BGP ANOMALIES IDENTIFICATION AND ANALYSIS

Eurecom Semester Project

Vahur Varris, Shubham Rai & Ander De Miguel Aramburu

Appendix

Introduction

Border Gateway Protocol (BGP) is an application layer protocol designed for communication between autonomous systems (AS) to exchange information about routes and paths. As with many other protocols in the network stack, BGP is not designed with security in mind, therefore it remains vulnerable to many different attacks and anomalies such as prefix hijacks.

The goal of this semester project is to learn how high-level routing in the internet works and perform the data analysis on the publicly available BGP data of duration of 6 months, to identify possible anomalies that occur in the routing. In order to do that it is needed to first build the database from RIPE RIR datasets and parse into the format that is usable for the analysis. During the analysis there are few potentially suspicious cases presented.

Engineering setup

In order to start analysing the data, it is first needed to build the database. During the project we analysed the data between 1st of May and 31st of October. The RIPE RIS dumps the BGP updates every 5 minutes and the full BGP dumps 3 times a day [1]. So In the given period we would collect the data from around 3*30*6 = 540 dumps.

BGP packets have many different attributes [2]. For our analysis the most important are *prefix, as_path* and *time* as we only care about the announcements of prefixes.

As a database engine, we chose Postgres due to its support for *cidr* data types and rich selection of functions to manipulate with these types [3]. We also decided to run it in a containerized environment using Docker for flexibility and fast setup.

RIPE RIS stores the dumps in binary MRT format which can be parsed by a tool called libbgpdump [4][5]. Initial approach was to run the libbgpdump on the dumps to convert them into text files, and then run java application on them that reads the file, removes unneeded attributes, keep only the *time, as_path,* and *cidr,* and performs

the batch insert to the database and then on the database side we would use SQL queries to group the timestamps by cidr and as_path. The schema of the table is presented below.

When we tried out implementing the approach, we ran into serious performance issues. First, the libbgpdump took around 10 minutes per dump to convert MRT to text based representation, and also it had quite a big expansion ratio. The MRT dumps had size between 1.8-2.2GB, while the converted text file had it 2-3 fold. We realized that our machines with small SSDs are not capable of handling this kind of volume of data, so we moved the project to Google Cloud Compute Engine.

Another issue we faced was that the Java parser was not fast enough - it took around 22 minutes to parse and insert a single dump worth of data, so it would mean it takes more than a week to just insert all the data. We also realized that grouping the timestamps in the database side is not feasible as it was quite slow with only a few dumps, and since the operation scales linearly, it would only get slower as we would add more data.

To solve the aforementioned problem, we came up with a workaround: instead of inserting the data with Java JDBC connection, we used Postgres copy command [6]. To get the data into the suitable format for inserts, instead of running the libbgpdump

to convert the dump to text file, we took approach where the Java program would fork the libbgpdump, and then parses the output (removes IPV6 and unnecessary attributes) on the go and only then writes the output to csv. With this approach it took only around 5 minutes per dump, and the output csv is smaller in size than input MRT binary. The Postgres *copy* function also took only around a few minutes to load the dump into the database.

