



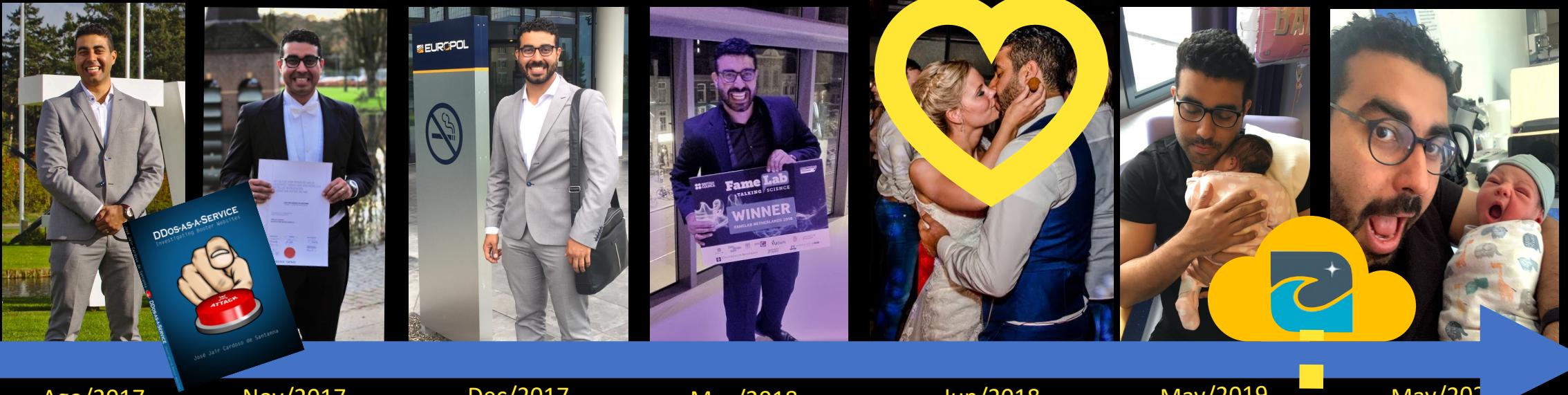
On DDoS Attacks

Jair Santanna

[jairsantanna@gmail.com]

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!

Cloud Security Lead
@Northwave

May/2022
Father of
A boy!

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!

PART I

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.

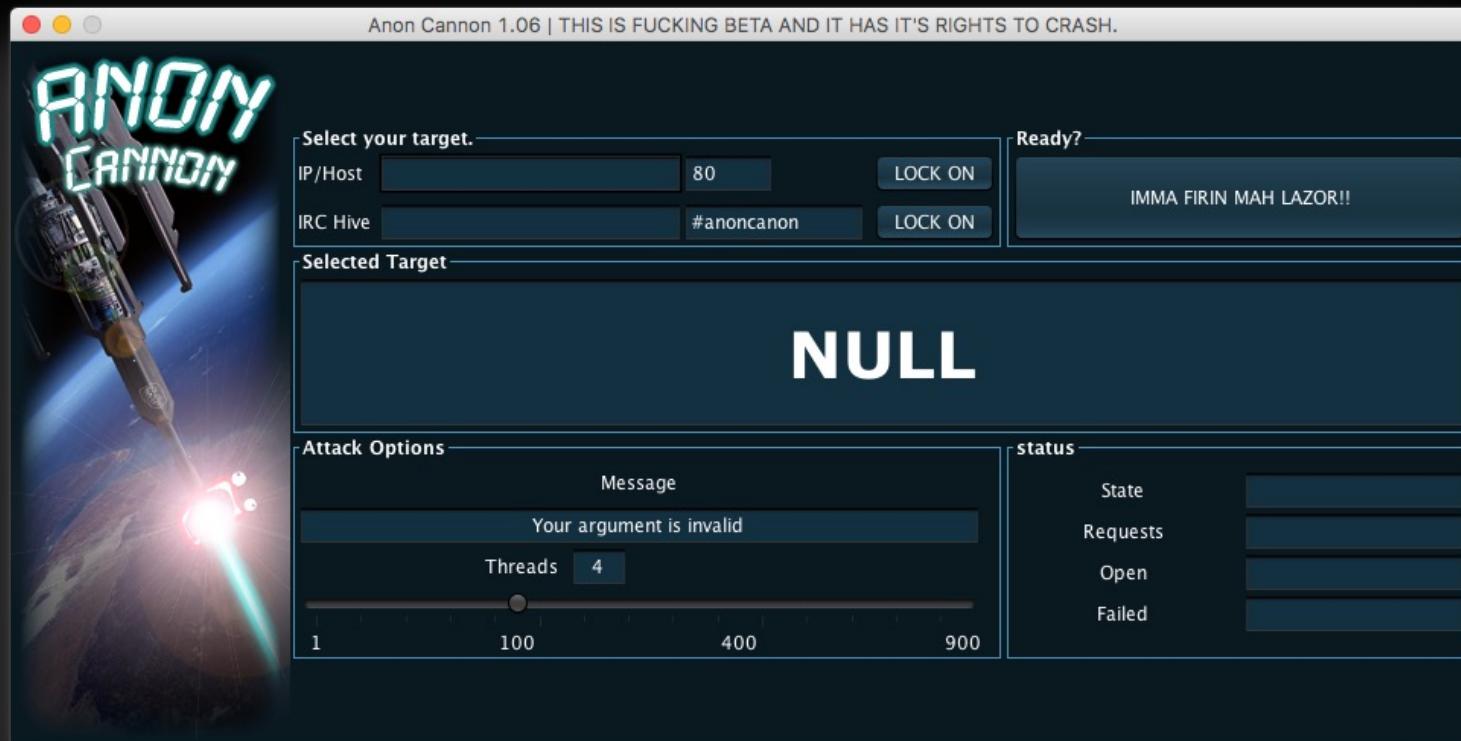
DDoS Attack definition(s) - Analogy



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

Learning by doing...

<http://bit.ly/2wWiM43>



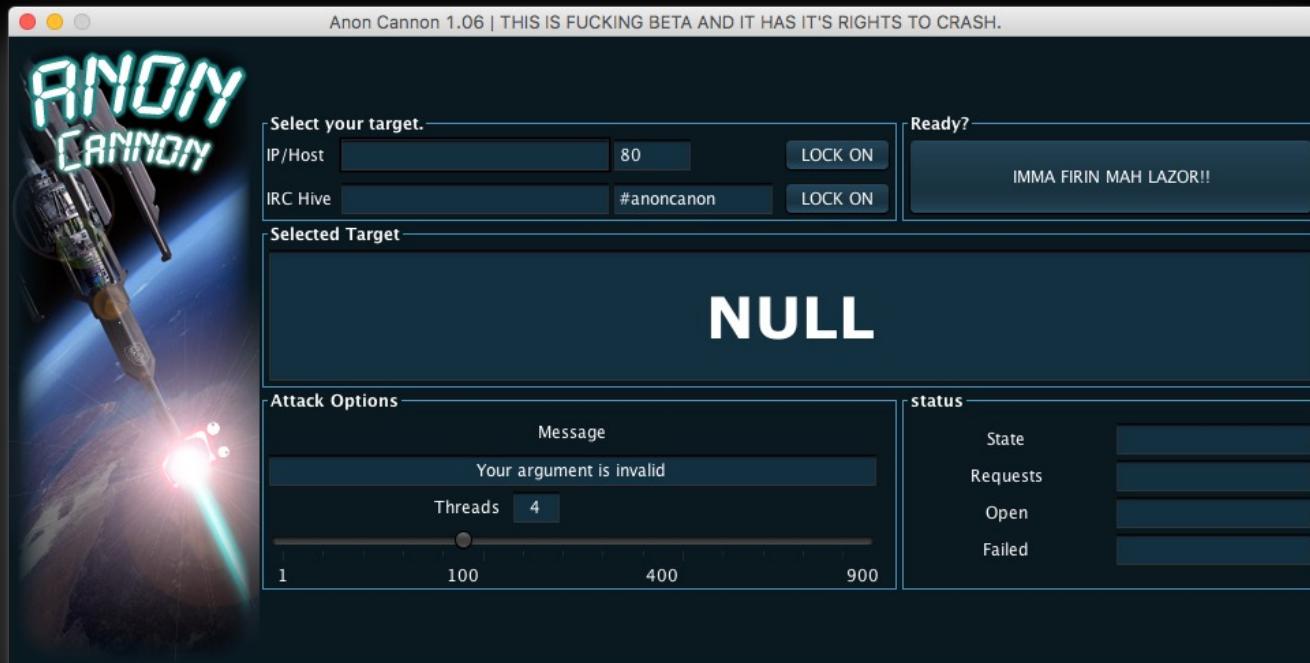
Learning by doing...



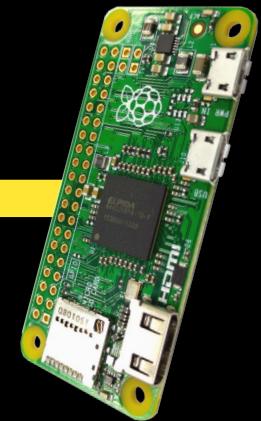
*pwd: **jairsantanna.com***

Learning by doing...

192.168.1.135



ssid: DDoS 2021



pwd: ddos2021

192.168.1.135

Learning by doing...



