A First Look at the Adoption of BGP-based DDoS Scrubbing Services: A 5-year Longitudinal Analysis

Shyam Krishna Khadka[*], Suzan Bayhan[*], Ralph Holz[‡*], Saeedeh Shokoohi[§], Marinho Barcellos[§], Cristian Hesselman[†*]
[*]University of Twente, Enschede, The Netherlands, [†]SIDN Labs, Arnhem, The Netherlands
[‡]University of Münster, Münster, Germany, [§]University of Waikato, Hamilton, New Zealand

***Abstract*—Besides being the de facto routing protocol of the Internet, the Border Gateway Protocol (BGP) has also been used for mitigating Distributed Denial of Service (DDoS) attacks for many years. In such situations, victims of DDoS attacks use BGP to redirect attack traffic to a "scrubber" outside their network, which separates clean traffic from DDoS traffic and forwards the former to the victim's network. While there exist many BGP-based DDoS scrubbing providers, their adoption on the global Internet remains unstudied. This paper aims to fill this gap by identifying and characterizing Autonomous Systems (ASes) and prefixes protected by five of the leading scrubbing providers, using AS path patterns in public BGP routing data. Our study focuses on scrubbers that allow their protected ASes to originate their prefixes themselves. We find that the percentage of ASes using this kind of protection has increased almost three times (from 0.7% to 2% and from 464 ASes to 1,730 ASes) between 2020 and 2024. Similarly, the percentage of protected prefixes has also increased three times in the same period, from 0.3% to 0.9% and from 3,154 to 12,362 prefixes, across both IPv4 and IPv6. Globally, we observe a higher adoption rate among financial institutions, while adoption remains low among educational institutions. We believe our insights will be useful for individual AS operators to find the transit providers or peers that are DDoS-protected. It might also be useful for (national) policy-makers to incentivize the adoption of DDoS protection services and for researchers studying the phenomenon of DDoS scrubbing.**

***Index Terms*—DDoS protection, BGP-based scrubbing.**

I. Introduction

Distributed Denial of Service (DDoS) attacks have been plaguing the Internet since at least 1999 [1] and have caused large-scale outages [2], [3]. The size of volumetric DDoS attacks is now in the Tbps range and continues to increase. For example, network layer DDoS attacks increased by 51% QoQ (Quarter-on-Quarter) and 45% YoY (Year-over-Year), and HTTP DDoS attacks increased by 61% QoQ and 68% YoY in 2024, according to a recent Cloudflare report [4].

To mitigate the effects of DDoS attacks, potential victims often use various protection mechanisms. Examples include Remotely Triggered Blackholing (RTBH) [5], UTRS (Unwanted Traffic Removal Services) [6], and "scrubbing" [7]. The latter is the focus of our paper and involves a DDoS protection provider known as a "scrubber". It operates a global network to attract DDoS traffic addressed to networks it protects, filters attack traffic, and forwards the rest to the protected networks. We refer to the activity of filtering and forwarding as the "scrubbing service" and call the receiver of the cleaned traffic a "protected AS" and its prefixes "protected prefixes". A protected AS can have protection for one or more of its prefixes. In BGP-based scrubbing, the protected AS modifies its BGP configuration to redirect DDoS traffic to the scrubber.

In this paper, we study *the deployment of BGP-based scrubbing services* on the global Internet, which, to the best of our knowledge, is largely unexplored. We believe such insight is important for multiple stakeholders. For example, individual AS operators could use insights from our work to select transit providers or peers that are DDoS-protected, especially if peering databases like PeeringDB [8] include DDoS-protection attributes in the future. The MANRS+ working group, which aims to enhance routing security through stricter compliance and audits, values data on ASes' DDoS protection levels. Our dataset can support their "DDoS Attack Prevention" metric, which tracks ASes using BGP-based DDoS protection [9]. Also, national policymakers or network operator groups can use our work to consider the adoption of DDoS protection services in their country or community, respectively.

In this paper, we aim to obtain an initial understanding of the adoption of BGP-based DDoS scrubbing services. We therefore answer the following three research questions:

- How has the deployment of BGP-based DDoS scrubbing services on the Internet evolved longitudinally?
- What are the characteristics of the protected ASes in terms of service type and geographical coverage?
- What are the characteristics of the protected prefixes in terms of popular domains hosted there?

To answer these questions, we develop a novel methodology to identify and characterize protected ASes using public BGP data, focusing on scrubbers that let ASes originate their own prefixes. We study five leading scrubbers following this model: Akamai Prolexic, Cloudflare, Imperva, Vercara (formerly Neustar), and Radware. We verified their working models via documentation and discussions with Cloudflare, Akamai, and Radware. We selected these scrubbers based on the 2021 Forrester Wave market analysis [10], also used in prior works [7], [11]. We speculate that this model dominates because it preserves the original origin ASN, giving the protected AS more control while avoiding routing issues such as RPKI-invalid announcements.

The mechanism behind our methodology is to look for AS path patterns in public BGP data that involve a scrubber's AS Number (ASN) and consider an AS positioned downstream

978-3-903176-75-1 ©2025 IFIP

from the scrubber AS as a protected AS. We choose this mechanism as there exists no explicit attribute in BGP that would identify which ASes are protected by a scrubber, unlike the BGP blackhole community attribute [5] for RTBH.

