Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP

Leo Oliver
University of Waikato
Hamilton, New Zealand
leo@oliver.nz

Gautam Akiwate
UC San Diego
La Jolla, CA, USA
gakiwate@cs.ucsd.edu

Matthew Luckie
University of Waikato
Hamilton, New Zealand
mjl@wand.net.nz

Ben Du
UC San Diego
La Jolla, CA, USA
bendu@ucsd.edu

kc claffy
CAIDA, UC San Diego
La Jolla, CA, USA
kc@caida.org

ABSTRACT

We analyze the properties of 712 prefixes that appeared in Spamhaus' Don't Route Or Peer (DROP) list over a nearly three-year period from June 2019 to March 2022. We show that attackers are subverting multiple defenses against malicious use of address space, including creating fraudulent Internet Routing Registry records for prefixes shortly before using them. Other attackers disguised their activities by announcing routes with spoofed origin ASes consistent with historic route announcements, and in one case, with the ASN in a Route Origin Authorization. We quantify the substantial and actively-exploited attack surface in unrouted address space, which warrants reconsideration of RPKI eligibility restrictions by RIRs, and reconsideration of AS0 policies by both operators and RIRs.

CCS CONCEPTS

• **Networks → Network security**.

KEYWORDS

BGP hijack, blocklists, routing security, IRR, RPKI

ACM Reference Format:
Leo Oliver, Gautam Akiwate, Matthew Luckie, Ben Du, and kc claffy. 2022. Stop, DROP, and ROA: Effectiveness of Defenses through the lens of DROP. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3517745.3561454

1 INTRODUCTION

Malicious use of Internet address space has been a persistent threat for decades. In some cases this malicious use involves an actor falsely asserting ownership of addresses they do not in fact own. In other cases a malicious actor uses its own address space for fraudulent activity such as spam or malware distribution. They may obtain such addresses fraudulently, e.g., by forging documentation needed to procure it, or they may acquire it from hosting companies that knowingly lease address space for malicious use.

There have been at least four classes of approaches to prevent and detect address space abuse: (1) the use of blocklists [29], (2) route hijack detection [21, 23, 26, 47, 51], (3) validation against databases of address ownership such as Internet Routing Registry (IRR) databases [20] and the Resource Public Key Infrastructure (RPKI) [18], and (4) authentication of the AS path announcement, not just the origin network [7, 19].

We undertook a study of the effectiveness of IRR and RPKI, through the lens of one of the most respected blocklists on the Internet: Spamhaus' Don't Route Or Peer (DROP) list [28]. Spamhaus investigators regularly update the DROP list with IPv4 address prefixes that pose a presumed threat to the Internet community [48]. Our goal was to understand what these prefixes tell us about the effectiveness of IRR and RPKI as routing security mechanisms. We use the prefixes added to DROP over a nearly three-year period from June 2019 to March 2022. We use DROP for four reasons. First, it is well documented – each entry describes why it was added [50]. Second, it represents the most seriously abused prefixes, which Spamhaus encourages operators to refuse to carry traffic to/from. Third, a human validates the decision to add blocks to the DROP list, increasing its accuracy [49]. Fourth, access to this data is free, enabling others to more easily reproduce our work.

Our findings and contributions are as follows. We show that attackers are circumventing defenses against malicious use of address space, including (1) registering IRR records for prefixes shortly before using those prefixes, (2) announcing routes with origin ASes consistent with historic route announcements, and (3) announcing routes with the RPKI-signed origin. Encouragingly, the process of an owner reclaiming their prefix and having it removed from DROP appears to have spurred RPKI adoption: prefixes removed from DROP were RPKI-signed at a higher rate (42.5%) than prefixes that were not added to DROP (22.3%). However, current Regional Internet Registry (RIR) policy around issuing and using Route Original Authorizations (ROAs) for unallocated address space provides a vulnerability that attackers are exploiting, with 40 unallocated prefixes appearing on DROP during our study period. Further, of the 36.7 /8 equivalents of allocated but unrouted address space, 6.7 (18.3%) had a ROA that would allow hijacking the address space. Because deployment of AS path authentication mechanisms [7, 19] may take at least one more decade, our analysis demonstrates the

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10…$15.00
https://doi.org/10.1145/3517745.3561454

interim benefit of operators deploying RPKI policies that protect their allocated but unrouted address space from abuse, and illustrates that routing security does not stop with prefix signing, but requires active maintenance of ROAs.

2 BACKGROUND & RELATED WORK

2.1 BGP Hijacks

An AS uses the Border Gateway Protocol (BGP) to announce IP prefixes for which it has routes. Because BGP relies on trust between ASes, an AS can announce a prefix which it does not own. When an AS does so without permission (illegitimately), it is a *BGP hijack*. In 2002, accidental misconfigurations were a common type of hijack [31]. Intentional hijacks have been used for interception of traffic destined to the hijacked addresses [8], or using the addresses to send spam [42] or perform large-scale DDoS attacks [53].

In 2015, Vervier et al. [60] documented hijacks occurring regularly in the wild. They examined the BGP behavior of 437 prefixes that sent spam to spam traps under their control, and found 64 had behavior that resembled a hijack. All 64 prefixes were unannounced by their owner prior to being hijacked. For 5 of the 64 prefixes, the hijacker forged the AS path by using the ASN that previously originated the prefix as the origin of their paths, making the announcement falsely appear as if by the legitimate owner [17, 40].

In 2018, Testart et al. [52] profiled the behavior of serial hijackers – repeat offending hijacker ASes. The authors acquired a set of known hijacking ASes from network operator mailing lists to analyze the characteristics and behavior patterns of these serial hijackers and how they differed from legitimate ASes. They used this knowledge to train a classifier to infer other ASes with similar features to also be serial hijackers.

