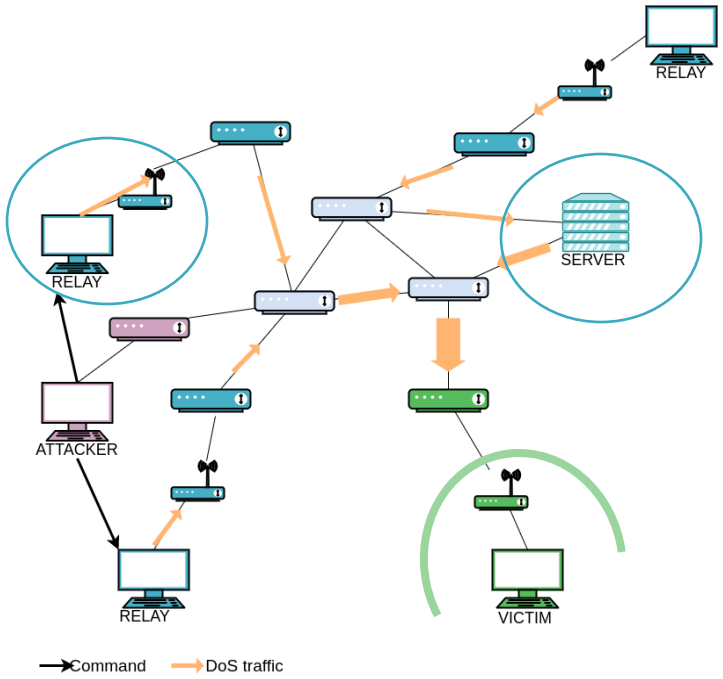
October, 5th 2021

Characterization of relays in Distributed Denial of Service (DDoS) attacks

Our focus:

Study volumetric DDoS relays to better understand them and tackle the problem at the source level.



Camille Moriot (PhD student, Phénix & Agora, CITI), François Lesueur (CASA, IRISA), Nicolas Stouls (Phénix, CITI), Fabrice Valois (AGORA, CITI), Marie-Pierre Escudié (Institut Gaston Berger)

camille.moriot@insa-lyon.fr

From massive DDoS to their characterization and properties

What type of socio-organizational and technical structures host typical DDoS relays?

What is already known about DDoS relays:

Botnet members [1]

- IoT objects
- Infection mechanism

[1] A. Wang, W. Chang, S. Chen, and A. Mohaisen, "Delving Into Internet DDoS Attacks by Botnets : Characterization and Ana-lysis," IEEE/ACM Trans. Netw., vol. 26, no. 6, pp. 2843–2855, 2018.

Amplifiying servers[2]

- DNS, SMTP, ICMP
- Spoofed address

[2] C. Rossow, "Amplification Hell : Revisiting Network Protocols for DDoS Abuse," in 21st Annual Network and Distributed System Security Symposium, NDSS,USA, 2014.

Cloud Servers[3]

- Great Bandwith, small price, short lease periods

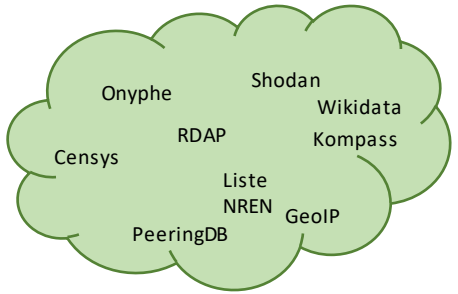
[3] Z. He, T. Zhang, and R. B. Lee, "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," in 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017, USA, 2017, pp. 114–120.

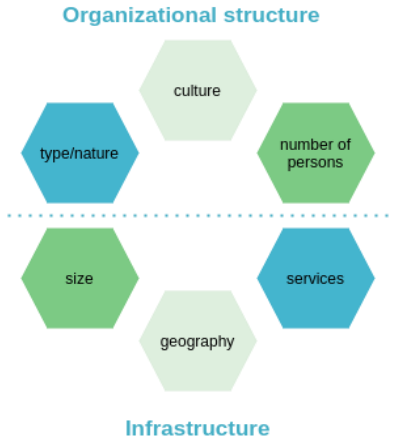
Geographic location of relays [4]

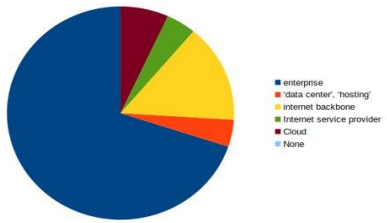
[4] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in IFIP/IEEE International Symposium on Integrated Network Management, IM 2015, Canada, 2015, pp. 243–251.

Our methodology:

DDoS traces :
Recent actual attack capture recorded as close as possible to the victim.







Dashboard and Wireshark dissector