

# New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks

Tiago Heinrich<sup>1</sup>[0000–0002–8017–1293], Rafael R. Obelheiro<sup>2</sup>[0000–0002–4014–6691],  
and Carlos A. Maziero<sup>1</sup>[0000–0003–2592–3664]

<sup>1</sup> Federal University of Paraná – Curitiba, Brazil

<sup>2</sup> Graduate Program in Applied Computing, UDESC – Joinville, Brazil  
heinrichtx@gmail.com, rafael.obelheiro@udesc.br, maziero@inf.ufpr.br

**Abstract.** Distributed reflection denial of service (DRDoS) attacks are widespread on the Internet. DRDoS attacks exploit mostly UDP-based protocols to achieve traffic amplification and provide an extra layer of indirection between attackers and their victims, and a single attack can reach hundreds of Gbps. Recent trends in DRDoS include multiprotocol amplification attacks, which exploit several protocols at the same time, and carpet bombing attacks, which target multiple IP addresses in the same subnet instead of a single address, in order to evade detection. Such attacks have been reported in the wild, but have not been discussed in the scientific literature so far. This paper describes the first research on the characterization of both multiprotocol and carpet bombing DRDoS attacks. We developed MP-H, a honeypot that implements nine different protocols commonly used in DRDoS attacks, and used it for data collection. Over a period of 731 days, our honeypot received 1.8 TB of traffic, containing nearly 20.7 billion requests, and was involved in more than 1.4 million DRDoS attacks, including over 13.7 thousand multiprotocol attacks. We describe several features of multiprotocol attacks and compare them to monoprotoocol attacks that occurred in the same period, and characterize the carpet bombing attacks seen by our honeypot.

**Keywords:** Amplification Attacks, Network Characterization and Distributed Reflection Denial of Service.

## 1 Introduction

Distributed denial-of-service attacks (DDoS) have been seen on the Internet for nearly 25 years [13]. In these attacks, a set of machines sends traffic to a victim in a coordinated fashion. The volume of data leads to the exhaustion of system and/or network resources at the victim, causing service unavailability and hurting legitimate customers [17].

One kind of DDoS attack are Distributed Reflection Denial of Service (DRDoS) attacks (also known as amplification DDoS attacks), in which traffic is bounced off unsuspecting intermediate systems, known as reflectors [24]. DRDoS attacks not only make attribution harder due to an extra layer of indirection,

but they also provide traffic amplification, thus making it easier to generate enough traffic to disrupt the target, especially when multiple reflectors are used simultaneously. Moreover, DRDoS attacks can leverage several different protocols, notably UDP-based ones, and there is a large number of vulnerable and/or misconfigured Internet servers that can be used as reflectors [26]. All these benefits to attackers help to explain the prevalence of DRDoS traffic on the Internet. A study [19] has shown a 9% increase in DRDoS attacks between the second semester of 2017 and the same period of 2018, and statistics from April 2019 indicate that nearly 70% of DDoS attacks use reflection [6]. It has also been reported that attacks grew 15% from 2019 to 2020 (25% during the lockdown period due to the COVID-19 pandemic) [20].

Given the relevance of DRDoS attacks, researchers have worked on the analysis and characterization of the traffic associated with such attacks. However, there is a lack of research on multiprotocol DRDoS attacks, where a victim is attacked using multiple amplification protocols simultaneously, which is an emerging trend in the DDoS scene [21]. Most existing research considers either individual protocols [1,5,25,7,27], or multiple protocols in isolation from each other [10,26,9,22,29]. Another trend in DRDoS are carpet bombing attacks, which target multiple IP addresses in the same subnet (instead of a single IP address) in order to evade detection while still being able to cause disruption by flooding access links. Such attacks have not been discussed in the literature, although [9] presents some results when victims are aggregated by /16 CIDR blocks.

Our research aims to bridge these gaps in knowledge by characterizing multiprotocol and carpet bombing DRDoS attacks. We have designed and implemented MP-H, a honeypot that emulates reflectors for several protocols that are exploited in DRDoS attacks: Chargen, DNS, NTP, Memcached, QOTD, SSDP, CoAP, CLDAP, and Steam. Results from 731 days of data collected by our honeypot comprise nearly 20.7 billion requests and confirm that multiprotocol attacks are found in the wild: 2.9% of the victims of DRDoS attacks carried out using our honeypot as a reflector suffered a multiprotocol attack, with up to three protocols being used simultaneously. More than 3.7% of all attacks employed carpet bombing, affecting 21.8% of the victims observed.

In summary, this paper makes the following contributions: we propose a definition for what constitutes a multiprotocol DRDoS attack; we describe several characteristics of multiprotocol DRDoS attacks and compare them with monoprotocol attacks observed on the same honeypot; and we characterize carpet bombing attacks observed on our honeypot.

The remainder of this paper is organized as follows. Section 2 discusses related work. Section 3 describes our honeypot MP-H. Section 4 presents our data analysis. Finally, Section 5 concludes the paper.

