Debogonising 2a10::/12
Analysis of one week's visibility of a new /12

Stephen D. Strowes, *RIPE NCC*, *sds@ripe.net*
René Wilhelm, *RIPE NCC*, *wilhelm@ripe.net*
Florian Obser, *RIPE NCC*, *fobser@ripe.net*
Riccardo Stagni, *RIPE NCC*, *rstagni@ripe.net*
Agustín Formoso, *RIPE NCC*, *aformoso@ripe.net*
Emile Aben, *RIPE NCC*, *emile.aben@ripe.net*

***Abstract*—In mid 2019, IANA allocated `2a10::/12` to the RIPE NCC, the first IPv6 allocation to a Regional Internet Registry (RIR) in over twelve years. By early 2020, we were preparing to issue space from this `/12` to our members. Without measurement, it is unclear whether this `/12` is safe to use: routing policies, long-forgotten router configurations, malicious traffic, or networks making private use of unallocated address space may reduce the usability of some or all of the space. In order to provide an opportunity for operators to test the space prior to operational use, we announced the full `/12` via BGP for one week followed by eight smaller allocations, each with one target responsive to ICMP echo requests. We captured all packets sent to this `/12` while the BGP announcements were active. In addition, a RIPE Atlas measurement campaign was conducted, and route propagation was inspected via the RIPE Routing Information Service (RIS).**

Notable traffic captured includes low-volume TCP traceroute scans into the address space and DNS traffic, including some from misconfigured DNS servers. No traffic type is pervasive, and disregarding traffic generated by RIPE Atlas, only 6.2M packets carrying various transport payloads were captured during this study. Analysis of RIS data indicates that route visibility is good, and RIPE Atlas data shows that reachability to this space is also generally good. From RIPE Atlas measurements we identify a small number of networks where reachability is reduced, in line with reasonable route filtering practices.

This work forms the first significant IPv6 darknet study since 2013. We provide fresh insight into the activity of unsolicited IPv6 traffic today. We show that while there is more unsolicited traffic in the IPv6 space than in the past, this traffic is not as pervasive as in the IPv4 space. Further, this work assists our understanding of the feasibility of operating previously-unused address space from future IANA allocations.

***Index Terms*—bgp, ipv6, debogonisation**

I. Introduction

On 5 June 2019, the RIPE NCC received its second `/12` IPv6 allocation from the Internet Assigned Numbers Authority (IANA), the first large allocation from IANA to a Regional Internet Registry (RIR) since 2 Oct 2006 [1]. By early 2020, we were preparing to allocate from this space to members.

The IANA allocations for IPv6 global unicast space had therefore not changed in over twelve years. This introduced the risk that allocations drawn from the new `/12` may fall outwith the list of acceptable global unicast ranges in long-forgotten network configurations, preventing route propagation or packet forwarding. Identifying such problems requires testing.

978-3-903176-27-0

Additionally, we were interested in unsolicited traffic, and potential "hot-spots" in the space. Unsolicited traffic evolves and can have a variety of sources, such as botnets, network scanners, or misconfigured devices. However, IPv6 studies on unsolicited traffic on this scale are not recent and a `/12` is an address range so vast that we cannot draw conclusions from patterns observed in IPv4 studies. As this was previously unallocated space, we had no expectation of the volume of the traffic we would collect. IPv6 traffic trends observed since the IPv6 Launch events in 2011 and 2012 [2], [3] demonstrate increasingly widespread IPv6 adoption, and therefore a higher risk of misconfigured services or malicious traffic.

In this paper, we present an observational study of the announcement of this `/12`, and a detailed analysis of the traffic we collected while the address space was announced. We observe low-volume TCP traceroute scans, DNS traffic from misconfigured DNS servers, and various other traffic types. We show that the address space propagates widely through BGP, and that it is widely reachable from the RIPE Atlas measurement platform; we identify a handful of networks where reachability is reduced relative to a stable target.

This paper is structured as follows: related work is covered in Section II. Our experimental setup and ethical considerations are detailed in Section III. A detailed analysis of the packet data captured is covered in Sections IV, V, VI, and VII. We discuss aspects of routing and reachability based on public routing data and RIPE Atlas measurement results in Sections VIII and IX. We conclude the paper in Section X.

II. Related Work

Related work in the area of darknet traffic and "background radiation" tends to focus on IPv4. Given the size of the IPv4 address space, scanning is trivial and lessons learned from an IPv4 `/8` may be generally applicable. Off-the-shelf IPv4 scanning tools include zmap [7] and masscan [8].

Various IPv4 studies on unused address space are related to this work, but are not directly comparable. Some of the most significant work comes from the UCSD Network Telescope, maintained by CAIDA [9], which formerly operated as darknet composed of a `/8`, now a `/9` and a `/10`. A study of four largely unused `/8`s was published in 2010 [10], and showed billions of packets per week at each address block.

Related work on IPv6 is scarce, and from before significant IPv6 deployment. For reference, Google's IPv6 statistics [11]

TABLE I: IPv6 prefixes announced in January 2020, with their announcement timestamp and IRR/ROA configuration; all prefixes were withdrawn Jan 20, at 10:04:36 UTC. Responsive targets inside blocks are listed, the percentage of successful responses in the collected ping data, and the RIPE Atlas measurement IDs with measurement results. Measurement ID marked † was an accidental duplicate, increasing the number of ping measurements to this target.

