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 [6]. 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) [3]., 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 [2]. 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 [5]. 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 [7] [4]. 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 [8]. 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 academic datasets

This analysis seeks to bridge our recorded DDOS event data with insights derived from academic datasets, specifically those provided by Telescopes and Honeypots. Telescopes operate by analyzing backscattered traffic, indicative of attacks spoofing their source address to mimic that of the Telescopes' own address blocks. This detection method suggests that, despite our robust mitigation mechanisms, there is a nuanced possibility of overlap between the dates recorded by Telescopes and our event dataset. Such an overlap may either precede our event window, suggesting early detection and subsequent mitigation activation, or follow our event timeframe, possibly indicating an attack's resurgence post-mitigation.

Contrastingly, Honeypots offer a distinct perspective by actively participating in attack mechanisms, thereby aligning their data with DDOS events perhaps serendipitously. The presence of a Honeypot record during a DDOS event does not directly correlate with our mitigation processes due to their independent operation.

Building upon this foundation, our victim mapping effort leverages these academic datasets—enriched with dates and victim IP addresses from entities like Orion, UCSD, AmpPot, and Hopscotch—to correlate external attack indicators with our internal DDOS attack records. This correlation focuses on attack specifics such as duration (`startTime` to `endTime`), magnitude, types, and targeted victims, aiming to determine if academic data can preemptively signal potential threats to our clients. This is assessed across three critical junctures: before detection by our systems, during the transition to our

protective measures, and following successful attack mitigation.

Our methodology unfolds in two phases. Initially, we extract our customers' IP address spaces from the academic datasets, filtering out irrelevant data to define a subset termed "customer IP space." Subsequently, we map these academic datasets' dates and victim IP addresses against our defined attack periods and the IP addresses associated with our customers' DDOS attack events. This meticulous mapping yields a refined dataset, "customer event IP," facilitating a targeted analysis of the interplay between academic insights and our DDOS event records.

Fig 1 presents the relationships among our refined datasets.

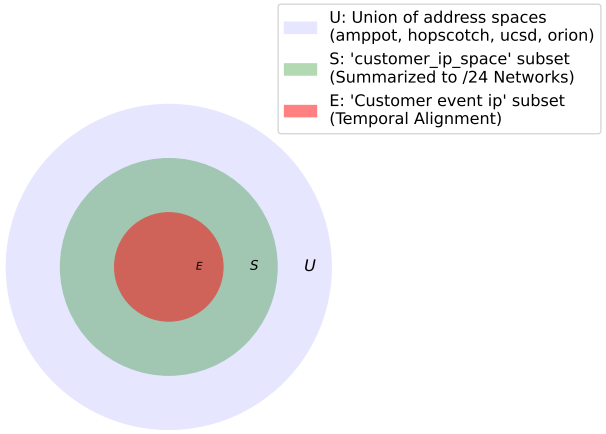

Figure 1: Address sets relationship

7.1 'Customer IP Space S' Definition

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 /24 Networks**: Each IP address in S is summarized to a /24 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.

3. The necessity for this summarization approach stems from the operational framework of our network protection strategy By receiving and propagating these prefixes (minimum /24 prefix for Internet reachability), we can redirect all inbound traffic destined for our customers from the Internet using Border Gateway Protocol (BGP).

7.2 'Customer event ip E' Definition

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.

7.3 Analysis of 'Customer IP Space S'

The refined dataset under analysis includes active customers who have reported DDOS attacks from January 1, 2019, to October 12, 2023. This dataset deliberately excludes those who have not reported any DDOS activities within this period, as well as customers who utilize non-network protection services, such as traffic redirection through DNS record management.

Included within this dataset are instances of attack traffic detected both prior to and subsequent to the initiation of our mitigation efforts. Before these efforts commence, data from both telescopes and honeypots contain records of attack activities directed at our customers. This initial state provides a comprehensive view of the attack landscape before any intervention.

After customers redirect their traffic to our platform and our mitigation measures become operational, the impact on attack traffic visibility varies by the nature of the monitoring systems. For darknet telescopes, the effect of our platform's attack traffic filtering leads to a significant reduction in backscattered traffic, effectively rendering these attacks invisible in the dataset. Conversely, when attacks originate from honeypots acting as DDOS reflectors, although our platform successfully filters the incoming attack traffic, the honeypots' ability to continuously send attack traffic means they can still document traffic and activities.

The differential impact of our filtering mechanisms on these datasets leads to an expected discrepancy in recorded attack events between telescopes and honeypots.

While honeypot setups may document a sustained or increased number of attack events due to their operational continuity, the telescope dataset is anticipated to show a reduced count as a direct consequence of our mitigation efforts.