Improvising... “alternate applications”

The screenshot shows a web browser window with the following content:

English version

The "official" news in the Russian Federation is mostly fake and we believe it is better to shut them down and let people switch to truthful news.

Please, just open this page and let it be open on your devices. It will flood the Russian propaganda websites and pose a huge load on their infrastructure.

Your browser will be slow. It's ok, don't worry and keep it run.

A small contribution from each of us will save Ukraine 🙏

URL

https://lenta.ru/
https://ria.ru/
https://ria.ru/lenta/
https://www.rbc.ru/
https://www.rt.com/
http://kremlin.ru/
http://en.kremlin.ru/
https://smotrim.ru/
https://tass.ru/
https://tvzvezda.ru/
https://vsoloviev.ru/
https://www.ltv.ru/
https://www.vesti.ru/
https://online.sberbank.ru/
https://sberbank.ru/
https://zakupki.gov.ru/
https://www.gosuslugi.ru/
https://er.ru/
https://www.rzd.ru/
https://rzdlog.ru/
https://vgtrk.ru/
https://www.interfax.ru/
https://www.mos.ru/uslugi/

Русская версия

«Официальные» новости в РФ полны пропаганды и транслируют лживую информацию о событиях на Украине. Мы считаем, что лучше их закрыть и позволить людям переключиться на достоверные новости.

Пожалуйста, откройте эту страницу на ваших устройствах. Это запьёт российские пропагандистские сайты запросами и создаст огромную нагрузку на их инфраструктуру.

Ваш браузер будет работать медленно. Все в порядке, не волнуйтесь и держите его открытым.

Небольшой вклад каждого из нас спасет Украину 🙏

Українська версія

«Офіційні» новини в РФ сповнені пропаганди та транслюють брехливу інформацію про події в Україні. Ми вважаємо, що краще їх закрити та дозволити людям переключитися на достовірні новини.

Будь ласка, відкрийте цю сторінку на вашому пристрої. Це закідає російські пропагандистські сайти запитами та створить величезне навантаження на їхню інфраструктуру.

Ваш браузер працюватиме повільно. Все гаряць, не хвилюйтесь та тримайте його відкритим.

Невеликий внесок кожного з нас врятує Україну 🙏

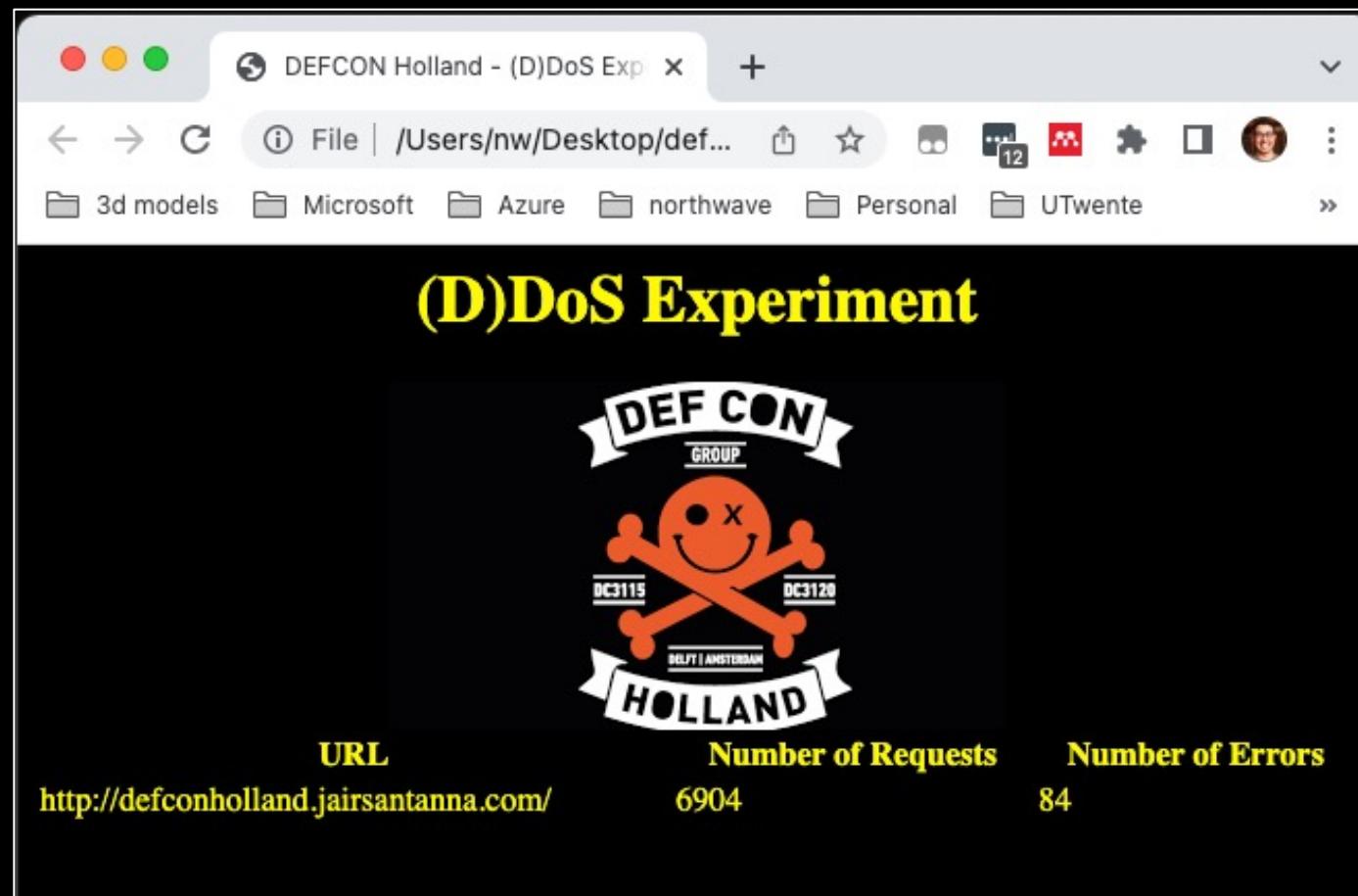
	Number of Requests	Number of Errors
1042	16	
43	3	
44	5	
51	8	
46	2	
64	64	
67	67	
45	7	
51	7	
50	5	
48	8	
59	8	
45	4	
50	3	
45	7	
46	5	
43	4	
45	2	
49	4	
43	5	
43	2	
44	9	
47	2	

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

wget
index.html

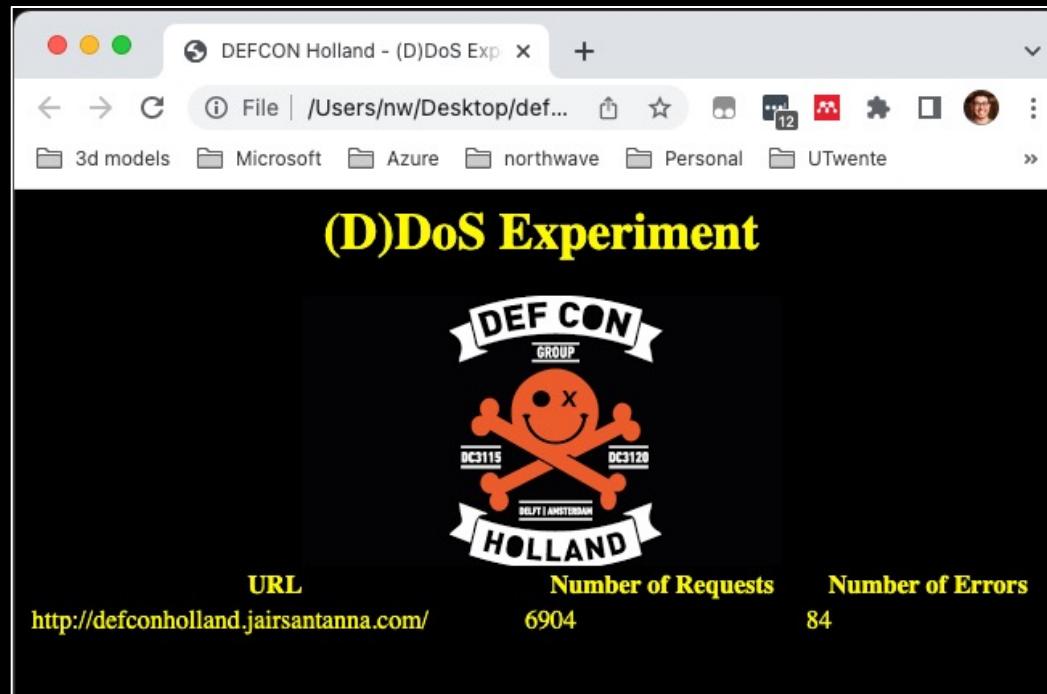
github.com/jjsantanna/defcon_holland_ddos

Improvising... “alternate applications”



Improvising... “alternate applications”

192.87.172.166:8888



“Alternate applications” for (D)DoS

The screenshot shows a GitHub repository page for 'jjsantanna/Denial-of-Service-DOS-Tools-Script-Kiddies'. The repository is public and contains 30 commits from Jair Santanna. The README.md file is visible, containing a section titled 'List of Denial of Service (DoS) Tools' which discusses the collection of DoS tools for script kiddies. The repository has 1 star, 1 watching, and 0 forks. It is written in Python.

