

# SOLVING DDOOS ATTACKS IN THE NETHERLANDS, EUROPE, AND BEYOND

---

FACILITATING BRIDGING SOLUTIONS AND STAKEHOLDERS

# DDOOS CLEARING HOUSE

# SOLVING DDoS ATTACKS

---

**Koen van Hove**

**Researcher at the University of Twente**

**THE PROBLEM AND OUR IDEA**







scholar.google.nl

ddos attack

Scholar About 46,800 results (Sorted by relevance)

YEAR

**A taxonomy of DDoS attack and DDoS defense mechanisms** [PDF] psu.edu

[J Mirkovic, P Reiher](#) - ACM SIGCOMM Computer Communication ..., 2004 - dl.acm.org

Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper presents two taxonomies for classifying attacks and defenses, and thus provides researchers with a better ...

☆ Cited by 1913 Related articles All 51 versions

**Statistical approaches to DDoS attack detection and response** [PDF] uccs.edu

[L Feinstein, D Schnackenberg](#)... - Proceedings DARPA ..., 2003 - ieeexplore.ieee.org

The nature of the threats posed by distributed denial of service (DDoS) attacks on large networks, such as the Internet, demands effective detection and response methods. These methods must be deployed not only at the edge but also at the core of the network This ...

☆ Cited by 618 Related articles All 12 versions

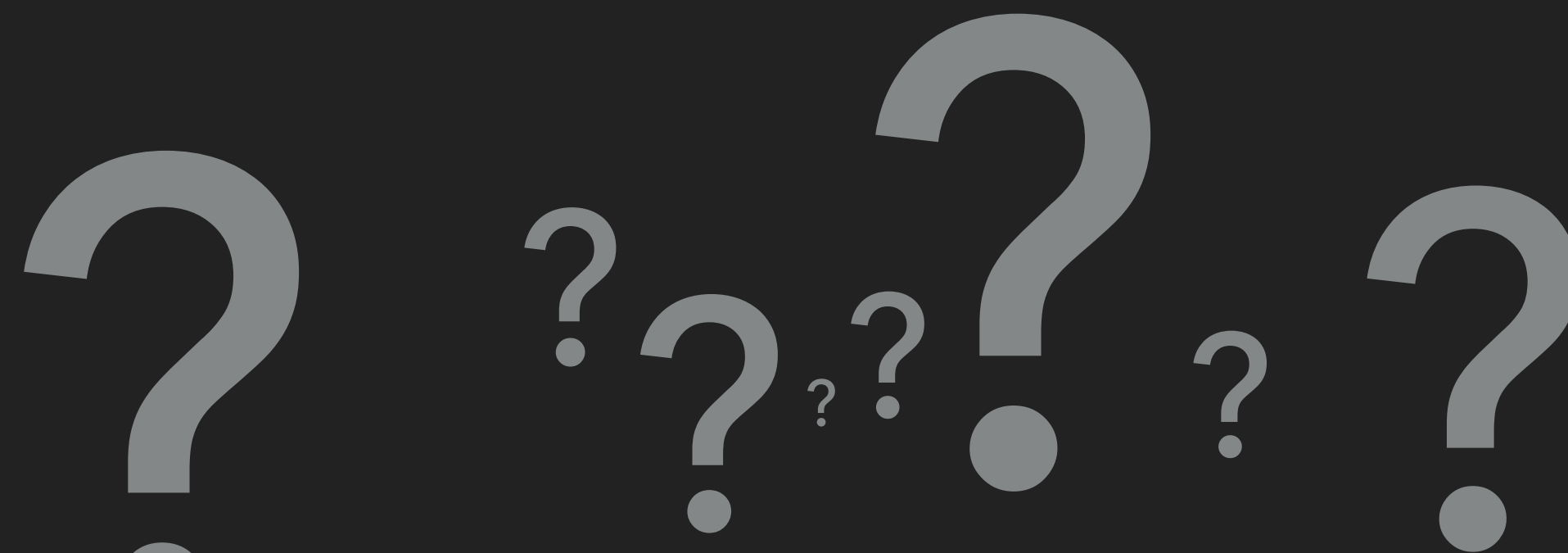
**Lightweight DDoS flooding attack detection using NOX/OpenFlow** [PDF] researchgate.net

[R Braga, E Mota, A Passito](#) - IEEE Local Computer Network ..., 2010 - computer.org