Our contributions and key findings are as follows:

- We develop and implement a methodology that sheds light on the adoption of the five top BGP-based DDoS scrubbers from 2020 to 2024.
- We find that the global adoption of these top scrubbers is surprisingly small, an indication that the overall adoption of scrubbing may not be high.
- Despite the low adoption, we find that the number of ASes protected by scrubbers has grown substantially in 5 years, from 0.7% to 2%.
- We characterize protected ASes and find that most belong to finance and insurance organizations.
- We rank the top 8 countries that use scrubbing services and the proportion of the ASes with the total ASes registered in that country.
- We characterize the protected prefixes and find they cover 1.12% of the top 100k domains of the Tranco list in 2024.

II. Background

We provide a brief overview how BGP-based DDoS scrubbers work and two types of protection modes they support. We refer to the literature for details on other DDoS mitigation techniques, such as DNS-based scrubbing [12], UTRS [6], and blackholing [12], [13].

A. *Working of BGP-based DDoS scrubbing*

Figure 1 shows a high-level overview of how a BGP-based DDoS scrubber works. A protected AS establishes a connection to its scrubber via methods such as GRE connections [14], direct connections [15], or a peering setup (e.g., via an Internet exchange or data center [16]) (step 1 in Figure 1). The AS announces its route to the scrubber via BGP or static routing. BGP-based scrubbing simplifies network management and is a method that we confirmed to be used by scrubbers such as Akamai.

The scrubber announces the protected AS' prefixes to the rest of the Internet (step 2). This way, the traffic addressed to the protected network will subsequently pass through the scrubber. During a DDoS attack, the scrubber identifies the legitimate traffic, blocks the DDoS attack traffic (step 3), and forwards the legitimate traffic to the protected AS (step 4) using the connection established in step 1.

The scrubber generally runs a globally distributed network of data centers so that it can mitigate a DDoS attack as closely as possible to the source. The outbound traffic from the protected network (step 5) goes through a normal upstream Internet Service Provider (ISP).

B. *Protection modes of BGP-based DDoS scrubbing*

BGP-based scrubbers offer two types of protection modes: "always-on" and "on-demand" [15], [17], [18], [19], [20]. In the always-on mode of protection, an AS always announces its

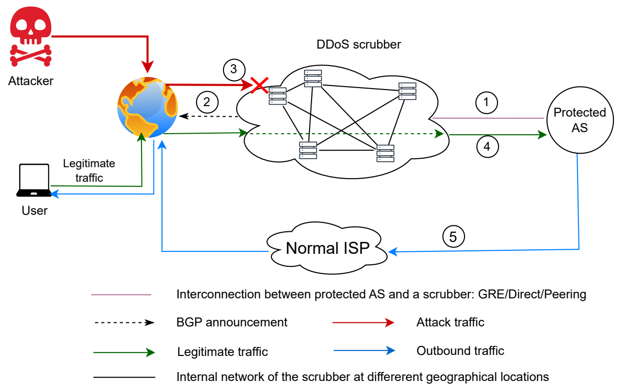

Attacker
DDoS scrubber
3
2
1
4
Protected AS
Legitimate traffic
User
Normal ISP
5
Interconnection between protected AS and a scrubber: GRE/Direct/Peering
BGP announcement
Attack traffic
Legitimate traffic
Outbound traffic
Internal network of the scrubber at differerent geographical locations

Fig. 1: Working of a BGP-based DDoS scrubber.

prefix through a scrubber, so that the scrubber always appears on the paths toward that AS. In on-demand mode, a protected AS announces its prefix via the scrubber only during an attack, so the scrubber appears on the path only then.

III. Related work

To the best of our knowledge, no prior work has measured the longitudinal adoption of BGP-based DDoS scrubbing. Tung et al. [21] propose a method to distinguish DDoS attacks from other BGP anomalies and analyze scrubber behavior during attacks. However, their study covers only one attack on three prefixes of a single AS, lacks longitudinal analysis, and detects only ASes that were past victims. In contrast, our method infers the protected ASes of BGP-based scrubbers regardless of prior attacks, and these scrubbers allow ASes to originate their own prefixes.

Jonker et al. [7] study the adoption of the top nine DNS-based DDoS Protection Services (DPSs) identified via Forrester Wave. They consider a website DDoS-protected if its DNS records (NS, A, or CNAME) point to any of these DPSs. Giotsas et al. [22] infer BGP blackholing activities on the Internet by building a dictionary of BGP communities that ASes use for blackholing. They then use public BGP route collectors to find blackholed prefixes. Anghel et al. [6] analyze UTRS and find it to be largely ineffective: only 10% of 1,200+ members triggered mitigation, 0.025% of ASes responded to AmpPot attacks, and 1.03% of attacks targeted UTRS members.

IV. Methodology

This section presents our methodology to find ASes and prefixes that are protected by BGP-based scrubbers.

A. *Identifying AS path patterns of scrubbers*

To understand how BGP-based DDoS scrubbers operate in practice, we explored the documentation of eight scrubbers: the top five [15], [19], [23]–[25] according to Forrester Wave, as well as F5 [26], NexusGuard [27], and DDoS-Guard [28]. We also analyzed reports on historical scrubbing activities, including blogs [29], [30] and mailing lists [31]. We validated our understanding of the mechanisms with operators from four scrubbers: NaWas from the Netherlands, DDoS-Guard, Akamai, and Radware.