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master 1 branch 0 tags

Jair Santanna new dos tools 757792e on 15 Nov 2021 30 commits

tools new dos tools 5 months ago

README.md Update README.md 5 months ago

About

Analysis of Denial of Service (DoS) Tools

Readme 1 star 1 watching 0 forks

Releases

No releases published Create a new release

Packages

No packages published Publish your first package

Languages

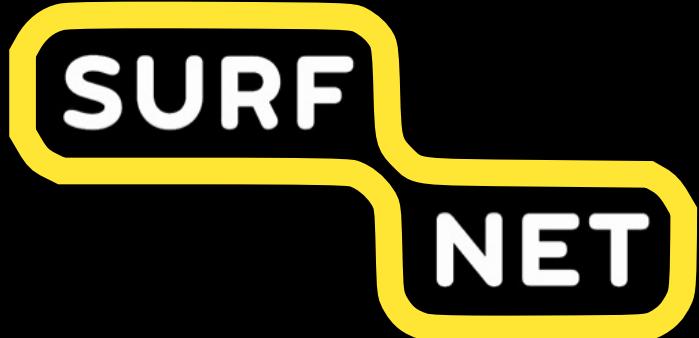
Python 100.0%

Name		Link
AnonCannon JavaScript Attack	.jar	sourceforge

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

MY STORY IN NL
&
BOOTERS

2013



Online Exams!



Let me Google for you... booter or stresser

A screenshot of a Google search results page on a Mac OS X interface. The search bar at the top contains the query "booter". Below the search bar, the "All" tab is selected, along with other options like Images, Videos, Shopping, News, More, Settings, and Tools. The search results indicate approximately 1,590,000 results found in 0.48 seconds. The first result is a link to "Booter - Wikipedia" with a snippet about PC booters and tools. The second result is "Str3ssed Booter - Best IP Booter / IP Stresser - 3 Years running!" with a snippet about its long-running nature and power. The third result is "What Are Booter Services? Webopedia Definition" with a snippet about DDoS services. The fourth result is "Booter.pw - Best Booter/Stresser | DDoS Attack Tools | TOP 1 L4/L7" with a snippet about its role in server stress testing.

booter

All Images Videos Shopping News More Settings Tools

About 1.590.000 results (0,48 seconds)

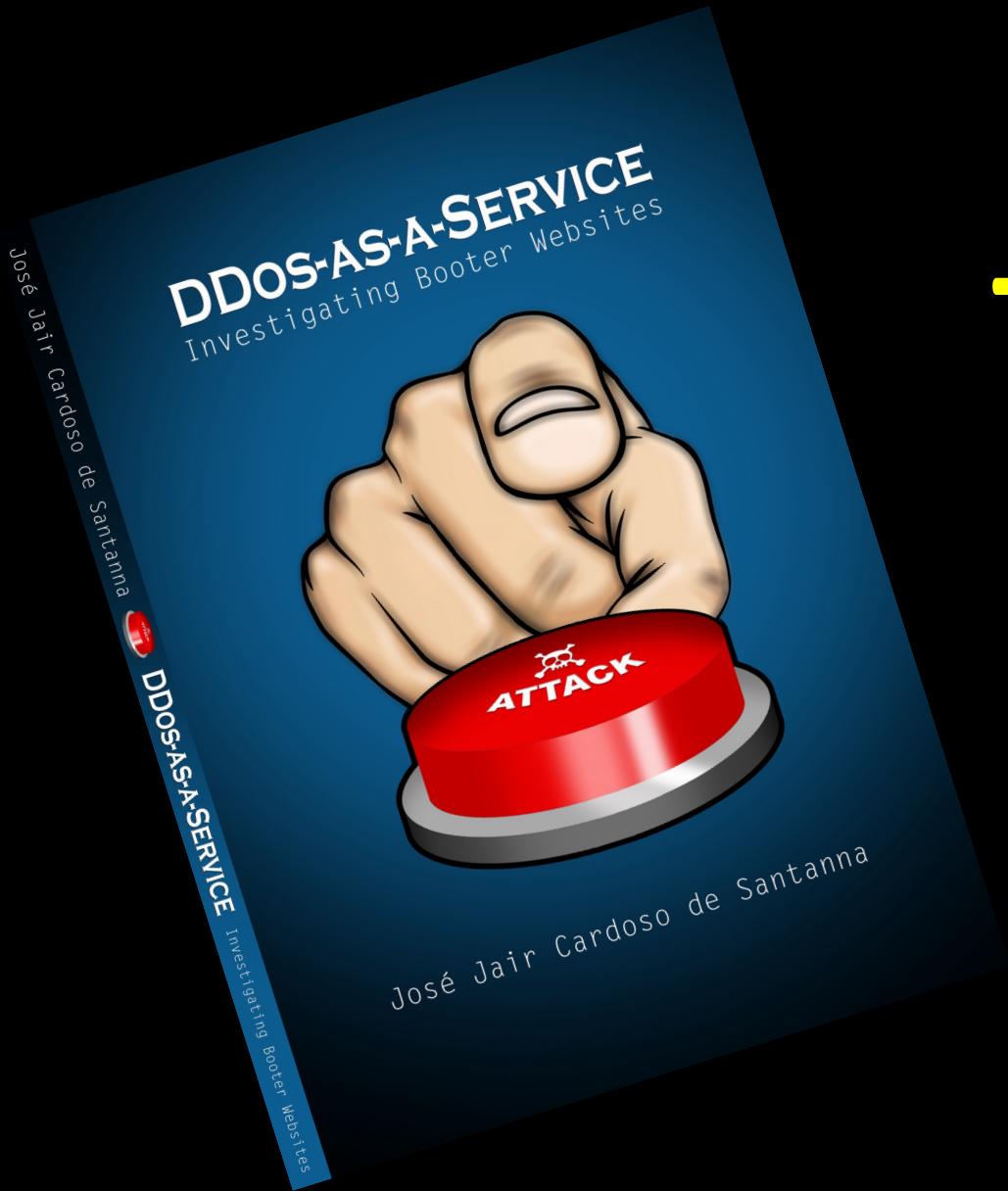
Booter - Wikipedia
<https://en.wikipedia.org/wiki/Booter> ▾
Booter may refer to: PC booter, software loaded directly at the bootup of a computer, without the help of an operating system; Booter, a tool for performing a ...

Str3ssed Booter - Best IP Booter / IP Stresser - 3 Years running!
<https://str3ssed.me/> ▾
Str3ssed Booter is hard hitting strongest ip stresser / booter on the booter market. Longest running booter with consistent network power of 250Gbps.
Sign Up · Login · TOS · Skype resolver

What Are Booter Services? Webopedia Definition
https://www.webopedia.com/TERM/B/booter_services.html ▾
A service offered by cyber criminals that provides paying customers with distributed denial of service (DDoS) attack capabilities on demand. According to this article on eWeek, Booter services, or Booters, are "Web-based services that do DDoS for hire at very low prices and are ..."

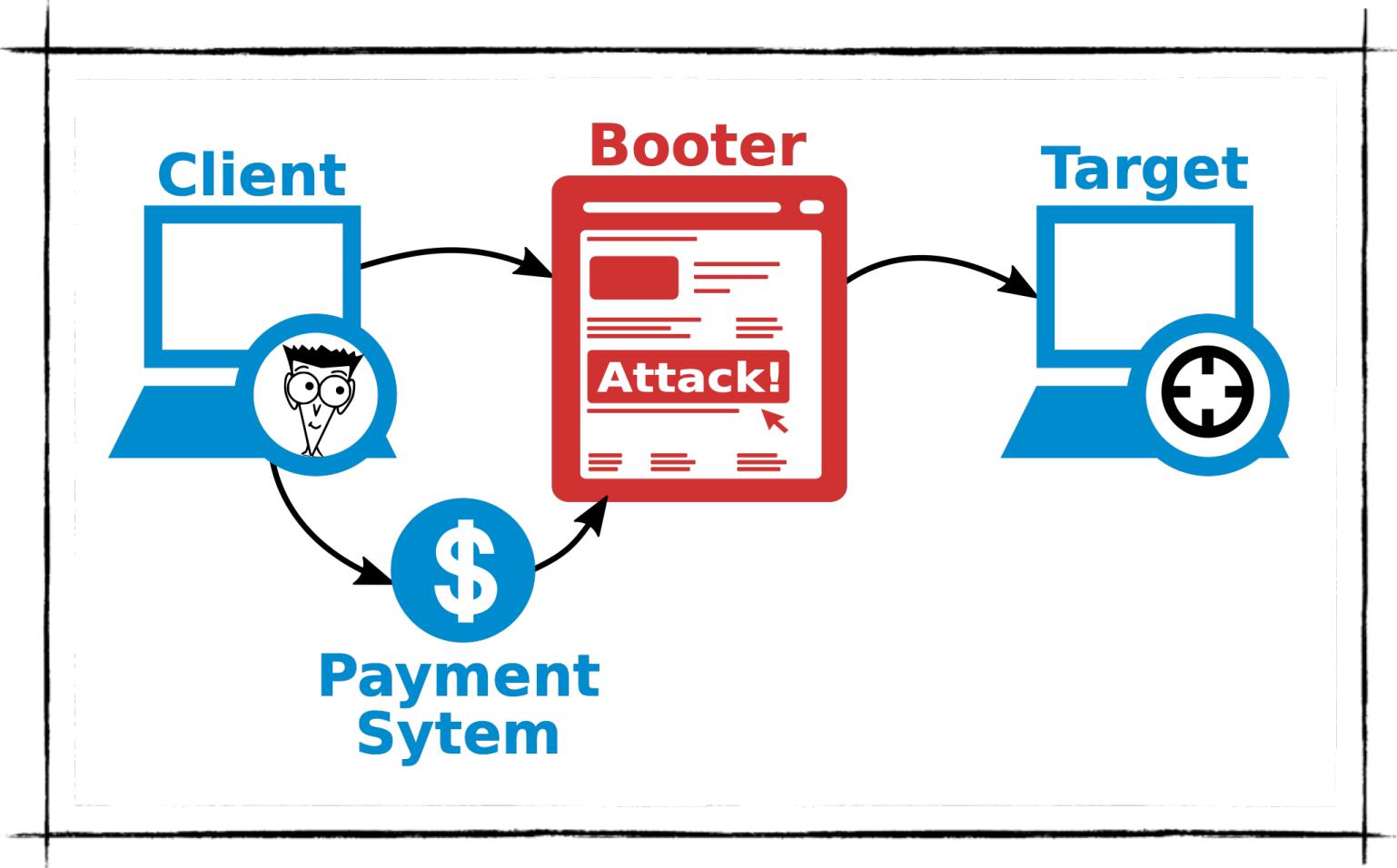
Booter.pw - Best Booter/Stresser | DDoS Attack Tools | TOP 1 L4/L7
<https://booter.pw/> ▾
Booter.pw is the best Booter/Stresser leading in the Server Stress Testing with hard hitting attacks.
Booter.pw is the best Booter/Stresser on the market.

