Privacypolicy

Ontwikkelfase DDoS-database

Datum
1 februari 2022

Classificatie
Publiek

Auteur
SIDN Labs

Blad
1/8

Contact
T 026 352 55 00
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

Naam onderzoek/applicatie	Ontwikkelfase DDoS-database (DDoSDB.nl)
Ingangsdatum policy	1 februari 2022
Doel van de applicatie of het onderzoek	DDoS-DB is de database van het DDoS-clearinghouse, een systeem waarmee organisaties in een anti-DDoS Coalitie (ADC) metingen van de DDoS-aanvallen die ze te verwerken krijgen kunnen delen in de vorm van 'DDoS-fingerprints'. Het clearinghouse verruimt zo het zicht van deze organisaties op het DDoS-aanvalslandschap en stelt hen in staat hun netwerken voor te bereiden op een bepaalde DDoS-aanval voordat deze hen daadwerkelijk treft. Het DDoS-clearinghouse wordt ontwikkeld in CONCORDIA, een project dat door de Europese commissie wordt gefinancierd via het Horizon-2020 initiatief. Het clearinghouse bestaat uit drie onderdelen: de dissector, die netwerk samples van DDoS-aanvallen samenvat in een fingerprint; DDoS-DB, de database waarin fingerprints worden opgeslagen en gedeeld met andere coalitieleden; en de converter, die DDoS mitigatieregels genereert uit een fingerprint. Dit privacybeleid betreft DDoS-DB, en specifiek de instantie van DDoS-DB die wordt gehost op DDoSDB.nl welke wordt onderhouden door SIDN Labs. Dit beleid is bedoeld om de ontwikkelfase hiervan te ondersteunen en zal geldig zijn tot het eind van het CONCORDIA project. In deze periode zullen we het DDoS-clearinghouse piloten met de Nederlandse anti-DDoS coalitie (NL-ADC). Voor deze pilot host SIDN Labs een DDoS-DB instantie op DDoSDB.nl, welke de DDoS fingerprints die worden gemaakt door de deelnemers aan de pilot zal opslaan.

Persoonsgegevens

DDoSDB.nl is de instantie van de DDoS-DB database die in het netwerk van SIDN Labs wordt gehost. DDoSDB.nl slaat de volgende persoonsgegevens op:

- Gebruikersaccounts. We slaan de naam, het e-mailadres, en de affiliatie van gebruikers op. Deze informatie is nodig om toegang tot het systeem te regelen. Alleen leden van de NL-ADC die aan de pilot van het DDoS-clearinghouse deelnemen hebben toegang, en hun IP-adres wordt aan een whitelist toegevoegd.
- DDoS fingerprints zijn JSON-bestanden die samengevatte informatie van een DDoS aanval bevatten, zoals bron IP-adressen, poorten, protocollen, en geaggregeerde informatie zoals gemiddelde bps, pps, en aantal verstuurde pakketten. Alle velden van een fingerprint zijn te zien in de bijlage.
- De netwerk capture bestanden (FLOW of PCAP) met welke een fingerprint is gegenereerd worden niet opgeslagen in DDoS-DB.
- De DDoS netwerk captures moeten voor zover mogelijk worden gefilterd zodat legitiem internetverkeer van een systeem niet wordt opgenomen in een fingerprint.

Grondslag

Door het verzamelen en delen van fingerprints kunnen we een systeem ontwikkelen dat ADC leden in staat stelt om zich te kunnen voorbereiden op DDoS-aanvallen. Zo draagt dit systeem bij aan de stabiliteit van het internet en de belangrijke diensten die hiervan afhankelijk zijn.