## 2 Related Work

This section reviews related work on DRDoS traffic characterization, with an emphasis on the analysis of attacks in the wild rather than in controlled envi-

ronments. Some studies are focused on a single protocol, such as DNS [1,25,7] and NTP [5,27]. Attack characteristics examined include temporal distribution, intensity and duration of attacks, victim locations, packet-level attributes (TTL, size), amplification factor, and payloads.

Rosow [26] explored how 14 different protocols could be used in amplification attacks, and estimated the amplification factor provided by each one. He also performed traffic analysis: flow data from an European ISP were used to identify victims and amplifiers within the network, UDP scans to darknet addresses were used to identify potential attackers, and honeypots were used mainly to confirm the occurrence of attacks, without deeper analysis.

Krämer et al. [9] introduced AmpPots, which are honeypots designed for observing and collecting DRDoS traffic using nine protocols (NTP, DNS, Chargen, SSDP, MS-SQL, NetBIOS, QOTD, SIP, and SNMP). They analyzed data collected from 21 AmpPots between February and May 2015, totaling more than 1.5 million attacks, and described characteristics such as attack duration, victim geolocation, and request entropy (payload diversity). They also performed an analysis of DDoS botnets.

Noroozian et al. [22] analyzed DRDoS traffic collected from eight AmpPots during 2014–2015, with a total of six network protocols (NTP, DNS, Chargen, SSDP, QOTD, and SNMP). The main thrust of their study is a characterization of DRDoS victims, including their network type (access, hosting, enterprise) and geolocation. They also discuss the duration of attacks per victim type.

Thomas et al. [29] analyzed DRDoS traffic collected from a large set of UDP honeypots for eight protocols (QOTD, Chargen, DNS, NTP, SSDP, MS-SQL, Portmap, and mDNS). They observed more than 5.8 million attacks over a period of 1010 days, and analyzed scanning behavior and several attack characteristics (duration, packet counts, number of attacks). NTP and DNS were the most popular protocols, but they also noticed significant amounts of SSDP traffic.

Jonkers et al. [8] analyzed DDoS traffic using both AmpPots and backscatter traffic from an Internet telescope. They observed more than 20 million attacks over two years (2015–2017), affecting more than 2.2 million /24 networks. They also describe joint attacks, which are attacks that employ both DRDoS and regular DDoS with spoofed source addresses (mostly TCP SYN floods).

While these studies investigated DRDoS attacks involving several protocols, they mostly ignore how these protocols are used together. In fact, Krämer et al. [9] acknowledge the existence of attacks using multiple protocols, but do not explore this further, while the joint attacks in [8] are combinations of DRDoS and regular DDoS. None of the studies consider carpet bombing attacks. In this paper we specifically address multiprotocol DRDoS and carpet bombing attacks, aiming to understand their characteristics and how they compare to monoprotocol ones.

### 3 MP-H, a Multiprotocol Honeypot

To observe and collect DRDoS traffic, we developed MP-H, a multiprotocol honeypot that supports nine different UDP-based protocols: Chargen, QOTD, DNS, NTP, SSDP, Memcached, CoAP, CLDAP, and Steam (used in online games). CoAP and CLDAP have been added in March and July 2020, respectively, while the other protocols have been supported from the beginning (September 2018). MP-H is designed to mimic a reflector: it receives requests and provides responses that look legitimate, logging all the received traffic. A list of ongoing attacks (with source IP address, number of requests, and the timestamps of the first and last seen requests) is updated in real-time and kept in memory, and periodically written to permanent storage when activity is low. Full packets are captured using `Tcpdump` [28] for off-line processing (e.g., payload analysis).

Since it does not host any publicly advertised service, an MP-H instance will become a reflector after it has been found through scanning. Once it has been uncovered, the honeypot address can be used in DRDoS attacks and will likely be shared among miscreants. Observing reflection attacks, however, does not require actually taking part in them. Therefore, the honeypot should respond correctly to scans (increasing the odds that it will be recruited for future attacks), but not contribute significantly to DRDoS attacks. To achieve this, MP-H responds to at most five responses per IP address per day; this should be enough to both provide positive feedback to a scanner and severely limits the amount of attack traffic it sends to a single victim. Every hour MP-H scans the list of banned IP addresses and removes offenders that have been there for 24 h or more.

There are several projects that scan the Internet for open reflectors, such as [4] and [23]. In order to avoid being reported as an open reflector, MP-H has a list of banned IP addresses for which no responses are sent. This list was compiled from several sources (e.g., [16], project web pages), and is updated manually whenever we discover new scanning addresses while analyzing logs.

MP-H is similar in design to `AmpPot` [9], with the main differences being in implementation specifics and in the set of supported protocols. In MP-H, DNS and Memcached requests are proxied to actual servers (thus eliciting truthful responses), while the other protocols are emulated by the honeypot, which synthesizes legitimate-looking responses with fabricated content. The honeypot is written in Python, and runs on Linux. The source code is not publicly available yet, but we are open to sharing the tool with interested researchers.