To analyze the evolution of scrubbing over five years, we sample BGP data on the first day of each month (see Section IV-D). Each sample contains a mix of attack and non-attack scenarios. Since we consider only one day per month, we cannot distinguish between on-demand and always-on protection, which requires continuous prefix monitoring. Based on our exploration of scrubbing mechanisms and collected BGP data, we identified the following four AS path patterns.

Pattern 1: scrubber as the immediate provider. We consider an AS a protected AS when its immediate provider is a scrubber AS in an AS path. For example, in the AS path *41666 34927 1299 198949 6352*, AS6352 is a protected AS because AS198949 is a known scrubber (Radware). An example of a scrubber that follows pattern 1 is Cloudflare, whose documentation indicates that an AS connecting to Cloudflare's BGP-based scrubbing service via its Network Interconnect can choose its own ASN as the origin with Cloudflare's ASN prepended [17]. The mode of operation that this AS path pattern represents is also mentioned in Cisco ThousandEyes [32] and Kentik [33] blogs.

Pattern 2: scrubber prepended with the protected AS. We also consider an AS protected if it performs path prepending toward a scrubber. This signals that the AS has a BGP connection with the scrubber that it activates by prepending itself on the AS path toward either the scrubber or their ISP so that BGP favors the path through the scrubber. For example, in the AS path *1798 3356 198949 12235 12235*, AS12235 is a protected AS because it prepends itself toward the scrubber (AS198949). Examples of path prepending in practice are documented by scrubbers such as Imperva [34] and Radware [35].

Pattern 3: scrubber prepended with siblings of the protected AS. This pattern is similar to pattern 2, except that the protected AS uses multiple *different* ASNs that it holds to prepend itself. For example, in the AS path *37721 2914 198949 26613 28006*, ASNs 28006 and 26613 are owned by the same organization (an ISP in Ecuador) and are "sibling" ASes. We find sibling ASes through the CAIDA AS Rank API [36]. In this case, we mark AS28006 as the protected AS because it is the one that owns and originates the prefix. Organizations may route traffic through one ASN with a scrubber connection, letting siblings avoid separate BGP sessions. This simplifies routing and centralizes scrubbing.

Pattern 4: scrubber prepended with non-sibling ASes. This fourth pattern does not confirm whether an AS is using a scrubbing service. We found some cases where an AS is neither prepending its own ASN nor one of its siblings. For example, in the AS path *1798 174 1299 198949 12625 15814*, the scrubber ASN (*198949*) comes in the third-last position, but the origin AS15814 neither prepends its ASN nor that of one of its siblings. We are hence unable to conclude that AS15814 is using a scrubber. This pattern is very rare (see Section IV-D): we find it on occasion for Akamai (18 unique ASes), Cloudflare (0), Vercara (1), Imperva (4), and Radware (7), which corresponds to 2.7%, 0%, 2.4%, 2.7%, and 5.9% of the total protected ASes, respectively.

TABLE I: ASNs of scrubbers

Scrubber	ASN	Resources and methods used to find ASN
Akamai Prolexic	32787	Akamai Prolexic website [15], Cloudflare Radar report [39], and Cisco ThousandEyes blogs [32], [40].
Cloudflare	13335	Cloudflare Magic Transit website [17], and Kentik blog [29].
Vercara	19905	Vercara UltraDDoS product website [19], Kentik blog [33], Checked RIBs records and found only AS 19905 appears as upstream AS in AS paths.
Imperva	19551	Imperva website [24], checked RIBs records and found only AS19551 appears as upstream AS in AS paths.
Radware	198949	Out of 3 ASNs that belong to Radware, we found only AS198949 appears as an upstream AS in AS paths (in RIB records).

Out of scope: scrubber as an origin. In this first study into the adoption of BGP-based scrubbing services, we focus on patterns in which the protected AS originates its own prefixes (patterns 1, 2, and 3). However, documentation from Cloudflare [17] indicates that it also allows the protected networks to use Cloudflare's ASN. When this occurs, a different methodology is required to identify protected ASes, which we consider future work (Section VII).

B. Selection of BGP-based DDoS scrubbers

To the best of our knowledge, there is no collated, comprehensive, and authoritative list of DDoS scrubbers. Prior studies have therefore used different sources for their studies. For example, Hiesgen et al. [37] use a list of vendors from a survey report, while Jonker et al. [12], [7], [11] use a list of DDoS protection services from Forrester Wave. We use the 2021 market analysis from Forrester Wave [10] because their research is well known for its open methodology, unlike other market research rankings. The Forrester Wave report identifies the top 11 most significant DDoS protection vendors based on 28 criteria, such as volumetric scrubbing, security operations centers, pricing model, and installation base.

For our study, we focus on the top five vendors: Akamai, Cloudflare, Imperva, Vercara, and Radware. We exclude the others for several reasons: A10 offers only on-premises protection and outsources scrubbing [38]; Lumen (AS3356) is a tier-1 provider, making it impossible to infer scrubbing use from AS paths; and Alibaba Cloud, AWS, and Google provide DDoS protection only within their clouds, which is not visible in public BGP data. Although we use Forrester Wave's list of scrubbers, our method applies to any scrubber, provided its scrubbing ASNs are known and the patterns in Section IV-A are followed.