My PhD thesis

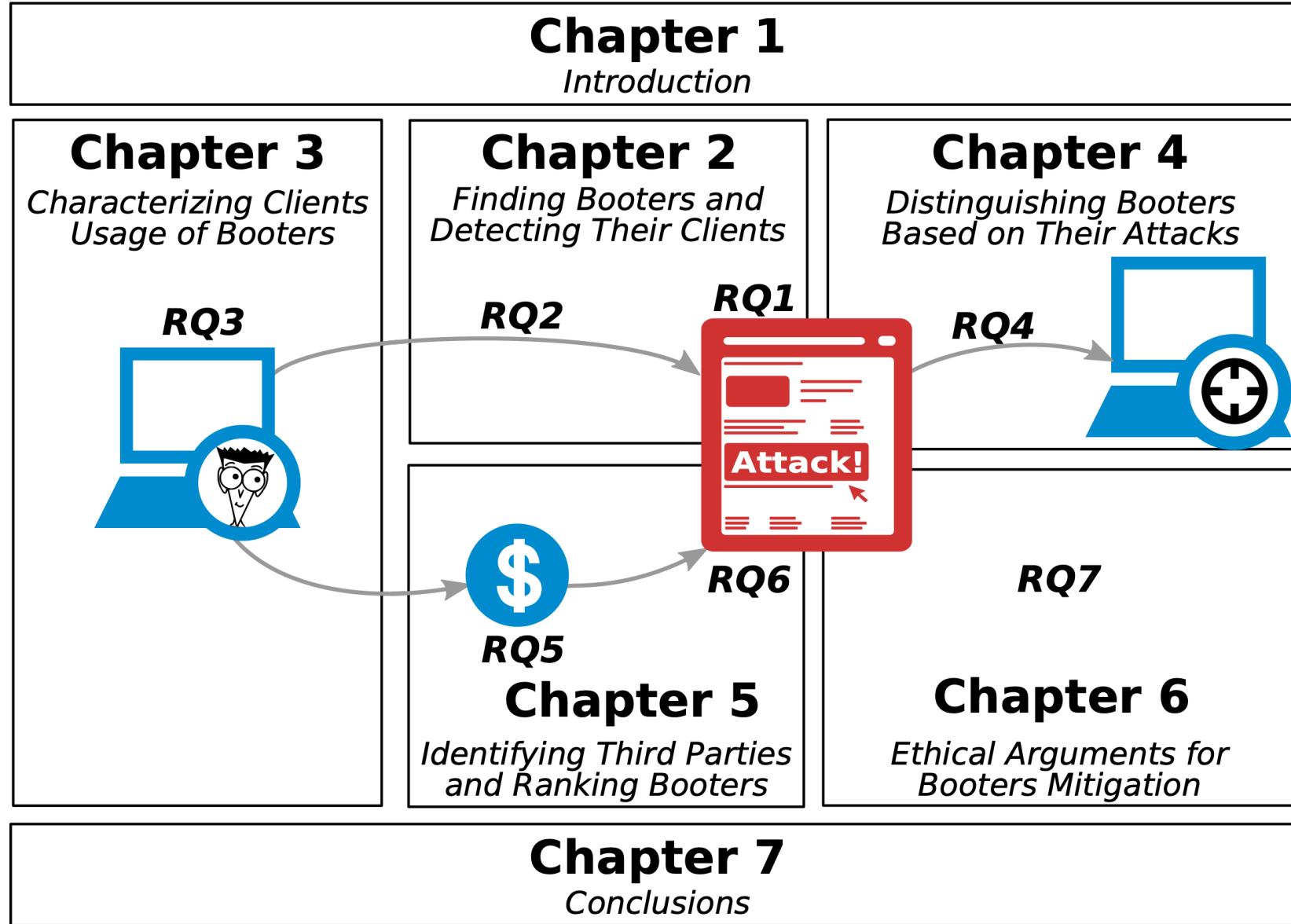


7 CHAPTERS
bit.ly/jjsantanna_thesis
FOR FREE!

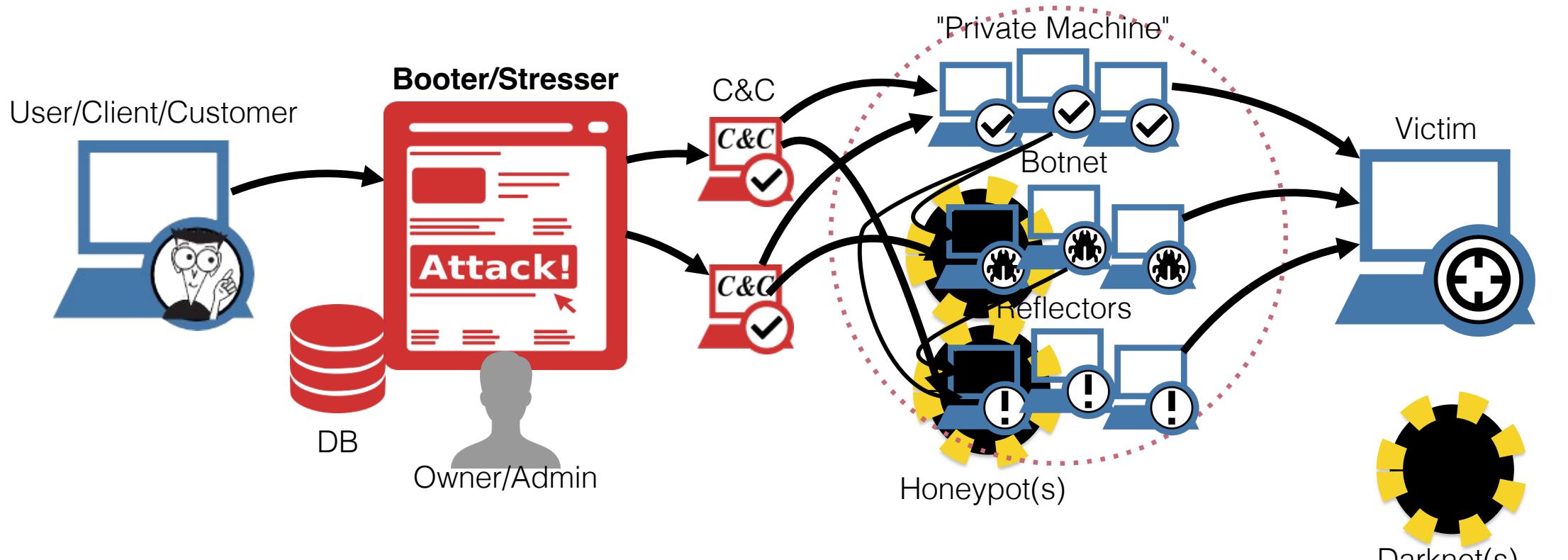
Chapter 1



Chapter 1



Conclusion



Payment Service



Web-Hosting



Netw. Opera.



