On DDoS Attacks

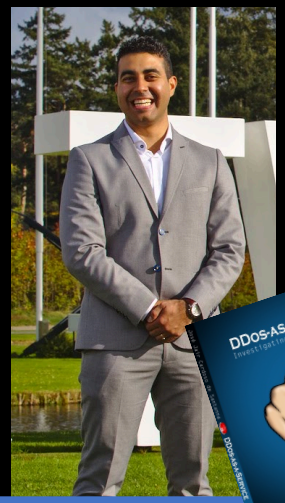
Jair Santanna

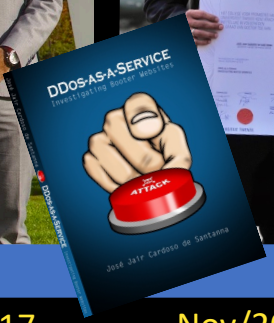
[jairsantanna@gmail.com]

07-04-2022

Who am I?

Dr. José Jair Cardoso de Santanna





Mar/2013
Begin PhD
1st DDoS Researcher

Ago/2017
Utwente
Assistant Professor

Nov/2017
Doctor Degree

Dec/2017
'Helper' of the Dutch Team High Tech Crime Unit (Midden NL, Japanese, Danish, NCA, FBI)

May/2018
Best Science Communicator of the Netherlands (FAMELAB2018)

Jun/2018
Married to a "bitterballen lover"

May/2019
Father of
A girl!

May/202
Father of
A boy!

Cloud Security Lead
@Northwave

My goal? What is DefCon Holland?

“DefCon Holland […] in Amsterdam (DC3120) and […] in Delft (DC3115).”

What is DefCon Holland? and my goal.

"DefCon Holland meetups are meetups for Dutch Hackers[…]"

"an enthusiastic and skilful computer programmer or user."

"help you learn new things"

"for folks interested in the alternate applications of modern technology, referred to properly as 'hacking'"

"discussion of technology and security topics"

3 PARTS!

DDOS THEORY + PRACTICE & ALTERNATE APPLICATIONS

Distributed Denial of Service Attack

DDoS Attack definition(s) - 2

When a service is unavailable to its intended users, intentionally caused by multiple sources.

DDoS Attack definition(s) - Analogy

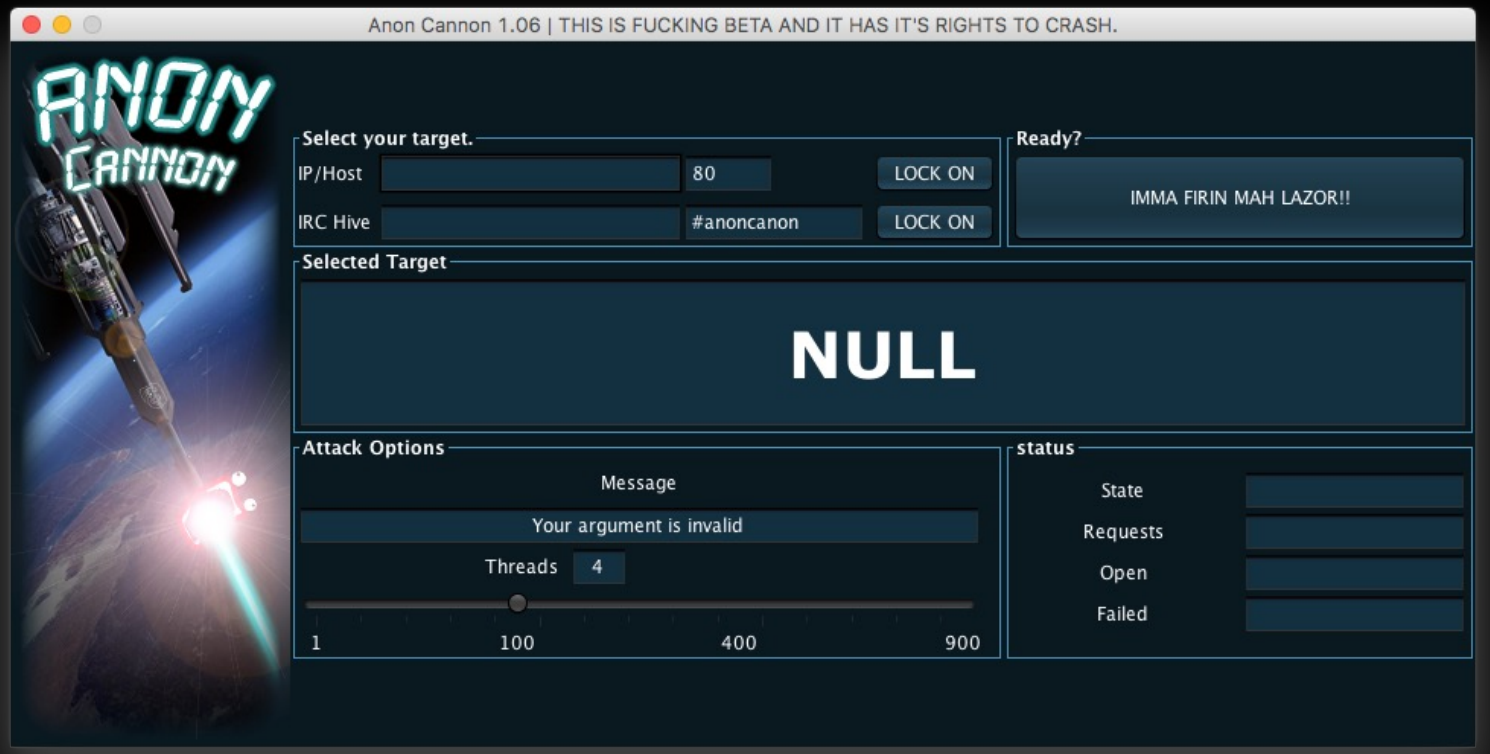
DDoS Attack definition(s) - 3

High repetition of network traffic with similar characteristics coming from >1 source IP address to 1 destination IP address