### 4 Data Analysis

An MP-H instance has been deployed in our university network since September 2018, collecting data 24/7. It has a public IP address and is exposed to the Internet (i.e., it is not behind a firewall or NAT box). In this section we analyze data collected using this instance over a period of 731 days, from September 2018 to September 2020. Section 4.1 gives overall traffic statistics. Section 4.2 explores attack intensity. Section 4.3 performs per-protocol analyses. Section 4.4 describes the victims. Finally, Section 4.5 dissects carpet bombing attacks.

## 4.1 Overview

Over a period of 731 days, our honeypot received 1.8 TB of traffic, containing nearly 20.7 billion (B) requests, an average of 28.3 million (M) requests per day. Only a tiny fraction (less than 7.2 M, 0.034% of the total) of those requests received a response, showing the effectiveness of the response limiting mechanism.

In this work, we define a *monoprotocol 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. Victims are defined as IP addresses within a CIDR block instead of a single IP address due to carpet bombing attacks, as discussed in Section 4.5. The thresholds (5 requests and 60 seconds) were established empirically: we analyzed the traffic collected by the honeypot during the first three weeks manually, and observed distinct behaviors from the same source IP address:

1. “Slow”: a small number ( $\leq 3$ ) of requests, a few (1–2) seconds apart;
2. “Fast”: many ( $\geq 10$ ) nearly identical requests, in quick succession;
3. “Bursty”: sequences of bursts of “fast” traffic, tens of seconds apart.

We classified the first as scan traffic and the others as attack traffic. We then experimented with distinct thresholds until we reached an automatic classification that closely matched our manual classification. We believe this approach is reasonable on a problem without ground truth, but acknowledge that future work may require different thresholds as we learn more about typical attacker behavior.

By analogy, we define a *multiprotocol attack* as a set of five or more requests with source IP addresses belonging to the same CIDR block and with two or more unique destination UDP ports, in which consecutive requests are at most 60 seconds apart. By this definition, two monoprotocol attacks against the same victim that use different protocols and are spaced by at most 60 seconds become a multiprotocol attack.

Table 1 shows the overall attack statistics. The honeypot observed nearly 1,4 M DRDoS attacks, of which 99.05% were monoprotocol attacks and 0.95% were multiprotocol attacks. While monoprotocol attacks are much more prevalent, there were 13.8 k multiprotocol attacks. Multiprotocol attacks account for 2.9% of the victims and 2.5% of the requests. The average number of requests per attack for multiprotocol attacks is 38.2 k, almost twice the average for monoprotocol attacks, which is 19.8 k requests per attack.

Table 1: Attack statistics

| Type of attack | Requests       | %     | Victims   | %     | Attacks   | %     |
|----------------|----------------|-------|-----------|-------|-----------|-------|
| Monoprotocol   | 20,203,393,971 | 97.50 | 1,079,210 | 97.08 | 1,432,775 | 99.05 |
| Multiprotocol  | 518,684,765    | 2.50  | 32,369    | 2.91  | 13,798    | 0.95  |
| Total          | 20,722,078,736 | 100   | 1,111,579 | 100   | 1,446,573 | 100   |

Our data collection period covered the Brazilian presidential elections (October 2018) and the lockdown period of COVID-19 (from March 2020 onwards), with some interesting results. Compared to the previous month, the packet rate doubled during the election month, and on the day of the second round (Oct 28th) the number of attacks had a 227% increase. We compared the four-month period with stricter lockdown (March–June) to the same period in 2019 and to the four months before it. We observed  $4\times$  growth of the packet rate during the lockdown period compared to the other two periods, and the emergence of new victims in health organizations, e-commerce, and academic institutions.

## 4.2 Attack Intensity

Figure 1 presents the empirical cumulative distribution function (CDF) for the number of requests per attack, and Table 2 (top) shows a statistical summary. Both types of attacks have right-skewed distributions. Multiprotocol attacks had more requests than monoprotocol attacks up to the 99.99th percentile. This means that a large majority of multiprotocol attacks had more requests than the corresponding fraction of monoprotocol attacks.

Table 2: Attack intensity statistics

|                                       | Monoprotocol       | Multiprotocol      |
|---------------------------------------|--------------------|--------------------|
| No. of attacks w/ $\geq 1$ M requests | 1,927 (0.1%)       | 60 (0.4%)          |
| Attack w/ most requests               | 221.9 M (1.0%)     | 7.8 M (1.5%)       |
| Duration (median)                     | 612.5 s            | 2673.9 s           |
| No. of attacks lasting $\geq 1$ h     | 39,886 (2.7%)      | 1,737 (12.5%)      |
| Longest attack                        | 178.6 h (7.4 days) | 180.0 h (7.5 days) |
| Requests per day (avg/max)            | 27.6 M/253.7 M     | 1.3 M/17.5 M       |
| Packets per second (avg)              | 31.7 pps           | 13.8 pps           |

Figure 2 shows the CDF for the duration of attacks. The duration is measured as the time difference between the first and last requests in an attack. The distribution is left-skewed for both mono and multiprotocol attacks. Multiprotocol attacks last longer than monoprotocol attacks up to the 99.99th percentile. Table 2 (middle) presents some statistics. In [9], 62% of the attacks were shorter than 15 minutes and 90% lasted up to 1 hour; the corresponding fractions for MP-H were 87% and 95.9%, respectively, which means that the attacks we observed were shorter overall.

