# Hazardous Echoes: The DNS Resolvers that Should Be Put on Mute

Ramin Yazdani, Yevheniya Nosyk, Ralph Holz, Maciej Korczyński, Mattijs Jonker, Anna Sperotto

# Hazardous Echoes: The DNS Resolvers that Should Be Put on Mute

Ramin Yazdani*, Yevheniya Nosyk†, Ralph Holz‡*, Maciej Korczyński†, Mattijs Jonker*, Anna Sperotto*
*University of Twente, Enschede, The Netherlands
†Université Grenoble Alpes, Grenoble, France
‡The University of Sydney, Sydney, Australia

***Abstract*—Connectionless networking protocols such as DNS continue to be widely misused for Reflection & Amplification (R&A) DDoS attacks. Early efforts to address the main cause of DNS-based R&A were focused on identifying and attempting to eradicate open DNS resolvers. One characteristic of open resolvers that has not received much attention so far is that – as a result of unexpected behavior – resolvers can react to a single query with multiple DNS responses. We refer to these as *Echoing Resolvers*.**

**In this paper, we quantify the problem of echoing resolvers in the wild. We identify thousands of such resolvers on the Internet and show how some reply on the order of tens of thousands of times to a single query, further escalating the potential of R&A DDoS attacks. We analyze the cause of response repetition, study behavioral differences among echoing resolvers, and categorize resolvers on the basis of the underlying causes of the observed behavior. We show how the interplay between DNS traffic and the traversed networks is responsible for echoing resolvers. In particular, we identify IP broadcasting as a cause of echoing resolvers, on top of phenomena already described in the literature (e.g., routing loops). Furthermore, we show that using sensitive labels in queries can lead to a more powerful echoing effect while using different query types does not significantly affect echoing behavior. Finally, seeing how some underlying causes of response repetition also affect or can be turned against authoritative nameservers, we quantify the potential impact of echoing resolvers on these as well.**

## I. Introduction

It is well-known that open Domain Name System (DNS) resolvers can be – and are – frequently misused to bring about R&A Distributed Denial of Service (DDoS) attacks. In such a scenario, the attacker sends DNS queries with spoofed source IP addresses to open DNS resolvers. The responses to these queries are sent to the victim whose IP address was spoofed as the source address (reflection). This technique becomes even more powerful when combined with queries that trigger large responses (amplification).

Several studies investigated open resolvers and proposed ways to limit their misuse [14]–[16], [26], [35]. Early efforts largely focused on quantifying open resolvers (of which there are currently around 2.7 million). Recent research efforts have started considering resolver characteristics such as bandwidth and amplification potential to help identify heavy hitters, to prioritize takedowns [32], [35]. Other works have instead investigated the authenticity of DNS responses, focusing on censorship, malware distribution, and phishing [14], [26]. Only a few studies, however, have investigated the less understood interplay between the DNS packets and the networks their traverse. In a recent paper, Nosyk et al. [24] studied how routing loops cause so-called mega amplifiers by creating a stream of repeated responses. In this paper, we take a step forward with the goal of analyzing repeated DNS responses and their underlying causes without limiting our analyses to mega DNS amplifiers.

In a typical DNS resolution process, a stub resolver sends a query to a recursive DNS resolver. The recursive resolver then contacts authoritative nameservers in the DNS hierarchy until it finds the answer to the query and returns this answer to the client. Assuming the client sent a single query, if the DNS resolution goes as expected, a single answer should be returned to the client. This, however, is not always the case in practice. DNS queries issued towards certain resolvers on the Internet result in receiving multiple responses. We refer to this situation as *echoing DNS resolvers*. Echoing can be attributed to routing loops [24] and middleboxes [12], [23], among other causes. As we show, IP broadcasting is also a potential cause.

One might argue that locating echoing resolvers requires more effort from attackers compared to simply misusing open resolvers. However, as we later show in this paper, thousands of echoing resolvers can be discovered with a simple DNS scan. More importantly, when it comes to R&A DDoS attacks, echoing resolvers elevate the risk to Internet infrastructure (e.g., authoritative nameservers), and bring in a damage potential that can one up that of resolvers that behave as expected. In this paper, we study this phenomenon and present the following contributions:

- We investigate the underlying causes of DNS echoing behaviors, confirming routing loops and middleboxes to be partially responsible for echoes, while further identifying IP broadcasting as another underlying cause.
- We study the behavioral differences among echoing resolvers using various DNS queries and show that using different query types does not significantly affect echoing behavior.
- We show that using sensitive labels in DNS queries (further) increases the attack potential of echoing resolvers.
- We explore the impact of echoing resolvers on authoritative

978-3-903176-58-4 

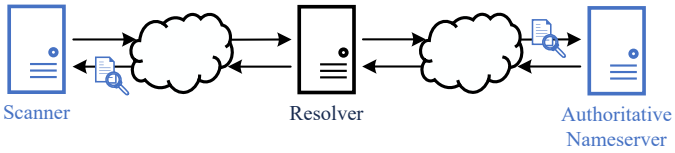


Fig. 1. Our DNS measurement setup. We configure a scanner machine and an authoritative nameserver for the queried domain name while having no control over tested recursive resolvers. We capture the traffic arriving at our scanner as well as the authoritative nameserver to identify echoing resolvers.

nameservers and show that authoritative nameservers can receive echoing queries similar to DNS clients.

The remainder of this paper is structured as follows. In Section II, we detail our methodology to measure the DDoS potential of echoing resolvers and to tie echoing behaviors to underlying causes. We study the diversity among echoing resolvers in Section III and notify the network administrators hosting echoing amplifiers in Section IV. We discuss the limitations of our work in Section V and provide an overview of the related work in Section VI. Section VII discusses the ethical considerations for our research and Section VIII concludes the paper.

## II. Echoing Resolvers in the Wild

Our approach to detecting echoing resolvers starts with active DNS measurements, which provide a client-side perspective on echoing behaviors by recursive resolvers. We also consider echoing behaviors on the upstream side, by analyzing traffic that reaches an authoritative nameserver under our control. In this section, we first describe our measurement methodology. We then tie, on the basis of properties of the DNS responses received, echoing behavior to various underlying causes.

### A. DNS Scans

We run weekly DNS scans targeting the publicly routable IPv4 address space (roughly 3.7B IP addresses) over a 1.5-year period between September 2021 and March 2023. Note that not all of the targeted IP addresses are announced in BGP. Thus, the number of probes exiting our network is around three billion queries per scan. Fig. 1 depicts our measurement setup. Our scanner embeds the destination IP address of the queried host in each query name so that incoming responses can be matched with a query sent toward a specific destination. In order to avoid caching, we also embed a timestamp into the queried domains. We have full control over the domain name used in our scans and its authoritative nameserver. We capture the traffic both at our scanner and the authoritative nameserver of our domain name, and we post-process these traces to infer the behavior of each resolver.

