CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe

L'IHEDN, 08-12-2021

Thijs van den Hout

(SIDN Labs)

Partners: SIDN, UT, TI, FORTH, UZH, SURF, ULANC, CODE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

In this presentation

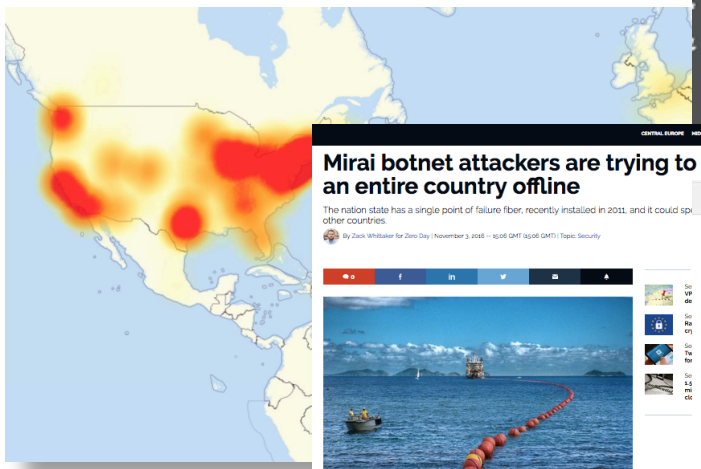
- DDoS attacks
- Introduction to the DDoS Clearing House
- The DDoS Clearing House testbed
- Demonstration

About DDoS

- Overwhelming a victim with network traffic
- “Bot nets” send traffic
- Vulnerable services on the internet amplify the traffic
- Mitigation by “scrubbing services”