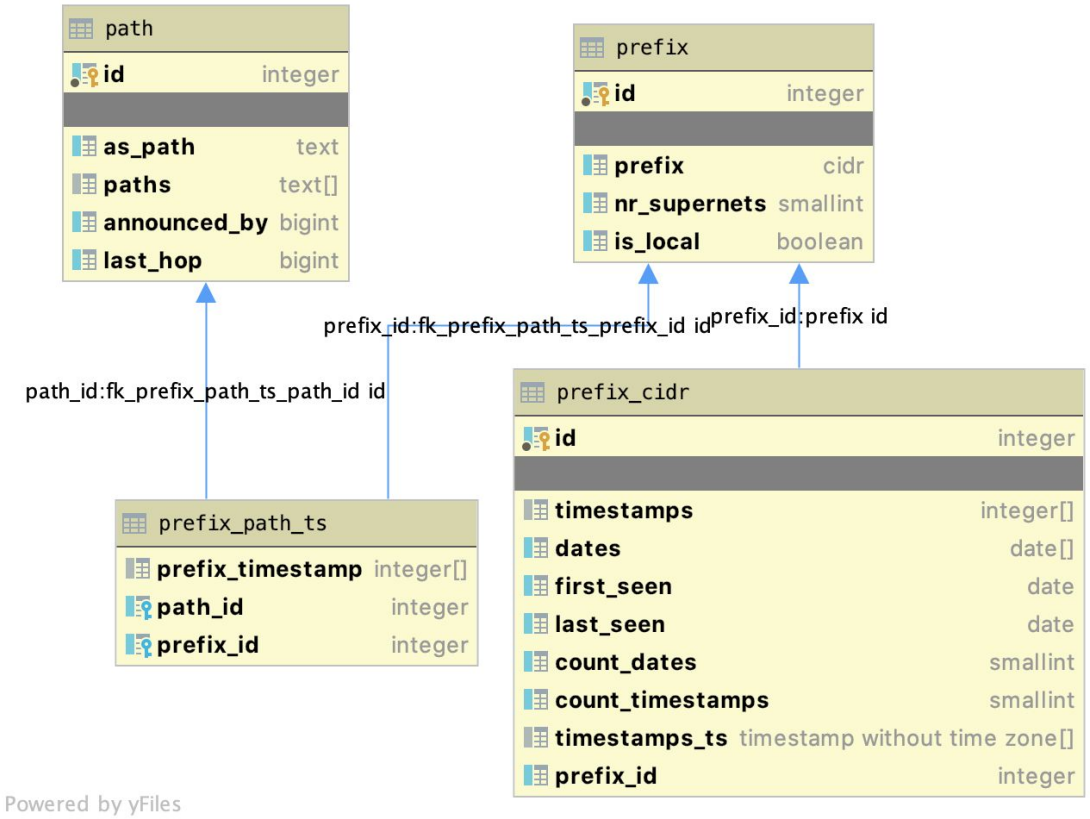
We still had the issue of grouping the timestamps by prefix and as_path took too much time. We tried 3 different strategies:

- Load all data and run the grouping then - means that we would have to aggregate on 21,5 billions rows
- Group after each dump - after each dump so after 40 million rows
- Group on each entry during parsing

All of these approaches were too slow and would have taken too long to complete. So we came up with another 2 alternatives: First of them would include some kind of cluster computation setup with apache Spark or Flink to parse all the files and group the timestamps by prefix and as_path and then load into the database, and the second approach would be taking the same approach, but instead of vertical scaling, do horizontal scaling.

We took the 2nd approach, as setting up the cluster would have been quite complex, and would have taken more time. So we created a python script that parses all the dumps and performs the grouping operation in-memory and writes the output as csv file. We used the machine with 400GB of memory and it took a few hours to complete. After that we could load the resulting csv to the database using the Postgres copy command. To accommodate the resulting data, we used the table described below.

We dumped the resulting csv to the table above. We split the data into different tables and precomputed some attributes as new columns to make it easier to query on these parameters. Full schema is presented in a table below.

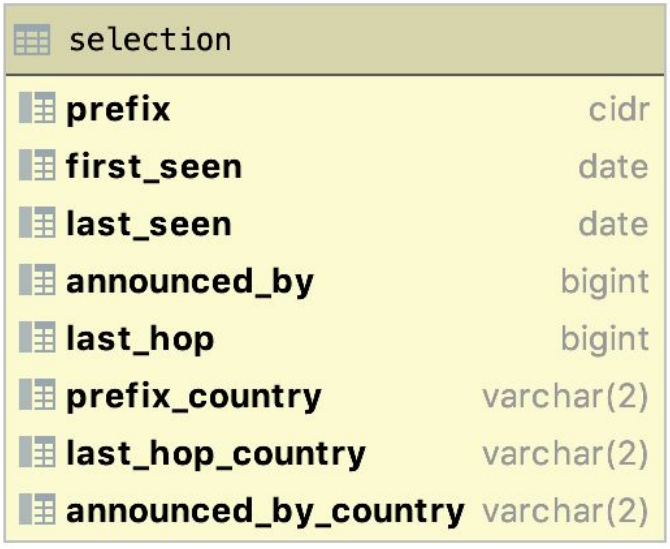


Selection criteria

The criteria for selecting interesting cases was following:

1. Prefixes that are announced for at most 2 days
2. Remove local/bogons prefixes
3. Remove prefixes that are subnets of others

In order to analyse the data we created a new table from a query result that has the specified filters, we also added the countries of prefix, and the hops from RIPE Api. The resulting table is presented below.