Prefix	Responsive address	Announced	IRR	ROA	ping % response	RIPE Atlas measurement IDs ping	traceroute
2a10::/12		Jan 13 09:24:04 UTC	no	no		23825523, 23825524	
2a10:4::/32	2a10:4::1	Jan 15 10:49:39 UTC	yes	yes	95.5%	23836754	23841181
2a10:5::/32	2a10:5::1	Jan 15 10:49:39 UTC	no	yes	94.8%	23836758	23841182
2a10:6::/32	2a10:6::1	Jan 15 10:49:39 UTC	yes	no	95.5%	23843272	23841183
2a10:7::/32	2a10:7::1	Jan 15 10:49:39 UTC	no	no	88.1%	23836761	23841184
2a10:3:4::/48	2a10:3:4::1	Jan 15 10:49:39 UTC	yes	yes	95.4%	23836747	23841175
2a10:3:5::/48	2a10:3:5::1	Jan 15 10:49:39 UTC	no	yes	95.5%	23836751, 23842797	23841176
2a10:3:6::/48	2a10:3:6::1	Jan 15 10:49:39 UTC	yes	no	95.5%	23836752	23836765†, 23841177
2a10:3:7::/48	2a10:3:7::1	Jan 15 10:49:39 UTC	no	no	88.2%	23836753	23841180

TABLE II: Comparison of key related works: address ranges, durations, and packets collected. Rate indicates average packets collected per day. ‡ is the total packets captured during this study, without the RIPE Atlas ICMP echo requests.

Study	Prefix	Period	Packets	Rate
Ford *et al.*, 2006 [4]	unspec. /48	16 mos.	12	0.025
APNIC, 2010 [5]	2400::/12	10 days	21.2K	2,210
Merit, 2013 [6]	2400::/12	3 mos.	1.3B	14.4M
	2600::/12	3 mos.	2.5B	27.8M
	2800::/12	3 mos.	504.8M	5.6M
	2c00::/12	3 mos.	20.3M	226K
	2a00::/12	5 days	25.5M	5.1M
	2a04::/14 2a08::/13	3 mos.	3K	33.3
This study, 2020	2a10::/12	1 week	85.2M 6.5M‡	8.5M 652K

show over 25% deployment in 2020, while before 2013 deployment was under 1%. The main studies of relevance are listed in Table II.

Ford *et al.* studied traffic collected at a /48 between December 2004 and March 2006, and collected only twelve packets [4]. A later study was conducted over 10 days by APNIC in June 2010, using their /12 allocation [5]. 21,166 packets were collected in this time, with a mix of TCP, UDP including some DNS, and ICMP.

A significant study was conducted by Merit between 2012 and 2013, using the the five original /12 allocations to the RIRs [6], [12], [13]. This study collected significant traffic. One of the largest contributors to this dataset was DNS traffic, though this varied wildly between the prefixes studied. These prefixes were covering prefixes over address space already allocated to members (excepting the RIPE prefix, which was withdrawn then partially reannounced), and the authors assert that most captured traffic is caused by misconfiguration. In the RIPE space, once the non-covering prefixes were used, very little traffic generated through misconfiguration was captured.

Owing to the scale of the IPv6 address space, targeted approaches to scanning seek ways to reduce the search space: using knowledge of IPv6 allocations or addressing plans, or using knowledge of traditional SLAAC IIDs and MAC address assignments can drastically reduce the search space for an IPv6 scanner [14]. There have also been projects to leverage DNS semantics based on DNS error messages for NXDOMAIN versus NOERROR [15], [16]. More recent work has attempted to leverage DNSSEC infrastructure [17].

Address generation techniques have been implemented in network scanners, with varying degrees of success. Some work uses techniques already discussed in [14] and additional heuristics to generate sets of target IP addresses [18]. Some work attempts to infer structure in existing patterns and extrapolate using measures of entropy [19] or address density [20], both of which require a set of "seed" addresses. IPv6 hitlists drawn from public resources such as DNS are one such approach to generating seed lists, though these lists must be constantly refreshed [21]. The maintenance of seed lists requires ongoing work. Other work attempted similar approaches to seeding, target generation, and scanning [22].

Finally, research into IPv6 network scanning leads us full-circle to the *detection* of scanning behaviour in active IPv6 space [23] by observing DNS "backscatter" traffic triggered by network devices querying the reverse DNS *ip6.arpa* domain.

III. Experimental Setup

For this investigation we announced the full 2a10::/12 from the RIPE Routing Information Service (RIS, AS12654) using RIS Route Collector 03 (RRC03). RRC03 is well connected via AMS-IX and NL-IX.

Subsequent to the /12 being announced, one /29 was drawn from this space, from which eight smaller prefixes were drawn to also be announced via RRC03. These prefixes are /32s and /48s, prefix lengths typically visible in global routing tables [24]. The parent /29 is in line with current RIPE NCC IPv6 allocation policy [25]. Each prefix was configured differently: four with a route object in the Internet Routing Registry (IRR), and four with an RPKI Route Origin Authorisation (ROA). We chose this permutation of options because it

allows for further studying of route filtering, which is thought to be very heterogeneous based on each network operators' preference for either using prefix length-based, ROA, and/or IRR based filtering.

The experiment proceeded as follows:

Initial mailing list announcement: Various network operator groups and other mailing lists were notified on 8 January 2020 of our intention to announce the full `/12` and some smaller blocks from this space.

Phase 1: Initial BGP announcement: Announced via BGP on 13 January 2020.

Phase 2: Subsequent BGP announcements: Announced via BGP on 15 January 2020. First set of RIPE Atlas ping and traceroute measurements started towards `::1` addresses in each prefix.

Phase 3: Updates sent to mailing lists: 16 January 2020, we updated mailing lists with the status of the experiment, and indicated the eight responsive addresses for operator testing. `2a10:4::1` is identified as the primary target.

Withdrawal: All prefixes were withdrawn from BGP simultaneously on 20 January 2020. Packet capture and RIPE Atlas measurements were stopped once fully withdrawn.

A. Ethical Considerations

We took care with our considerations around data collection and the future use of this address space. We made a reasonable choice that there is value in understanding whether there is significant "noise" in this previously unannounced address space which may affect network operators.

There was the unlikely risk that a private network may have been using some of the space, against policy. In this case we may have attracted some of their private traffic. To identify such usage, packet capture is necessary. If we had identified any networks already using this address space, this space could have been quarantined until such a time it could be reclaimed.

To understand the traffic observed, full payloads were captured. Aside from soliciting ICMP echo requests to the eight targets listed in Table I, we solicited no traffic, and no other part of this address space was responsive to any traffic.

Having solicited ICMP echo requests to some addresses, the `/29` from which this address space was drawn was quarantined and will not be issued to RIPE NCC members for at least six months.