Filters

ADC leden maken zelf de DDoS fingerprints met de dissector en de netwerk capture bestanden. Zij dienen zelf, voor het maken van een fingerprint, de netwerk capture voor zo ver mogelijk te filteren tot alleen het aanvalsverkeer, zodat zo min mogelijk legitiem verkeer door de dissector kan worden geïnterpreteerd als aanvalsverkeer. DDoS-DB zal netwerk capture bestanden zoals PCAP's negeren, als deze per ongeluk zijn geüpload, bijvoorbeeld door een oude versie van de dissector te gebruiken. Een fingerprint is een samenvatting van een DDoS-aanval. Het bevat beschrijvende informatie zoals het type aanval, de bron IP-adressen en poorten, en het tijdstip en de duur van de aanval. Het doelwit van de aanval wordt geanonimiseerd.

Retentie

De fingerprints die zijn geüpload naar DDoSDB.nl tijdens de ontwikkelfase worden voor maximaal 1,5 jaar opgeslagen. Dit

geeft een half jaar om onderzoek te doen op een jaar aan fingerprints, waarvan wij verwachten dat het voldoende is.

Toegang

DDoSDB.nl is een webapplicatie voor een gesloten gebruikersgroep en is niet publiekelijk beschikbaar. Alle communicatie tussen de server en clients is versleuteld met TLS. Gebruikers worden IP-gefilterd en moeten inloggen met een wachtwoord om toegang te krijgen tot gegevens en/of deze te uploaden.

Er wordt onderscheid gemaakt tussen drie soorten gebruikers van DDoSDB.nl:

- [Lezers] Deze gebruikers mogen gegevens van DDoS-aanvallen opvragen. Alleen leden van de Nederlandse anti-DDoS coalitie kunnen optreden als ontvanger van fingerprints.
- [Uploaders] Deze gebruikers mogen gegevens van DDoS-aanvallen zowel opvragen als uploaden. Alleen leden van de Nederlandse anti-DDoS-coalitie die deelnemen aan de pilot zullen een dergelijk account hebben.
- [Applicatiebeheerders met beheerdersrechten] Deze gebruikers kunnen accountverzoeken goedkeuren en gebruikersrechten wijzigen. Verder hebben beheerders toegang tot query- en toegangslogs. Zo kunnen zij nagaan of er misbruik wordt gemaakt van het systeem en of er nieuwe functionaliteiten moeten worden toegevoegd. Er bestaan slechts enkele beheerdersaccounts. Systeembeheerders hebben ook toegang tot het OS-niveau van de machine waarop DDoSDB.nl draait en de bijbehorende gegevens. Het aantal systeembeheerders is beperkt. Systeembeheerders hebben alleen toegang tot de machine vanaf het SIDN-netwerk met SSH of via een systeemconsole.

DDoSDB.eu is een andere instantie van DDoS-DB die wordt gebruikt voor ontwikkeling in CONCORDIA. DDosDB.eu wordt gebruikt voor het opslaan van fingerprints die zijn gegenereerd op het gedistribueerde testbed van het DDoS Clearing House en bevat geen persoonlijk identificeerbare informatie. Dit privacybeleid geldt alleen voor DDoSDB.nl en is niet van toepassing op DDoSDB.eu.

Publicatie/delen	Alleen de deelnemende partijen mogen (naast SIDN) bij de data. De deelnemende partijen dienen een data sharing agreement met SIDN te tekenen, alvorens ze toegang krijgen tot de data en deze (van elkaar) mogen inzien. Deelnemende partijen zijn geen van allen buiten de EU gevestigd.
Type	R&D
Andere beveiligingsmaatregelen	N.v.t.

Bijlage: DDoS-fingerprintformat

Een DDoS-fingerprint bestaat uit:

- Samenvattende statistieken die de gehele aanval beschrijven.
- Een lijst van één of meer aanvalsvectoren die elk één aanvalsvector beschrijven.
- Een paar velden die worden toegevoegd bij het uploaden naar DDoS-DB

Het volgende formaat betreft fingerprints die zijn gegenereerd uit netwerk captures in FLOW-format. Fingerprints gegenereerd uit PCAP's bevatten minstens deze velden, maar kunnen meer details bevatten van de specifieke aanvalsvectoren uit de inhoud van het pakket, zoals de DNS-query's, 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	If 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 addressed that sent traffic to the target on this attack vector	Array of string