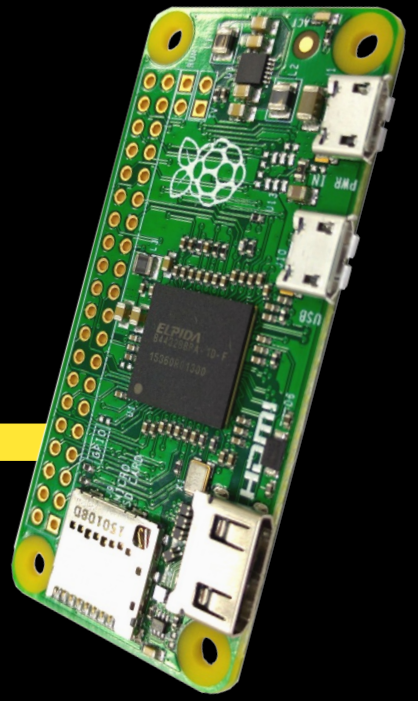
*Multi-vector

Learning by doing…

http://bit.ly/2wWiM43



Learning by doing…

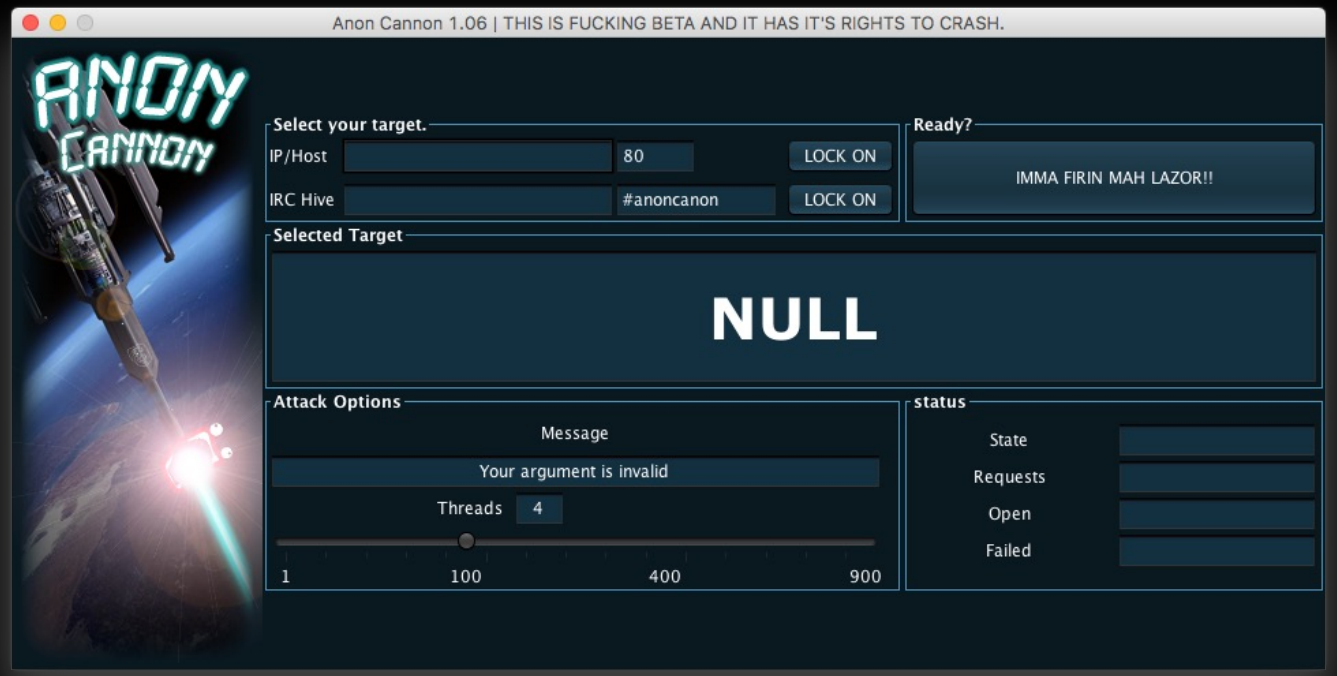


ssid: DDoS_handson

pwd: ***jairsantanna.com***

Learning by doing…

192.168.1.135



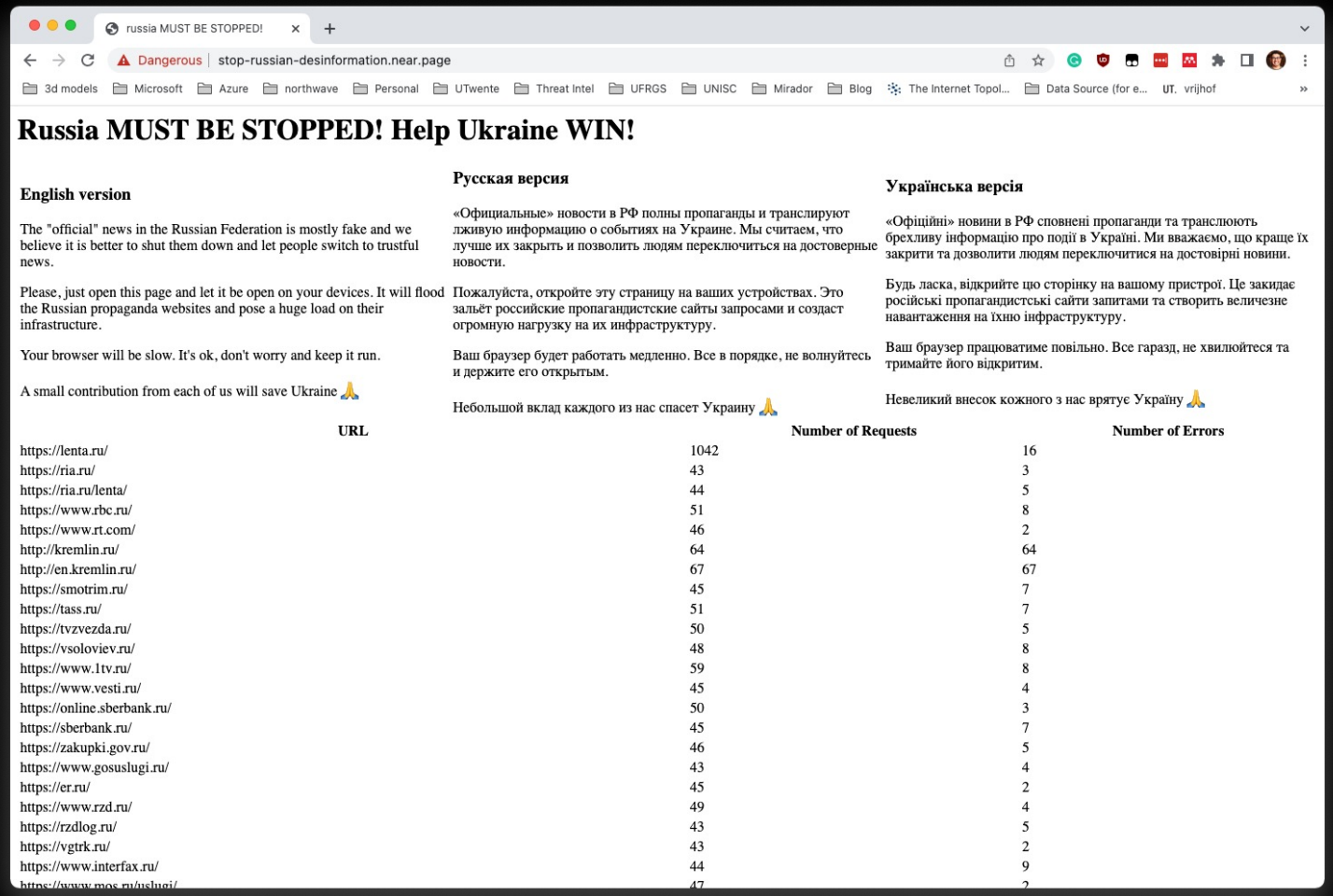
ssid: DDoS 2021

pwd: ***ddos2021***

192.168.1.135

Learning by doing…

Improvising… “alternate applications”



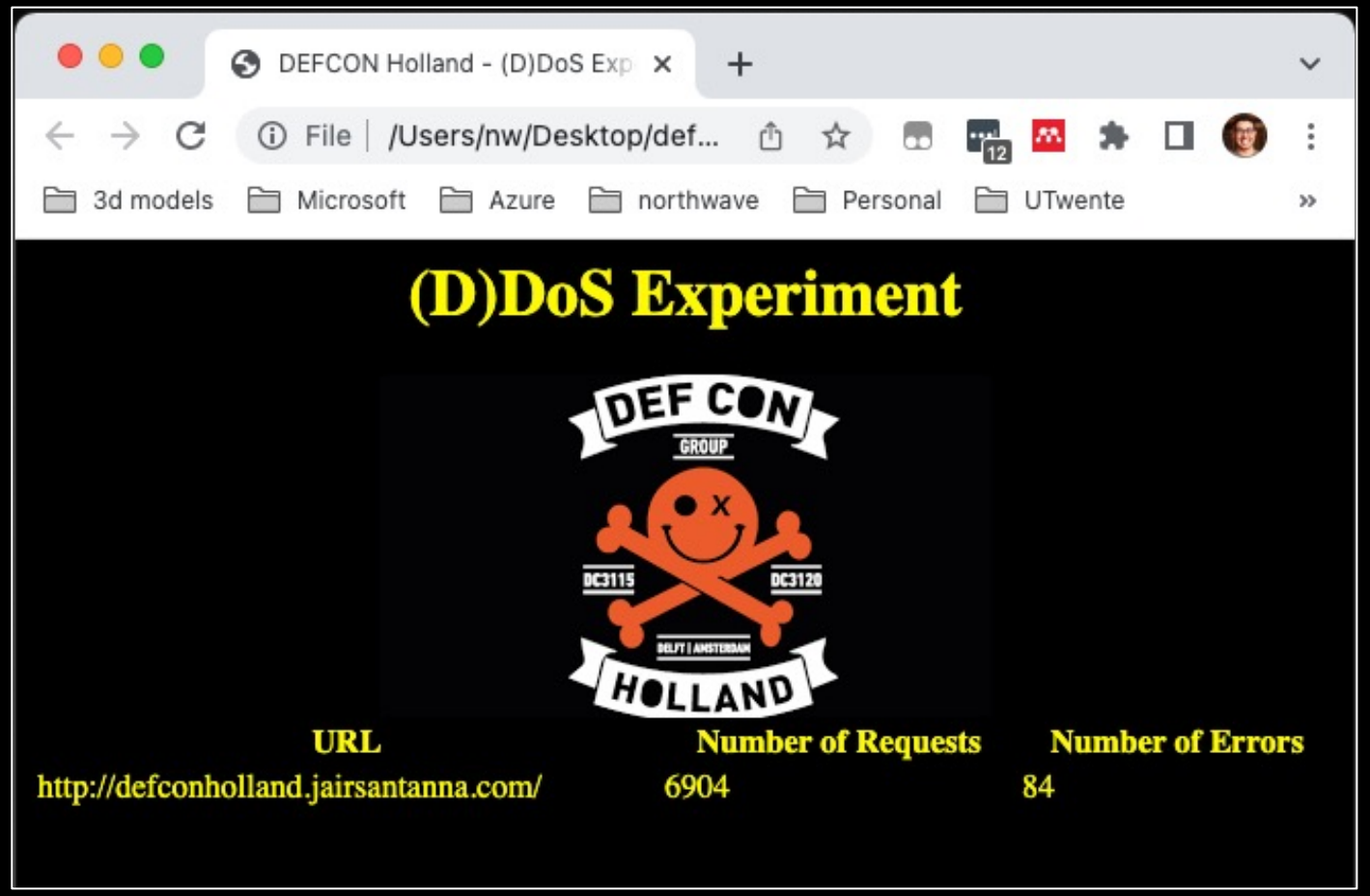
https://stop-russian-desinformation.near.page

wget

index.html

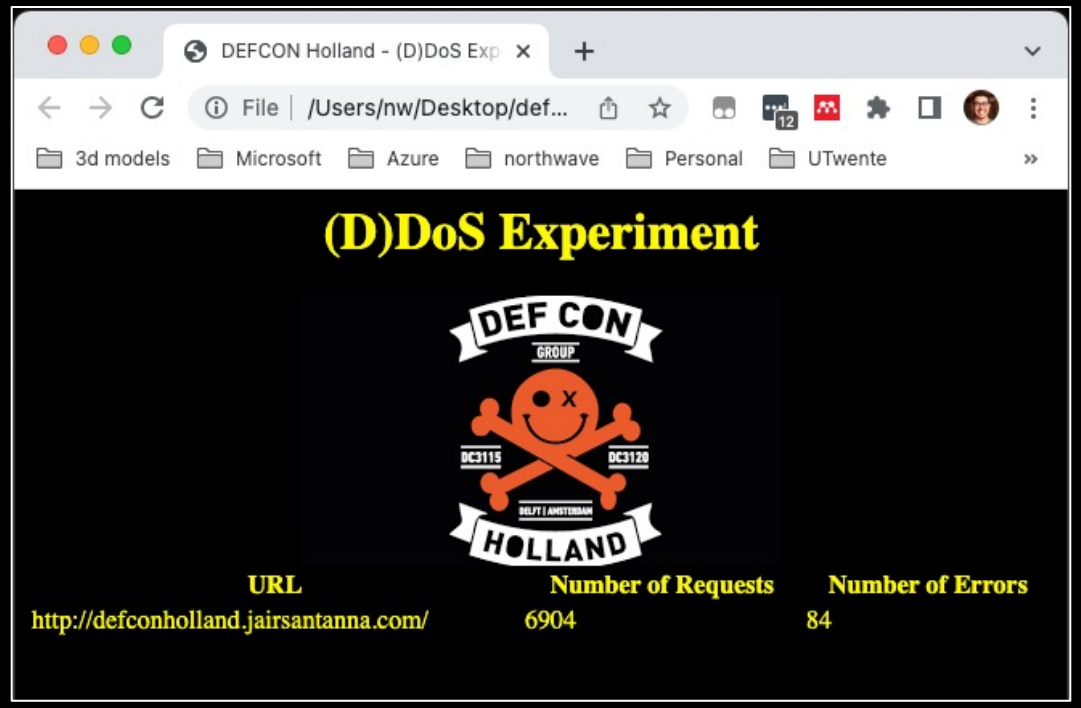
github.com/jjsantanna/defcon_holland_ddos

