CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe

Online meetup @ ABNAMRO Bank

May 7, 2021

Cristian Hesselman

(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.

DDoS clearing house in the Netherlands

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

No More DDoS
Anti-DDoS-Coalitie

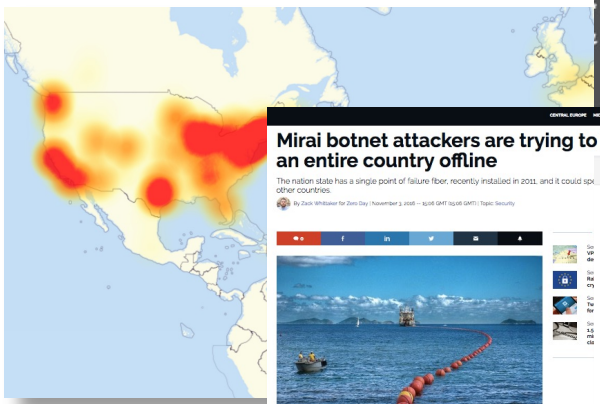
- DDoS clearing house R&D
- DDoS clearing house cookbook
- Technical evaluation through pilots in the Netherlands and Italy

- Sharing of operational experience
- Large-scale multi-party DDoS drills
- DDoS clearing house operations
- Operational ADC organization

CONCORDIA is funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/

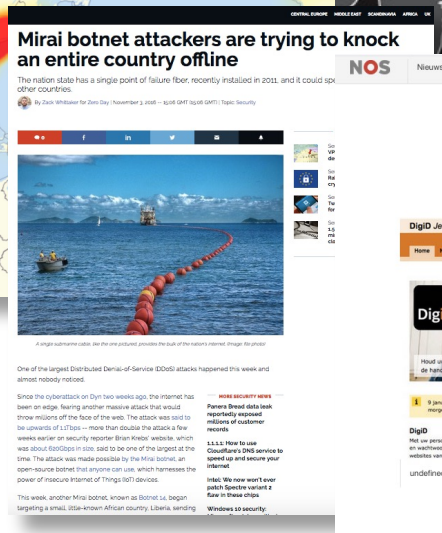
High-impact DDoS Examples

Mirai botnet, 2016



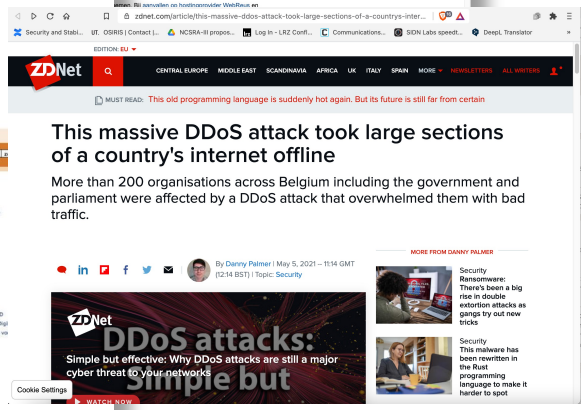
Estonia, 2007

The Netherlands, September 2020



Liberia, 2016

The Netherlands, January 2018



Belgium, May 2021

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

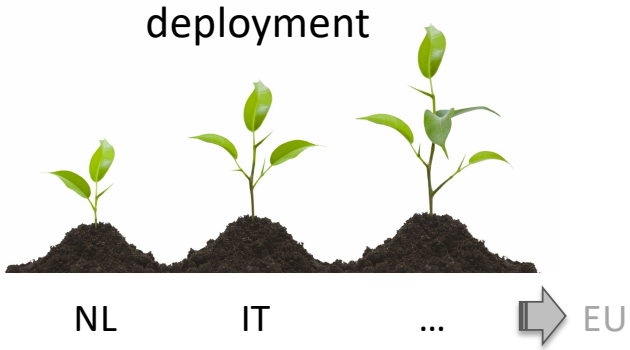
Objective

- Pilot a DDoS Clearing House with European industry for Europe to proactively and collaboratively protect European critical infrastructure against DDoS attacks

- Learn how to bridge **multidisciplinary gap** to deployment, more than tech!