Whois Privacy



CBSP



Registrar



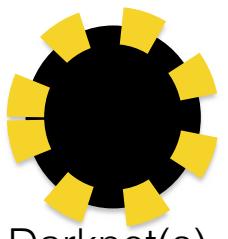
Search Engines



Law Enforcement Agencies

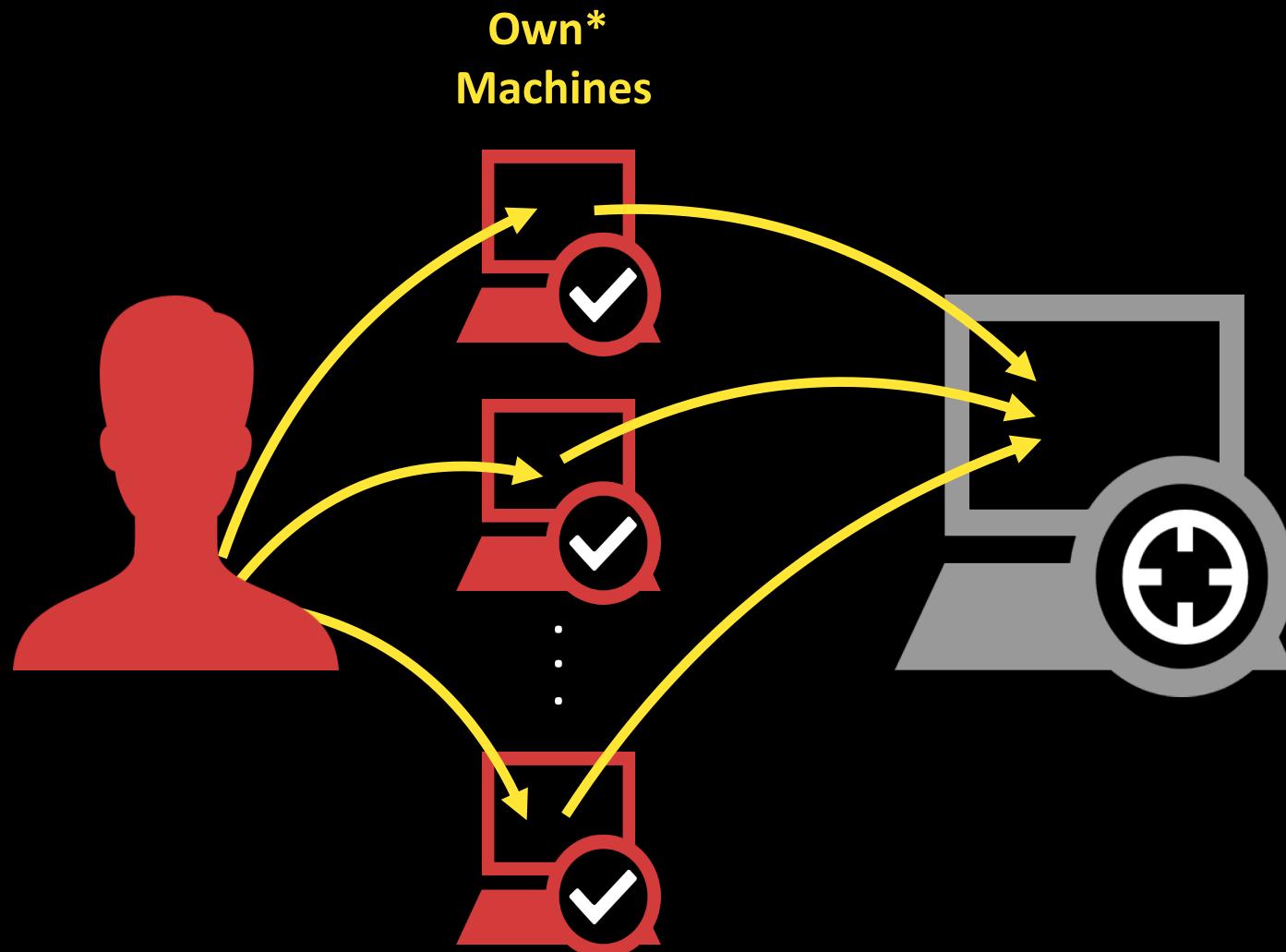


Legislators +
Judges

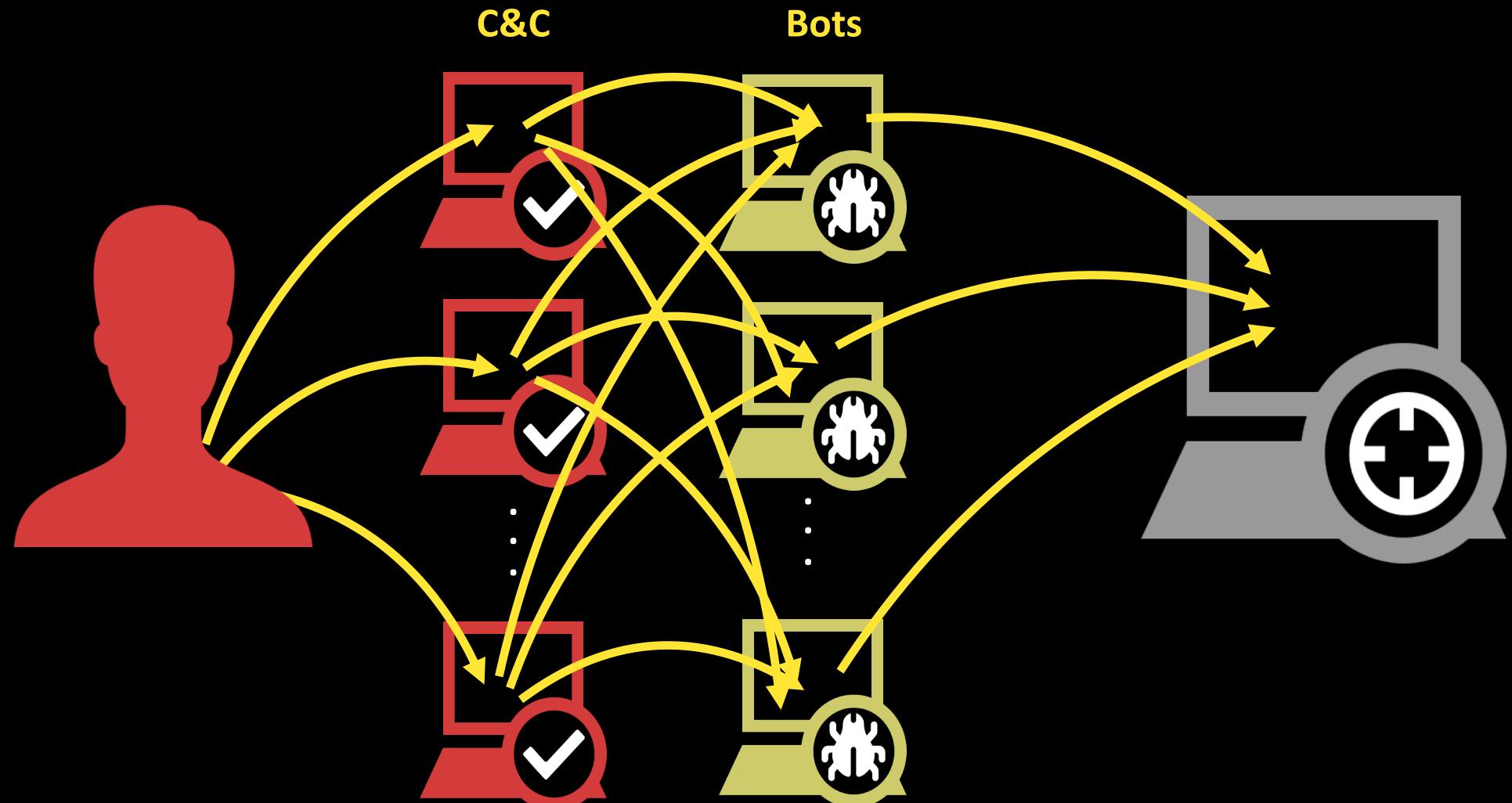


Darknet(s)