2.2 Internet Routing Registry (IRR)

In the 1990s, the network operator community created the IRR system, which enables network operators to publish address ownership and routing policy information [20]. Merit's Routing Assets Database (RADb) is the most complete IRR, mirroring various other IRRs [33]. The most important IRR record in the IRR is the *route object*, which contains the IP prefix and origin AS that a network intends to announce in BGP. Lack of incentive for network operators to maintain accurate records in IRR has reduced its utility. Worse, lack of validation of registration data renders the IRR vulnerable to abuse by attackers who can easily register false information [13, 37, 45, 54].

2.3 Resource Public Key Infrastructure (RPKI)

The integrity limitations of the IRRs ultimately led to development of the RPKI [18, 27]. RPKI supports cryptographic attestation that a network, identified by its ASN, is authorized to *originate* a route for a prefix into the global routing system (known as a *route origin authorization* or ROA). Each of the five RIRs has their own key to sign ROAs provided by their members. A ROA may contain an ASN that is permitted to originate a prefix, or AS0 if the prefix, and any more specific (contained) prefix, should not be routed. A route is *RPKI-valid* if *any* ROA asserts the announcement as valid – i.e., the origin AS matches a ROA for the prefix, and the prefix length is less than or equal to the maximum prefix length (maxLength), if the ROA contains the maxLength attribute.

Success of the RPKI at preventing origin hijacks requires two sides of participation: networks must register their own prefixes in the RPKI, and networks must drop all BGP assertions for prefixes that are not RPKI-valid. This latter practice is called *route origin validation* (ROV) and achieved by operators configuring the RIRs' Trust Anchor Locators (TALs) in their validation software.

RPKI misconfigurations may result in the flagging of legitimate announcements as invalid [61], a risk that has slowed the deployment of ROV [10]. Network operators began gradually deploying RPKI in 2011. As of March 2022, approximately 35% of observably routed prefixes have RPKI-valid announcements [36].

However, RPKI does not protect from rogue ASes performing *BGP path manipulation hijacks* [9], where a hijacker forges the legitimate owner's ASN for the origin of the prefix. In 2015, Vervier et al. highlighted that hijacks spoofing the owner's ASN are still possible with RPKI [60]. In 2016, Cohen et al. proposed *path-end validation*, where the resource owner signs the ASNs that are allowed to be adjacent to the origin in the BGP announcement [11], reducing the chance a hijacker's route is BGP-selected ahead of a legitimate announcement by the owner, when ties are broken by AS path length. In 2017, Yossi et al. illustrated that sub-prefix hijacks were still possible if an AS uses the maxLength attribute, as an attacker can announce more-specific sub-prefixes that the legitimate owner does not announce if the attacker also forges the owner's ASN [15]. They found that, in June 2017, 84% of ROAs with a maxLength longer than the prefix length were vulnerable to forged-origin sub-prefix hijacks, and as of August 2022, an Internet Draft likely to become a Best Current Practice recommends that operators do not use the maxLength attribute in their ROAs [14]. BGPsec solves these path manipulation hijacks by providing cryptographic assurance that the AS path is valid [7], but its deployment may take at least one more decade. In this work, we identify an example of a prefix hijack in the wild that was RPKI-valid.

2.3.1 AS0 Policies. Both RIRs and individual networks can create AS0 ROAs that assert a prefix, and any more specific prefix, should not be routed; these prefixes will be rejected by networks that validate routes with RPKI. Any other unrouted prefix, including those with a non-AS0 ROA, is otherwise unprotected and subject to an attacker announcing the prefix. It is best current practice for Internet exchange point (IXP) peering LAN address space to be covered by an AS0 ROA, as it should not be routed [39].

An RIR can use AS0 to assert that unallocated address space in their free pool should not be routed. Controversy over enabling RIRs to use the AS0 mechanism to effectively blocklist address space from the public Internet has limited RIR adoption of policies allowing it [32]; some critics considered it a dangerous slippery slope giving the RIRs too much operational responsibility when they were not 24x7 operations [12]. In 2019, APNIC was the first RIR to propose an *AS0 policy*. APNIC implemented an AS0 policy [4] on September 2, 2020, and LACNIC implemented an AS0 policy on June 23, 2021 [38]. RIPE NCC proposed an AS0 policy on October 22, 2019, but ultimately withdrew the proposal [1]. AFRINIC proposed an AS0 policy in November 2019, but have yet to implement it as of May 2022 [16]. ARIN has not made any AS0 proposal.

As of May 2022, only APNIC and LACNIC had implemented policies to create AS0 ROAs for unallocated address space. These

RIRs implemented their AS0 policy (1) using a different TAL that is not configured in any RPKI validation software by default, and (2) recommending the AS0 TAL be used solely for information purposes and alerting, rather than for automatic route filtering, owing to risks of unintended interruption to routing [3, 34, 35].

2.3.2 Challenges in RPKI Signing of Legacy Address Space. Legacy prefixes directly allocated to a recipient without involving an RIR have stronger property rights than operators who obtain prefixes from RIRs [30]. This leads to a tussle between legacy prefix holders and the RIRs, as RIRs are trust anchors in RPKI validation who directly sign prefixes, and control delegation to other parties who can also sign prefixes. ARIN and AFRINIC will not RPKI-sign resources unless the resource holder signs the RIR's Registration Services Agreement (RSA) [2, 6]. APNIC, LACNIC and RIPE will RPKI-sign legacy address space without the resource holder signing an RSA, provided the legacy resource holder can prove their ownership of the resource [24, 25, 43, 46]. These ARIN and AFRINIC policies have limited RPKI-signing of legacy space in those regions [62].

3 DATA SETS

In addition to the Spamhaus DROP blocklist data set, we use four additional data sources to support analysis and interpretation of the blocklist data. We use **BGP announcement** data recorded by all 36 RouteViews collectors. We use Merit's archives of the **RADb IRR** [41] and RIPE's daily **RPKI ROA archive** [44] to extract route objects and ROAs related to prefixes on the date each appeared on DROP. Finally, each RIR publishes and archives daily **"RIR stats"** file snapshots of the status of Internet number resources [5], which we use to analyze allocation status of DROP addresses.

