DDoS Filtering Tool
A Design Paper

José Jair Santanna and Julik Keijer

University of Twente, the Netherlands
j.j.santanna@utwente.nl & keijerjs@gmail.com,
http://ddosdb.org/ddosfiltering

1 Introduction

2 Collaborators Requirement

Main requirement:

- Facilitate the removing of any private information that can be potentially used for identifying either the collaborators or their clients;
- Generate a summary of the attack and the IP addresses that are involved in the attack;
- Generate a new network file with only the attack records.

Additional requirements:

- Process the traffic at the collaborators' infrastructure to avoid leak of information;
- Facilitated the deployment of the filtering tool;
- Speedup the loading process of visualizations;
- Create simple and meaningful visualizations;
- Have a dynamic (and manual) filtering interface;
- Highlight outliers.

3 Tasks & Modules

The steps needed to achieve the main requirement are the following:

1. Receive an uploaded network file that contains a DDoS attack (pcap[ng] or nfdump types);
2. Pre-filter the uploaded network file keeping only the ingress traffic;
3. Highlight the potential attack targets, i.e., the destination IP addresses that received more network traffic);
4. Highlight the IP protocol that generates more network traffic towards the highlighted destination IP address;
5. Present summarized information of source IPs that sent traffic using the highlighted IP protocol;

6. Highlight (and manually remove) the source IPs that does not follow an attack pattern (outliers);
7. Classify the set of remaining source IPs as a type of DDoS attack;

*8. Use the set of remaining source IPs to filter the pre-filtered traffic (output of step 2) towards identify multi-vector attacks;

9. Repeat steps 3, 4, 5 and 6 until the collaborator is satisfied about the remaining information;
10. Generate a new network attack file with only the remaining information;
11. Export the new network attack file and the summary of the attack to DDoSDB.

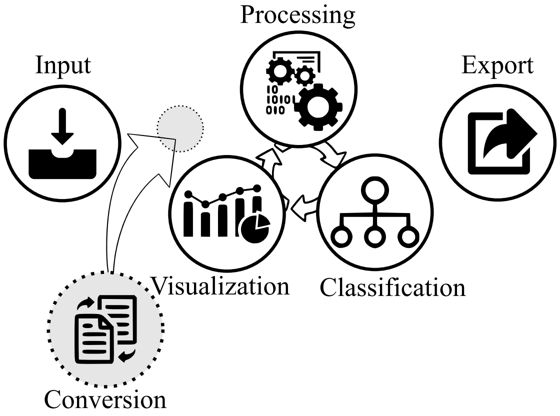

Fig. 1. DDoS filtering tool modules.

Web-based that performs offline filtering;

4 Preliminary results

Table 1. Attack information shared by initiative.

	Information	**Obtained**	[?]	[?]	[?]	[?]	[?]
1	Start time	field	✓	✓			
2	Duration	field*	✓				
3	Max bit rate	field*	✓				
4	Src. port	field	✓				
5	Dst. port	field	✓	✓			✓
6	Attack type	heuristic	✓	✓	✓		✓
7	Src. IP	field		✓	✓		
8	Src. IP country	enrich	✓	✓	✓	✓	✓
9	Src. IP city	enrich		✓			
10	Src. IP ASN	enrich		✓			
11	Dst. IP	field			✓		
12	Dst. IP country	enrich	✓	✓	✓	✓	
13	Dst. IP City	enrich		✓			
14	Dst. IP ASN	enrich		✓			

Table 2. Missing attack information.

	Information	**Obtained**
1	Packet peak rate	field*
2	# Src. IPs	field*
3	# restricted Src. IPs	enrich
4	# Src. IPs with fragm.	field
5	Attack responsible (blame)	manual
6	Src. IP # total packets	field
7	Src. IP # frag. packets	field
8	Src. IP data rate	field*
9	Src. IP packet rate	field*
10	Src. IP restricted?	enrich
11	Src. IP packet length	field
12	Src. IP TTL	field
13	Src. IP TCP flags	field
15	Src. IP HTTP payload*	field
14	Src. IP DNS query	field
16	Src. IP open ports	enrich