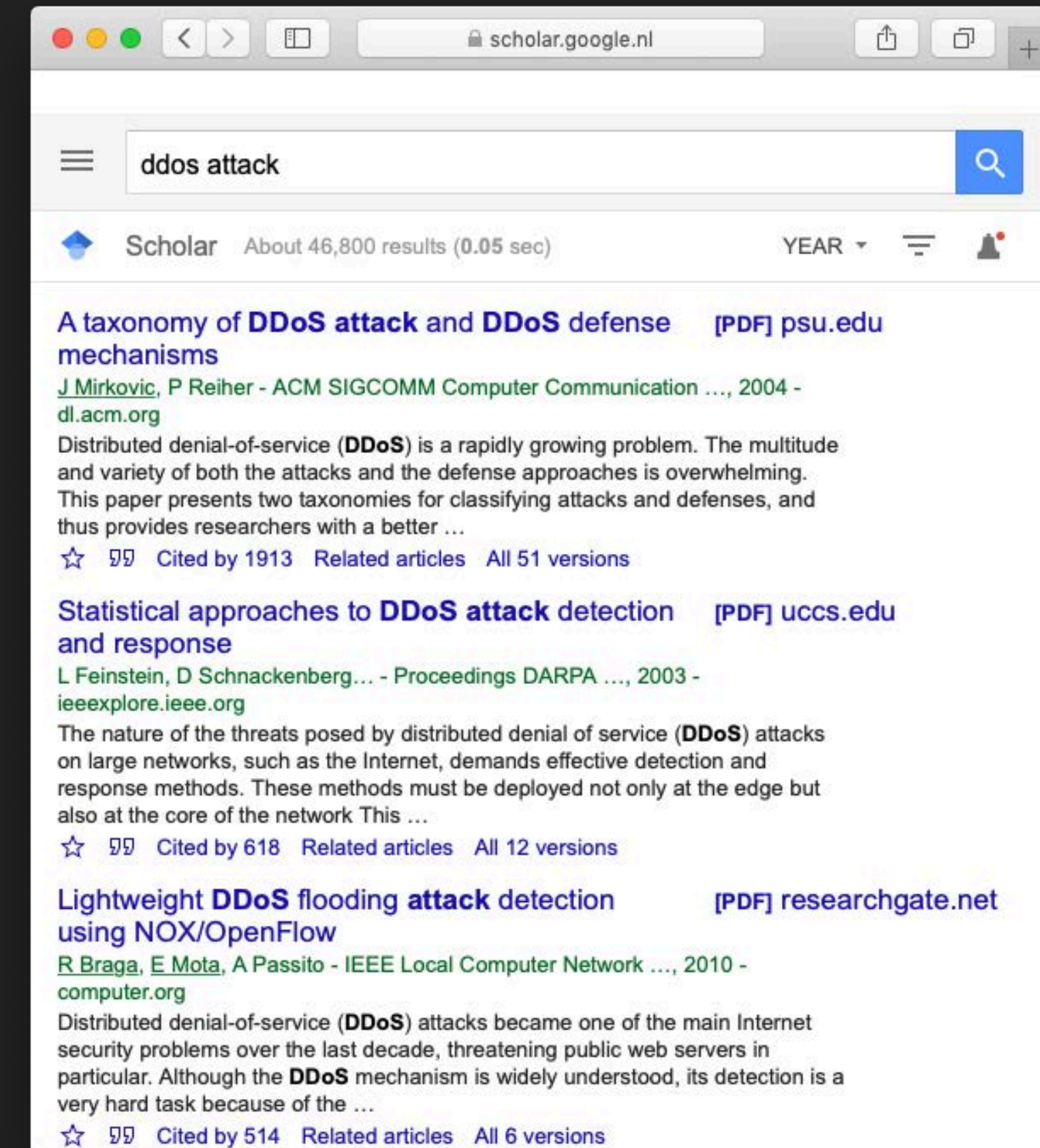
Distributed denial-of-service (DDoS) attacks became one of the main Internet security problems over the last decade, threatening public web servers in particular. Although the DDoS mechanism is widely understood, its detection is a very hard task because of the ...

