Facilitating the analyze of DDoS attack as a service databases

Jair Santanna (from Northwave Security) in collaboration with Curated Intelligence has shared his methodology on analyzing databases of Websites that offer Distributed Denial of Service (DDoS) attacks as a paid service. These Websites are commonly called Booters, Stressers, DDoS-for-hire, and DDoS-as-a-Service. He applied his methodology on the analysis of stresser.gg database that was recently took down by international law enforcement bodies.

The scripts, data, and analysis of stresser.gg are publicly available at Github (<https://bit.ly/stressergg_analysis>). His analysis cover (1) attacks per day, (2) attacks per user, (3) attacks on a same target, (4) the difference between users (anyone with an account), customers (any user that paid anything), and attackers, (5) number of login times per user, (6) the average time for a user perform an attack since he/she logins, (7) users using TOR, (8) IP addresses used by users, (9) IP addresses of targets, (10) the country of attackers and victims, (11) the payment records, and much more. It also has a facilitated way of querying the data per username, user\_id, country and autonomous system number (ASN).

With this this initiative Jair intends to facilitate the security community and law enforcement bodies to analyze Booters’ data with a minimum effort. Finally, he aims at create some impact to reduce the damage that Booters cause in the Internet as a hole.