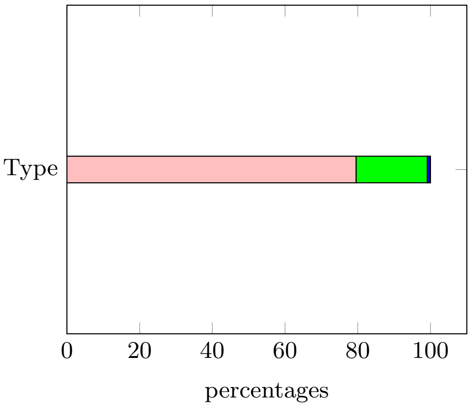

Figure 9. Rootzone type division (pink=generic, green=country-code, blue=sponsored, yellow= generic-restricted and red=error). Generic-restricted is 0.12%. 0.21% of the rootzone resulted in an error.

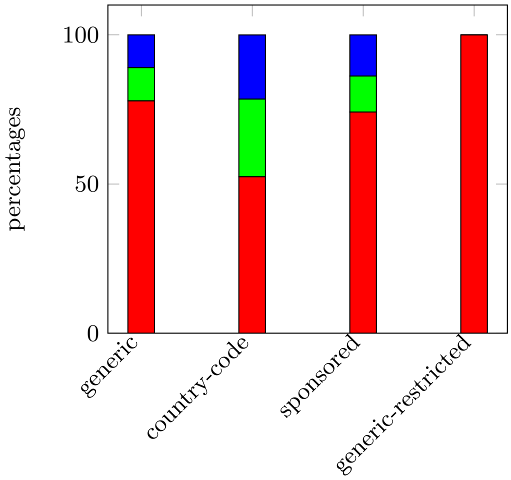

Figure 10. Protected DNS servers per TLD type (red=unprotected,green=IPv4 protected and blue=IPv6 protected)

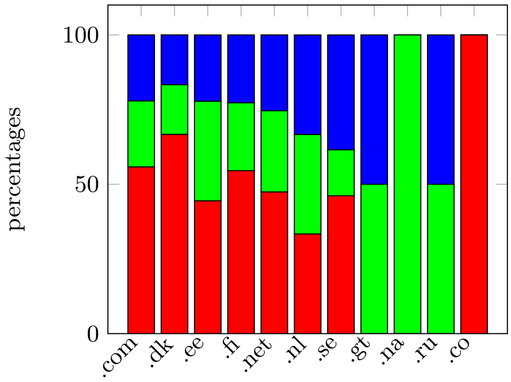

Figure 11. Protected DNS servers per TLD (red=unprotected,green=IPv4 protected and blue=IPv6 protected). On average 40.76% is protected.

6. DISCUSSION

6.1 Conclusion

How vulnerable are DNS name servers during a BGP hijack?

The main result of this research is that (considering table 6) 45% of the DNS servers reside in a protected prefix. Overall IPv4 (71,85%) seems to perform better than IPv6 (28,15%). Even though RPKI has not used that long, there is still a reasonable amount of prefixes that are protected. Contacting some of the companies behind the *big impact* prefixes or *big impact* ASN could quickly increase the amount of protected prefixes. The fact that companies behind a prefix are located in potentially any country could make this process more difficult.

Looking at the root zone, there are considerable differences between TLD's. Some (.co) are completely unprotected and some are completely protected (.gt, .na and .ru). Overall 40.76% of the DNS servers reside inside of a protected prefix. This is slightly lower than the 2nd level DNS servers.

6.2 Future work

Currently 11 TLD's are studied, including more TLD's would give a better overview on the current state of RPKI deployment. The paper focused on RPKI deployment. Analyzing how companies are filtering or checking for a ROA certificate would enhance understanding the usage of RPKI. Are there differences? Is it done correctly and/or effective?

6.3 Recommendations

A short list of recommendations (no hierarchical order) which have the biggest impact on deployment of RPKI is presented below:

- **Include in decision** Table 11 gives a feeling on RPKI when selecting a DNS server for a domain. 28,84% has a mixed set of DNS servers in a protected and unprotected prefixes. Making this part of the decision for operators would contribute to an increase of the amount of protected prefixes. This can be achieved by advertising directly to operators, for example by a congress in The Netherlands [25]. This event is meant for Dutch network operators. These are the professionals who can implement a ROA certificate when needed.

- **Focus on rootzone** The rootzone scores below the average for the 2nd level DNS servers on protection. Since these DNS servers are higher in the DNS 'chain', they should be of a higher priority.