C. Identifying the AS numbers of scrubbers

All five scrubbers that we choose have multiple ASNs that they use for delivering different types of services, including

BGP-based DDoS scrubbing. To find the ASNs they use for scrubbing, we *manually* went through the companies' websites, other websites showing the mapping of an organization to ASNs (e.g., CAIDA AS rank and PeeringDB), and documents about historical DDoS attacks. We validated that historical DDoS attacks and the scrubbing to mitigate them were captured by the public collectors we selected. We also used BGP Routing Information Bases (RIBs) data, collected by the public route collectors from the RIPE RIS and Routeviews projects. The RIBs data contains snapshots of the global routing data as seen by all public route collectors.

Table I shows the ASNs that the five scrubbers use for scrubbing, and the resources and methods we used to find them. For example, Cloudflare has a product "Magic Transit" for DDoS protection that uses ASN 13335.

D. Building a dataset of protected ASes and prefixes

We use the patterns discussed in Section IV-A to build a dataset of protected ASes that use the kind of BGP-based scrubbers we study here. The scripts we developed go through the following six steps:

Step 1: Collect and sample RIBs. We first obtain routes with the scrubber on the AS path using RIB data. Our objective is to provide insight into the longitudinal adoption of BGP-based DDoS scrubbers, so we choose a monthly snapshot of routing data, taken at 00:00 UTC of the first day of each month. This reduces storage needs and allows faster processing of RIBs data. The disadvantage is that a protected AS might sign up for DDoS protection but cancel before the next snapshot, so our methodology will miss such ASes.

Step 2: De-duplicate BGP data. We remove repeated announcements for the same prefix with identical AS paths. We observed these occur for various reasons, such as a collector peer dumping the same data to multiple collectors, and multiple collector peers dumping the same data.

Step 3: Remove records with a scrubber as an origin. When a scrubber appears as the origin ASN for a prefix, the prefix may not necessarily be related to scrubbing activity. A scrubber can also originate its prefixes for internal network management purposes. Therefore, we exclude records where the scrubber ASN appears as the origin of a protected prefix.

Step 4: Remove unwanted ASNs. We filter out unnecessary AS paths, including those with private ASNs [41], AS sets [42] which obscure the originating AS, and siblings of the scrubber.

Step 5: Apply AS pattern detection. We identify records that follow the patterns presented in Section IV-A and consider the origin ASes protected and the originated prefixes protected if they correspond to one of our first three patterns.

Step 6: De-duplicate prefixes and ASNs. We find cases where the same protected AS follows both AS path pattern 1 and AS path pattern 2 for its prefixes. We speculate that prefixes matching AS pattern 1 may host critical services of the protected AS and therefore utilize always-on scrubbing, whereas prefixes following pattern 2 may rely on on-demand protection, enabling them to remove path prepending dynamically when an attack is detected. We remove duplicates to consider unique ASes and unique prefixes.

V. Results

We analyze the adoption of BGP-based scrubbers from 2020 to 2024,[1] based on the dataset of protected ASes and prefixes described in Section IV. Further, we characterize the significance of protected ASes by examining the services they provide (e.g., financial, government). We also map the protected prefixes to the most popular domain names from the Alexa and Tranco 1M lists.

A. Global adoption of BGP-based scrubbers

Using RIBs data from 2020–2024, we observe the number of ASes growing from 68k to 84k and prefixes from 1.1M to 1.4M in the Internet. Figure 2a shows the percentage of ASes using BGP-based scrubbing increased from 0.7% to 2% (464 ASes to 1,730 ASes), while protected prefixes grew 3.06 times, from 0.3% (3,154) to 0.9% (12,362), including both IPv4 and IPv6.

Figures 2b, 2c, and 2d show the adoption trends for the five scrubbers. For fair comparison, we map IPv4 prefixes to /24, the smallest commonly routable prefix. Akamai Prolexic leads in protected ASes and prefixes, though its IPv4 coverage declines after 2022. Cloudflare protects a similar number of ASes but far fewer prefixes, suggesting its customers are smaller ASes. Imperva and Radware show comparable levels, while Vercara has the fewest protected ASes and prefixes.

B. Coverage of different types of AS path patterns

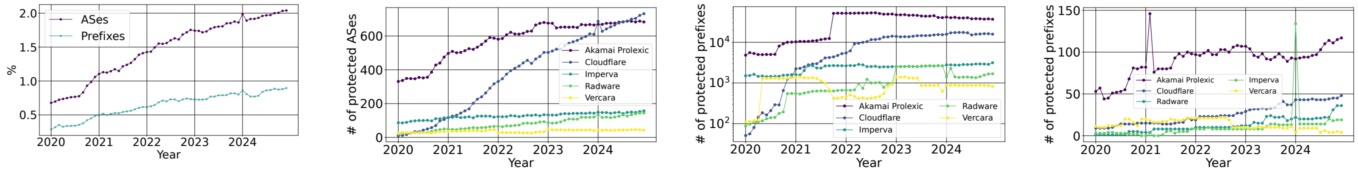
We analyze the distribution of protected ASes across the patterns in Section IV-A, averaging their percentages over 12 monthly snapshots from 2024 (the most recent year). We focus on 2024 to examine how often each pattern occurs and which scrubbers use them. Figure 3 shows the average distribution of the four AS path patterns. Pattern 1 dominates, covering at least 75% of ASes for all five scrubbers. Cloudflare appears as the immediate provider in 99.73% of cases. Pattern 2 accounts for the remaining 0.27%, with no other patterns observed. Pattern 3 remains rare, peaking at 2.17%. Path prepending (pattern 2) occurs more often with Imperva than with other scrubbers.