Figure 3 depicts the daily attacks observed by the honeypot. The number of attacks climbed quickly after the honeypot was deployed, and remained relatively steady until June 2020. The notable exception was a 15-day period bridging July (last 8 days) and August 2019 (first 7 days), when the average jumped from 1.9 k to 18.4 k attacks per day. This period saw predominantly small attacks (80% of attacks had up to 127 requests) that targeted unrelated victims, and we could

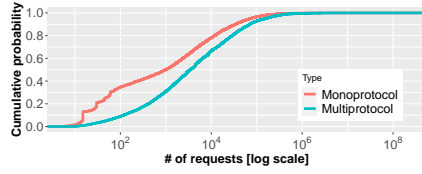


Fig. 1: ECDF for requests per attack

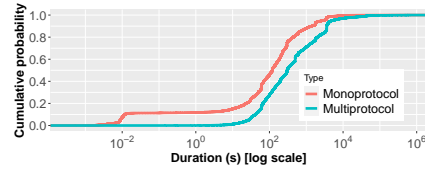


Fig. 2: ECDF for attack duration

not find an explanation for this spike. The rise starting in July 2020 is due to the deployment of the CLDAP honeypot; the average for July–September was 6,621 attacks per day. Overall, the number of attacks per day was 1,449, and the maximum was 20.9 k. Only 29 out of 731 days (4.0%) had 5,000 attacks or more, with 15 of these days in July–August 2019. There were 33 multiprotocol attacks per day on average, but they were observed on only 386 days (52.8%).

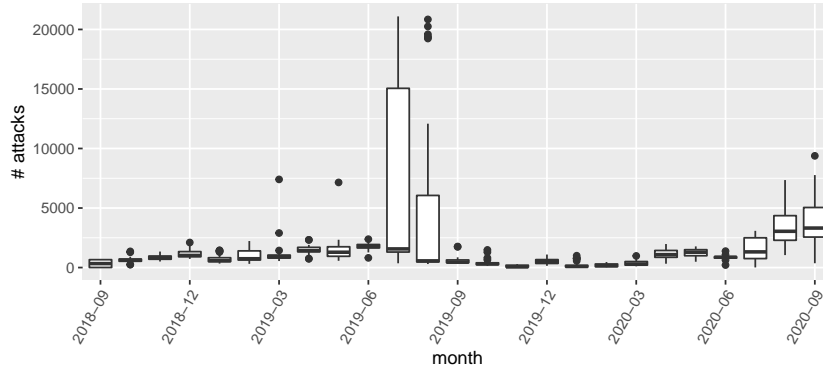


Fig. 3: Evolution of the number of attacks per day

Figure 4 depicts the number of requests per month, broken down by protocol. The number of requests varies each month, without discernible trend. The number of requests follows the number of attacks shown in Figure 3, but imperfectly: in 2019, June had the most requests but not too many attacks, while July and August has the most attacks with a moderate number of requests (since most attacks were small). The protocol breakdown shows that Memcached and Chargen had the most monthly requests until July 2020, when we started collecting CLDAP traffic and this protocol became prevalent (this is further discussed in Section 4.3). Table 2 (bottom) shows statistics about requests per day/second. The number of requests per day for multiprotocol attacks is heavily skewed, and the average considers only days with attacks. The number of requests for other protocols fluctuated, but were mostly dwarfed by the leading protocols. Putting the two dimensions (attacks and requests) together, we find a rather low intensity of 30.6 pps for attack traffic (considering only busy periods).

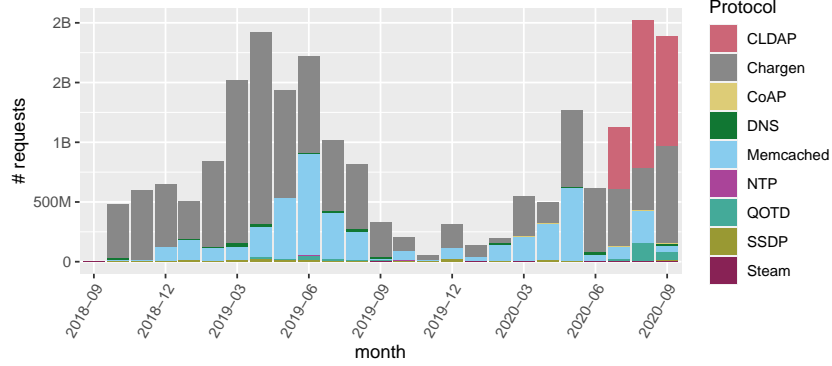


Fig. 4: Evolution of monthly requests (overall). We started observing CoAP and CLDAP traffic in 2020-03 and 2020-07, respectively.