Fig. 2 shows the number of echoing resolvers over time in our measurement data. The plot is divided into subcategories, clustering resolvers based on the extent to which echoing occurs. Note that the vast majority of echoing reflectors trigger two responses per query, while a few resolvers cause more than a thousand replies.

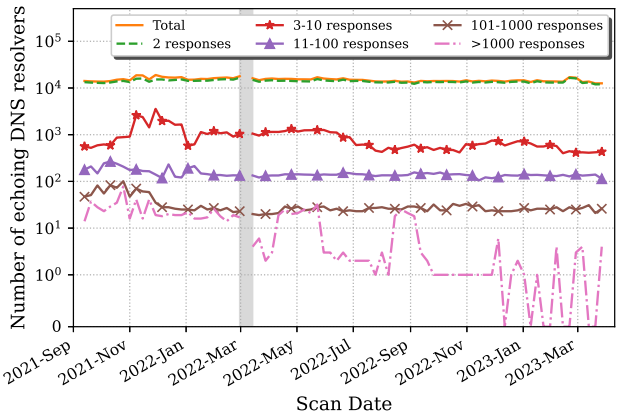


Fig. 2. The number of echoing resolvers and the number of responses returned for a single DNS query over time. The gray bar on 2022-03-07 corresponds to a missing data point due to a measurement failure.

To further investigate the echoing amplifiers, we look at the source IP addresses that the responses originate from. We do this using a single snapshot of our weekly measurements[1]. We detect echoing resolvers in roughly 1.6k Autonomous Systems (ASes). More details about the top-10 origin ASes for echoing resolvers are given in Section III-C. Fig. 3 illustrates the scatter plot of the number of returned responses per scanned IP address. Two patterns are visible. First, a diagonal pattern represents resolvers for which there is a one-to-one mapping between the number of source addresses and the total number of responses (i.e., each host is involved in generating a single response). Second, a horizontal pattern at the bottom represents a single host behind a flow of arriving responses. Mixed patterns are also visible in between. Roughly 80% (11.1k) of echoing resolvers in Fig. 3 are those that trigger two (correct) answers from a single source IP address. 78% of these answers arrive with at most 1ms time difference. In the following sections, we explore differences among the observed patterns.

### B. Underlying Causes of Echoing Behaviors

We analyze the queries sent, the received responses, and their network characteristics to identify a number of possible underlying causes of echoing behaviors. In this section, we specifically focus on the client perspective (i.e., responses received on our scanner).

**Routing Loops –** Routing loops have previously been identified in the literature as one of the underlying causes of echoing resolvers [24]. These loops can be transient (i.e., appearing due to routing topology changes and disappearing when the routing protocol converges) or persistent. Routing loops can be detected using traceroute [2], [18], [24], [34].

[1]Note that the reason to pick a single snapshot is to keep our analysis simple. Nevertheless, a similar behavior is observable in other snapshots of our dataset.

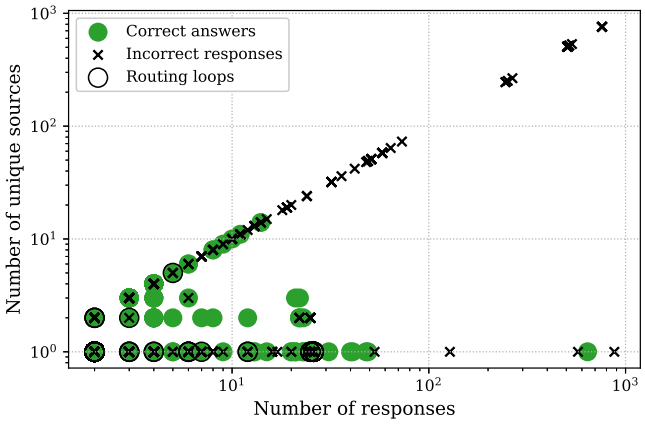


Fig. 3. The number of responses per source IP address in the 2023-01-23 scan. The diagonal pattern shows a one-to-one mapping, while the horizontal line represents echoing resolvers that returned multiple responses.

Using a single snapshot[2], we ran UDP-paris traceroute measurements using Scamper [19] for the roughly 14k echoing resolvers detected. Considering that routing loops can be transient, we ran a second DNS scan just before the traceroute measurements. The results show that 10.6k resolvers still trigger echoing responses. Our traceroute results reveal loops in the route from our scanner towards 524 echoing resolvers (3.7% of the total number of echoing resolvers). Roughly 93.9% of these loops trigger two responses to us. The total number of detected routing loops is much smaller than the echoing resolvers that we detect. This suggests that routing loops are not the only cause for the existence of echoing amplifiers.

Our measurement might not be able to detect all routing loops due to the following reasons. First, some routing loops are known to be transient. Considering our stateless measurement setup (in which we wait for the entire measurement to be concluded before inferring echoing resolvers), there is a chance that the routing protocol converges sometime between the moment we observe an echoing resolver and the moment we run traceroute measurements. At the same time, transient loops are less relevant for attackers, as they will disappear before being misused. Second, a number of traceroutes include hops that are not configured to reply to ICMP/UDP traffic, which prevent us from detecting them if they are responsible for routing loops. This means that our findings represent a lower bound to the number of routing loops.

**Broadcast Addresses –** IP broadcast is used to send packets to all the devices attached to a specific network. It is categorized into the *limited* and *directed* types [4]. The first one is typically referred to when talking about traditional IP broadcast, namely when packets are relayed within the same local network. It is used, e.g., in DHCP exchanges to send requests to a DHCP server at an unknown IP address. In this case, the DHCP client sets all target address bits to one (i.e., `255.255.255.255`). The second type of IP broadcast (i.e., directed broadcast, which is the concern of our paper) refers to when a packet is delivered to all devices in a remote network. In this scenario, all host bits are set to one and the network subnet bits define the target network. Fig. 4 is an example scenario in which a packet is sent using directed broadcast over the Internet. Any router on the path to the destination network will treat this packet as a unicast packet since they lack information about the destination network. On the other hand, the edge router of the destination network recognizes this packet to be a broadcast packet and delivers it to every host in the destination network. According to RFC2644, the directed broadcast must be disabled in a router configuration by default due to its potential to facilitate DDoS attacks [30]. However, our observations suggest that a number of networks still accept queries sent to directed broadcast addresses.

[2]We use the same snapshot as before (i.e., 2023-01-23) consistently in our single snapshot analysis.