Few Stats from the table that were part of the analysis performed:

- Total unique 391 ASNs
- Total unique 843 prefix cidr
- 199 unique cidr were announced by AS16509, Amazon and hence was not considered into evaluation

Initial plan was to analyse based on the count of unique cidrs each ASN announced (evaluate the ones that announce the most), however, there were too many false positives.

AS Case Studies

In this section we present a selection of ASNs that were studied with the hope to find unusual patterns in their routing behaviours that could match with BGP hijacking cases.

The following ASs have been chosen from the group of 391 unique ASs that were left in the table after the filtering process. First the ASNs with more than one distinct prefix announcement were manually analyzed. Then a subset of the remaining ASNs was randomly selected and also manually analyzed.

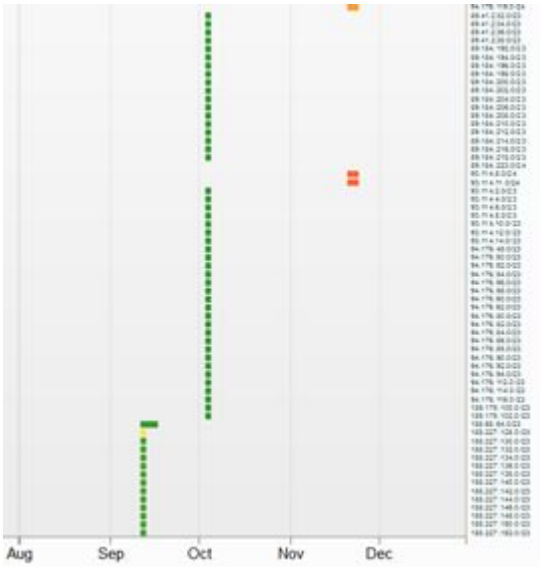
The 6 ASs which are explored below were selected due to their similarity in routing behaviour with the BGP Hijacking phenomena.

ASN: AS47582

aut-num	47582
as-name	ansonnet-as-uk
org	ORG-ANL20-RIPE
status	ASSIGNED
mnt-by	RIPE-NCC-END-MNT
mnt-by	uk-anl-1-mnt
source	RIPE

The ASN is owned by Anton Network Services Limited registered in Great Britain. From our query and stat.ripe.net, we observed that the ASN has been announcing prefixes from China.

We looked at the routing history for the ASN and found that it matched the expected behaviour we were looking for i.e. ASNs that announce only for a very short period as shown in figure below.



89.184.206.0/23

To further analyse, we randomly picked a few prefixes that were announced by this ASN. We looked at the routing history for 89.184.206.0/23 and observed that Anton Network this prefix block and also noticed that it owns the ASN “AS206819”.

aut-num	206819
as-name	anl-uk
descr	ANSON NETWORK LIMITED
org	ORG-ANL20-RIPE
status	ASSIGNED
mnt-by	RIPE-NCC-END-MNT
mnt-by	uk-anl-1-mnt
source	RIPE

188.227.130.0/23

We also looked at the routing history for 188.227.130.0/23 and found the same behaviour, AS47582 announced it and later it was announced by AS206819, both being owned by Anton Network.

To find reason for this behaviour we looked at the services provided by Anton Network and it provides DDOS mitigation services. We believe that Anton Network is providing BGP based DDOS mitigation services. BGP rerouting can mitigate DDoS

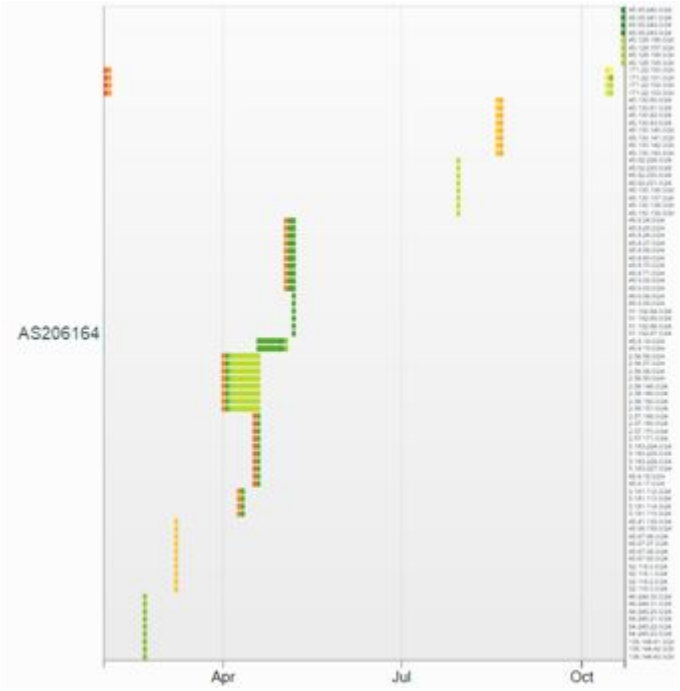
attacks by screening all incoming network traffic before it reaches its target. It basically functions at the network level by rerouting malicious network packets to security providers before they can reach DNS servers or other computing resources. So, it seems like AS47582 announces the bigger /23 block and then AS206819 takes over and announces it.

