How DRDoS Attacks Vary Across the Globe?

Tiago Heinrich¹, Newton C. Will², Rafael R. Obelheiro³, Carlos A. Maziero¹

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

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 14, 2018, and Apr 28, 2022.

References


Overview

Table 1 presents 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.

Evaluation

Table 1: Characteristics of observed attack traffic

<table>
<thead>
<tr>
<th>Region</th>
<th>Attacks</th>
<th>Africa</th>
<th>Europe</th>
<th>North America</th>
<th>South America</th>
<th>Oceania</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median</td>
<td>92,000</td>
<td>22,543</td>
<td>556,265</td>
<td>1,208,759</td>
<td>77,042</td>
<td>56,366</td>
</tr>
<tr>
<td>Duration (sec) [avg/median]</td>
<td>1,244 / 40</td>
<td>2,115 / 30</td>
<td>862 / 156</td>
<td>913 / 174</td>
<td>7,015 / 169</td>
<td>653 / 196</td>
</tr>
<tr>
<td>Carpet bombing attacks</td>
<td>16,674 (2.1%)</td>
<td>521 (2.3%)</td>
<td>6,520 (1.1%)</td>
<td>17,018 (1.2%)</td>
<td>10,833 (14.0%)</td>
<td>152 (0.2%)</td>
</tr>
<tr>
<td>Requests per attack [avg/median]</td>
<td>35,140 / 2,356</td>
<td>39,764 / 2,969</td>
<td>19,252 / 491</td>
<td>18,906 / 832</td>
<td>169,985 / 622</td>
<td>24,702 / 1,054</td>
</tr>
<tr>
<td>Countries with attacks &gt; 10M requests</td>
<td>9</td>
<td>1</td>
<td>15</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Top protocol (% attacks)</td>
<td>NTP (58.6%)</td>
<td>NTP (46.5%)</td>
<td>DNS (41.2%)</td>
<td>CLDAP (36.6%)</td>
<td>CLDAP (36.7%)</td>
<td>CLDAP (45.2%)</td>
</tr>
<tr>
<td>Top protocol (% requests)</td>
<td>NTP (44.5%)</td>
<td>NTP (68.9%)</td>
<td>CLDAP (41.6%)</td>
<td>CLDAP (39.6%)</td>
<td>CLDAP (92.8%)</td>
<td>CLDAP (60.4%)</td>
</tr>
<tr>
<td>Annual growth [avg/median]</td>
<td>1.0% / 1.0%</td>
<td>1.0% / 1.0%</td>
<td>1.0% / 1.0%</td>
<td>2.0% / 0.1%</td>
<td>1.7% / 0.1%</td>
<td>2.4% / 0.3%</td>
</tr>
</tbody>
</table>

Protocol

- 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 3: 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.