Privacy Policy

Development of DDoS Database

Date
01 February 2022

Classification
Public

Author
SIDN Labs

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Title of application/study

Development of DDoS Database (DDoSDB.nl)

Policy start date

1 February 2022

Purpose of application/study

DDoS-DB is the database of the DDoS Clearing House, a system by which the members of an anti-DDoS Coalition (ADC) share measured data concerning incoming DDoS attacks, in the form of 'DDoS fingerprints'. Hence, the Clearing House gives member organisations a broader view of the DDoS attack landscape, enabling them to prepare their networks for a particular DDoS attack before they themselves are targeted.

The DDoS Clearing House is being developed within CONCORDIA, a project funded by the European Commission through the Horizon 2020 initiative. The Clearing House has three component parts: the dissector, which summarises samples of network traffic captured during DDoS attacks to produce fingerprints; DDoS-DB, the database in which the fingerprints are stored and shared with other coalition members; and the converter, which generates DDoS mitigation rules from fingerprints.

This Privacy Policy relates to DDoS-DB, specifically the instance of DDoS-DB hosted on DDoSDB.nl and maintained by SIDN Labs. This policy is intended to support the development phase of DDoS-DB and will remain in effect until the end of the CONCORDIA project. In that phase, we will pilot the DDoS Clearing House withing the Dutch National Anti-DDoS Coalition (NL-ADC). For the pilot, SIDN Labs will host an instance of DDoS-DB on DDoSDB.nl for the storage of DDoS fingerprints generated by pilot participants.

Personal data

DDoSDB.nl is the instance of the DDoS-DB database hosted on the SIDN Labs network. The following types of personal data are recorded in DDoSDB.nl:

- User accounts. We record the name, e-mail address and affiliation of each user. That information is required in order to manage access to the system. Only NL-ADC members participating in the DDoS Clearing House pilot have access, and their IP addresses are included on a whitelist.
- DDoS fingerprints are JSON files containing summarised information about individual DDoS attacks, such as source IP addresses, ports and protocols, plus aggregated information such as average bps, pps and number of packets sent. A full list of fingerprint fields is given in the appendix.
- The network capture files (FLOW or PCAP) used for fingerprint generation are not stored in DDoS-DB.
- The DDoS network captures have to be filtered as thoroughly as possible to exclude legitimate internet traffic from the fingerprints.

Legitimate basis

By collecting and sharing fingerprints, we can develop a system that enables ADC members to prepare for DDoS attacks. Such a system would therefore contribute to the stability of the internet and the important services that depend upon it.

Filters

ADC members produce DDoS fingerprints independently using the dissector and the network capture files. When producing a fingerprint, a member is expected to filter the network capture as thoroughly as possible, so that it contains only attack traffic, while legitimate traffic is excluded to prevent such traffic being interpreted as malicious by the dissector. DDoS-DB will ignore network capture files, e.g. PCAP files, that are uploaded accidentally as a result of using an old version of the dissector, for example.

A fingerprint is a summary of a DDoS attack. It only contains descriptive information such as the type of attack, the source IP addresses and ports, the destination ports, and the start time and duration of the attack. The target of the attack is anonymised.

Retention

The fingerprints uploaded to DDoSDB.nl during the development phase will be retained for up to eighteen months. That retention period provides a six-month window for research projects involving a full year of fingerprints, which we believe to be sufficient.

Access

DDoSDB.nl is a closed-user-group web application. It is not publicly accessible. All communication between the server and client is encrypted using TLS. Users are IP-filtered and required to log in using a password in order to access and/or upload data.

Three types of DDoSDB.nl user are distinguished:

- [Readers] These users are allowed to query data on DDoS attacks. Only members of the Dutch National Anti-DDoS Coalition will be able to receive fingerprints.
- [Uploaders] These users are allowed to both query and upload data on DDoS attacks. Only members of the Dutch Anti-DDoS Coalition that are taking part in the pilot will have Uploader accounts.
- [Application managers with administrator rights] These users can approve account requests and change user permissions. They can also access query logs and access logs. Those rights enable them to check whether the system is being misused and whether new functionalities should be added. Only a small number of administrator accounts exist. System administrators also have OS-level access to the machine that runs DDoSDB.nl and the associated data. The number of system administrators is limited. System administrators can access the machine only from the SIDN network, using SSH or via a system console.

