A FIRST LOOK AT AUTONOMOUS SYSTEMS RECURRENTLY CAUSING BGP ORIGINATION CONFLICTS

A Thesis
Presented to
The Academic Faculty

By

Olivier Bemba

In Partial Fulfillment
of the Requirements for the Degree
Master of Science in the
School of Electrical and Computer Engineering
Department of Computer System and Software

Georgia Institute of Technology

May 2024

A FIRST LOOK AT AUTONOMOUS SYSTEMS RECURRENTLY CAUSING BGP ORIGINATION CONFLICTS

Thesis committee:

Dr. Cecilia Testart, Co-Advisor
School of Cybersecurity and Privacy
Georgia Institute of Technology

Dr. Frank Li, Co-Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Alberto Dainotti
School of Computer Science
Georgia Institute of Technology

Dr. Fabian Monrose
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Brendan Saltaformaggio
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date approved: January 23, 2024

ACKNOWLEDGMENTS

I would like to thank my advisors, Cecilia Testart and Alberto Dainotti, for the opportunity, guidance, and insightful feedback throughout the entire process of researching and writing this thesis.

I am also very grateful to my research committee, Frank Li, Fabian Monrose, and Brendan Saltaformaggio for reviewing my thesis.

I would also like to thank all the members of the Internet Intelligence laboratory, who were always ready to listen and helped me throughout this year of research. It is an honor to be part of the laboratory.

Special thanks are due to my family and friends for all the support they provided during this journey. Their patience, understanding, and encouragement have been a constant source of strength and motivation.

Finally, I would like to acknowledge the Georgia Institute of Technology for providing resources and facilities that facilitated the completion of this thesis, and also Telecom SudParis for enabling me to complete this double degree.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The Border Gateway Protocol (BGP) plays a key role in the Internet as it provides the path for packets to travel between independent networks (Autonomous Systems). However, it also allows multiple networks to announce reachability for the same prefix, which makes it vulnerable to attacks and misconfigurations that modify Internet traffic. This is known as an origin conflict. According to the Global Routing Intelligence Platform (GRIP), a software that detects this kind of event, less than 1% of all Internet networks is responsible for almost 40% of the most suspicious origin conflicts detected between January 1, 2020, and January 1, 2023. Therefore, it is important to try and understand whether these networks are not causing these conflicts for malicious purposes, or whether it is a matter of new routing habits, or simply misclassification from GRIP. As a first step, we leverage GRIP to isolate autonomous systems (ASes) that have been involved in at least one origin conflict on 50 different days. Then, for all these ASes, we collect data about their organization, their location, their type, and their GRIP events. In parallel, we retrieve routing data using the RIPE Stat API to provide more context. Finally, we combine and analyze these data to find indicators of malicious activity, configuration error, or legitimate behavior. Thanks to this first look at GRIP data from an AS perspective, we were able to observe some already seen legitimate behavior, such as the use of private ASNs or Internet exchange point prefixes. Next, we also observed several business relationships, such as hosting providers with their customers, IP space lessors with their lessees, and DDoS mitigation providers with their customers. These business relationships need to be studied in greater depth to better characterize and detect them. We also present two use cases: a global mobile operator that is known to make frequent configuration errors, and a hosting provider that is known to provide services to malicious customers. This study is a first building block towards finding new insights into the routing habits of Internet operators and thus contributes to improving the global routing monitoring system.

CHAPTER 1
INTRODUCTION

As the standard protocol for inter-domain routing, the Border Gateway Protocol (BGP) plays a crucial role in today's Internet. BGP enables networks, also known as Autonomous Systems (ASes), to exchange reachability information with their neighbors and select the preferred path to each block of address space in the public Internet. However, BGP lacks validation of information. In particular, two different ASes can claim to host (partially) the same block of IP address space, i.e. these networks are at the origin of the path to the IP address blocks. This is commonly known as an *origin conflict*. Unfortunately, origin conflicts are sometimes caused for malicious purposes. For example, an AS can intentionally advertise a prefix that it does not own to attract legitimate Internet traffic for malicious purposes, known as *BGP hijacking*. It happened in February 2022, when a BGP hijack targeting the Korean crypto-currency KlaySwap resulted in the theft of nearly 2 million dollars from its users [1]. The attackers impersonated one of the platform's vital services by announcing the prefix hosting this service. Worse still, some malicious actors on the Internet have made BGP hijack a business and do not hesitate to advertise bogus routes regularly. For instance, it has been revealed in [2] that Bitcanal, a Portuguese web hosting company nicknamed the "hijacking factory", hijacked over 1,500 prefixes over 4 years.

However, what makes the case of origin conflicts rather complex is that several studies have shown that most of these situations are not caused by malicious intent [3, 4]. Indeed, many of them result from configuration errors. For example, on June 12, 2015, AS4788 (Telekom Malaysia) caused major Internet slowdowns for two hours after accidentally announcing over 179,000 prefixes. The routes were propagated across much of the Internet as they were relayed by an AS owned by Level3 (now Lumen), one of the world's largest transit operators [5]. On the research side, Mahajan *et al.* [4] polled network operators and

discovered root causes such as initialization bugs, old configurations, and bad or forgotten filters. Then, Cho *et al.* [6] also came up with two types of human error that can lead to situations where an AS unintentionally advertises a prefix: typos in ASN or prefixes and wrong AS path prepending.

In addition to configuration errors, some origin conflicts are legitimate — although RFC 1930 [7] discourages them. Numerous studies over the last 20 years have shown that these conflicts often occur for many reasons. First, multi-homing can create a situation of two ASes announcing the same prefix. Multi-homing refers to connecting an AS to multiple Internet Service Providers (ISP) or upstream providers to achieve network redundancy, improve reliability, and optimize traffic routing. In a multi-homed network, the organization maintains connections to two or more ISP, allowing it to distribute its internet traffic across these connections. There are traffic engineering practices (e.g., load balancing) that also lead to origin conflicts. In addition, ASes from the same organization (i.e. *siblings* ASes), ASes hosting services in a data center, organizations doing IP leasing, and DDoS protection Systems are potential root causes of origin conflicts, as already observed in [8, 9, 3, 2].

For all these reasons, it is hard to know whether an origin conflict is legitimate, the result of a configuration error, or the beginning of a cyber attack. In parallel, considerable efforts have been made by the research community to mitigate both configuration errors and intentional hijacks. The most notable solution is the Resource Public Key Infrastructure (RPKI) which has been designed by the SIDR Working Group within the Internet Engineering Task Force (IETF) [10]. RPKI is a cryptography-based framework that links an AS to its Internet resources (e.g. AS Number and IP prefixes) using a certificate. Then, when an AS receives a BGP announcement, it can check whether the origin and prefix of the announcement are bound to the same RPKI certificate. Unfortunately, RPKI has not yet been adopted by all Internet actors, and origin conflicts continue to occur frequently and spread across the Internet [11].

Pending full adoption of RPKI, detection and characterization of these conflicts remains

a topical issue, in an attempt to better protect against them. The Global Routing Intelligence Platform (GRIP) [12] has been developed for this purpose, it:

1. Uses BGP data from Routeviews and RIPE RIS projects [13, 14]
2. Detects origin conflicts using BGPView [15]
3. Collects contextual information about origins and prefixes involved in the event from 10 datasets (including [16, 17, 18, 19, 20, 21])
4. Classifies the event as benign, misconfiguration, suspicious or unexplained, based on the contextual information

Between January 1, 2020, and January 1, 2022, GRIP detected 3,605,776 origin conflicts, including 20,406 *suspicious* and 14,753 *unexplained*. Even though this is less than 1% of the total, it is still a significantly high number. On the one hand, not all of the 20,406 suspicious events ended up in a cyber attack, thus this cluster includes a lot of false positives. On the other hand, the number of unexplained events is also very high, implying that GRIP classification system is not complete yet. In addition, nearly 40 % of them were caused by only 0.6% of all ASes present on the Internet. This implies that (1) some ASes are persistently causing origin hijacks (i.e. *serial hijackers* [2]), or (2) some ASes have unknown and legitimate routing practices that lead to origin conflicts, or (3) GRIP classification system can not identify some known use cases.

This master thesis is a first step towards a better understanding of these *a priori* suspicious or unexplained cases, as this could help to:

1. **Spot serial hijackers**
2. **Discover new routing habits leading to origin conflicts**
3. **Improve GRIP's inference rules**

First of all, we leverage GRIP data to conduct an empirical analysis of the ASes regularly involved in *suspicious* or *unexplained* origin conflicts between January 1, 2020, and January 1, 2023. We compiled a list of 47 ASes and manually investigated the causes of conflicts these networks caused. We used data from GRIP to have some contextual information about each event, IPinfo to have information about the activity of the AS (e.g hosting, ISP, etc.), RIPE Stat to have an overview of prefixes and ASes routing history, and IRR data to find ownership information about prefixes. Thanks to these first investigations, we discovered that these networks were mainly American and that they were mostly classified as ISP or hosting AS by IPinfo. Next, we observed that some ASes were participants in the Mutually Agreed Norms for Routing Security (MANRS) initiative, which aims to improve routing habits, while other ASes are currently partnering with Routeviews and RIPE RIS to share their BGP data. We also noticed that some ASes were causing conflicts always with the same ASes, and sometimes always with the same prefix. Finally, we present the detailed results of a dozen or so investigations, in which we saw already well-identified causes of conflict, such as the use of private ASN, or Internet exchange point prefixes, but also less studied cases, such as IP delegation and IP leasing. These initial insights enable us to better identify GRIP's needs and lay the foundations for improving its classification system.

The remaining chapters in this thesis are structured as follows. We discuss background in chapter 2. In chapter 3, we present GRIP and other tools used in the context of this thesis. In chapter 4, we propose our approach to investigate the ASes regularly causing origin conflicts. In chapter 5, we present the results of the investigation using the methodology discussed in chapter 4. In chapter 6, we discuss the benefits and limitations of these approaches and future work. Lastly, we conclude the thesis in chapter 7.

CHAPTER 2

BACKGROUND

In this chapter, we review all the basic concepts that will enable the reader to understand the following chapters better. We begin by recalling some important notions of the BGP protocol.

2.1 The Border Gateway Protocol

The Internet is based on networks of various kinds, independently administered by a large number of operators. Each operator manages blocks of IP addresses, which it can divide into smaller prefixes for its own needs or those of its customers. These independent networks are interconnected using the BGP protocol, the aim of which is to exchange information on the reachability of their prefixes. The last version of the protocol is defined in RFC4271[22]. In BGP terminology, a network is called an Autonomous System (AS) and is identified by an AS number (ASN). A company using the BGP protocol will generally have a unique ASN on the Internet.

Functionally, BGP operates as a Bellman-Ford distance vector routing algorithm, enabling interconnected routers (BGP speakers) to learn the topology of the network. Essentially, when a neighbor communicates reachability to an IP address prefix, the receiving BGP speaker compares it with existing knowledge. If the new information improves the path to the prefix, the speaker updates its forwarding table and notifies neighbors, designating itself as the next hop. BGP tracks route advertisement propagation across domains using the "AS Path" attribute, which records the sequence of ASes through which the advertisement traversed. The example below illustrates a BGP announcement. The rightmost ASN, 27919, is the one supposed to be the origin of the prefix (i.e. the authorized entity to originate the prefix):

$$112.10.10.0/24 : 174\ 9009\ 138686\ 27919$$

Moreover, there exists a withdrawal mechanism within BGP, activated when a BGP speaker concludes it lacks a feasible route to a specific prefix. In such instances, it notifies all neighboring speakers by issuing a "withdrawal" message. Upon receiving a withdrawal, a router will check if the withdrawn neighbor previously served as the preferred next hop for the prefix. If yes, it is going to look for an alternative path to update its forwarding table. If no such path is found, it is going to issue a withdrawal for that same prefix to the rest of its neighbors.

We briefly mentioned that a BGP speaker may receive multiple paths leading to the same destination prefix. In this situation, it has to make a choice. BGP RFC [22] defines a best path selection algorithm, which is an ordered sequence of comparisons criteria:

1. Highest LOCAL PREF attribute. This is an attribute exchanged between routers within the same AS to indicate the preferred exit point for a particular prefix. Note that this attribute is set within one AS and will not be used in any other AS

2. Shortest AS PATH attribute. An AS path with fewer ASNs in it will be preferred because it indicates a more direct path to the destination prefix

3. Lowest Multi-Exit Discriminator (MED) attribute value. As LOCAL PREF, MED is also set by network operators and it is used to communicate the preferred entry point for inbound traffic from a neighbor. Note that MED can only influence neighbors, not force them.

4. eBGP routes are preferred over iBGP routes. In other words, a BGP speaker will rather choose a route to a prefix learned from a BGP speaker not in the same AS

5. Lower IGP metrics (OSPF, RIP,...) to the next-hop are preferred

6. Lower BGP router ID is preferred. Tie-breaker when all other factors are equal

It is worth noting that the choice of the LOCAL PREF attribute is often motivated by business relationships between ASes. Indeed, like every industry, the Internet is also based on a customer-provider hierarchy. A customer AS will pay a provider AS for the transit of their Internet traffic, this is a customer-provider relationship. In addition, some ASes, generally of the same size, may also agree to provide transit to each other for free, this is a peer-to-peer relationship. As a consequence, an AS will tend to prefer a route learned from its customer to a route learned from a peer or supplier, for financial reasons [23].

Now that the basic principles of BGP have been presented, we will explain in more detail what origin conflicts are.

2.2 BGP Origin Conflicts

In this work, we study two types of origin conflicts: MOAS and subMOAS. For this reason, we briefly introduce them.

First of all, a *MOAS* conflict occurs when two or more ASes announce a the same IP prefix:

Definition 2.2.1. If prefix p is associated with $aspath_1 = (AS_1, AS_2, ..., AS_n)$ and $aspath_2 = (AS'_1, AS'_2, ..., AS'_m)$ and $AS_n \neq AS'_m$, then a MOAS conflict occurs.

BGP speakers use the best path selection algorithm if they have two different routes leading to the same prefix. Thus, in the event of a MOAS conflict, a BGP speaker will go through each step of the algorithm to decide which origin to send the traffic to. Based on what we explained in the previous section, a route is more likely to be chosen if it has been learned from a customer or if it is shorter in terms of AS hops.