### 4.3 Per-protocol Analyses

As discussed in Section 3, MP-H supports nine protocols: Chargin, DNS, Memcached, NTP, QOTD, SSDP, CoAP, CLDAP and Steam. Table 3 shows their relative contribution both in number of monoprotoal attacks and in number of requests. Chargin and Memcached dominate, appearing in 52.1% of the attacks and 84.2% of the requests. These protocols offer large amplification factors (60 for Chargin, 262 for Memcached), which helps to explain their prevalence. DNS gained prominence in 2020, and CLDAP, which was deployed in July 2020, has already climbed to number three in requests and number four in attacks (in absolute numbers).

Table 3: Protocol breakdown for monoprotoal attacks and requests

| Protocol            | Chargin | CLDAP | CoAP   | DNS  | Memcached | NTP  | QOTD | SSDP | Steam    |
|---------------------|---------|-------|--------|------|-----------|------|------|------|----------|
| <b>Attacks (%)</b>  | 21.5    | 9.2   | 0.01   | 25.0 | 30.5      | 5.3  | 2.0  | 5.8  | 0.05     |
| <b>Requests (%)</b> | 60.9    | 12.6  | 0.0002 | 0.9  | 23.3      | 0.01 | 1.5  | 0.5  | 0.000004 |

Table 4 shows the average amplification factors observed for each protocol (Steam is omitted due to low traffic), along with factors previously reported in the literature. Memcached had the largest amplification factor, 262. Most protocols exhibited lower amplification factors than reported before; a possible explanation might be that our number is the average factor, while others may be the maximum factor rather than the average one. The exceptions were CLDAP and DNS, which remained within the reported range, and SSDP, which had a larger amplification factor than previously reported. The latter is due to the response synthesized by the honeypot being larger than the responses in [11,26].

Table 5 presents the most popular combinations of protocols in multiprotocol attacks, ranked both by number of attacks and by number of requests. The most



Table 4: Amplification factors observed in MP-H and in the literature

| Protocol | MP-H | Literature     | Protocol  | MP-H | Literature      |
|----------|------|----------------|-----------|------|-----------------|
| Chargen  | 60   | 556.9 [26]     | Memcached | 262  | 51,200 [12]     |
| CLDAP    | 62   | 46–70 [2,15]   | NTP       | 42   | 556.9 [26]      |
| CoAP     | 25   | 34–46 [3,18]   | QOTD      | 78   | 140.3 [26]      |
| DNS      | 50   | 28.7–64.1 [26] | SSDP      | 97   | 20–75.9 [11,26] |

used protocols were Chargen, DNS, CLDAP, and SSDP; attacks with Chargen and one of the other three account for 82.2% of the attacks and 64.1% of the requests. Two noteworthy aspects are (i) Chargen being used in all top combinations, and (ii) CLDAP already being used in nearly two-thirds of the attacks. The Chargen:CLDAP attacks are less intense, however, than Chargen:DNS and Chargen:SSDP attacks, which account for a larger fraction of requests. There were just 230 attacks (1.66% of the multiprotocol attacks) with more than two protocols. We can conclude that monoprotocol attacks are exploiting a wider range of protocols, focusing on those with higher amplification factors. Multiprotocol attacks exploit a smaller set of protocols, with varying combinations, which explains the concentration in four protocols.

Table 5: Protocol combinations used in multiprotocol attacks (CG=Chargen)

| Protocol            | CG:DNS | CG:CLDAP | CG:SSDP | CG:Memcached | Others |
|---------------------|--------|----------|---------|--------------|--------|
| <b>Attacks (%)</b>  | 8.2    | 65.4     | 8.6     | 5.6          | 12.2   |
| <b>Requests (%)</b> | 27.9   | 16.7     | 19.5    | 9.2          | 26.7   |

For protocols where responses do not depend on request contents, such as Chargen and QOTD, attackers can maximize the amplification factor by minimizing payload size. 100% of Chargen requests observed had just one byte of payload and 98.2% of QOTD requests had two bytes or less.

When amplification depends on message contents, not just size, we can identify some prevalent patterns. SSDP had 99.9% of `M-SEARCH` requests, used for service discovery, while NTP had 99.9% of `MONLIST` requests, used for listing recent peers. The protocols recently added to MP-H, CoAP and CLDAP, follow a similar pattern. 99.5% of the CoAP requests contained a null URI, while 99.1% of the CLDAP requests contained a `searchRequest <R00T>` operation. In all cases, the aim is to maximize amplification.

DNS requests exploit a wide variety of resource records (RRs). 115.9 k distinct RRs were observed, and the six most used, which account for 34.5% of the queries, are listed in Table 6 (size is not available for `access-board.gov` because its name servers no longer answer `ANY` queries). The top two queries were also reported in [9]. The most frequent query, `isc.org ANY`, yields an amplification factor of 71.1. While there are other names that provide larger responses, a possible reason for using this name is that ISC is responsible for the BIND

name server, and thus at the forefront of DNS developments, which suggests the existence of many records in the zone apex and good name server availability. The query types observed are shown in Table 7. The vast majority (91.9%) of the queries were for **ANY**, which returns all records for a given name (regardless of type), usually resulting in larger responses.

