How DRDoS Attacks Vary Across the Globe?

Tiago Heinrich
Carlos A. Maziero
{theinrich,maziero}@inf.ufpr.br
Federal University of Paraná
Curitiba, Paraná, Brazil

Newton C. Will
will@utfpr.edu.br
Federal University of Technology - Paraná
Dois Vizinhos, Paraná, Brazil

Rafael R. Obelheiro
rafael.obelheiro@udesc.br
State University of Santa Catarina
Joinville, Santa Catarina, Brazil

ABSTRACT

In this study we characterize Distributed Reflection Denial of Service (DRDoS) attack traffic taking into consideration the geographical distribution of victims. This type of characterization is not widely explored in the literature and could help to better understand this type of attack. We aim to explore this gap in the literature using data collected by four honeypots over three and a half years. Our findings highlight attack similarities and differences across continents.

CCS CONCEPTS

• **Security and privacy** → **Denial-of-service attacks**; • **Networks** → *Network measurement*.

KEYWORDS

DRDoS Attacks, Traffic Characterization.

ACM Reference Format:
Tiago Heinrich, Carlos A. Maziero, Newton C. Will, and Rafael R. Obelheiro. 2022. How DRDoS Attacks Vary Across the Globe?. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3517745.3563026

1 INTRODUCTION

Distributed Reflection Denial of Service (DRDoS) attacks (Fig. 1) are a variation of DDoS attacks that continue to plague the Internet, and have gained attention in the literature in recent years [1, 2]. In a DRDoS attack, the attacker commands bots to send traffic to misconfigured hosts that act as reflectors. As the source address of attack traffic is spoofed, reflectors send their responses to a chosen victim, rather than the actual origin. Since responses are usually larger than the corresponding requests, this also achieves amplification. A wide set of Internet protocols can be exploited for this purpose, especially UDP-based protocols, with different amplification factors. The characterization of DRDoS attacks helps to understand how they are perpetrated and who are the victims.

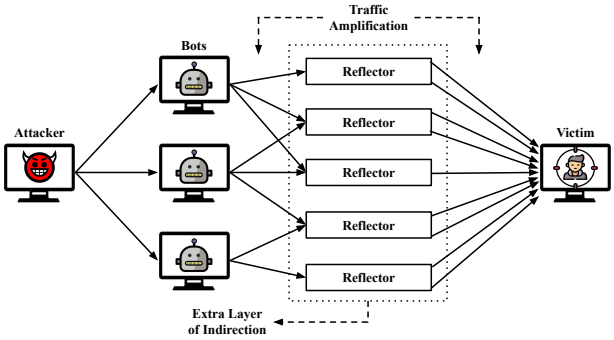

Figure 1: Scheme of a DRDoS attack.

In this study we analyze traffic collected by four MP-H honeypots [1], three in South America and one in Europe, between Sep 24, 2018, and Apr 28, 2022. Instead of analyzing attack traffic as a whole, as in [1–3], we analyze traffic for each continent separately, according to geolocation data from the MaxMind database.[1] This allows us to look at how attacks differ across regions, aiming to identify behaviors that may be associated with the location of victims.

2 EVALUATION

Table 1 present an overview of the observed traffic. Following [1], we defined an attack as a set of five or more requests with source IP addresses belonging to the same CIDR block (a victim) and the same destination UDP port, in which consecutive requests are at most 60 seconds apart. North America (NA) and Asia (AS) are the continents that receive more attacks. Within these continents, we observe a concentration of attacks in the United States (US) (90.8% of the attacks in NA), and Hong Kong (HK) and China (CN), with respectively 41.4% and 21.8% of attacks in AS.

The mean duration observed for the continents ranges from a minimum of 10.9 min and a maximum of 2.9 h. Overall 86.2% of attacks are shorter than 10 min, and 93.3% are shorter

[1] https://dev.maxmind.com/geoip

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10.
https://doi.org/10.1145/3517745.3563026

Table 1: Characteristics of observed attack traffic.