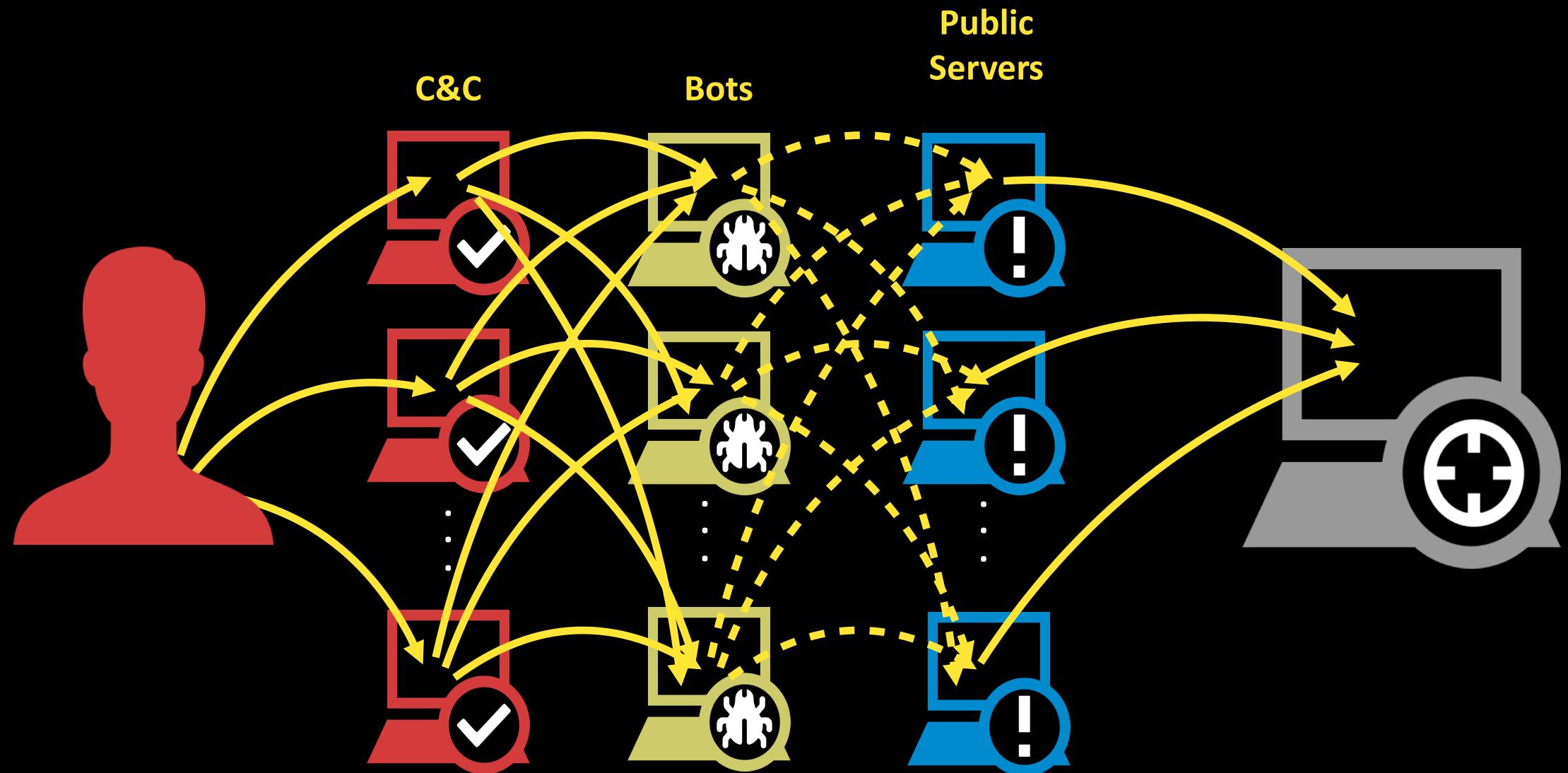
Infrastructure - Case 1



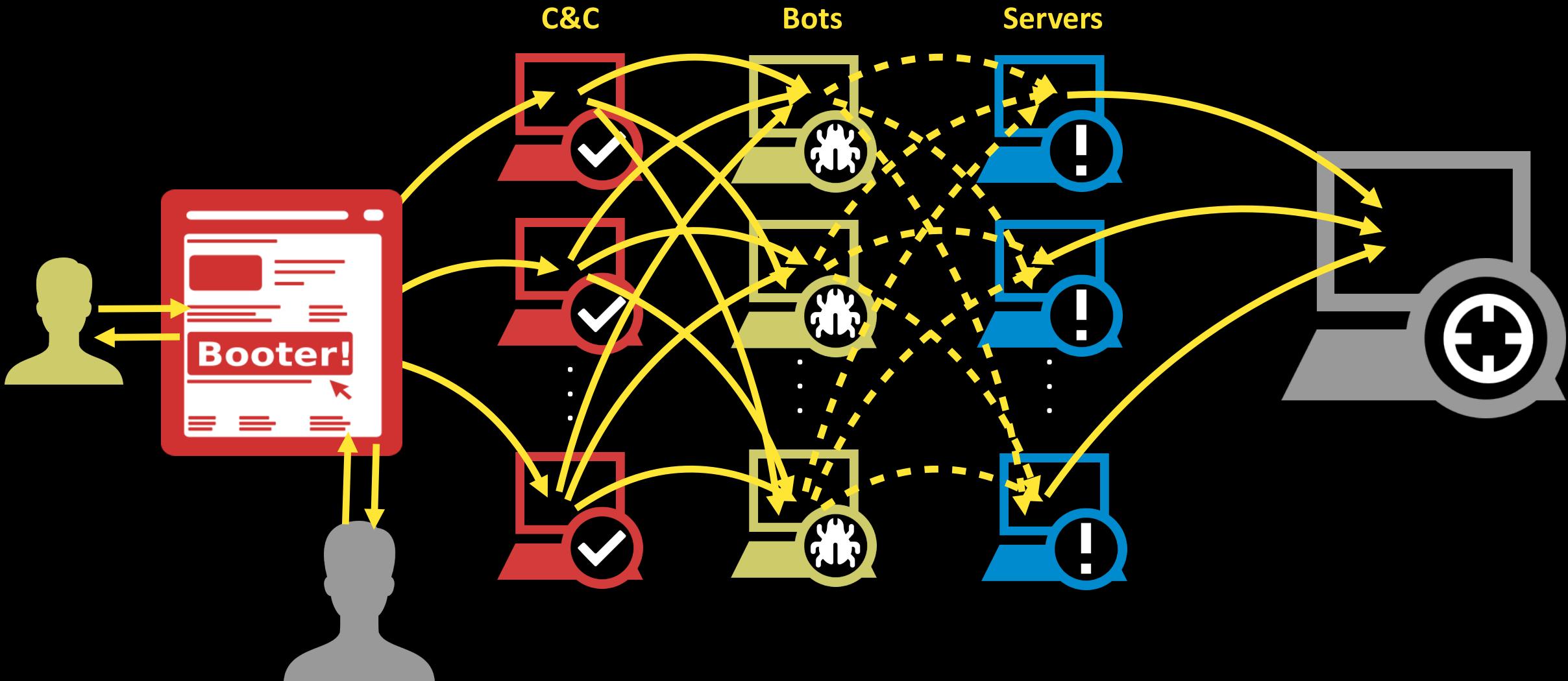
Infrastructure - Case 2



Infrastructure - Case 3



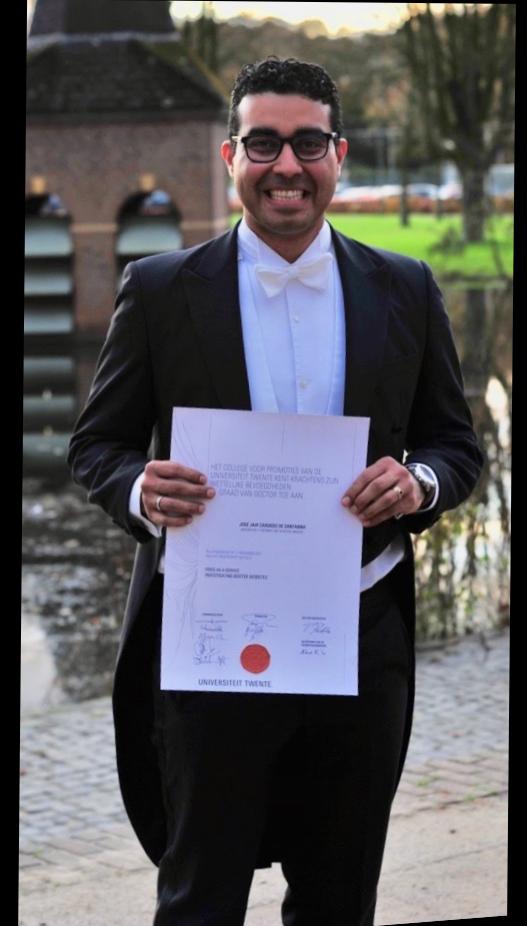
Infrastructure - Case 4



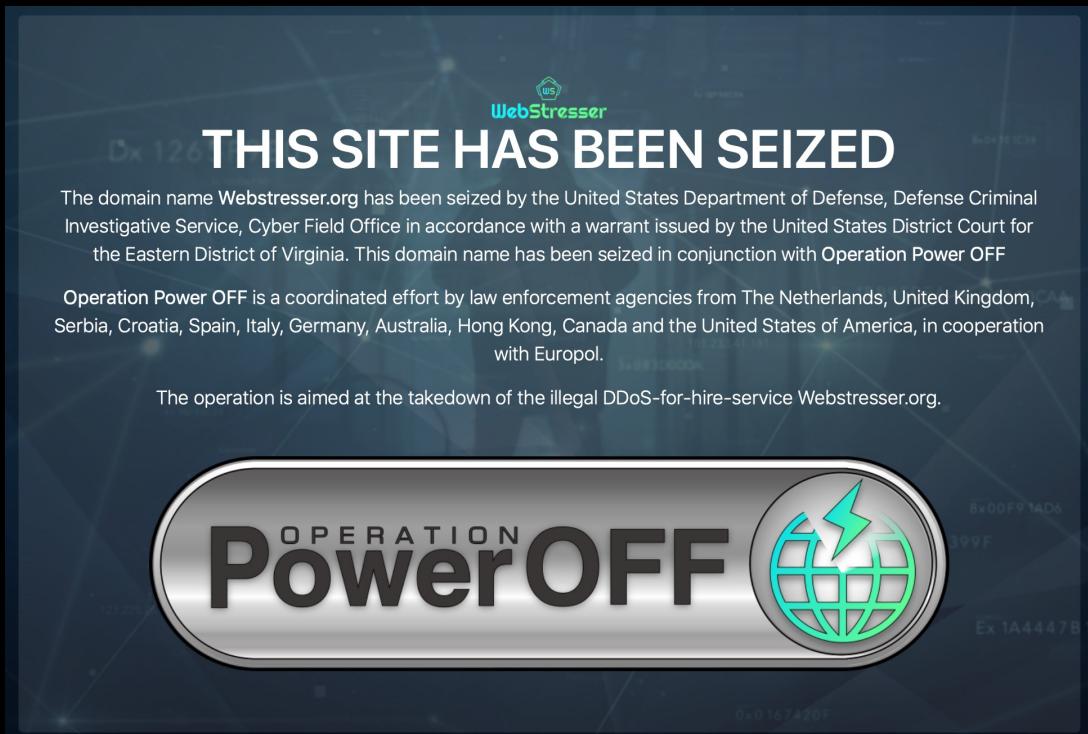
[Akamai, 2017]