Improvising… “alternate applications”

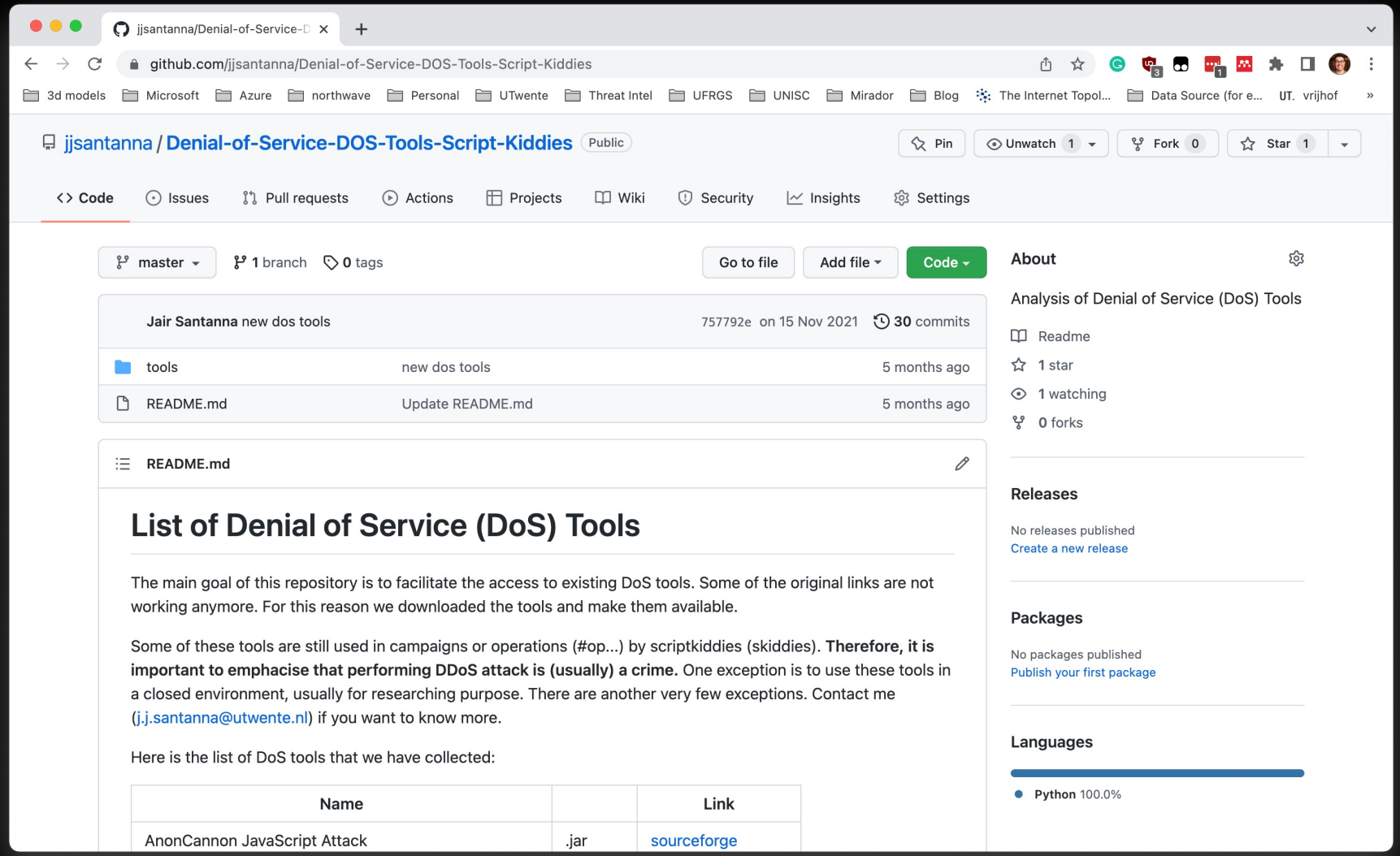


Improvising… “alternate applications”