3.1 Spamhaus DROP and SBL

Spamhaus compiles several widely used blocklists, including the Don't Route Or Peer (DROP) list of IPv4 prefixes that Spamhaus deems pose a threat to Internet users [48]. Spamhaus manually confirms serious evidence of malicious activity before adding a prefix to the list [49]. Finally, Spamhaus maintains the Spamhaus Block List (SBL) database, which documents why they added a prefix to the list [50].

We used daily snapshots of the DROP list compiled by Firehol over a nearly three-year period from June 2019 to March 2022 [55]. We processed the SBL record (which is freeform text) for each prefix, using the semi-automated categorization process described in Appendix A, which placed each prefix into one or more of the following categories:

(1) **Hijacked (HJ)**. Prefixes an attacker obtains through fraud from an RIR or through announcing a prefix that an RIR assigned to another network.
(2) **Snowshoe Spam (SS)**. Prefixes used by spammers to send spam from many IP addresses within the prefix, to evade detection.
(3) **Known Spam Operation (KS)**. Prefixes under the control of, or otherwise connected with, a spam operation.
(4) **Malicious Hosting (MH)**. Prefixes used by bulletproof hosting services, which knowingly host malicious actors and ignore complaints [22].
(5) **Unallocated (UA)**. Prefixes that neither IANA nor an RIR has allocated to an AS, but attackers are using.

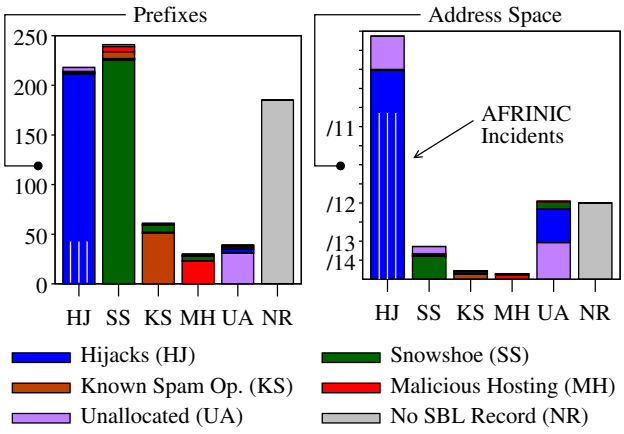

Figure 1: Classification of DROP entries by prefixes and address space. The bottom segments of the bars represent labels that Spamhaus assigned to the prefix exclusively, the segments above represent additional labels, and the vertical hatches represent the portion of *hijack* prefixes associated with AFRINIC incidents. Although prefixes with the *snowshoe* label took up nearly a third of the prefix additions to DROP, they were small prefixes and constituted only 8.5% of address space covered by DROP prefixes. In contrast, the *hijack* and *unallocated* categories had larger portions of address space.

(6) **No SBL Record (NR)**. Prefixes for which we were unable to obtain the SBL record, because Spamhaus had removed the record after the prefix holder had remediated.

We found 712 unique prefixes added to the DROP list in this period, of which 526 (73.9%) had SBL records. Figure 1 shows the category breakdown. The DROP categories show little overlap: SS prefixes show the most overlap with other categories, but only 15 such prefixes had a second classification. We also annotated each prefix with any ASNs listed in the SBL records as the "malicious ASN". We found ASNs for 190 (36.1%) of the 526 prefixes that had SBL records, 130 of which Spamhaus classified as *hijacked*.

AFRINIC Incidents. 48.8% of the DROP address space related to two isolated AFRINIC incidents of allegedly fraudulent address acquisition [56–59]. Although the 45 DROP prefixes related to both of these incidents made up only 6.3% of the prefixes that appeared on DROP, they made up 48.8% of the DROP address space. Given the size and anomalous character relative to the other prefixes, we excluded these prefixes from our analyses. Figure 1 shows the contribution of the incidents' prefixes to hijacks listed on DROP with vertical hatches identifying the portion of both HJ columns related to those incidents.

3.2 Limitations

The DROP list contains a small subset of all malicious prefixes. Other malicious prefixes, such as those listed on other blocklists or not on any blocklist at all, may have different behavior than the behavior for the DROP prefixes that we report on in this paper. Although we cannot prove causation with the available data, we reveal evidence of likely causal relationships.

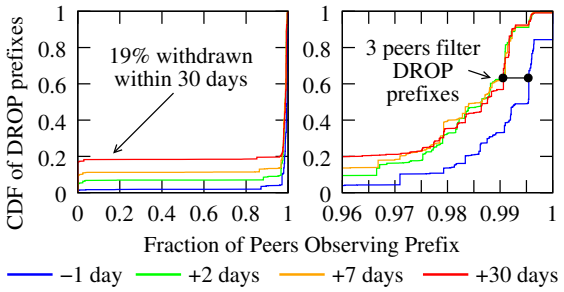

Figure 2: 19% of prefixes listed on DROP were not BGP-observed 30 days after being listed. Three RouteViews peers appeared to filter DROP prefixes from BGP announcements.

4 INFERRING EFFECTS OF BLOCKLISTING

In this section, we investigate the correlation that blocklisting has with routing visibility and RPKI uptake.

4.1 Routing Visibility

Our BGP data set provides evidence that a prefix being listed on DROP may have caused the attacker (or their transit providers) to withdraw the prefix: 19% of the prefixes on DROP during our measurement window were withdrawn within 30 days of being listed on DROP (left panel in Figure 2). For prefixes labeled *hijacked* or *unallocated* this percentage was higher: 70.7% and 54.8%, respectively. These two categories stand out as expected; prefixes in these categories were being advertised illegitimately, and illegitimate announcers likely withdrew prefixes once the addresses were less effective for their malicious applications. Further, at the transit level, we surprisingly found three RouteViews peers that provided their full tables but appeared to use the DROP list to filter BGP announcements (right panel in Figure 2). We contacted operator contacts at each of the three ASes, and received a response from one, who confirmed that they filtered out prefixes on the DROP list. The categories with low fractions of prefixes that were withdrawn from BGP contained mostly prefixes that RIRs legitimately allocated to these ASes who were using them maliciously, e.g. bulletproof hosting companies.