DDoSDB.eu is another instance of DDoS-DB, which is used for development work in the context of CONCORDIA. DDosDB.eu is used to store fingerprints generated on the DDoS Clearing House's distributed testbed; no personally identifiable information is held there. This Privacy Policy applies only to DDoSDB.nl; it does not apply to DDoSDB.eu.

Publication/sharing

Only SIDN and Coalition members taking part in the pilot have access to the data.
Each participant is required to enter into a data sharing agreement with SIDN before being allowed access to the data and to view other participants' data. None of the participants are located outside of the EU.

Type

R&D

Other security measures	N/a

Appendix: DDoS fingerprint format

A DDoS fingerprint consists of:

- Summary statistics defining the attack as a whole
- A list of one or more attack vectors, each defining a single attack vector
- Data added during the process of uploading to DDoS-DB (a small number of fields only)

The format of fingerprints generated from FLOW-format network captures is as set out below. Fingerprints generated from PCAPs contain at least the fields defined below. They may also contain additional details regarding attack vectors associated with the particular contents of the packets, e.g. DNS queries, NTP timestamps, etc.

Summary statistics

Field name	Description	Data type
attack_vectors	Array of attack vectors that make up this attack (see below)	Array of objects (see Attack Vector statistics)
target	IP address or subnet of the attack target, or "Anonymous" (when uploaded to DDoS-DB)	String
tags	Tags assigned to this attack, e.g., "Amplification attack", "Multi-vector attack", "TCP SYN flag attack"	String
key	MD5 hash digest of the fingerprint, used as identifier and as file name of the fingerprint	String
time_start	Timestamp of the start of the attack (time zone local to the attack target)	String
duration_seconds	Duration of the attack in seconds	Integer
total_flows	Total number of flows in the attack capture	Integer
total_megabytes	Total volume of the attack in megabytes (MB)	Integer

total_packets	Total number of packets in the attack	Integer
total_ips	Total number of unique source IP addresses from which attack traffic originated	Integer
avg_bps	Average number of bits/s during the attack	Integer
avg_pps	Average number of packets/s during the attack	Integer
avg_Bpp	Average number of Bytes per packet	Integer

Added in DDoS-DB

Field name	Description	Data type
submitter	User account that submitted the fingerprint to DDoS-DB	String
submit_timestamp	Timestamp of the upload (UTC)	String
shareable	Whether this fingerprint can be shared with other users / other DDoS-DB instances	Boolean
comment	Comment field for this fingerprint	String

Attack vector statistics (for each attack vector)

Field name	Description	Data type
service	Name of the service used in this attack vector, determined by the source port and protocol. e.g. UDP port 53 -> DNS. Or: "Unknown service" or "Fragmented IP packets" for the	String

	vector of packet fragments that cannot be assigned to another vector	
protocol	IP protocol, e.g. TCP, UDP, ICMP	String
source_port	Source port of this attack vector, or "random"	Integer or "random"
fraction_of_attack	The fraction of the entire DDoS attack that this attack vector makes up [0, 1], not considering the vector of packet fragments (null)	Float or null
destination_ports	List of outlier destination ports (if any) with the corresponding fraction of the traffic, or "random". e.g. {"443": 0.65, "80": 0.35}. (The keys are strings because of the JSON format)	Float or null
destination_ports	List of outlier destination ports (if any) with the corresponding fraction of the traffic, or "random". e.g. {"443": 0.65, "80": 0.35}. (The keys are strings because of the JSON format)	Map<String, Float> or "random"
tcp_flags	List of outlier TCP flags (if any) with the corresponding fraction of the traffic, e.g. {"...A....": 0.987}. null if the protocol is not TCP, or there are no outliers	null or Map<String, Float>
nr_flows	Number of flows that contribute to this attack vector	Integer
nr_packets	Number of packets in this attack vector	Integer

nr_megabytes	Number of megabytes sent through this attack vector	Integer
time_start	Timestamp of the start of the attack vector: the first flow of this attack vector (time zone local to the attack target)	String
duration_seconds	Duration of this attack vector in seconds (last timestamp - first timestamp)	Integer
source_ips	Array of unique IP addresses that sent traffic to the target on this attack vector	Array of strings