192.87.172.166:8888



“Alternate applications” for (D)DoS



https://github.com/jjsantanna/Denial-of-Service-DOS-Tools-Script-Kiddies

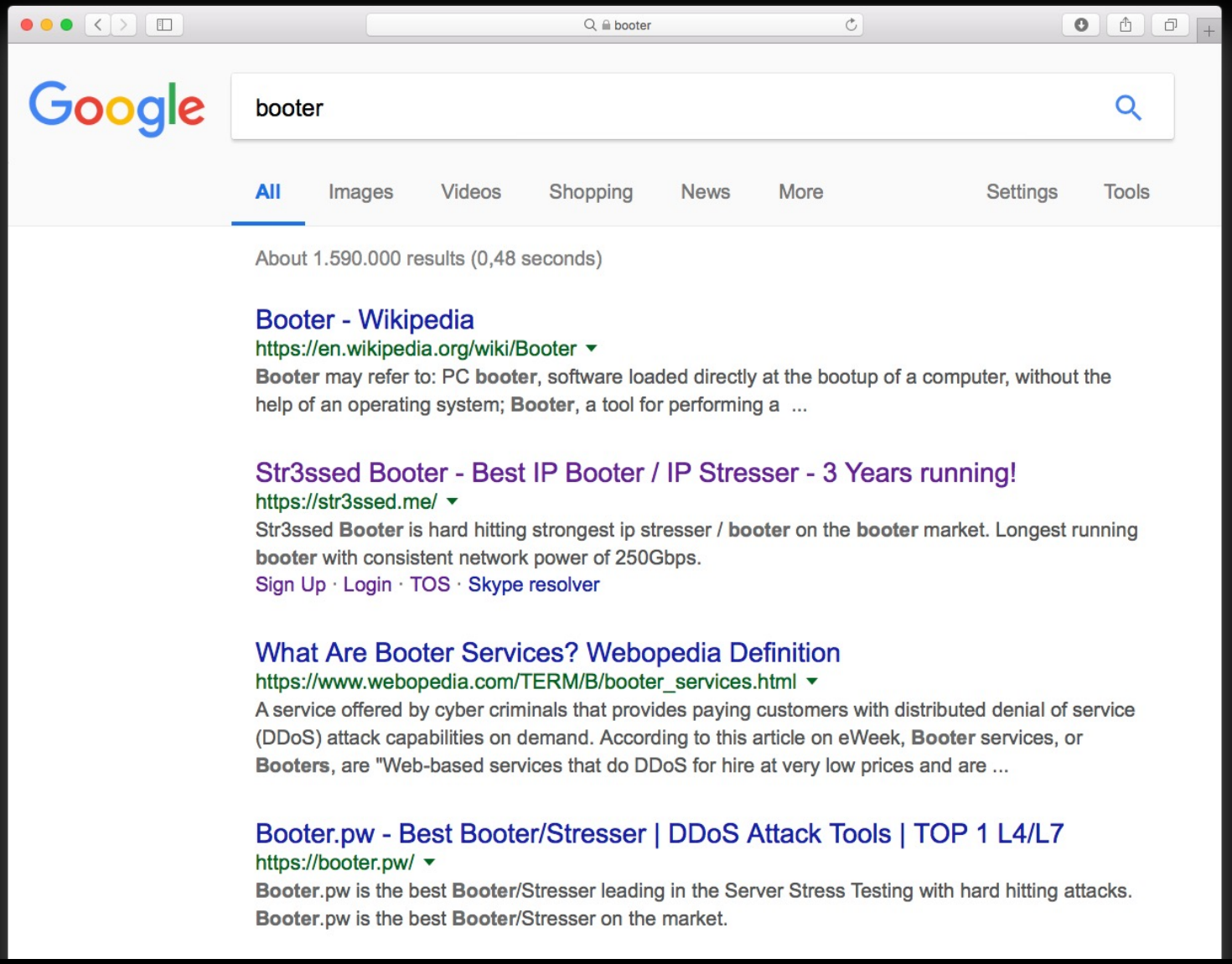
MY STORY IN NL
&
BOOTERS

2013

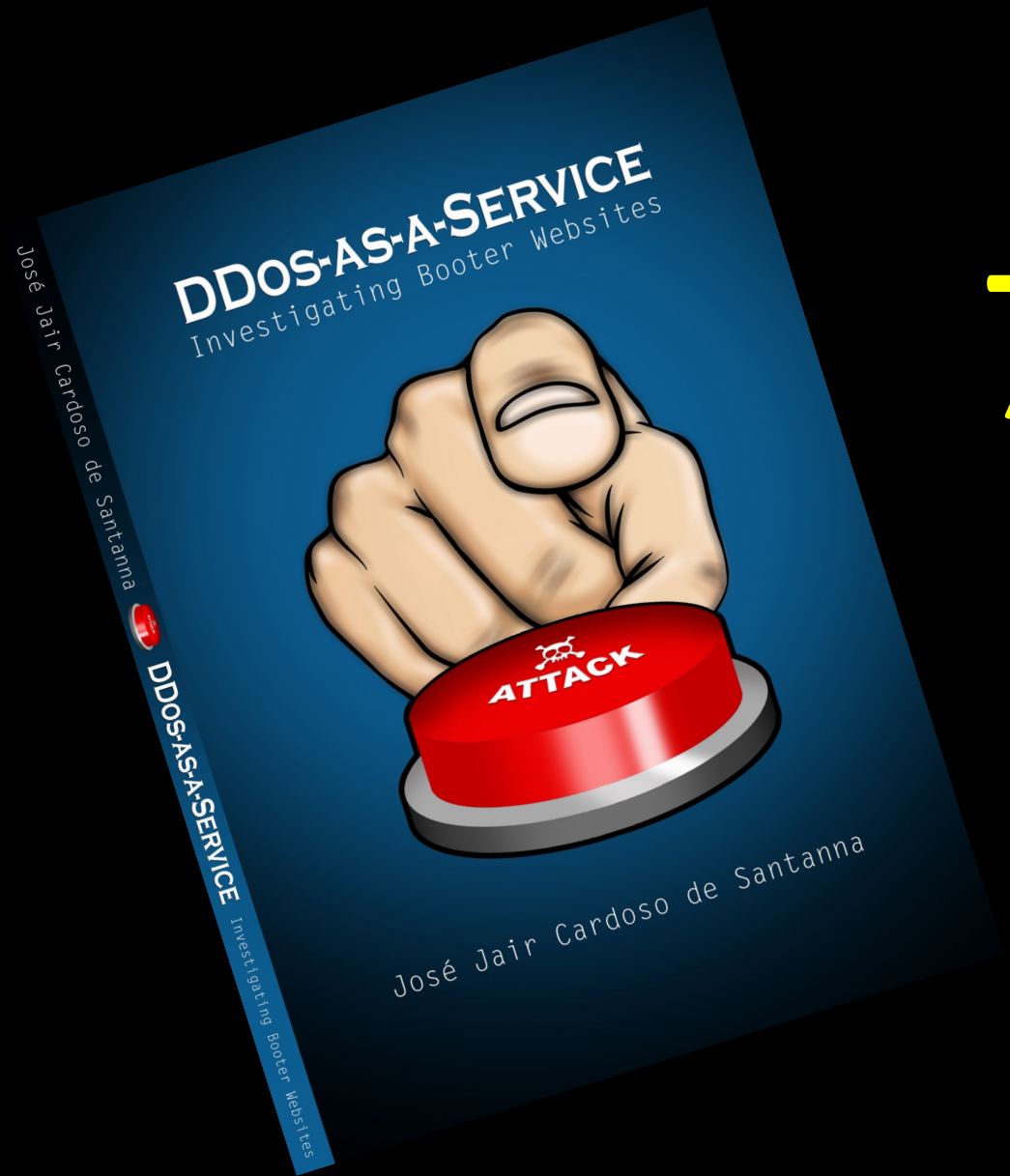
SURF NET

Online Exams!

Let me Google for you… booter or stresser



My PhD thesis

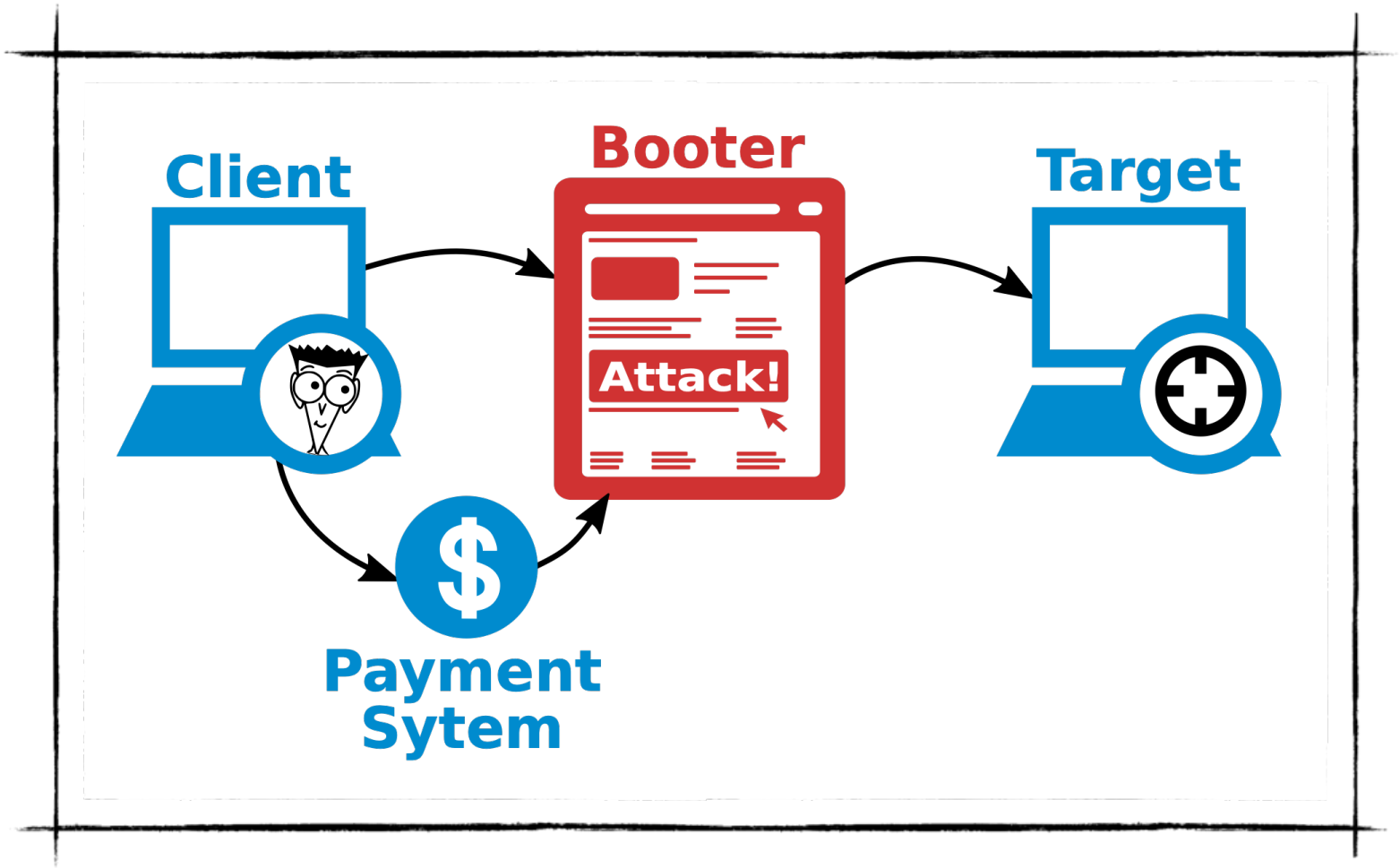


7 CHAPTERS

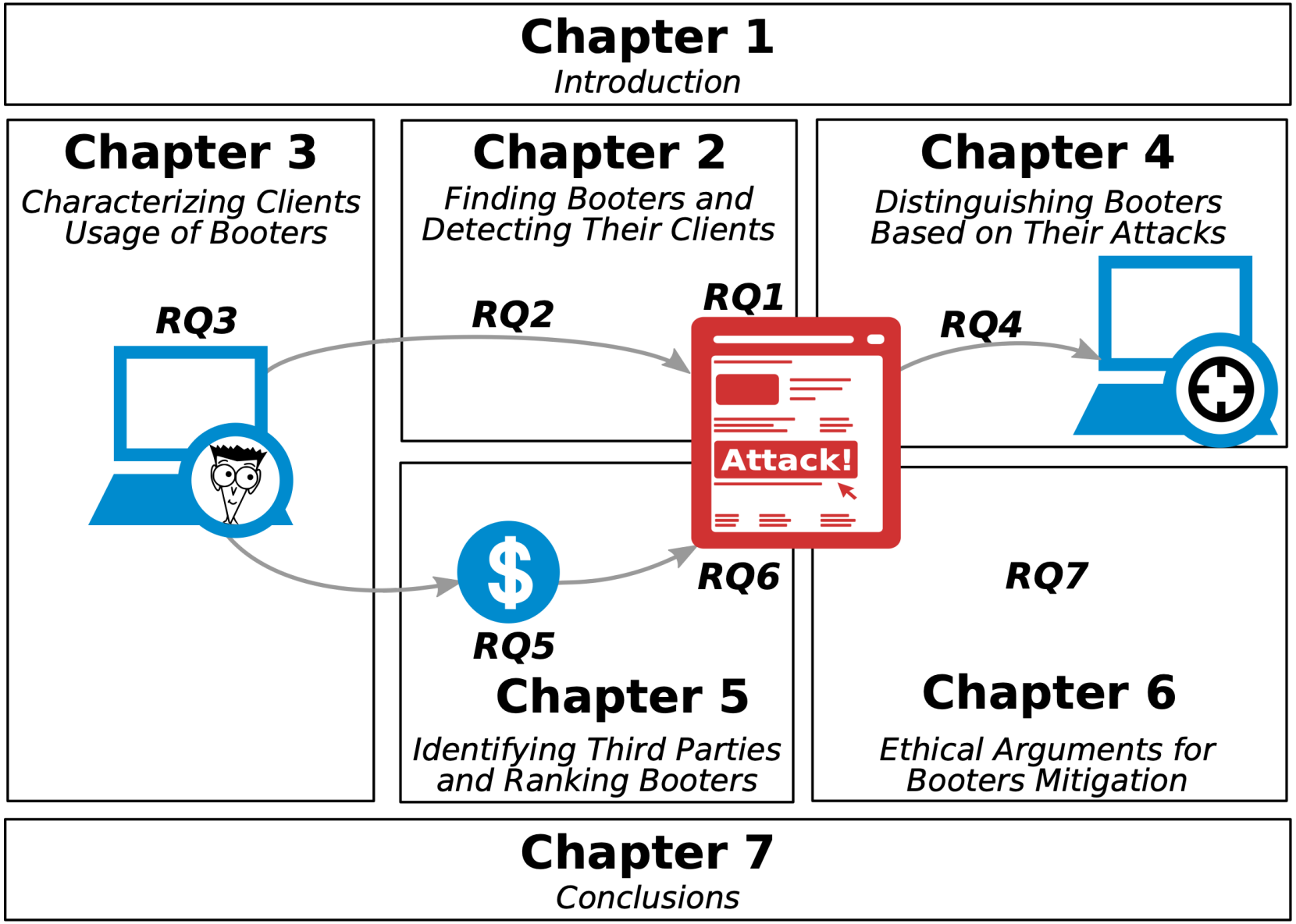
bit.ly/jjsantanna_thesis

FOR FREE!

