



Cyber security cOmpeteNCe fOr Research andD 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



In this presentation

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

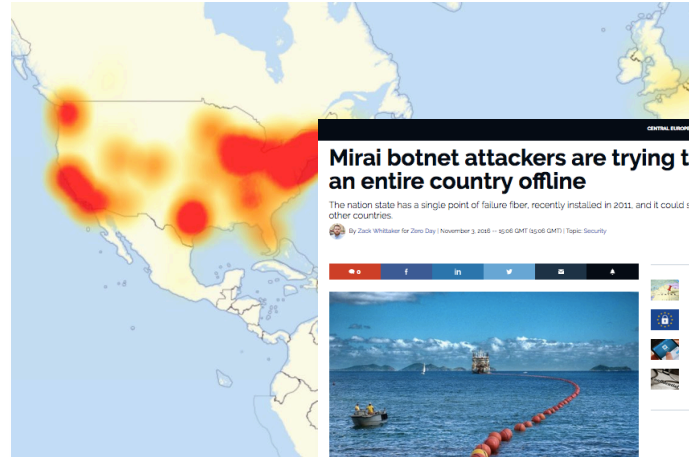
About DDoS

- 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

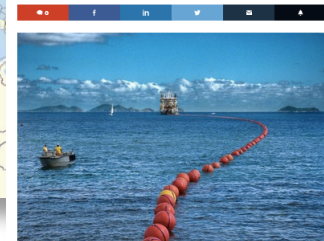
Mirai botnet, 2016



Mirai botnet attackers are trying to knock an entire country offline

The nation state has a single point of failure fiber, recently installed in 2011, and it could spread to other countries.

By Zack Whitaker for Zero Day | November 3, 2016 -- 8:06 GMT (8:06 GMT) | Topic: Security



A single submarine cable, like the one pictured, provides the bulk of the nation's internet. Image: AP photo

One of the largest Distributed Denial-of-Service (DDoS) attacks happened this week and almost nobody noticed.

Since the cyberattack on Dyn two weeks ago, the internet has been on edge, fearing another massive attack that would throw millions off the face of the web. The attack was said to be upwards of 1.1 Tbps — more than double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 600Gbps in size, said to be one of the largest at the time. The attack was made possible by the Mirai botnet, an open-source botnet that anyone can use, which harnesses the power of insecure Internet of Things (IoT) devices.

This week, another Mirai botnet, known as Botnet 14, began targeting a small, little-known African country, Liberia, sending

Liberia, 2016

Estonia, 2007



NOS Nieuws Sport Uitzendingen

Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

MA 29 JANUARI, 10:50 AANGEPAST MA 29 JANUARI, 11:37 BINNENLAND, ECONOMIE

DigiD Je eigen inlogcode voor de hele overheid

Home Nieuws Over DigiD Mochtigen Veiligheid Vraag & antwoord

DigiD

- DigiD aanvragen
- DigiD activeren
- Machtiging regelen
- Inloggen Mijn DigiD

Houd uw burgerservicenummer en uw mobiele telefoon bij de hand. [Boden de achtergrond](#)

Handige links

- Wachtwoord vergeten?
- Nieuw mobiel nummer regelen?
- Herinstellcode ontvangen?

Laatste nieuws

- Maatschappij valde e-mails DigiD
- Veranderingen in nieuwe versie DigiD
- Is uw computersysteem geschikt?

De golf van DDoS-aanvallen op Nederlandse instellingen houdt aan. Vandaag is de Belastingdienst tweemaal getroffen, en sinds 15.45 uur heeft ook DigiD last van een DDoS-aanval waardoor de site slecht bereikbaar is.

Volgens een woordvoerder van DigiD "gebeurt een aanval wel vaker, maar dit is wel zwaar". Er wordt hard gewerkt aan een oplossing. Hoelang dat nog gaat duren, kan de woordvoerder niet zeggen.

The Netherlands, January 2018

The Netherlands, September 2020

tweakers Nieuws Reviews Pricewatch Vraag & Antwoord Forum Carrière Meer

Opnieuw vinden grootschalige ddos-aanvallen op Nederlandse providers plaats

Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddos-aanvallen. Die lijken groter in omvang te worden en ook redelijk gevarieerd te zijn. Onder andere Signet, Calway en Delta zijn dinsdag slachtoffer.