B. Data Release

The data used in this paper is purposefully as public as possible, to facilitate further study of the routing and reachability during the early stages of releasing new IPv6 address space.

This study makes use of three main data sources. These are:

Packet traces: Our intent is to share this data, with respect to privacy concerns. As this data is not yet available like the other sources, we focus on it in this paper.

RIPE RIS routing data: Routing data is available for download from RIS [26].

RIPE Atlas measurements: Measurement data is available via the RIPE Atlas API. Direct links to data are in Table I.

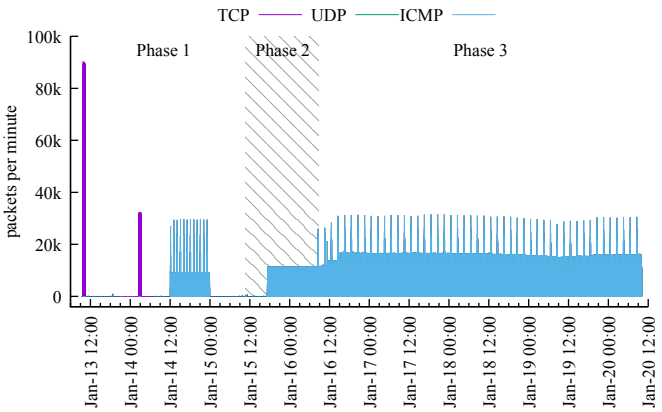

Fig. 1: All traffic observed, by transport protocols.

IV. Traffic Analysis Overview

We captured all inbound packets received at RRC03 that were destined for `2a10::/12` while the BGP announcements were active. In total, we collected 85,246,303 packets. Fig. 1 shows all packets received.

We define three groups for this traffic. First, the vast majority of collected traffic (78,721,469 packets; 92.3%) was generated by the RIPE Atlas measurement platform. We discuss this traffic in Sections VII and IX. Next, 5,491,117 (6.4%) packets appear to be performing TCP traceroutes into the address space. This behaviour is covered in Section V-A.

Finally, 1,033,717 (1.2%) packets are mixed traffic from a variety of sources, and this traffic is shown in Fig. 2. These packets primarily contain ICMPv6, TCP, or UDP; there is a negligible amount of traffic apparently carrying other transport protocols. Breaking down this traffic, we have:

- ICMPv6: 581,399 packets (56.2%); see Section VII.
- TCP: 315,434 packets (30.5%); see Section V.
- UDP: 132,591 packets (12.8%); see Section VI.
- Unknown/other: 4,293 packets (0.4%).

Prior work in 2012 collected over 25 million packets in 24 hours at the previous RIPE NCC `/12` allocation. Once this was reduced to a `/13` and `/14` to avoid covering space allocated to members, only 3,000 packets were collected over a subsequent three months. Thus, while today's traffic volumes are still low, there is more activity in this unused space than there was previously in other unused space.

A. Origin diversity

Most of the traffic received originates from space allocated to an RIR; very little of the traffic received contains addresses drawn from address space that is not globally routable (Table III). In the full dataset, we observe 162,771 distinct origin IP addresses (excluding RIPE Atlas, which has approximately 4,000 probes operating with IPv6). These IP addresses are drawn from 150,720 `/64`s. The high number of `/64`s implies that these sources are not highly concentrated; indeed, matching these origins to BGP tables during the study shows us that traffic originates from 1,075 ASNs in total.

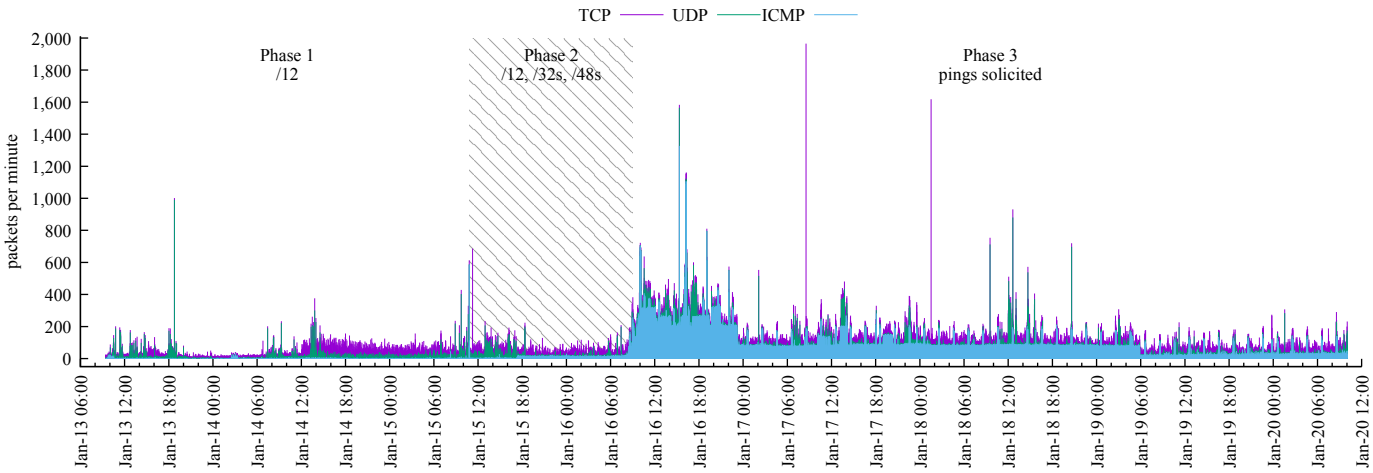

Fig. 2: Stacked histogram of packets observed, per minute, split into transport protocols. Atlas traffic and TCP traceroute scans are omitted, to be discussed in Sections IX and V-A. Other protocols are sufficiently rare that they are omitted.

TABLE III: Source address categories during this study. Phases here refer to Fig. 2. Address classes are derived from [27]. Large volumes of TCP traffic during phase 1 is considered in Section V-A; row marked ◇ is all traffic from RIR-allocated space except TCP traceroute activity.