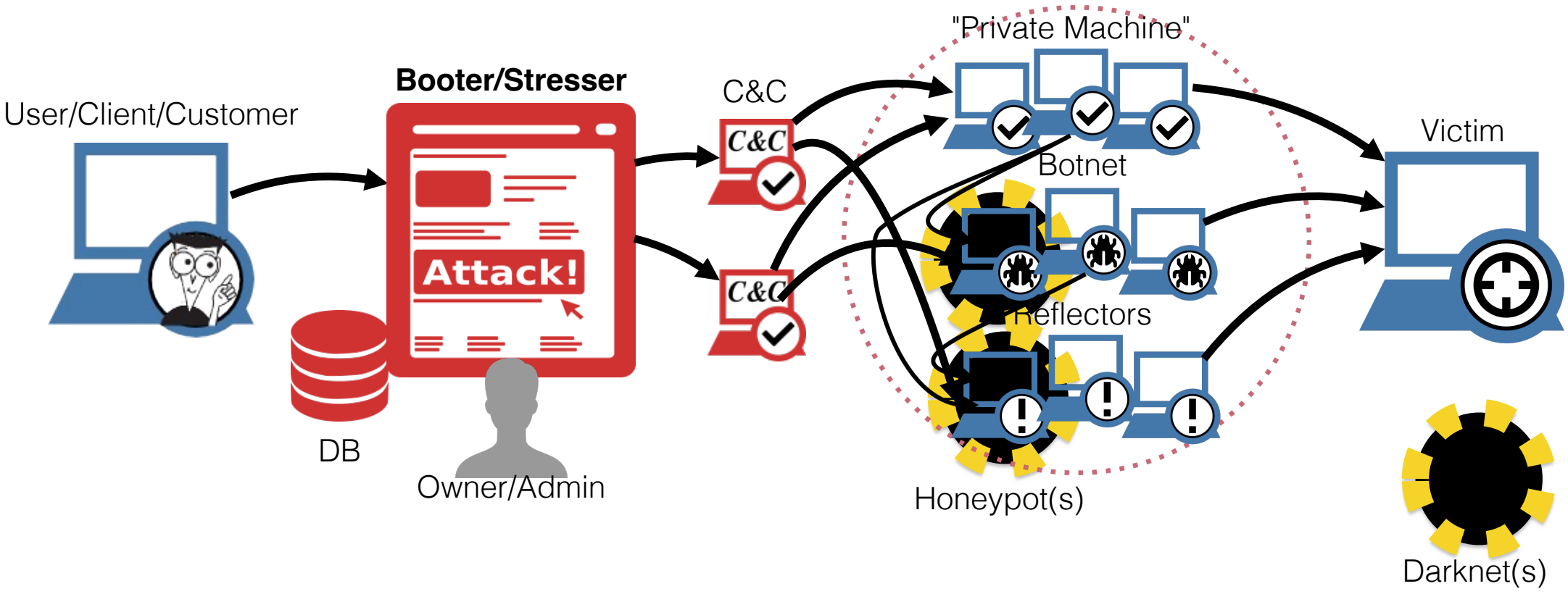
Chapter 1



Chapter 1

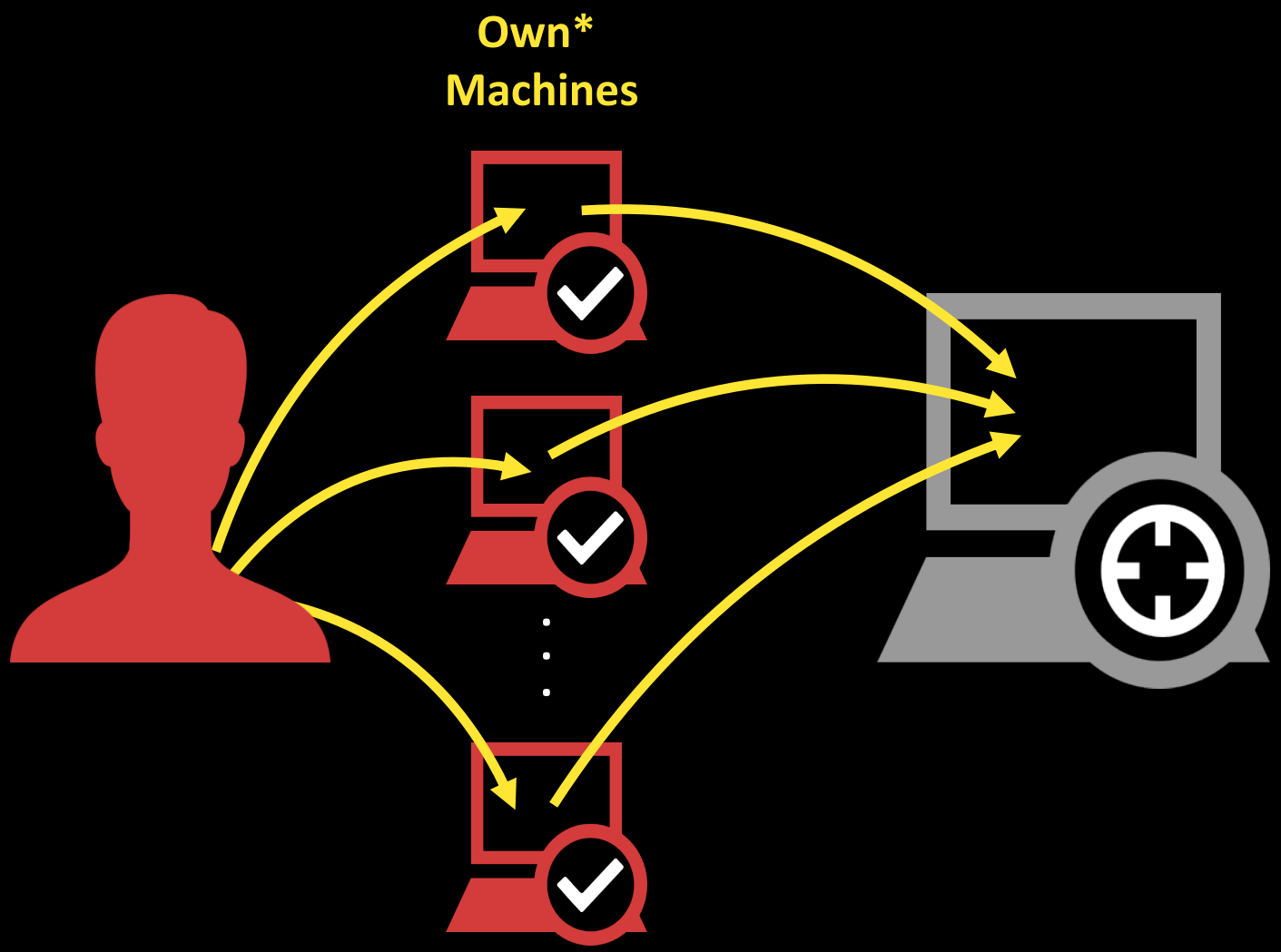

Chapter 1
Introduction
Chapter 3
Characterizing Clients Usage of Booters
Chapter 2
Finding Booters and Detecting Their Clients
Chapter 4
Distinguishing Booters Based on Their Attacks
RQ1
RQ2
RQ3
RQ4
Attack!
RQ5
RQ6
RQ7
Chapter 5
Identifying Third Parties and Ranking Booters
Chapter 6
Ethical Arguments for Booters Mitigation
Chapter 7
Conclusions

Conclusion

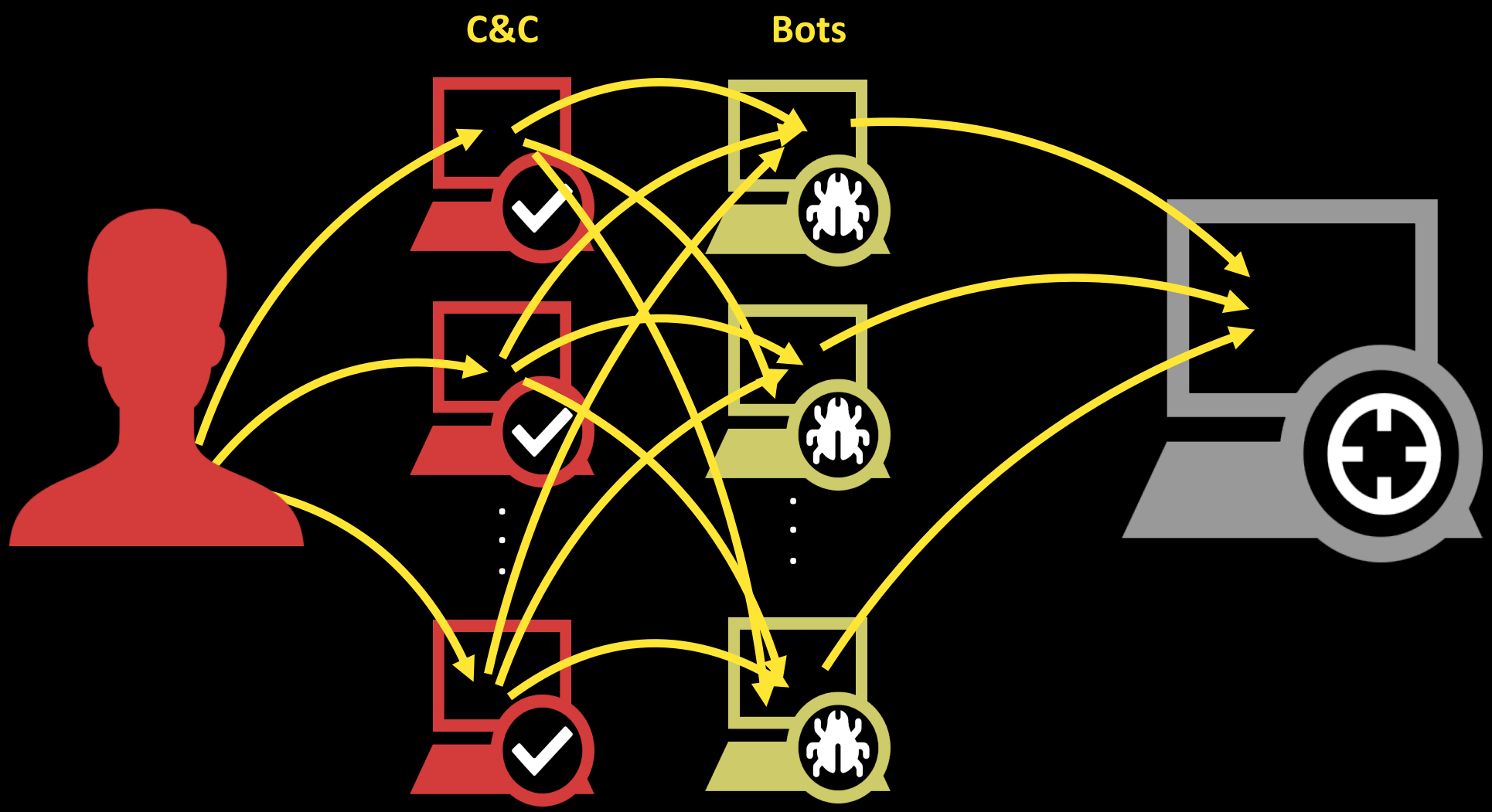

User/Client/Customer
Booter/Stresser
Attack!
DB
Owner/Admin
C&C
C&C
C&C
"Private Machine"
Botnet
Reflectors
Honeypot(s)
Victim
Darknet(s)