- **Big impact prefixes** This could probably have the biggest impact on existing prefixes. Table 9 is constructed specifically for this goal. It gives a complete overview of prefixes that have the biggest impact. A large amount of DNS-servers *indeed* reside in similar prefixes. Directly contacting the operators of these prefixes would be worthwhile since the impact would be significant. Brum is equipped to automatically generate a top 5 for a zone file. Brum is able to assist in creating suggestions on which prefixes to fix first for a particular zone.

- **Big impact AS** Contacting the owner of a AS with a large amount of DNS servers inside can be beneficial too (similar to the prefixes). Only one company (the owner of the AS) needs to be contacted.

- **MANRS** MANRS stands for *Mutually Agreed Norms for Routing Security* and provides a worldwide norm on what secure routing should look like. Currently RPKI is included in the norms, but very loosely. MANRS [26] puts both IRR and RPKI on the same level of security norm. In this document RPKI should be put forward more and should be given as the main and most secure option to use.

7. REFERENCES

[1] Logan Rivenes, "The History of Border Gateway Protocol," 12 2016. https://datapath.io/resources/blog/the-history-of-border-gateway-protocol/.

[2] M. J. Levy, "RPKI - The required cryptographic upgrade to BGP routing," 9 2018. https://blog.cloudflare.com/rpki/.

[3] RIPE, "RIPE API IP/domain lookup (including BGP information)." https://stat.ripe.net/8.8.8.8tabId=at-a-glance.

[4] Cloudflare, "Bgp hijacking explanation." https://www.cloudflare.com/img/learning/security /glossary/bgp-hijacking/bgp-hijacking-technical-flow.png.

[5] D. B. Terry, M. Painter, D. W. Riggle, and S. Zhou, "The berkeley internet name domain server," Tech. Rep. UCB/CSD-84-182, EECS Department, University of California, Berkeley, May 1984. http://www2.eecs.berkeley.edu/Pubs/TechRpts /1984/5957.html.

[6] K. Beaumont, "Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed." https://doublepulsar.com/hijack-of-amazons-internet-domain-service-used-to-reroute-web-traffic-for-two-hours-unnoticed-3a6f0dda6a6f.

[7] V. Manojlovic, "Join the amsterdam RPKI Deployathon 2019)." https://labs.ripe.net/Members/becha/join-the-amsterdam-rpki-deployathon-2019.

[8] I. Arghire, "China telecom routes european traffic to its network for two hours," 2019. https://www.securityweek.com/china-telecom-routes-european-traffic-its-network-two-hours.

[9] BGP Looking Glass, "BGP Looking Glass Database." http://www.bgplookingglass.com/.

[10] Noction, "Number of bgp hijacks," 2018. https://www.noction.com/wp-content/uploads/2017/06/BGP-Hijacking-incidents.png.

[11] T. Chung, B. Chandrasekaran, B. M. Maggs, E. Aben, D. Choffnes, A. Mislove, T. Bruijnzeels, D. Levin, R. Van Rijswijk-Deij, J. Rula, and N. Sullivan, "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 406–419, 2019. www.scopus.com.

[12] P. Foremski, O. Gasser, and G. C. M. Moura, "Dns observatory: The big picture of the dns," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 87–100, 2019. www.scopus.com.

[13] T. Chung, D. Levin, R. Van Rijswijk-Deij, B. M. Maggs, C. Wilson, D. Choffnes, and A. Mislove, "Understanding the role of registrars in dnssec deployment," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, vol. Part F131937, pp. 369–383, 2017. Cited By :4.

[14] M. Wählisch, R. Schmidt, T. C. Schmidt, O. Maennel, S. Uhlig, and G. Tyson, "Ripki: The tragic story of rpki deployment in the web ecosystem," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks, HotNets-XIV 2015*, 2015. Cited By :15.

[15] OpenIntel, "Zone list of all .nl domains." https://openintel.nl/.

[16] Wikipedia, "Public recursive name server." https://en.wikipedia.org/wiki/Public$_{r}ecursive_{n}ame_{s}erver$.

[17] RIPE, "The ripe ris database lookup tool." https://stat.ripe.net/.

[18] R. Linssen, "Brum." https://github.com/roeltje788/brum.

[19] IANA, "Root files." https://www.iana.org/domains/root/files.

[20] Wikipedia, "Dns resolvers list." https://en.wikipedia.org/wiki/Public_recursive_name_server.

[21] RIPE, "Rpki deployment tool v3 (beta)." https://ftp.ripe.net/tools/rpki/validator3/rc/generic/.

[22] CountryCode.org, "Country codes." https://countrycode.org/.

[23] IANA, "Root zone database." https://www.iana.org/domains/root/db.

[24] IANA, "Root zone database."

[25] NLNOG, "Nlnog day 2018." https://nlnog.net/nlnog-day-2018/.

[26] MANRS, "Manrs ixp programme." https://www.manrs.org/ixps/.