



DDoS Clearing House for Europe (Task 3.2)

Demonstrating the DDoS Clearing House testbed

Thijs van den Hout
(SIDN Labs)

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



In this presentation

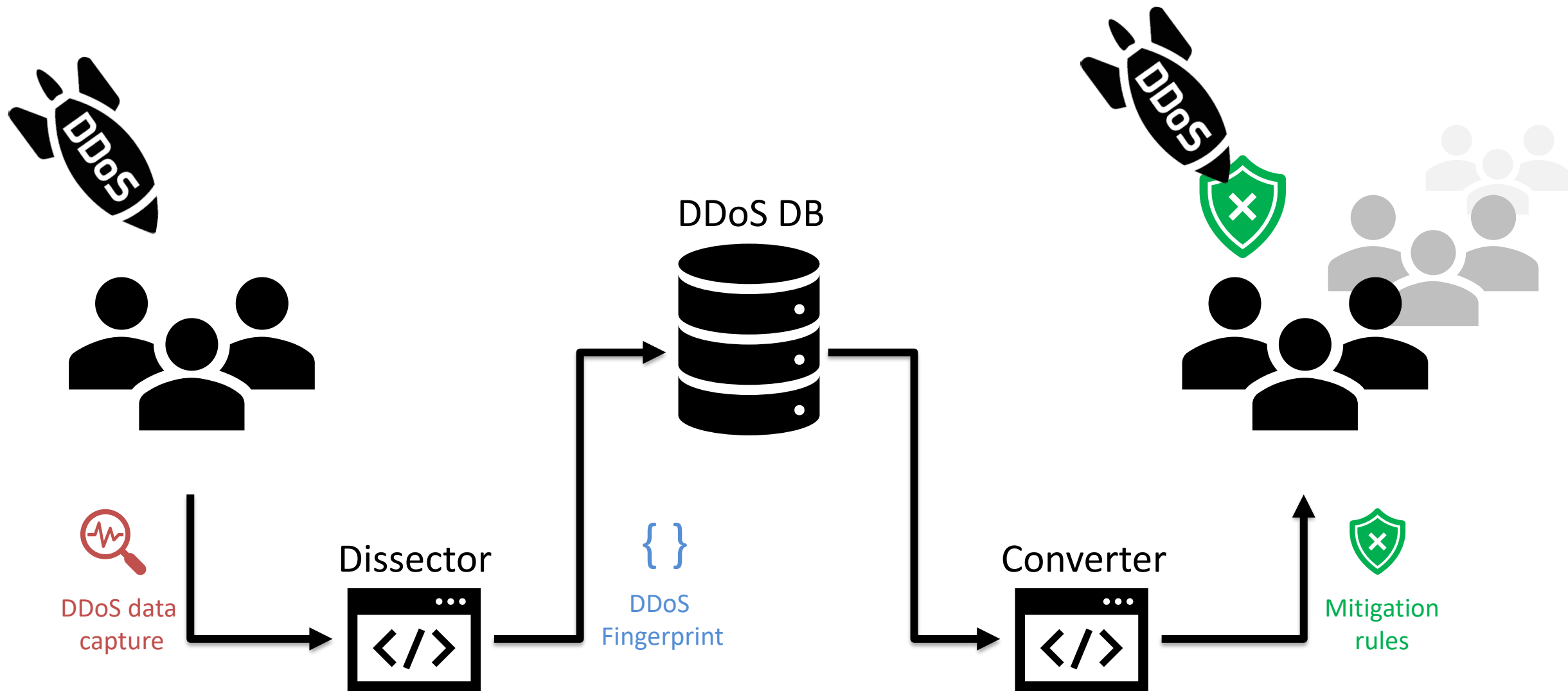
- Short introduction to the DDoS Clearing House
- Why we set up a testbed
- How the testbed is used to test the Clearing House
- Testbed demonstration