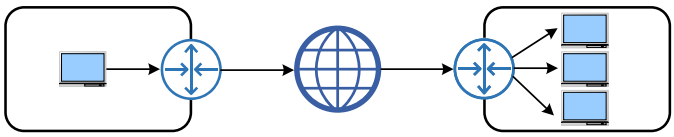

Fig. 4. Directed broadcast example. The machine on the left sends a single packet to the destination network on the right. The destination network router treats the incoming packet as a broadcast one and relays it to all the hosts in its network.

Going back to Fig. 3, we link the diagonal pattern to the directed IP broadcast. Considering that we do not know the remote subnets, we cannot undoubtedly determine the broadcast IPs of remote networks. However, there are two reasons which allow us to make this inference. First, looking at the IP addresses of top echoing resolvers in this category, we see that many end with `.255` which defines the broadcast address for a `/24` prefix length (the longest publicly routable IPv4 prefix). Second, for most of the resolvers in this category, the set of responding hosts excludes the queried resolver itself, which is again a property of IP broadcast.

The top-right corner of Fig. 3 shows clusters of IP addresses forming a network prefix together and replying to a single query. Assuming this is related to IP broadcast, we are still wondering why each and every host in a prefix should be an open resolver. We consider two possible explanations. First, there might be a shared software image used for hosts, e.g., in a cloud network. Second, a single host might be bound to all the IP addresses in a network. We manually checked a handful of prefixes for broadcast attributed echoing resolvers on Censys [7]. For networks with the majority of hosts answering the broadcast query, we observe that the detected publicly running services on these hosts are almost identical.

**DNS Interception –** Middleboxes can interfere with DNS queries in different ways. For example, they can redirect queries to a resolver other than one specified by the client, or replicate them and return additional responses before the genuine ones arrive [17]. In these cases, the client can receive two or more responses to a single query originating from the

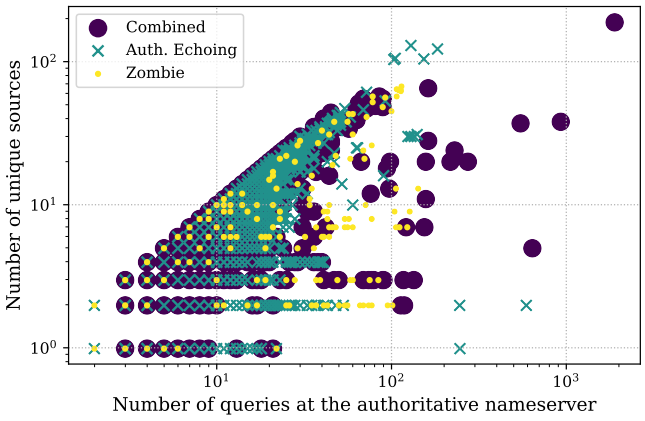


Fig. 5. The number of queries arriving at the authoritative nameserver compared to the number of unique source IPs issuing these queries on 2023-01-23.

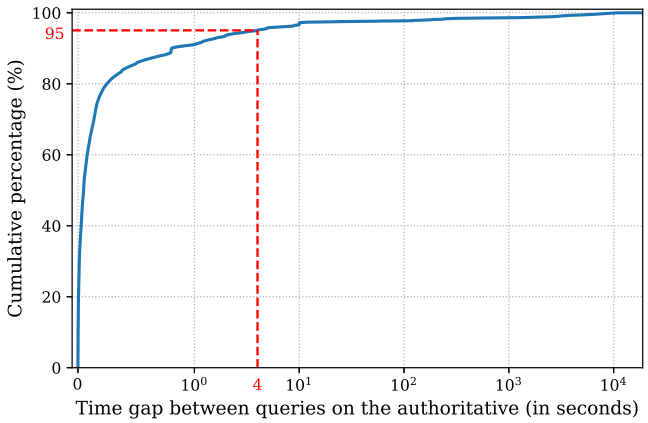


Fig. 6. The cumulative distribution of the time gap between duplicate queries arriving on our authoritative nameserver on 2023-01-23.

originally queried DNS resolver and/or the interceptor.

Note that as we do not query sensitive domain names, the above-observed behavior cannot be linked to censorship middleboxes [12], [23]. However, as we later show in Section III-C, a carefully crafted domain name can trigger a new set of amplifiers that react to sensitive keywords. Meanwhile, the number of resolvers echoing *correct* answers would stay roughly the same.

**Key Takeaway:** *We reveal that IP broadcast is responsible for echoing resolvers, next to routing loops and DNS interception. These causes are not mutually exclusive and may collectively increase the echoing power.*

### C. Response Authenticity

DNS queries are not always served with correct responses. Earlier research has extensively explored this phenomenon and shown that malicious resolvers might respond to queries with incorrect responses to lure users towards malicious endpoints [14], [25], [26]. This can also be done for censorship purposes. From a DDoS attack point of view, resolvers responding with correct answers are typically more appealing. This is because an attacker can craft a specific query (such as an `ANY` query for a DNSSEC-signed domain) and estimate the volume of traffic to be generated. However, this does not make other incorrectly responding resolvers altogether unattractive to attackers. As Fig. 3 shows, a number of resolvers responded with incorrect responses (either failed or forged), but could still be more powerful than non-echoing open resolvers. Our measurement on 2023-01-23 resulted in 11.8k (84.5%) resolvers echoing correct answers and 2.1k (14.7%) resolvers echoing incorrect responses. Approximately 0.8% of resolvers trigger a combination of responses.

### D. The Authoritative Nameserver Perspective

In a normal DNS resolution process, once a client sends a query to a recursive resolver, the latter contacts the authoritative nameserver to get the answer (provided the resolver caches are empty). If this process is unsuccessful (e.g., due to a packet loss), then the resolver might retry the same query. This typically happens within a few seconds.

Our investigations so far concerned the effect of echoing resolvers on the host to which traffic is reflected as part of the R&A DDoS attack. Echoing resolvers can (but do not necessarily do) involve repeating DNS queries, which can adversely affect upstream infrastructure, i.e., authoritative nameservers [25].

Literature reports that zombie queries are another source of unwanted load on authoritative nameservers. They are issued to proactively refill the cache of recursive DNS resolvers for previously observed domain names. The resolvers behind these queries keep repeatedly querying authoritative nameservers long after the original query issued by a client and account for roughly 25% of all queries arriving at DNS servers [13].