C. Correlating protected prefixes with top-domain lists

To assess the relevance of the protected prefixes in our dataset, we determine how many of the top 100k domains from Alexa 1M [44] and Tranco 1M lists [45] map to a protected prefix. The analysis between 2020 and 2022 is based on the top 100k prefixes from the Alexa list, which was discontinued in 2022, and then on Tranco, for 2023 and 2024.

We use OpenIntel's DNS data [46] to extract *A* records of the domains. Some domains have multiple *A* records, and some IPs host multiple domains. We count unique domains

[1] We choose 2020 as the starting year it coincides with Cloudflare's launch of its DDoS scrubbing service [43].



(a) Aggregate protected ASes and prefixes of the scrubbers.

(b) Protected ASes.

(c) Protected prefixes IPv4 mapped to /24.

(d) Protected prefixes IPv6.

Fig. 2: (a) The adoption rate of BGP-based DDoS scrubbers globally, showing the aggregated number of protected ASes and prefixes; (b) the number of protected ASes for individual scrubbers; (c) the number of protected IPv4 prefixes of different lengths, normalized to /24 and shown in log scale; and (d) the number of protected IPv6 prefixes.

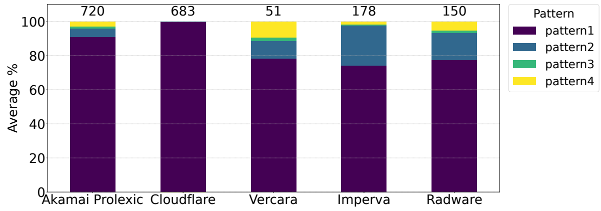


Fig. 3: Distribution of protected ASes across four patterns in 2024 (see Section IV-A). Numbers at the top bars indicate the average number of protected ASes per scrubber.

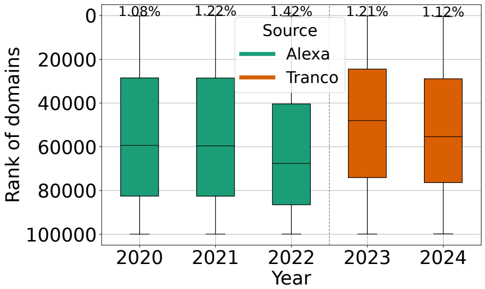


Fig. 4: Distribution of Alexa (2020 to 2022) and Tranco 100k (2023-2024) domains hosted on IP addresses in protected prefixes based on their rank. The percentage is the share of domains on protected IP addresses.

and IPs regardless of such overlaps. For example, in 2022, 1,031 protected prefixes hosted 1,424 Alexa domains, with the highest-ranked domain at position 147 and the lowest at 99,961.

Figure 4 shows a box plot illustrating the distribution of Alexa and Tranco's top 100k domains covered by a protected prefix in our dataset. The percentages at the top of each box plot give the proportion of the top 100k domains that are hosted on protected IP addresses for the corresponding year. We see a growing trend in this percentage between 2020 and 2022: from 1.08% in 2020 to 1.42% in 2022, indicating a growing adoption of protected IP hosting among the Alexa-ranked domains. For Tranco, the share of protected domains is 1.21% in 2023 and 1.12% in 2024.

The falling median rank in Figure 4 suggests that recently, mainly mid-ranked and lower-ranked websites use BGP-based scrubbing. Possible reasons for this include top sites having adopted protection before 2020 (e.g., early COVID) and growing reliance on CDNs, which offer their own DDoS protection outside the scope of the five scrubbers studied. This may also explain the decline in protected domains in 2024.

D. *Service types of protected ASes globally*

We classify ASes globally based on the services they offer, such as financial ASes, cloud ASes, and education ASes. We use the Stanford ASdb dataset [47], which maps an AS to an organization and then classifies the AS based on the organization's industry, based on 17 categories and 95 subcategories. We use 2021 data as it is the earliest available.

We find that most of the protected ASes (1,295 out of a total of 1,730 protected ASes) belong to the following 9 categories: Finance, Health, Retail, Manufacturing, Cloud, Government, IT, ISP, and Education.[2] For the selected categories, we compute the percentage of ASes of each type, shown in Figure 5. As of December 1, 2024, 7.04% of financial ASes (494 out of 7,021, as classified by ASdb) used scrubbing services. Financial institutions have consistently led in BGP-based scrubbing adoption since 2021. In contrast, adoption rates among educational ASes (0.61% i.e. 5053 in total) and ISPs (0.66%) remain notably low. ISPs represent the largest group, with 37,735 in 2024. In absolute terms, ISPs rank second only to financial institutions in the number of ASes protected by scrubbing.