☆ Cited by 514 Related articles All 6 versions



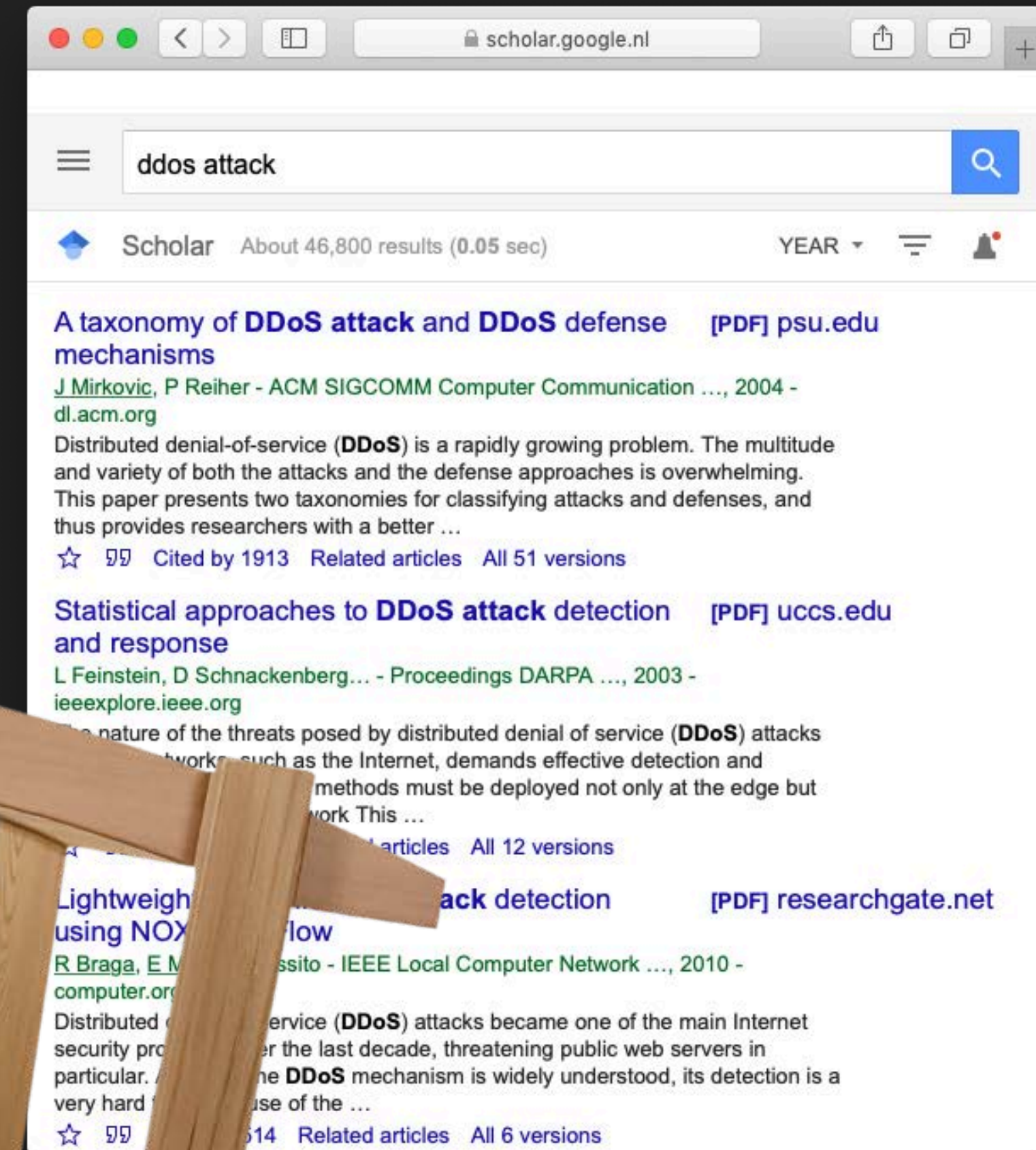


# WHY DOES DDOS STILL EXIST?





# SOLVING DDOS ATTACKS





# SOLVING DDOS ATTACKS

DDOS  
PROTECTION  
PROVIDERS

ACADEMIA





**VICTIMS**

**DDOS  
PROTECTION  
PROVIDERS**

**NETWORK  
OPERATORS  
+  
CERT/CSIRT**

**LAW  
ENFORCEMENT  
AGENCIES**

**ACADEMIA**



# DDOS CLEARING HOUSE





# DDOS CLEARING HOUSE



DB





## NETWORK MEASUREMENT

(PCAP, NET FLOW, IPFIX, SFLOW, LOGS, ...)



## DDOS\_DISSECTOR

INPUT: NETWORK MEASUREMENT

OUTPUT: DDOS FINGERPRINT (+\*NOTES)

FILTERED & ANONYMIZED NETWORK MEASUREMENTS



## DDOS\_FINGERPRINT\_CONVERTERS

INPUT: DDOS FINGERPRINT

OUTPUT: RULE/SIGNATURE FOR SPECIFIC HW/SW SOLUTION(S)  
(SNORT, SURICATA, BRO, IPTABLES, EBPF, BGP FLOWSPEC, ...)