High-impact DDoS Examples

Mirai botnet, 2016



Liberia, 2016

Estonia, 2007

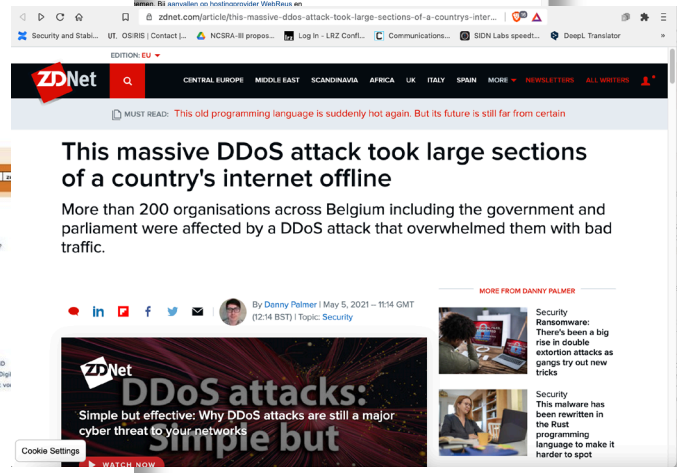
The Netherlands, January 2018

The Netherlands, September 2020

House of Representatives of The Netherlands, Oct 2020

Tweede Kamer
DER STATEN-GENERAAL

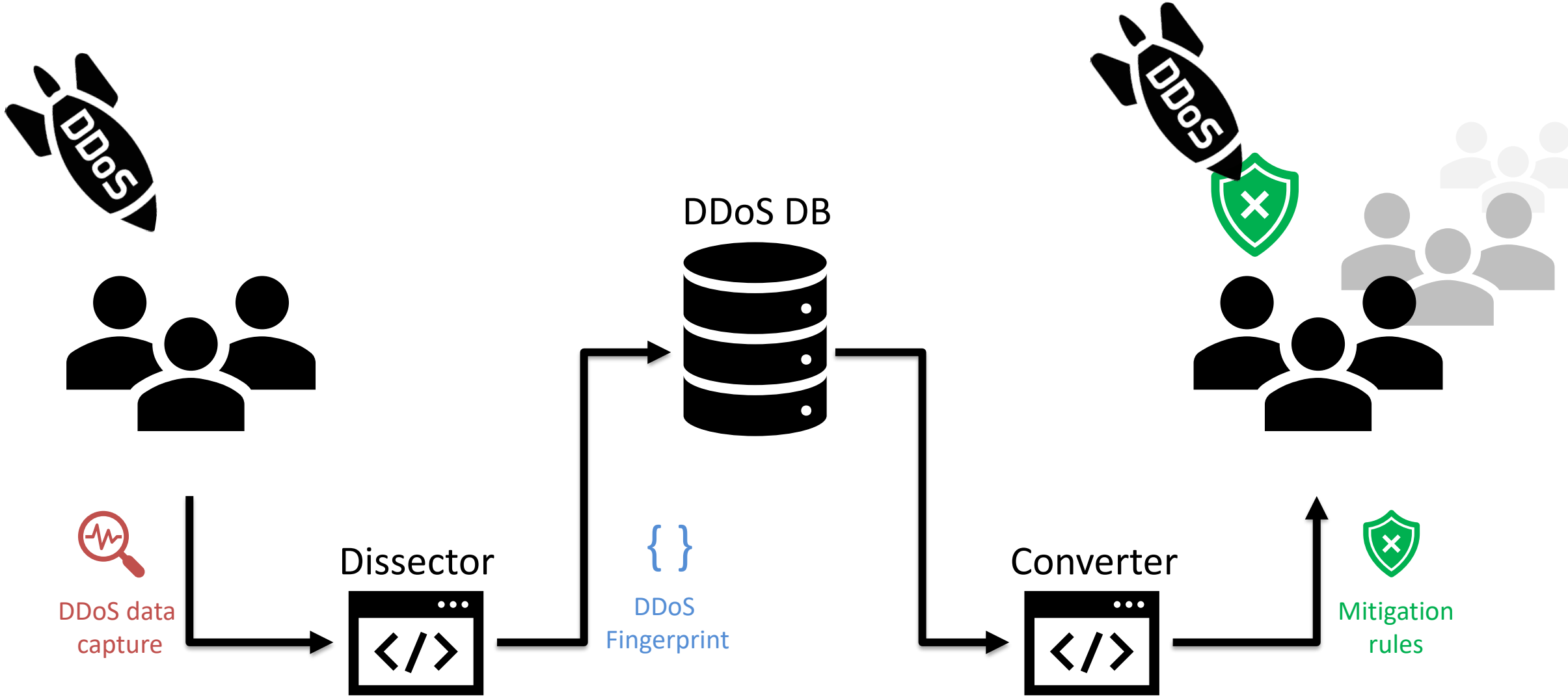
Belgium, May 2021



DDoS Clearing House

- Share summarized information about DDoS attacks
- Core service of an anti-DDoS Coalition: collaboratively fight DDoS
- Broaden the view of the DDoS landscape
- 3 key components: Dissector, DDoS-DB, Converter

DDoS Clearing House



DDoS fingerprint

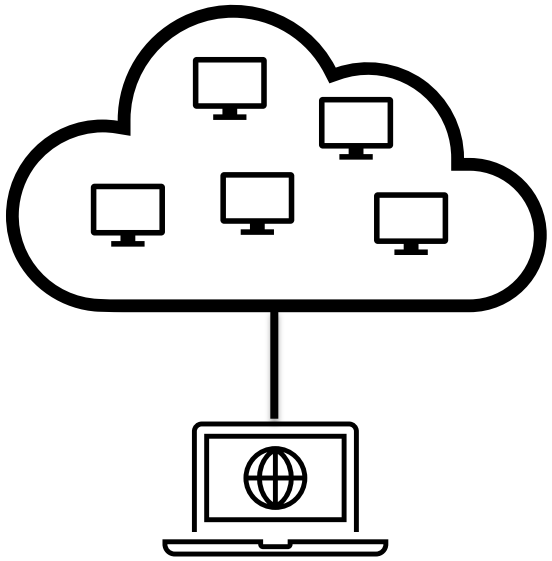
- Summary of the DDoS attack
- Meta-data such as protocols, attack types, nr. of packets, duration, etc.


```
{
  attack_vector: [
    {
      ip_proto: [
        "UDP"
      ]
      highest_protocol: [
        "UDP"
      ]
      frame_len: [
        132
      ]
      udp_length: [
        28
      ]
      dstport: [
        8989
      ]
      fragmentation: [
        False
      ]
      src_ips: [
        "109.74.195.132"
        "172.105.209.31"
        "198.74.60.20"
        "97.107.135.252"
        "172.105.59.184"
      ]
      attack_vector_key: "e7a48aec33750e1ecc64ee3a33db8bbc2cd42cce508aaf6d91956ad83fb9d455"
      one_line_fingerprint: "{'ip_proto': 'UDP', 'highest_protocol': 'UDP', 'frame_len': 132,
      'udp_length': 28, 'dstport': 8989, 'fragmentation': False, 'src_ips': 'omitted'}"
    }
  ]
  start_time: "2021-09-15 14:21:41"
  duration_sec: 13.0
  total_dst_ports: 1
  avg_bps: 65563
  total_packets: 6457
  ddos_attack_key: "343e479a35aee4dfd878a6cdedf85a2d855a25e669a38049957c1687b8fe1958"
  key: "343e479a35aee4d"
  total_ips: 5
  file_type: "PCAP"
  tags: [
    "SINGLE_VECTOR_ATTACK"
    "UDP"
    "UDP_SUSPECT_LENGTH"
  ]
  submitter: "sidnlabs"
  submit_timestamp: "2021-10-13T12:55:21.822069"
  shareable: False
}
```

Clearing House testbed

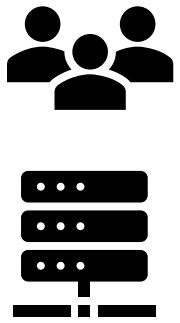
- Goal: pilot in Dutch Anti-DDoS Coalition & Italian consortium
- Obstacle: production systems and legal agreements
- Solution: representative environment in which to test the technical developments of the Clearing House