ASN: AS206164

aut-num	206164
as-name	ASREACHABLENET
org	ORG-RNL23-RIPE
status	ASSIGNED
mnt-by	RIPE-NCC-END-MNT
mnt-by	za-reachable-1-mnt
source	RIPE

The ASN is owned by Reachable Network (Pty) LTD Limited registered in Great Britain. We looked at the website of the company to figure out where the company is registered and noticed that they are registered in South Africa and are into IT Consulting and Infrastructure Management. They also act as a mediator between clients and all Regional Internet Registries such as AFRINIC, APNIC, RIPE etc.

We looked at their routing history and noticed that they were announcing multiple prefixes for very short duration and were not announcing any prefix continuously. Next, we randomly picked a few prefixes to investigate their owners and analyse the routing history as shown below.



171.22.101.0/24

We looked at prefix 171.22.101.0/24, announced by AS206164 in October, and found that it is owned/ announced by AS3257 (GTT-BACKBONE - GTT Communications Inc), seems like it started announcing a bigger block /22 compared to the earlier announced /24 block. IT was earlier being announced as /24 block by m247.com, a network and cloud company based in the UK.

45.95.241.0/24

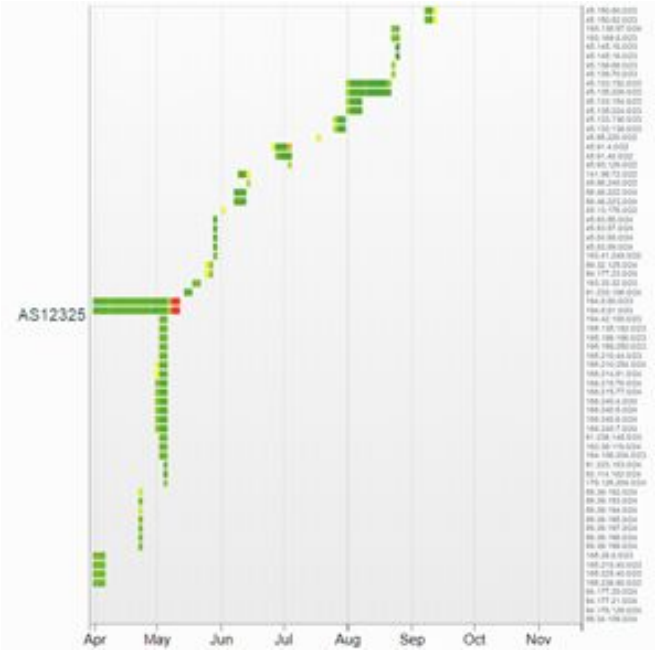
We looked at another prefix 45.95.241.0/24, and found that it is owned by Maxozo BV, Netherlands. We looked at the routing history and understood that it was earlier announced as /16 block by another ASN (AS6589). We couldn't obtain who owns the AS6589, but checked (http://www.bgplookingglass.com) and understood that it belongs to BTCPROD - Beneficial Technology. However, we were unable to make any connections or reasoning in this case.

This seems to be the case where the announcement was made earlier as part of some bigger block. We couldn't really co-relate all the scenarios to come up with a possible justification for the behaviour.

ASN: AS12325

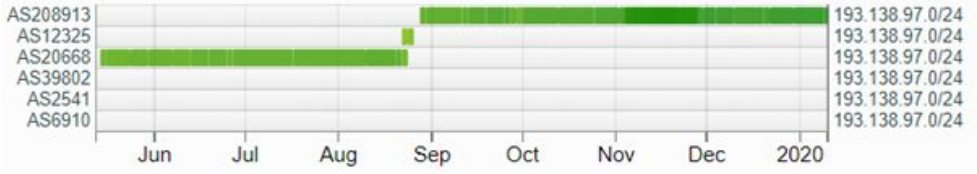
aut-num	12325
as-name	IPv4-AS
org	ORG-ATAS1-RIPE
status	ASSIGNED
mnt-by	RO-MNT
mnt-by	RIPE-NCC-END-MNT
source	RIPE

The ASN is owned by IPv4 Management SRL registered in Romania and provides domain registration and IP management services. To analyze the ASN, we looked at the routing history of the ASN, and it has the same behaviour as per our filters, wherein prefix was announced for a short duration as shown below.