## DDOSDB

STORE, ENRICH, AND DISTRIBUTE DDOS ATTACK RELATED INFO



**VICTIMS**

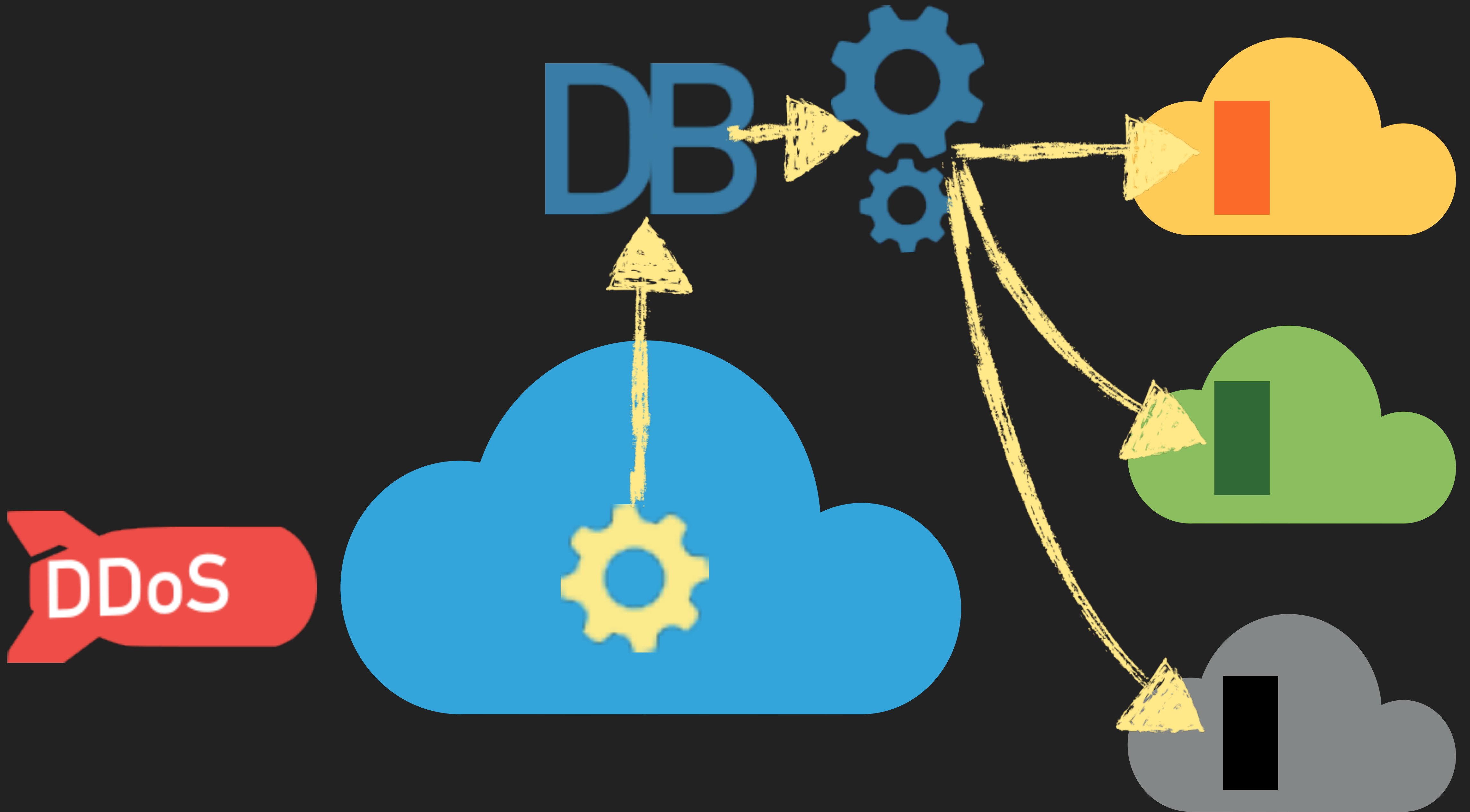
**DDOS  
PROTECTION  
PROVIDERS**

**NETWORK  
OPERATORS  
+  
CERT/CSIRT**

**LAW  
ENFORCEMENT  
AGENCIES**

**ACADEMIA**











**VICTIMS**



**DDOS  
PROTECTION  
PROVIDERS**



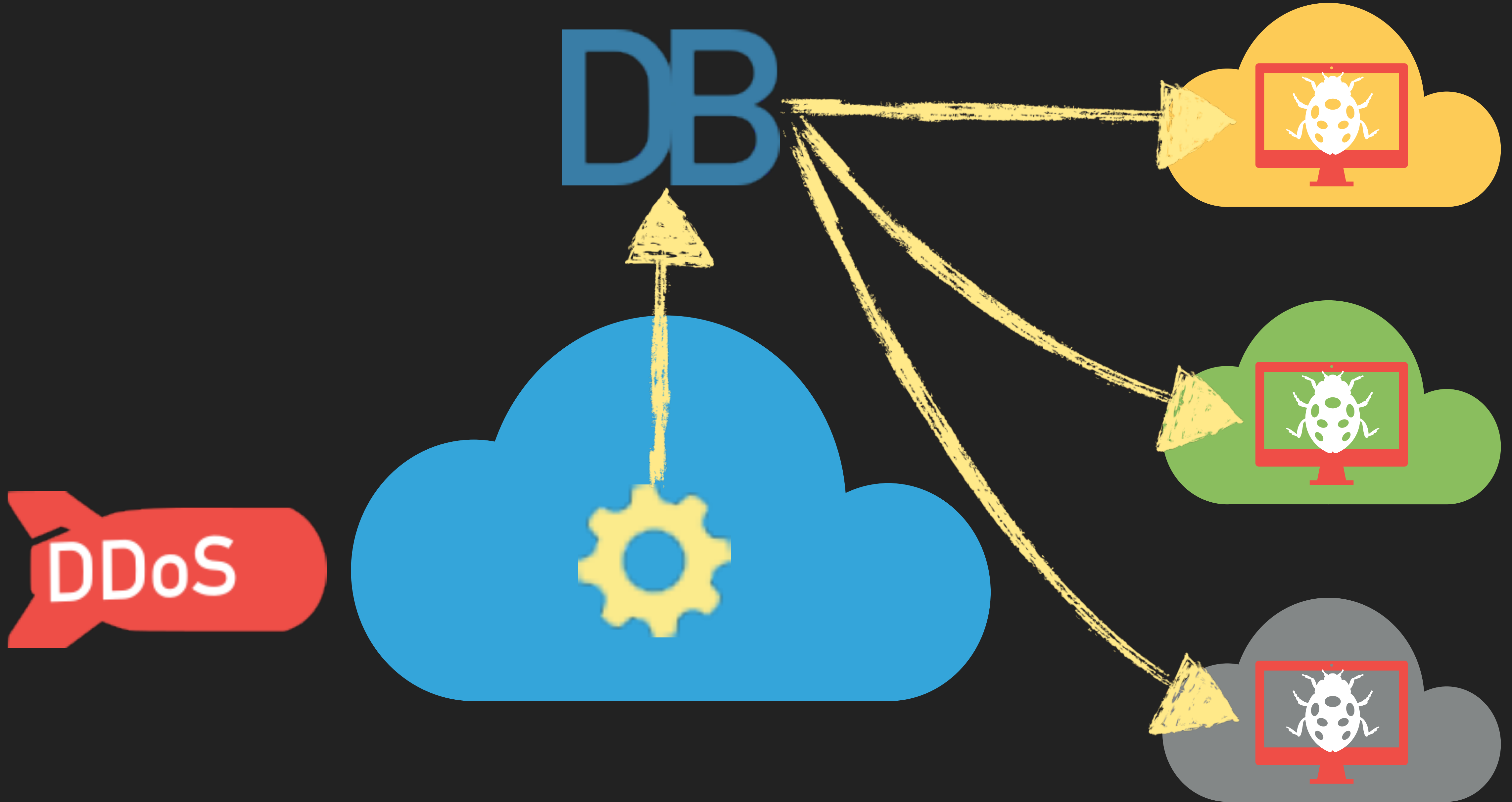
**NETWORK  
OPERATORS  
+  
CERT/CSIRT**