The traffic that we capture at the authoritative nameserver for our domain name includes echoed as well as zombie queries. Although a precise differentiation of the two is beyond the scope of this paper, we are able to classify the type of repeated responses based on a time heuristic. Fig. 5 shows the number of queries sent to our authoritative nameserver during a single snapshot of our measurement. Each distinct dot corresponds to one query issued by our scanner host. By studying the interval of time between duplicate arrivals of a query, we observe that 95% of the queries arrive at our authoritative nameserver within four seconds of each other (see Fig. 6). Since the issuing of zombie queries is driven by an expiring TTL (which is set to 180 seconds for our authoritative), we choose four seconds as a threshold to distinguish echoed queries from zombies. We associate queries to an *echoing* resolver if there are two or more queries with a time delta of less-than-four seconds at any point in time in our snapshot. We mark queries with time gaps always over four seconds as *zombie*. The queries with time gaps among duplicates both shorter and longer than four seconds are marked as *combined*. Considering that we set a TTL

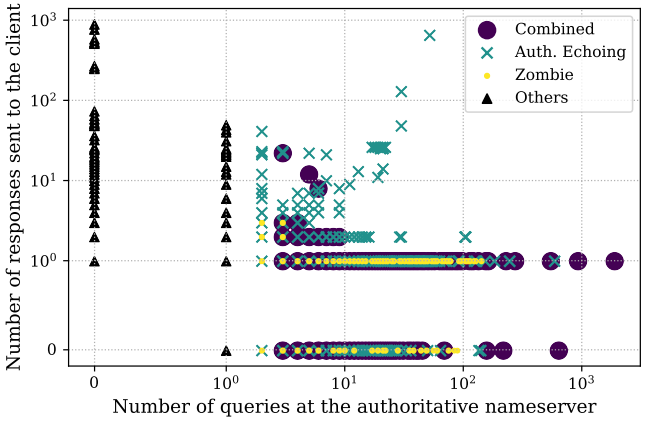


Fig. 7. The number of queries arriving at the authoritative nameserver compared to the number of responses returned to the client issuing initial queries on 2023-01-23.

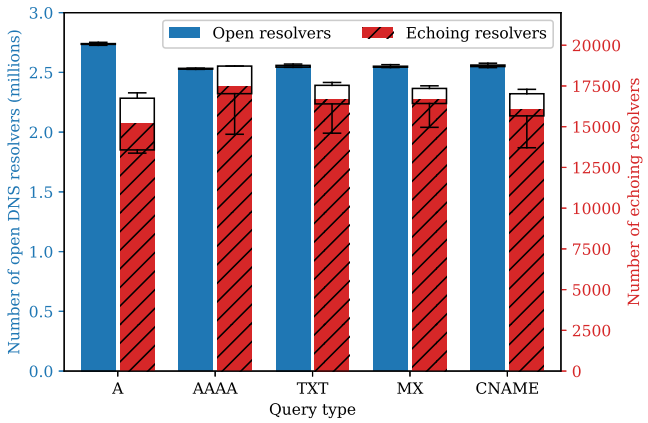


Fig. 8. The number of open and echoing resolvers for each query type. While A type query triggers the highest number of open resolvers, most of the echoing resolvers were located with AAAA queries.

value of 180 for the queried resource record in our DNS zone, the threshold chosen should be conservative enough to distinguish echoing resolvers from zombies. However, not all resolvers comply with the TTL value set by authoritative nameservers. Thus, further analyses are required to study the echoing behavior of resolvers on the authoritative nameservers, which we leave as future work.

Queries issued towards 911k resolvers are observed more than once on our authoritative nameserver. Based on the above-mentioned threshold, we associate 92.3% of these with echoing resolvers, 0.9% with zombie resolvers, and 6.8% with a combination of the two. The top right dot in Fig. 5 shows the worst case, in which 187 distinct IP addresses have queried the authoritative nameserver 1.9k times in a combined echoing and zombie pattern to serve a single query issued by our scanner.

Fig. 7 shows a scatter plot of echoing effects as observed by the clients and nameservers. As we can see, there are a number of resolvers (roughly 10k) that never (or only once) contact the authoritative nameserver but send echoing responses to the client (labeled as *Others*). The opposite behavior is also visible: resolvers never respond to the client but trigger multiple queries to the authoritative nameserver. A third category includes resolvers that have collateral echoing behavior both towards the client and the authoritative nameserver. Thus, from a DDoS attack point of view, depending on who the victim is, different sets of echoing resolvers might be appealing to attackers.

**Key Takeaway:** *Echoing behavior can affect authoritative nameservers as well. This could be leveraged to increase the power of DDoS attacks against nameservers.*

## III. In-depth Study of Echoing Resolvers

We now take a closer look at the diversity among echoing resolvers, in particular at traits that can make some more appealing for misuse in DDoS attacks.

### A. Address Record Query Type versus Other Types

Typically, DNS A queries are used to identify open resolvers. However, as Yazdani et al. [35] have shown, open resolvers might react differently to certain query types. Moreover, ANY and TXT queries are especially misused by attackers, as they result in larger responses. Also, Liu et al. [17] have shown that middleboxes intercept and handle DNS queries differently based on the query type. We, therefore, investigate whether different query types elicit different echoing behaviors.

We sent DNS queries for A, AAAA, TXT, MX, and CNAME records to all the routable IPv4 addresses. To avoid transient biases affecting our results, we repeat this measurement multiple times. Fig. 8 shows the number of open resolvers correctly resolving our queries (left y-axis) as well as the number of echoing resolvers for each record type (right y-axis). We conducted these measurements over five consecutive days, collecting one snapshot daily for a specific query type. This was repeated in four consecutive weeks (from 2023-02-13 to 2023-03-10). We observe that the number of open resolvers for type A is slightly higher than for other query types. In contrast, AAAA queries trigger slightly more echoing behaviors on average.

We aggregated echoing resolvers per AS to investigate whether specific networks are responsible for this difference. On average, three ASes (AS4538, AS4837 & AS4134) trigger the majority of the AAAA echoing resolvers that did not echo for A queries. All of these networks originate from China. We suspect that the echoing behavior in these networks is related to the application layer (e.g., an interception by middleboxes) and not a network-layer issue such as a routing loop.

The number of open resolvers responding to different query types is quite stable over the measurement period. However, a considerable fluctuation is seen for echoing resolvers. We further investigated this and observed that a single AS (AS31034) was triggering echoing responses during our measurements

and fixed it two weeks later.

**Key Takeaway:** *Generally, using different query types does not have a significant impact on triggering echoing resolvers. However, some networks treat various query types differently, most-likely due to interception by middleboxes.*

### B. Vantage Point Comparison

Routing loops and DNS middleboxes are the two causes of echoing DNS amplifiers that are route dependent, as both need to be on the path of a packet. In our case (echoing responses sent to a client), this means between our scanner and the echoing resolver. As such, the vantage points can have an impact on triggering echoing resolvers. To quantify this, we ran our scans from two vantage points at the University of Twente in the Netherlands (VP1) and the University of Sydney in Australia (VP2) on two consecutive days. We chose two geographically distinct networks to increase the chance of packets taking different routes. Our measurements result in a roughly equal number of echoing resolvers from the two vantage points (14.7k from VP1 vs. 14.2k from VP2), including 12.1k (more than 82.5%) observed from both vantage points. Since it is possible that – due to IP churn – echoing resolvers move to different IP addresses, we cannot directly attribute the difference to the vantage points. Thus, for the symmetric difference of echoing resolver sets observed from two vantage points, we group the number of resolvers observed per announced network prefix using *pyasn*[3] and BGP data from the Route Views Project. This results in 1.5k prefixes, with a long tail of networks that differ by fewer than ten echoing resolvers. This leaves us with only 25 networks for which our vantage points detect echoing resolvers with a difference of $\geq$ 10 IP addresses.