	Asia	Africa	Europe	North America	South America	Oceania
Attacks	782,000	22,543	556,265	1,358,759	77,042	56,366
Duration (secs) [avg/median]	1,244 / 40	2,115 / 30	862 / 156	913 / 174	10,715 / 169	653 / 196
Carpet bombing attacks	16,874 (2.1%)	521 (2.3%)	6,520 (1.1%)	17,018 (1.2%)	10,833 (14.0%)	152 (0.2%)
Requests per attack [avg/median]	35,140 / 2,356	39,764 / 2,969	19,252 / 491	18,906 / 832	169,985 / 622	24,702 / 1,054
Countries with attacks ≥ 10M reqs	9	1	15	2	2	2
Top protocol (% attacks)	NTP (50.6%)	NTP (46.5%)	DNS (41.2%)	CLDAP (36.6%)	DNS (36.7%)	CLDAP (45.2%)
Top protocol (% requests)	NTP (44.5%)	NTP (68.9%)	CLDAP (41.6%)	CLDAP (39.6%)	CLDAP (92.8%)	CLDAP (60.4%)
Annual growth [avg/median]	1.0% / 1.0%	1.7% / 1.0%	2.0% / 0.1%	1.7% / 0.1%	2.4% / 0.3%	0.7% / 0.1%

than 30 min. The median for all continents remained below 3.2 min. It is possible to state that the observed attacks have a short duration, lasting only a few minutes, in line with was reported in previous studies [1, 2].

In South America (SA), 78.7% of the attacks affected victims in Argentina (AR) and Brazil (BR). The continent had the highest incidence of carpet bombing attacks, where multiple IP addresses in a CIDR block are targeted in the same time frame. This is reflected in a higher average of IP addresses per attack: 9.8 for SA, compared to 1.8 for the other continents. Having 3 of our 4 honeypots located in SA might contribute to this discrepancy.

Attack intensity is usually higher for AS and Africa (AF), with medians of 2,356 and 2,969 requests per attack respectively, more than twice the median for Oceania (OC) (1,054), the third-highest continent. The attack intensity for AF is even more surprising when taking into consideration that the median duration of attacks in the continent is only 30 s. AS and AF also had averages of more than 35k requests per attack, but this is dwarfed by SA, with an average of 170k requests per attack. This is more than 4× the averages for AS and AF, and shows that the most intense attacks observed by our honeypots affected victims in SA (this observation may also be influenced by the location of the honeypots). All continents have countries that experienced attacks with 10M requests or more; Europe (EU) and AS lead in number of countries, with 15 and 9, respectively.

The prevalent protocol varies by region. In AS and AF, Network Time Protocol (NTP) came up first in volume both of attacks and requests. In NA and OC, Connection-less Lightweight Directory Access Protocol (CLDAP) was the most prevalent protocol both in attacks and in requests. In EU and SA, Domain Name System (DNS) was the most used protocol in volume of attacks, but CLDAP was first in volume of requests. DNS accounts for 41.2% of the attacks but only 5.5% of the requests in EU, and 36.7% of the attacks but just 0.7% of the requests in SA. These contrasts indicate that, in these continents, DNS attacks are frequent but have low intensity. The differences in protocol popularity among continents could be related to the availability of reflectors in each region.

During the years of data collection, we evaluated the annual growth of attacks in each region. Overall, the average growth in all regions is low. Nonetheless, several countries had periods of a few days or weeks with increased concentration of attacks.

3 CONCLUSION

This study presents a brief discussion of some of the findings when taking into account the geographical distribution of the victims of DRDoS attacks. Some of our findings are: (I) the preferred protocol for amplification attacks changes according to the region; (II) Africa had highest median for the number of requests per attack, even with the lowest median for attack duration; (III) South America had the highest concentration of carpet bombing attacks and the most intense attacks seen by our honeypots; (IV) all continents have experienced heavy DRDoS attacks, with several countries affected in Asia and Europe; and (V) the annual growth of attacks is similar across all regions.

REFERENCES

[1] Tiago Heinrich, Rafael R Obelheiro, and Carlos A Maziero. 2021. New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks. In *Proceedings of the 22nd International Conference on Passive and Active Network Measurement*. Springer, Cottbus, Germany, 269–283. https://doi.org/10.1007/978-3-030-72582-2_16

[2] Daniel Kopp, Christoph Dietzel, and Oliver Hohlfeld. 2021. DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks. In *Proceedings of the 22nd International Conference on Passive and Active Network Measurement*. Springer, Cottbus, Germany, 284–301. https://doi.org/10.1007/978-3-030-72582-2_17

[3] Daniel R Thomas, Richard Clayton, and Alastair R Beresford. 2017. 1000 days of UDP amplification DDoS attacks. In *Proceedings of the APWG Symposium on Electronic Crime Research*. IEEE, Scottsdale, AZ, USA, 79–84. https://doi.org/10.1109/ECRIME.2017.7945057