Payment Service
Web-Hosting
Netw. Opera.
Whois Privacy
CBSP
Registrar
Search Engines
Advert. Places
Law Eforcement Agencies
Legislators + Judges

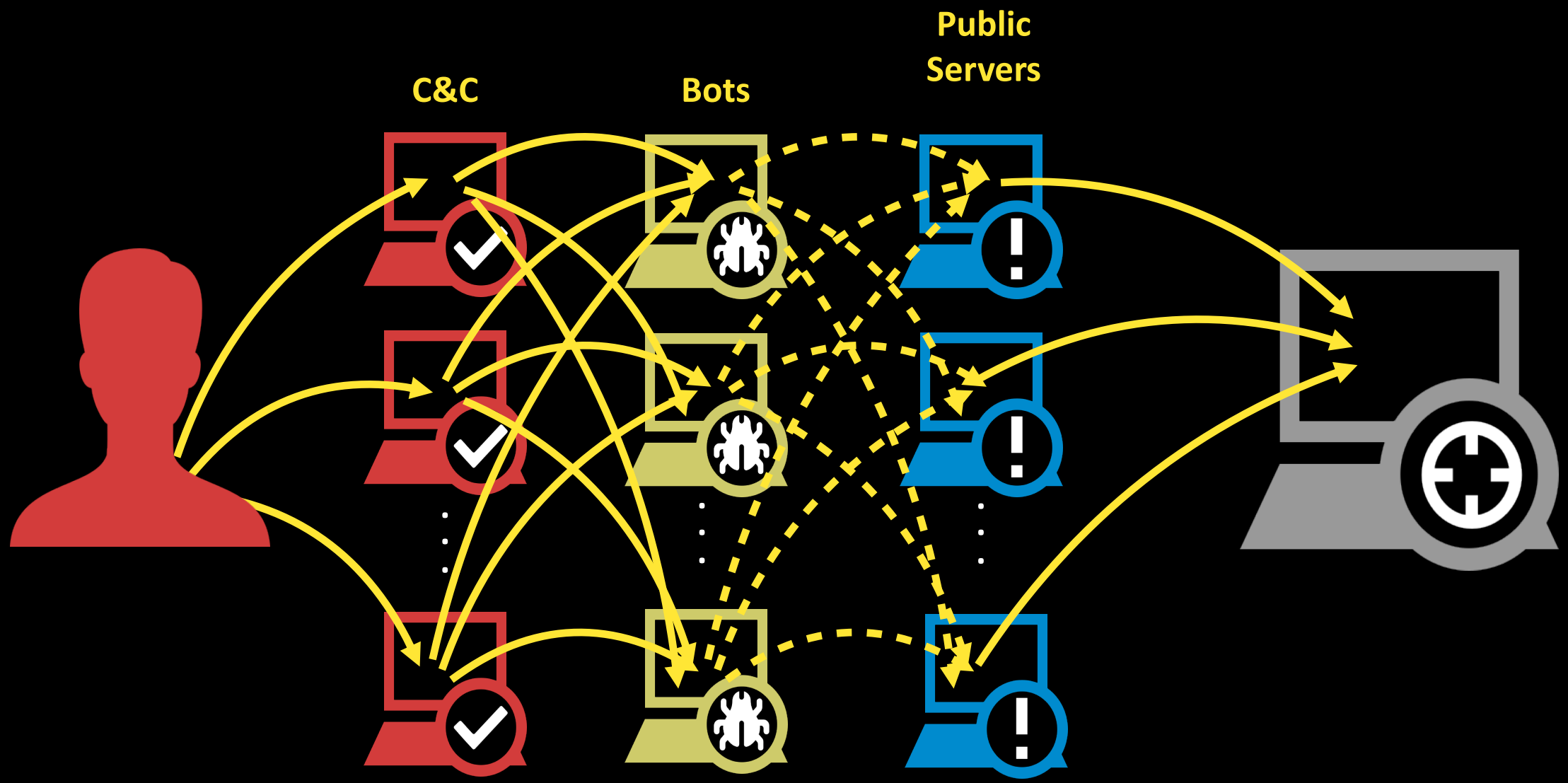
Infrastructure - Case 1



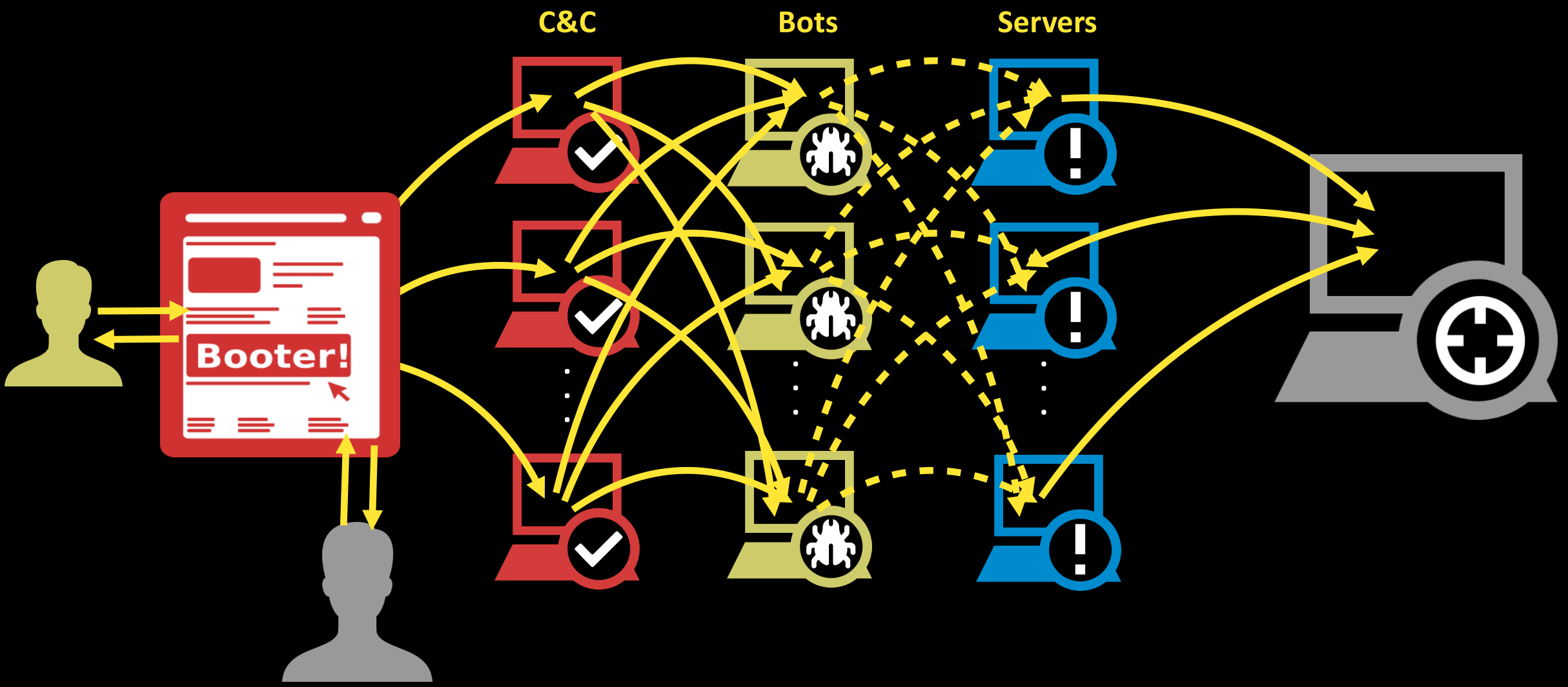
Infrastructure - Case 2



Infrastructure - Case 3



Infrastructure - Case 4



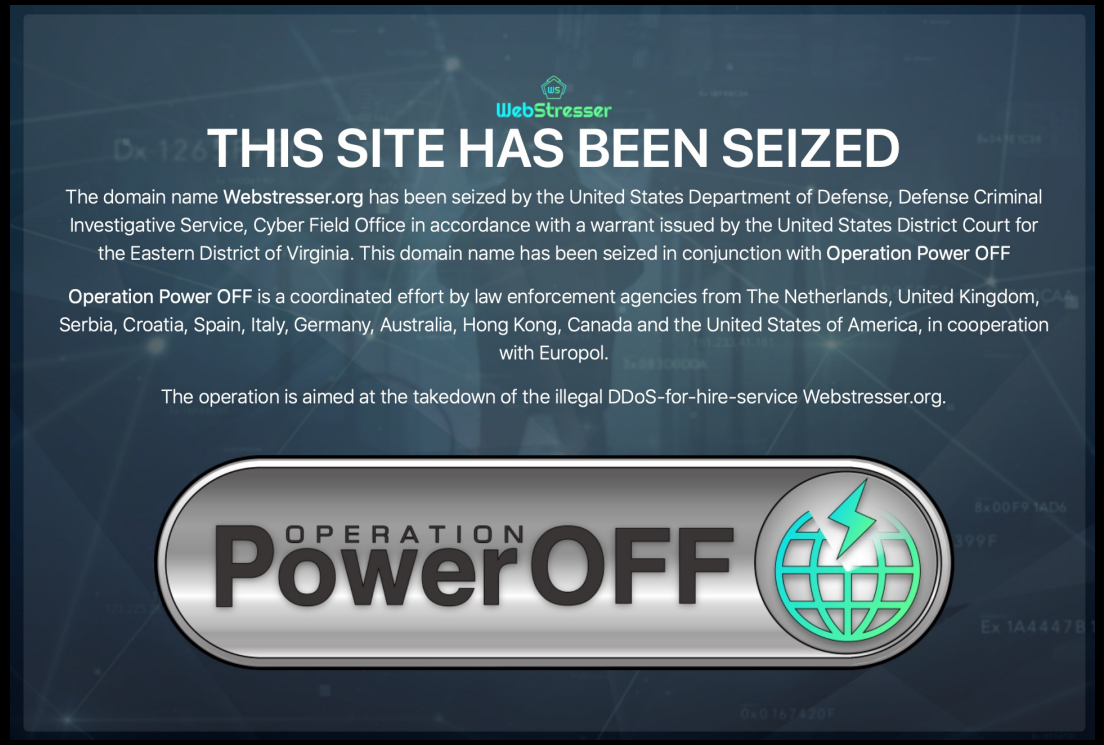
Chapter 7

[Akamai, 2017]

“There is one factor that seems to be affecting the DDos landscape as a whole:

LAW ENFORCEMENT"

Voilà!