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 [REDACTED]"
        "172.10 [REDACTED]"
        "198.74 [REDACTED]"
        "97.107 [REDACTED]"
        "172.10 [REDACTED]"
      ]
      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: "343e479a35aee4dfd878a6cdef85a2d855a25e669a38049957c1687b8fe1958"
  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
}
```

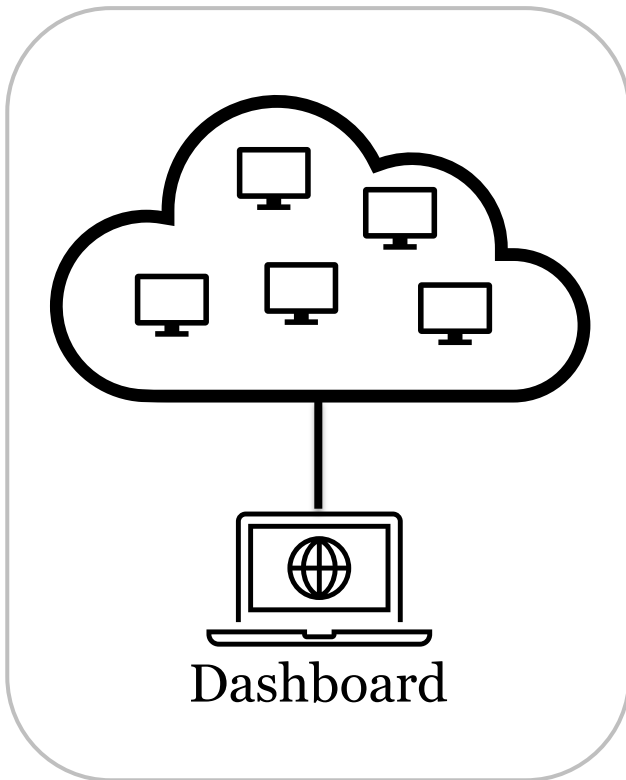


Why a testbed?

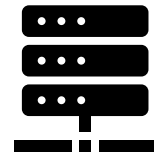
- Goal: pilot in Dutch Anti-DDoS Coalition & Italian consortium