The category with the largest percentage of address space that was deallocated by an RIR after appearing in DROP was *malicious hosting*. Of the *malicious hosting* prefixes, 17.4% were allocated when they appeared on DROP and were deallocated by the end of March 2022. A similar pattern occurred for prefixes Spamhaus removed from DROP: 8.8% of the prefixes Spamhaus removed were deallocated. Half of these prefixes Spamhaus removed within a week of an RIR deallocating them.

4.2 Improved RPKI Uptake

Table 1 examines the RPKI properties of 650 prefixes that did not have a ROA when they were added to DROP. Each region had a base level of RPKI activity, with the RIPE region having the largest fraction of unsigned prefixes whose resource holders signed them during our study. For all but AFRINIC, the signing rate of prefixes that Spamhaus removed from DROP was higher than this base level. Operators may have been motivated to deploy RPKI as part of the process of getting their prefix removed from DROP, which requires the prefix owner to prove that the problem has been resolved and will not continue, or as a measure to prevent their prefix re-appearing on DROP. The signing rate of prefixes that remained on DROP was lower than this base level, consistent with these prefixes being relatively neglected. Of the prefixes that appeared on DROP that were RPKI-signed between June 5, 2019 and March 30, 2022, the prefixes that Spamhaus removed from DROP were mostly (82.3%) signed with an ASN that was different from the ASN originating the prefix at the time the prefix appeared on DROP. Only 6.3% of prefixes that were removed from DROP that were RPKI-signed between June 5, 2019 and March 30, 2022 were signed with an ASN the same as the ASN originating the prefix at the time the prefix appeared on DROP.

	Never on DROP	Removed from DROP	Present on DROP
AFRINIC	11.8% of 3901	14.3% of 7	0.0% of 11
APNIC	26.3% of 42.2K	44.4% of 18	21.6% of 37
ARIN	8.5% of 65.2K	25.0% of 40	0.6% of 169
LACNIC	25.5% of 15.1K	35.1% of 37	0% of 9
RIPE NCC	33.0% of 68.2K	54.2% of 83	19.8% of 172
Overall	22.3% of 195.6K	42.5% of 186	13.8% of 420

Table 1: RPKI signing rate of prefixes without a ROA that Spamhaus added to DROP between June 5, 2019 and March 30, 2022. A larger fraction of prefixes had a ROA created if they were removed from DROP than if they were never on DROP for most regions. A smaller fraction of prefixes had a ROA created if they were not removed from DROP.

5 EFFECTIVENESS OF IRR

In this section, we investigate the effectiveness of the IRR by analyzing how operators and attackers both used IRR for prefixes that appeared on DROP.

In the 7-day window before appearing on DROP, 226 DROP prefixes (31.7%) covering 68.8% of the DROP address space had either a route object in the RADb IRR (§2.2) with an exact match or a more specific prefix. The RADb IRR contains evidence suggesting attackers are using IRR to make their activities appear legitimate, as 32% of the prefixes with route objects had their route object created during the month before the prefix appeared on DROP. More encouragingly, 43% of prefixes with route objects had their route object removed a month after they appeared on DROP.

Focusing on the 130 DROP prefixes whose SBL record reported the prefix as hijacked by a specific ASN, 69 (55%) either had no route object or had a route object with a different ASN from the labeled hijacking ASN. The remaining 57 prefixes (45%) had the labeled hijacking ASN in the route object, because RADb allowed the attacker to register a route object for an ASN without any authorization (§2.2). Overall, there were 13 different hijacking ASNs in the route objects for these 57 prefixes.

Of the 57 prefixes, 49 had route objects with different origin ASes but shared three different ORG-IDs, indicating the bulk of the fraudulent entries were created by three entities. One of these ORG-IDs created IRR records for 15 of the hijacked DROP prefixes, using various origin ASes. Each of these prefixes were announced shortly after the route object was created and each had a common

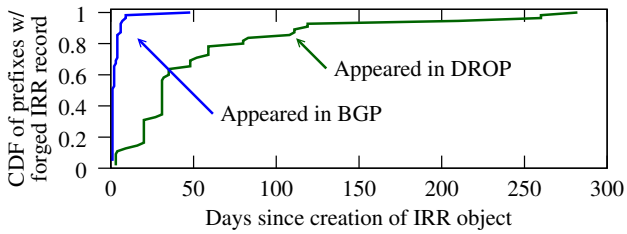

Figure 3: Other than 2 prefixes that had already been in BGP for over a year, the remaining prefixes appeared in BGP shortly after creation of the IRR record.

AS in their announced path: AS50509, which hijacked unrouted prefixes using defunct ASes as the origin, and creating IRR route objects with these defunct ASes. For all but 2 of the 57 prefixes, the hijacker AS started announcing the prefix in BGP less than a week after they created the IRR record (Figure 3). In the other 2 instances, the hijacker created the IRR record more than a year after they had already been announcing the prefix in BGP. The prefixes these hijacking ASes were targeting were all apparently abandoned, as only 5 of the prefixes had existing IRR entries prior to the DROP-labeled AS creating their entry.

We also found one prefix on DROP that was unallocated when an AS created a route object for it. No unallocated prefix should be routed, therefore unallocated prefixes should not be accepted into the IRR. The fact that it was further highlights the lack of verification performed by RADb.

6 EFFECTIVENESS OF RPKI

In this section, we investigate the effectiveness of RPKI by analyzing hijacks of RPKI-signed prefixes added to DROP. We discuss the implications of hijacks for RPKI-signed prefixes more broadly, and potential solutions such as AS0.