Fig. 2 show that AmpPot and Hopscotch collectively detected more than 50% of attack events. This indicates a significant coverage and effectiveness in detecting DDOS attacks within the customer IP space managed by these honeypots. In contrast, Telescope UCSD and Orion reported lower detection rates, revealing around 29.3% and 18.39% of addresses, respectively.

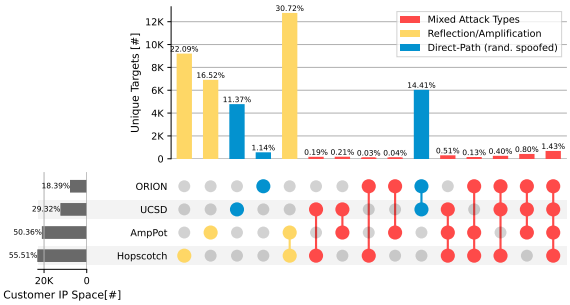

Figure 2: Customer IP Space Analysis.

7.4 Analysis of Customer Event IP E'

The analysis of Customer Event IP E' is designed to enforce a more rigorous approach in identifying coincidences between the attacks detected by Telescopes and Honeypots and the attack events reported in our customer records. This entails a meticulous process where the 'Customer Event IP Datasets' must closely align victim IP addresses with the specific time periods of reported attacks.

We project that setups involving honeypots will uncover a higher frequency of coincidental events. This is attributed to their proactive role in engaging with and capturing malicious traffic, thus providing a rich dataset for analysis. On the other hand, observations from darknets are anticipated to present a lower occurrence of coincidental events. The passive nature of darknets, focused on the surveillance of unsolicited traffic across designated IP spaces, contributes to this expected discrepancy. The insights derived from this comparative analysis are invaluable, offering a deeper understanding of the threat environment confronting our customers and enabling the refinement of our defensive strategies accordingly.

Fig. 3 This figure demonstrates that AmpPot's detection rate has risen to 61.13%, while Hopscotch has recorded a 49.38% detection rate. Such figures underscore their substantial reach and efficiency in identifying DDOS attacks within the customer event IP space. In comparison, Telescope UCSD and Orion have registered lower detection rates, decreasing to 26.48% and 18.08% of addresses, respectively.

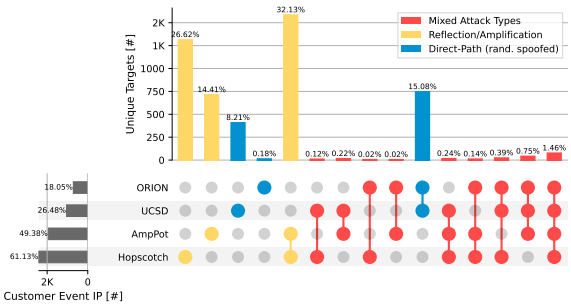

Figure 3: Customer Event IP Analysis.

Fig. 7 summarises the analysis of Customer IP Space, S and Customer Event IP E.

7.5 Special Attack Incidents Analysis

The observed spike in Fig. 5 shows an abrupt jump in the number of victim (target) addresses on a particular date, which indicates that our customer prefix(es) in the Customer IP Space dataset may under horizontal attack. Normally, we observe the number of target addresses to be less than 50 daily, as indicated in Fig. 6, which shows the distribution of the number of target addresses grouped by victim /24 prefix and date of attack. This observation is particularly interesting as mentioned in our company blogs [1]. We are seeing an increasing trend of horizontal attacks, referring to simultaneous DDoS attacks aimed at multiple, unrelated targets (which is why they're sometimes called carpet bomb attacks). Instead of prioritizing a single high-value target, the attacker selects multiple targets in order to distribute the attack, making it more challenging for security teams to mitigate and maximizing the possibility of widespread disruption.

7.6 Spikes Detected by Academic datasets

Table 1 outlines the detection of significant attack instances confirmed with our reported events, illustrating that some malicious activities are observable through network telescopes, while others are unveiled by honeypot infrastructures.

- **Network Telescopes:** Instruments like UCSD and Orion are crucial for identifying spoofed assault attempts on IP ranges, evidenced by anomalous backscatter signals. These incidents predominantly occur in two situations:

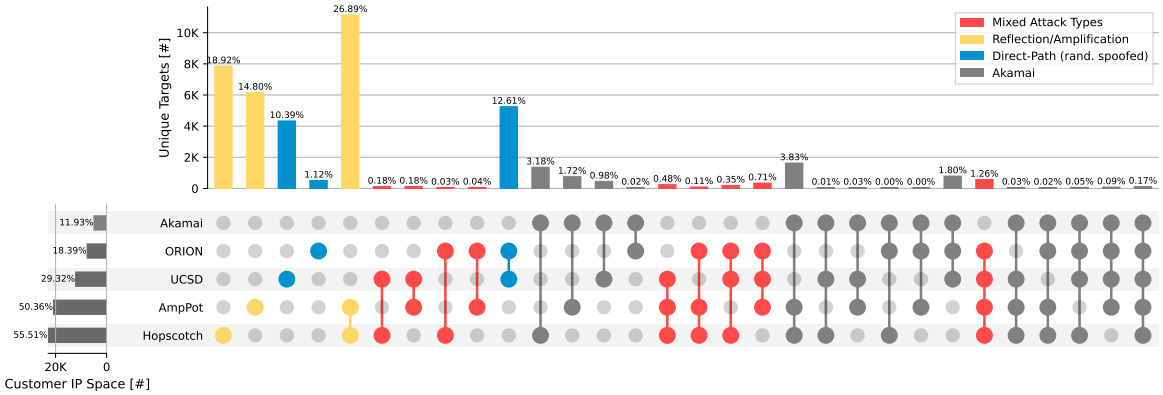

Figure 4: Customer IP Space and event Analysis.

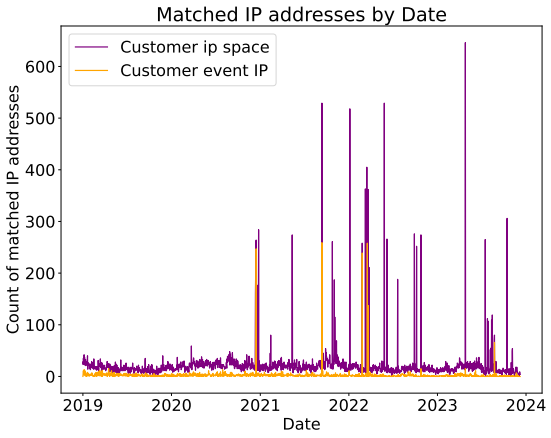

Figure 5: Mapping customer ip space and event.

1. When an entity engages DDoS Protection Services for imminent threat mitigation.
2. During the initial phase before the full implementation of mitigation strategies.

- **Honeypots:** Tools such as Amppot and Hopscotch are effective in detecting both straightforward and complex attacks, maintaining vigilance over entire targeted IP segments.

Telescope detections often involve straightforward attack mechanisms like UDP, SYN, and NTP floods, as well as TCP irregularities, leveraging the telescope's IP space as spoofed origins.

In contrast, honeypots reveal the intricacies of amplification and reflection attacks, such as those involving DNS and NTP, demonstrating their capability to expose and analyze these more complex attack vectors.

The information in Table 1 correlates directly with the DDoS events we've monitored, specifically through the sudden increases observed within our Customer Event IP dataset. This dataset pinpoints IP addresses within our customers' network prefixes that have been flagged by either the telescope or honeypot monitoring systems. The term "Customer Event IP" is particularly attributed to those IP addresses that are not only detected in the monitoring datasets but also align with the wider time windows marked by the `startTime` and `endTime` of observed DDoS incidents. It's important to note that this alignment does not rely on the precise timing (hour, minute, and second) due to the monitoring data's lack of such detailed timestamps. Instead, the matching process is based on the assumption that each date recorded represents the entire 24-hour period from midnight to midnight, ensuring that the correlation considers the full day's potential for attack activity.

References

[1] Dennis Birchard. DDoS Attacks in 2022: Targeting Everything Online, All at Once. https://www.akamai.com/blog/security/ddos-attacks-in-2022-targeting-everything-online, 2023. Accessed: [5th Feb 2024].

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

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

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

[5] Kyle Schomp, Onkar Bhardwaj, Eymen Kurdoglu, Mashooq Muhaimen, and Ramesh K Sitaraman. Aka-