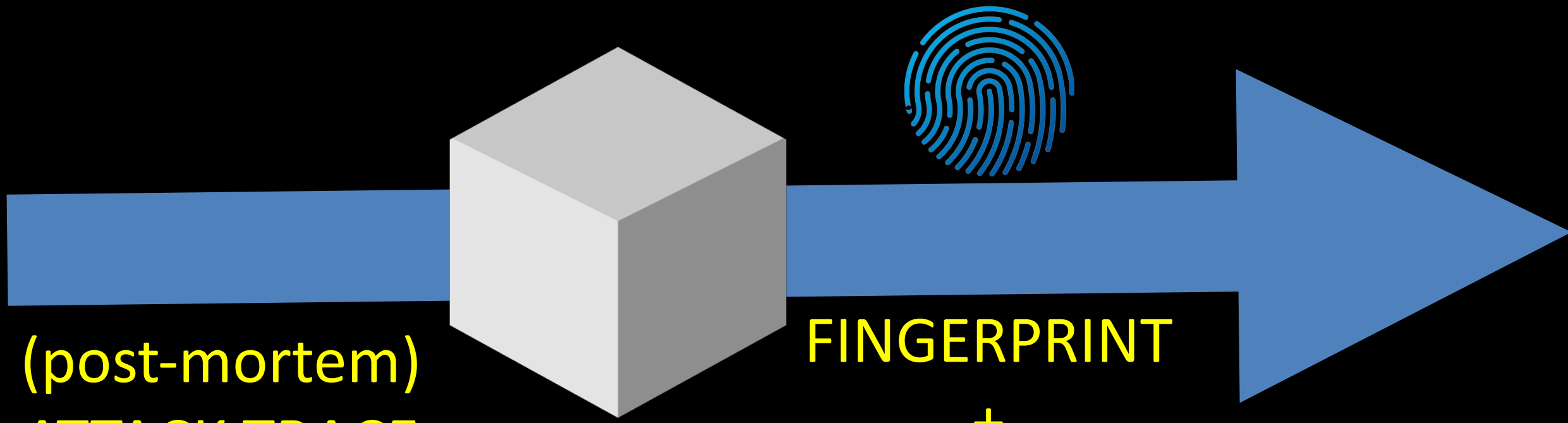
webstresser.org

anonsecurityteam.com
booter.ninja
bullstresser.net
critical-boot.com
defcon.pro
defianceprotocol.com
downthem.org
layer7-stresser.xyz
netstress.org
quantumstress.net
ragebooter.com
ragebooter.net
str3ssed.me
torsecurityteam.org
vbooter.org
request.rip

WHAT ELSE?

