Telemetry from DDOS Protection Sevices Providers

1 DDOS protection Services Provider (DPS)

DDoS Protection Service (DPS) providers mitigating DDoS attacks through scrubbing centres, DPS can be categorized into BGP-based and DNS-based services BGP-based DPS [5]. is favoured for large-scale attacks, leveraging the Border Gateway Protocol to reroute overwhelming malicious traffic from the victim's network to more resilient networks, significantly reducing the attack's impact.

Conversely, DNS-based DPS utilizes DNS redirection, altering the DNS records of the target domain to reroute traffic to the DPS provider's servers. This method filters traffic, removing malicious activities and ensuring only legitimate traffic reaches the target. It hinges on changing DNS resolution, directing domain requests to DPS servers instead of the target's original servers. newbranch-name

2 BGP-Based DPS: Benefits and Limitations

BGP-based DPS excels in mitigating large-scale volumetric attacks. Utilizing the Border Gateway Protocol, it diverts malicious traffic from the victim's network to robust networks equipped for traffic scrubbing. This strategy effectively diminishes the attack's impact and upholds the integrity of the target network, making it a preferred solution for defending against significant DDoS threats. However, implementing BGP-based DPS requires a substantial network infrastructure, typically involving extensive connectivity through multiple transits, Private Network Interconnects (PNI) [2]., and Network Access Points (NAPs), leading to significant investment requirements. Moreover, there is a minimum network size constraint: the network must possess at least a Class C /24 prefix for public internet propagation, as this is the smallest network prefix that can be propagated on the public internet via BGP routing [1]. Smaller networks, which do not have a /24 network or larger, might find this requirement challenging, limiting the feasibility of BGP-based DPS for such organizations.

3 DNS-based DPS: Benefits and Limitations

DNS-based DDoS Protection Services (DPS) offer effective mitigation strategies by modifying the address record (A-record) in the target's DNS server [4]. The strategic adjustment of the Time-To-Live (TTL) values facilitates rapid updates and propagation of DNS records, which is essential in rerouting traffic efficiently during an attack. This method proves especially beneficial for web portals or applications dependent on DNS for reachability, offering a viable solution for small and medium-sized enterprises (SMEs) or organizations with smaller network infrastructures, as it does not necessitate a /24 network prefix. However, the effectiveness of DNS-based DPS is constrained when facing direct-to-IP attacks. Such attacks include services like FTP (File Transfer Protocol), SSH, SMTP (Simple Mail Transfer Protocol) for email, or other proprietary protocols often used in enterprise applications. Given that these services typically operate using fixed IP addresses rather than DNS lookups, DNS-based DPS may struggle to adequately mitigate attacks targeting them.

4 Operational Strategies: Detection and Mitigation

BGP-Based DPS operational strategies are designed to address high-volume attacks targeting network bandwidth. These services utilize a comprehensive detection approach that encompasses Deep Packet Inspection (DPI), netflow analysis, and traffic graph examina-

tion [6] [3]. DPI, including critical payload inspection, is essential in accurately identifying Layer 3 and 4 attacks and is central to attack traffic fingerprinting, providing in-depth information crucial for the mitigation process. DPI's ability to delve into the specifics of packet content makes it an invaluable tool in distinguishing between attack and legitimate traffic. Complementing DPI, netflow and traffic graphs offer insights into traffic flow characteristics and aid in profiling normal legitimate user traffic. This helps in detecting anomalous patterns indicative of DDoS activities. Nonetheless, DPI strategies come with limitations, including their complexity, computational demands, and challenges in analyzing encrypted traffic.

In contrast, DNS-Based DPS targets application-layer attacks and emphasizes analyzing content requests [7]. Unlike Layer 3 or 4 attacks where DPI provides significant benefits, application-layer attack detection in DNS-based DPS can rely on sufficient telemetry from traffic graphs and netflow analysis without necessitating DPI. This is particularly relevant when the network traffic is unrelated to the application layer, such as UDP packet floods or TCP packets on unrelated ports, which are not pertinent for a targeted web server's DPI analysis. DNS-based DPS instead places a greater emphasis on application logs from targeted systems. These logs are pivotal in identifying activities that exploit application vulnerabilities or functionalities, offering direct insights into how the application is being manipulated or overwhelmed by attack traffic. While DPI offers thorough traffic analysis, its effectiveness for DNS-based DPS is limited due to the complexities and demands of DPI, and its limited utility in encrypted traffic analysis.

5 The telemetry discrepancy among DPS in the industry

The telemetry discrepancy between BGP-Based and DNS-Based DDoS Protection Services (DPS) is primarily attributed to the difference in detection and mitigation strategies across various OSI layers and the distinct nature of their customer bases.

