Feeling proud. My PhD thesis was never so updated!

[Context] November 2017, five years ago, I had my PhD defence and received the title of doctor. My thesis was about investigating Websites that offer Distributed Denial of Service (DDoS) attacks as a paid service in the public Internet, a.k.a. Booter, Stresser, DDoS-for-Hire, and DDoS-as-a-Service. Just Google “booter” and you may find them offering DDoS attacks that you can pay and easily target anyone that you don’t like (including that company that sent you a wrong Christmas gift [off topic]). Ah, just remember or be aware, in 99,999% of the cases, it is a crime to perform or be involved with DDoS attacks!

[Why am I proud?] A couple of months ago, the Dutch Police (giant kudos to the Cybercrime team Midden-Nederland) the NCA, the FBI and many other law enforcement bodies took-down 48 Booters. YES!!!! This was THE biggest operation ever performed against Booters and made super proud. Besides this wonderful news, one week ago, I friend of mine @Ralph (and thanks to [@CuratedIntel](https://twitter.com/CuratedIntel)) gave me as Christmas gift: one of the operational databases of those Booters that were took-down, stresser.gg. AND to my surprise, one chapter of my PhD thesis helped me to analyze the entire data in less than 1h. My book/thesis is publicly available at <https://bit.ly/jjsantanna_thesis>, I’ve used chapter 3 that comes with the scripts available at <https://github.com/jjsantanna/booter_dbs_analyses>. (The problem was to write the following paragraphs with kids at home full time between Christmas and New Year’s Eve).

[Highlights of the analysis] EVERYTHING (data, enrichments, figures, graphs, and scripts) related to the analysis of stresser.gg database is publicly available at <https://github.com/jjsantanna/stresser.gg_db_analysis> let me give you a quick list of observations.

* The database dump file (named stresse\_xr.sql) contains 154k lines
* The database was created by someone Turkish (columns have Turkish words)
* The data contains records only between November/2021 and March/2022
* Total number of attacks: 104.842
* Total number of unique users: 24.501
* Users that performed one or more payment: 173 (only!)
* Top5 countries that most attacked (IP addresses) in the Netherlands:
  + NL -> NL : 731 attacks
  + US -> NL : 160 attacks
  + AR -> NL : 87 attacks
  + CA -> NL : 67 attacks
  + DE -> NL : 64 attacks
* Top5 countries most attacked by users (logged) in the NL:
  + NL -> NL : 731 attacks
  + NL -> US : 209 attacks
  + NL -> TR : 124 attacks
  + NL -> GB : 99 attacks
  + NL -> NO : 97 attacks
* There are many graphs and even an interface to search for records, just access <https://github.com/jjsantanna/stresser.gg_db_analysis>

[Takeaway message]

* The ‘cyber’ police worldwide are doing a LOT but there is still a LOT to do!
* For Booters investigation you can still use my PhD thesis (<https://bit.ly/jjsantanna_thesis>)
* Side-note: YES, I can personally identify MANY users (linked to their Twitter, Instagram, Tiktok, Youtube, Steam, Facebook, Linkedin, Github, Gmail, and others). If I can the police, THTC, HackRight, and beyond also will (I hope)!

[Final Message]

* Would you like me to write a more detailed blog post about it?
* What else would you like to see from this data?