**LAW  
ENFORCEMENT  
AGENCIES**

**ACADEMIA**









VICTIMS



DDOS  
PROTECTION  
PROVIDERS

NETWORK  
OPERATORS  
+  
CERT/CSIRT



LAW  
ENFORCEMENT  
AGENCIES

ACADEMIA





DB





VICTIMS



DDOS  
PROTECTION  
PROVIDERS

NETWORK  
OPERATORS  
+  
CERT/CSIRT

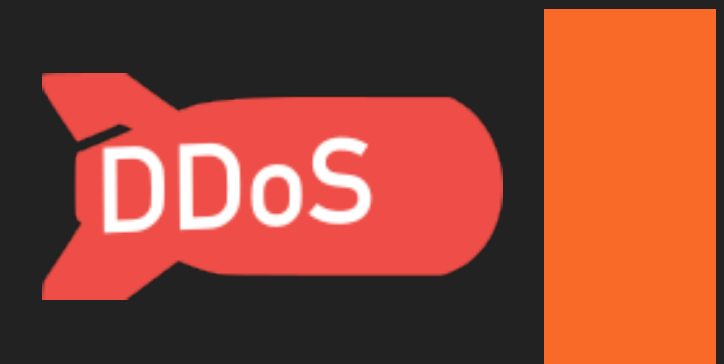


LAW  
ENFORCEMENT  
AGENCIES



ACADEMIA









VICTIMS



DDOS  
PROTECTION  
PROVIDERS

NETWORK  
OPERATORS  
+  
CERT/CSIRT



LAW  
ENFORCEMENT  
AGENCIES

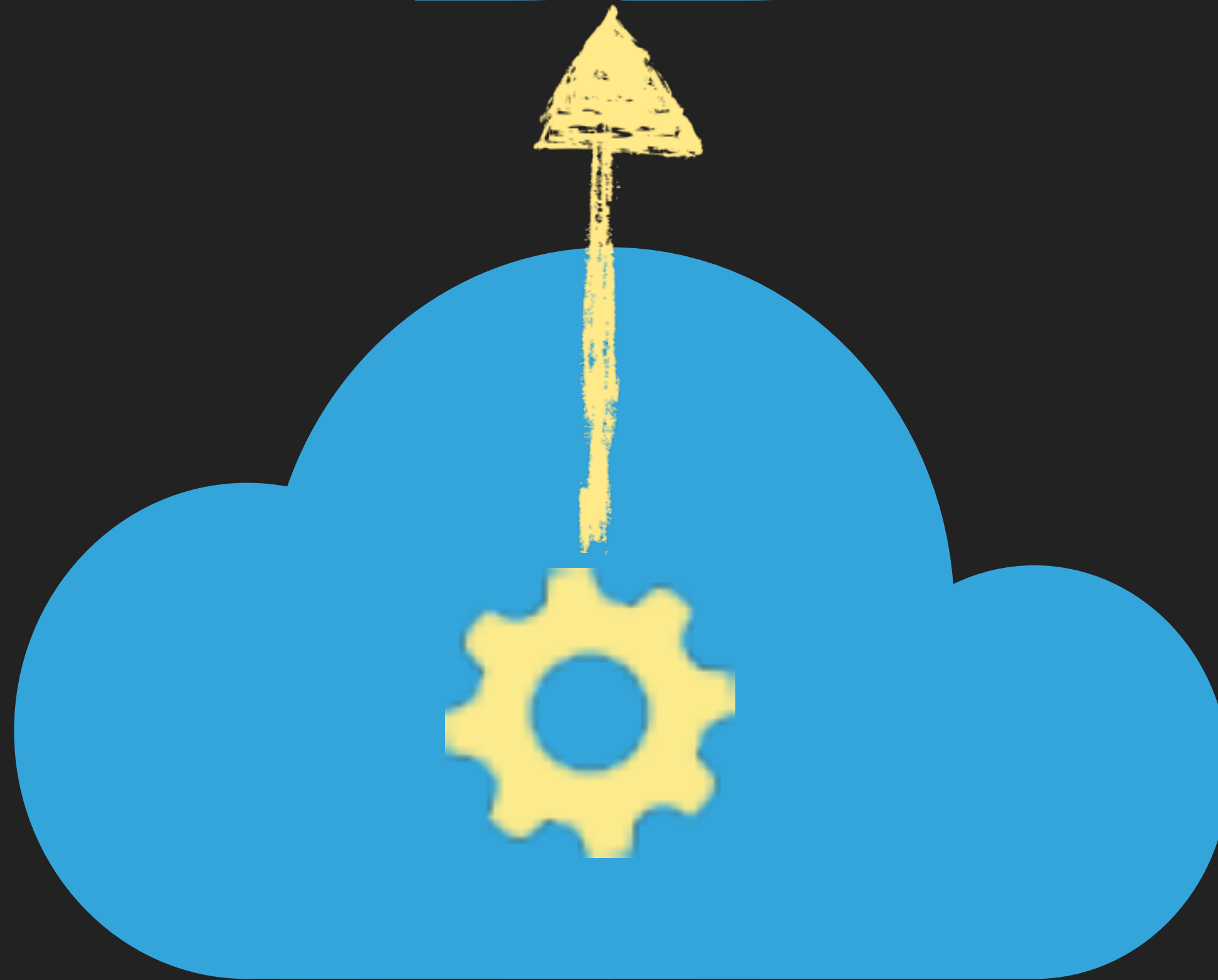


ACADEMIA



**ONE EXTRA ELEMENT...**

DB



DDOS OPEN THREAT SIGNALING (DOTS) [IETF]