- Obstacle: production systems and legal agreements
- Solution: representative environment in which to test the technical developments of the Clearing House



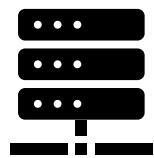
Remote cloud-hosted Traffic simulator



Coalition



Member 1

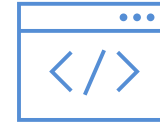


Member 2

DDoS Clearing House



Converter



Dissector



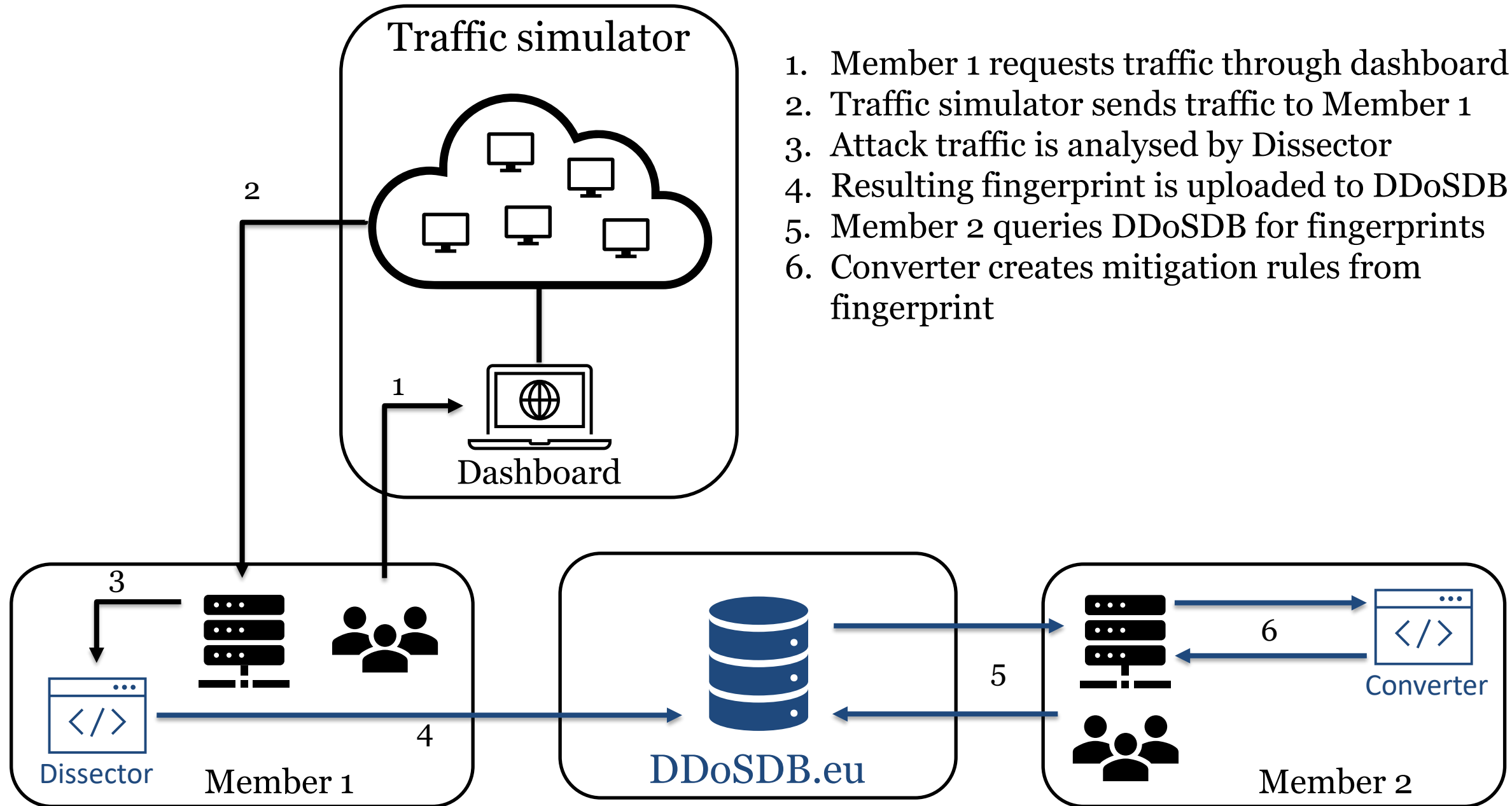
Converter



Dissector

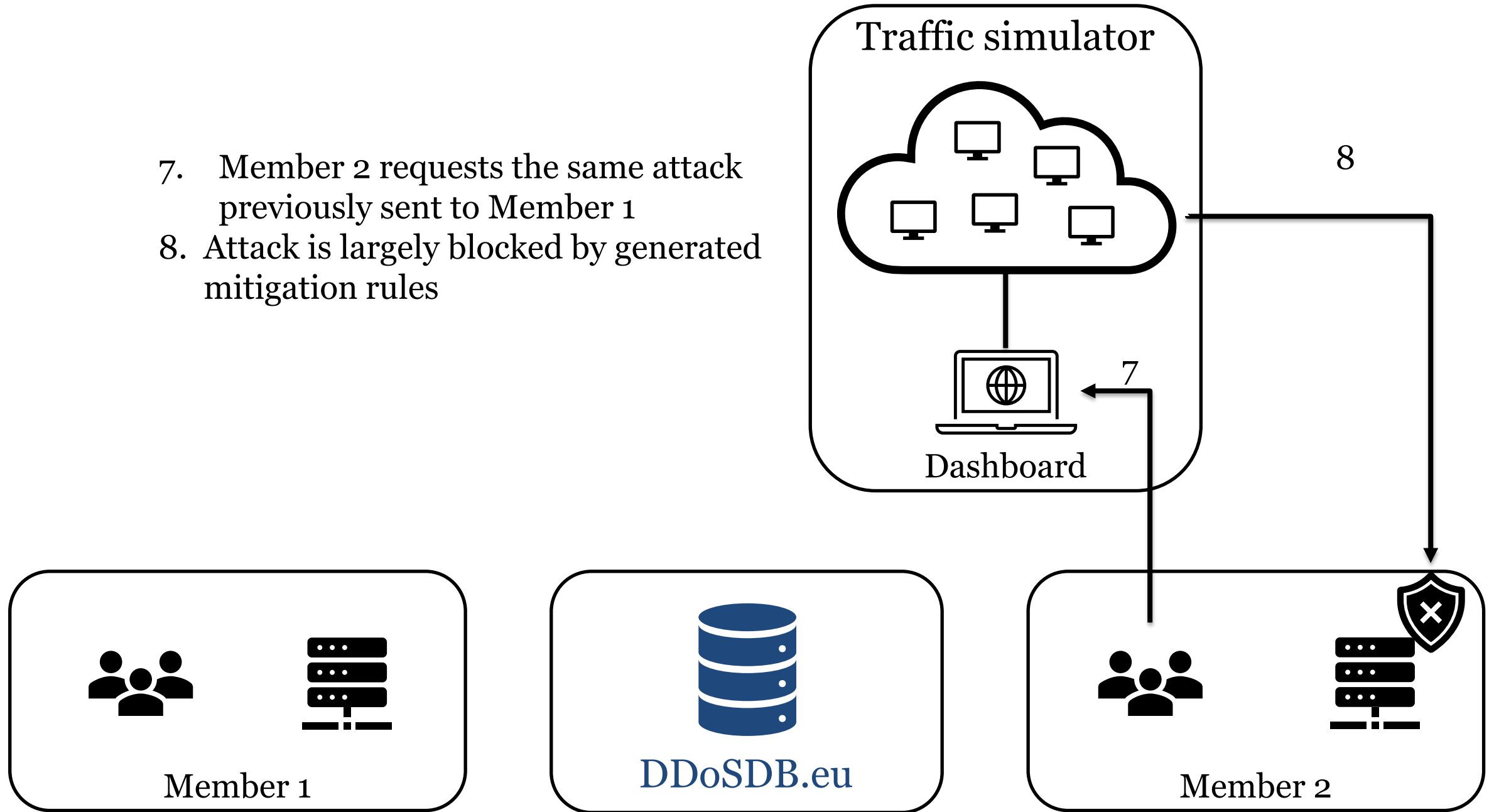


DDoS DB



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 demo video