A *subMOAS* conflict is similar to a MOAS conflict except one of the prefixes announced is more specific than the other:

Definition 2.2.2. If prefix p (e.g., $112.10.10.0/22$) is associated with $aspath_1 = (AS_1, AS_2, ..., AS_n)$ and prefix q covered by prefix p (e.g., $112.10.10.0/24$) is associated with $aspath_2 = (AS'_1, AS'_2, ..., AS'_m)$ and $AS_n \neq AS'_m$, a subMOAS conflict occurs.

In BGP, two prefixes with different network masks are considered different, so when receiving these two prefixes, a BGP speaker will not run the best path selection algorithm and will both push them in the forwarding table. However, forwarding is based on the longest prefix matching strategy, so in case the router needs to forward a packet with a destination IP address covered by both prefixes, it will select the route leading to $112.10.10.0/24$, as it is longer than $112.10.10.0/22$. Thus, subMOAS are more dangerous than MOAS in the sense that they are more likely to propagate in all forwarding tables.

When MOAS and subMOAS are caused intentionally for malicious purposes or are the result of a misconfiguration, some Internet traffic may be routed to an undesirable destination network. This can lead to connectivity issues if the new origin simply drops the traffic. There may also be integrity and privacy issues (e.g. eavesdropping, data tampering) if the traffic is routed back to the right destination. Eventually, the new origin can impersonate a service (e.g. DNS Server, Web server) hosted in the legitimate destination. For these reasons, the IETF proposed a solution to prevent MOAS and subMOAS conflicts from happening.

2.3 Resource Public Key Infrastructure

RPKI is a security framework designed to authenticate the origin AS of a BGP advertisement. Using certificates called *Route Origin Authorisation* (ROA), a resource holder can prove ownership of its Internet resources (e.g., IP addresses and ASN).

RPKI has two main stages:

- ROA issuance: Resource holders, such as ISP and network operators, cryptographically sign their ROA using digital certificates issued by a trusted authority known

as a Certificate Authority (CA)[1]. ROAs are then stored in a repository maintained by the CA.

- Route Origin Validation (ROV): when a BGP speaker receives an advertisement, it checks whether the origin is authorized to announce the prefix using the related ROA(s) stored in the CA repository. There are three possible outcomes:
  - *Valid*: the origin is authorized to announce the prefix
  - *Invalid*: the origin is not authorized to announce it
  - *Not found*: no ROA covers the prefix

Then operators can set up filters to refuse invalid announcements and only accept *valid* and *not found* ones. As of today, still around 50% of IPv4 BGP announcement ROV status is *not found* according to NIST RPKI Monitor [24], so refusing them would mean blocking access to almost half of all IPv4 prefixes. Here we see one of the limitations of RPKI: if not all operators implement it, then there is still room for configuration errors and attacks to spread and harm the Internet global routing.

[1]CA is very often one of the Regional Internet Registries: AFRINIC, APNIC, ARIN, LACNIC or RIPE.

CHAPTER 3

DATA

The main purpose of this chapter is to introduce GRIP, the BGP route monitoring system on which the entire study is based. Next, we give a quick presentation of other data sources used in the context of this study.

3.1 GRIP

The Global Routing Intelligence Platform (GRIP) [12] is a BGP monitoring framework that aims at detecting and classifying BGP hijacks in near-real time through inference techniques that combine diverse datasets. The architecture of the software is presented in Figure 3.1.

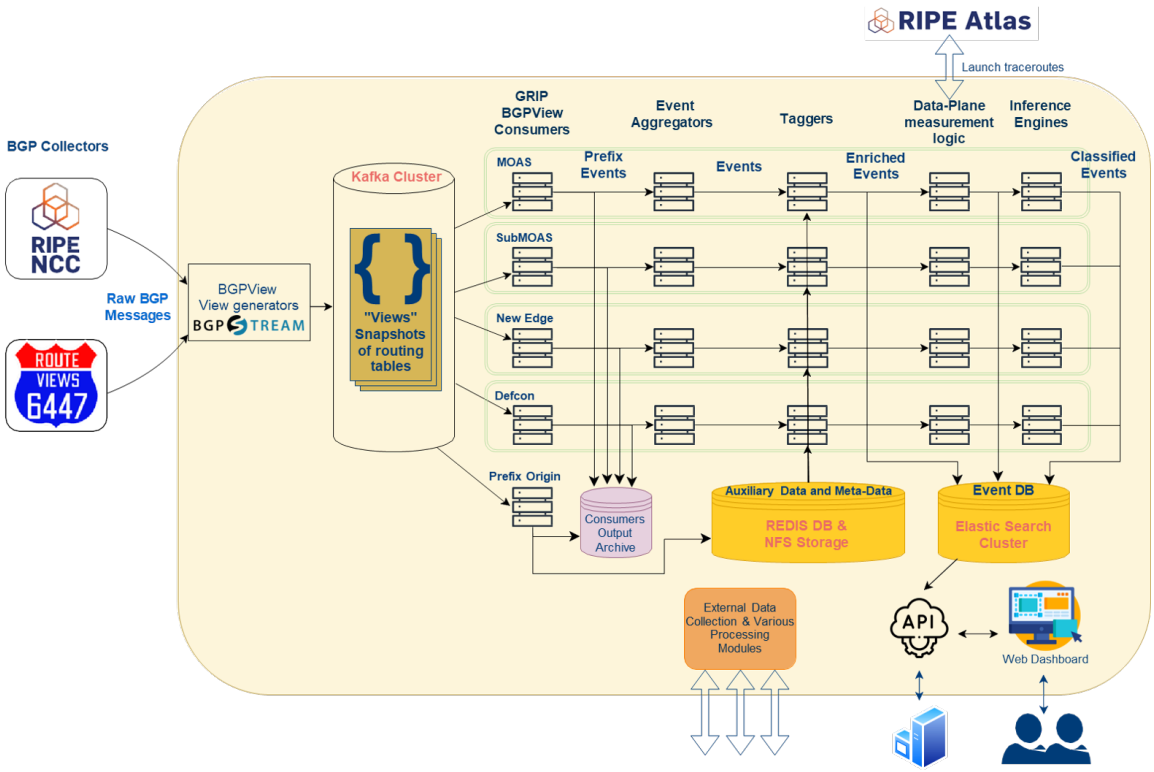


Figure 3.1: GRIP Architecture

3.1.1 BGP Data Collectors

Routeviews [13] and RIPE RIS [14] are both projects that collect and share data related to internet routing dynamics. Both projects work similarly: they operate a network of monitoring collectors distributed across the internet to collect BGP routing information. This data includes real-time and historical information from multiple organizations that volunteer to peer their routers with the collector to share their routing information. Eventually, both projects provide public access to this data in two possible formats:

- *Dump files* that store the state of the routing system at a given time (every 8 hours for RIPE RIS and every 2 hours for Routeviews)
- *Update files* that store all changes to the routing system for a particular interval (every 5 minutes for RIPE RIS and every 15 minutes for Routeviews)

3.1.2 Event Detection

GRIP can detect four types of anomalous BGP announcements: MOAS, SubMOAS, New Edge, and Defcon. The two latter are outside the scope of this study, and thus will not be discussed further (see [25, 26] for more information), while the two former have been defined in chapter 2.

To handle the detection, GRIP uses *BGPView* [15], a software that first collects Routeviews and RIPE RIS update files and dump files. Second, it provides snapshots - *views* - of collectors' peers routing tables with an adjustable granularity. In the context of GRIP detection, a view is generated every 5 minutes. Then, each view is compared with the previous one to detect abnormal events. For example, to detect MOAS, the corresponding BGPView consumer is tracking changes in prefix-origin AS pairs between two different views. If it sees multiple origins advertising the same prefix in the current view but not in the previous one, it creates a new MOAS *prefix event*. Similarly, when it sees a prefix being advertised by a different set of ASes than its closer super-prefix in the current view but not

in the previous one, it creates a new subMOAS prefix event. A prefix event is identified by:

- Event type: MOAS or subMOAS
- Prefix(es):
  - one prefix for MOAS
  - two for subMOAS: *subprefix* (longer) and *super prefix* (shorter)
- Set of ASN:
  - *oldcomers*: ASes which have been announcing the prefix in both the previous and the current views
  - *newcomers*: ASes which have started to announce the prefix in the current view
- View timestamp: the timestamp of the current view
- AS paths: set of AS paths associated to the involved prefix(es) in the current view

If multiple prefix events have the same type, the same origins, and the same timestamp, they are aggregated into one same event.

3.1.3 Event Enrichment

Once prefix events have been detected and potentially aggregated, GRIP will enrich its events using 10 different datasets:

- **ASNDrop** [16]: Spamhaus ASN DROP List of hijacked ASes or ASes controlled by spammers, collected daily
- **RPKI** [27]: Verified ROA Payloads from RIPE NCC RPKI Validator, collected every 5 minutes

- **IRR** [17]: WHOIS data from 20 major Internet Routing Registries including the 5 RIRs, RADB, LEVEL3, NTTCOM, TC, WCGDB, ALTDB, CANARIE, IDNIC, PANIX, REACH, OPENFACE, JPIRR, and NESTEGG, collected regularly

- **ASRank** [18]: information about the ASes, their organizations, their customer cones and the relationships between ASes (customer, provider, peer) using CAIDA AS Relationships [28] and CAIDA AS Organisation [29] datasets, collected monthly and trimonthly respectively

- **Hegemony** [19]: Global and local hegemony scores by the IHR project. The hegemony score is a metric to measure AS dependency., calculated every 15 minutes

- **TrustedASNs**: manually maintained whitelist of ASes providing DDoS protection services

- **OrgFriends**: manually maintained whitelist of sibling ASes

- **ReservedPrefixes** [21]: Reserved prefixes in IANA's IPv4 Special-Purpose Address Registry

- **ReservedASN** [20]: ASN reserved for private use

- **BlacklistASNs**: ASes found to be serial hijackers ([2]), manually verified

Based on all this information, GRIP is *tagging* every event. Each tag has a signification and a level of suspicion. There are three levels of suspicion: trusty (green), neutral (grey), and suspicious (yellow). Examples of tags can be found in table Table 3.1.

Table 3.1: Examples of GRIP tags

Tag name	Explanation	Suspicion
rpki-all-newcomer-invalid-roa	all newcomer origins have invalid RPKI ROA record for the announced prefix (subprefix)	suspicious
irr-ARIN-all-newcomer-more-specific-record	all newcomer origins have less specific IRR records for the announced prefix (subprefix)	suspicious
all-origins-same-country	the origins' organizations are in the same country	neutral
all-victims-stub-ases	all potential victim origins are stub ASes (have only providers)	neutral
previously-announced-by-all-newcomers	the prefix was previously announced by all newcomer origins in the past 10 months	trusty
all-siblings	all origins are sibling or friend ASes	trusty

3.1.4 Inference Engine

After adding context to each event, GRIP classifies them using the *inference engine*, a set of static rules with conditions based on tags and if-then-else statements. For example, one rule is designed to check whether the origins are siblings:

```
if event has tag ``all-siblings'':
    inference_id=``sibling-origins'',
    explanation=``All ASes involved are siblings'',
    suspicion_lebel=1,
    confidence=99,
    labels=[LABEL_BENIGN]
```

A rule therefore assigns *inferences* to each event according to the tags it has. An inference includes an explanation, a suspicion score between 0 and 100, a confidence score between 0 and 100, and a label (BENIGN, MISCONFIG, SUSPICIOUS, or TRACEROUTE).

For now, GRIP has around 20 rules, most of which are designed to rule out the obvious benign or legitimate cases (BENIGN label) already mentioned in the introduction: customer-provider relationship, DDoS protection AS, private ASN, prefix ownership change, the newcomer has already issued a ROA for the advertised prefix, etc. Then, one rule checks for potential configuration errors (MISCONFIG label) such as prefix or ASN typos and wrong path prepend. Next, one rule checks if the newcomer announcement is RPKI invalid, and thus the event is classified as suspicious (SUSPICIOUS label). Eventually, if an event does not match any rule, it is assigned a default inference (TRACEROUTE label) depending on the suspicion level of its tags. If the event has one green tag, it will be classified as *default-not-tr-worthy*, meaning "unexplained but looks benign". Else, the event is assigned *default-tr-worthy* inference ID, meaning "unexplained".

An event can have multiple inferences. When it has gone through all the rules, the set of inferences is sorted first on the confidence score, and then on the suspicion score in the case of a tie. The *primary inference* is the one on top of that list. In this study, we look only at this primary inference, and as stated in the introduction, we are going to focus only on events having a suspicious primary inference or a *default-tr-worthy* inference. In other words, we only keep the events where the newcomer's announcement is RPKI invalid or if the event does not match any rule from the inference engine and does not have any green tag.

3.2 Other Data Sources

3.2.1 RIPE Stat

RIPE Stat [30] is a tool provided by RIPE NCC, designed to provide comprehensive and up-to-date information about IP prefixes and ASN. In the context of this study, we use their data API to have access to four different information:

- Routing History: the history of announcements for a specific prefix and/or ASN

- RPKI History: the history of validated ROA payload for a particular prefix or an ASN
- ASN Neighbours History: the history of neighbors for an ASN

3.2.2 CAIDA AS Rank

We also used the CAIDA AS Rank [18] dataset, which aims at ranking ASes based on their connectivity and importance in the global Internet infrastructure. In particular, it uses:

- AS Customer Cone: it represents all the downstream ASes that are directly or indirectly connected to an AS network, including the AS' customers and their customer's customers, and so on.
- AS Degree: it refers to the number of other ASes that it directly peers with or connects to, including customers, peers, and providers

3.2.3 IPinfo

IPinfo [31] is a service that provides information mostly about IP addresses and ASes with a focus on the former. In particular, we used the type they assign to each AS. It is one of the following types: hosting, isp, business, education, or inactive. Their methodology is not public, although they explain that the classification is mostly based on the WHOIS data of each AS [32].

3.2.4 MANRS

MANRS [33] is a global initiative developed by network operators and supported by the Internet Society. It proposes a set of best practices and actions that network operators can voluntarily adopt to enhance routing security, including filtering, anti-spoofing, coordination, and validation of routing information. ASes that are part of the initiative have already

been used to build a ground truth dataset of legitimate ASes in [2]. We also used the list of participants in the context of the study.