**DDOS OPEN THREAT SIGNALING (DOTS) [IETF]**

**DEMO:**

**USING THE DDOOS DISSECTOR**

# DEMO: QUERYING DDOSDB



**[THE CURRENT]**

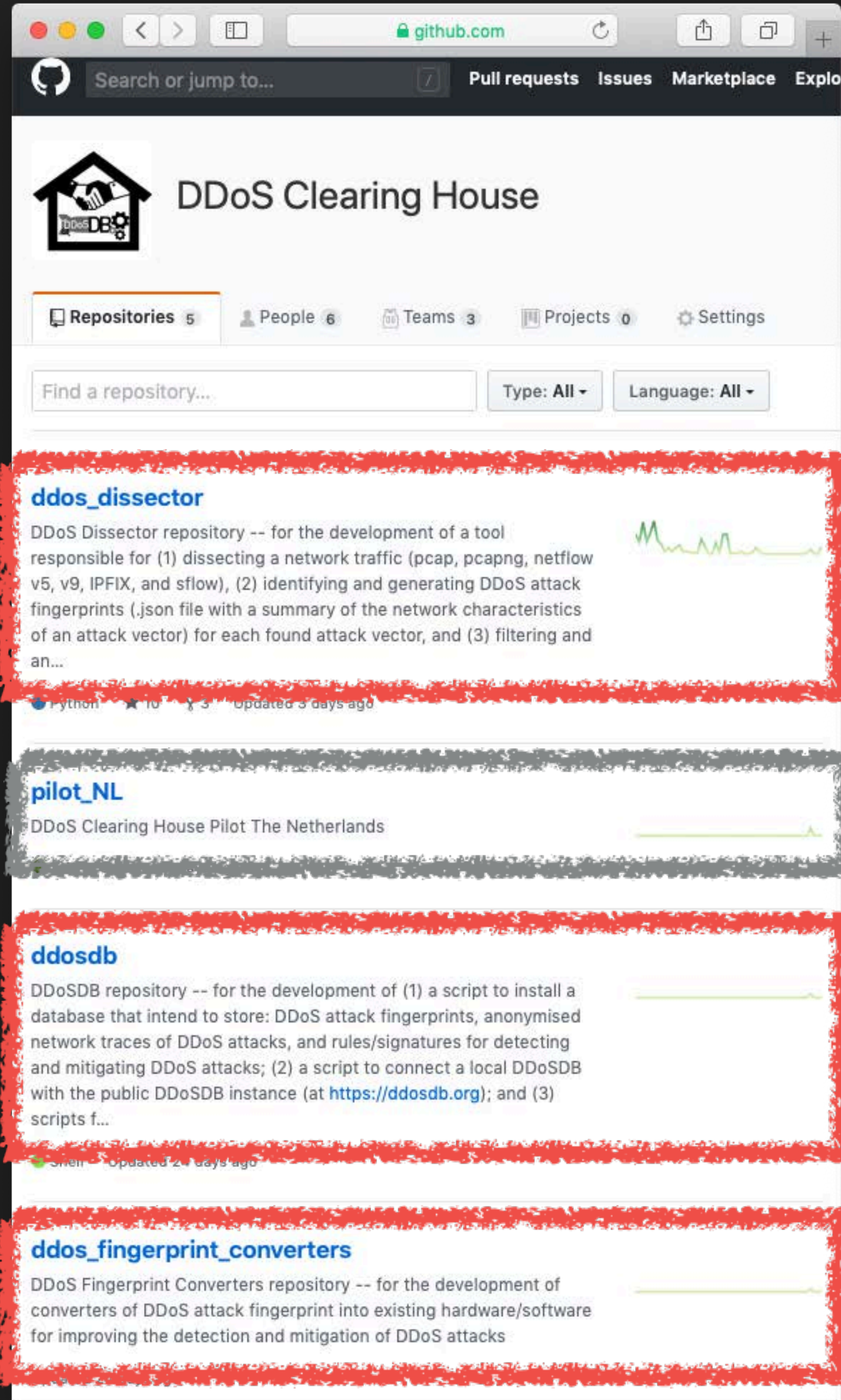
**DEPLOYMENT & GOVERNANCE**

# TIMELINE



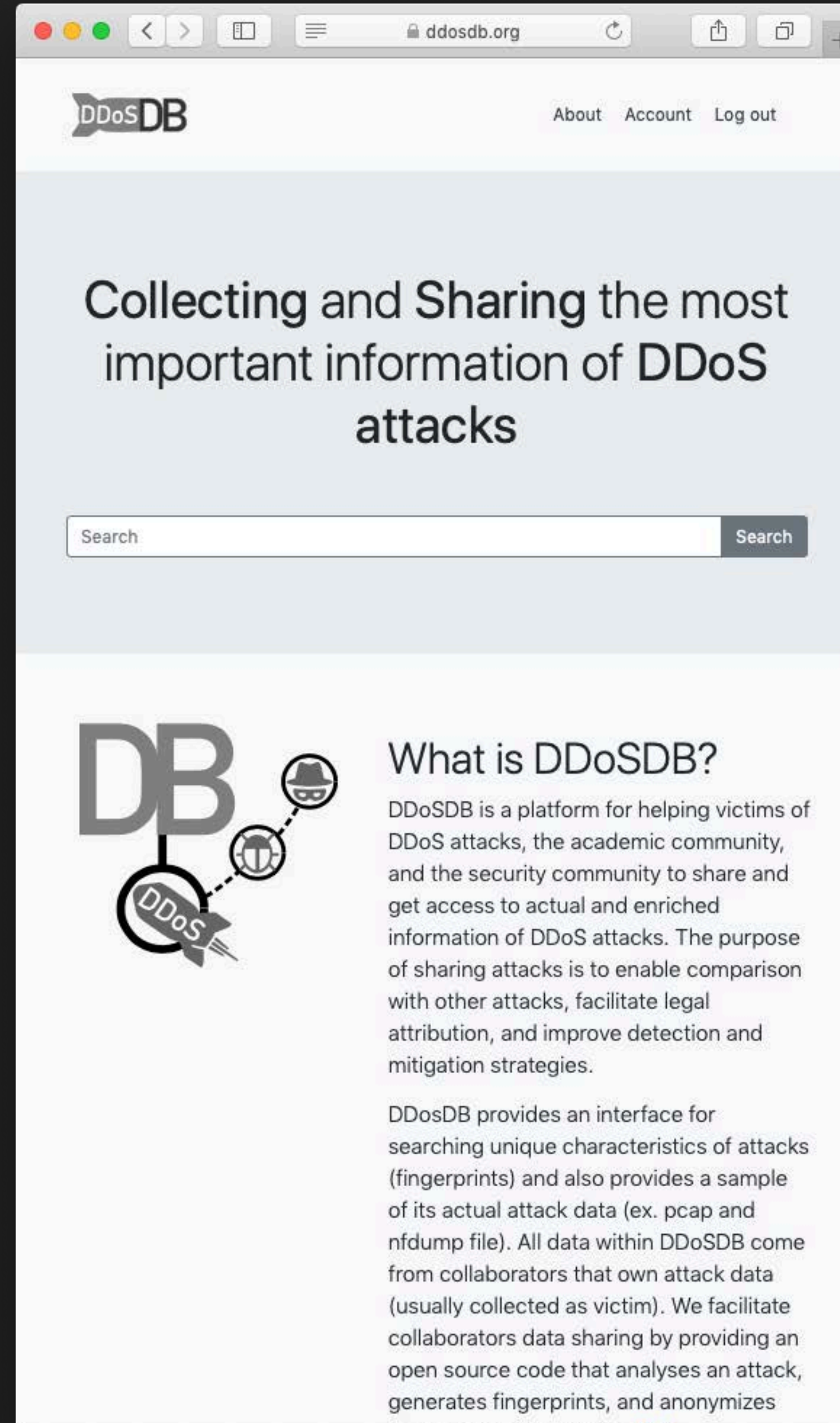


<https://github.com/ddos-clearing-house>



The screenshot shows the GitHub repository page for 'DDoS Clearing House'. The repository is highlighted with a red border. It is a Python repository with 10 stars and 3 forks, updated 3 days ago. The description states: 'DDoS Dissector repository -- for the development of a tool responsible for (1) dissecting a network traffic (pcap, pcapng, netflow v5, v9, IPFIX, and sflow), (2) identifying and generating DDoS attack fingerprints (.json file with a summary of the network characteristics of an attack vector) for each found attack vector, and (3) filtering and an...'. Below this, there are two more repositories listed: 'pilot\_NL' (DDoS Clearing House Pilot The Netherlands) and 'ddosdb' (DDoSDB repository -- for the development of (1) a script to install a database that intend to store: DDoS attack fingerprints, anonymised network traces of DDoS attacks, and rules/signatures for detecting and mitigating DDoS attacks; (2) a script to connect a local DDoSDB with the public DDoSDB instance (at <https://ddosdb.org>); and (3) scripts f...). The 'ddosdb' repository is also highlighted with a red border. At the bottom, there is a repository named 'ddos\_fingerprint\_converters' (DDoS Fingerprint Converters repository -- for the development of converters of DDoS attack fingerprint into existing hardware/software for improving the detection and mitigation of DDoS attacks), which is also highlighted with a red border.

<https://ddosdb.ORG>



The screenshot shows the homepage of the DDoSDB website. The header includes the DDoSDB logo and navigation links for 'About', 'Account', and 'Log out'. The main heading reads: 'Collecting and Sharing the most important information of DDoS attacks'. Below this is a search bar with the placeholder text 'Search'. The page features a large graphic on the left with the letters 'DB' and a magnifying glass over a 'DDoS' label, with a bug icon nearby. To the right of the graphic, the text 'What is DDoSDB?' is followed by a paragraph: 'DDoSDB is a platform for helping victims of DDoS attacks, the academic community, and the security community to share and get access to actual and enriched information of DDoS attacks. The purpose of sharing attacks is to enable comparison with other attacks, facilitate legal attribution, and improve detection and mitigation strategies.' Below this, another paragraph states: 'DDoSDB provides an interface for searching unique characteristics of attacks (fingerprints) and also provides a sample of its actual attack data (ex. pcap and nfdump file). All data within DDoSDB come from collaborators that own attack data (usually collected as victim). We facilitate collaborators data sharing by providing an open source code that analyses an attack, generates fingerprints, and anonymizes the identity of the victim ([link](#))'.