To further analyze the source of difference, we compare a VP1 measurement with another VP1 measurement a week apart. For the later measurement from VP1, we detect 13.9k echoing resolvers, 11.2k of which intersect with the earlier VP1 measurement. The difference rests in 1.8k prefixes, of which 97.5% differ in less than ten echoing resolvers. Based on this observation, we relate the majority of vantage point differences to the dynamicity of the Internet, while keeping in mind that path diversity can still account for a minor part.[4] Our findings are in line with previous findings by Nosyk et al. [24], who show that the majority of routing loops are located in the destination networks. This means that for routing-loop-based echoing resolvers, we should not see a significant difference between vantage points.

**Key Takeaway:** *Echoing resolvers observed from two distinct vantage points are almost identical. This suggests that echoing resolvers are triggered by elements close to or in the destination networks.*

[3]https://github.com/hadiasghari/pyasn

[4]It would be possible to limit the effect of dynamicity by running our measurements from two vantage points at exactly the same time, but to avoid putting undue burden on destination networks we decided not to do this.

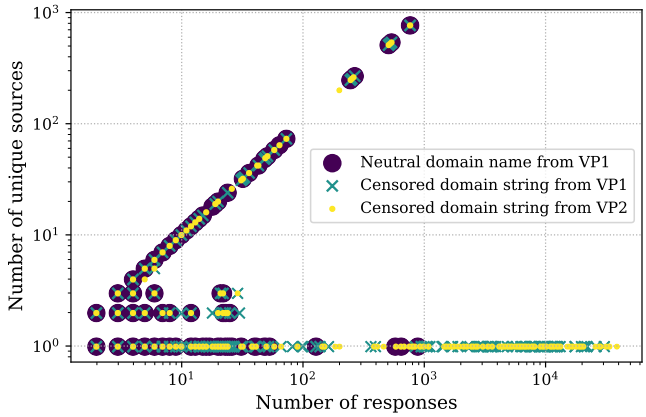


Fig. 9. Echoing effect for a sensitive label (measured from VP2 on 2023-01-24 and VP1 on 2023-01-27) compared to a neutral domain name (measured from VP1 on 2023-01-23).

### C. Impact of Using Sensitive Qnames

Literature has shown that issuing DNS queries for domain names with censored strings can result in triggering middleboxes [3], [8], [12], [17]. To evaluate the extent to which middleboxes are responsible for echoing resolvers, we issue DNS queries including the label `facebook.com` under and for a domain name under our own control. In practice, such a domain name is not anyhow related to `facebook.com`, but it can trigger overblocking censors [12]. We expect that directly using a censored domain name (e.g., `www.facebook.com`) would lead to stronger results. However, since our purpose is to measure the echoing impact of resolvers, we need to be able to tailor query names to each individual IP address. As we do not have the authority over a censored domain name, doing such is impractical. Besides, due to ethical considerations, we do not want to put extra load on the authoritative nameservers of censored, third-party domain names.

Fig. 9 compares the echoing effect of resolvers for a neutral domain name and a sensitive domain name including `facebook.com` as a subdomain label. We observe that the horizontal part of the echoing resolvers is extended in multiple orders of magnitude (note the logarithmic scale of the x-axis). Besides, the number of echoing resolvers observed from VP1 when using a sensitive label increases to roughly 1.68M, compared to roughly 13.9k resolvers for a neutral domain name. Resolvers triggering two responses originating from a single IP address (1.67M) are responsible for the majority of this increase. 99.4% (1.67M) of all echoing resolvers are in China, according to IP2Location geolocation metadata. As a comparison point, China accounted for only 21.2% (3k) of echoing resolvers in the case of using a neutral domain name in our queries. Other countries among the top ten countries hosting echoing resolvers do not exhibit a substantial difference between measurements of neutral and sensitive domain names. Our findings verify that the Great Firewall of China performs a keyword-based interception [12].

TABLE I
RANKING OF THE TOP-10 ORIGIN ASES FOR ECHOING RESOLVERS OBSERVED FROM VP1 FOR A NEUTRAL DOMAIN SCAN ON 2023-01-23 AND A DOMAIN CONTAINING A SENSITIVE LABEL SCAN ON 2023-01-27.

| Neutral domain name | | | | |
|---|---|---|---|---|
| ASN | AS Name | CC | Count | Percentage |
| AS4812 | China Telecom Group | CN | 2414 | 17.38% |
| AS22085 | Claro SA | BR | 393 | 2.83% |
| AS4847 | China Networks Inter-Exchange | CN | 283 | 2.04% |
| AS2497 | Internet Initiative Japan Inc. | JP | 172 | 1.24% |
| AS17970 | SKYBroadband SKYCable Corporation | PH | 159 | 1.14% |
| AS37308 | COOLLINK | NG | 157 | 1.13% |
| AS35366 | ISPpro Internet KG | DE | 141 | 1.01% |
| AS263218 | Internet Telecomunication Company de Guatemala | GT | 129 | 0.93% |
| AS2 | University of Delaware | US | 123 | 0.89% |
| AS208769 | Nicalia Internet, S.L.U | ES | 118 | 0.85% |

| Sensitive domain name | | | | |
|---|---|---|---|---|
| ASN | AS Name | CC | Count | Percentage |
| AS9808 | China Mobile Communications Group Co. | CN | 1138k | 67.59% |
| AS4134 | China Telecom Backbone | CN | 379.4k | 22.54% |
| AS4837 | China Unicom Backbone | CN | 108.1k | 6.42% |
| AS137694 | CHINATELECOM Xinjiang Kezhou MAN network | CN | 17.3k | 1.03% |
| AS137695 | CHINATELECOM Xinjiang Wulumuqi MAN network | CN | 11.1k | 0.66% |
| AS140553 | CHINATELECOM XINJIANG province Shengji 5G network | CN | 9.7k | 0.58% |
| AS7497 | Computer Network Information Center | CN | 4.0k | 0.24% |
| AS4812 | China Telecom Group | CN | 2.5k | 0.15% |
| AS4538 | China Education and Research Network Center | CN | 2.1k | 0.13% |
| AS22085 | Claro SA | BR | 0.4k | 0.02% |

Considering autonomous systems, we observe that while AS9808 (China Mobile Communications Group Co., Ltd.) accounts for 63.7% of echoing resolvers, all of the high-profile echoing resolvers (the extended horizontal tail in Fig. 9) are in AS4538 (China Education and Research Network Center). A comparison of the Top10 ASes for echoing resolvers between neutral and sensitive domain name measurements is given in Table I.