"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

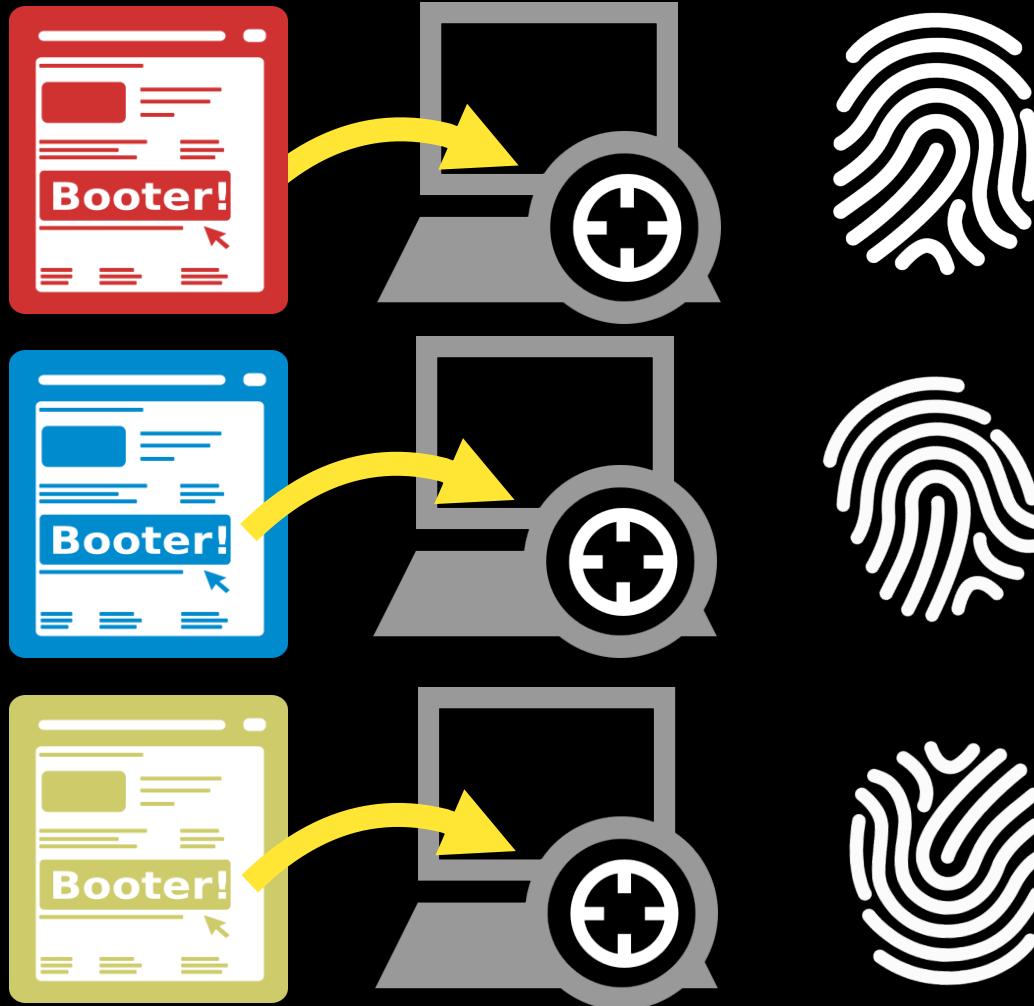
downthem.org
layer7-stresser.xyz
netstress.org
quantumstress.net
ragebooter.com
ragebooter.net

str3ssed.me
torsecurityteam.org
vbooter.org
request.rip

PART III

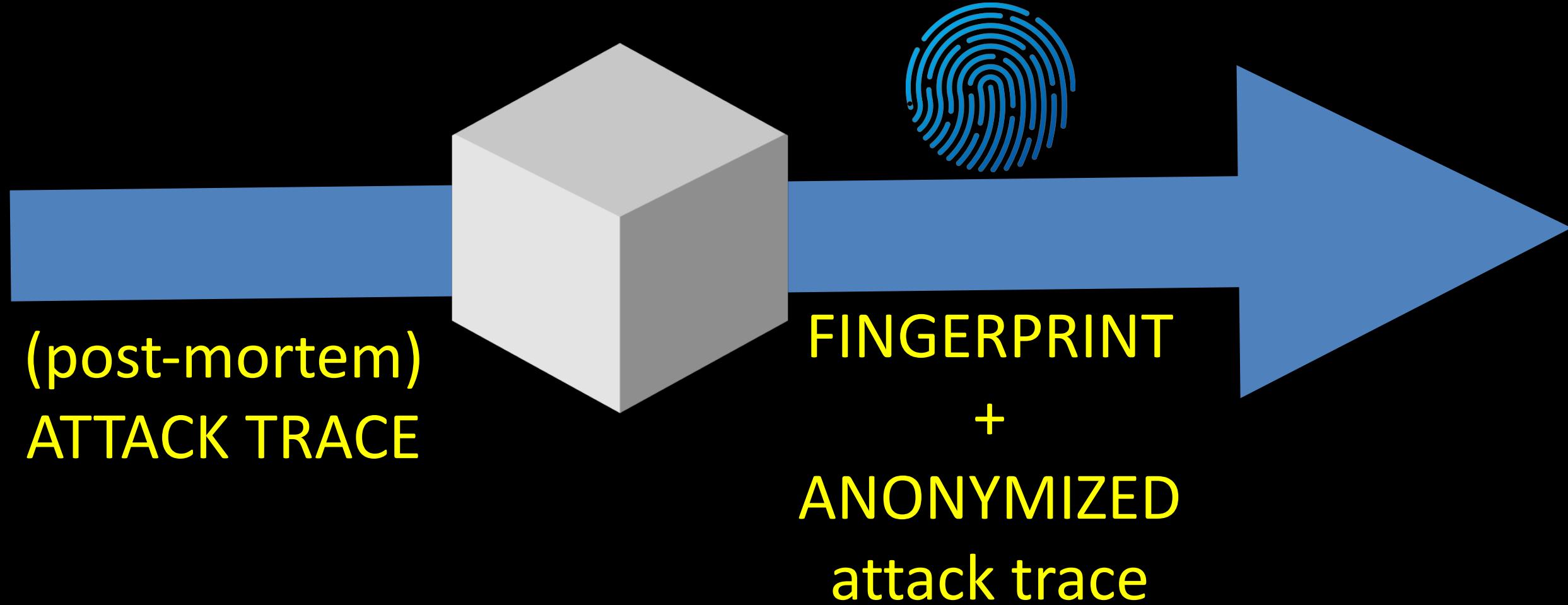
WHAT ELSE?

The need for fingerprinting



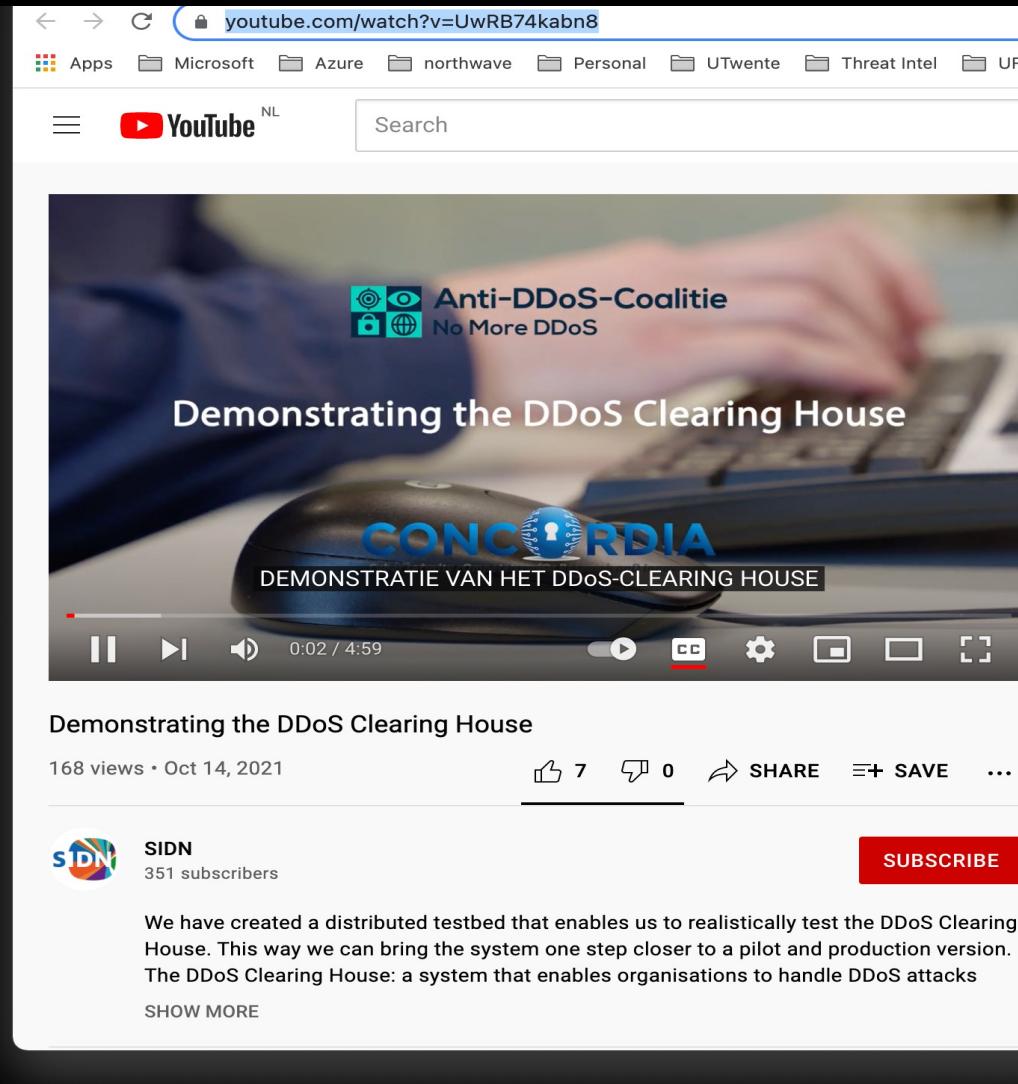
UNIQUE?!

