How DRDoS Attacks Vary Across the Globe?

Tiago Heinrich[1], Newton C. Will[2], Rafael R. Obelheiro[3], Carlos A. Maziero[1]

[1]Federal University of Paraná, Curitiba, Paraná, Brazil
[2]Federal University of Technology – Paraná, Dois Vizinhos, Paraná, Brazil
[3]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.

DRDoS

DRDoS attacks bounce traffic off misconfigured Internet hosts (reflectors) to achieve high-volume Distributed Denial-of-Service (DDoS) attacks. DRDoS attacks consist of two phases: (i) Internet Protocol (IP) spoofing to hide attackers by using the reflector; (ii) amplification used to maximize the size of responses relative to the request size.

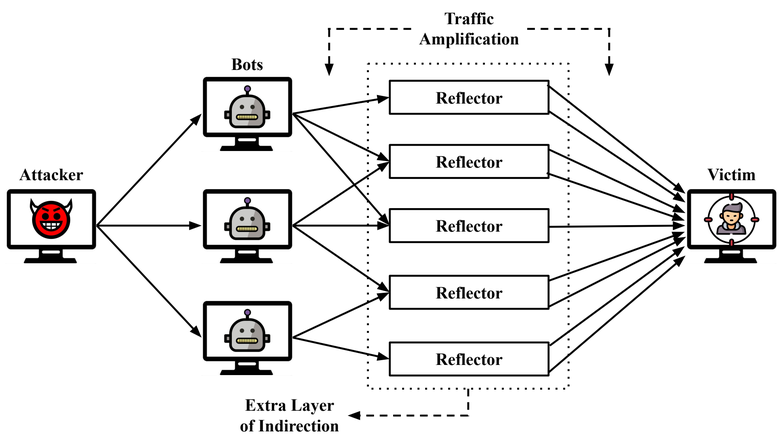

Fig. 1: Scheme of a DRDoS attack.

MP-H

MP-H [1] is a honeypot designed to observe and record DRDoS attack traffic. MP-H supports 9 protocols: CHARGEN, CLDAP, CoAP, DNS, Memcached, NTP, QOTD, SSDP, and Steam.

Objectives

While previous studies [1–3] analyze global attack traffic, we analyze traffic for each continent separately, according to geolocation data from the MaxMind database. This allows us to look at how attacks differ across regions, aiming to identify behaviors that may be associated with the location of victims.
An evaluation that limits the data observations for each continent, allows us to:

1. Isolate behaviors that could remain hidden by looking only at the full dataset; and
2. Highlight differences between regions.

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.

References

[1] Tiago Heinrich et al. “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*. Cottbus, Germany: Springer, 2021, pp. 269–283. DOI: 10.1007/978-3-030-72582-2_16.

[2] Daniel Kopp et al. “DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks”. In: *Proceedings of the 22nd International Conference on Passive and Active Network Measurement*. Cottbus, Germany: Springer, 2021, pp. 284–301. DOI: 10.1007/978-3-030-72582-2_17.

[3] Daniel R Thomas et al. “1000 days of UDP amplification DDoS attacks”. In: *Proceedings of the APWG Symposium on Electronic Crime Research*. Scottsdale, AZ, USA: IEEE, 2017, pp. 79–84. DOI: 10.1109/ECRIME.2017.7945057.

Overview

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 Classless Inter-Domain Routing (CIDR) block (a victim) and the same destination UDP port, in which consecutive requests are at most 60 seconds apart.

	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 $\geq$ 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%

Table 1: Characteristics of observed attack traffic.

Evaluation

Attacks

- North America (NA) and Asia (AS) are the continents that receive more attacks;
- Concentration of attacks in the United States (US) (90.8%), and Hong Kong (HK) (41.4%) and China (CN) (21.8%).

Fig 2: Attacks by day.

Duration

- Mean duration of attacks ranges from a minimum of 10.9 min and a maximum of 2.9 h;
- 86.2% of attacks are shorter than 10 min, and 93.3% are shorter than 30 min;
- Median for all continents remained below 3.2 min.

Victims

- In South America (SA), 78.7% of the attacks affected victims in Argentina (AR) and Brazil (BR);
- SA had the highest incidence of carpet bombing attacks;
- Honeypot location might contribute to this discrepancy.

Attack intensity

- Attack intensity is usually higher for AS and Africa (AF);
- Median duration of attacks in AF is only 30 s;
- AS and AF also had averages of more than 35k requests per attack;
- SA, with an average of 170k requests per attack;
- Most intense attacks observed by our honeypots affected victims in SA;
- 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.

Protocol

- Prevalent protocol varies by region;

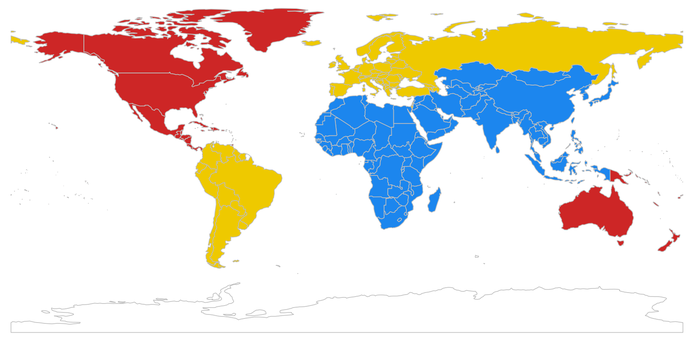

Fig 3: Top protocol (% attacks).

- Domain Name System (DNS) accounts for 41.2% of the attacks but only 5.5% of the requests in EU;
- 36.7% of the attacks but just 0.7% of the requests in SA;
- DNS attacks are frequent but have low intensity.

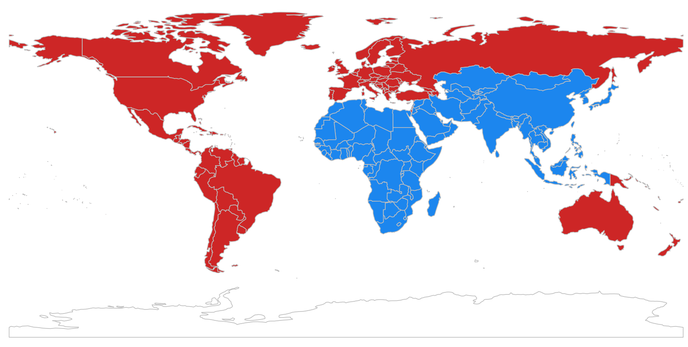

Fig 4: Top protocol (% requests).

- The differences in protocol popularity among continents could be related to the availability of reflectors in each region.

General Observations

- AF had highest median for the number of requests per attack, even with the lowest median for attack duration;
- The average annual growth in all regions is low;
- Several countries had periods of a few days or weeks with increased concentration of attacks.
- All continents have experienced heavy DRDoS attacks, with several countries affected in Asia and Europe.

Contact: theinrich@inf.ufpr.br