CHAPTER 4
METHODOLOGY

In this chapter, we first present the selection criteria for ASes. Then, we describe how investigations were led on these ASes to find out why they generated so many alerts observed by GRIP.

4.1 Recurring Suspicious Behavior

The first step was to define what we considered to be a *recurring attacker* in the context of this study.

Definition 4.1.1. In the context of this study, a recurring attacker is an Autonomous System that caused a suspicious event on at least 50 different days between January 1, 2020, and January 1, 2023.

First of all, an *event* refers to either a MOAS or a subMOAS (see section 2.2 for definitions). We decided not to include the other two types of event: New Edge and Defcon, for the simple reason that detection algorithms for both Defcon and New Edge events have so far only been applied to BGP data collected after January 1, 2023. Also, we did not involve the year 2023 in the study for consistency reasons. Indeed, at the time of the beginning of the study, projects involving new inference rules were underway. Nowadays, events detected between 2020 and 2022 have already been subject to the new classification rules, but not yet those for 2023.

Then, the word *suspicious* also requires some clarification. As we explained in the previous chapter, each event is assigned a *primary inference* that contains a potential explanation for the event, a classification label, a suspicion level, and a confidence level. In this study, we considered an event suspicious if it has the label *suspicious* or if it has the

inference id *default-tr-worthy*. As a reminder, events with default-tr-worthy for primary inference are events that match none of the other rules and have no green tags for clearing them. As for events labeled as suspicious, table Table 4.1 contains a list of the inferences concerned, with explanations.

Table 4.1: List of inferences associated with label *suspicious*

Explanation	**Suspicion Score**	**Confidence Score**
All newcomers have invalid ROAs while oldcomers have valid ROAs but all traffic flows through oldcomers	75	80
All newcomers have invalid ROAs while some oldcomers have valid ROAs but all traffic through oldcomers	75	70
All newcomers have invalid ROAs while oldcomers have valid ROAs	80	85
All newcomers have invalid ROAs while some oldcomers have valid ROAs	80	75
All newcomers have invalid ROAs	80	70

Finally, let's explain the *at least 50 different days*. As we were only interested in networks causing *persistent* origin incidents, we first thought of setting a limit only on the number of events. However, some ASes could end up on the list of recurring attackers because they had mistakenly announced a large number of prefixes on the same day and thus caused a large number of independent events from GRIP's point of view. For example, on September 29, 2020, Telstra AS1221 caused 127 different events on GRIP [34]. The day after, an official statement from a senior network engineer at Telstra indicated that this was an error [35]. Even though the same AS caused a large number, this is not the result of recurring behavior, so it is necessary to filter out these cases. While new rules have now been integrated into GRIP to aggregate all events into one in such cases, this was not the case at the beginning of the study. Thus, to overcome this issue at that time, we decided to introduce the notion of time spreading. Finally, 50 days is an arbitrary threshold as a first step to build on something that can be larger.

4.2 Investigation

Based on this definition, we build up a list of recurring attackers. First, it is necessary to develop an investigation methodology to understand the root causes of their behavior. The idea is to classify behaviors into three categories:

- This type of behavior has already been described in the literature
- This type of behavior has never been described in the literature
- The data collected does not allow us to determine what happened with sufficient certainty

To make hypotheses about the root causes of these events, we first collected data that can help us characterize them: organization, location, size, and routing history (see Table 4.2). Next, we created an overview of the suspicious activity of each AS: duration, events spreading over time, visibility, and tag frequency. Finally, depending on the hypothesis formulated, we investigate external sources/elements that may or may not validate it.

Table 4.2: List of information collected for each recurring attacker

Description	**Data source**
AS Name	CAIDA AS Rank [18]
Organization Name	
Country	
AS degree (# customers, # peers & # providers)	
Customer cone (# ASN, # prefix & # address)	
MANRS participant (Yes or No)	manrs.org [33]
RV or RIS peer (Yes or No)	Routeviews [36] & RIPE [37]
IPinfo type	ipinfo.io [31]
Routing history	RIPE Stat [30]

For the study of suspicious events per AS, we collected data from GRIP for each event:

- **Inference ID** and **event type** to plot the distribution of all events according to their inference id or type
- **View timestamp** to plot the spreading of all events over time
- **Duration** to plot the cumulative distributive function of duration for all events
- **Prefixes** and **victims** to get the distinct number of victims and prefixes
- **Tags** to compute the frequency for each tag across all events
- **AS paths** observed by collector's peers to plot the cumulative distributive function of visibility for all events[1]

In the context of an event, *attacker visibility* (resp. victim visibility) is the number of collectors' peers seeing the announcement of the attacker (resp. the announcement of the victim) at the time the event was observed. To compare the various visibilities, we then normalized them. For this, we considered two approaches: normalize by the total number of peers used by GRIP or normalize by the number of peers seeing the event (attacker visibility + victim visibility). We finally calculated both for each recurring attacker, as the combination of the two metrics allows us to better assess the impact of an event. Indeed, the first visibility is more global and indicates the size of the event (*does it affect a large part of the Internet or just a small part?*), while the second one is more local and indicates the impact on the path selection process (*What is the fraction of ASes that have now a path to the potential attacker?*).

[1] All events caused by one recurring attacker, **not** all recurring attackers.

CHAPTER 5

RESULTS

This chapter presents the results of this study. First, we give an overview of the detected recurring attackers. In particular, we provide insights into the location, organization, and type of these ASes. Finally, we also look at whether they have particular characteristics that could help us to filter them out.

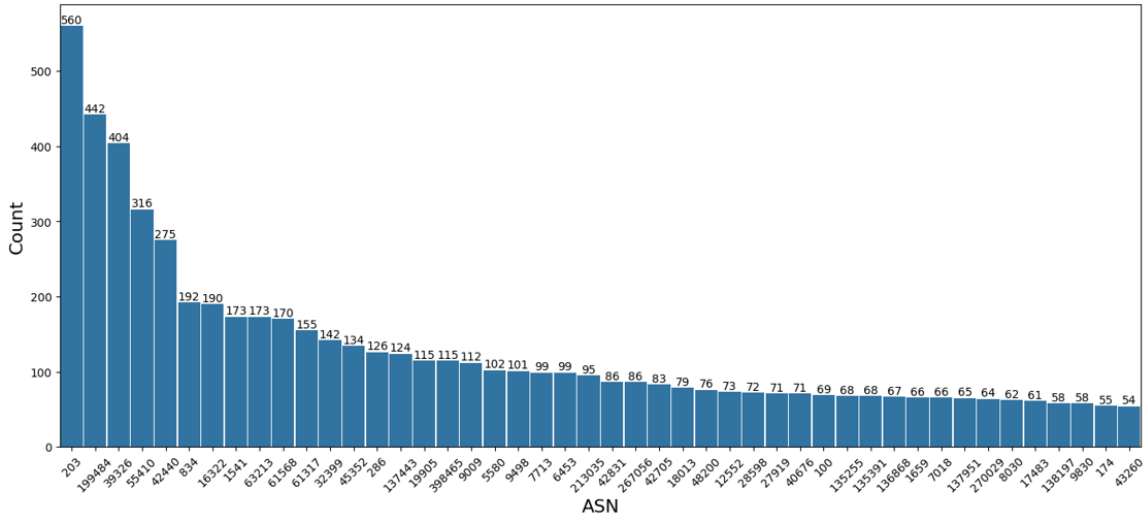


Figure 5.1: List of GRIP Recurring Attackers

5.1 Overview

Figure 5.1 shows the list of recurring attackers built using criteria presented in section 4.1. To bring some context, 3,605,776 events were detected by GRIP between January 1, 2020, and January 1, 2023. Among them, 20,406 were classified as suspicious (RPKI invalid announcement) and 14,753 as "default-tr-worthy" (unexplained), for a total of 35,159. To put it differently, GRIP already ruled out more than 99% of all MOAS and SubMOAS during these three years. Then, among the 35,159 suspicious and unexplained events, these 47 ASes have caused 5,992 of them. As there are around 70,000 ASes, this means that

0.6% of ASes are responsible for 17% of suspicious and unexplained events detected by GRIP.

5.1.1 Location

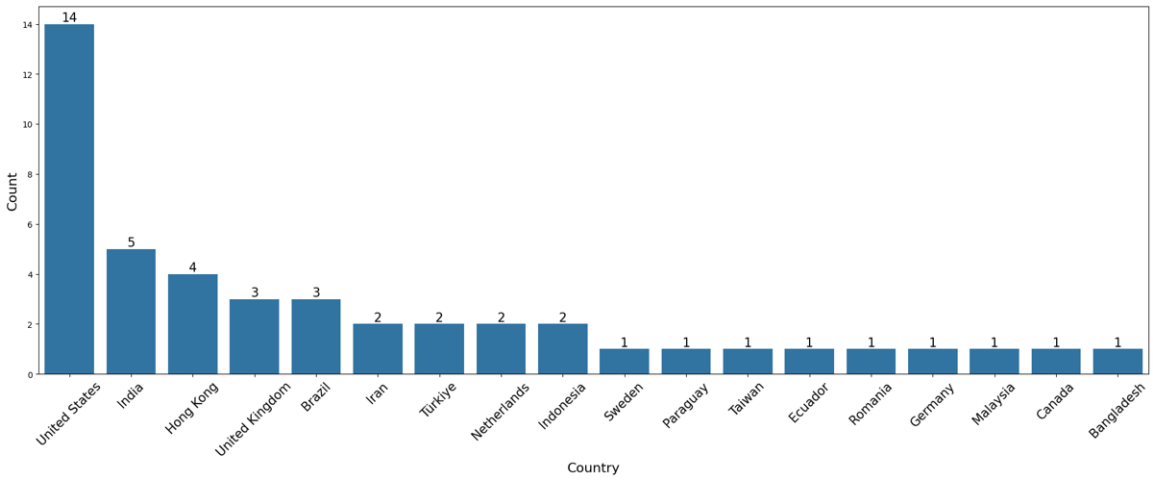


Figure 5.2: Recurring Attackers Countries

Figure 5.2 shows the countries of our various recurring attackers. We can see that the majority is located in the United States. According to IPGeolocation [38], the USA accounts for almost 30% of allocated ASN, so this is not surprising. However, this could also be because the data provided by the RIPE RIS and Routeviews projects are biased, as many of their collectors are located in North America and Europe. We are going to see in the next section that most of these American ASes are owned by large ISP having backbones spread all over the world.

We have also noticed that two ASes have changed location. The first is AS61317, which belonged to the IP leasing company IPXO and was located in the UK until August 2023. Since then, this AS is now owned by an American company providing storage and servers: Hivelocity Inc. Actually, IPXO and Hivelocity are business partners: Hivelocity servers are using IPXO IP addresses [39]. The second is AS286, which belonged to the Dutch company KPN International until July 2021, when it passed into the hands of the American multinational GTT Communications [40].

5.1.2 Organization

As mentioned in the previous section, some ASes are owned by big American Internet providers: AT&T (2 ASes), GTT (2 ASes), Lumen, Cogent, and TATA. Then, we have also two major Indian ISP: Bharti Airtel and Vodafone. As for the rest, we will see in the next section that these are mainly regional ISP or organizations providing hosting services (storage and/or servers).

It seems quite unlikely that large multinationals would intentionally hijack prefixes. Otherwise, it would have probably hit the news. Thus, in the context of this study, we assumed that their activity is probably not malicious. However, we still tried to understand why they caused so many incidents.

5.1.3 AS Type

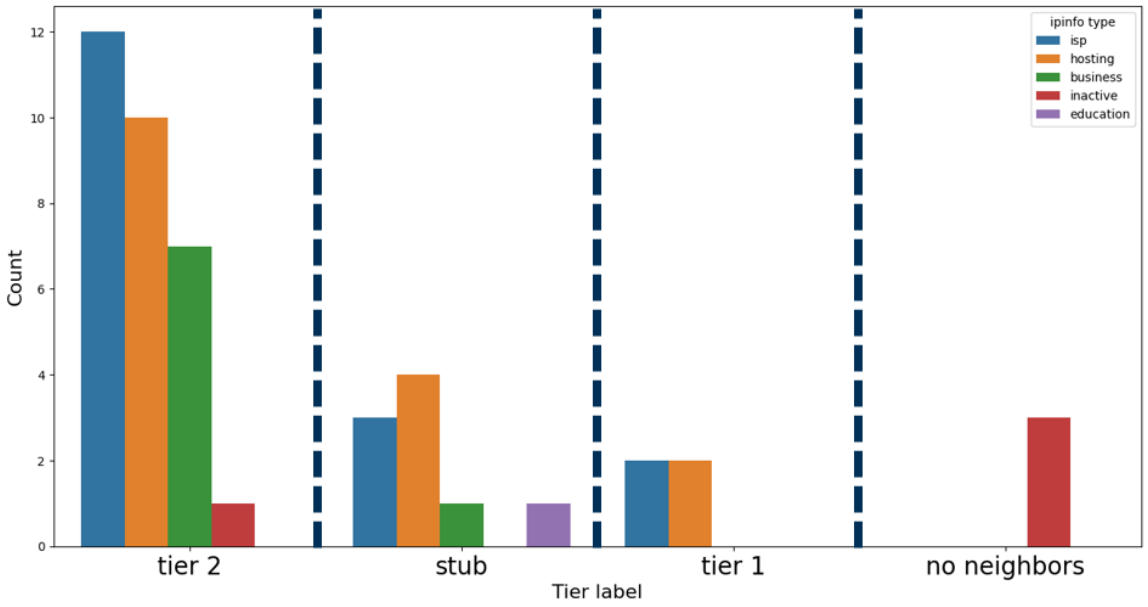


Figure 5.3: Recurring Attackers Type

Figure 5.3 shows two types of classification. The first one is using IPinfo [31] AS type. The second one is using AS Degree from CAIDA AS Rank dataset [18]:

- Tier 1: the AS does not have any providers (only customers and/or peers)

- Stub: the AS does not have any customers (only providers and/or peers)
- Transit: the AS has at least one customer and one provider
- No neighbors: the AS does not have any neighbors

This classification was carried out with the current AS degree of each AS (same for IPinfo type). IPinfo classification illustrates the fact that there is a majority of ASes are classified as either *isp* or *hosting*. In comparison, when looking at the IPinfo type of the first 8,934 US ASes [41],[1] *isp* ASes represent 10%, *hosting* ASes represent 8%, while *education* ASes represent 11% and *business* ASes represents 70%.