6.1 Evidence of RPKI-valid Hijacks

Of the 179 prefixes labeled hijacked, only three were RPKI-signed *before* they were blocklisted. We infer that hijackers do not usually target RPKI-signed prefixes but rather target unallocated or unrouted non-RPKI signed address spaces. The entity allegedly hijacking two of these prefixes appeared to control the ROA, as the ASN in the published ROAs changed when the BGP origin ASN changed in the two years prior to the prefix appearing on DROP. However, the third prefix is a real-world demonstration of the limitations in capability of the current RPKI deployment.

Consider the hijacked RPKI-signed prefix 132.255.0.0/22 illustrated in Figure 4, with a ROA authorizing AS263692 – a Peruvian network under LACNIC – to originate the prefix. While AS263692 routed the prefix via a South American transit provider (AS21575) for many years, in July 2020 it stopped *i.e.*, the prefix became unrouted. In December 2020, we see the prefix again originated by AS263692 but routed via Russian ASes AS50509 and AS34665 who had hijacked the prefix. Recall, AS50509 is also implicated in hijacking unrouted prefixes by creating IRR route objects with the defunct ASes (Section 5). Since the origin AS matched the ROA, the announcement was deemed RPKI-valid, subverting RPKI protections. On inspecting the BGP routing data for a similar pattern

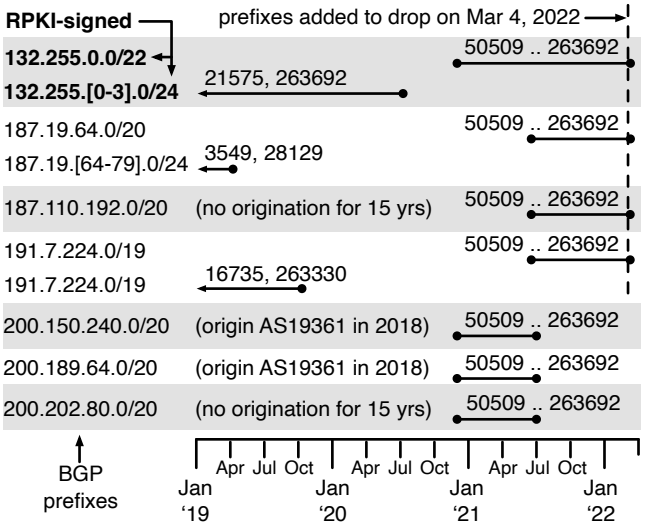

Figure 4: Case study of hijacker considering origin AS of historic BGP announcements. AS263692 is a Peruvian AS with historic transit through a South American transit provider (AS 21575) and one RPKI-signed prefix: 132.255.0.0/22. In December 2020, a hijacker begins BGP-announcing that prefix, along with prefixes historically unrouted or originated with a different ASN, with further announcements in June 2021, through a Russian transit provider (AS 50509).

– originated by AS263692 and routed via AS50509 – we find six additional non-RPKI signed prefixes (Figure 4). Of these six, three prefixes were added to DROP by Spamhaus.

To prevent hijacks of unrouted RPKI-signed prefixes, the ROA should use AS0 as the authorized origin. As such, the underlying reason why the hijack of 132.255.0.0/22 was successful was because not only did the AS not route the prefix, but the ROA contained a non-AS0 ASN. This hijack is a real-world demonstration that that any *unrouted* non-AS0 RPKI-signed prefixes are no better protected than non-RPKI signed prefixes. Figure 5 shows that while the amount of IPv4 address space covered by a ROA has increased, the volume of unrouted but signed prefixes has also increased, and as of March 2022, the equivalent of 6.7 /8 prefixes (≈112M IPs) are signed but not routed. While these prefixes are susceptible to hijacks, this risk could be eliminated by signing the ROAs with AS0.

Figure 5 also shows that as of March 2022, the equivalent of 30.0 /8s were allocated but unrouted and had no ROA. We examined the RIRs managing this address space, and found that the equivalent of 18.25 /8s (60.8%) was managed by ARIN. Because ARIN manages the bulk of this allocated but unrouted address space, we encourage ARIN members to develop policy that incentivizes resource holders to not only use RPKI but also issue AS0 ROAs.

6.2 AS0 Policies at Operator and RIR level

An AS0 ROA prevents unallocated or unrouted address space from being routed [18] (Section 2.3). Given the potential for AS0 policies to considerably reduce the attack surface in today's routing system, we discuss the different policy considerations and challenges at the operator and RIR level.

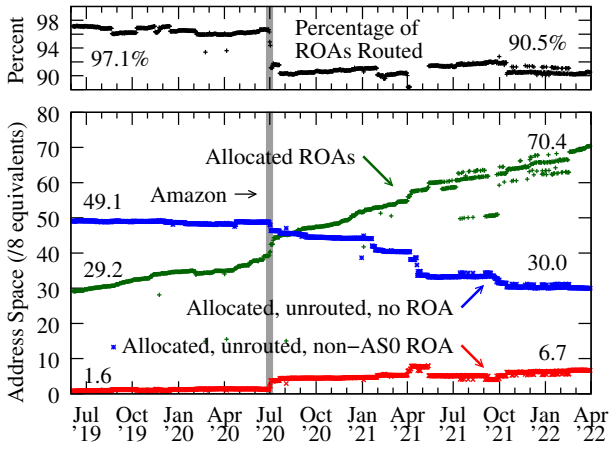

Figure 5: Routing status of ROAs. The majority of ROAs were routed, though the percentage of signed address space routed declined from 97.1% to 90.5%. Address space equivalent to 6.7 /8s was signed with a non-AS0 ROA and unrouted as of March 2022.

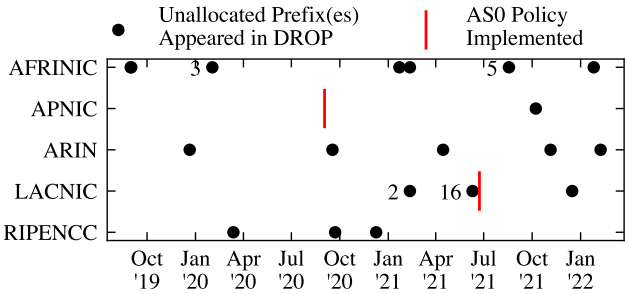

Figure 6: Timeline of when address space unallocated by RIRs appeared on DROP, and when an AS0 policy was implemented by an RIR. In practice, the ability of an attacker to hijack an unallocated prefix is not affected by the RIRs' current AS0 policies.