Address category	Phase 1	Phase 2	Phase 3
RIR-allocated	5,607,622	74,438	839,396
◇	122,922	72,540	834,877
IANA (reserved)	30	43	165
6to4	10	0	42
Other GUA, `2000::/3`	121	114	610
ULA, `fc00::/7`	1	2	35
Link-local, `fe80::/10`	0	0	10
No match	180	350	1,665
Totals	5,607,964	74,947	841,923

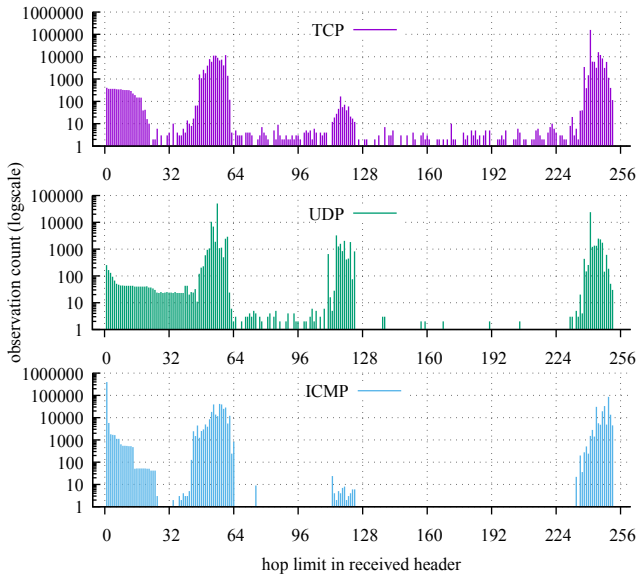

Fig. 3: Observed values in the *hop limit* packet header field.

B. Target diversity

It is useful to understand whether there are specific regions in the address space that attract traffic. Such regions may imply targeted attacks (unlikely against previously unused space), misconfiguration, or a network using the space privately.

We find that in the 1,033,717 'mixed' packets, 555,968 packets targeted the eight responsive addresses defined in Table I. The remaining 447,749 packets were destined for 178,390 distinct target addresses, located in addresses located in 153,118 target `/64`s. The TCP traceroute behaviour sends packets in higher volume, but only covers an additional 261,157 distinct targets (in the same number of `/64`s); this traffic is discussed separately in Section V-A.

The set of targets is broad, relative to the traffic volume. Two of the most highly targeted IPs attract UDP packets carrying DNS queries; these are discussed in Section VI-A. The distribution of the remaining packets to destinations is not flat, but most of the remaining targets receive at most thousands of packets over the week, and generally hundreds or fewer.

Looking briefly at the bottom 64 bits of the target addresses – the interface identifiers (IIDs) – we observe 153,719 unique target IIDs. There are some common patterns in this set, *e.g.*, 13,753 IIDs have zeroes in bit positions 64–96 (in total, 157,937 packets); 4,315 IIDs that set zero or more of the lowest bits in any hextet (97,534 packets); 1,590 IIDs that contain the substring "`face:b00c`" (24,828 packets). Finally, target addresses with SLAAC IIDs are rare. We observe 21 such target addresses, in only 22 packets.

C. Hop Limits

In Fig. 3 we show a histogram of the observed hop-limit values in packets received, excepting the TCP traceroute be-

haviour to be discussed in Section V-A which over-emphasises lower values through repetition.

We observe the primary peaks around hop limit values of around 55–58 and around 250 in all protocols. Less frequently, 123; 128 is a typical starting value on Microsoft Windows.

If we assume the starting values of these is 64, 256, and 128 respectively, then we infer that many common paths measured into `2a10::/12` are on the order of 5–10 IP hops in length.

V. TCP

In total, we collected 5,806,551 IPv6 packets with a TCP payload. The vast majority of this traffic relates to a mass TCP traceroute campaign, which we describe in Section V-A. Section V-B covers the rest of the TCP traffic.

A. Mass TCP Traceroute

94.6% of TCP packets captured, 5,491,117 in total, are part of what appears to be a set of TCP traceroute measurements into the address space. Most of this traffic is clearly visible in Fig. 1, during two spikes of TCP traffic on 13 January (09:44:26 – 10:30:52, UTC) and 14 January (02:31:02 – 03:16:12, UTC). This traffic originates primarily from two IP addresses located in two different networks:

- `2a05:e740:162::2`, announced by AS39063
- `2605:fe00:0:17::1`, announced by AS23033

AS39063 is held by Leitwert GmbH, who advertise services including Internet intelligence and Routing Assessment. AS23033, and other ASNs observed later in the study (AS49367, AS17139, AS23470), originate traffic with the same characteristics.

Each destination address is targeted multiple times, the only difference between individual packets is the increasing *hop limit* value in the IP header. Otherwise, all of these captured packets have the same characteristics. They are all TCP segments with only the SYN flag set and no payload. The destination port is port 80, and the source port is 49152, the first port number in the dynamic range. DSCP, ECN, and flow label are always 0. TCP sequence numbers do not increment strictly linearly, but in batches; see Fig. 4. The TCP headers carry one TCP option to indicate the receiver's Maximum Segment Size (MSS), and is always 1,460 bytes. This implies an MTU 20 bytes too large for general Internet packet forwarding, suggesting that this application is designed for IPv4. The window size parameter is always 29,200 bytes. These distinctive characteristics are observed in all of this traffic regardless of origin.

The scanning hosts cycle through various target IP addresses, and the targets are coordinated and shared across origins. In total, they attempt to reach 261,157 distinct addresses. The targeted addresses appear to be pseudo-randomly generated, and no `/64` is targeted twice. Note that there are 2^{52} (4.5 quadrillion) `/64`s to target.