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

Fragment packets

More fragments flag

No more fragments flag

SYN flag

ACK flag

FIN flag

Stop traffic

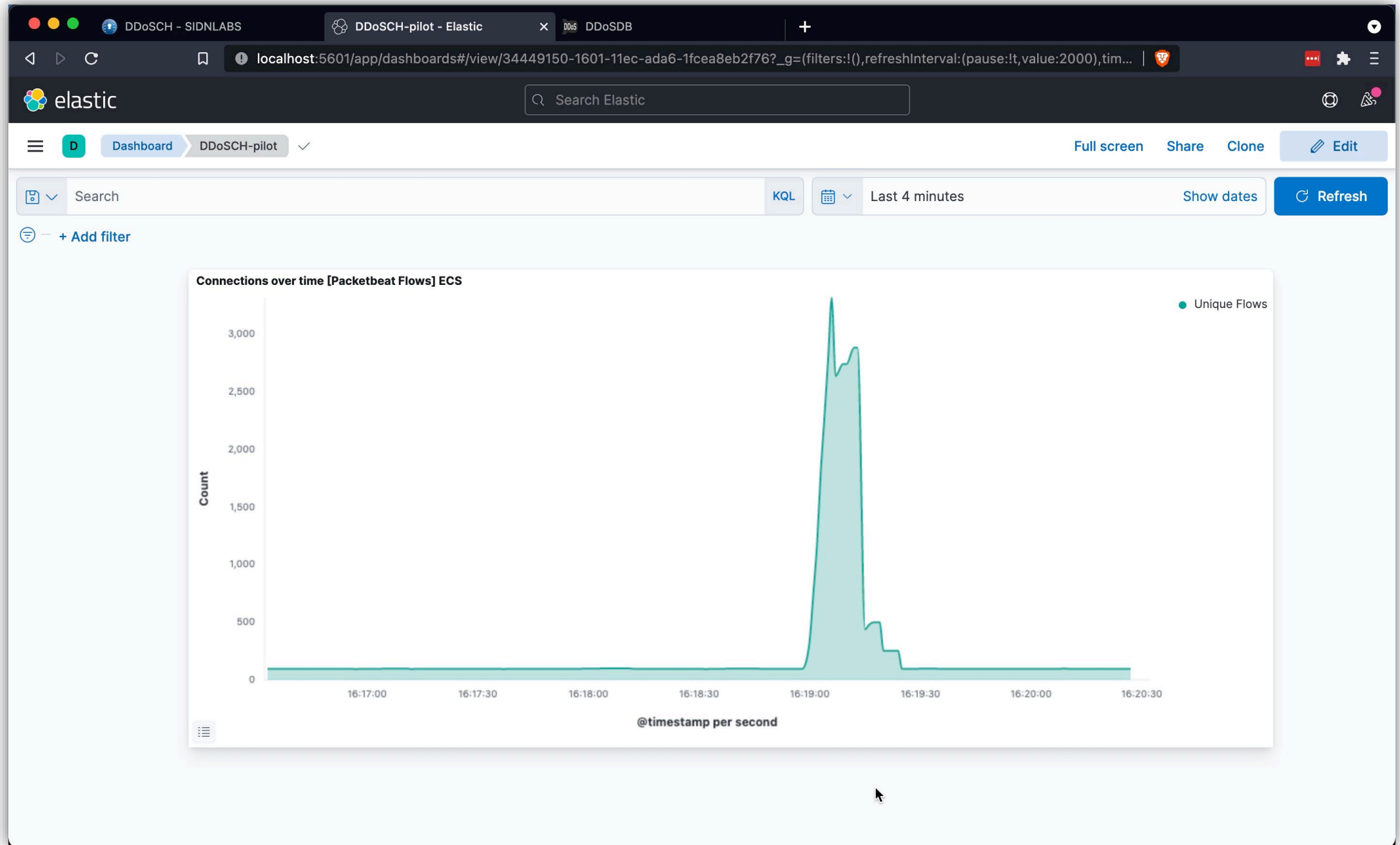
Stop!

Next

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 — 110x25
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 NFL0G (Linux netfilter log messages), capture size 262144 bytes
```





```
~ -- converters: cat -- ssh -L 5601:localhost:5601 ddos@ddosdbpilot.nl -- 110x25  
ddos@ddos-test:~/converters$
```