Table 1: Matched IP counts showed as spikes in Fig 5

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

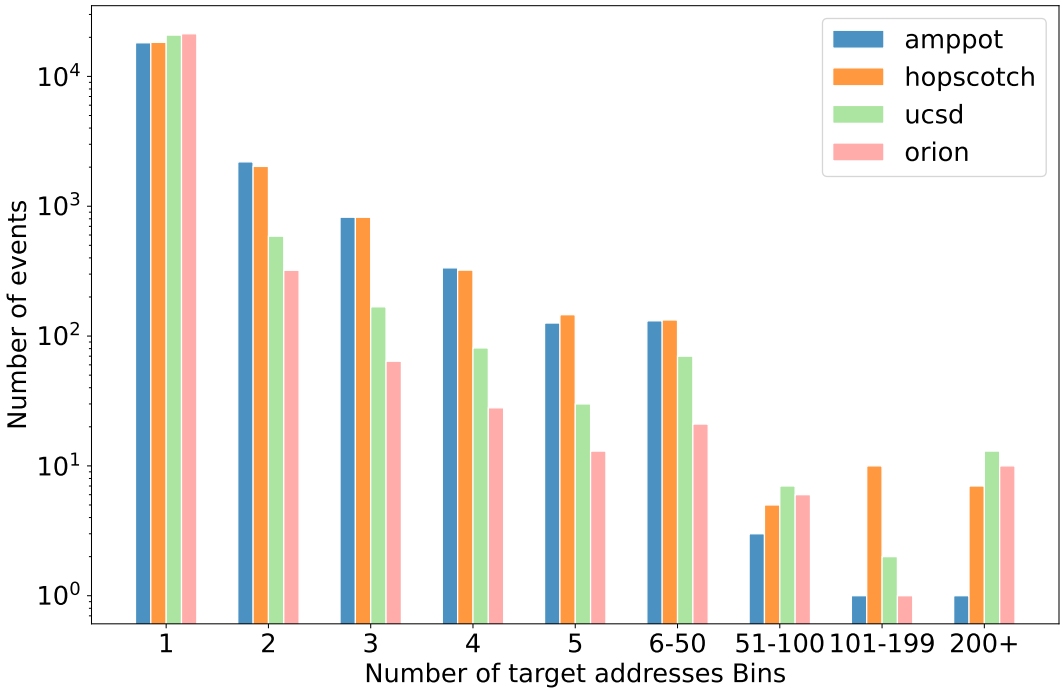

Figure 6: Distribution of Number of victim ip grouped by date and /24 prefixes.

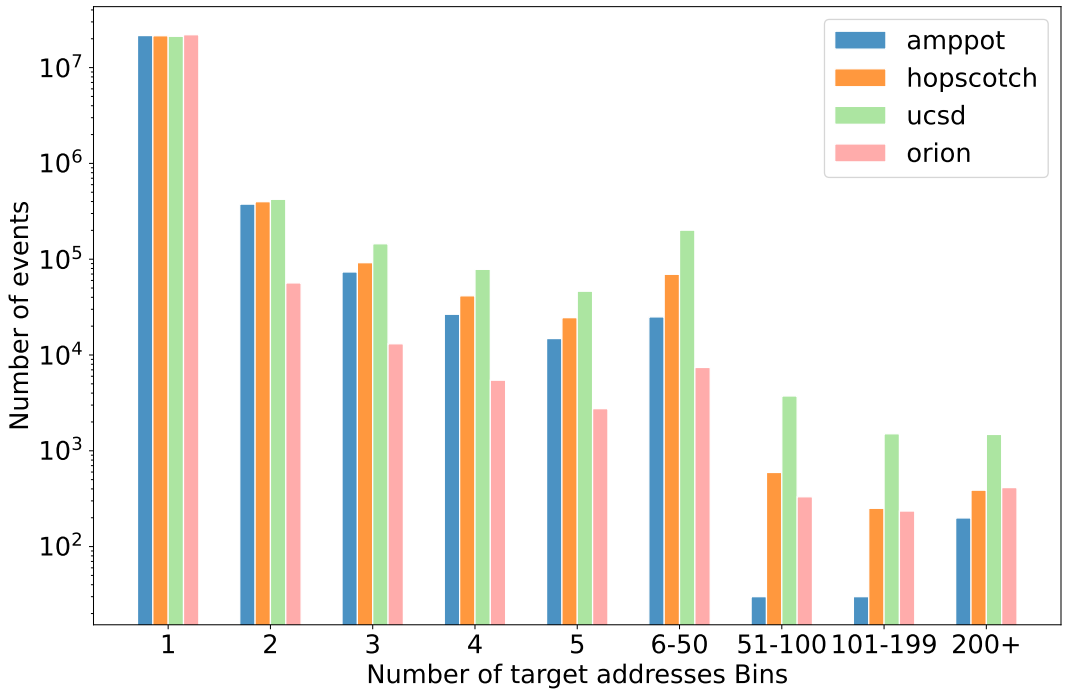

Figure 7: Academic datasets - Distribution of Number of victim ip grouped by date and /24 prefixes.

Row	Subnet	Attacks	Bits per Second	Packets per Second
0	A	CLDAP Reflection, DNS Reflection, NTP Reflection, SNMP Reflection, UDP Fragment	69.86 Gbps	8.12M
1	B	SYN ACK Flood	364.08 Mbps	867.27k
2	C	CLDAP Reflection, DNS Reflection, NTP Reflection, SNMP Reflection, SSDP Reflection, DHdiscovery, UDP Fragment	101.85 Gbps	20.68M
3	D	DNS Reflection, NTP Reflection, SNMP Reflection, SYN Flood, UDP Flood, UDP Fragment	29.44 Gbps	8.41M
4	D	ACK Flood, FIN PUSH Flood, PSH ACK Flood, RESET Flood, SYN Flood	3.84 Gbps	690.47k

Table 2: Consolidated Data on Network Attacks and Traffic

mai dns: Providing authoritative answers to the world's queries. 2020.

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

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

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