Next, we see three ASes considered *inactive* and without neighbors: AS1541 (owned by US Army), AS27919 (owned by IXP Ecuador), and AS32399 (owned by Alorica Inc). In fact, according to their routing history, they no longer advertise any prefixes. However, AS42440 (owned by Rayaneh Danesh Golestan Complex P.J.S. Co.) is also considered *inactive* by IPinfo, even though it has neighbors according to CAIDA AS Rank, and its routing history shows prefix announcements. This may be a problem with IPinfo's classification.

Another interesting point is that not all Tier 1 ASes are considered *isp* by IPinfo. Among the four ASes are AS286 (GTT), AS6453 (TATA), AS7018 (AT&T), and AS174 (Cogent), so only companies providing IP transit. The two classified as hosting ASes by IPinfo are AS286 and AS6453. This illustrates either the fact that multinational ISP are likely to diversify into other areas or another mistake in IPinfo's classification. Note that there is also one AS classified as education, AS1659, belonging to a Taiwanese university.

5.1.4 Other Noticeable Facts

Table 5.1 shows a list of recurring attackers having less than five victims. These were the first ASes we studied based on the intuition that if an AS would cause a large number of

[1] These are the ones having at least 1024 IPv4 addresses, the equivalent of a /22-prefix. We stopped there because we had to retrieve the list manually.

conflicts with the same victim, the cause of the conflicts would probably be the same. We set the limit to five victims, as all the other recurring attackers had more than 10 victims.

Table 5.1: List of Recurring Attackers with fewer than 5 victims

ASN	Company	Victim Count
32399	Alorica Inc	1
42705	Talia Ltd	1
135255	Agrawal Techonology Solutions	1
270029	Meganet S.R.L.	1
136868	PT. Terasys Virtual	2
27919	IXP Ecuador	3
1659	National Chung Hsing University	4
48200	Opteamax Gmbh	4
1541	USAISC	5

Next, some ASes are pairing with Routeviews [36] and/or RIS collectors [37] as we can see on Table 5.2. As explained in section 3.1, GRIP data comes from the peers of RIS and Routeviews collectors, thus assuming this data is safe.

Table 5.2: List of recidivist attackers peering with a collector. *: Routeviews, °: RIPE RIS.

ASN	Company	Collectors it pairs with
398465	Rackdog	Chicago*, eqix*, linx*, NY* and Sydney*
6453	TATA	Linx*, RRC03°
7018	AT&T	route-views*, route-views2*, route-views6*, RRC00°
7713	Telekomuniskasi Indonesia	amsix*, SG*
9009	M247	soxrs*
45352	IP Server One	route-views3*
61568	ALOO Telecom	route-views3*
267056	Everest Ridge Do Brasil	rio*
174	Cogent Communications	RRC25°

Eventually, we have four recurring attackers that were already used to build a ground truth dataset in [2]. On the one hand, there are two *legitimate AS*: AS174 and AS286. They were considered as such because they are both part of the MANRS initiative [33]. AS174 is owned by Cogent while AS286 is owned by GTT. On the other hand, we have two *serial hijackers*: AS9498 and AS9009. The first one belongs to the Indian mobile operator Bharti Airtel while the second belongs to M247, a Romanian hosting company. They have been

identified as such based on recurring complaints found on NANOG mailing lists. NANOG mailing lists [42] are email lists maintained by NANOG, a professional association of network operators who exchange technical information and discuss operational issues about the Internet infrastructure. They are highly regarded within the networking community for their technical depth and relevance.

In the following section, we present some results of investigations we have carried out.

5.2 Investigation Results

5.2.1 Internet Exchange Prefixes

AS48200 belongs to Opteamax GmbH, a German local ISP. It caused 71 MOAS and 5 subMOAS with three internet exchange prefixes:

- 48 MOAS with 185.170.0/23. WHOIS netname: DE-CIX-DUS-IXP-IPv4
- 23 MOAS with 185.1.208.0/23. WHOIS netname: DE-CIX-MUC-IXP-IPv4
- 5 subMOAS with 185.1.210.0/24. WHOIS netname: DE-CIX-HAM-IXP-IPv4[2]

As explained in [8], internet exchange point addresses can be directly reachable from all the ASes peering at the exchange point and each of these ASes might announce the prefix. Thus, it could cause MOAS conflict.

To consolidate our hypothesis, we checked the public exchange points where each AS is present using PeeringDB[3] website. For example, the PeeringDB record for our recurring attacker AS48200 indicates that the network is present at DE-CIX Dusseldorf, DE-CIX Hamburg, and DE-CIX Munich. This explains why AS48200 would announce the three prefixes involved in the conflicts. Then, regarding our victims:

[2]DE-CIX operates multiple Internet Exchange Points around the world, including in Dusseldorf, Munich, and Hamburg

[3]https://www.peeringdb.com

- AS9009 caused 47 MOAS with the prefix DE-CIX-DUS-IXP-IPv4, and according to its PeeringDB record, AS9009 is present in DE-CIX Dusseldorf
- AS61438 caused 47 MOAS with prefix DE-CIX-MUC-IXP-IPv4, and according to its PeeringDB record, AS61438 is present in DE-CIX Munich
- AS61438 caused 47 MOAS with prefix DE-CIX-MUC-IXP-IPv4, and according to its PeeringDB record, AS61438 is present in DE-CIX Munich
- AS211083 caused 1 MOAS with prefix DE-CIX-DUS-IXP-IPv4, 1 MOAS with prefix DE-CIX-MUC-IXP-IPv4 and 1 subMOAS with DE-CIX-HAM-IXP-IPv4, and according to its PeeringDB record, AS211083 is present in all three facilities
- AS199610 caused 2 MOAS with prefix DE-CIX-DUS-IXP-IPv4 and 4 subMOAS with DE-CIX-HAM-IXP-IPv4, and according to its PeeringDB record AS199610 is not present in DE-CIX Dusseldorf nor in DE-CIX Hamburg, but it is present in both DE-CIX Frankfurt and DE-CIX New York

Note that AS9009 is also in the recurring attacker's list.

5.2.2 Private ASN

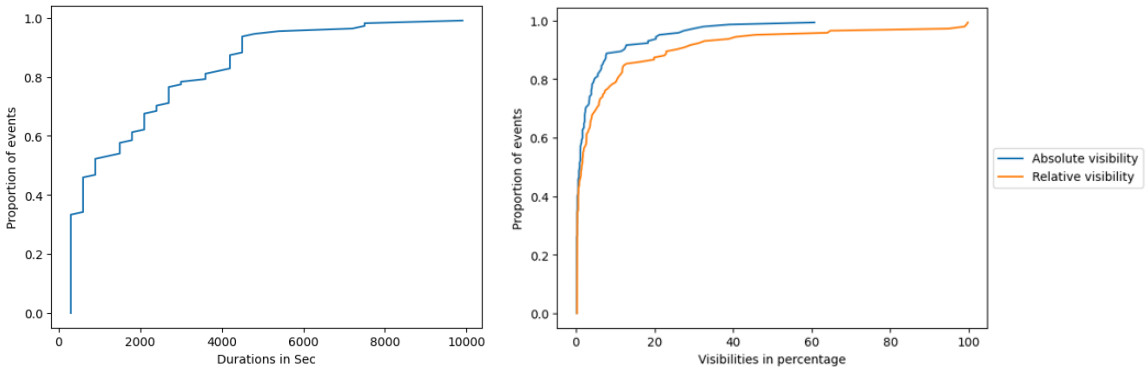
An interesting ASN appears in our list of recurring attackers: AS65535. It caused 136 MOAS and 6 subMOAS. AS65535 seems to be a private ASN but it was not considered as such by GRIP, whereas as explained in chapter 2, GRIP is using an IANA reserved ASN list to detect the use of private ASN.

Originally, as stated in RFC1930 Private ASN ranged from 64512 to 65535 [7]. However, since [43], Private AS numbers range from 64512 to 65534, and no longer 65535. Indeed, all BGP reserved communities now begin with 0xFFFF, which is 65535 in decimal [44]. However, some network operators might still be using AS65535 for private purposes.

Zhao *et al.* [8] already observed MOAS cases involving Private ASN and multi-homing. More precisely, a small AS with several providers could announce its prefixes to each of

its upstream using the same private ASN. Then, each of these providers would remove the private ASN from the AS path attribute and put their public ASN instead. Finally, each provider would forward the route to the rest of the Internet, thus creating MOAS conflicts. In our case, the private ASN is visible to the rest of the Internet, so it is a bit different.

First of all, private ASN are used within private networks for internal routing and communication purposes. They should not be advertised on the public internet. Secondly, private ASN are usually used in large organizations to segment different departments or divisions, but also in data centers in leaf and spine architecture [45]. To prevent the private ASN from becoming public when forwarding an internal prefix to the rest of the Internet, one should not forget to remove it from the AS path attribute before advertising it to the rest of the Internet. Thus, visible MOAS conflicts involving a private ASN are probably the result of an AS neglecting to remove the private ASN from the AS path. In GRIP, the potential victim would be the one doing this configuration error. Then, as this is an error, we would expect the conflicts to have a low duration. Finally, we would also expect low visibility because most ASes should not select this route as it originates from a private ASN.



(a) Fraction of Events Vs. Duration (b) Fraction of Events Vs. Visibility

Figure 5.4: AS65535

In Figure 5.4a, we can see that half of the events caused by AS65535 lasted less than 15 minutes and 75% of events lasted less than 45 minutes. Then, Figure 5.4b shows the visibility of events, with *absolute visibility* being the attacker visibility normalized by the

total number of peers used by GRIP and the *relative visibility* being the attacker visibility normalized by the number of peers seeing the conflict (see section 4.2 for more details). We can see that in 75% of the events, the attacker announcement has less than 4% absolute visibility and less than 7% relative visibility, which means that the attacker announcement does not propagate globally, while the victim announcement does. In other words, the attacker announcement has a very small impact. In addition, more than 88% of the events have the tag *oldcomers-always-on-newcomer-originated-paths*, which means that the potential victim is on the attacker's AS paths as seen by the collector's peers. All these factors make the configuration error theory highly credible.

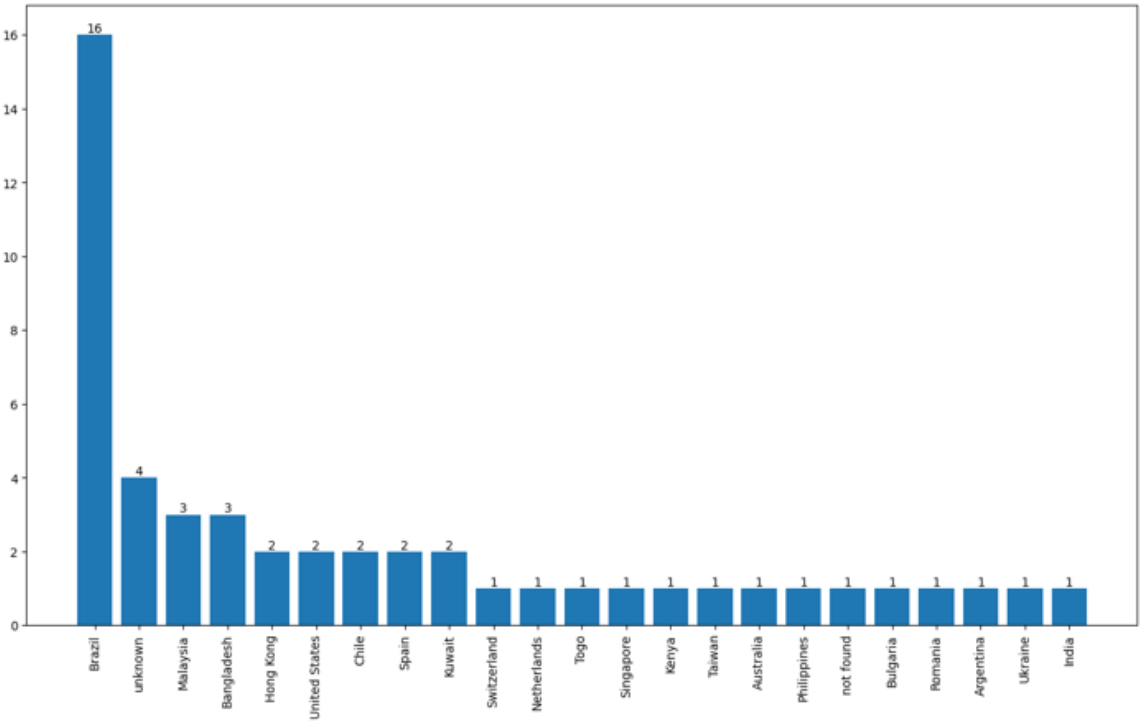


Figure 5.5: AS65535 Victims Countries

Figure 5.5 shows the supposed nationality of the ASes causing the most conflict. Note that 16 of the 50 "victims" are Brazilian. These 16 ASes are either classified as ISPs by IPinfo or belong to ISPs through manual verification.