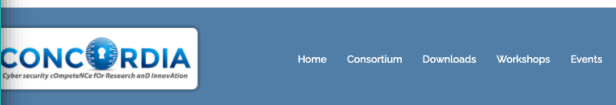
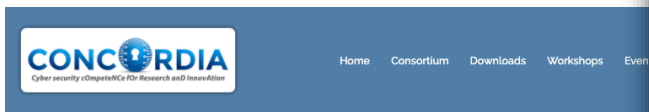
The screenshot shows a web browser window displaying the Elastic dashboard. The browser tabs include 'DDoSSCH - SURF', 'DDoS-DB - Elastic', and 'DDoSDB - Detailed View'. The address bar shows the URL: `localhost:5601/app/dashboards#/view/12a48790-1650-11ec-a1fb-ef992897cd49?_g=(filters:!),refreshInterval:(pause:!f,value:2000),time:(from:n...`. The dashboard header includes the Elastic logo, a search bar, and navigation options like 'Full screen', 'Share', 'Clone', and 'Edit'. Below the header, there are controls for search, KQL, time range (set to 'Last 4 minutes'), and a 'Refresh' button. The main content area features a terminal window on the left and a line graph on the right. The terminal window title is `~ -- converters: tcpdump -- ssh -L 5601:localhost:5601 ddos@ddosdbpilot.nl -- 110x25` and shows the prompt `ddos@ddos-test:~/converters$`. The line graph is titled 'Unique Flows' and shows a fluctuating teal line over a time period from 08:12:30 to 08:16:00. The x-axis is labeled '@timestamp per second'.