Remote cloud-hosted Traffic simulator



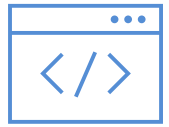
Coalition

Member 1

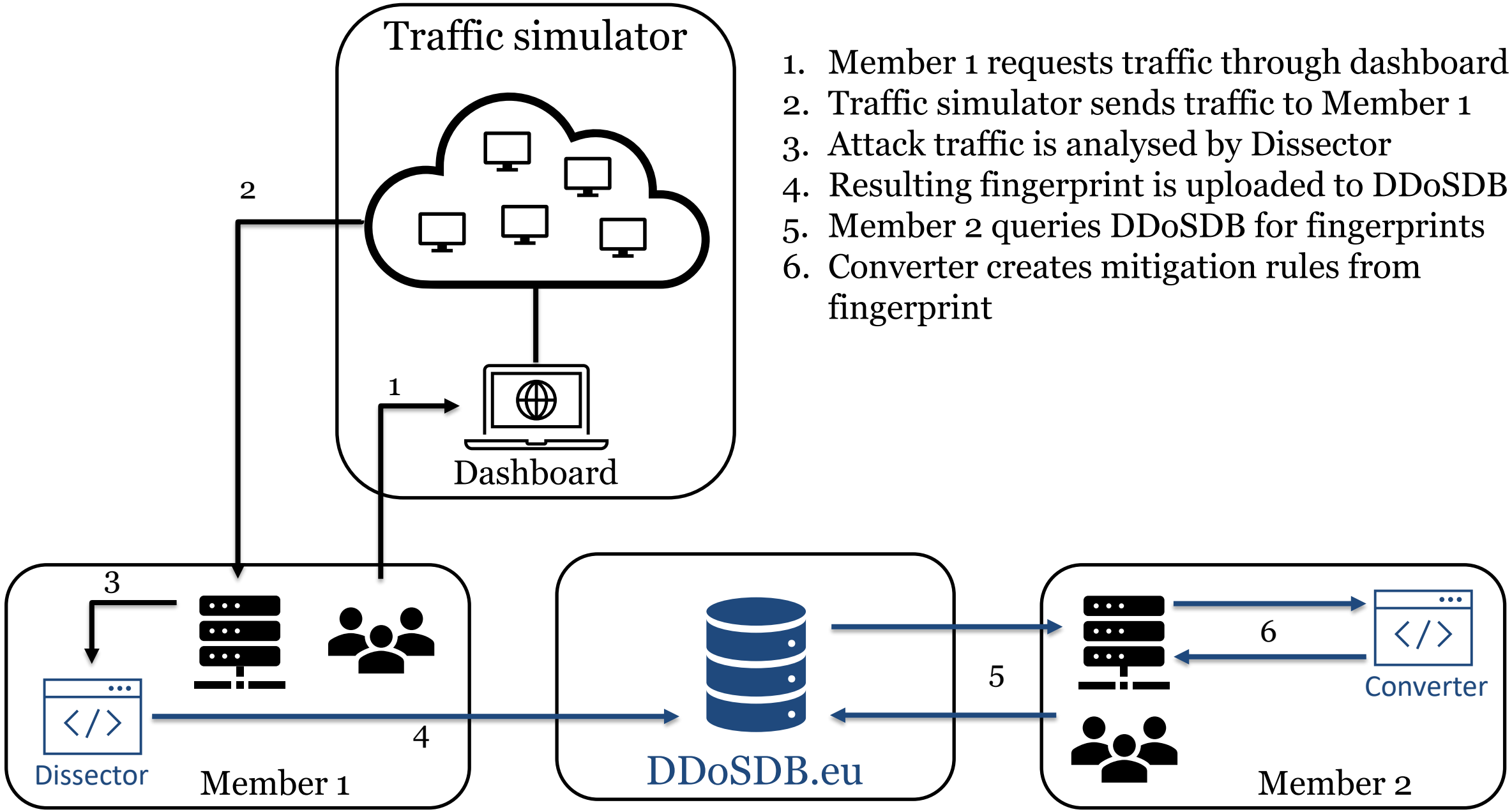


Member 2

DDoS Clearing House

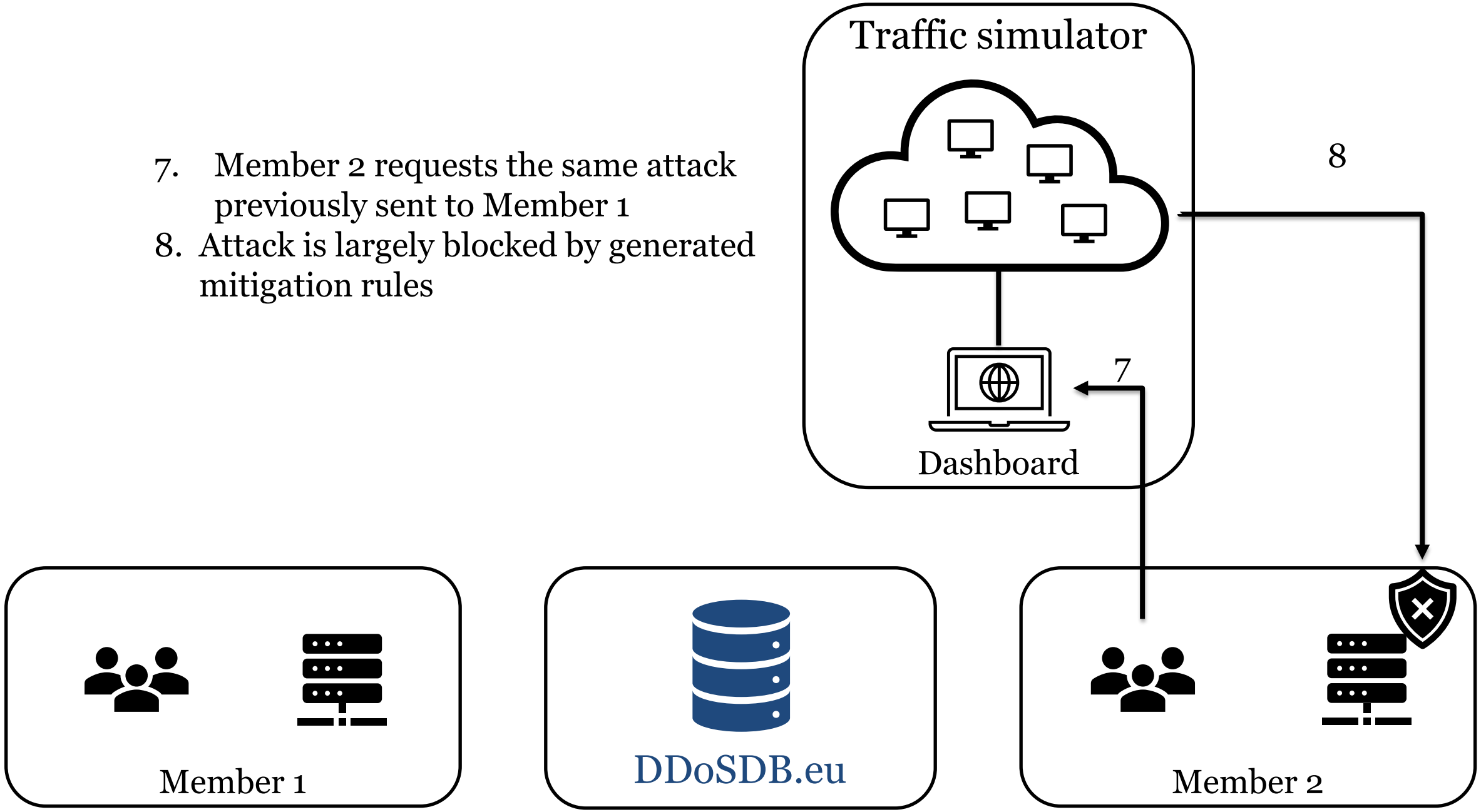


DDoS DB



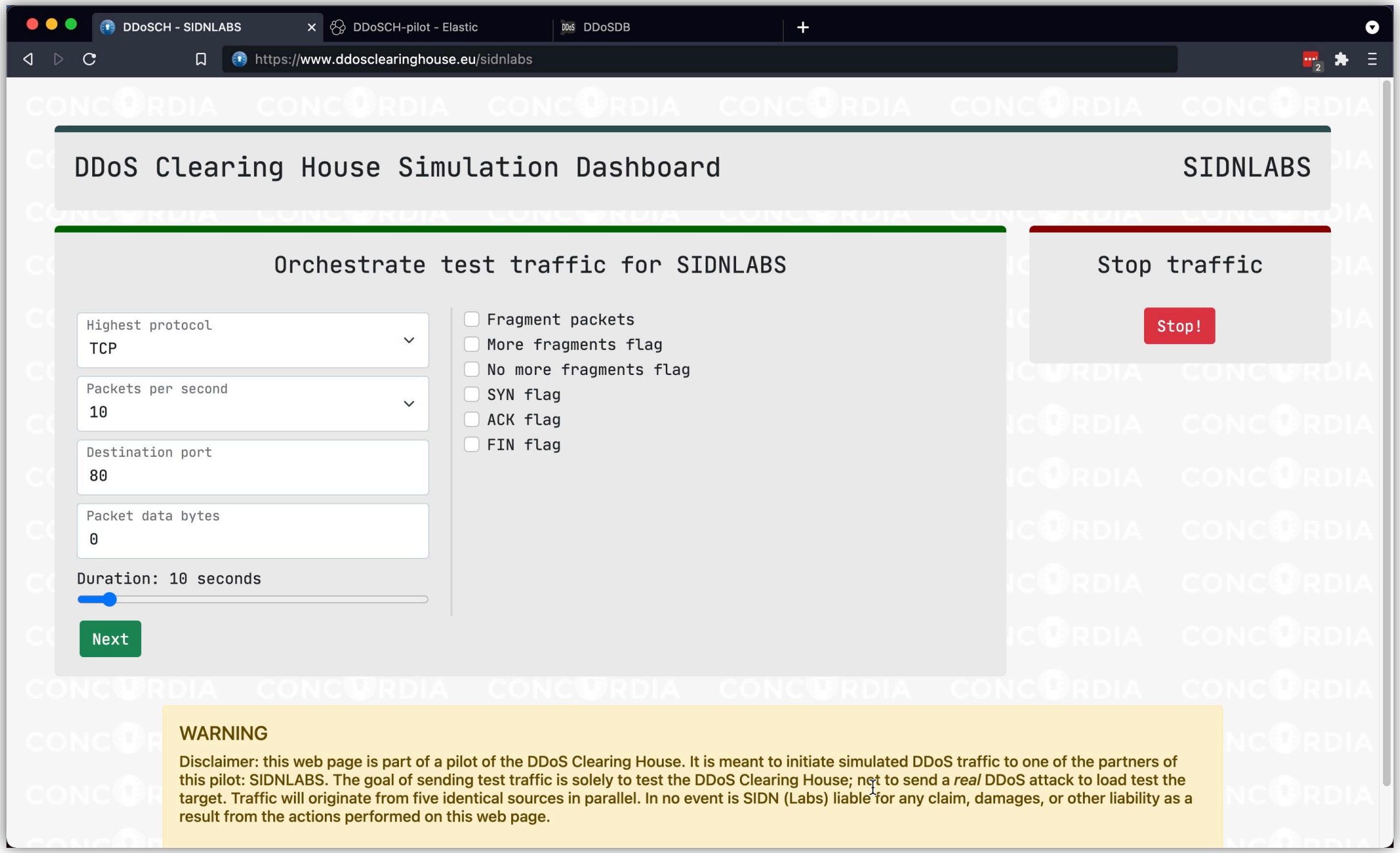
1. Member 1 requests traffic through dashboard
2. Traffic simulator sends traffic to Member 1
3. Attack traffic is analysed by Dissector
4. Resulting fingerprint is uploaded to DDoSDB
5. Member 2 queries DDoSDB for fingerprints
6. Converter creates mitigation rules from fingerprint