Scope and Target Audience Differences BGP-Based DPS, focusing on network prefixes, caters predominantly to large corporations and enterprises. Within a single network prefix, BGP-Based DPS addresses a multitude of entities spanning different network, transport, and application protocols. Conversely, DNS-Based DPS typically provides services per application, often associated with a single IP address, as outlined in the operational strategies section.

Balancing Volumetric Protection and Application Layer Control Additionally, customers utilizing BGP-Based DPS, such as financial institutions, government bodies, and banks, may seek volumetric protection while retaining control over their application layer. For instance, banking customers might be reluctant to share SSL certificates for their portals with the DPS, preferring to maintain exclusive control over the decryption of application content and requests.

6 Industry Trends: Offering Hybrid DPS Solutions

Some DPS providers in the industry are now offering both BGP-based and DNS-based services to provide a comprehensive DDoS mitigation portfolio. This hybrid approach allows for a more versatile defense strategy, catering to a broader range of attack vectors and offering tailored solutions based on the specific needs and infrastructure of the client.

7 Mapping victims with Telescopes and Honeypot

This analysis establish a relationship between our recorded DDOS event data and the Telescopes and Honeypots datasets. It specifically focuses on aligning full-day dates, spanning from midnight to the end of the day, with our defined intervals of DDOS events, as marked by startTime and endTime. In Telescopes' operational design, attacks are detected by analyzing backscattered traffic. This traffic typically results from attack traffic that spoofs its source address to resemble that of the Telescopes' address blocks. Based on this detection method, we can anticipate two primary scenarios: Due to our mitigation mechanisms, there is only a slim chance that the date recorded by Telescopes will coincide with our event dataset. If Telescopes record a date that precedes the startTime and endTime of a DDOS event, it might be indicative of an attack being detected early by the Telescopes. Following this early detection, mitigation measures might be activated within the DDOS event window to address the attack. On the other hand, if a date recorded by Telescopes falls after the DDOS event timeframe, it could imply a re-emergence of the attack, occurring after the mitigation measures detailed in the DDOS event data. The Honeypots dataset, however, provides a contrasting perspective. Unlike Telescopes, Honeypots are not just detection tools; they actively participate in attack mechanisms. As such, their data might align with DDOS events by coincidence. The occurrence of a Honeypot record during a DDOS event does not inherently suggest a direct

link with the event's mitigation processes, as Honeypots operate independently of these countermeasures

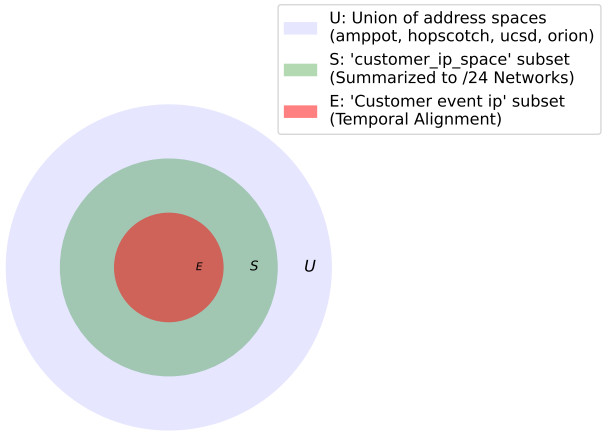

Figure 1: Address sets relationship

'Customer IP Space S' Definition

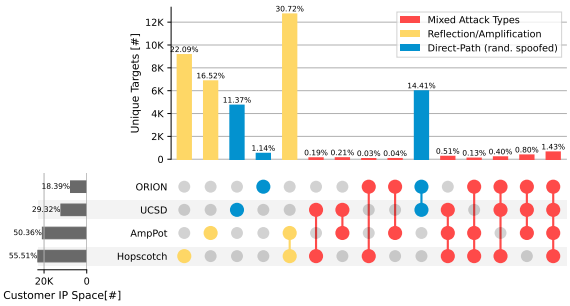

Figure 2: Customer IP Space Analysis.

Fig. 2 shows the attack event detected by telescopes and honeypots for our interested ip space S.

Let U represent the union of address spaces from the categories 'amppot', 'hopscotch', 'ucsd', and 'orion'. The 'customer_ip_space' condition identifies a subset of U, denoted as S, characterized by the following criteria:

1. **Summarization to Class C Networks**: Each IP address in S is summarized to a Class C network, represented by the first three octets of the IP address, effectively transforming the address into a /24 network notation.

2. **Match with Summarized /24 Networks**: An address $s \in S$ is considered part of 'customer_ip_space' if its summarized /24 network matches with any summarized /24 network within U.