193.138.97.0/24

We randomly selected a few prefixes to analyse the behaviour and figure out who owns it. We looked at “193.138.97.0/24” and see that AS12325 announces it and then AS208913, Mouk, LLC (Netherlands) starts announcing it. Before being announced by AS12325, it was announced by AS20668, AQUA JUMP SRL, which we found out belongs to IPv4 Management SRL only.



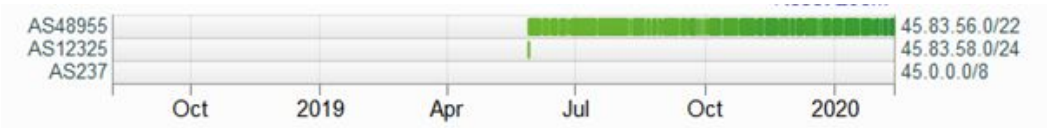

```
Domain Name: jump.ro
Registered On: 2003-12-01
Expires On: 2020-08-17
Registrar: IPv4 Management SRL
Referral URL: www.ip.ro

DNSSEC: Inactive

Nameserver: ns1.jump.ro
Nameserver: ns2.jump.ro
```

45.83.58.0/24

We picked one more prefix “45.83.58.0/24” and saw the same behaviour, where AS12325 announced it for a short time and then AS48955, which is also owned by IPv4 Management SRL, took it and started announcing it.

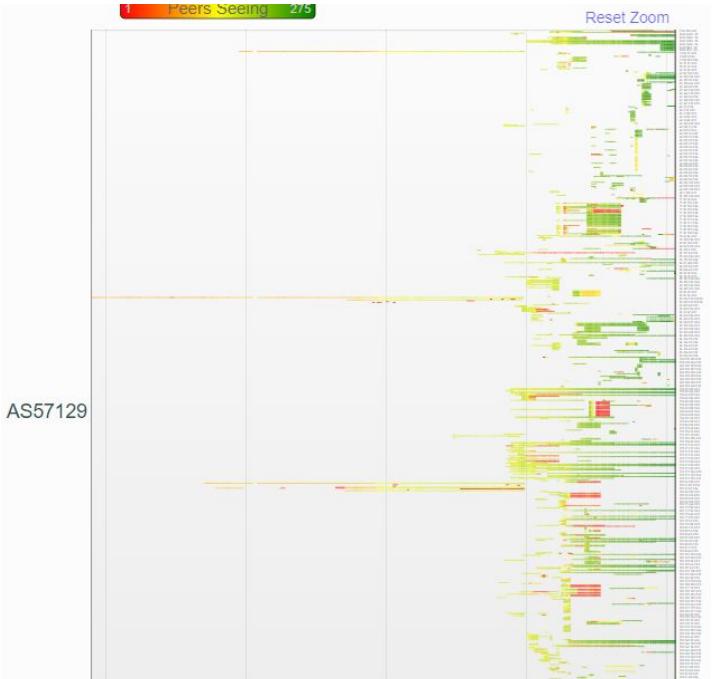


We note similar behaviour in other cases too, and according to our understanding it seems like IPv4 Management SRL starts announcing the blocks and then sells it to the customers which start announcing from that point onwards.

ASN: AS57129 - Optibit LLC

aut-num	*57129*
as-name	*RU-SERVERSGET-KRSK*
org	*ORG-OL159-RIPE*
status	*ASSIGNED*
mnt-by	*RIPE-NCC-END-MNT*
mnt-by	*ru-igra-service-1-mnt*
source	*RIPE*

This ASN corresponds to Optibit LLC, a russian cloud service provider. This AS is announcing prefixes from all over the world and checking the routing information, we can see that it has a really variable behaviour, it both announces some prefixes for a long time and some for a short time.