During phase 2 of the study there are intermittent scans to individual target addresses, in total generating only an additional 1,015 packets. So while the announcement of the more-specific prefixes triggers additional measurement, only five or

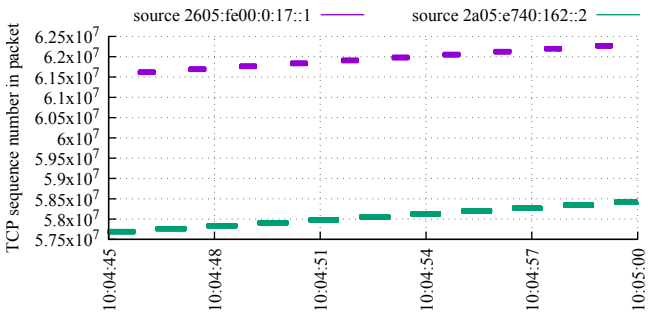

Fig. 4: Fifteen seconds of sequence number behaviour; ranges increment through measurement cycles.

six target addresses are chosen for each prefix. We observe fewer packets are received for targets in `2a10:7::/32` and `2a10:3:7::/48`, perhaps related to their routability.

Given the apparent coordination of destination addresses, increasing IP hop limits in packets, and identical TCP options, we surmise that Leitwert GmbH is the controller for these measurements. It is not clear why the packet rate was so high initially, or why these scans stop abruptly. Finally, prior work does not identify traceroute behaviour as we do here.

B. Remaining TCP Traffic

The remaining TCP traffic consists of 315,434 packets.

50.2% of these originated from two IP addresses located within `240e:f7:4f01:c::/64`. This traffic does not behave as the TCP traceroute traffic previously discussed. This traffic uses a wide range of source ports (ports 5000 through 64999), and a small set of 312 non-contiguous target ports. The most common target port is 6379 (redis), but other commonly targeted ports include 9030 (Tor), 8112 (related to PACcoin, a cryptocurrency), 8081, port 6697 (IRC), well-known ports for services such as HTTPS, POP3, IMAP, and so forth.

In these packets, the hop limit is always high when received (typically 241). In all cases, only the SYN flag is set, and there is no payload. Otherwise, some characteristics are the same as the TCP traceroute traffic discussed in the last section, such as the default window size, the presence of the MSS option (set to the 1,460 bytes typical of IPv4 traffic), and the lack of other TCP options.

The target cycling is narrow, targeting three specific `/96` ranges roughly equally: `2a10:4f8:10b:699::/96`, `2a10:4f8:010b:699:1::/96`, and `2a13:6f00:3::/96`. In each of these cases, the scanning activity walks primarily across the bottom 16 bits, and occasionally the bottom 32 bits. The generated addresses appear to either feature 16 or 32-bit pseudorandom values, and not an incremental sequence. This traffic is light, but appears to behave as a fairly naïve scanner as one might write for IPv4. The target ports suggest probing to locate common services.

The next most coherent subset of the TCP traffic targets port 443 and contains what appears to be encrypted payloads, generally only with the TCP ACK flag set as if there were

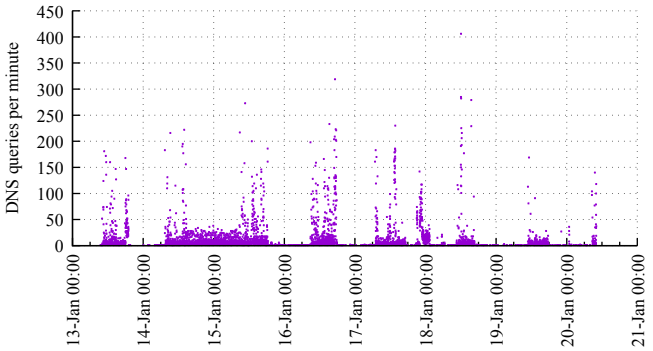

Fig. 5: DNS query arrival rates are intermittent.

an active connection. This is the case for 13.0% of the 315,434 TCP segments. These carry a wide range of source and destination IPs, and so do not appear to be coordinated in the same manner as the TCP traceroute or the apparent port scanning above.

Finally we observe a vanishingly small set of TCP segments with various flags set, often in conflicting states, and often targeting seemingly randomly selected destination addresses.

VI. UDP

UDP traffic constitutes 132,591 of the packets captured. Of this, 68,303 packets were destined for port 53 and contain DNS payload; we discuss these in Section VI-A; we look at the rest of the UDP traffic in Section VI-B.

A. DNS

In this section, we briefly focus on the DNS traffic received. Previous work has observed DNS traffic as one of the largest contributors of traffic pollution [13]. The queries we received are low-volume, and the arrival rates are bursty, as shown in Fig. 5.

We collect 68,303 UDP packets containing DNS queries, including 61 apparently malformed DNS packets. No queries are sent to any of the addresses listed in Table I. There are 1,032 destination addresses (in 711 distinct /64s) observed from 594 distinct origins (in 530 distinct /64s). Two destination addresses in particular within `2a10:168:a510:1400::/64` attracted most queries, 60,023 in total, all originating from AS13030, the vast majority of which – all but 570 packets – are A and AAAA queries generally for popular domains. We contacted this network, and they determined this was a misconfiguration made by one of their customers. We disregard this DNS traffic. This is similar to prior work [6], where significant volumes of DNS queries were generated through misconfiguration.

The remaining packets are predominantly 6,708 HINFO queries from 62 IP addresses (from 4 ASNs: ASNs 715, 3330, 13335, and 15169). These targeted 198 distinct addresses (and `/64`s) within `2a10::/12`, and many of the origin hosts target the same addresses. All of these queries contain a string of the form "@(*some.domain*).contacts.abuse.net", as is specified on the abuse.net information pages [28]. We also see 569 CHAOS queries with the string 'version.bind', and 309 PTR queries for '_services._dns-sd._udp.local.' which may be related to certain reflection attacks [29]. A handful of other query types exist in the data, but are exceedingly rare.

Only 284 queries for AAAA records and 273 for A records arrive in the space during the study (for 171 and 176 names respectively, and 300 distinct names in total). The names are generally real names: most names appear in the Cisco Umbrella 1 Million list during this study. The ranks of these names varies wildly but they are often ranked in the top 5,000; many are subdomains for popular CDNs.

B. Other UDP Traffic

The remaining UDP traffic consists only of 64,288 packets.

10,378 of these have source from port 4600, with destination port 1. The traffic originates from 90 distinct sources, and targets ten distinct IP addresses across ten separate `/48`s. All but one of these targets has the form `2a1`, followed by 28 bits, followed by `01:900::`.