'Customer event ip E' Definition

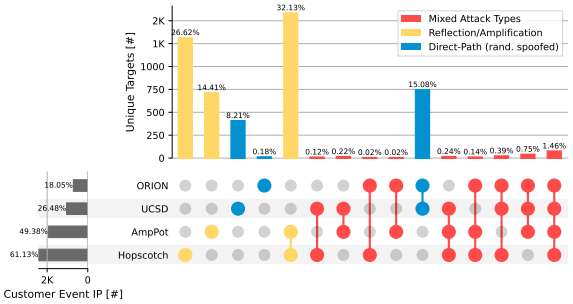

Figure 3: Customer Event IP Analysis.

Fig. 3 shows the attack event detected by telescopes and honeypots for our interested ip attack events S.

Fig. 5 shows summarised the analysis of Customer IP Space, S and Customer Event IP E.

The 'Customer event ip' condition extends the identification of relevant IP addresses by incorporating temporal alignment with specific events. It represents a subset of 'customer_ip_space', denoted as E, with the following additional condition:

1. **Temporal Alignment with Events**: For an address $e \in E$, not only must it satisfy the 'customer_ip_space' criteria, but it must also coincide with an event whose duration (p) matches a specified date (d). The event duration is defined by the start and end times of activity associated with the IP address. An event is considered to match if d falls within this duration, indicating that the event occurred within the specified timeframe.

Fig. 1 shows relationship among the U S E.

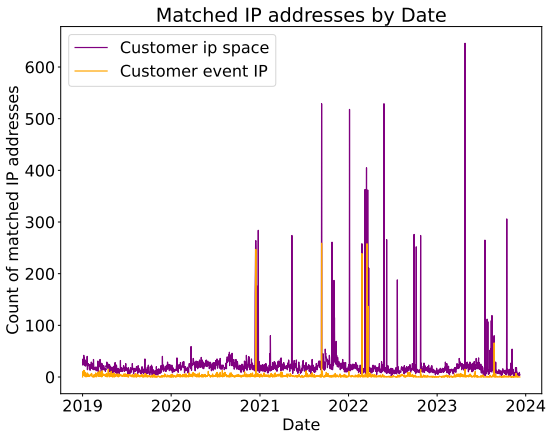

Figure 4: Mapping customer ip space and event.

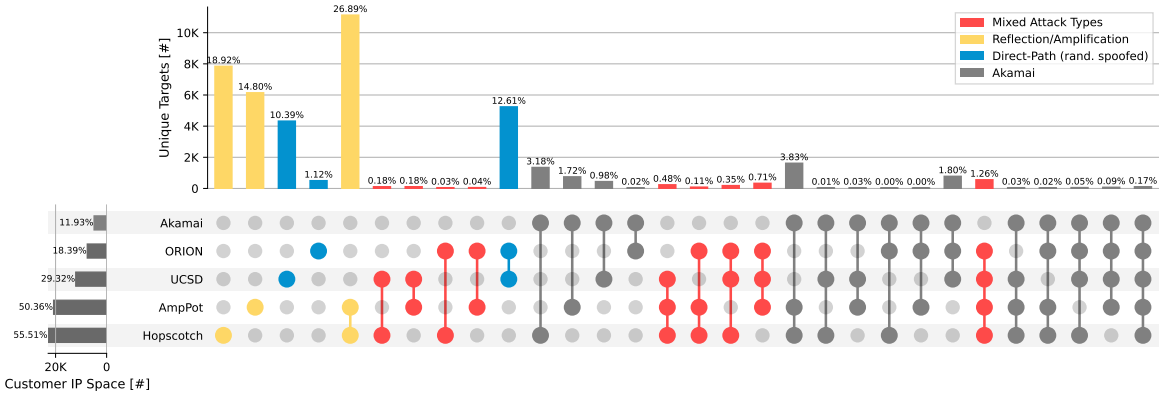

Figure 5: Customer IP Space and event Analysis.

8 Attack Incidents Analysis

Fig. 4 visualizes the count of matched IP addresses over time, distinguishing between "Customer IP Space" and "Customer Event IP". It shows spikes indicating significant events: (A) a large number of targets detected from the Customer IP Space S by telescopes/honeypots and (B) a large number of targets from Customer Events records by the DPS coincided with the telescopes/honeypots, address space E.

8.1 Spikes Detected by Amppot, Hopscotch, UCSD, and Orion

Table 1 presents the recorded spike events, indicating that some attack events can be detected by telescope setups, while others are detected by honeypot setups.

- **Telescope Detection:** UCSD and Orion identify spoofed attacks targeting IP subnets, manifested as backscattered traffic. This phenomenon is observed in two specific scenarios:
  1. When a customer transitions to DDoS Protection Services (DPS) for mitigation.
  2. Before the DPS mitigation measures take effect.
- **Honeypot Detection:** Amppot and Hopscotch detect direct and reflection attacks, actively engaging with all IP addresses within the targeted subnets.