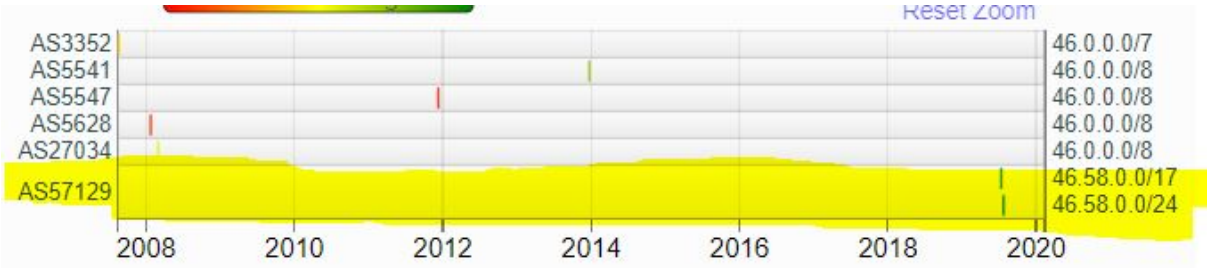
Just with a quick Google search, we discovered that the website https://scamalytics.com/ rates Optibit LLC as a high fraud risk ISP.

Going further in our research, we identified in our database 4 prefixes that were announced by this AS: 46.58.0.0/17, 124.242.0.0/16, 178.171.112.0/22 and 98.9.128.0/17.

46.58.0.0/17

This prefix is owned by a company called “Amcor Flexibles Finland OY” which is a subsidiary of the British company Amcor.

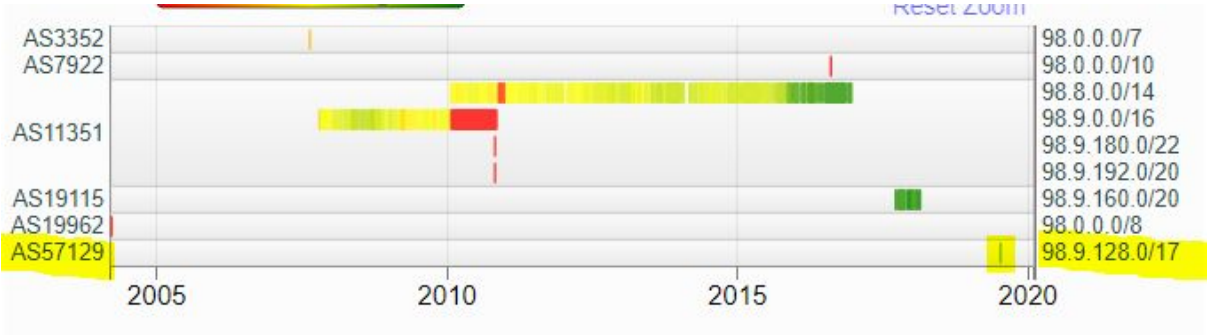
If we take a look at the routing history of this prefix, we can see that it has only been announced one day throughout history, precisely by this Russian AS.



98.9.128.0/17

This prefix is probably not allocated, because we haven’t found any information about the owner in any of the search engines.

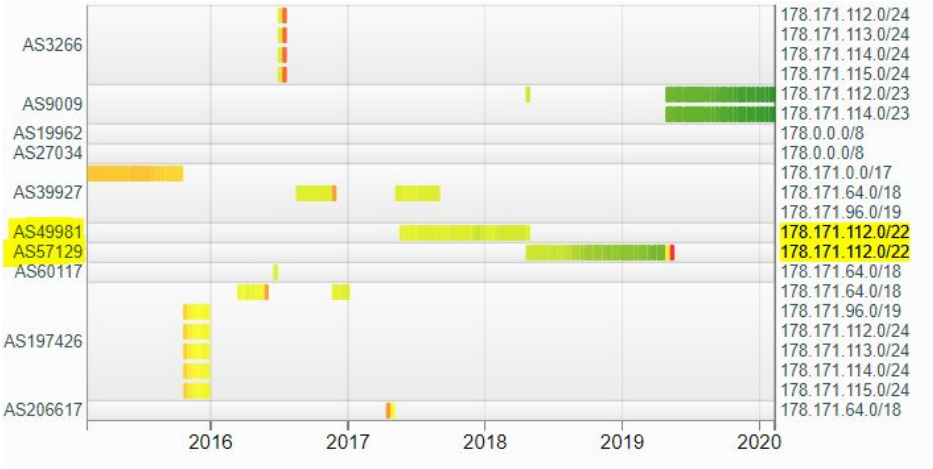
However, if we look at the routing history, we find the same pattern as with the first prefix, it is only announced one day and by the Russian AS.