Memcached is abused for amplification in two ways. One is requesting statistics from the server, which provides an amplification factor of 32 on average. The other is using **set** to store large values in the in-memory database and later repeatedly retrieving these values with **get** requests for the associated key. 99.99% of the requests observed in MP-H were of the second kind, mostly with random data. The amplification factor depends on the value size.

Table 6: DNS queries observed

| Resource Record      | %    | Size |
|----------------------|------|------|
| isc.org ANY          | 22.1 | 2701 |
| 067.cz ANY           | 4.0  | 388  |
| access-board.gov ANY | 3.6  | N/A  |
| irs.gov ANY          | 2.1  | 4302 |
| 1x1.cz ANY           | 1.6  | 1501 |
| pbgc.gov ANY         | 1.1  | 4223 |
| Others               | 65.5 | —    |

Table 7: DNS query types observed

| QTYPE  | %     |
|--------|-------|
| ANY    | 91.9  |
| TXT    | 7.9   |
| A      | 0.035 |
| CNAME  | 0.014 |
| NS     | 0.009 |
| Others | 0.14  |

#### 4.4 Victims

Since DRDoS attacks employ IP spoofing, we consider the source IP addresses of attack traffic as victim addresses. They are grouped by CIDR block according to the GeoLite2 database [14], also the source for AS numbers and geolocation.

Monoprotocol attacks affected victims in 226 countries (country codes, actually), and 111 countries had victims of multiprotocol attacks. Table 8 shows the top countries in terms of monoprotocol and multiprotocol attacks. Victims in United States and China are targeted by 39.8% of the monoprotocol attacks and 63.6% of the multiprotocol attacks, with United Kingdom ranking third for both types of attacks. In spite of the top 3 countries being the same, the targets of monoprotocol and multiprotocol attacks are poorly correlated: the rank correlation for countries with at least one attack of each kind is weak (Spearman’s coefficient  $r_s = 0.36, p < 0.01$ ).

Table 9 shows the top six AS Numbers in terms of victims of both monoprotocol and multiprotocol attacks. Victims are widely distributed across ASNs, with the top ASNs accounting for just 16.6% of the victims. ASNs 7922 (COMCAST), 7018 (AT&T INTERNET), 20115 (Charter Communications), and 701 (UUNET) belong to Internet service providers, while ASNs 37963 (Hangzhou Alibaba Advertising Co), and 16276 (OVH) belong to cloud providers.

Table 8: Top target countries in number of attacks













| <b>Mono</b>  | <b>%</b> | <b>Multi</b>   | <b>%</b> |
|--|----------|--|----------|
| US  | 32.6     | US  | 49.6     |
| CN  | 7.2      | CN  | 14.0     |
| GB  | 3.6      | GB  | 4.7      |
| FR  | 2.6      | CA  | 3.4      |
| CA  | 2.2      | BR  | 2.7      |
| DE  | 2.1      | AU  | 2.4      |
| Others   | 49.7     | Others   | 23.2     |

Table 9: Top target ASNs in number of victims







| <b>ASN</b> | <b>Country</b>   | <b>Victims (%)</b> |
|------------|--|--------------------|
| 7922       | US  | 7.1                |
| 7018       | US  | 3.3                |
| 20115      | US  | 1.8                |
| 37963      | CN  | 1.6                |
| 701        | US  | 1.5                |
| 16276      | FR  | 1.3                |
| Others     | –  | 83.4               |

Table 10 presents statistics about the number of attacks per victim. In general, there were more monoprotoocol than multiprotoocol attacks per victim, which was expected. Most victims received few attacks, which is similar to the findings in [9], where 79% of the victims were attacked just once and 0.8% suffered more than 10 attacks (our fraction of victims with more than 10 monoprotoocol attacks is higher, though).

Table 10: Attacks per victim

|  | <b>Monoprotoocol</b> | <b>Multiprotoocol</b> |
|--|----------------------|-----------------------|
| Attacks per victim (median)              | 2                    | 1                     |
| Attacks per victim (max)                 | 3,837                | 229                   |
| Fraction of victims w/ only one attack   | 60.2%                | 83.8%                 |
| Fraction of victims w/ $\leq 10$ attacks | 97.7%                | 99.2%                 |
| Fraction of victims w/ $> 10$ attacks    | 2.3%                 | 0.8%                  |

#### 4.5 Carpet Bombing Attacks

A recent trend in DRDoS attacks are carpet bombing attacks, which target multiple IP addresses within the same subnet or CIDR block in lieu of a single IP address [19]. The goal is to flood the access links of the intended victims while evading detection and hampering mitigation. Carpet bombing detection requires looking for anomalous traffic across entire subnets or CIDR blocks instead of anomalous flows involving a single IP address, while mitigation involves filtering traffic to the entire subnets/blocks, and/or diverting it to a scrubbing service.