Please be noted that The data from the telescopes/Honeypots, which aligns with our DDOS events, is vividly represented by the spikes Customer IP Space in this context identifies IP addresses of our customers that are detected and logged within the telescopes/honeypot datasets. The designation Customer Event IP, however, is more specifically applied to those customer IPs that not only appear in the telescopes/honeypot datasets but also coincide with the broader timeframes delineated by the `startTime` and `endTime` of our DDOS events. Crucially, this correlation is not based on exact hour, minute, and second details, since the telescopes/honeypot data does not include these precise time elements. Rather, matching is determined by the day, with the assumption that each recorded date encompasses the full 24-hour span from one midnight to the next.

Fig 6 shows the distribution of attacks grouped by date and subnet detected by the telescopes/honeypots in the Customer IP Space.

References

[1] Matthew Caesar and Jennifer Rexford. Bgp routing policies in isp networks. 2005.

[2] Nikolaos Chatzis, Georgios Smaragdakis, Anja Feldmann, and Walter Willinger. There is more to ixps than meets the eye. 2013.

[3] Alan Saied, Richard E Overill, and Tomasz Radzik. Detection of known and unknown ddos attacks using artificial neural networks. 2016.

[4] Kyle Schomp, Onkar Bhardwaj, Eymen Kurdoglu, Mashooq Muhaimen, and Ramesh K Sitaraman. Akamai dns: Providing authoritative answers to the world's queries. 2020.

[5] Tony Miu Tung, Chenxu Wang, and Jinhe Wang. Understanding the behaviors of bgp-based ddos protection services. 2018.

[6] An Wang, Wentao Chang, Songqing Chen, and Aziz Mohaisen. Delving into internet ddos attacks by botnets: Characterization and analysis. 2018.

Table 1: Matched IP counts showed as spikes in Fig 4

Date	Victim Subnet	Amppot	Hopscotch	UCSD	Orion	Akamai
2020-12-15	Subnet A	83	246	0	0	246
2021-09-12	Subnet B	0	0	256	256	256
2022-02-25	Subnet C	1	1	239	0	239
2022-03-18	Subnet D	1	256	1	1	256
2022-03-22	Subnet D	0	135	1	1	135
2023-08-24	Subnet E	0	0	66	66	66

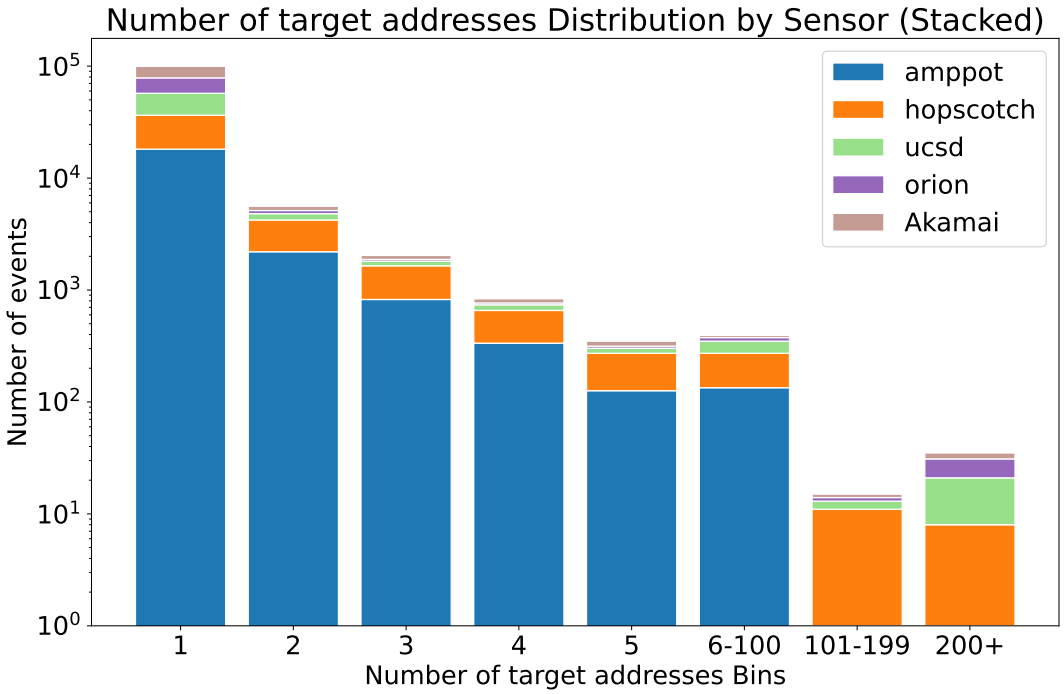

Figure 6: Customer IP Space and event Analysis.

[7] Yi Xie and Shun-Zheng Yu. Monitoring the application-layer ddos attacks for popular websites. 2008.