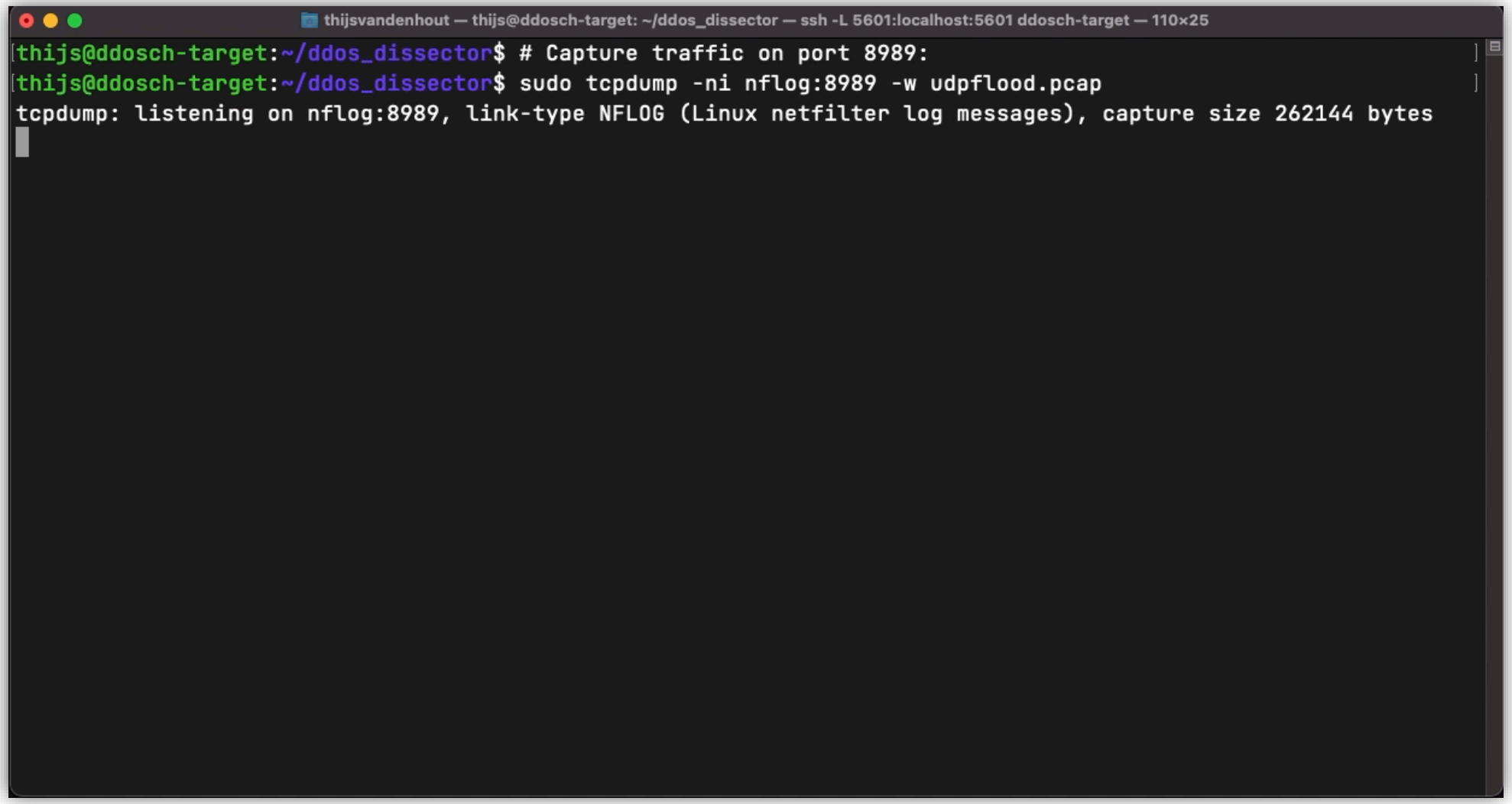
7. Member 2 requests the same attack previously sent to Member 1
8. Attack is largely blocked by generated mitigation rules