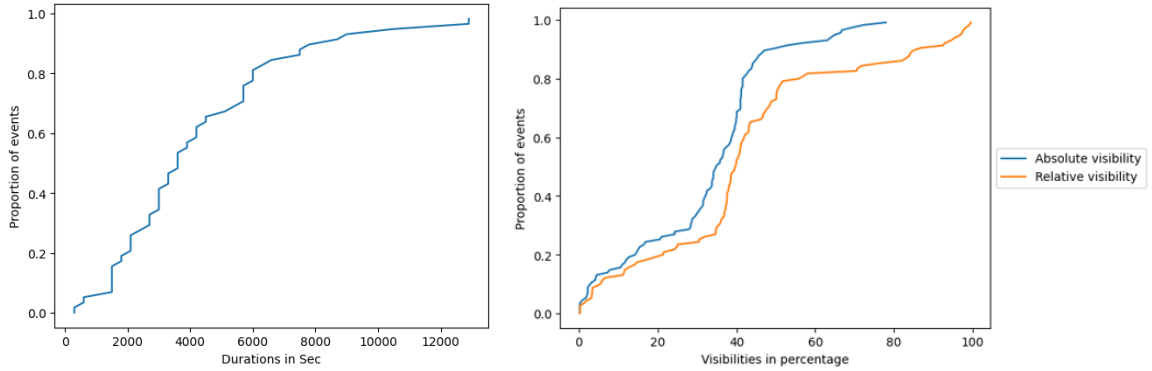
5.2.3 DDoS Protection Services

AS19905 belongs to Neustar Security Services, now Vercara, a division of Neustar Inc. which is a company that provides solutions in marketing, risk, security, and communication services. In particular, Neustar Security Services offers a range of solutions including DDoS protection. RADB object description for AS19905 is "Neustar Security Services UltraDDoS Protect". However, ASes providing DDoS protection services are known to present a legitimate case of recurring hijacking behavior [2].

There is already a manually populated whitelist containing ASes known to provide DDoS protection services, and there is an inference engine rule using this whitelist. However, the confidence placed in this whitelist is lower than the one placed in the fact that the announcement is RPKI invalid, so events involving an AS in the DDoS protection whitelist but with an RPKI invalid announcement are considered suspicious by GRIP (see section 3.1 for more information about GRIP inference engine).

DDoS mitigation essentially consists of advertising customer prefixes to attract all traffic destined for attacked networks to a scrubbing center. In this center, all DDoS traffic is dropped, while legitimate traffic is forwarded to the customer's network. According to Vercara's official website, detection, which usually takes just a few seconds, automatically triggers the announcement of the attacked client's prefix, so mitigation begins fairly quickly. It is also explained that the client is supposed to withdraw its prefix announcement at the time of an attack, probably to enable Vercara to attract all traffic to its scrubbing centers. However, it is not specified whether Vercara has control over this operation. This could explain why a MOAS conflict is created when Vercara announces the prefix. Regarding the duration of mitigation, and therefore the duration of Vercara's announcement, it depends on the duration of the attack. According to the website, it takes a few minutes in most cases, but some rare attacks may last a few days [46, 47, 48]. Thus, we would first expect the victims of the conflict to be Vercara customers. With everything we have just described, we would expect AS19905 announcements to have high visibility and to be only

/24 as the goal is to attract as much traffic as possible. Eventually, we would expect most events to last some minutes or potentially a few hours, and a very few more than a day.



(a) Fraction of Events Vs. Duration

(b) Fraction of Events Vs. Visibility

Figure 5.6: AS19905

In Figure 5.6a, we can see that half of the events caused by AS19905 lasted less than an hour, while 75% of events lasted less than one hour and a half. Maximum duration is 3 hours and 35 minutes. Then, Figure 5.6b shows that in 50% of the events, the attacker announcement has less than 35% absolute visibility and less than 39% relative visibility. In the context of a DDoS attack, this would mean that the network under attack would still attract more traffic than the protection network, which is supposed to mitigate the DDoS attack. This could be because Vercara's announcements are RPKI invalid and may be filtered by certain ASes. Of course, we need to qualify these statements, as visibility is calculated from a snapshot of AS paths at the time of the incident, and so perhaps 5 or 10 minutes later, Vercara's announcement has more visibility in the majority of cases. This hypothesis on RPKI therefore needs to be studied in greater depth to validate it. Regarding prefix length, it is more in line with our assumption, as all AS19905 announcements involved in the conflicts have prefixes of length 24.

Concerning the victims, given that Vercara's customer list is not public, we had to find another way of establishing a link between Vercara and its victims. One way we have found is to see if AS19905 is present in all the countries with which they caused conflict. To do this, we once again used the PeeringDB records. Figure 5.7 shows the countries

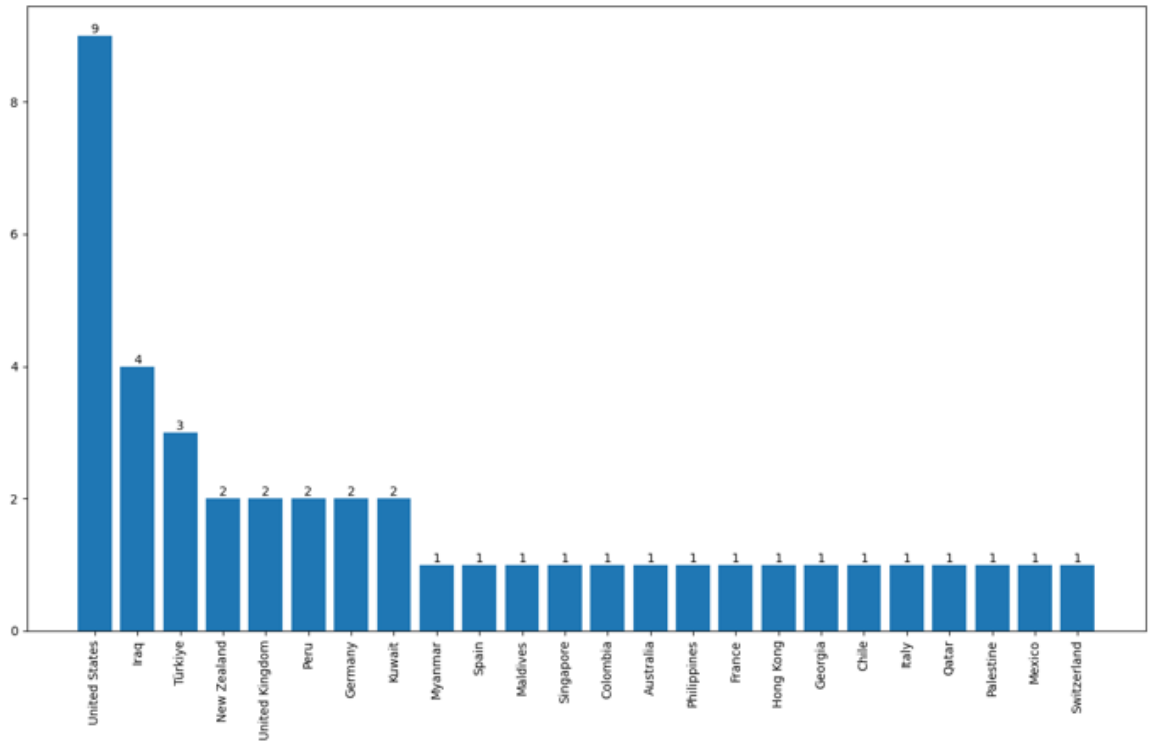


Figure 5.7: AS19905 Victims Countries

of AS19905's victims. Unsurprisingly, the United States is the most represented country, as Vercara is an American company. We can also see Germany, France, United Kingdom, Spain Australia, Singapore, Colombia, and Hong Kong which are all countries where either AS19905 or AS12008 (also Vercara) are present. For the rest, we found that most of the victims were involved in multiple conflicts spread over time with AS19905, so they are more likely to be customers. Secondly, some of them were present in the same facilities as either AS19905 or 12008. Eventually, we even found three cases where AS19905 had a RADB object with the prefix involved in the conflict.

5.2.4 Siblings

In this list of recurring attackers, we have one AS owned by the US Army: 1541. This AS caused 166 subMOAS and 7 MOAS with prefixes already advertised by ASes also owned by the US Army: AS749, AS721, AS1600, AS326, and AS5994. We therefore concluded

that these ASes were probably siblings and that the events were probably legitimate. To deduce that these ASes all belonged to the US Army, we used AS information available on GRIP and directly pulled from the CAIDA ASRank dataset. For our recurring attacker, the organization name is *Headquarters, USAISC*[4] and the AS Name is *DNIC-ASBLK-01534-01546*. DNIC stands for *DoD*[5] *Network Information Center*. In addition, our four victims have all the same organization name: DoD Network Information Center. As mentioned in the previous section, AS1541 is now inactive and no longer causes conflicts.

We have also decided to put AS1659 in the siblings category. This AS belongs to the National Chung Hsing University and caused 8 MOAS and 58 subMOAS over the period. The four victims are:

- AS17712: National Chung Cheng University (49 subMOAS)
- AS18420: National Central University (9 subMOAS)
- AS17713: National Sun Yat-sen University (6 MOAS)
- AS18177: National Cheng Kung University (2 MOAS)

National Chung Hsing University, National Chung Cheng University, National Cheng Kung University, and National Sun Yat-sen University all form a research-led university alliance called the Taiwan Comprehensive University System [49]. Then, National Central University is also a Taiwanese university. All the subMOAS events caused with the two origins have the same scenario: AS18420 is already announcing 140.115.0.0/16 and AS1659 starts announcing 140.115.38.0/24 and 140.115.32.0/24[6]. These two prefixes are covered by 140.112.0.0/12 which has been announced by AS1659 since 2005 (see routing history since 2019 on Figure 5.8). In addition, other Taiwanese universities have announced sub prefixes of the /12 at some point since 2005, including National Center

[4]US Army Information System Command
[5]Department of Defense
[6]Example: https://grip.inetintel.cc.gatech.edu/events/submoas/submoas-1627532100-18420=1659

for High-performance Computing (AS7539), Academia Sinica (AS9264), National Chiao Tung University (AS9916), National Taiwan University (AS17716), National Tsing-Hua University (AS18047) and National Taiwan Normal University (AS38844). We can therefore conclude that is 140.112.0.0/12 probably a prefix shared by Taiwanese universities.

AS834 from IPXO also caused 13 of its 192 events with AS61317, which was also owned by IPXO at the time of the events. We saw in subsection 5.1.1 that AS61317 is now owned by Hivelocity and that the two companies are closely related.

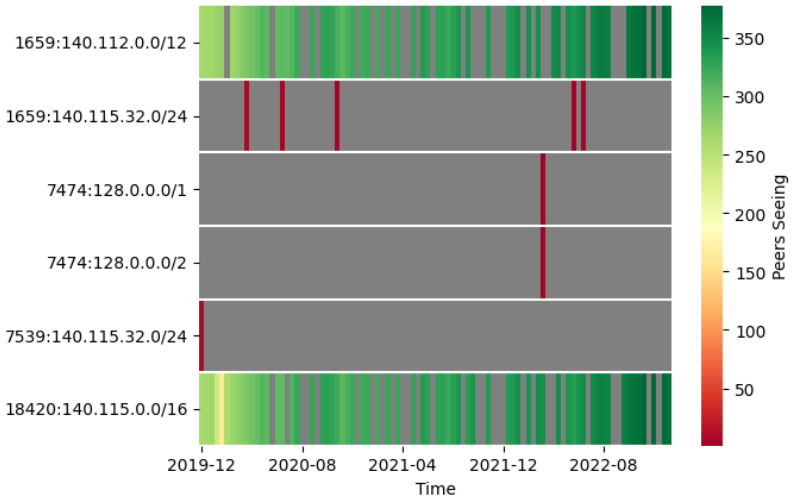


Figure 5.8: Routing history (RIPE Stat) of 140.115.32.0/24 between 2020 and 2022. It also includes some super prefixes. On the y-axis,it should be read origin_AS:prefix.

5.2.5 Customer Provider relationships

Jacquemart *et al.* [3] observed that most of the MOAS conflicts were probably caused by the customer and provider both announcing a prefix. We have indeed found several cases.

GRIP Inference Engine Bias

First of all, AS27919, a network owned by *IXP Ecuador* caused 71 events. As this AS has been inactive since October 17, 2023, we did not find a lot of information about it. According to PeeringDB, the AS was peering with an exchange point called “IXP Ecuador - STD”, and both have the same contact information, so this AS was probably owned by

the facility. Regarding the events, 70 out of 71 events were caused by the same victim: AS264668, which was a provider of AS27919 at the time of the events according to the CAIDA Relationships dataset. GRIP has a rule to infer relationships between origins and all the 70 events have both "all-newcomers-are-customers" and "all-newcomers-rpki-invalid-all-oldcomers-valid-roa". However, the latter has a confidence score of 80, while the former has an inference score of 70, thus the primary inference is "all-newcomers-rpki-invalid-all-oldcomers-valid-roa".

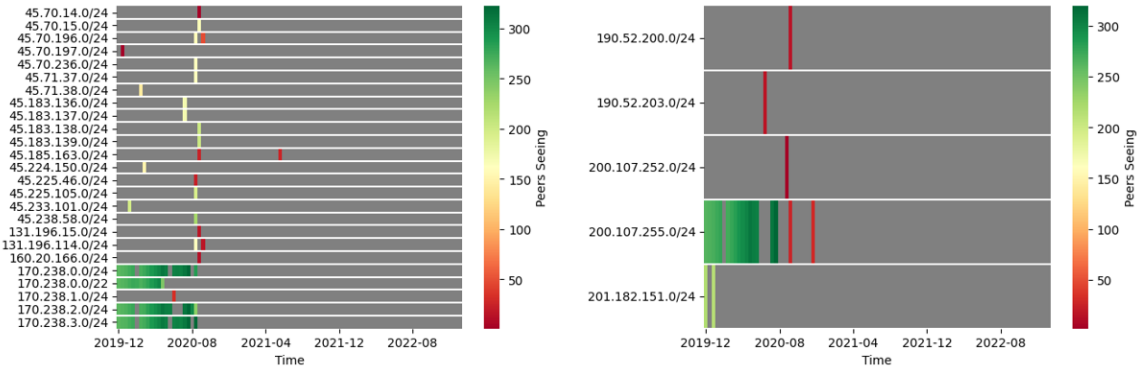


Figure 5.9: AS27919 Routing History

This is quite understandable, given that RPKI is more reliable than the CAIDA dataset. However, 70 origin conflicts were caused in this case, 75% of which lasted less than 15 minutes. In addition, we can see from its routing history in Figure 5.9 that it advertised quite a few prefixes for a very short time in mid-2020. This is also when most of the events took place as we can see in Figure 5.10, so there could be a correlation and it could be due to traffic engineering practices or misconfigurations.

Another similar case is AS136868 (P.T Terasys Virtual, Indonesian company providing hosting services) and AS138368 (Instacom, Pakistani ISP), which caused 57 events on GRIP in 3 years, even though AS138868 was AS136868's provider during the period. Same as above, these events were considered suspicious because AS136868's announcement was considered invalid. To conclude with these two recurring attackers, we would need an external confirmation (e.g. contact the operator) to be sure if these are indeed

traffic engineering practices and/or misconfigurations.

