Solving DDoS Attacks by Standing on the Shoulders of Giants*

DDoS Clearing House, DDoSDB, DDoS Dissector, DDoS Fingerprint and Converters

1 INTRODUCTION

Distributed Denial of Service attacks exist since the beginning of the Internet. The goal of these types of attacks is to make target systems (services, devices, or even entire networks) unreachable to its intended users. Over time, these types of attacks increased in frequency and intensity. In 2011, the peak record was reported as 60Gb/s [], in 2015 it was 500Gb/s [], and in 2016 was 1.1Tb/s []. As the dependency of our society to online service also increased, the damage cause by DDoS attacks has become extremely big. While in 2015 large corporations reported the average loss of $US410.000 per attack [], in 2017 this figure increased to $US2.500.000 [].

There are hundreds of companies worldwide offering DDoS protection and a large volume of academic work on DDoS attacks. Overall, DDoS attacks have been addressed as a reactive approach, waiting for attacks to hit a network infrastructure and see whether (i) the usual anomaly-based detection/mitigation solution works, or (ii) the network operators are skilled enough to mitigate the attack as fast as possible, or (iii) by simply paying more to third-party companies for having more network capacity and better protection. From the academic side, by the end of February 2019, Google scholar returned more than 47 thousand works on 'ddos attack'.

The question that we intend to discuss in this paper is **why and how (we believe), together, we can solve DDoS attacks?** The answer is technically simply and it is **not** by "reinventing the wheel", instead, facilitating filling the gaps of existing solutions and stakeholders (*e.g.,* victims, network operators, network security community, network security companies, law enforcement agencies, and the academic community). What we propose is a proactive approach that any stakeholder involved with a DDoS attack would benefit and trust.

Overall, we propose to facilitate: (1) victims, (2) network operators, and (3) network security companies to share their attack measurements (filtered and properly anonymized) and to get in return specific rules for detecting and mitigating those attack based on the already in-place solutions; (4) law enforcement agencies to compare attacks suffered in the society, for enabling legal attribution and prosecution of attackers (and buyers of attacks); (5) network security community (specially CERT/CSIRT) to get frequent feeds with IP addresses involved in attacks, towards preventing misused machines from performing attacks; and (6) the academic community on getting real/'fresh' DDoS attack data for testing and improving their solutions. For satisfying these six stakeholders, we propose and extensively validate the following three elements:

- **DDoS Dissector**: is a tool for analysing any type of network trace containing a DDoS attack (for example, pcap, pcapng, neflow, ipfix, sflow, and apache log), filter only the main characteristics of the attack, called **DDoS fingerprint**, and enable to share only the DDoS fingerprint and the anonymized version of the filtered attack. The requirements, the design and the validation of the tool is presented at section 2;
- **DDoS Fingerprint Converters**: is a set of tools for parsing the generic DDoS fingerprints into specific detection and mitigation technologies, for example, BGP Flowspec, eBPF, IPtables, SNORT, SURICATA, BRO, ModSecurity, and even 'black-boxes' from private security companies. An additional, and very important tools added to this set of converters, called **DDoS Mitigation Impact Quantification**, is responsible to validate and adapt detection and mitigation rules. The descriptions and explanations are presented at section 3;
- **DDoS Database (DDoSDB)**: is a distributed database that receives, enriches, distributes, and make available: filtered anonymized attack traces, DDoS fingerprints, signatures/rules for specific hardware/software detecting/mitigating DDoS attacks, lessons learned from network operators, information from law enforcement agencies and feeds for CERT/CSIRT sanitize their networks. The requirements, the design and the validation of the tool is presented at section 4.

After we describe the DDoS Dissector, the DDoS Fingerprint Converters, and the DDoS Database (DDoSDB), we introduce what we call as **DDoS Clearing House** in section 5. Only at that point we put all the pieces together and show how we have deployed ???? instances of the DDoSDB, collected more than ???? , and benefit more than ???? organizations. The development of the tools are available at

*This document was not peer-reviewed.

https://github.com/ddos-clearing-house and the public version of DDoSDB is available at https://ddosdb.org.

2 DDOS DISSECTOR

There are several words used in academia and the security community for what we will define as a DDoS attack fingerprint. The words are DDoS 'characteristics', 'fingerprint', 'profile', 'pattern', 'signature', and 'rule'. Oxford dictionary defines these words as the following:

- **characteristics**: "a feature or quality belonging typically to a person, place, or thing and serving to identify them";
- **profile**: "a graphical or other representation of information relating to particular characteristics of something, recorded in quantified form";
- **pattern**: "a regular and intelligible form or sequence discernible in the way in which something happens or is done";
- **signature**: "a distinctive pattern, product, or characteristic by which someone or something can be identified";
- **rule**: "a principle that operates within a particular sphere of knowledge, describing or prescribing what is possible or allowable";

We will however use an umbrella term, a **fingerprint**, from which the above five can be derived. A fingerprint is the smallest set of features that summarizes the main characteristics of each attack vector in a DDoS attack, extracted from a network measurement of the attack.