6.2.1 Operator AS0. While there was the equivalent of 6.7 /8s unrouted and covered by a non-AS0 ROA (Figure 5) the bulk of this address space (70.1%, the equivalent of 4.7 /8s) was held by three organizations: Amazon with the equivalent of 3.1 /8s (ROA creation event labeled in Figure 5), Prudential Insurance with one unrouted /8, and Alibaba with the equivalent of 0.64 /8s. As such, a few organizations adopting AS0 could remediate the majority of the attack surface.

Notably, one DROP prefix was RPKI-signed with an AS0 ROA by a network operator. Spamhaus added 45.65.112.0/22 to DROP on January 28, 2020. The operator signed it with AS0 on May 5, 2021, and Spamhaus removed it from DROP on June 16, 2021.

The most likely reason that the unannounced hijacked address space that appeared on DROP never got signed with AS0 is because the address space was abandoned with no one to sign it. Another reason operators may hesitate to RPKI-sign their unused address space with AS0 is because it indicates to RIRs that address space is not being used, and RIRs have historically sought to reclaim IP address space.

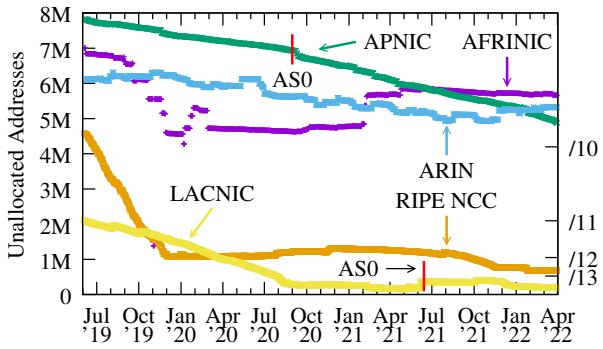

Figure 7: Amount of unallocated address space remaining in each RIR's free pool, over time. AFRINIC and ARIN have the most unallocated address space not covered by an AS0 ROA.

6.2.2 RIR AS0. RIRs can create AS0 ROAs for unallocated prefixes, although (1) only APNIC and LACNIC have implemented policies to enable these AS0 ROAs, (2) those RIRs use different TALs that are not configured in any RPKI validation software by default, and (3) those RIRs recommend operators do not automatically filter routes using those TALs (§2.3.1). For these reasons, hijacks of unallocated address space continued beyond the implementation of an AS0 policy. From the period of June 5, 2019 to March 30, 2022, 40 unallocated prefixes appeared on DROP (Figure 6), with events clustered for LACNIC (19) and AFRINIC (12) resources. The size of these clusters is not correlated with the amount of unallocated address space remaining in the RIRs (Figure 7). We examined RouteViews tables for peers that provided a full routing table on March 30, 2022, and found no evidence that any of them used APNIC or LACNIC AS0 TALs to filter routes, as every peer reported ≈30 prefixes that would have been filtered with those TALs.

7 CONCLUSION

We used 712 prefixes from the last three years of Spamhaus' DROP list as a lens to analyze IP address abuse risks and mitigations. We found that blocklisting may have had an effect on the prefixes – a hijacked or unallocated prefix added to the DROP list led to most attackers withdrawing those routes, and prefixes that were blocklisted were more likely to adopt RPKI than prefixes that were not. We also presented evidence that illustrates the hijack risk to *all* unrouted RPKI-signed prefixes, equivalent to 6.7 /8s *i.e.*, ≈112M IPs. While unrouted RPKI-signed prefixes can use AS0 ROAs to prevent hijacks, the unrouted unsigned prefixes (equivalent to 30.0 /8s *i.e.*, ≈480M IPs) will continue to be easy targets for hijackers. As such, our results indicate that policies concerning RPKI, and AS0 more specifically, merit re-evaluation by both operators and RIRs.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their feedback. Leo Oliver was supported by the Sir William Gallagher Cyber Security Scholarship at the University of Waikato. This work was partly supported by U.S. NSF awards OAC-2131987 and CNS-2120399; this work does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred.

REFERENCES

[1] Melchior Aelmans, Martijn Schmidt, and Massimiliano Stucchi. 2019. Slurm file for unallocated and Unassigned RIPE NCC Address Space. https://www.ripe.net/participate/policies/proposals/2019-08

[2] AFRINIC. 2020. Legacy resource holders. https://afrinic.net/membership/legacy-resource

[3] APNIC. 2020. Important notes on the APNIC AS0 ROA. https://www.apnic.net/community/security/resource-certification/apnic-limitations-of-liability-for-rpki-2/.

[4] APNIC. 2020. Prop-132: RPKI ROAs for Unallocated and Unassigned APNIC Address Space (Was: AS0 for Bogons). https://www.apnic.net/community/policy/proposals/prop-132.

[5] APNIC. 2022. RIR statistics exchange format. https://www.apnic.net/about-apnic/corporate-documents/documents/resource-guidelines/rir-statistics-exchange-format/.

[6] ARIN. 2022. Services available to organizations holding Legacy Resources. https://www.arin.net/resources/guide/legacy/services/

[7] Rob Austein, Steven Bellovin, Russ Housley, Stephen Kent, Warren Kumari, Doug Montgomery, Chris Morrow, Sandy Murphy, Keyur Patel, John Scudder, Samuel Weiler, Matthew Lepinski, and Kotikalapudi Sriram. 2017. BGPsec Protocol Specification. RFC 8205.

[8] Hitesh Ballani, Paul Francis, and Xinyang Zhang. 2007. A Study of Prefix Hijacking and Interception in the Internet. In *SIGCOMM*. 265–276.