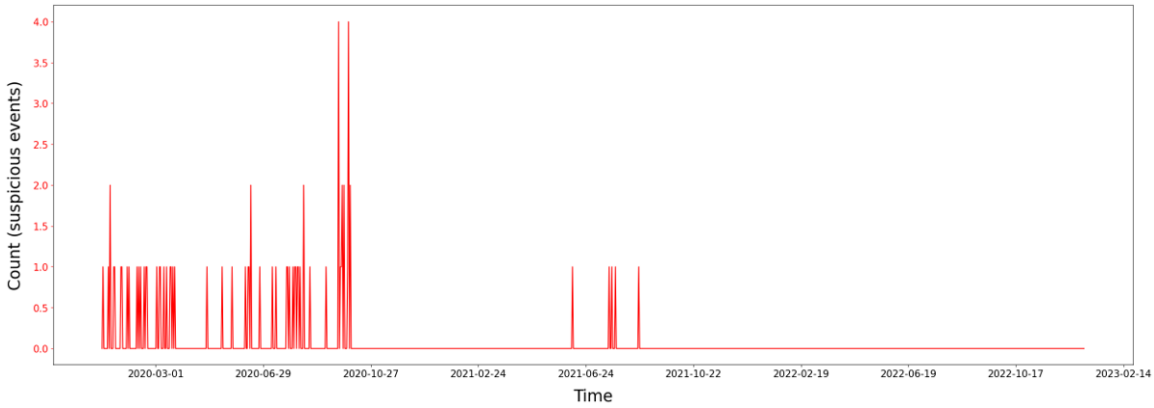


Figure 5.10: AS27919 Events Over Time

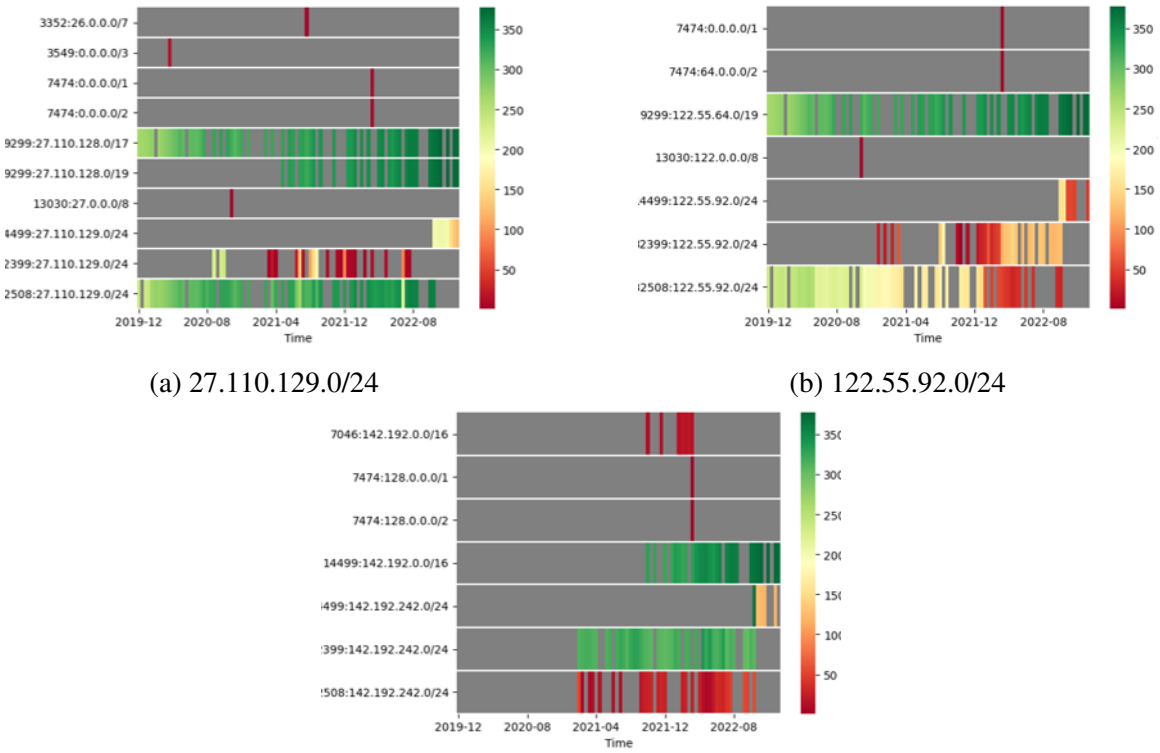
Multi-Homing

AS32399 belongs to Alorica Inc., a US company offering digital Customer Experience support. The AS caused 142 events, all with a single victim and three prefixes: AS132508, 27.110.129.0/24 (105 events), 122.55.92.0/24 (36 events) and 142.192.242.0/24 (1 event). AS132508 belongs to PLTD Inc.[7], a Philippine telecommunication provider. 27.110.129.0/24 and 122.55.92.0/24 have an *inetnum* object in APNIC database with:

- Description: "1-14RLRYF_ALORICA TELESERVICES, INC."
- Incident Response Team (IRT) Contact: abuse@pldt.net
- Abuse Contact: abuse@pldt.net
- Person Contact: juliusray.basa@alorica.com for 27.110.129.0/24 and JamesChristopher.Austria@ncogroup.com[8] for 122.55.92.0/24
- Route Object Origin: AS132508 for 27.110.129.0/24 and AS14499 (Alorica too) for 122.55.92.0/24

[7]PLDT = Philippine Long Distance Communication
[8]NCO Group was part of Expert Global Solution (EGS), acquired in 2016 by Alorica [50]

The last prefix (142.192.242.0/24) has an ARIN inetnum object related to the Alorica ARIN organization object. In other words, 142.192.242.0/24 belongs to Alorica according to the ARIN database. Moreover, according to Alorica's website [51, 52], the company appears to be operating in the Philippines.



(a) 27.110.129.0/24

(b) 122.55.92.0/24

(c) 142.192.242.0/24

Figure 5.11: AS32399's Prefixes Routing History

Next, Figure 5.11 shows the routing history of the three prefixes between 2020 and 2022. Notice that our two origins, AS32399 and AS132508 both stopped announcing the three prefixes at the same time. Moreover, as soon as they stopped announcing them, AS14499 (Alorica) started announcing them. In parallel, we can see that AS9299, which belongs to PLDT is announcing less specific prefixes (Figure 5.11a and Figure 5.11b). Eventually, AS14499 is a customer of AS9299 according to the CAIDA AS Relationships dataset.

In conclusion, PLDT is probably the Internet provider of Alorica in the Philippines and until late 2022, both Alorica and PLDT were advertising the same prefixes, probably due

to multi-homing without BGP. More precisely, AS32399 had another provider at the time of the event, AS4775, owned by Globe Telecom, another Philippines telecommunication company and which is now AS14499's provider. Thus, Alorica had probably two Internet providers: Globe Telecom and PLDT, and the link with PLDT was probably using either static routing or another routing protocol (e.g. OSPF), which would explained why the relationship never appeared on AS paths collected by RIPE RIS and Routeviews collectors.

5.2.6 IP transfer

The transfer of IP addresses from one organization to another is becoming more and more frequent, especially in the case of IPv4 as they have been exhausted. For the purposes of this study, we are interested in two types of IP transfer: delegation and leasing.

IP delegation

Large ISPs (e.g., Cogent) can delegate a part of their address space to some customers when they are not using it. As a consequence, the customer starts advertising the delegated prefix while the provider keeps advertising a less specific prefix, leading to a subMOAS situation.

AS270029, from Meganet S.R.L (Paraguayan ISP), appears to have caused 64 sub-MOAS with one victim: AS12956 (from Telxius, a Spanish ISP operating worldwide). All events involved the same super prefix: 66.249.192.0/19 (announced by AS12956) and the same sub prefix: 66.249.222.0/24 (announced by AS270029). There is one inetnum object associated with 66.249.192.0/19 in the ARIN database. This object is related to two organizations: Telxius and Copaco (a Paraguayan ISP). Three-quarters of the events were tagged with "all-newcomer-are-rel-downstream", which means that AS270029 was the customer of a customer of AS12956 at the time of the events, according to CAIDA AS Relationships dataset. Looking at the AS paths collected by GRIP, we see that they always have the same

suffix for those involving 270029:

12956 27768 270029

AS27768 belongs to Copaco S.A., the same organization that is also associated with the super prefix.

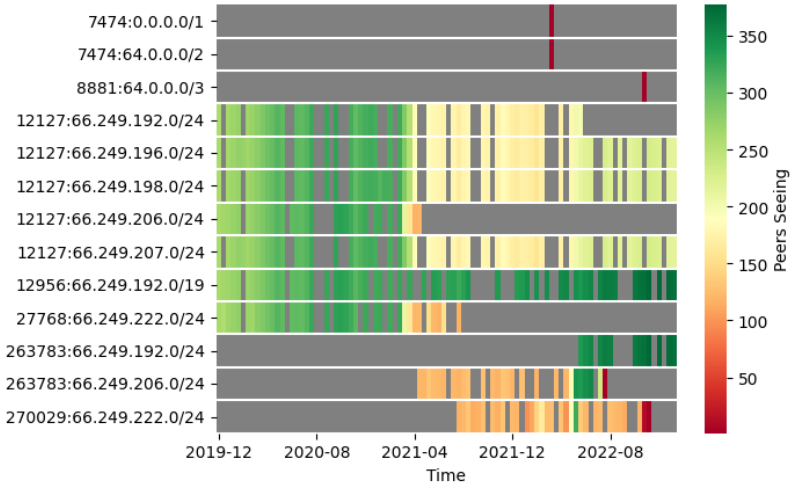


Figure 5.12: 66.249.192.0/19 Routing History

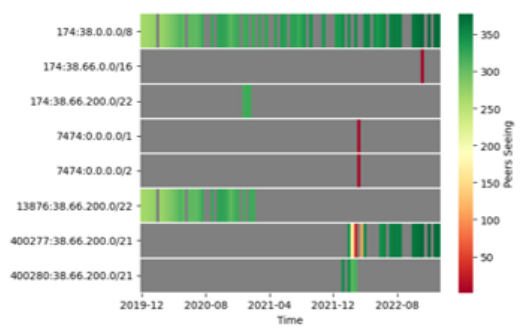
Figure 5.12 shows the routing history of the super prefix over the three years and we will point out some key observations. First, AS27768 from Copaco used to announce 66.1249.22.0/24. Second, in addition to our two protagonists, other ASes located in Latin America are also advertising /24-prefixes covered by 66.249.192.0/19: AS12127 and AS263783[9]. Both belong to Telefonica Movistar and are located in El Salvador. By looking at ARIN data for four of the prefixes still advertised today: 66.249.196.0/24, 66.249.196.0/24 and 66.249.198.0/24, 66.249.207.0/24, we found that they are all bound to both Telxius and Telefonica Movistar. Consequently, Telxius is probably leasing address space in Latin America.

In the list of recurring attackers, another AS shows evidence of IP delegation: AS174 (Cogent). During the three years, it caused 55 suspicious and unexplained events, with

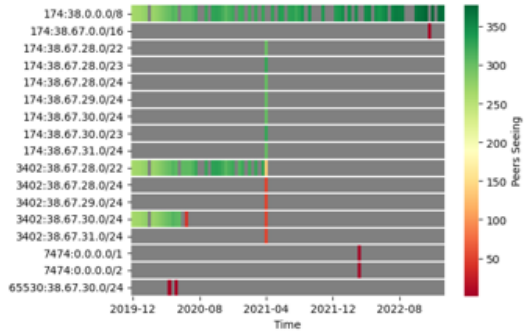
[9]They generated 421 events on GRIP.

some of them involving prefixes owned by Cogent. The most notable one is 38.0.0.0/8:

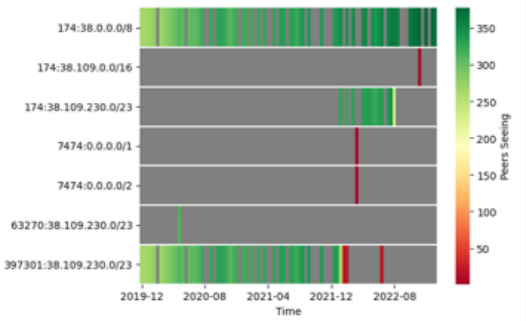
- NetName: COGENT-A
- OriginAS: AS174
- Organization: PSINet, Inc.[10]



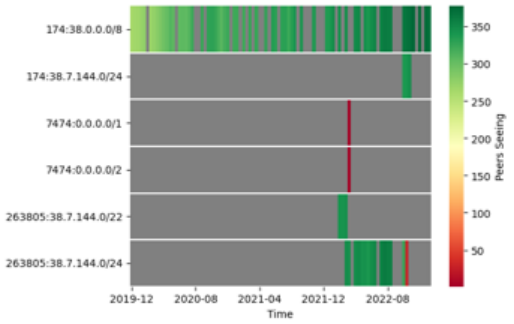
(a) Victim: 13876 prefix:38.66.200.0/22



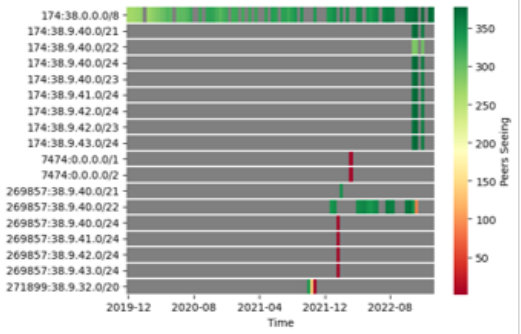
(b) Victim: 3402 prefix:38.67.28.0/22



(c) Victim: 397301 prefix:38.109.230.0/23



(d) Victim: 263805 prefix:38.7.144.0/24



(e) Victim: 269857 prefix:38.9.40.0/22

Figure 5.13: Routing History of Prefixes Covered by 38.0.0.0/8 and Involved in AS174 Events

[10]PSI Net used to be a Tier 1 ISP, it was acquired by Cogent in 2002 [53].