The need for fingerprinting

DDoS Dissector + DDoSDB + DDoS Fingerprint converters

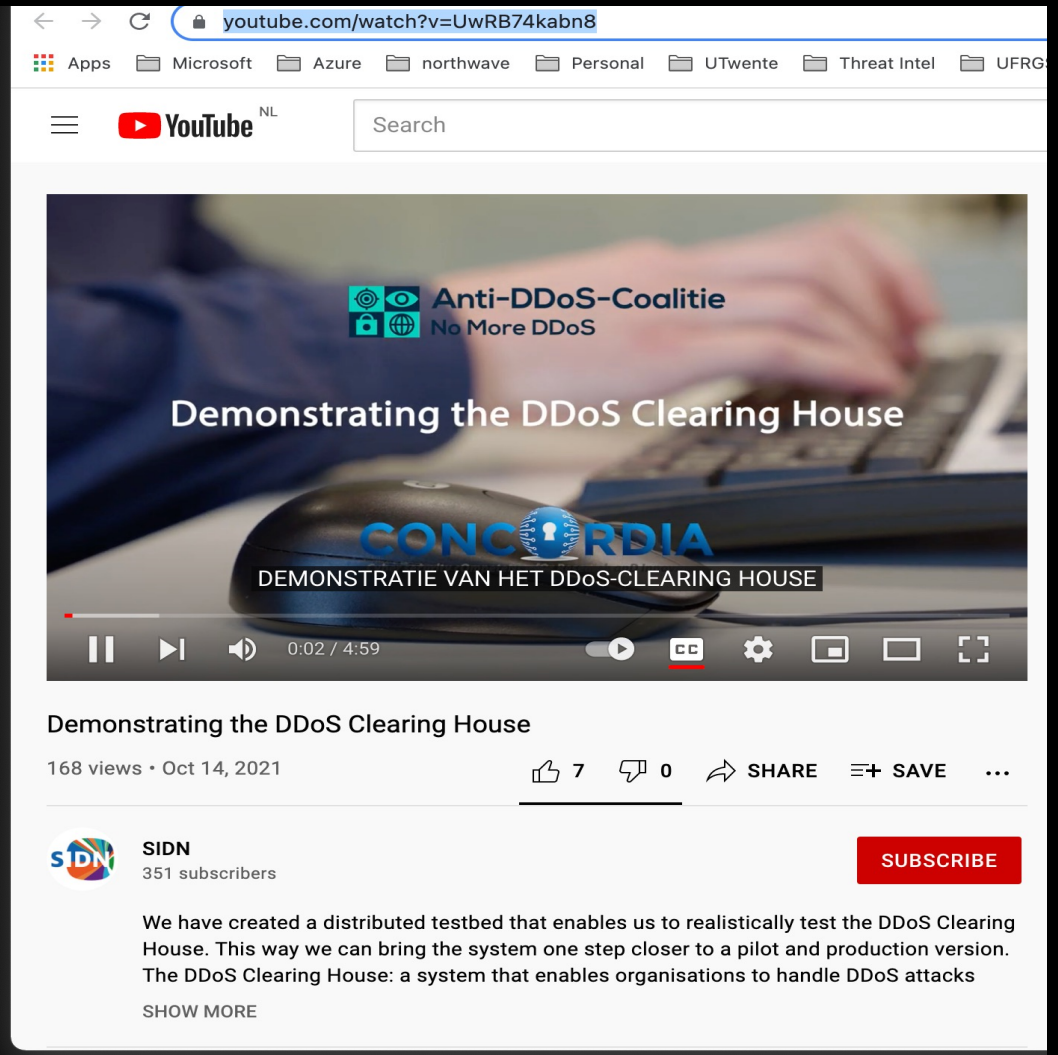


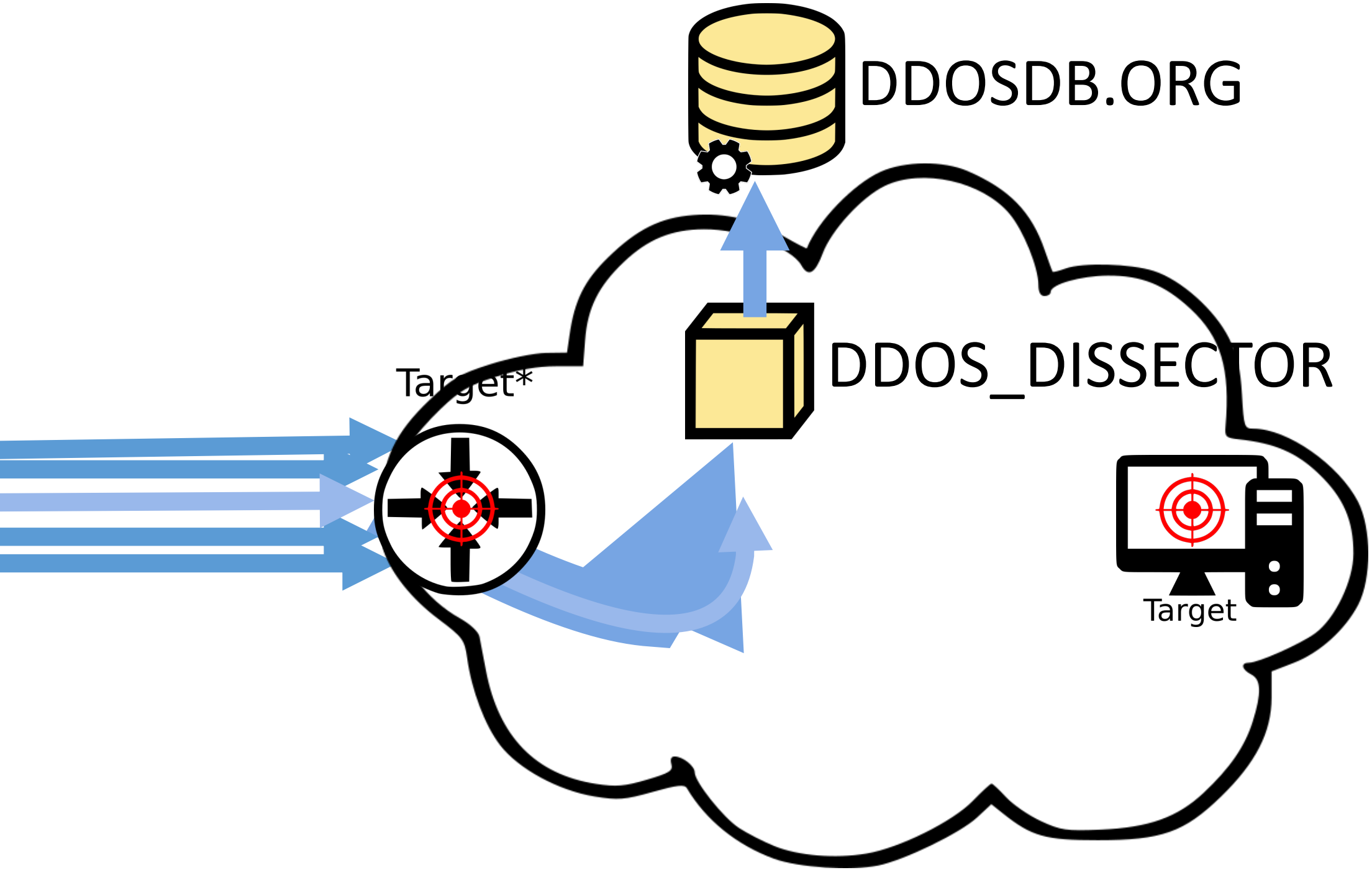
(post-mortem)
ATTACK TRACE

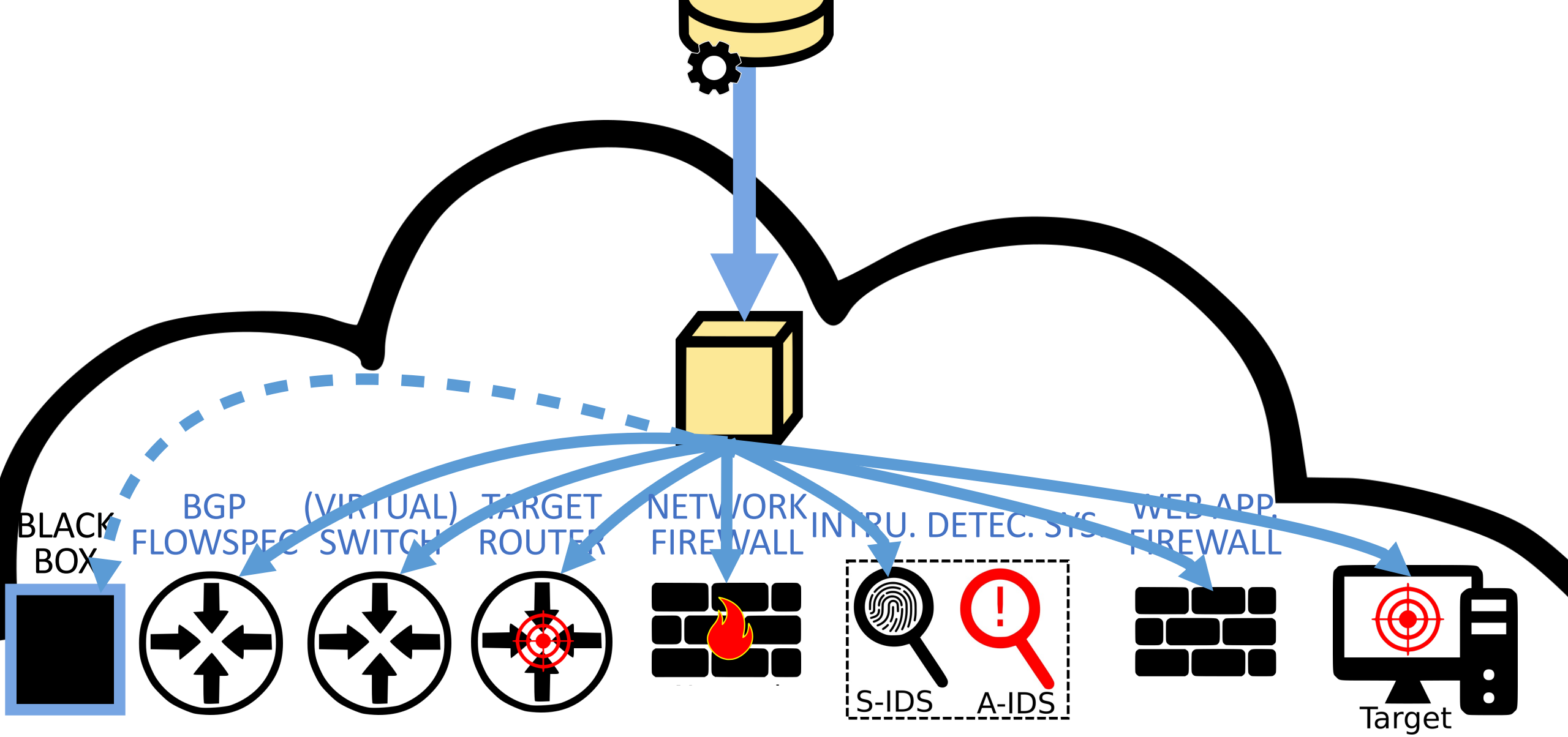
FINGERPRINT
+
ANONYMIZED
attack trace

DDoS Dissector + DDoS Fingerprint converters

https://www.youtube.com/watch?v=UwRB74kabn8




DDOSDB.ORG
DDOS_DISSECTOR
Target*
Target



Communicating Upstream Provider via IETF DDoS Open Threat Signaling (DOTS)

Everything into the **DDoS Clearing House** == Anti-DDoS Coalition

DDoSDB

https://ddosdb.[redacted]/

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

https://www.concordia-h2020.eu/

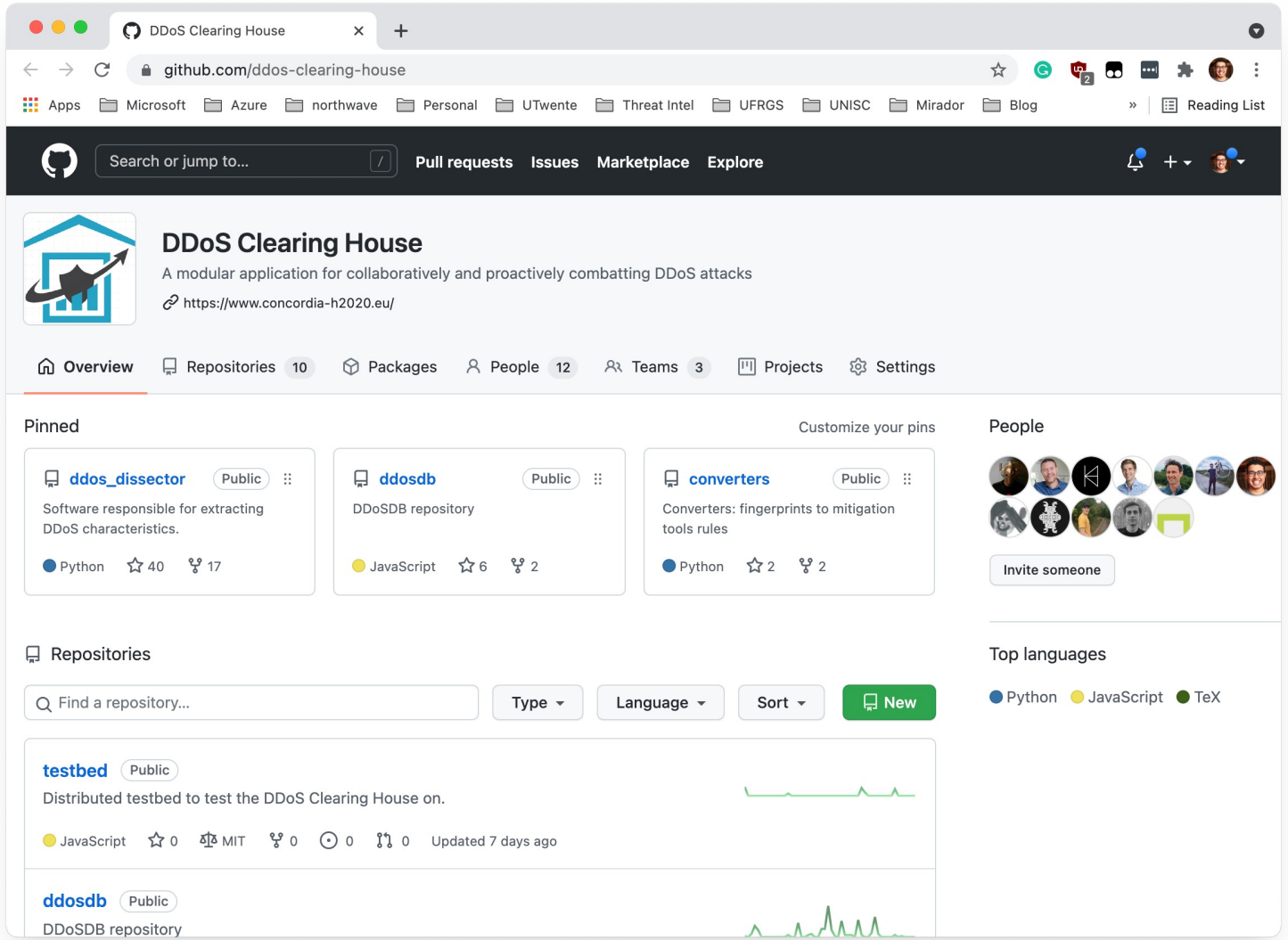
Anti-DDoS-Coalitie
No More DDoS

https://www.nomoreddos.org/

European Commission

The DDoS Clearing House has been designated a 'key innovation' by the European Commission and selected for the Commission's Innovation Radar.

https://bit.ly/eu_key_innovation



https://github.com/ddos-clearing-house

Recap…

"for folks interested in the **alternate applications** of modern technology, referred to properly as 'hacking'"

"discussion of technology and **security topics**"

"help you learn new things"

On DDoS Attacks

Jair Santanna

[jairsantanna@gmail.com]

07-04-2022