178.171.112.0/22

The prefix is owned by a Russian Telecommunication Service provider.

In this case, if we check the routing history, we can see a totally different pattern, the prefix s announced by the Russan AS for a longer time. The reason why our database has detected this case is that they stopped announcing it the 1st of May 2019, which is the first day in our database records.



124.242.0.0/16

This prefix is owned by Hangzhou Netbank Technologies, which owns the AS55959, but this last AS does never announce the prefix we have studied.

In the routing history we can see the pattern of the first two prefixes, the prefix is permanently unannounced, until the Russian AS does it. However, this is a really interesting case, as the Russian AS is not the only one announcing it only for one day. Other two ASs, AS3689 and AS135091 also announced it for a really short period.

AS3689 is a non operative AS that has only announced 5 prefixes in all its history and only for a few days. It has been inactive since 2015.

AS135091 however, has a really interesting routing history, because it also has a pattern of announcing prefixes that doesn't own for short periods, therefore it will be individually studied later in the report.

Conclusions

AS57129 is a case that we have considered highly suspicious of BGP hijacking activities, as it is announcing for a really short period of time prefixes that were not previously announced, both with a known owner or probably even without being allocated.

However, we have seen in the routing history and with the prefix 178.171.112.0/22 that it also announces prefixes for a longer period of time. Therefore one hypothesis is that it may be covering this malicious activity under legit announcing behaviour.

ASN: AS135091 - Possibly Lizards

aut-num	135091
as-name	POSSIBLY-LIZARDS-AS-AP
descr	Possibly Lizards
country	SG
org	ORG-VL5-AP
mnt-by	APNIC-HM
source	APNIC

This ASN corresponds to “Possibly Lizards” and although it has not been detected by our database, because it became inactive in the beginning of 2018, we have decided to analyze it, as it announced the prefix 124.242.0.0/16, which is a normally unannounced prefix which was also announced only for one day, by our previous interesting case (Russian AS57129).

After a quick search we discovered that “Possibly Lizards” is a company registered in the United Kingdom, although ripe and other sources give as country Singapore. They also own a website https://possiblylizards.com which only has a landing page. Unfortunately, we were not able to discover the actual business of this company.

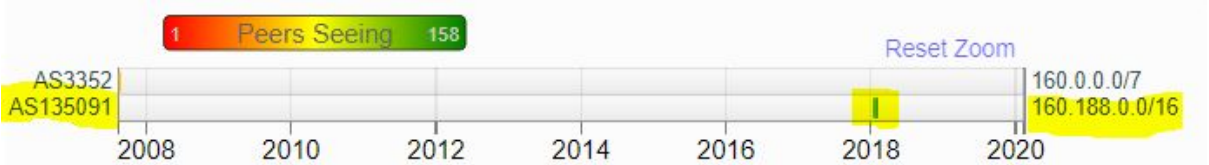
The routing history of this AS has a really interesting pattern, as it announces really different prefixes that belong to different companies, for a moderately short period of time.

In order to research deeper the behaviour of this AS we randomly chose 4 prefixes that were announced by it.

160.188.0.0/16

This prefix is owned by a Japanese machine tool manufacturer, Okuma Corporation.

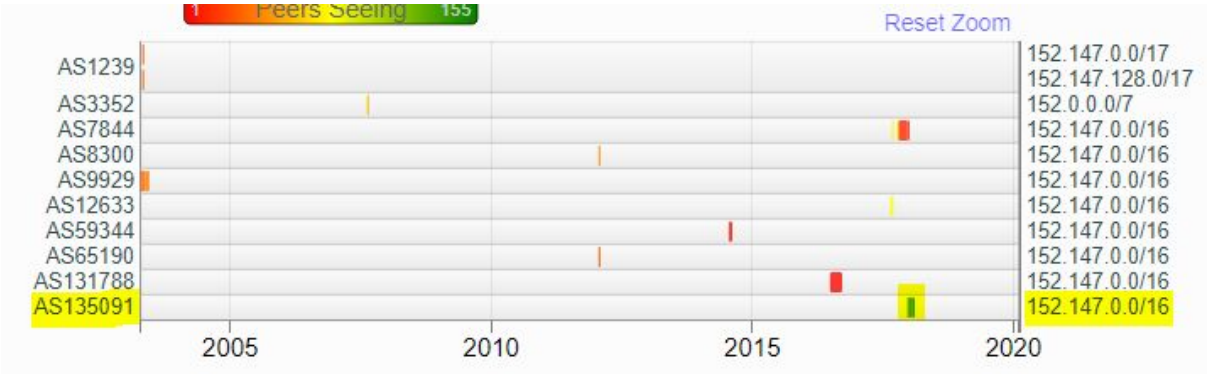
The routing history shows that it has only been announced once and for a period of 11 days, by the AS we are researching.