This prefix is involved in 5 MOAS that we collected and all have the same scenario: the "victim" (in the event) was announcing the prefix before the event, and then AS174 starts announcing it and the victim stops more or less quickly to advertise the prefix. Figure 5.13 shows the routing history of each of these prefixes. It looks like AS174 is intentionally advertising the prefix, and thus creating a MOAS situation, to state the end of the IP prefix delegation.

More generally, AS174 caused 13,502 events between January 1, 2020, and January 1, 2023, and in 10,292 of them, a prefix covered by 38.0.0.0/8 is involved. To put it differently, around 76% of the events caused by AS174 are potentially due to IP prefix delegation. However, to validate this hypothesis, we would need further investigation or even validation by Cogent itself.

IP leasing

IP leasing is another form of IP address transfer in which the organization leasing its IP space remains the official owner of it in RIR databases. Organizations wishing to lease some address space can contact an *IP broker*, a third-party company whose aim is to find customers for the IP. A well-known example of an IP broker is IPXO [54] and one of their AS, AS834, ended up in our list.

First of all, as we can read on their official website [55]: "subnets added to the IPXO Marketplace are announced from the IPXO's ASN (AS834)", but also "By announcing subnets from our trusted AS834, we establish a secure routing infrastructure". In other words, AS834 is announcing every /24-prefix of the IPXO marketplace to protect them against subMOAS. Around 65% of the events involve a /24-prefix, meaning that the victims of these events are potentially IPXO's customers, either leasers or buyers. Again, we would need further investigation and validation by IPXO itself.

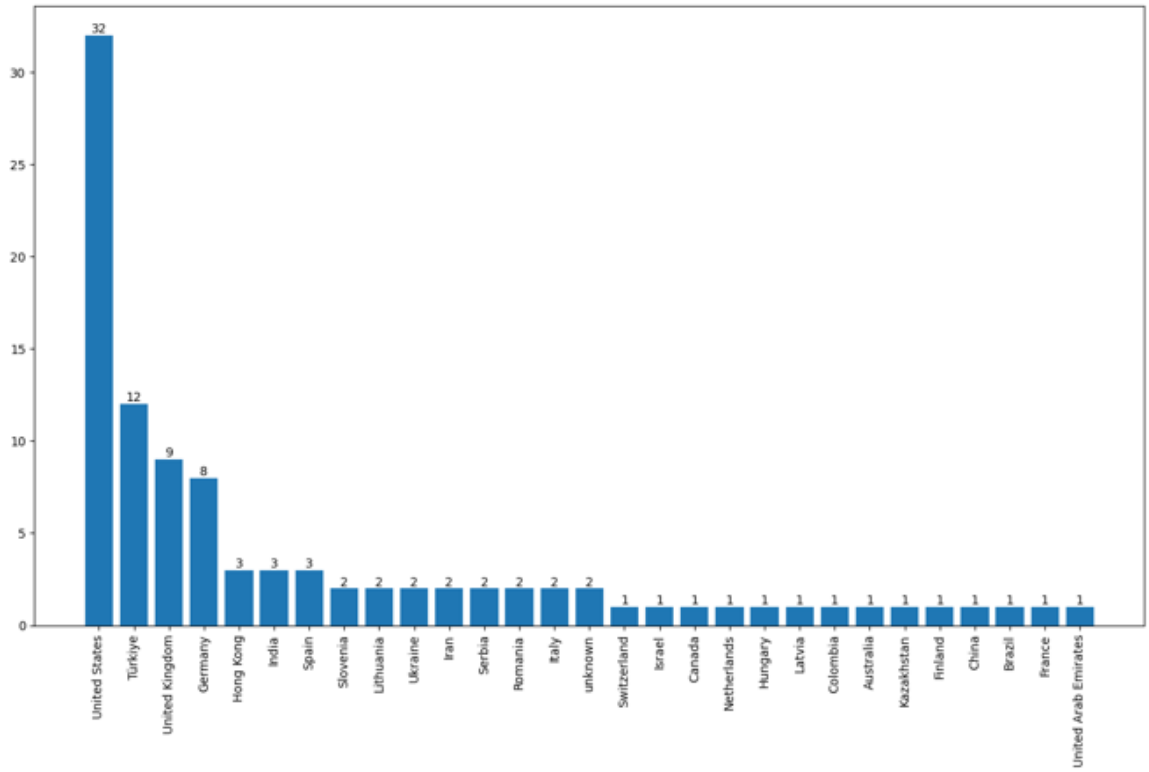


Figure 5.14: AS834 Victims Countries

Figure 5.14 shows the supposed nationality of the ASes causing conflicts. Half of these countries belong to the top 10 IPXO IPv4 Lessor Countries and/or the top 10 IPXO IPv4 Lessee Countries according to [56], meaning the ASes located in these countries are probably IPXO customers. This would also need IPXO validation. Among the rest of the countries, notice that a lot are from Eastern Europe: Slovenia, Lithuania, Ukraine, Serbia, Romania, Hungary, and Latvia, meaning that IPXO is probably well-developed in this region. Turkey also stands out with 12 ASes. On the one hand, 10 of them have at least 5 events with AS834 spread over time. On the other hand, one is on Spamhaus ASN DROP [16] list as of today: AS208485. It belongs to Eksen Bilism, a Turkish local ISP. Spamhaus DROP list is a list of ASN that have been reported for bad activities (e.g. spam, botnet controllers, DDoS, etc.). According to the Spamhaus website: “networks are inserted in the DROP lists only after dedicated investigators and forensics specialists have gathered evidence that they are controlled by cybercrime groups or by ’bulletproof’ hosters” [57].

Eventually, AS208485 and AS834 caused 9 other events detected by GRIP and the last one happened in August 2023.

Next, assuming that all 252 distinct prefixes involved in AS834 events are due to IP lease transfer, they are not responsible for such a large number of events compared to the total events detected by GRIP. In fact, over the three years of the study, the sum of distinct events in which these prefixes were involved represents 0.03% of total events and 0.8% of suspicious and unexplained events. Furthermore, these 252 prefixes represent a total of 195,336 usable IPv4 addresses, which is about 6.4% of IPXO total market size and 8.9% of leased IPv4[11]. The next step is to see whether IPXO prefixes involved in events detected by GRIP are also involved in malicious activities such as SPAM or DDoS.

To conclude this section about IP transfer, there is a lot of room for further investigation. First, large ISP like Cogent are causing origin conflicts due to IP delegation, and we have seen in section 5.1 that there are several large ISP among our recurring attackers (GTT, Lumen, AT&T, TATA, etc.). Second, concerning the IP leasing part, we saw that *a priori* it is not responsible for too many events, however, some of them could hide malicious actors, as we saw with AS204285.

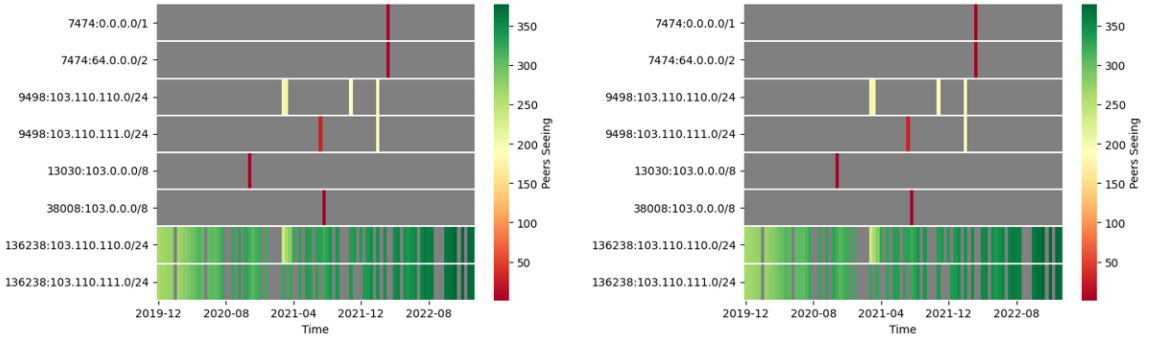
5.2.7 AS9009 and AS9498

Last but not least, it seemed important to reserve a part for ASes tagged as *serial hijackers* and to report what GRIP has seen about them.

First, AS9498 belongs to Bharti Airtel, one of the world's largest mobile networks with over 490 million customers across the world and ranked 23rd in the CAIDA AS rank dataset. Between 2015 and 2019, AS9498 has often been reported in NANOG threads [58, 59, 60, 61, 62, 63], which earned them a place on the ground truth serial hijackers list. In all cases, operators mentioned *route leaks* instead of hijacking for malicious purposes. More precisely, it was either filter errors causing the advertisement of routes that did not respect

[11] In January 2023, IPXO market size was 3,040,256 IPv4 address for a total of 2,190,080 leased IPV4[56].

BGP policies, or errors causing AS9498 to appear as the origin of several prefixes that did not belong to them. Since 2019, no new complaints regarding Airtel AS9498 behavior have been reported. Nevertheless, the AS is responsible for 2,138 events detected by GRIP between January 1, 2020, and January 1, 2023, including 101 unexplained or suspicious. In the context of this study, we only focus on the last ones, but it might be interesting to study the others as well to find any correlation. Half of the 101 events were generated with the same other origin: AS136238, a satellite ISP in the Maldives, and two prefixes: 36.255.104.0/23 and 103.110.110.0/23, both belonging to Satlink too. *A priori*, these two companies have nothing in common.



(a) 36.255.104.0/23 (b) 103.110.110.0/23

Figure 5.15: Routing History involved in conflicts generated by 9498 and 136238

Figure 5.15 shows the routing history of both prefixes. Notice that AS9498's advertisement looks short and not that visible compared to AS136238's ones. It is the same pattern with all the other prefixes involved: AS9498 only announces them for a very short time and then stops. 75% of events last less than 15 minutes. It is a type of behavior that closely resembles routing errors, especially as a large majority of the prefixes[12] they advertise are done so consistently with high visibility, not to mention that they belong to one of the world's largest mobile operators. However, we would need confirmation from the operator to be sure of this assumption.

Second, like AS9498, AS9009 was quoted in numerous NANOG threads between 2015

[12]More than 3,000 visible by RIPE collectors

and 2019, but for actions more suspicious than configuration errors [64]. Among its most notable feats, AS9009 provided transit for one of the AS belonging to the "hijack factory" mentioned in the introduction [65]. Moreover, unlike AS9498, some operators have been complaining about AS9009 again since 2019, about IP squatting and spam [66, 67, 68, 69]. The latter is not in the scope of our study as IP squatting is about advertising IP space not already announced, while the former could be, but the thread dates from 2024. Like Bharti Airtel, M247 (i.e. AS9009's organization) is a legitimate company, and it provides hosting services. It has advertised more than 4,400 prefixes, constantly for the majority of them, and with high visibility. In addition, it is also peering with one of Routeviews collectors as we saw in section 5.1. However, some of its servers have been used with malicious intentions as has been highlighted in NANOG threads. In the GRIP database, the AS has 6,938 events during the three years, including 112 suspicious or unexplained.

As we can see from Figure 5.16, the prefixes involved have different routing histories:

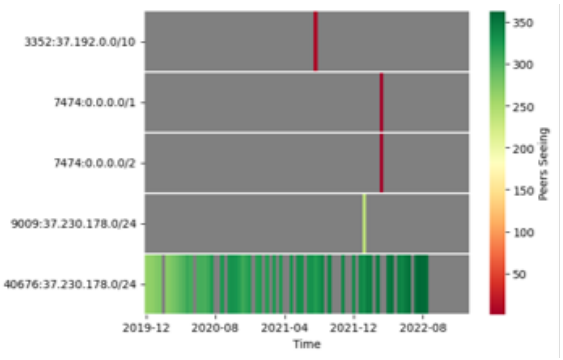
- From a) to c), we get the impression that the ads are rather unstable and there are frequent changes of ownership
- From d) to e), the advertisements are more stable

This supports our hypothesis that AS9009 is not malicious overall, but that there may be some M247 customers with access to the ASN who are using it for malicious purposes. However, we do not have enough elements to validate this assumption with certainty for the moment.

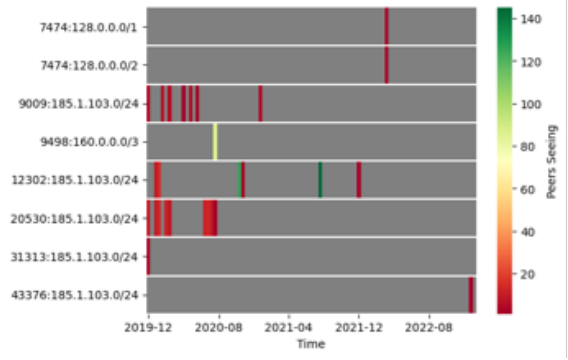
5.3 Conclusion

These initial investigations give us an overview of the networks that regularly cause GRIP conflicts. The cases of private ASN and siblings have been added to the whitelists already maintained for these specific cases. However, for the other cases, there are as yet no tags

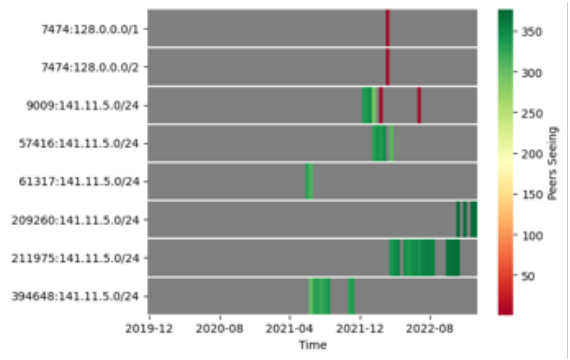
and therefore no inference rules to classify them properly. In the next chapter, we discuss potential solutions for improving GRIP classification system.