E. *Country-wise analysis of ASes*

We analyze the protected ASes to know which countries' ASNs use BGP-based scrubbing services the most. We identify the countries where the protected ASes are registered using the CAIDA AS Organizations.[3] We observe that the eight countries with the most ASes using the five scrubbers are the United States (676), the United Kingdom (100), Australia (82), Germany (58), Hong Kong (51), Canada (50), France (33), and Switzerland (31). These correspond to 2.2%, 3.2%, 2.8%, 1.9%, 4.2%, 2.2%, 1.5%, and 2.9% of the total ASNs registered in each respective country.

[2] We shorten ASdb category names for readability, e.g., Finance for "Finance and Insurance" and Cloud for "Hosting and Cloud Provider."

[3] https://www.caida.org/catalog/datasets/as-organizations

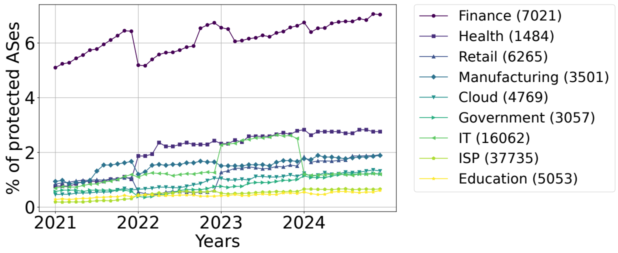


Fig. 5: Percentage of nine types of ASes that are more often protected by the five scrubbers over the years. The numbers in each legend show the total number of ASes of that type on the Internet as classified by ASdb on 01 Jan 2024.

VI. Discussion and limitations

Our findings show the overall growth in the adoption of BGP-based DDoS scrubbing services from 2020 to 2024, with the financial sector leading globally, followed by ISPs in terms of the absolute number of protected ASes, making them the second most protected business type as of December 1, 2024. When comparing proportions relative to the total number of ASes in each sector, finance ranks first, followed by the health sector. One possible explanation for the high adoption by financial institutions is that the financial sector received a high share of DDoS attacks: 30% of all attacks in 2023 are targeted at this sector, according to a report from Statista [48]. This suggests that financial institutions may be increasingly adopting scrubbing services in response to these threats. The number of popular Alexa-ranked domains hosted in protected prefixes has also increased.

We see the percentage of the educational sector being the lowest in terms of adoption of BGP-based scrubbing services globally. This may be because network connectivity for most educational institutions is provided by dedicated research and education networks such as SURF (Netherlands), Internet2 (USA), AARNet (Australia), and JANET (UK), which have their own DDoS mitigation capabilities. As a result, these institutions may not be using the commercial scrubbers.

Limitations. We use publicly available BGP data and the CAIDA AS Organizations dataset to identify scrubbing providers, sibling ASes, and map ASes to countries or organization types. Our analysis is limited by these datasets. RouteViews and RIS offer only a partial view of the Internet, possibly missing some scrubbing-protected prefixes and ASes. Similarly, while CAIDA groups ASes by organization, manual checks revealed misclassifications of sibling ASes, which may lead to undercounting some protected ASes and prefixes.

Beyond these inherent dataset limitations, we acknowledge the following limitations in the scope of our work:

1) In this initial study, we focus on five scrubbers, providing a limited view of BGP-based scrubbing adoption. Our results may not generalize to the entire ecosystem of such services.

2) We cannot identify a protected AS when the scrubber is the origin ASN, as the protected AS is absent from the path and the prefix may belong to the scrubber's network. One approach is to track prefix origin changes over time, from the protected AS to the scrubber, indicating delegated origin during an attack.

3) Our methodology likely misses ASes using on-demand protection, since we rely on 12 yearly BGP snapshots. Capturing these would require finer-grained BGP data, as DDoS attacks can be very short (e.g., minutes).

VII. Conclusion and future work

This paper presents the first study into the adoption and characterization of BGP-based DDoS scrubbers globally in the period 2020-2024, based on a novel method that we developed to find protected ASes and prefixes. Our study uses the top five scrubbers worldwide. We show that 2% of ASes out of around 84k ASes and 0.9% of prefixes out of 1.4M prefixes that are globally routable use one of our chosen BGP-based DDoS scrubbing services as of 1 Dec 2024.

To the best of our knowledge, the adoption of BGP-based DDoS scrubbing services is unexplored territory, and therefore, we believe our work also leads to new research questions. One topic we plan to explore is identifying protected ASes and prefixes where the scrubber appears as the origin ASN, providing DDoS protection for a network whose ASN is not visible in the AS paths. Assessing the effectiveness of scrubbing services in mitigating DDoS attacks is another future direction.

Acknowledgment

This research received funding from the Dutch Research Council (NWO) as part of the projects CATRIN (NWA.1215.18.003) and UPIN (CS.004). CATRIN is part of NWO's National Research Agenda (NWA). We thank Simon Kuhn from NaWas for valuable discussions on their scrubbing services.

References

[1] Technology Review, “The first DDoS attack was 20 years ago.This is what we've learned since.” last accessed 10-March-2025. [Online]. Available: https://www.technologyreview.com/2019/04/18/103186/the-first-ddos-attack-was-20-years-ago-this-is-what-weve-learned-since

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the mirai botnet,” in *Proceedings of the 26th USENIX Conference on Security Symposium*, ser. SEC'17. USA: USENIX Association, 2017, p. 1093–1110.