Previous studies [3] have shown that Internet censorship involves collateral damage when packets traverse networks with censorship middleboxes, even if these middleboxes are not in the destination network. We utilize our second vantage point to explore the impact of taking a route with on-path middleboxes. As shown in Fig. 9, both our vantage points (VP1 and VP2) result in similar echoing behavior, regardless of the use of a sensitive domain label. Further analyses are needed to compare the routes towards echoing resolvers from different vantage points.

**Key Takeaway:** *While DNS middleboxes are generally known to inject a handful of forged responses, our experiments show that they can be triggered to send tens of thousands of responses, hence increasing their abuse potential.*

### D. Persistence over Time

Open DNS resolvers appear and disappear over time due to reasons such as IP churn, being patched, etc. This applies to echoing resolvers as well. It is more appealing to DDoS attackers to misuse persistent resolvers as this reduces scanning efforts to identify them. To study the stability of echoing resolvers over time, we take echoing resolvers detected on our first measurement snapshot and check whether they are still active in subsequent scans for a period of 74 weeks. We observe that the number of echoing resolvers decays exponentially, but roughly 5% (679) of those were active during the entire measurement period. This set of resolvers would relieve an attacker from having to actively scan for new resolvers.

We further studied the stability of echoing resolvers to see if there is a behavioral difference between stable and non-stable ones. We plot echoing resolvers over time in Fig 10. The orange dots with a darker color represent echoing resolvers that were seen for a longer period in our measurement. The black circles represent the 5% of resolvers that were active for all of our snapshots. We see that while the long tail of echoing

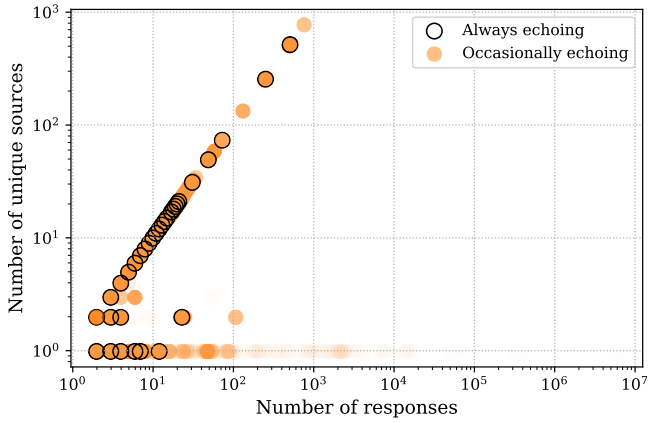


Fig. 10. Persistence of echoing resolvers over time between September 2021 and February 2023 (74 weeks). The 679 amplifiers available during the whole measurement period could be misused in DDoS attacks without needing to be frequently discovered.

resolvers with a single source address (the horizontal pattern) provide a packet amplification factor of up to multiple million times, they are less stable compared to the resolvers with a diagonal pattern (ones associated with IP broadcast).

**Key Takeaway:** *Echoing resolvers associated with broadcast IPs are often most-persistent over time. This redeems an attacker from frequent resolver discovery scans.*

## IV. VULNERABILITY DISCLOSURE

This paper discusses how certain resolver and network configurations can be misused in DDoS attacks. IP broadcast is even more dangerous by itself, as it lets someone from the outside reach all the hosts in remote networks. We located 94 echoing resolvers that triggered directed broadcast behavior (with 10 or more hosts involved) and notified corresponding network administrators. We found the contact email addresses using the RDAP protocol [22] and aggregated them into 34 organizations (mostly hosting providers). Each email contained a short description of the problem accompanied by IP addresses showing the broadcast behavior. We received seven automatically generated emails saying that abuse tickers were open, though one of them was closed the next day without further explanation. Three large hosting providers got back to us requesting more information (detailed logs with timestamps

and query names) and saying that they could not reproduce the reported behavior. We collaborated with these providers to help them reproduce our findings. At the time of writing, we did not receive any definitive response from the notified parties. However, our follow up measurements show that seven operators have stopped showing an echoing behavior for (a subset of) their IP addresses after our notification, while they had a persistent echoing behavior for a long time before we contacted them.

## V. Discussion and Limitations

Echoing DNS responses exist due to various underlying causes as we discussed in our paper, typically involving two elements. First, an artifact in the network (such as routing loops, middleboxes, and IP broadcast), and second, a DNS resolver. However, these two elements do not necessarily need to be present simultaneously. While we use the term *echoing DNS resolvers* throughout this paper, we are referring to the phenomenon of echoing behavior in response of our DNS queries. This does not necessarily involve a resolver, but could also involve a middlebox that takes action on an intercepted query and appears, from a measurement point of view, to behave as a resolver.

Our methodology to detect echoing resolvers comes with two limitations. As a consequence, we report lower bounds for the characterization of the phenomenon. The first lower bound concerns the number of routing loops. We leverage traceroute to detect routing loops. However, this does not guarantee their detection for the following reasons. First, our stateless measurement setup is deployed such that echoing resolvers are inferred once the full IPv4 scan is concluded. Only then we run traceroute measurements to detect routing loops. Thus, there is a gap between the point in time at which our measurement observes an echoing resolver and when we run traceroute to detect potential loops. Transient loops might be resolved in the meanwhile. To evaluate this limitation, we do a second check just before our traceroute measurements to confirm that the resolver is still echoing (showing a 25% drop in the number of echoing resolvers). Our measurement setup can be modified to a stateful scanner to avoid this limitation, which we leave as a future work. Second, not all hops in a traceroute are necessarily responsive to ICMP/UDP traffic. This prevents us to detect loops in such traceroutes. Thus, our traceroute-inferred findings present a lower bound for routing loops.

The second lower bound concerns the Packet Amplification Factor (PAF) [28] of the echoing resolvers. Our measurement setup is designed in a way that keeps monitoring the incoming traffic for a few minutes after we send our last query. However, we have seen a limited number of echoing resolvers that keep sending responses even multiple days after the original query. Our current setup would underestimate the amplification power of these resolvers and miss the long tail of responses. For the threat model in this paper, these resolvers do not necessarily provide additional amplification. This is because packets accumulating during a short time are more harmful in a DDoS scenario than a long tail of traffic. Additionally, we are unable to associate responses that exclude the query name (e.g., refused or malformed DNS responses) with the specific resolver queried. This also means that our results represent a lower bound for echoing behaviors.