A real example of carpet bombing observed on MP-H was an attack that lasted 14 minutes and used two protocols, Chargen and Memcached. This attack had 340 k requests that were spread across 43 different IP addresses in the same CIDR block, averaging 7.9 k requests per address.

Two variants of carpet bombing observed in MP-H are depicted in Figures 5 and 6. Figure 5 shows the most prevalent case, where addresses in the same CIDR

block are targeted in overlapping time intervals. The second case (Figure 6) presents what we called an attack *with antecedents*. Here, the carpet bombing attack occurs after a few days where a single address is targeted each day. We have considered these individual attacks to be antecedents to the carpet bombing because they have similar characteristics – protocol (Chargen and Memcached), duration, number of requests –, even if the addresses are different.

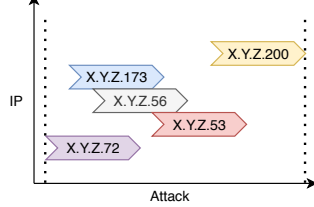


Fig. 5: Carpet bombing attack

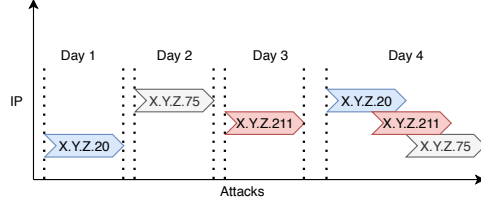


Fig. 6: Carpet bombing with antecedents

Table 11 presents statistics for carpet bombing attacks, with percentages relative to the totals in Table 1. We define a carpet bombing attack as an attack targeting multiple IP addresses from the same CIDR block. These attacks account for a small fraction of attacks and requests (3.7% of all attacks and 5.8% of the associated requests), but affect more than one-fifth of the victims (some victims suffered both mono- and multiprotocol carpet bombing).

Table 11: Carpet bombing statistics

| Carpet Bombing | Requests      | %    | Victims | %     | Attacks | %    |
|----------------|---------------|------|---------|-------|---------|------|
| Monoprotocol   | 1,117,437,837 | 5.39 | 235,244 | 21.16 | 52,689  | 3.64 |
| Multiprotocol  | 78,018,641    | 0.37 | 22,825  | 2.05  | 949     | 0.07 |
| Total          | 1,195,456,478 | 5.76 | 242,030 | 21.77 | 53,638  | 3.71 |

We observed a total of 1.1 M victims, of which 21.8% (242 k) suffered carpet bombing attacks. Carpet bombing attacks averaged 31.2 k requests overall, and 9.6 k per host in a CIDR block. Considering only attacks that use more than 50% of a CIDR block, the average rises to 41.5 k requests, albeit with an average of just 185 requests per host. This shows that, when attackers target a larger fraction of a CIDR block, the number of requests per host tends to be smaller. On average, each attack targeted 6.2% of the addresses in a CIDR block, but 1.7% of the attacks targeted 90% or more of a single CIDR block.

Table 12 shows the most popular protocols in carpet bombing attacks. Comparing to Tables 3 and 5, here we have a greater presence of SSDP, but there are still similarities with other choices of reflector protocols (90.8% of the multiprotocol attacks use just two protocols).

Table 13 presents statistics on the number of requests and duration of carpet bombing attacks, for both mono and multiprotocol attacks. Both distributions

Table 12: Top protocols in carpet bombing attacks

| Monoprotocol |       | Multiprotocol |       |
|--------------|-------|---------------|-------|
| SSDP         | 29.3% | Chargen:DNS   | 20.8% |
| Chargen      | 15.2% | CLDAP:SSDP    | 14.8% |
| Memcached    | 12.9% | DNS:SSDP      | 14.6% |
| others       | 42.6% | others        | 49.8% |

are heavily right-skewed. There were attacks with more than 1 M requests (0.4% for mono, 1.6% for multi), a significant amount from the vantage point of a single reflector. Another notable finding is that almost 25% of multiprotocol carpet bombing attacks lasted 1 h or more.

Table 13: Carpet bombing attack statistics

|                                   | Monoprotocol | Multiprotocol |
|-----------------------------------|--------------|---------------|
| Requests (avg)                    | 29.8 k       | 86.4 k        |
| Requests (99th percentile)        | 431 k        | 1.3 M         |
| Duration (avg)                    | 20 min       | 4 h           |
| No. of attacks lasting $\geq 1$ h | 1637 (3.1%)  | 221 (23.3%)   |
| Longest attack                    | 7 days       | 7.5 days      |

## 5 Conclusion

Distributed reflection denial of service (DRDoS) attacks still plague the Internet, and are constantly evolving to become more difficult to detect and mitigate. In this paper we present the first detailed study about multiprotocol DRDoS attacks. We used a honeypot that mimics a reflector to observe attack traffic. We found evidence that multiprotocol attacks are occurring but still in the minority; our belief is that they will increase in the future, due to the broader availability of reflectors and the increased difficulty of dealing with multiple protocols when defending. We also studied the recent phenomenon of carpet bombing attacks, describing several of their characteristics, including the potent combination of multiprotocol and carpet bombing. For the future we are working on a distributed honeypot platform so that we can deploy more data collection sensors, and on expanding the set of protocols supported by MP-H.