Success!



More content online:

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



POSTED APRIL 9, 2020 ADMIN CONCORDIA

Increasing the Netherlands' DDoS resilience together

First lessons learned from setting up a national anti-DDoS initiative, part I of III

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together. In this series of three blogs, we'll first discuss the rationale behind our initiative, then describe a technical facility called the DDoS clearing house that enables coalition members to automatically measure and share the properties of DDoS attacks (e.g. attack duration and source IP addresses), before finally reviewing our key challenges, the lessons learned and the way forward. Our lessons learned are an important input for a "cookbook" to set up anti-DDoS coalitions elsewhere in Europe.



POSTED SEPTEMBER 24, 2020 ADMIN CONCORDIA

Work in Progress: the CONCORDIA Platform for Threat Intelligence

Our first steps to improve Europe's information position in cybersecurity

We present CONCORDIA's vision for a cross-sector, pan-European platform for collecting, analyzing, and sharing threat intelligence, which combines datasets built up in different parts of the project.

What is threat intelligence?

Threat intelligence can be defined as the process of acquiring knowledge from multiple sources about threats to an environment. Threat intelligence includes attack techniques, indicators of compromise, and real-world datasets.

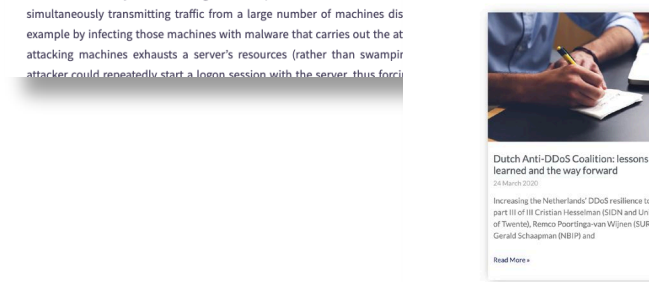
Note: we're using two types of reference in this blog series: hyperlinks for information, while numbers between straight brackets ([]) link to related papers.

DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with network the ability to service legitimate requests from their clients. The attacker simultaneously transmitting traffic from a large number of machines dis example by infecting those machines with malware that carries out the at attacking machines exhausts a server's resources (rather than swampi attacker could repeatedly start a login session with the server, thus forc

Wednesday 11 October 2021
Article by: Thijs van den Heuvel, Remco Poortinga van Wijnen, Cristian Hesselman, Christa Papachristos, mc Karin Vink CPPP

We have created a distributed testbed that enables us to realistically test the **DDoS Clearing House**: a system that enables organisations to handle DDoS attacks more proactively by automatically sharing measurements of the DDoS attacks they handle. Our testbed allows us to temporarily skip typically time-consuming organisational processes such as setting up data sharing agreements and deploying software in production systems, which helps to advance the system towards a pilot and a production version. We discuss the motivation for developing our testbed, its requirements, implementation and our lessons learnt. We're developing the Clearing House and the testbed as part of the CONCORDIA project, and we'll be using both in the Dutch Anti-DDoS Coalition.



Blog

Setting up a national DDoS clearing house
12 March 2020

Increasing the Netherlands' DDoS resilience together, part II of III Cristian Hesselman (SIDN and University of Twente), Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBBP) and

Read More +

Increasing the Netherlands' DDoS resilience together
10 March 2020

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together.

Read More +