## VI. Related Work

Open DNS resolvers pose a significant threat to the whole Internet. Even though their population has been gradually decreasing from 26.8 million in 2014 [14] to 2.6 million in 2022 [35], those can still be misused effectively in DDoS attacks. Recently, Yazdani et al. [35] characterized open resolvers in terms of their amplification potential by issuing 15 types of `A`, `TXT`, and `ANY` queries. The authors varied the DNSSEC OK flag (`DO` bit), the EDNS0 flag, and the EDNS0 buffer sizes. Interestingly, as few as 20% of open resolvers accounted for 80% of the overall amplification potential, suggesting that a relatively small number of resolvers is necessary to mount effective attacks. Those findings are in line with the work of Nawrocki et al. [21], showing that, usually up to 1,000 open resolvers and forwarders are involved in real-world DDoS attacks.

There exist several ways to misuse open resolvers. To amplify traffic towards the victim, an attacker sends DNS queries that will generate replies of a much bigger size. This is notably the case for `ANY` responses that can reach the amplification factor of 64 [28]. Van Rijswijk-Deij et al. [33] have further shown that the issue will be exacerbated when the queried domain name is DNSSEC-signed, thus increasing the amplification factor up to 179 times.

The majority of the above-mentioned literature focuses on the so-called Bandwidth Amplification Factor (BAF) [28]. Another class of attacks relies on DNS resolvers issuing a sequence of queries to satisfy a single DNS query. For example, the "DNS unchained attack" [6] aims at degrading the performance of networks hosting authoritative DNS infrastructure by creating long chains of `CNAME`s to be resolved. The NXNSAttack [1] exploits the fact that attackers can trigger the resolution of their own domain names and point thousands of referrals to victim domains. In that case, recursive resolvers will overload the target DNS zones with thousands of queries. Finally, the TsuNAME [20] attack relies on cyclic dependencies between two DNS zones that potentially trigger infinite resolution by recursive resolvers. This second class of attacks focus on a similar concept to our work by relying on the so-called Packet Amplification Factor (PAF).

To achieve an even higher packet amplification factor, attackers can benefit from DNS middleboxes, e.g., national censors [12], [23] or other interceptors [17]. In either case, such devices inject responses before genuine ones arrive from recursive resolvers, thus doubling the traffic received by victims. As shown by Nosyk et al. [24], when such middleboxes are located inside routing loops, they can generate as many as 655 million responses to a single DNS query. Referred to as "mega-amplifiers" in the existing work, similar systems can also abuse NTP [9], IGMP [29], and TCP-based protocols [5].

While focusing specifically on DNS and PAF metric, in this paper, we extend the existing work by exploring different underlying causes behind receiving multiple DNS responses to a single query.

## VII. Ethical Considerations

Large-scale Internet measurements must be planned and executed with great caution so that the operation of the tested networks is not disrupted. We contacted the two Institutional Review Boards (IRB) hosting our measurement vantage points and obtained one approval (the University of Twente vantage point) and one IRB exemption (the University of Sydney vantage point, because our study does not directly involve human subjects). We additionally applied best practices introduced by the measurement community [10], [11], [27].

We first considered whether it was necessary to perform our own DNS scans or if we could rely on the existing initiatives, such as Shadowserver's DNS Open Resolvers Report [31]. As our research heavily relies on examining DNS response packets and transient network events (i.e., routing loops), a provided list of open resolvers would not let us accomplish these goals. We instead ran our custom measurements but ensured to randomize the input list of destination hosts and set up a simple web page on all the queried domain names with our contact information. As our scanning infrastructure has been in place for several years, we further excluded more than 5 million IPv4 addresses from the input list as a result of past requests not to be scanned.

More broadly, as we set up a custom authoritative nameserver and performed the scans locally, it is our infrastructure that experienced most of the load from amplifiers. We thus believe not to have disrupted the operation of tested networks.

## VIII. Conclusion

We took an in-depth look at echoing DNS resolvers and identified underlying causes. We show that echoing resolvers can have different impacts on the clients and authoritative nameservers. Such resolvers can increase the power of DNS reflection-based DDoS attacks up to multiple orders of magnitude. Some do so by responding with authentic (large) answers, while others trigger a high-rate stream of failed responses.

We also analyze the behavior of echoing resolvers using various DNS query types. Our results show no significant difference among various query types in triggering echoing resolvers. This aligns with two of the causes behind the existence of echoing resolvers, namely routing loops and IP broadcasting, as these phenomena are DNS agnostic. With respect to IP broadcasting RFC2644 discourages its use. Thus, we recommend network operators to disable (or limit) directed IP broadcast to avoid their networks being exposed to misuse in DDoS attacks.

The third cause behind echoing behavior, i.e., middleboxes, prompted us to evaluate the impact of using a sensitive string in our query names. We show that doing so increases the number of echoing resolvers by a large factor. Moreover, some of these are even high-profile echoing resolvers, strongly suggesting that we are triggering censorship middleboxes.

Finally, we study the stability of echoing resolvers over time. We show that high-profile echoing resolvers typically have a shorter lifetime, which implies that attackers have to trade off between the frequency of discovery scans and the maximum amplification power available to be leveraged.

## Acknowledgments

We would like to thank the anonymous reviewers and our shepherd Matteo Varvello for their valuable feedback on our paper. We gratefully acknowledge the support by ip2location.com, who provided us with an academic license to use their data. This work was partially funded by the Netherlands Organization for Scientific Research (NWO) under grant number NWA.1215.18.003 (CATRIN project), Carnot LSI, and Grenoble Alpes Cybersecurity Institute under contract ANR-15-IDEX-02, the Dutch Centrum voor Veiligheid en Digitalisering (CVD), and the Twente University Centre for Cybersecurity Research (TUCCR).

## References

[1] Y. Afek, A. Bremler-Barr, and L. Shafir, "NXNSAttack: Recursive DNS Inefficiencies and Vulnerabilities," in *Proceedings of the 29th USENIX Conference on Security Symposium*, ser. SEC'20. USA: USENIX Association, 2020.

[2] A. Alaraj, K. Bock, D. Levin, and E. Wustrow, "A Global Measurement of Routing Loops on the Internet," in *Passive and Active Measurement*, A. Brunstrom, M. Flores, and M. Fiore, Eds. Cham: Springer Nature Switzerland, 2023, pp. 373–399.

[3] Anonymous Authors, "The Collateral Damage of Internet Censorship by DNS Injection," *Computer Communication Review*, vol. 42, no. 3, pp. 22–27, 2012.

[4] F. Baker, "RFC1812: Requirements for IP Version 4 Routers," 1995.

[5] K. Bock, A. Alaraj, Y. Fax, K. Hurley, E. Wustrow, and D. Levin, "Weaponizing Middleboxes for TCP Reflected Amplification," *Proceedings of the 30th USENIX Security Symposium*, pp. 3345–3361, 2021.