[9] Shinyoung Cho, Romain Fontugne, Kenjiro Cho, Alberto Dainotti, and Phillipa Gill. 2019. BGP Hijacking Classification. In *TMA*. 25–32.

[10] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, and Nick Sullivan. 2019. RPKI Is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *IMC*. 406–419.

[11] Avichai Cohen, Yossi Gilad, Amir Herzberg, and Michael Schapira. 2016. Jumpstarting BGP Security with Path-End Validation. In *SIGCOMM*. 342–355.

[12] Owen DeLong. 2019. prop-132-v002: AS0 for Bogons. https://mailman.apnic.net/mailing-lists/sig-policy/archive/2019/08/msg00064.html

[13] Ben Du, Gautam Akiwate, Thomas Krenc, Cecilia Testart, Alexander Marder, Bradley Huffaker, Alex C Snoeren, and KC Claffy. 2022. IRR Hygiene in the RPKI Era. In *PAM*. 321–337.

[14] Y. Gilad, S. Goldberg, K. Sriram, J. Snijders, and B.Maddison. 2022. The Use of maxLength in the RPKI. https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-rpkimaxlen-15.

[15] Yossi Gilad, Omar Sagga, and Sharon Goldberg. 2017. MaxLength Considered Harmful to the RPKI. In *CoNEXT*. 101–107.

[16] Frank Habicht, Mark Elkins, Jordi Palet Martinez, and Haitham El Nakhal Hytham. 2022. RPKI ROAs for Unallocated and Unassigned AFRINIC Address Space (Draft 3). https://afrinic.net/policy/proposals/2019-gen-006-d3

[17] Xin Hu and Z. Morley Mao. 2007. Accurate Real-time Identification of IP Prefix Hijacking. In *IEEE S&P*. 3–17.

[18] Geoff Huston and George G. Michaelson. 2012. Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs). RFC 6483.

[19] Geoff Huston, Mattia Rossi, and Grenville Armitage. 2011. Securing BGP — A Literature Survey. *IEEE Communications Surveys Tutorials* 13, 2 (2011), 199–222.

[20] IRR. 2022. Internet Routing Registry. https://www.irr.net/.

[21] Varun Khare, Qing Ju, and Beichuan Zhang. 2012. Concurrent Prefix Hijacks: Occurrence and Impacts. In *IMC*. 29–36.

[22] Maria Konte, Roberto Perdisci, and Nick Feamster. 2015. ASwatch: An AS Reputation System to Expose Bulletproof Hosting ASes. In *SIGCOMM*. 625–638.

[23] Christopher Kruegel, Darren Mutz, William Robertson, and Fredrik Valeur. 2003. Topology-Based Detection of Anomalous BGP Messages. In *RAID*. 17–35.

[24] LACNIC. 2022. LACNIC Legacy resources. https://www.lacnic.net/660/2/lacnic/legacy-resources

[25] LACNIC. 2022. LACNIC RPKI. https://www.lacnic.net/640/2/lacnic/resource-certification-system-rpki

[26] Mohit Lad, Dan Massey, Dan Pei, Yiguo Wu, Beichuan Zhang, and Lixia Zhang. 2006. PHAS: A Prefix Hijack Alert System. In *USENIX Security*.

[27] Matt Lepinski and Stephen Kent. 2012. An Infrastructure to Support Secure Internet Routing. RFC 6480.

[28] Vector Guo Li, Gautam Akiwate, Kirill Levchenko, Geoffrey M. Voelker, and Stefan Savage. 2021. Clairvoyance: Inferring Blocklist Use on the Internet. In *PAM*. 57–75.

[29] Vector Guo Li, Matthew Dunn, Paul Pearce, Damon McCoy, Geoffrey M. Voelker, Stefan Savage, and Kirill Levchenko. 2019. Reading the Tea Leaves: A Comparative Analysis of Threat Intelligence. In *USENIX Security*. 851–867.

[30] Marc Lindsey. 2010. Protect Your Pre-1997 IP Address. https://www.computerworld.com/article/2514777/protect-your-pre-1997-ip-address.html.

[31] Ratul Mahajan, David Wetherall, and Tom Anderson. 2002. Understanding BGP Misconfiguration. In *SIGCOMM*. 3–16.

[32] Augusto Luciano Mathurin. 2020. What's the AS0 ROA Policy, and What Should I Know as a Network Operator? https://www.manrs.org/2020/12/whats-the-as0-roa-policy-and-what-should-i-know-as-a-network-operator/.

[33] Merit Network. 2021. The Internet Routing Registry - RADb. https://www.radb.net/

[34] George Michaelson. 2020. Demystifying AS0. https://conference.apnic.net/52/assets/files/APBS588/demystifying-as0.pdf.

[35] George Michaelson. 2020. The two types of AS0. https://blog.apnic.net/2020/11/23/the-two-types-of-as0/.

[36] NIST. 2022. RPKI Monitor. https://rpki-monitor.antd.nist.gov/.

[37] Ostap Efremov. 2021. 196.52.0.0/14 revoked, cleanup efforts needed. RIPE NCC Anti-Abuse Working Group. https://www.ripe.net/participate/mail/forum/anti-abuse-wg/PENBT0dHenF6bUcwd1VOYnNZbz1oamQ9K1JjTmFvc09XR0xOMGpxV0JnVEpteFBocFItQUBtYWlsLmdtYWlsLmNvbT4=

[38] Ricardo Patara and Aftab Sidiqui. 2020. RPKI ASN 0 ROA Policy. https://politicas.lacnic.net/politicas/detail/id/LAC-2019-12/language/en

[39] Amresh Phokeer. 2019. AS0 Support in AFRINIC RPKI. https://afrinic.net/blog/457-aso-support-in-afrinic-rpki.

[40] Jian Qiu, Lixin Gao, Supranamaya Ranjan, and Antonio Nucci. 2007. Detecting Bogus BGP Route Information: Going beyond Prefix Hijacking. In *SecureComm*. 381–390.