Some 1,574 packets have port 443 as their *source*, and have a payload of 1,330 bytes. Most of these have source addresses located within `2a02:2f00::/28`, and each of these packets target an address inside `2a12:2f00::/28`. The same sources also send some TCP traffic with source port 443 and the ACK flag set. It is unclear if this is traffic intentionally seeking HTTP/QUIC servers, or if it is indicative of another configuration error. Regardless, these are rare.

Various other UDP ports receive traffic, but none in significant volume. The remaining UDP traffic does not exhibit any other particularly noticeable patterns.

VII. ICMP

As already discussed, we remove the echo request traffic generated by RIPE Atlas probes as part of the measurement campaign described in Section III.

RIPE Atlas probes are identified in the captured packet data: traceroute measurements have particular identifiable characteristics (*e.g.* known packet sizes), and an identifying payload containing the string "`http://atlas.ripe.net`". By identifying traceroute packets that match these characteristics, we can also identify the source IP addresses for all RIPE Atlas probes. Therefore, we can also isolate and remove RIPE Atlas "ping" measurements with a high degree of certainty.

A. ICMP Traffic to Responsive Addresses

Excepting the traffic generated by RIPE Atlas probes, at the set of eight responsive addresses we collect 581,399 ICMP packets. 426,342 (73.3%) of these packets are echo requests (ICMPv6 type 128). Error messages to these addresses are typically generated on the return paths to Atlas probes, which we inspect in the analysis in Section IX.

Table IV shows the primary ICMP message types received at each responsive address. The dominance of `2a10:4::1` stems from the email sent to mailing lists, which stated that this address was the simplest test to perform. Thus, it attracted

TABLE IV: Responsive targets: ICMPv6 message types collected. Type 128 is "Echo Request", type 1 is "Destination Unreachable", and type 3 is "Time Exceeded".

Target address	total ICMP	type:128	type:1	type:3	other
2a10:4::1	428,152	412,521	12,114	3,517	0
2a10:5::1	14,774	107	11,404	3,263	0
2a10:6::1	15,789	340	12,341	3,108	0
2a10:7::1	16,446	968	12,421	3,057	0
2a10:3:4::1	18,975	2,172	13,297	3,506	0
2a10:3:5::1	16,350	175	12,967	3,208	0
2a10:3:6::1	29,560	3,849	20,134	5,577	0
2a10:3:7::1	14,060	245	10,747	3,068	0
All other targets	27,293	5,965	19,336	241	1,059

most (78.7%) of the ICMP echo requests that were received from origins other than RIPE Atlas. ICMP echo requests to the pingable targets defined in Table I constitutes 95.3% of all ICMP traffic observed.

Having removed echo requests from RIPE Atlas probes in this table, the number of error types appears high. To confirm the origin of these errors, we extracted the original IP header from the message that caused the error. This allows us to determine when an error message was generated by a legitimate response back to a RIPE Atlas probe. We determined that only 34 error messages *in total* were generated by messages en-route to 8 destinations that were *not* RIPE Atlas probes. Recall that the RIPE Atlas measurements are recurring, and therefore errors will also accumulate. In all we received ICMP echo requests from 6,613 distinct IP addresses, including RIPE Atlas, and 256 (3.9%) of these addresses generated an error.

B. ICMP Traffic to Other Addresses

The final row in Table IV shows how many ICMP packets arrived on any address not in the set of eight. There were 27,293 packets that targeted other addresses during the study. 19,336 have type 1 ("*destination unreachable*"), almost all of which are code 0 ("*no route to destination*"), though of course no address in the `/12` generated traffic that could have triggered these errors. 5,965 of the ICMP packets contain echo requests, and 489 of them contain echo responses which were never solicited. The remainder is effectively noise, including many individual packets with unassigned ICMPv6 type values.

The most common targets are `2a10::1`, which received 1,239 ICMP echo requests from 52 origins, `2a10:4::` (607 echo requests from one origin), `2a10:3:4::` (493 echo requests from three origins), and `2a10::` (275 times from eight origins). Any of these could have been *ping6* terminal commands run by curious operators, and none of them would have generated an echo response.

In total, this traffic targets 20,108 addresses (in 19,732 `/64`s) and originates from 17,969 sources (in 17,758 `/64`s). Many of the selected targets exist within the longer prefixes announced, though the targets within them are widely dispersed and don't typically target low-number addresses. These are very broad source/target sets, suggesting essentially random probing.

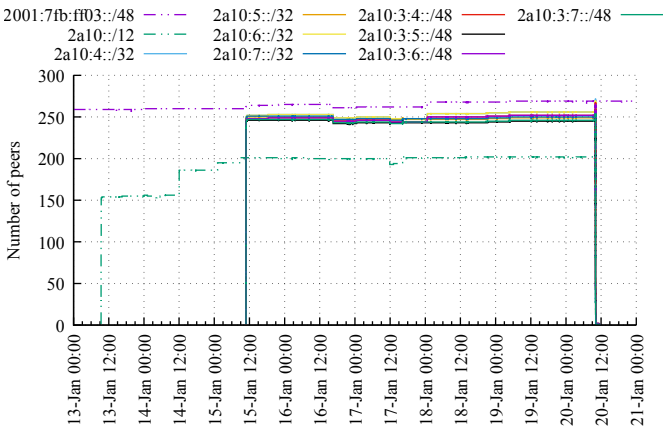

Fig. 6: Peers propagating routes to any RIS collector.

VIII. Routing Analysis

With new address space, it is important to understand whether and how corresponding BGP announcements propagate across the Internet. Cases of mismatches between intended and observed behaviour require manual intervention by those operating the network.

Table I lists the announcement and withdrawal times for each of the prefixes. In addition, each RRC announces a long-term stable *anchor* prefix [30]. The anchor prefix for RRC03 is `2001:7fb:ff03::/48`. Recall that each prefix is configured differently, in terms of corresponding route objects in the IRR and/or having ROAs, to allow diagnosis of filtering problems.