De ddos-aanvallen vinden onder andere plaats bij Calway, bevestigd de provider. Eerder op dinsdagochtend had provider Delta last van een ddos-aanval die werd veroorzaakt door een ddos-aanval. Verder wordt er dinsdagochtend een grote aanval plaats op Signet. Dit is een signaal dat de infrastructuur voor veel kleine providers verzorgd. Ook behoort Signet infrastructuur voor TransIP. Daar hadden klanten vrijdagochtend ook last van door de aanval, al zijn die inmiddels opgelost.

Het lijkt erop dat het om dezelfde aanvallen gaat als de vorige week. Nederlandse providers troffen, af is dat niet met zekerheid te zeggen. Volgens een woordvoerder van het DigiD gaat het voornamelijk om drie ernstigere en vroege aanvallen. Het Nederlandse Beheerorganisatie Internet Providers behoeft de i en bedrijven ddos-verkeer naar toe kunnen toelaten om energie capaciteit om de aanvallen af te slaan, zegt de

zinet.com/articles/massive-ddos-attack-took-large-sections-of-a-countrys-internet-offline

Security and Stab... UT, OS/IS | Contact | NCDRIA-81 propos... Log in - LRZ Conf... Communications... SIDN Labs speed... DeepL Translator

ZDNet CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: This old programming language is suddenly hot again. But its future is still far from certain

This massive DDoS attack took large sections of a country's internet offline

More than 200 organisations across Belgium including the government and parliament were affected by a DDoS attack that overwhelmed them with bad traffic.

By Danny Palmer | May 5, 2021 - 11:14 GMT (12:14 BST) | Topic: Security

DDoS attacks: Simple but effective: Why DDoS attacks are still a major cyber threat to your networks

Simple but effective: Why DDoS attacks are still a major cyber threat to your networks

Belgium, May 2021

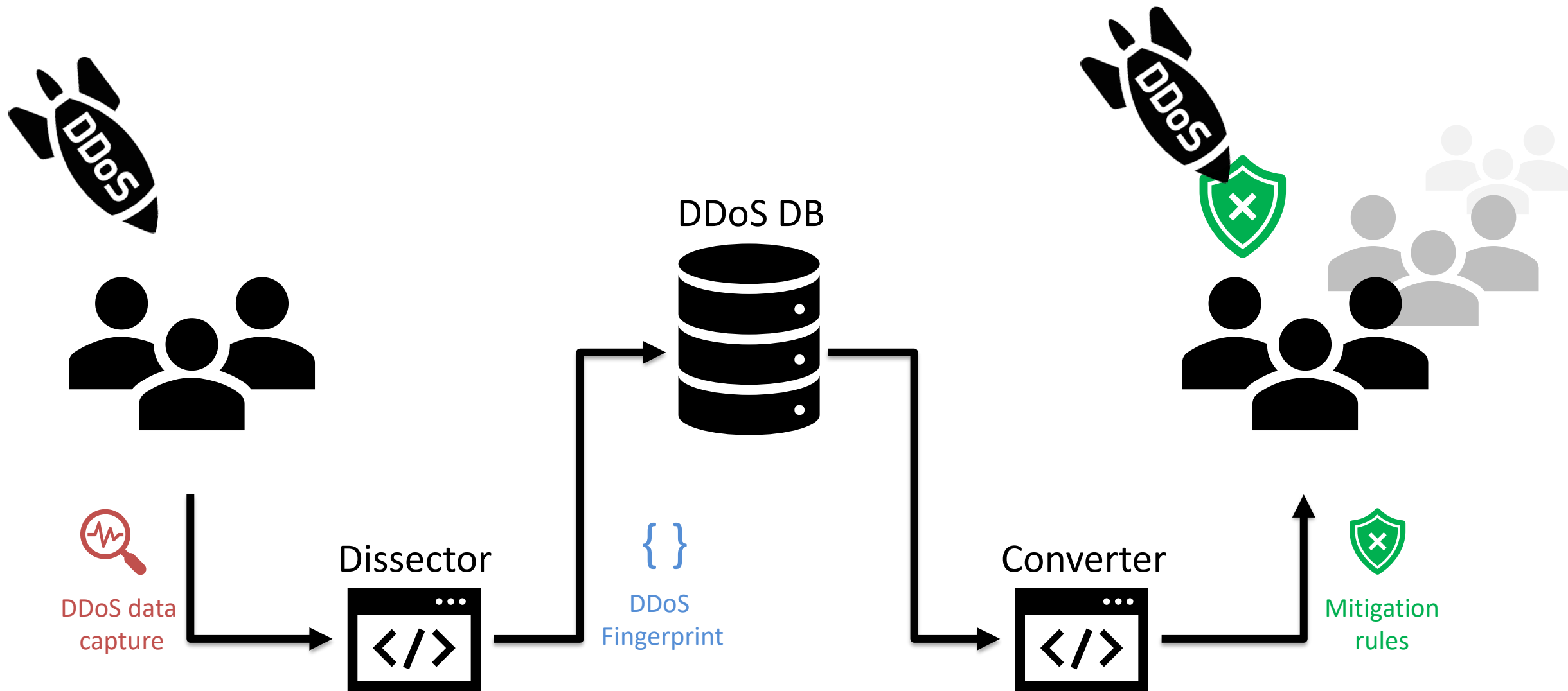
House of Representatives of The Netherlands, Oct 2020