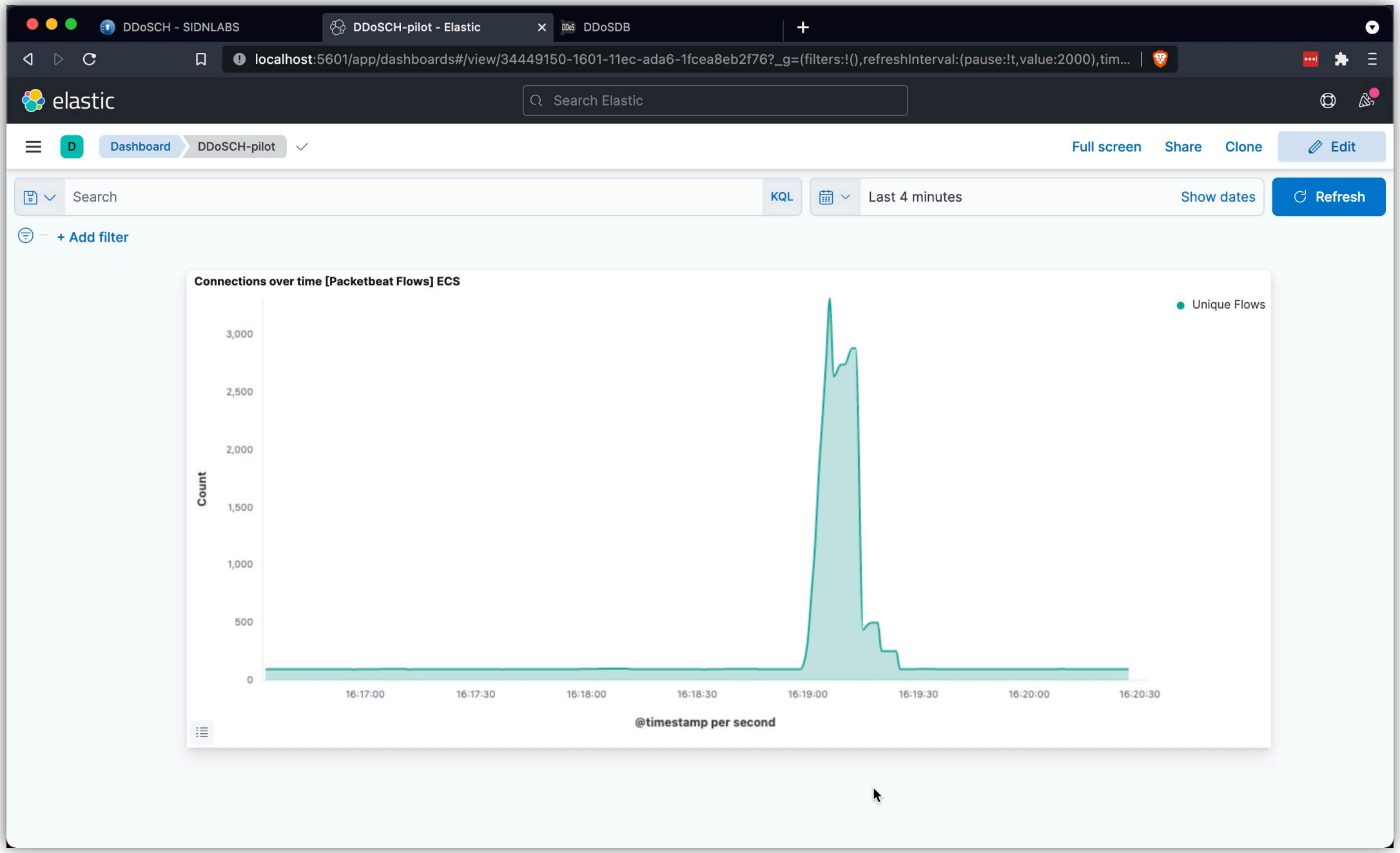


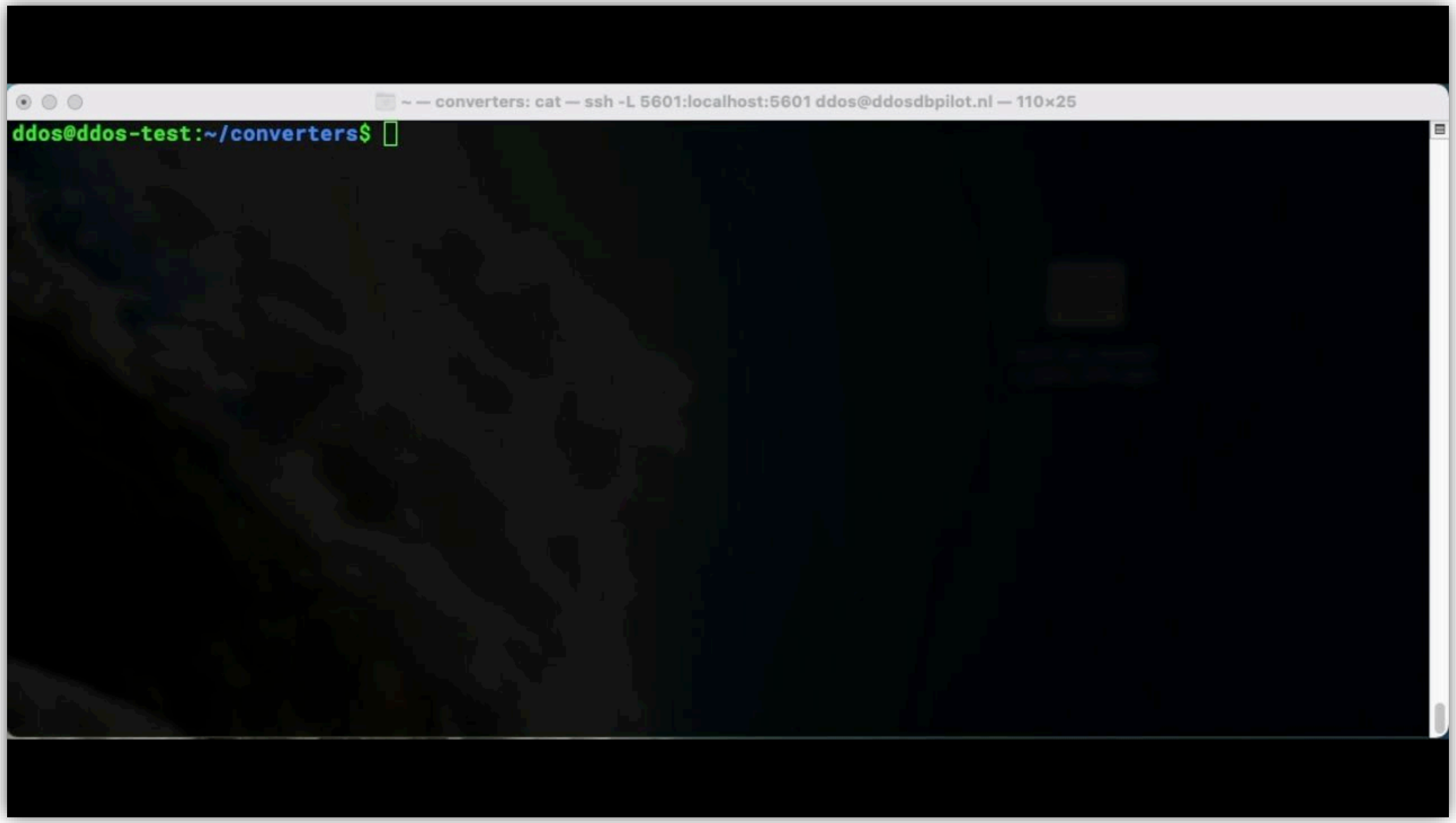
Demonstration