All prefixes announced for this study are visible at all RRCs. However, this does not imply that all peers forward the announcements. Fig. 6 shows how many RIS peers observed the nine prefixes. For reference, during this study around 270 peers carry over 50% of a "full" IPv6 table, and there are over 450 peers carrying any IPv6 routes at all. The anchor prefix is typically visible at 265 peers across all RRCs.

The `/12` is visible at the fewest peers throughout this study. Without an entry in the Internet Routing Registry and without an RPKI ROA, filtering this route is considered reasonable behaviour. Nonetheless, the visibility of `2a10::/12` increases in multiple steps early in this study. Initially, on 14 January, when the prefix is propagated for the first time via two large transit networks, AS3257 (GTT) then AS174 (Cogent) (all AS174 paths route via AS3257). Then on 15 January, we observe route propagation to RIS peers via smaller networks, AS33891 (CORE-Backbone) and AS20612 (SWISS-IX).

A /12 is an atypical prefix length for global routing, where `/32`s through `/48`s are more typical [24]. The longer prefixes are more widely visible, at around 245–255 peers. The prefixes with the greatest visibility are the two `/32`s with IRR objects, followed by the two `/48`s with IRR objects. The two `/48`s without IRR objects are least visible across the RIS peers. The presence of a ROA seems to neither help nor hinder the propagation of these prefixes.

Following withdrawal at the origin, there is a brief increase in the number of peers propagating the these prefixes to RRCs. At this time, the eight test prefixes are observed via an additional 20 peers across all RRCs; eight of these peers are at RRC03 itself. Peak visibility of 2a10:4::/32, 2a10:6::/32, 2a10:3:4::/48, and 2a10:3:6::/48 (*i.e.*, the prefixes with IRR entries) is similar to that of the anchor prefix, which peaked at 270 peers during the study.

During withdrawal, we observe no additional AS paths of length 2; only longer, indirect paths are revealed. This suggests that many RIS peers are propagating announcements with prefixes originating from AS12654, but they are not propagating directly back along the path they were initially received. The observed path lengths increase during withdrawal, matching intuition, up to paths of length 10.

IX. RIPE Atlas Analysis

We ran ping and traceroute measurements from all RIPE Atlas probes tagged as having a working IPv6 connection to nine targets: the responsive addresses in Table I, and the responsive address in the anchor prefix[1]

In total, 4,173 RIPE Atlas probes participated in measurements to all nine targets at some point during the study. We disregard 42 probes that receive no responses from any target, including the anchor target. The lack of measurement results suggests ICMP filtering upstream or some other misconfiguration, rendering the resulting data from those probes not useful.

Table I lists the percentage of responses received by the remaining probes for each of the test targets. The anchor target has a response rate to RIPE Atlas echo requests of 99.0% for the same duration. The aggregate response rate for the test targets is therefore lower than the anchor target. We identify two distinct behaviours that lead to the discrepancy.

No response from any test address: 138 probes receive responses from the anchor target, but no response from any of the test targets. Generally, we observe ICMP echo requests from the probes in the captured packet data, suggesting that ICMP filtering on the return path or at the probe's host network are the likely causes for a lack of response. All 69 IPv6-enabled probes located in AS8881 (1&1 Versatel Deutschland GmbH) fall into this category. 12 other probes are located in AS22773 (Cox Communications), out of 19 IPv6-enabled probes in that network. The other probes in this category are distributed across 37 other ASNs, in various regions.

No response from the :7: prefixes: 266 probes receive no responses from neither 2a10:7::1 nor 2a10:3:7::1 but on all other test targets we observe high-levels of responsiveness. 262 of these probes were in AS3320 (DTAG), representing 100% of all IPv6-enabled probes that were in AS3320 throughout this study. One probe is located in AS206549 which appears to accept routes via AS3320 and AS8881. The three other probes are located in ASNs 5409, 8302, and 29169, each being the only probe hosted in those networks. This represents a small set of networks, but in all cases we collect no ICMP echo requests to the ":7:" addresses from these probes in the captured packet data. These probes collect no ICMP error conditions from the forward path. There are an additional 29 probes in 11 networks that filter the ":5:" announcements.

By inspecting the response rates on the probes that do not fit into the two categories above, aggregate responses are in line with the anchor target: 98.8–99.0% response rate or higher, with a slightly lower response rate of 98.5% on the ":7:" targets. This is derived from a set of 3,698 probes, widely dispersed across 1,338 ASNs.

In summary, there exists a small set of networks within which RIPE Atlas probes receive no echo responses, and one network within which the ":7:" addresses are not reachable. Without IRR objects or RPKI ROAs we expect reduced reachability, though it is striking that it appears to be in so few networks. These networks are primarily responsible for the differences between the test addresses and the anchor address.

X. Conclusions

This paper has covered our findings from a week-long observational study of a new /12, the first in over 12 years, and the first significant IPv6 darknet study since 2013.

We have described the packet-level activity observed at 2a10::/12 which, aside from eight individual target addresses, was entirely unresponsive. The volume of traffic that we observe appears to be higher than prior studies: we collect over 6.5M packets – including solicited pings from operators but excluding intentional RIPE Atlas measurements – in one week, while the adjacent /13 and /14 studied for three months in 2012–2013 [6] collected 3,000 packets in total.

The primary unsolicited contributor to this dataset is a coordinated TCP traceroute campaign. The campaign's target selection appears randomised, and parameter settings (including port number selection) do not vary. We also see evidence of misconfiguration, in this case with DNS traffic, in the collected data. We consider neither case malicious. We see no evidence of private networks using parts of this address space, and no evidence of "hot spots" that attract excessive traffic, which we would consider withholding from members. The captured traffic is light, and arrives from many sources.

We've shown that route visibility is close to that of a baseline long-lived announcement, and reachability is good in most cases. We identify a small set of networks which have reduced reachability to the test addresses. Both operate sufficiently well for general use of this address space.