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
}
```

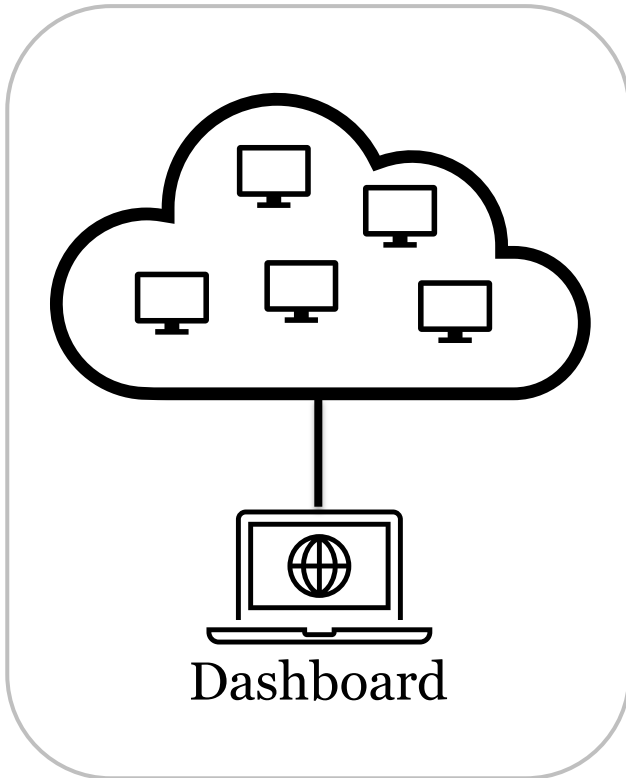


Clearing House testbed

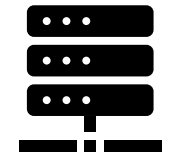
- Goal: pilot in Dutch Anti-DDoS Coalition & Italian consortium
- Obstacle: production systems and legal agreements
- Solution: representative environment in which to test the technical developments of the Clearing House



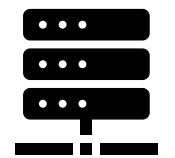
Remote cloud-hosted Traffic simulator



Coalition

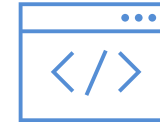


Member 1

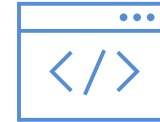


Member 2

DDoS Clearing House



Converter



Dissector



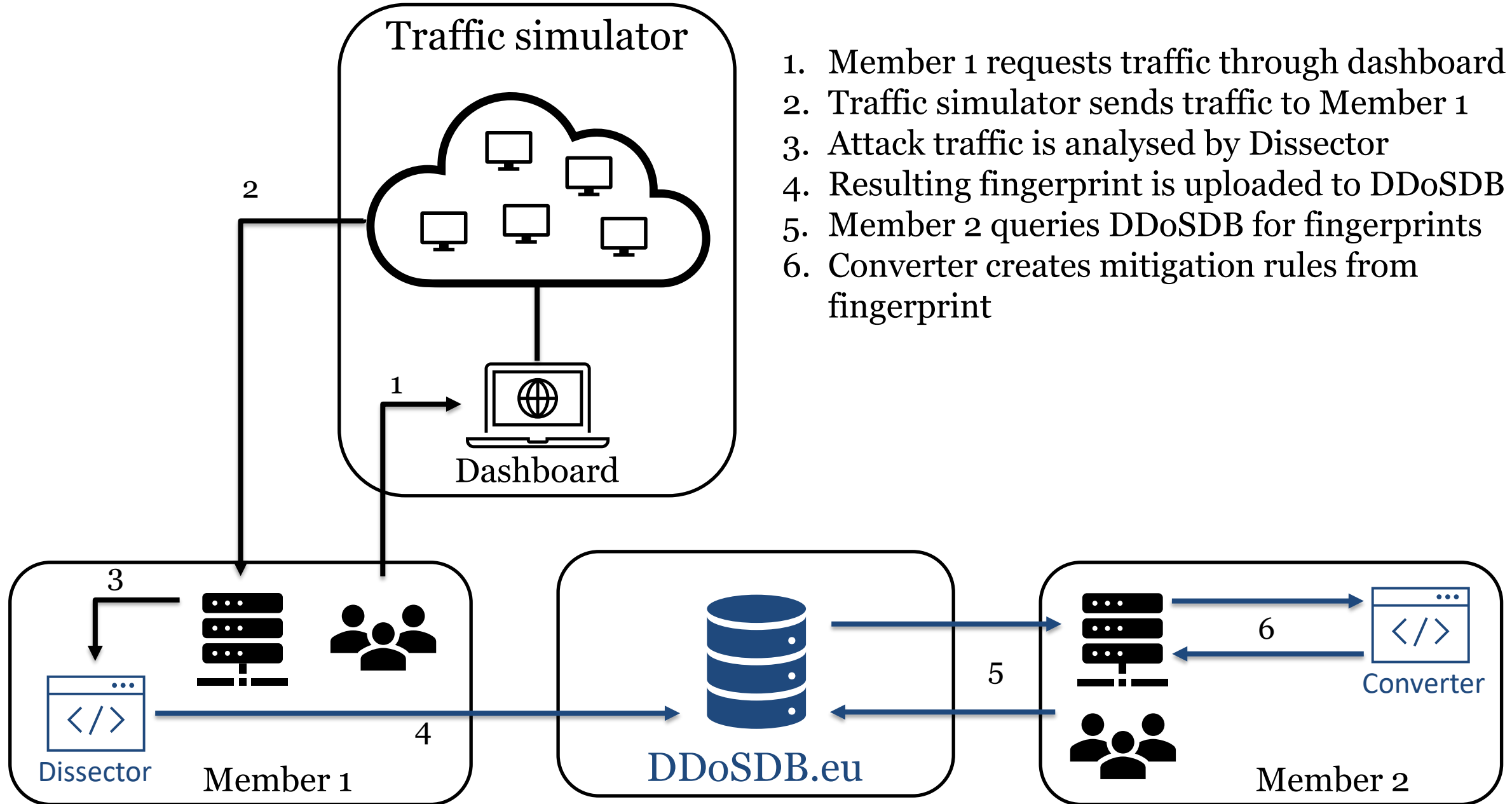
Converter



Dissector

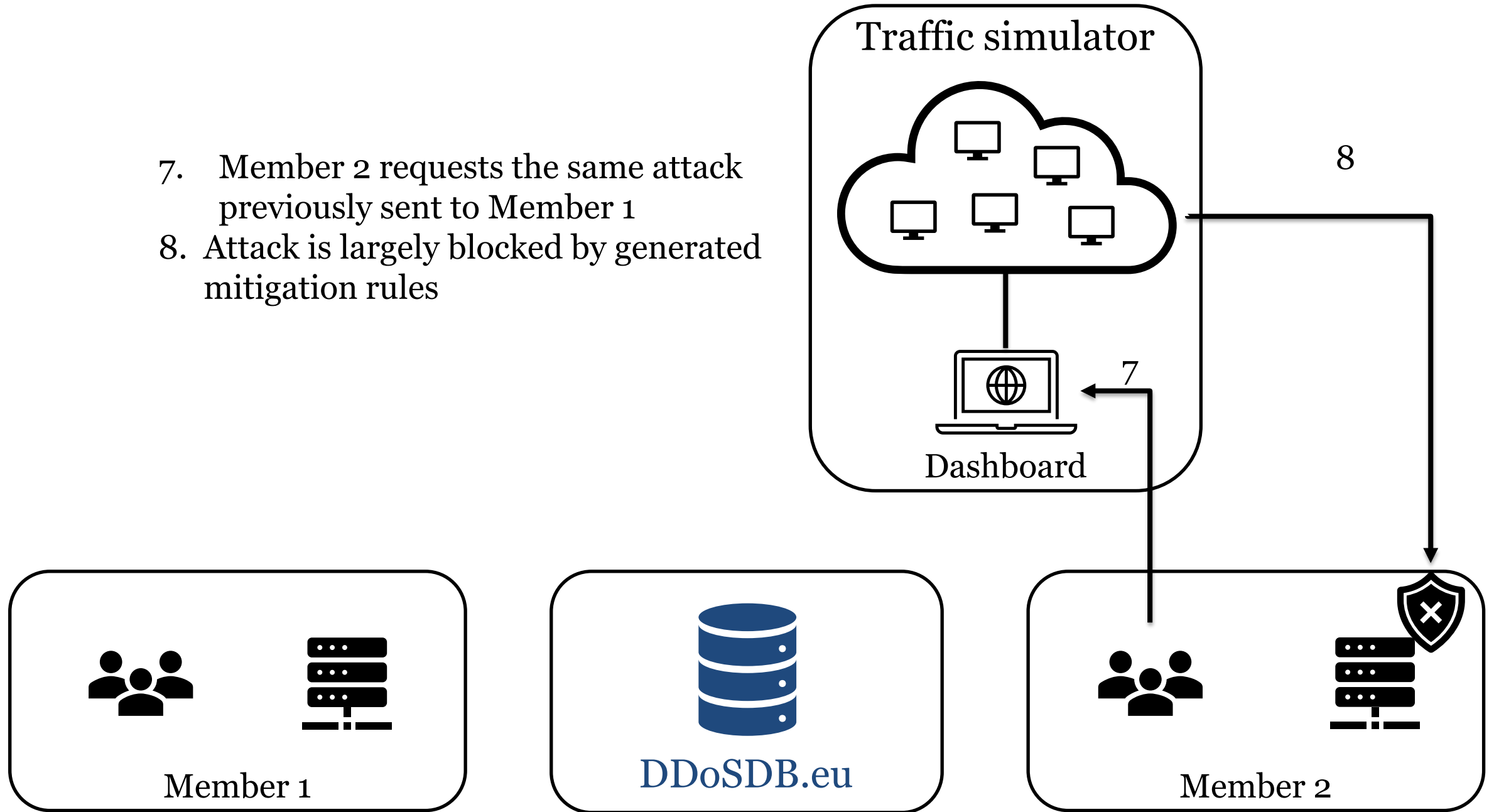


DDoS DB