[6] J. Bushart and C. Rossow, "DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives," in *Research in Attacks, Intrusions, and Defenses*, M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis, Eds. Cham: Springer International Publishing, 2018, pp. 139–160.

[7] Censys. [Online]. Available: "https://censys.io"

[8] A. Chaabane, T. Chen, M. Cunche, E. De Cristofaro, A. Friedman, and M. A. Kaafar, "Censorship in the Wild: Analyzing Internet Filtering in Syria," *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC*, pp. 285–298, 2014.

[9] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks," in *Proceedings of the 2014 Conference on Internet Measurement Conference*, 2014, pp. 435–448. [Online]. Available: http://dx.doi.org/10.1145/2663716.2663717.

[10] D. Dittrich and E. Kenneally, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," https://catalog.caida.org/paper/2012_menlo_report_actual_formatted, accessed: 2023-2-5.

[11] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-Wide Scanning and Its Security Applications," in *Proceedings of the 22nd USENIX Conference on Security*, ser. SEC'13. USA: USENIX Association, 2013, p. 605–620.

[12] N. P. Hoang, A. A. Niaki, J. Dalek, J. Knockel, P. Lin, B. Marczak, M. Crete-Nishihata, P. Gill, and M. Polychronakis, "How Great is the Great Firewall? Measuring China's DNS Censorship," in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 3381–3398. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/hoang

[13] G. Huston, "DNS Zombies," 2016. [Online]. Available: https://blog.apnic.net/2016/04/04/dns-zombies/

[14] M. Kührer, T. Hupperich, J. Bushart, C. Rossow, and T. Holz, "Going Wild: Large-Scale Classification of Open DNS Resolvers," in *Proceedings of the 2015 ACM Internet Measurement Conference - IMC '15*. New York, USA: ACM Press, 2015, pp. 355–368. [Online]. Available: http://dx.doi.org/10.1145/2815675.2815683

[15] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Exit from hell? Reducing the Impact of Amplification DDoS Attacks," in *Proceedings of the 23rd USENIX Security Symposium*, 2014, pp. 111–125.

[16] E. Leverett and A. Kaplan, "Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate," *Journal of Cyber Policy*, vol. 2, no. 2, pp. 195–208, 2017.

[17] B. Liu, C. Lu, H. Duan, Y. Liu, Z. Li, S. Hao, and M. Yang, "Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1113–1128. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/liu-baojun

[18] Q. Lone, M. Luckie, M. Korczyński, and M. van Eeten, "Using Loops Observed in Traceroute to Infer the Ability to Spoof," in *Passive and Active Measurement*, M. A. Kaafar, S. Uhlig, and J. Amann, Eds. Cham: Springer International Publishing, 2017, pp. 229–241.

[19] M. Luckie, "Scamper-CAIDA," 2004. [Online]. Available: https://www.caida.org/catalog/software/scamper/

[20] G. C. M. Moura, S. Castro, J. Heidemann, and W. Hardaker, "TsuNAME: Exploiting Misconfiguration and Vulnerability to DDoS DNS," in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 398–418. [Online]. Available: https://doi.org/10.1145/3487552.3487824

[21] M. Nawrocki, M. Jonker, T. C. Schmidt, and M. Wählisch, "The Far Side of DNS Amplification: Tracing the DDoS Attack Ecosystem from the Internet Core," in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 419–434. [Online]. Available: https://doi.org/10.1145/3487552.3487835

[22] A. Newton, B. Ellacott, and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)," RFC 7480, Mar. 2015. [Online]. Available: https://www.rfc-editor.org/info/rfc7480

[23] A. A. Niaki, N. P. Hoang, P. Gill, and A. Houmansadr, "Triplet Censors: Demystifying Great Firewall's DNS Censorship Behavior," *FOCI 2020 - 10th USENIX Workshop on Free and Open Communications on the Internet, co-located with USENIX Security 2020*, 2020.

[24] Y. Nosyk, M. Korczyński, and A. Duda, "Routing Loops as Mega Amplifiers for DNS-Based DDoS Attacks," in *Passive and Active Measurement*, O. Hohlfeld, G. Moura, and C. Pelsser, Eds. Cham: Springer International Publishing, 2022, pp. 629–644.

[25] J. Park, R. Jang, M. Mohaisen, and D. Mohaisen, "A Large-Scale Behavioral Analysis of the Open DNS Resolvers on the Internet," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 76–89, 2022.

[26] J. Park, A. Khormali, M. Mohaisen, and A. Mohaisen, "Where Are You Taking Me? Behavioral Analysis of Open DNS Resolvers," in *49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019*. IEEE, 2019, pp. 493–504.

[27] C. Partridge and M. Allman, "Ethical Considerations in Network Measurement Papers," *Commun. ACM*, vol. 59, no. 10, p. 58–64, sep 2016. [Online]. Available: https://doi.org/10.1145/2896816

[28] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," in *NDSS*, 2014, pp. 1–15.

[29] M. Sargent, J. Kristoff, V. Paxson, and M. Allman, "On the Potential Abuse of IGMP," *SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 1, p. 27–35, jan 2017. [Online]. Available: https://doi.org/10.1145/3041027.3041031

[30] D. Senie, "RFC2644: Changing the Default for Directed Broadcasts in Routers," 1999.

[31] Shadowserver, "DNS Open Resolvers Report," https://www.shadowserver.org/what-we-do/network-reporting/dns-open-resolvers-report/, Feb. 2023.

[32] O. van der Toorn, J. Krupp, M. Jonker, R. van Rijswijk - Deij, C. Rossow, and A. Sperotto, "ANYway: Measuring the Amplification DDoS Potential of Domains," in *2021 17th International Conference on Network and Service Management (CNSM)*. United States: IEEE, Oct. 2021.

[33] R. van Rijswijk-Deij, A. Sperotto, and A. Pras, "DNSSEC and Its Potential for DDoS Attacks: A Comprehensive Measurement Study," in *Proceedings of the 2014 Conference on Internet Measurement Conference*, ser. IMC '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 449–460.

[34] J. Xia, L. Gao, and T. Fei, "Flooding Attacks by Exploiting Persistent Forwarding Loops," in *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement*, 2005, pp. 36–36.

[35] R. Yazdani, R. van Rijswijk-Deij, M. Jonker, and A. Sperotto, "A Matter of Degree: Characterizing the Amplification Power of Open DNS Resolvers," in *Passive and Active Measurement*, O. Hohlfeld, G. Moura, and C. Pelsser, Eds. Cham: Springer International Publishing, 2022, pp. 293–318. [Online]. Available: https://doi.org/10.1007/978-3-030-98785-5_13