The IPv6 address space is so large that broad scanning techniques become impossible. It is therefore difficult to draw common trends from this study, or prior studies. Thus, observational studies such as this remain important to help understand what is on the network today. Our aims in constructing a sound experimental setup were to enable the further study of this space from multiple viewpoints: the BGP routing system, packet capture at the route origin, and a wide-scale network measurement platform allows us to perform this type of observational study. Our aim is always to make as much of this data publicly available as possible.

[1]RIPE Atlas measurement ID 23836750.

Acknowledgment

We are grateful to the anonymous reviewers and our shepherd, Kenjiro Cho, for their time and comments which helped improve this paper.

References

[1] RIPE NCC, "RIPE NCC Receives /12 IPv6 Allocation From IANA." [Online]. Available: https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/ripe-ncc-receives-12-ipv6-allocation-from-iana

[2] Internet Society, 2012. [Online]. Available: https://web.archive.org/web/20120523165208/http://www.worldipv6day.org/

[3] ——, 2013. [Online]. Available: https://www.worldipv6launch.org/

[4] M. Ford, J. Stevens, and J. Ronan, "Initial Results from an IPv6 Darknet," in *International Conference on Internet Surveillance and Protection (ICISP06)*, Aug. 26–29, 2006.

[5] G. Huston, "Background Radiation in IPv6," Oct. 2010. [Online]. Available: https://labs.ripe.net/Members/mirjam/background-radiation-in-ipv6

[6] J. Czyz, K. Lady, S. G. Miller, M. Bailey, M. Kallitsis, and M. Karir, "Understanding IPv6 Internet Background Radiation," in *Proceedings of the Internet Measurement Conference (IMC)*, 2013.

[7] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *USENIX Security*, 2013.

[8] R. Graham, "MASSCAN: Mass IP port scanner," https://github.com/robertdavidgraham/masscan, 2013.

[9] "UCSD Network Telescope." [Online]. Available: https://www.caida.org/projects/network_telescope/

[10] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, "Internet Background Radiation Revisited," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC)*, 2010.

[11] "Google IPv6 Statistics." [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html

[12] M. Kühne and D. Karrenberg, "IPv6 Darknet Experiment," Nov. 2012. [Online]. Available: https://labs.ripe.net/Members/mirjam/ipv6-darknet-experiment

[13] S. G. Finn, M. Médard, and R. A. Barry, "IPv6 Pollution Traffic Analysis," presented at RIPE 66, Dublin, Ireland, May13–17 2013. [Online]. Available: https://ripe66.ripe.net/presentations/121-v6darknet-ripe2013.pdf

[14] F. Gont and T. Chown, "Network Reconnaissance in IPv6 Networks," Mar. 2016. [Online]. Available: https://tools.ietf.org/html/rfc7707

[15] P. van Dijk, "Finding v6 hosts by efficiently mapping ip6.arpa," https://web.archive.org/web/20170603234058/http://7bits.nl/blog/posts/finding-v6-hosts-by-efficiently-mapping-ip6-arpa, Mar. 2012.

[16] T. Fiebig, K. Borgolte, S. Hao, C. Kruegel, and G. Vigna, "Something From Nothing (There): Collecting Global IPv6 Datasets From DNS," in *Proceedings of the 18th Passive and Active Measurement Conference (PAM)*, Mar. 2017.

[17] K. Borgolte, S. Hao, T. Fiebig, and G. Vigna, "Enumerating Active IPv6 Hosts for Large-scale Security Scans via DNSSEC-signed Reverse Zones," in *Proceedings of the 39th IEEE Symposium on Security & Privacy*, ser. S&P, May 2018.

[18] J. Ullrich, P. Kieseberg, K. Krombholz, and E. Weippl, "On Reconnaissance with IPv6: A Pattern-Based Scanning Approach," in *Availability, Reliability and Security Conference*, 2015.

[19] P. Foremski, D. Plonka, and A. Berger, "Entropy/IP: Uncovering Structure in IPv6 Addresses," in *Proceedings of the Internet Measurement Conference (IMC)*, 2016.

[20] A. Murdock, F. Li, P. Bramsen, Z. Durumeric, and V. Paxson, "Target generation for internet-wide ipv6 scanning," in *Proceedings of the Internet Measurement Conference (IMC)*, 2017.

[21] O. Gasser, Q. Scheitle, P. Foremski, Q. Lone, M. Korczyundefinedski, S. D. Strowes, L. Hendriks, and G. Carle, "Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists," in *Proceedings of the Internet Measurement Conference (IMC)*, 2018.

[22] R. Beverly, R. Durairajan, D. Plonka, and J. P. Rohrer, "In the IP of the Beholder: Strategies for Active IPv6 Topology Discovery," in *Proceedings of the Internet Measurement Conference (IMC)*, 2018.

[23] K. Fukuda and J. Heidemann, "Who Knocks at the IPv6 Door? Detecting IPv6 Scanning," in *Proceedings of the Internet Measurement Conference (IMC)*, 2018.

[24] S. D. Strowes, "Visibility of IPv4 and IPv6 Prefix Lengths in 2019," Apr. 2012. [Online]. Available: https://labs.ripe.net/Members/stephen_strowes/visibility-of-prefix-lengths-in-ipv4-and-ipv6

[25] RIPE, "IPv6 Address Allocation and Assignment Policy," Mar. 2020. [Online]. Available: https://www.ripe.net/publications/docs/ripe-738

[26] RIPE NCC, "RIS Raw Data." [Online]. Available: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data

[27] IANA, "IPv6 Global Unicast Address Assignments." [Online]. Available: https://www.iana.org/assignments/ipv6-unicast-address-assignments/

[28] "Using abuse.net from programs," Jul. 2014. [Online]. Available: https://www.abuse.net/using.phtml

[29] A. Atlasis, "An Attack-in-Depth Analysis of multicast DNS and DNS Service Discovery." [Online]. Available: https://conference.hitb.org/hitbsecconf2017ams/materials/D2T2%20-%20Antonios%20Atlasis%20-%20An%20Attack-in-Depth%20Analysis%20of%20Multicast%20DNS%20and%20DNS%20Service%20Discovery.pdf

[30] RIPE NCC, "Current RIS Routing Beacons." [Online]. Available: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/current-ris-routing-beacons