[41] RADb. 2022. RADb Archive. ftp://ftp.radb.net.

[42] Anirudh Ramachandran and Nick Feamster. 2006. Understanding the Network-Level Behavior of Spammers. In *SIGCOMM*. 291–302.

[43] RIPE. 2021. Resource Certification (RPKI) for Provider Independent End Users and Legacy End Users. https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/resource-certification-rpki-for-provider-independent-end-users

[44] RIPE. 2022. RIPE RPKI Archive. https://ftp.ripe.net/ripe/rpki/.

[45] Ronald F. Guilmette. 2019. Cogent & FDCServers: Knowingly aiding and abetting fraud and theft? https://mailman.nanog.org/pipermail/nanog/2019-September/102963.html

[46] Sanjaya. 2021. RPKI services now available to APNIC historical resource holders. https://blog.apnic.net/2021/03/26/rpki-services-now-available-to-apnic-historical-resource-holders/

[47] Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos, Danilo Cicalese, Alistair King, and Alberto Dainotti. 2018. ARTEMIS: Neutralizing BGP Hijacking Within a Minute. *IEEE/ACM Transactions on Networking* 26, 6 (Dec. 2018), 2471–2486.

[48] Spamhaus. 2022. DROP - Don't Route or Peer. https://www.spamhaus.org/drop/.

[49] Spamhaus. 2022. DROP (FAQ). https://www.spamhaus.org/faq/.

[50] Spamhaus. 2022. SBL - Spamhaus Blocklist. https://www.spamhaus.org/sbl/.

[51] Meenakshi Syamkumar, Ramakrishnan Durairajan, and Paul Barford. 2016. Bigfoot: A Geo-Based Visualization Methodology for Detecting BGP Threats. In *IEEE Symposium on Visualization for Cyber Security (VizSec)*. 1–8.

[52] Cecilia Testart, Philipp Richter, Alistair King, Alberto Dainotti, and David Clark. 2019. Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In *IMC*. 420–434.

[53] Andree Toonk. 2013. Looking at the spamhaus DDOS from a BGP perspective. https://www.bgpmon.net/looking-at-the-spamhouse-ddos-from-a-bgp-perspective/

[54] Andree Toonk. 2014. Using BGP data to find Spammers. https://bgpmon.net/using-bgp-data-to-find-spammers/.

[55] Costa Tsaousis. 2022. FireHOL IP Lists | IP Blacklists | IP Reputation Feeds. http://iplists.firehol.org/.

[56] Jan Vermeulen. 2019. The Big South African IP Address Heist – How Millions Are Made on the "Grey" Market. https://mybroadband.co.za/news/internet/318205-the-big-south-african-ip-address-heist-how-millions-are-made-on-the-grey-market.html.

[57] Jan Vermeulen. 2019. How Internet Resources Worth R800 Million Were Stolen and Sold on the Black Market. https://mybroadband.co.za/news/internet/330379-how-internet-resources-worth-r800-million-were-stolen-and-sold-on-the-black-market.html.

[58] Jan Vermeulen. 2021. Afrinic Bank Accounts Frozen after R740 Million Damages Claim. https://mybroadband.co.za/news/internet/407770-afrinic-bank-accounts-frozen-after-r740-million-damages-claim.html.

[59] Jan Vermeulen. 2021. Internet Addresses Worth R1.8 Billion Seized. https://mybroadband.co.za/news/internet/405640-internet-addresses-worth-r1-8-billion-seized.html.

[60] Pierre-Antoine Vervier, Olivier Thonnard, and Marc Dacier. 2015. Mind Your Blocks: On the Stealthiness of Malicious BGP Hijacks. In *NDSS*.

[61] Matthias Wählisch, Olaf Maennel, and Thomas Schmidt. 2012. Towards detecting BGP route hijacking using the RPKI. *ACM SIGCOMM Computer Communication Review* 42, 4 (Oct. 2012), 103–104.

[62] Christopher S. Yoo and David A. Wishnick. 2019. Lowering Legal Barriers to RPKI Adoption. U of Penn Law School, Public Law Research Paper No. 19-02, https://ssrn.com/abstract=3308619.

A SPAMHAUS DROP CATEGORIZATION

To classify each prefix, we searched SBL records for: 'hijack' + 'stolen', 'snowshoe', 'known spam operation', 'hosting', and 'unallocated'+'bogon', which we illustrate in Table 2. The word 'hosting' in the first record of Table 2 led to our classifying that SBL record as *malicious hosting*. We manually verified that Spamhaus used 'hosting' in relation to a malicious activity – e.g. spam hosting, bulletproof hosting, botnet hosting etc, to avoid spurious classifications that could occur when hosting was not used in that context, such as in the second and third records in Table 2. 90% of SBL records contained one keyword, 2.7% of SBL records contained two keywords, and the remaining 7.3% of SBL records contained none. For this last category we manually inferred the prefix's category, e.g., we classified the last record in Table 2 (SBL325529) as *snowshoe spam* because Spamhaus had reason to believe that the IP range could be used for high volume spam emission. For two prefixes, Spamhaus did not provide enough information to infer an accurate label.

Record	Keyword	Classification
SBL310721	AS204139 spammer **hosting**	*malicious hosting*
SBL240976	**hijack**ed IP range ... billing@a**hosting**inc.com	*hijack*
SBL502548	**Snowshoe** IP block on **Stolen** AS62927 ... james.johnson@networx**hosting**.com	*snowshoe*, *hijack*
SBL322513	Register Of **Known Spam Operations** ... **snowshoe** range	*known spam operation*, *snowshoe*
SBL294939	Register Of **Known Spam Operations** ... illegal netblock **hijacking** operation	*known spam operation*, *hijack*
SBL325529	Department of Defense ... Spamhaus believes that this IP address range is being used or is about to be used for the purpose of high volume spam emission.	*snowshoe*

Table 2: Excerpts from SBL records that we used to classify DROP prefixes.