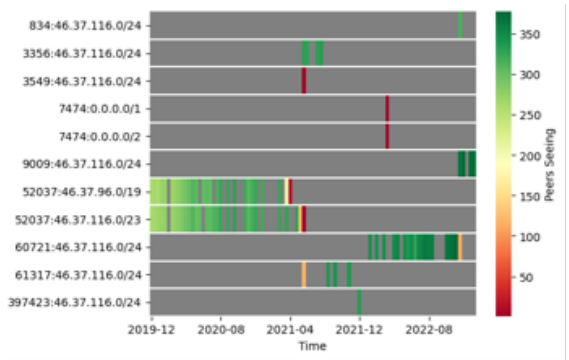
(a) Victim: 40676 prefix:37.230.178.0/24



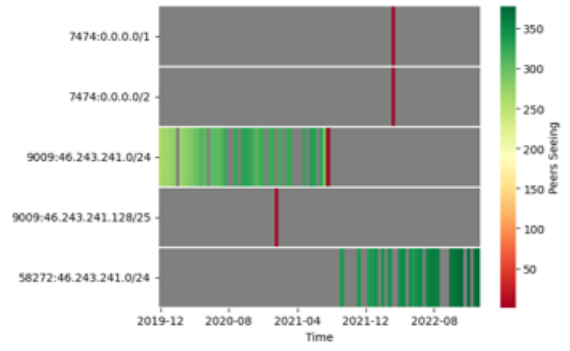
(b) Victim: 20530 prefix:185.1.103.0/24



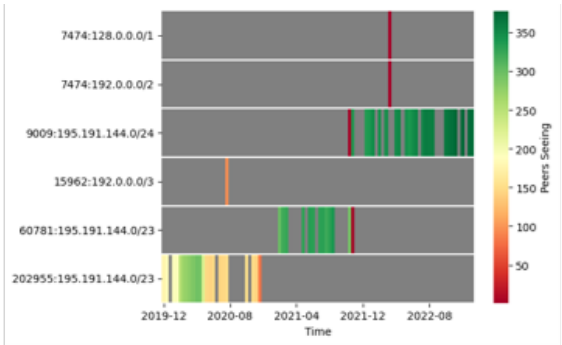
(c) Victim: 57416 & 211975 prefix:141.11.5.0/24



(d) Victim: 60721 prefix:46.37.113.0/24



(e) Victim: 58272 prefix:46.243.241.0/24



(f) Victim: 60781 prefix:195.191.144.0/24

Figure 5.16: Routing History of Some Prefixes Involved in AS9009 Events

CHAPTER 6
DISCUSSION

In this chapter, we discuss the main takeaways and limitations of our work, as well as future work.

We identified 47 ASes that have been persistently causing origin conflicts detected by GRIP between January 1, 2020, and January 1, 2023. This is the first time that a large number of events detected by the platform have been studied from the perspective of the Autonomous System causing the recurrent conflicts. First of all, we found that most of them are ISP or hosting providers located in the United States. Second, we observed that some of these networks always caused conflicts with the same other origins, potentially implying a business relationship between the multiple origins. Third, we saw that despite their adherence to the MANRS initiative, some ASes were regularly causing origin conflicts; while others, despite numerous complaints by network operators in the NANOG mailing list over the past 10 years, continued to cause conflicts. These observations are unseen and could be used as new tags to enrich GRIP characterization step.

Through an in-depth investigation of a dozen networks that cause persistent origin conflicts in BGP, we were able to provide explanations for most of the origin conflicts. First, we observed already-known situations, such as private ASNs, Internet exchange point prefixes, multi-homing, and sibling origins. Then, we saw an AS known for offering DDoS mitigation services and causing a large number of MOAS with invalid RPKI announcements, which raises the question about the interaction between DDoS solutions using BGP and RPKI. Similarly, we also observed several conflicts where one of the origins provides IP transit to the other origin according to the CAIDA AS relationships dataset, but at the same time, the announcements of at least one of the origins are RPKI invalid. For the moment, GRIP considers all these cases as suspicious, because the RPKI system is more

reliable than the CAIDA dataset. However, it may be appropriate to proceed on a case-by-case basis in the future. Indeed of the 1176 MOAS conflicts involving the same prefix, 44% of them are caused by 19 ASes that could be manually investigated. Finally, we noticed that the origin changes detected by GRIP captured changes in IP ownership, whether due to IP delegation or IP leasing. For the first time, we are observing inter-ASes business relationships through the lens of origin conflicts.

About these inter-ASes business situations, notice that they do not necessarily imply a BGP connection between the multiple origins involved in the conflict. For instance, in the case of hosting companies, it is possible that the AS providing hosting services and the customer AS have no BGP connections, so it would be impossible to see them side by side on AS paths collected by Routeviews and RIPE RIS collectors. Given that GRIP uses the CAIDA AS Relationships dataset to infer a potential relationship between origins, and that relationships of this dataset are deduced from the observation of adjacent ASN in AS paths [70], it is clear that GRIP is missing some of the business relationships that can cause origin conflicts. A first step towards solving this problem could be to build inference rules based on the historical data generated by GRIP over the last 5 years. For example, if two ASes are regularly causing origin conflicts, they are probably in a business relationship.

Although these initial observations using GRIP data are encouraging, our current approach has its limitations. The main one encountered during this study was efficiency. As our investigation method was half manual, gathering information cost us a great deal of time and prevented us from investigating more events. However, this work is a first step, and we aim to automate the research process further. In particular, we noticed that most of our assumptions are based on what we observed from the routing history of prefixes or ASes. Thus, the first step would be to characterize the global routing behavior of an AS or a prefix. Examples of features have already been covered in [2] and could be a good start. Next, we could add new features from the observation of AS paths using BGPStream [71].

CHAPTER 7
CONCLUSION

This study is a first look at Autonomous Systems causing persistent BGP origin incidents. We used GRIP, a BGP monitoring software that detects two types of origin conflicts: MOAS and subMOAS, and then classifies them using static rules. In this work, we focused on events not matching any of these rules - unexplained - or events involving an RPKI invalid announcement from the newcomer - suspicious. Then, we combine GRIP data with other data sources such as RIPE Stat to investigate the ASes causing the most suspicious or unexplained events.

First of all, we observed that most of our recurring attackers are actually American ASes and mostly classified as either *isp* or *hosting*. Then, we noticed some recurring attackers always caused events with the same victim, making the events probably legitimate. Among these ASes, we first observed that some of them were caused by Internet exchange prefixes, that are likely to be announced by multiple origins. Secondly, we saw that some ASes were probably using AS65535 as a private ASN and sometimes accidentally leaked an announcement with that ASN in the AS path. Next, we observed a use case of an AS providing DDoS protection services. Interestingly, AS19905's announcements were RPKI invalid and we conjectured that this could perhaps slow down mitigation. We also went through some examples involving either siblings or customer-provider relationships. In addition, we have shown some examples of IP transfer, including the case of AS174, which seems to cause many of the events detected by GRIP. Eventually, we showed two slightly more suspicious cases: AS9009 and AS9498, two ASes already spotted by Testart *et al.* [2]. However, it is important to note that these two ASes belong to legitimate companies: one of the largest mobile network operators in the world and a big hosting provider in Europe. For the case of Bharti, there seems to be a lot of configuration errors, while for M247, it

might be due to malicious customers.

To conclude, we identify three benefits from this thesis. First, we presented new insights concerning Autonomous Systems regularly causing origin conflicts in the global routing table. Next, we present suggestions for improving GRIP, in particular its classification system. Finally, we pave the way for new research on the subject of origin conflicts.

REFERENCES

[1] C. Cimpanu, "Klayswap crypto users lose funds after bgp hijack," *The record*, Feb. 13, 2022.

[2] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark, "Profiling bgp serial hijackers: Capturing persistent misbehavior in the global routing table," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 420–434.

[3] Q. Jacquemart, G. Urvoy-Keller, and E. Biersack, "A longitudinal study of bgp moas prefixes," in *Traffic Monitoring and Analysis: 6th International Workshop, TMA 2014, London, UK, April 14, 2014. Proceedings 6*, Springer, 2014, pp. 127–138.

[4] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding bgp misconfiguration," *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 3–16, 2002.

[5] A. Toonk, "Massive route leak causes internet slowdown," *BGPmon*, Jun. 15, 2015.

[6] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, "Bgp hijacking classification," in *2019 Network Traffic Measurement and Analysis Conference (TMA)*, IEEE, 2019, pp. 25–32.

[7] J. A. Hawkinson and T. J. Bates, *Guidelines for creation, selection, and registration of an Autonomous System (AS)*, RFC 1930, Mar. 1996.

[8] X. Zhao *et al.*, "An analysis of bgp multiple origin as (moas) conflicts," in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, 2001, pp. 31–35.

[9] K.-W. Chin, "On the characteristics of bgp multiple origin as conflicts," in *2007 Australasian Telecommunication Networks and Applications Conference*, IEEE, 2007, pp. 157–162.

[10] IETF, *Secure inter-domain routing (sidr)*.

[11] T. Chung *et al.*, "Rpki is coming of age: A longitudinal study of rpki deployment and invalid route origins," in *Proceedings of the Internet Measurement Conference*, 2019, pp. 406–419.

[12] G. T. I. I. Lab, *Global routing intelligence platform (grip)*.

[13] University of Oregon, *Routeviews project*.

[14] RIPE, *Routing information service (ris)*.

[15] G. T. I. I. Lab, *Bgpview*.

[16] Spamhaus, *Spam as drop list*.

[17] Merit, *List of internet routing registries*.

[18] CAIDA, *As rank*, https://doi.org/10.21986/CAIDA.DATA.AS-RANK.

[19] I. I. Japan, *Hegemony score*.

[20] IANA, *Autonomous system numbers*.

[21] IANA, *Ipv4 special-purpose address registry*.

[22] Y. Rekhter, S. Hares, and T. Li, *A Border Gateway Protocol 4 (BGP-4)*, RFC 4271, Jan. 2006.

[23] L. Gao and J. Rexford, "Stable internet routing without global coordination," *IEEE/ACM Transactions on networking*, vol. 9, no. 6, pp. 681–692, 2001.

[24] NIST, *Rpki monitor*.

[25] T. Holterbach, T. Alfroy, A. Phokeer, A. Dainotti, and C. Pelsser, "A system to detect forged-origin bgp hijacks,"

[26] A. Pilosov and T. Kapela, "Stealing the internet: An internet-scale man in the middle attack," *NANOG-44, Los Angeles, October*, pp. 12–15, 2008.

[27] R. NCC, *Rpki snapshots*.

[28] CAIDA, *As relationships dataset*.

[29] CAIDA, *Inferred as to organization mapping dataset*.

[30] RIPE, *Ripestat*.

[31] IPinfo, *Official website*.

[32] Abdullah, "How do we classify asn types?" *IPinfo Community*, Aug. 1, 2023.

[33] MANRS, *Official website*.

[34] *Telstra incident detected by grip*.

[35] M. Duffell, "An update on our september 30 bgp issue," *Telstra Exchange*, Oct. 2, 2020.

[36] University of Oregon, *Routeviews peers list*.

[37] RIPE, *Ris peers list*.

[38] IPGeolocation, *Country wise asn details*.

[39] IPXO, *About hivelocity*.

[40] K. International, *As286 status information*.

[41] IPinfo, *Information about united-states*.

[42] NANOG, *Nanog mailing list and archives*.

[43] J. Mitchell, *Autonomous System (AS) Reservation for Private Use*, RFC 6996, Jul. 2013.

[44] IANA, *Border gateway protocol (bgp) well-known communities*.

[45] A. Abhashkumar *et al.*, "Running {bgp} in data centers at scale," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 65–81.

[46] P. Johnson, "Neustar highlights rise in ransom-related ddos attacks and greater use of existing attack vectors," *Neustar Newsroom*, Jan. 28, 2021.

[47] Neustar, *Ultraddos protect faq*.

[48] P. Johnson, "Ddos attacks increase by 151% in first half of 2020," *Neustar Newsroom*, Sep. 16, 2020.

[49] TCUS, *Taiwanese comprehensive university system*.

[50] K. Much, "Alorica to acquire egs to provide exponentially more scalable customer experience solutions on a global scale for the world's leading brands," *Alorica, In the News*, Jun. 2, 2016.

[51] Alorica, *Take a trip with us… to the philippines!*

[52] Alorica, *The alorica philippines advantage*.

[53] Cogent, "Cogent communications acquires u.s. operations of psinet," *Cogent, News*, Apr. 2, 2002.

[54] IPXO, *Official website*.

[55] A. Srėbaliūtė, "2022 ipxo highlights: Accomplishments and milestones," *IPXO, Blog*, Dec. 14, 2022.

[56] IPXO, *Ip leasing market statistics*.

[57] Spamhaus, *Do not route or peer*.

[58] J. Bensley, *Wrong use of 100.64.0.0/10*, Oct. 2, 2015.

[59] A. Toonk, *Route leaks from as9498 (bharti airtel)?* Nov. 6, 2015.

[60] G. W. Herbert, *As9498 bharti bgp hijacks*, Apr. 1, 2017.

[61] C. Hawker, *[ausnog] 103.0.0.0/10 announcement*, Dec. 21, 2017.

[62] J. Weekes, *Tata scenic routing in lax area?* Nov. 15, 2018.

[63] Bottiger, *Anyone have contacts at bharti airtel?* Dec. 6, 2019.

[64] R. F. Guilmette, *The ongoing summer of hijacks: Mnt-serversget / dnsget.top*, Aug. 9, 2018.

[65] R. F. Guilmette, *As29073, 196.16.0.0/14, level3: Why does anyone peer with these schmucks?* Aug. 14, 2017.

[66] B. Panizzon, *Anyone from as9009 / globalaxs / m247 zurich noc?* Jan. 4, 2021.

[67] R. F. Guilmette, *As28753 - leaseweb deutschland gmbh – facilitating legacy squatting?* Dec. 20, 2020.

[68] R. F. Guilmette, *Second notice: Squatting / fraud / identity theft by as13259 - delta telesystems ltd. (ru)*, Jan. 2, 2021.

[69] spamcop-top200, *Spamcop-top200 2024-04-05 : Ru(30:2_064_320); as51520/ru(10:1_055_088); 95.31.136.47(1:175_297) ru as8402*, Apr. 4, 2024.

[70] M. Luckie, B. Huffaker, A. Dhamdhere, V. Giotsas, and K. Claffy, "As relationships, customer cones, and validation," in *Proceedings of the 2013 conference on Internet measurement conference*, 2013, pp. 243–256.

[71] CAIDA, *Bgpstream, a software framework for live and historical bgp data analysis*.