152.147.0.0/16

This prefix is owned by Housing Vic, an Australian housing company.

The routing history shows an interesting pattern, it has been announced by different ASs, but always for really short periods.



42.131.0.0/16

This prefix is owned by North Star Information Hi.tech, a Chinese IT services provider. Information found in https://www.spamhaus.org/ claim that IP addresses owned by this company are used for spamming.

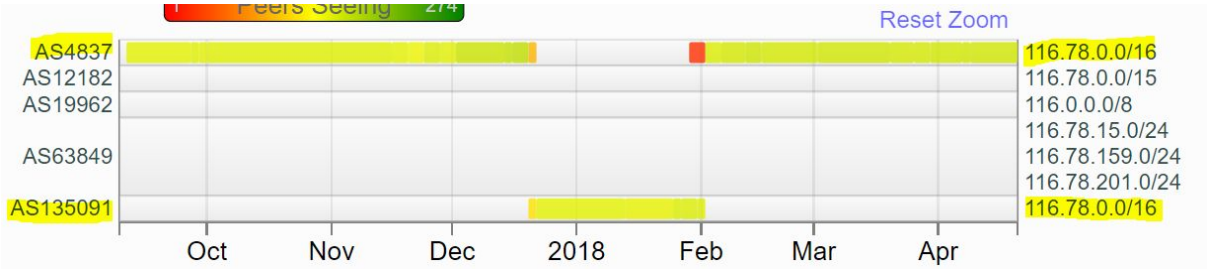
The routing history of this prefix is also quite suspicious, as it is only announced for short periods of time and by different ASs.

116.78.0.0/16

The prefix is owned by China Unicom, a telecommunication provider.

The interesting thing about the routing history in this case, that China Unicom is permanently announcing this prefix, but for approximately two months our AS takes

over and announces it. We can even see how in the beginning and the end of the possible hijack they both are visible by some peers.



Conclusions

AS135091 is a case that even if it is announcing prefixes out of the period covered by our database, we can consider it as highly suspicious. The routing history has a pattern that matches the cases that we were researching, and the 4 prefixes that we have studied also show us some suspicious behaviour.

ASN: AS27884-CABLECOLOR S.A.

aut-num	27884
owner	CABLECOLOR S.A.
country	HN
abuse-c	MRA
source	LACNIC

This ASN corresponds to Cablecolor S.A. an ISP from Honduras. This AS is announcing a group of prefixes that it owns regularly. However, in its history we can see a period of one day where many prefixes that it does not own are announced.

This happens for 8 hour the 21st of June of 2019 and the prefixes announced are prefixes from other operators of the countries around Honduras, like El Salvador, Guatemala or Costa Rica.

After analyzing this case we can conclude that probably this behaviour is caused by a misconfiguration or some kind of agreement between Central American ISPs.

Therefore we may consider this case as a false positive, because although it contains the pattern we were looking for, it doesn't seem to be because of a malicious activity.

Conclusion

In this project we have learned the high level working of the internet through the data analysis of publicly available BGP data. The scope has been set in the detection of anomalies such as prefix hijacks, performing for that goal an analysis of the routing behaviour of some ASs.

After a thorough filtering process we have selected 6 different ASs that show some kind of anomaly that follows a similar pattern that the prefix hijacks present in the literature.

Although, all of the selected cases show some kind of anomalous pattern, we have found out that in some of the cases this pattern could be caused by legit behaviours.

However, we consider that AS57129 and AS135091 could be involved in some malicious actions, thanks to the complementary information fetched from different sources.

All in all, the project has been an excellent exercise to discover the high level routing structure of the internet and the possible threats that could involve.

References

[1]https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data

[2]https://learningnetwork.cisco.com/docs/DOC-26826

[3]https://www.postgresql.org/docs/current/functions-net.html

[4]https://bitbucket.org/ripencc/bgpdump/wiki/Home

[5]https://tools.ietf.org/html/rfc6396

[6]https://www.postgresql.org/docs/current/sql-copy.html