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 a 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

Next

- Fragment packets
- More fragments flag
- No more fragments flag
- SYN flag
- ACK flag
- FIN flag

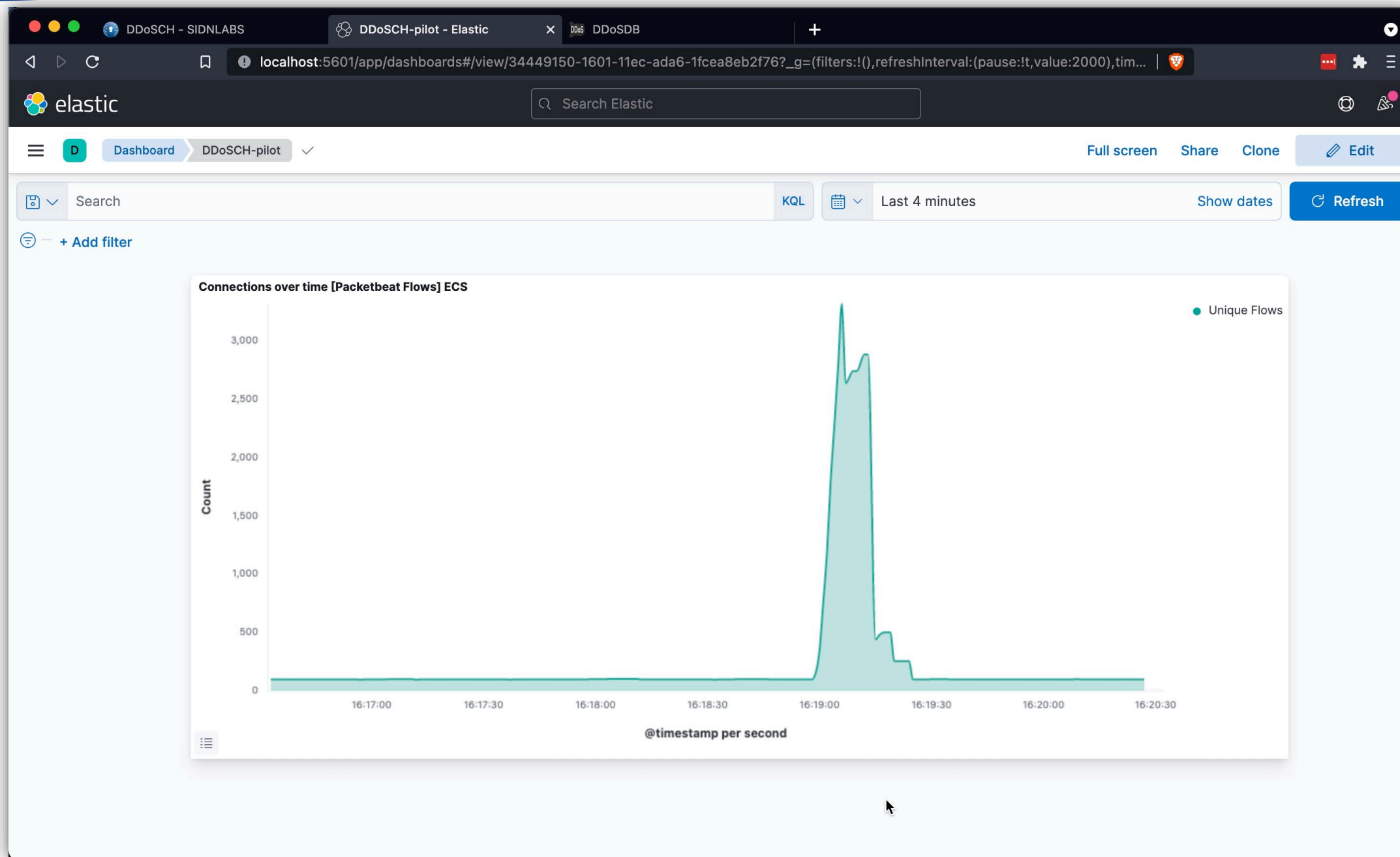
Stop traffic

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 — 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 (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 line graph over time, with the x-axis labeled '@timestamp per second' and the y-axis representing the number of unique flows. The x-axis has time markers from 08:12:30 to 08:16:00.

Success!



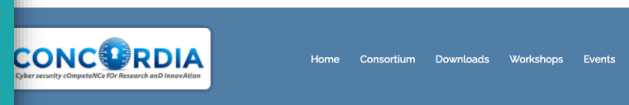
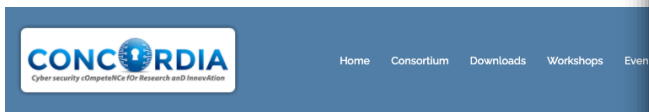


More content online:

sidnlabs.nl

nomoreddos.org

github.com/ddos-clearing-house