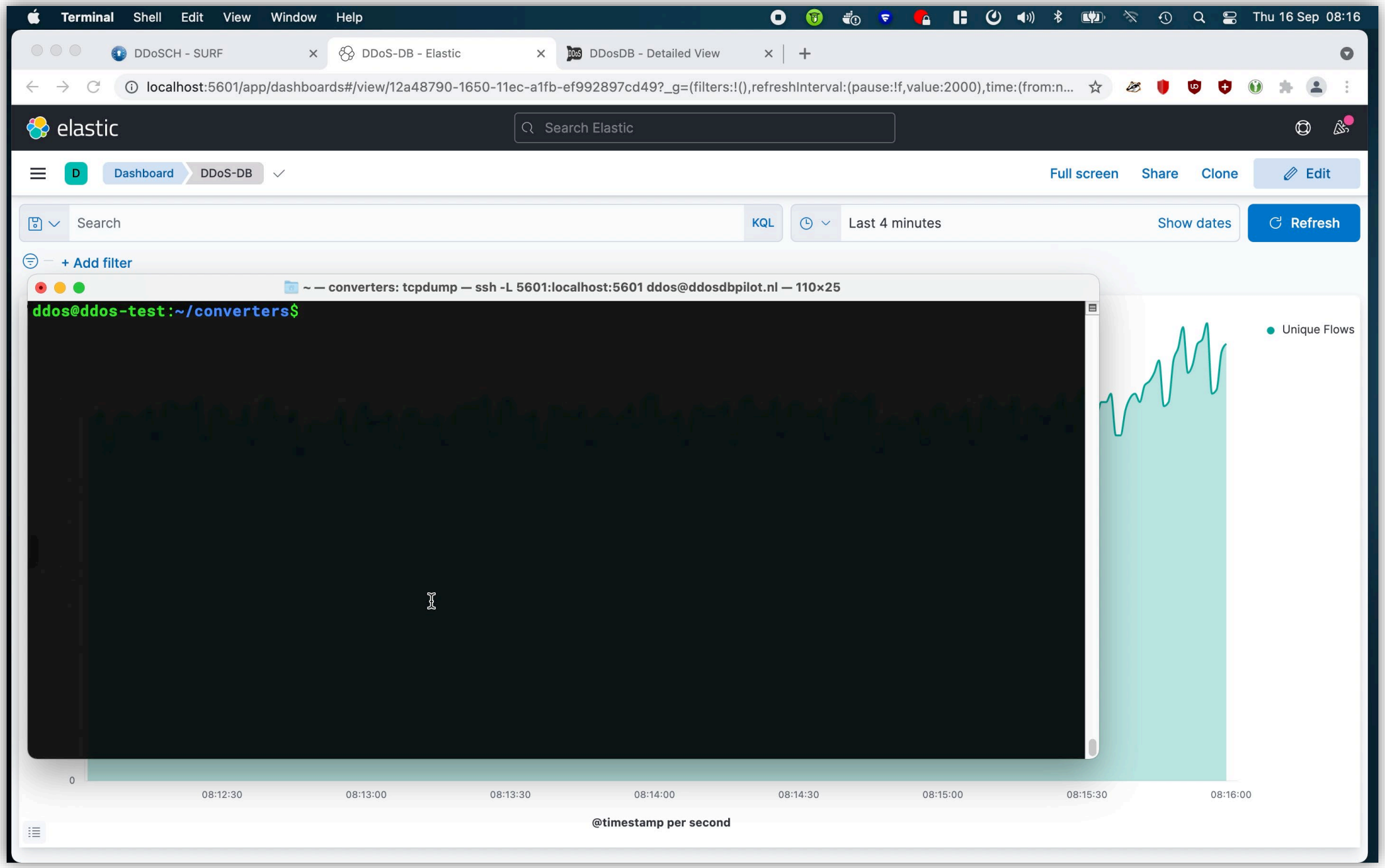
- Virtual anti-DDoS coalition with SIDN and SURF
- Recorded a demo video