**Acknowledgments** We thank the anonymous reviewers and our shepherd Bradley Reaves, for their helpful comments in reviewing this paper. This research was supported by FAPESC and UDESC, and financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

## References

1. Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., Gritzalis, S.: DNS amplification attack revisited. *Computers & Security* **39**, 475–485 (2013)
2. Arteaga, J., Mejia, W.: CLDAP reflection DDoS (apr 2017), <https://bit.ly/3kqylku>
3. Cimpanu, C.: The CoAP protocol is the next big thing for DDoS attacks. *ZDNet* (Dec 2018), <https://zd.net/333hymy>
4. Cymru, T.: DNS research at Team Cymru (2020), <http://dnsresearch.cymru.com/>
5. Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., Karir, M.: Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In: *Internet Measurement Conference*. pp. 435–448. ACM (2014)
6. DDoSmon: Insight into global DDoS threat landscape (Apr 2019), <https://ddosmon.net/insight/>
7. Fachkha, C., Bou-Harb, E., Debbabi, M.: Inferring distributed reflection denial of service attacks from darknet. *Computer Communications* **62**, 59–71 (2015)
8. Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A., Dainotti, A.: Millions of targets under attack: A macroscopic characterization of the DoS ecosystem. In: *Internet Measurement Conference*. p. 100–113. ACM, New York, NY, USA (2017)
9. Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., Rossow, C.: AmpPot: Monitoring and defending against amplification DDoS attacks. In: *Intl Workshop on Recent Advances in Intrusion Detection*. Springer (2015)
10. Kühner, M., Hupperich, T., Rossow, C., Holz, T.: Exit from hell? reducing the impact of amplification DDoS attacks. In: *USENIX Security Symposium* (2014)
11. Majkowski, M.: Stupidly simple DDoS protocol (SSDP) generates 100 Gbps DDoS (jun 2017), <https://bit.ly/35lq2W0>
12. Majkowski, M.: Memcrashed – major amplification attacks from UDP port 11211 (Feb 2018), <https://bit.ly/2HvD4Ix>
13. Mansfield-Devine, S.: The growth and evolution of DDoS. *Network Security* **2015**(10), 13–20 (Oct 2015)
14. MaxMind: GeoLite2 database (Oct 2020), <https://www.maxmind.com/>
15. McAuley, C.: Following the crumbs: Deconstructing the CLDAP DDoS reflection attack (nov 2016), <https://bit.ly/3mgR08h>
16. Mertens, X.: Port scanners: The good and the bad (Sep 2015), <https://bit.ly/3lQmFNF>
17. Nazario, J.: DDoS attack evolution. *Network Security* **2008**(7), 7–10 (2008)
18. NETSCOUT: CoAP attacks in the wild (Jan 2019), aSERT blog, <https://bit.ly/2HqNxou>
19. NETSCOUT: Dawn of the terrorbit era. Threat intelligence report 2H 2018 (2019), <https://www.netscout.com/>
20. NETSCOUT: Netscout threat intelligence report for the first half of 2020 (2020), <https://bit.ly/3mh3Tzb>
21. NETSCOUT, Arbor: Insight into the global threat landscape (October 2017), *Netscout Arbor’s 13th Annual Worldwide Infrastructure Security Report*
22. Noroozian, A., Korczyński, M., Gañan, C., Makita, D., Yoshioka, K., van Eeten, M.: Who gets the boot? analyzing victimization by DDoS-as-a-Service. In: *Intl Symposium on Research in Attacks, Intrusions, and Defenses*. Springer (2016)
23. OpenNTP: OpenNTPProject.org - NTP Scanning Project (2020), <http://openntpproject.org/>
24. Paxson, V.: An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Computer Communication Review* **31**(3), 38–47 (2001)

25. van Rijswijk-Deij, R., Sperotto, A., Pras, A.: DNSSEC and its potential for DDoS attacks: A comprehensive measurement study. In: Proceedings of the 2014 Conference on Internet Measurement Conference. pp. 449–460. ACM (2014)
26. Rossow, C.: Amplification hell: Revisiting network protocols for DDoS abuse. In: Network and Distributed System Security Symposium (NDSS) (2014)
27. Rudman, L., Irwin, B.: Characterization and analysis of NTP amplification-based DDoS attacks. In: Information Security for South Africa (ISSA). IEEE (2015)
28. TCPDUMP: TCPDUMP/LIBPCAP public repository (2020), <https://www.tcpdump.org/>
29. Thomas, D.R., Clayton, R., Beresford, A.R.: 1000 days of UDP amplification DDoS attacks. In: APWG Symposium on Electronic Crime Research (eCrime). pp. 79–84. IEEE (2017)