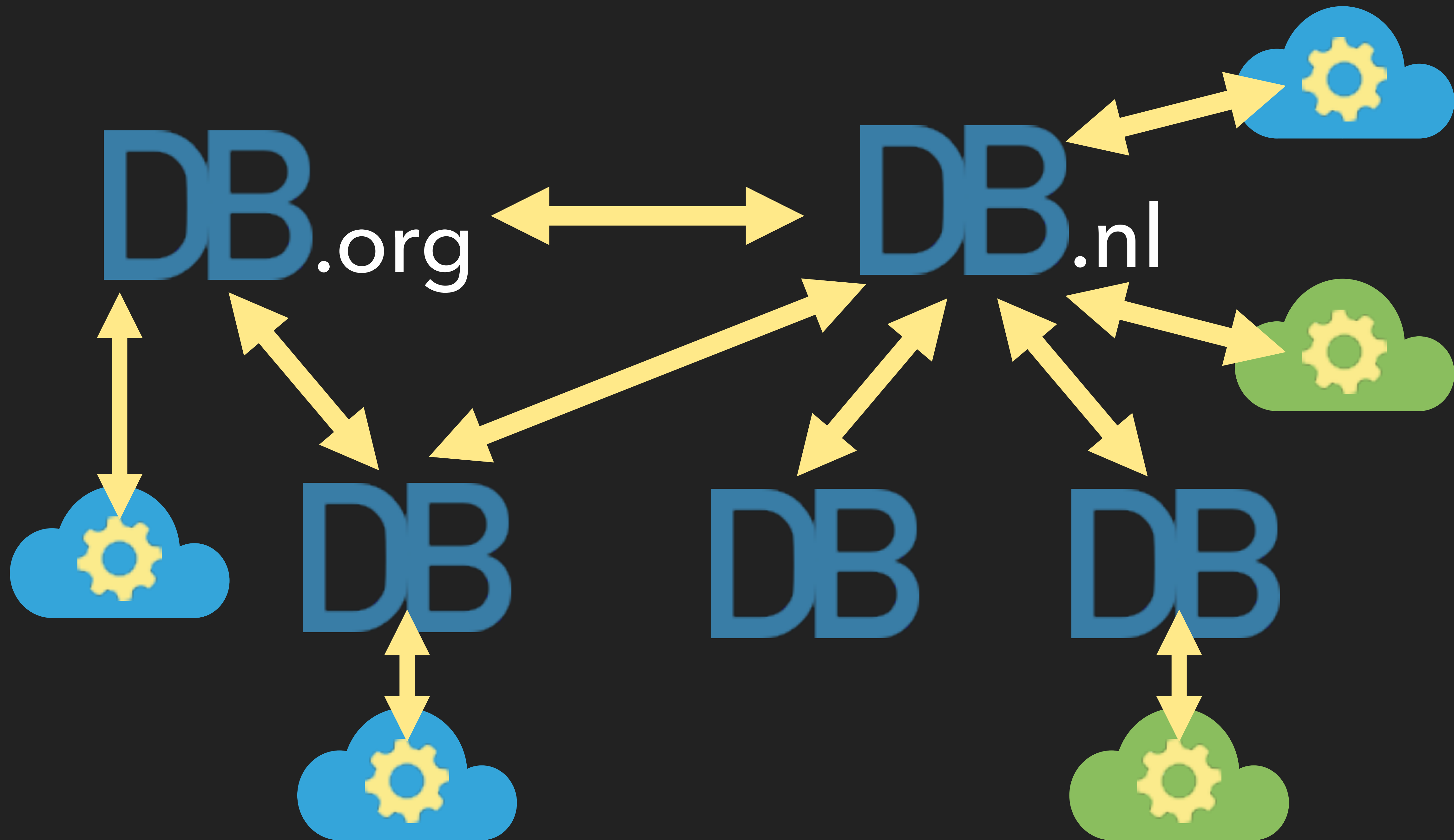
<https://ddosdb.NL>

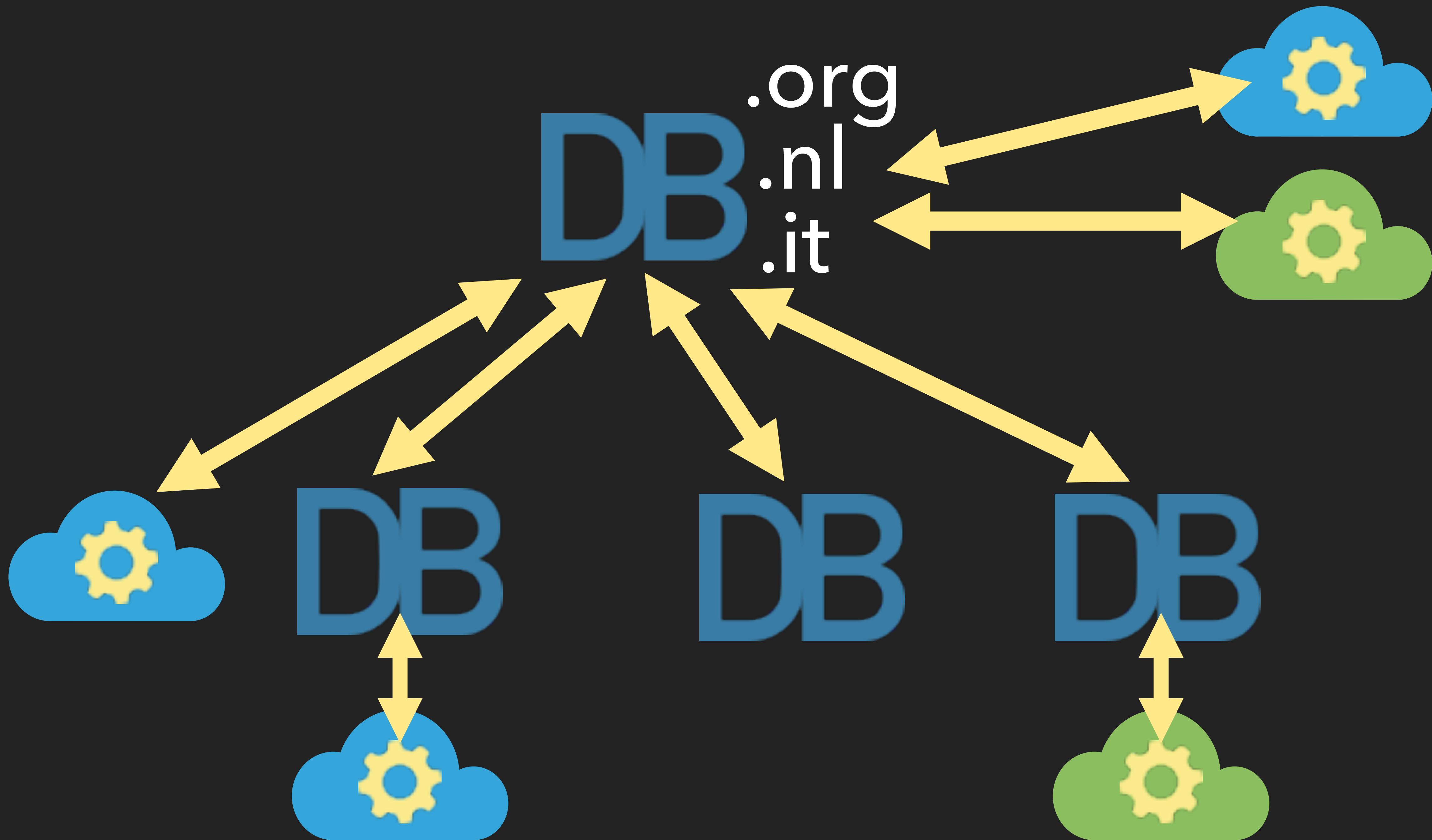


The screenshot shows the homepage of the DDoSDB website, identical to the previous one, but with a laptop overlay on the right side. The laptop screen displays the text 'WHITELISTED Programs Only' and an illustration of a man in a suit and sunglasses. The text on the laptop screen is partially obscured by the laptop's frame. The background of the laptop screen shows a red carpet and stanchions. The text on the laptop screen is 'WHITELISTED Programs Only'.



# CHALLENGES & FUTURE DIRECTIONS





# SOLVING DDOOS ATTACKS

Koen van Hove

Researcher at the University of Twente

[koen@ddosdb.org](mailto:koen@ddosdb.org)

## QUESTIONS?



**BACKUP SLIDES**



**NETWORK MEASUREMENT**  
(PCAP, NET FLOW, IPFIX, SFLOW, LOGS, ...)



**DDOS\_DISSECTOR**

INPUT: NETWORK MEASUREMENT

OUTPUT: DDOS FINGERPRINT (+\*NOTES)

FILTERED AND ANONYMIZED NETW. MEASU.

**DDOS\_FINGERPRINT\_CONVERTERS**

INPUT: DDOS FINGERPRINT

OUTPUT: RULE/SIGNATURE FOR SPECIFIC HW/SW SOLUTION(S)  
(SNORT, SURICATA, BRO, IPTABLES, EBPF, BGP FLOWSPEC,  
...)



**DB**

**DDOSDB**

STORE, ENRICH, AND DISTRIBUTE DDOS ATTACK RELATED INFO



# SOLVING DDOOS ATTACKS IN THE NETHERLANDS, EUROPE, AND BEYOND

---

FACILITATING BRIDGING SOLUTIONS AND STAKEHOLDERS

# DDOOS CLEARING HOUSE

# WHAT IS THE AVERAGE ECONOMIC LOSS PER DDOS ATTACK?

- A. \$25.000
- B. \$250.000
- C. \$2.500.000
- D. \$25.000.000