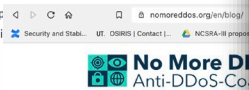
POSTED APRIL 9, 2020 ADMIN CONCORDIA

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.

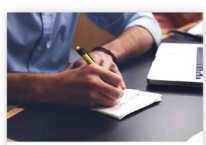
Note: we're using two types of reference in this blog series: hyperlinks for information, while numbers between straight brackets ([]) link to other papers.



DDoS attack landscape

A Distributed Denial-of-Service (DDoS) attack overwhelms a network with network the ability to service legitimate requests from their clients. 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

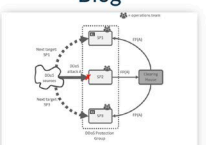
Blog



Dutch Anti-DDoS Coalition: lessons learned and the way forward
24 March 2020

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

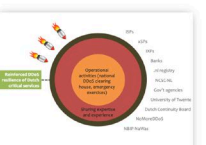
[Read More](#)



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](#)



Wednesday 11 October 2021
Article by: Thijs van den Heuvel, Remco Poortinga van Wijnen, Cristian Hesselman, Christa Papachristos, de 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.



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 identifying attack techniques, indicators of compromise, and real-world datasets.



The two cross-sector pillars of the "House for Europe" are the platform, which conceptually is related to threat intelligence.

We are developing the CONCORDIA platform for threat intelligence.

- Multi-source: the platform combines different data management systems and reported hotspots.
- Combine datasets: the platform combines different data management systems and reported hotspots.



youtu.be/UwRB74kbn8