[3] O. Yoachimik and J. Shi, “Record-breaking 5.6 Tbps DDoS attack and global DDoS trends for 2024 Q4,” Last accessed 10-March-2025. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q4/

[4] Omer Yoachimik and Jorge Pacheco, “DDoS threat report for 2024 q3,” 2024, Last accessed 26-November-2024. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-for-2024-q3

[5] T. King, C. Dietzel, J. Snijders, G. Döring, and G. Hankins, “BLACKHOLE Community,” RFC 7999, Oct. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7999

[6] R. Anghel, S. Vetrivel, E. T. Rodriguez, K. Sameshima, D. Makita, K. Yoshioka, C. Gañán, and Y. Zhauniarovich, “Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks,” in *Computer Security – ESORICS 2023: 28th European Symposium on Research in Computer Security Proceedings, Part II.* Berlin, Heidelberg: Springer-Verlag, 2024, p. 23–41. [Online]. Available: https://doi.org/10.1007/978-3-031-51476-0_2

[7] M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, “Measuring the adoption of DDoS protection services,” in *Proceedings of the Internet Measurement Conference*, 2016, pp. 279–285.

[8] Peeringdb, “PeeringDB,” 2024, Last accessed 13-November-2024. [Online]. Available: https://www.peeringdb.com/

[9] MANRS, “MANRS+ Controls,” Last accessed 31-January-2025. [Online]. Available: https://manrs.org/wp-content/uploads/2023/12/MANRSPlus_Controls.pdf

[10] D. Holmes, “The forrester wave™: DDoS mitigation solutions, q1 2021,” 2021, Last accessed 14-January-2025. [Online]. Available: https://allofsecurity.pl/wp-content/uploads/2021/03/The-Forrester-Wave-DDoS-Mitigation-Solutions-Q1-2021.pdf

[11] M. Jonker, A. Sperotto, and A. Pras, “DDoS Mitigation: A measurement-based approach,” in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2020, pp. 1–6.

[12] M. Jonker, A. Pras, A. Dainotti, and A. Sperotto, “A first joint look at DoS attacks and BGP blackholing in the wild,” in *Proceedings of the Internet Measurement Conference 2018*, ser. IMC ’18. Association for Computing Machinery, 2018, pp. 457–463. [Online]. Available: https://dl.acm.org/doi/10.1145/3278532.3278571

[13] M. Nawrocki, J. Blendin, C. Dietzel, T. C. Schmidt, and M. Wählisch, “Down the black hole: Dismantling operational practices of BGP blackholing at IXPs,” in *Proceedings of the Internet Measurement Conference*, ser. IMC ’19. Association for Computing Machinery, 2019, pp. 435–448. [Online]. Available: https://dl.acm.org/doi/10.1145/3355369.3355593

[14] Radware Support, “How to setup GRE tunnels,” 2019, Last accessed 05-December-2024. [Online]. Available: https://support.radware.com/app/answers/answer_view/a_id/1018552/~/how-to-setup-gre-tunnels

[15] Akamai, “Prolexic - comprehensive DDoS attack protection,” Last accessed 13-November-2024. [Online]. Available: https://www.akamai.com/resources/product-brief/prolexic

[16] Cloudflare Docs, “About | cloudflare network interconnect docs,” 2024. [Online]. Available: https://developers.cloudflare.com/network-interconnect/about/

[17] Cloudflare Magic Transit Docs, “Advertise prefixes,” 2024, Last accessed 14-November-2024. [Online]. Available: https://developers.cloudflare.com/magic-transit/how-to/advertise-prefixes/

[18] Radware Doc, “DDoS Protector Cloud Service,” https://www.radware.com/getattachment/bfc20642-47c5-4e1a-adb4-40350695541e/ds-checkpoint-ddos-protector-cloud-service.pdf.aspx, 2024, Last accessed 12-November-2024.

[19] Team, Vercara, “UltraDDoS protect - FAQs,” 2024, last accessed 19-November-2024. [Online]. Available: https://vercara.com/resources/ultraddos-protect

[20] Imperva, “Advanced DDoS Protection & Mitigation Services,” Last accessed 11-March-2025. [Online]. Available: https://www.imperva.com/products/ddos-protection-services/

[21] T. M. Tung, C. Wang, and J. Wang, “Understanding the behaviors of BGP-based DDoS protection services,” in *Network and System Security*, Man Ho Au et al., Ed. Springer International Publishing, 2018, pp. 463–473.

[22] V. Giotsas, G. Smaragdakis, C. Dietzel, P. Richter, A. Feldmann, and A. Berger, “Inferring bgp blackholing activity in the internet,” in *Proceedings of the 2017 Internet Measurement Conference*, ser. IMC ’17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1–14. [Online]. Available: https://doi.org/10.1145/3131365.3131379

[23] “Magic Transit — DDoS Protection for Networks — Cloudflar,” 2024, Last accessed 31-May-2024. [Online]. Available: https://www.cloudflare.com/network-services/products/magic-transit/

[24] Wallace Lee, “DDoS Protection for Networks: Combatting Local Preference from ISPs — Imperva ,” 2020, Last accessed 16-November-2024. [Online]. Available: https://www.imperva.com/blog/ddos-protection-for-networks-combatting-local-preference-from-isps/