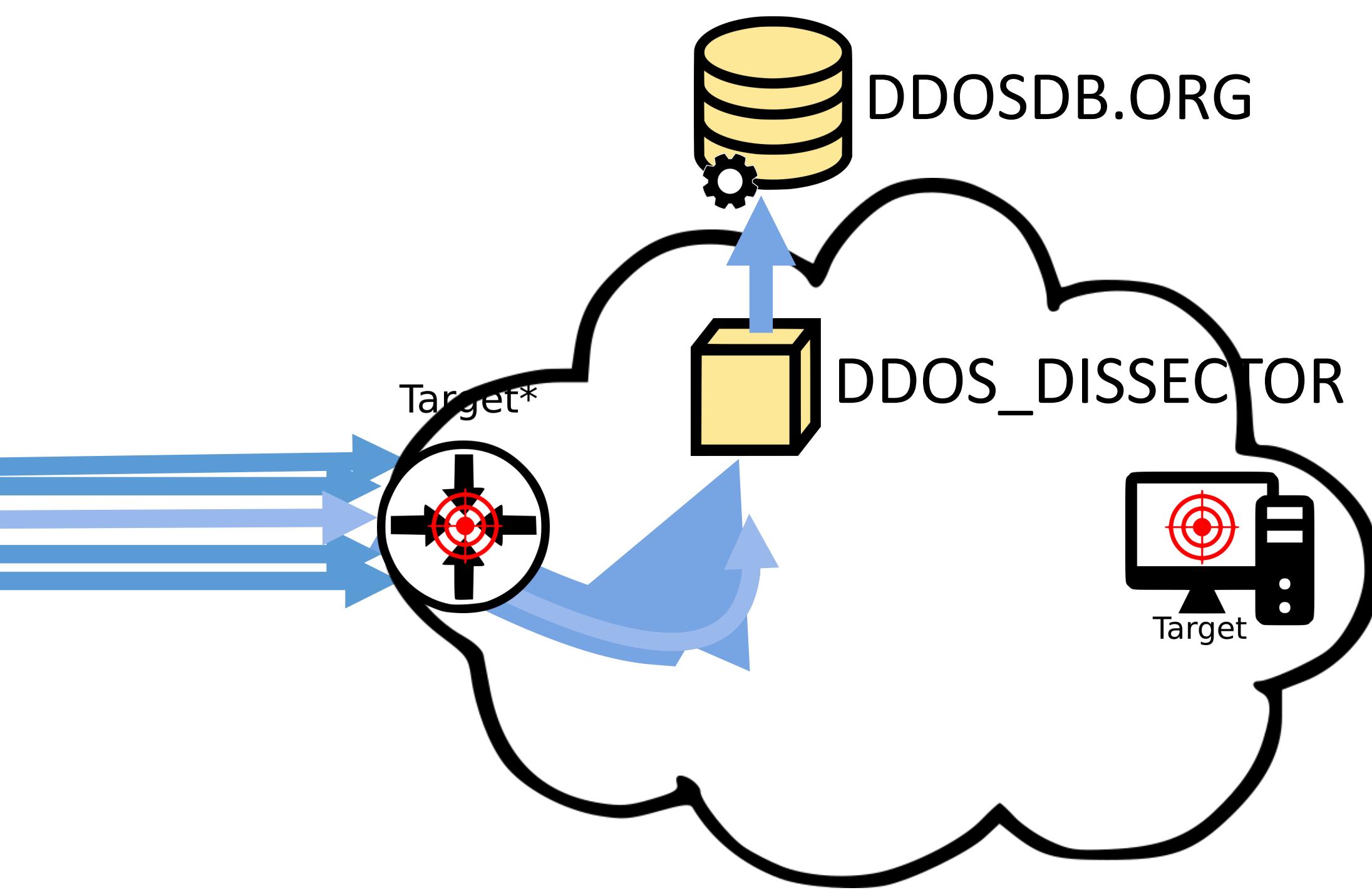
DDoS Dissector + DDoSDB + DDoS Fingerprint converters

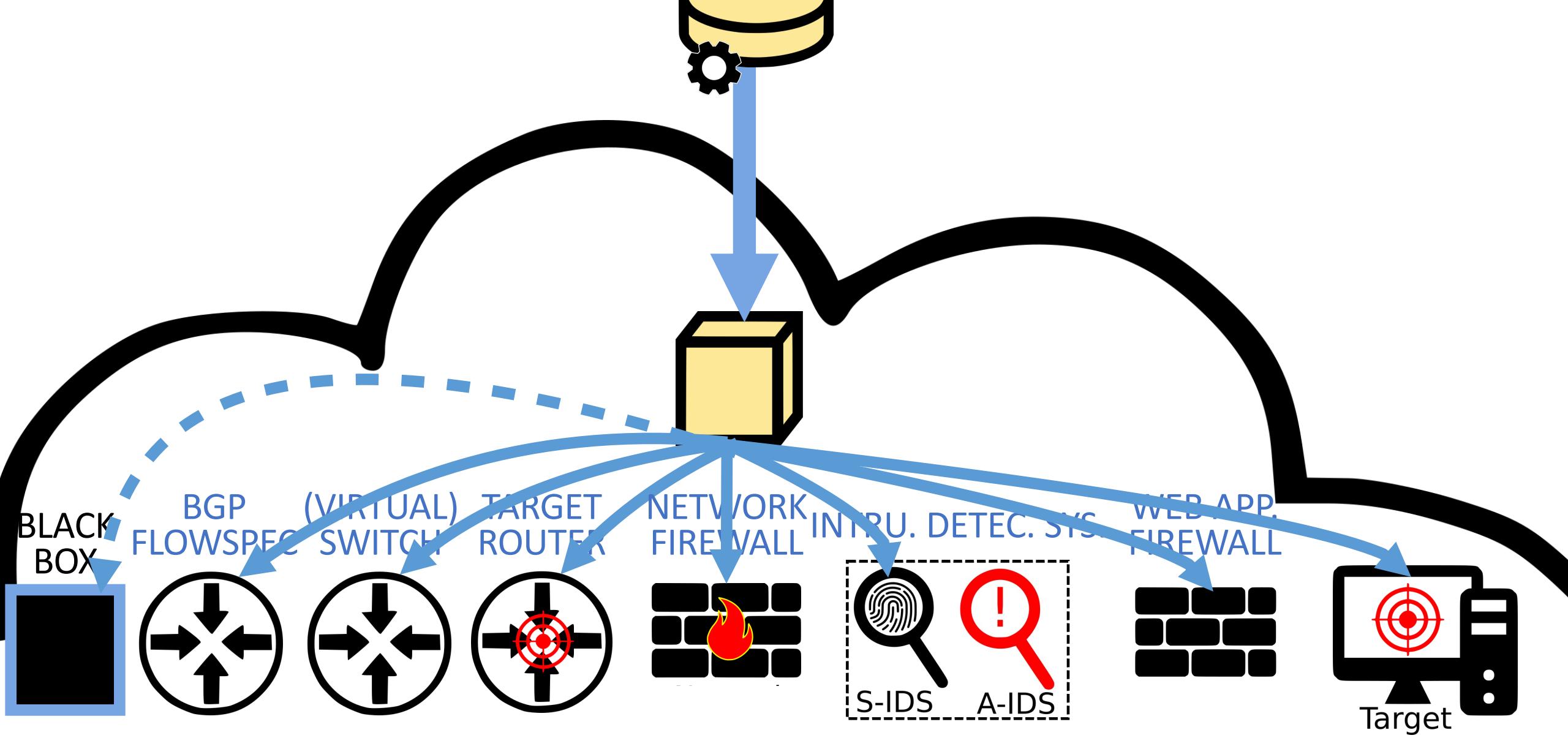


DDoS Dissector + DDoS Fingerprint converters

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







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

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



<https://ddosdb.ю/>



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



<https://www.nomoreddos.org/>



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

A screenshot of a GitHub repository page for "DDoS Clearing House". The repository has 10 repositories, 12 people, 3 teams, and 0 projects. It includes pinned repositories for "ddos_dissector", "ddosdb", and "converters", and a repository for "testbed". The "ddosdb" repository is described as a "DDoSDB repository". The "converters" repository is described as "Converters: fingerprints to mitigation tools rules". The "testbed" repository is described as a "Distributed testbed to test the DDoS Clearing House on". The "Top languages" section shows Python, JavaScript, and TeX. On the right, there is a "People" section showing profile pictures of team members and an "Invite someone" button.

<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]