The goal of determining the fingerprint is to extract a distinct set of properties that allow us to identify the attack (see figure 1). This set can later be used as a signature for a signature-based firewall, or to identify the source of the attack. We distinguish two types of properties, namely *a priori* and *a posteriori* properties. We assume that all packets are IP-based packets, so no AppleTalk or other legacy protocols. With that assumption, the following a priori properties are known for each packet: (1) type (TCP/UDP); (2) protocol (DNS, HTTP, etc.); (3) extra attributes based on the protocol; (4) source port; (5) destination port; (6) source IP; (7) destination IP. Once we have established the type of attack, for example UDP/DNS from port 23 from IP addresses x, y and z, we can determine several higher level properties, namely (1) the amount of packets per second; (2) the start time; (3) the duration. The low and high level properties together will be defined as a priori properties. With just the a priori properties, we can determine several a posteriori properties, such as the origin country of the IP addresses, autonomous system, whether the IP addresses are known for other malicious behaviour and whether the IP addresses were spoofed. The a priori and a posteriori information combined creates

```
{
  protocol: "DNS",
  additional: {
    dns_query: "example.org",
    dns_type: 255
  },
  src_ips: [
    {
      as: "1234"
      ip: "100.64.52.11"
      cc: "XX"
    }
    ...
  ],
  total_src_ips: 34,
  src_ports: [
    53
  ],
  total_src_ports: 1,
  dst_ports: [
    24018,
    5441
    ...
  ],
  total_dst_ports: 17132,
  key: "1a79a4d60de6718e8e5b326e338ae533",
  start_time: "2019-02-30 12:00:00",
  duration_sec: 35.794759473957483,
  avg_pps: 627.9138370201783,
  avg_bps: 1535724.0964006053,
  vector_filter: "...",
  multivector_key: "66b375b08fc869336..."
}
```

Figure 1: An example of an enriched fingerprint for one attack vector. The enriched part is the extra information about the IP, i.e. the Autonomous System number (AS) and country code (CC)

an attack vector. A DDoS attack is composed of one or more single vector attacks. All single vectors of a DDoS attack are linked to one multivector key.

Now that we have defined what an attack vector consists of, we will outline the way to retrieve aforementioned properties from a packet capture.

(1) The first step is determining the destination IP of the attack. Generally, this will be the most frequent destination IP address.
(2) Next, we determine the most frequent protocol used for the attack, e.g. DNS.

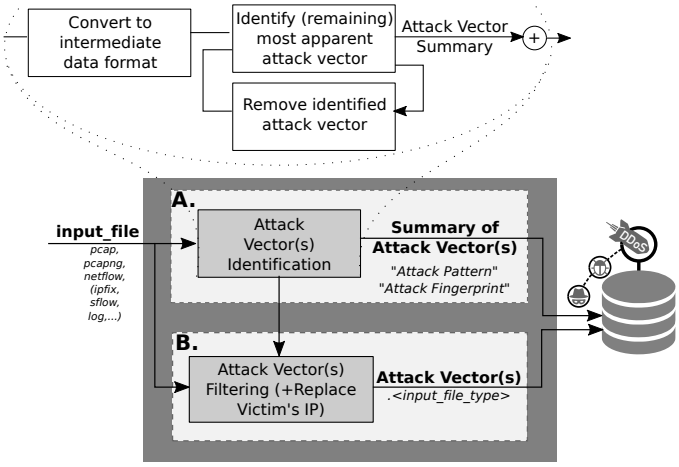

Figure 2: Process overview of the DDoS Dissector attack vector extraction

(3) Lastly, the source and destination ports are determined. The relation of source and destination ports is generally one-to-many, one-to-one, or many-to-one. In rare cases, the ports have a many-to-many relationship.

Based on these parameters, the packets belonging to the attack are extracted, the results are removed from the set and the process runs again, until there is no further probable attack vector left. This set of attack vectors gives us a key insight in the fingerprinting process. For instance, it can tell us the starting time of the attack, the amount of packets per second and more.

However, we still need to anonymize the data. After all, the victim would rather remain unknown, as the attack information is often sensitive. We do this by overwriting all destination IP data from the extracted data by 0 bytes. The destination IP can be safely removed as it is not part of the fingerprint, and provides no other value to our analysis.

We wish to minimize the amount of processing required during an attack, so all a priori properties are determined while the attack is happening, whilst the a posteriori properties are gathered after the attack has passed. This process can be done after the anonymised attack vector is uploaded to DDoSDB.

3 DDOS FINGERPRINT CONVERTERS

4 THE DDOSDB

More than a database with DDoS attack fingerprints.

Requirements:

- flexible regarding the number and types of fields;
- flexible access control
- distributed fashion;
- enrich the fingerprint;
- facilitate queries;
- enable download of fingerprints and anonymized data;
- facilitate notification;
- distribute information;
- upload information from only from trusted parties;

The aim of DDoSDB is twofold. On the one hand, it can help to create proactive measures of defying DDoS attacks, or recognise them in a very early stage. On the other hand, it can help us link the origin of multiple independent attacks together, thereby aiding law enforcement in the apprehending of the perpetrator.

As stated in 2,

5 DDOS CLEARING HOUSE

5.1 Risks of running a version of DDoSDB

- Input normal network measurement (in case ops team analyze flash crowd)
- Data leakage on the 'user database' (malicious access and upload)
- Data leakage on the 'fingerprint database';
- Data leakage on the 'filtered and annonymized network measurements';
- Data leakage of the 'logs';
- Ill-intentioned users.

6 CONCLUSION AND FUTURE WORK

DDoS attacks are not likely to stop occurring. However, we strongly believe that an community effort would extinguish the

Would be very interesting DDoSDB being a target of DDoS attack. In this way, we could get new attacks, because old attacks are not supposed to take us down.

ACKNOWLEDGEMENTS

The ideas in this document were originally funded, in 2017, by SIDNfonds (an independent foundation established by the .nl ccTLD), then in 2018, these ideas were embraced by a coalition of 25 Dutch players from industry (ISPs, xSPs,IXPs, banks, not-for-profit DDoS protection providers) and gov't (ministries and agencies), facilitated by Dutch National Cyber Security Centre (NCSC-NL), and, in 2019, it got funded by the European Commission in a project involving 46 partners.