[25] Radware, “Radware Cloud DDoS Protection Service Onboarding Guide,” Last accessed 11-March-2025. [Online]. Available: https://www.radware.com/getattachment/96afe5ae-a67d-405f-a1be-1a651b3f513f/Radware-Cloud-DDoS-Protection-Service-Onboarding-Guide.pdf.aspx

[26] F5 Doc, “How to configure BGP for DDoS Protection?” Last accessed 11-March-2025. [Online]. Available: https://f5cloud.zendesk.com/hc/en-us/articles/20388402037399-How-to-configure-BGP-for-DDoS-Protection

[27] Nexusguard, “Safeguarding Customer Assets with Nexusguard On-Net,” Last accessed 12-March-2025. [Online]. Available: https://www.nexusguard.com/blog/safeguarding-customer-assets-with-nexusguard-on-net

[28] DDoS-Guard, “What is BGP-Based DDoS Protection,” Last accessed 05-February-2025. [Online]. Available: https://ddos-guard.net/blog/bgp-based-ddos-protection

[29] Phil Gervasi, “How Kentik Visualizes the BGP Propagation of a DDoS Mitigation ,” 2022, Last accessed 14-November-2024. [Online]. Available: https://www.kentik.com/blog/how-bgp-propagation-affects-ddos-mitigation/

[30] Nick Kephart, “Using BGP to Reroute Traffic during a DDoS,” 2014, Last accessed 31-May-2024. [Online]. Available: https://www.thousandeyes.com/blog/using-bgp-reroute-traffic-ddos

[31] Tom Krenn, “Re: announcing IPs by scrubbing service to help with DDoS attacks and ROAs ,” Last accessed 05-February-2025. [Online]. Available: https://seclists.org/nanog/2023/Nov/96

[32] Archana Kesavan, “Outage Analyses How GitHub Successfully Mitigated a DDoS Attack,” 2018, Last accessed 13-November-2024. [Online]. Available: https://www.thousandeyes.com/blog/how-github-successfully-mitigated-ddos-attack

[33] Justin Ryburn, “BGP Flowspec Doesn’t Suck. We’re Just Using it Wrong.” 2024, Last accessed 17-July-2024. [Online]. Available: https://www.kentik.com/blog/bgp-flowspec-doesnt-suck-were-just-using-it-wrong/

[34] W. Lee, “DDoS Protection for Networks,” Last accessed 05-February-2025. [Online]. Available: https://www.imperva.com/blog/ddos-protection-for-networks-utilizing-as-prepending-to-route-traffic-through-imperva/

[35] Radware, “Choosing the Best Diversion For Your Needs,” 2019, Last accessed 05-December-2024. [Online]. Available: https://support.radware.com/app/answers/answer_view/a_id/1018554/related/1

[36] CAIDA, “AS Rank,” March 2024. [Online]. Available: https://doi.org/10.21986/CAIDA.DATA.AS-RANK

[37] R. Hiesgen, M. Nawrocki, M. Barcellos, D. Kopp, O. Hohlfeld, E. Chan, R. Dobbins, C. Doerr, C. Rossow, D. R. Thomas, M. Jonker, R. Mok, X. Luo, J. Kristoff, T. C. Schmidt, M. Wählisch, and K. Claffy, “The age of DDoScovery: An empirical comparison of industry and academic DDoS assessments,” in *Proceedings of the 2024 ACM on Internet Measurement Conference*. ACM, 2024, pp. 259–279.

[38] Digitalisation World, “A10 networks extends multi-vector DDoS protection,” 2016, Last accessed 19-November-2024. [Online]. Available: https://m.digitalisationworld.com/news/46791/a10-networks-extends-multi-vector-ddos-protection

[39] Cloudflare Radar, “AS32787 overview,” 2024. [Online]. Available: https://radar.cloudflare.com/as32787

[40] Mike Hicks, “Akamai Prolexic Routed Outage Analysis,” Last accessed 05-February-2025. [Online]. Available: https://www.thousandeyes.com/blog/akamai-prolexic-routed-outage-analysis

[41] J. Mitchell, “Autonomous System (AS) Reservation for Private Use,” RFC 6996, 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc6996

[42] Y. Rekhter, S. Hares, and T. Li, “A Border Gateway Protocol 4 (BGP-4),” RFC 4271, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4271

[43] Rustam Lalkaka, “Magic Transit makes your network smarter, better, stronger, and cheaper to operate,” Last accessed 05-February-2025. [Online]. Available: https://blog.cloudflare.com/magic-transit/

[44] Mindaugas Slivka, “What is Alexa Rank and Its Value?” Last accessed 20-February-2025. [Online]. Available: https://attentioninsight.com/what-is-alexa-rank-and-its-value/

[45] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, “Tranco: A research-oriented top sites ranking hardened against manipulation,” in *Proceedings of the 26th Annual Network and Distributed System Security Symposium*, ser. NDSS 2019, Feb. 2019.

[46] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, “A high-performance, scalable infrastructure for large-scale active dns measurements,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, pp. 1877–1888, 2016.

[47] CAIDA, “Stanford ASdb,” 2024, Last accessed 10-December-2024. [Online]. Available: https://catalog.caida.org/dataset/stanford_asdb

[48] Statista, “Distribution of DDoS attacks worldwide in 2023, by industry ,” Last accessed 05-February-2025. [Online]. Available: https://www.statista.com/statistics/1537973/ddos-attacks-global-by-industry/