DDoSCH - SIDNLABS
DDoSCH-pilot - Elastic
DDoSDB
https://www.ddosclearinghouse.eu/sidnlabs
DDoS Clearing House Simulation Dashboard
SIDNLABS
Orchestrate test traffic for SIDNLABS
Highest protocol
TCP
Packets per second
10
Destination port
80
Packet data bytes
0
Duration: 10 seconds
Next
Fragment packets
More fragments flag
No more fragments flag
SYN flag
ACK flag
FIN flag
Stop traffic
Stop!
WARNING
Disclaimer: this web page is part of a pilot of the DDoS Clearing House. It is meant to initiate simulated DDoS traffic to one of the partners of this pilot: SIDNLABS. The goal of sending test traffic is solely to test the DDoS Clearing House; not to send a real DDoS attack to load test the target. Traffic will originate from five identical sources in parallel. In no event is SIDN (Labs) liable for any claim, damages, or other liability as a result from the actions performed on this web page.


thijsvandenhout — thijs@ddosch-target: ~/ddos_dissector — ssh -L 5601:localhost:5601 ddosch-target — 110×25
thijs@ddosch-target:~/ddos_dissector$ # Capture traffic on port 8989:
thijs@ddosch-target:~/ddos_dissector$ sudo tcpdump -ni nflog:8989 -w udpflood.pcap
tcpdump: listening on nflog:8989, link-type NFLOG (Linux netfilter log messages), capture size 262144 bytes


DDoSCH - SIDNLABS
DDoSCH-pilot - Elastic
DDoSDB
localhost:5601/app/dashboards#/view/34449150-1601-11ec-ada6-1fcea8eb2f76?_g=(filters:!(),refreshInterval:(pause:!t,value:2000),tim...
elastic
Search Elastic
D
Dashboard
DDoSCH-pilot
Full screen
Share
Clone
Edit
Search
KQL
Last 4 minutes
Show dates
Refresh
+ Add filter
Connections over time [Packetbeat Flows] ECS
Unique Flows
3,000
2,500
2,000
1,500
1,000
500
0
Count
16:17:00
16:17:30
16:18:00
16:18:30
16:19:00
16:19:30
16:20:00
16:20:30
@timestamp per second


~ — converters: cat — ssh -L 5601:localhost:5601 ddos@ddosdbpilot.nl — 110×25
ddos@ddos-test:~/converters$


Terminal Shell Edit View Window Help
Thu 16 Sep 08:16
DDoSCH - SURF
DDoS-DB - Elastic
DDosDB - Detailed View
localhost:5601/app/dashboards#/view/12a48790-1650-11ec-a1fb-ef992897cd49?_g=(filters:!(),refreshInterval:(pause:!f,value:2000),time:(from:n...
elastic
Search Elastic
D
Dashboard
DDoS-DB
Full screen
Share
Clone
Edit
Search
KQL
Last 4 minutes
Show dates
Refresh
+ Add filter
~ — converters: tcpdump — ssh -L 5601:localhost:5601 ddos@ddosdbpilot.nl — 110×25
ddos@ddos-test:~/converters$
Unique Flows
0
08:12:30
08:13:00
08:13:30
08:14:00
08:14:30
08:15:00
08:15:30
08:16:00
@timestamp per second

Success!


DDoS
DDoS DB
DDoS data capture
Dissector
DDoS Fingerprint
Converter
Mitigation rules

More content online:

sidnlabs.nl
nomoreddos.org
github.com/ddos-clearing-house