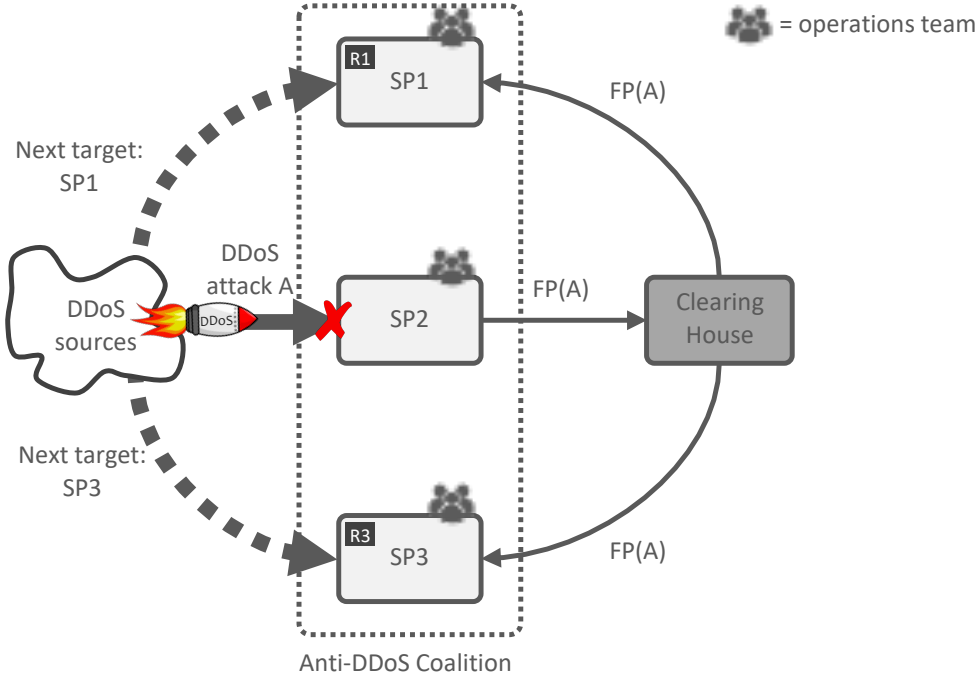
- Key outputs: **pilots** in NL >> IT, DDoS clearing house **blueprint**

Key challenge: increase to TRL 5-7 and grow deployment



DDoS Clearing House Concept

- Continuous and automatic sharing of “DDoS fingerprints”, buys providers time (proactive)
- Extends DDoS protection services that critical service providers use and does not replace them
- Generic concept: across sectors, Member States, business units, etc.



Fingerprint Example


```
{
  "attack_vector": [
      "src_ips": [
        ommited;
      ],
      "attack_vector_key": "66f2e83fde0e6351d3f5ad967c6230aa3b60dbc498ad13b074296cb5f84c7734",
      "one_line_fingerprint": "{'dns_qry_type': 1, 'ip_proto': 'UDP',
      'highest_protocol': 'DNS', 'dns_qry_name': 'a.packetdevil.com',
      'frame_len': 1514, 'udp_length': 4103, 'srcport': 53,
      'fragmentation': True, 'src_ips': 'omitted'}"
    }
  ],
  "start_time": "2013-08-14 23:04:00",
  "duration_sec": 0.16,
  "total_dst_ports": 4649,
  "avg_bps": 143426993,
  "total_packets": 16471,
  "ddos_attack_key": "44518107642b9ac7098174a16cbf220395c862bf26389c734e0b109b318e9291",
  "key": "44518107642b9ac",
  "total_ips": 2065,
  "tags": [
    "AMPLIFICATION",
    "DNS",
    "FRAGMENTATION",
    "UDP_SUSPECT_LENGTH",
    "DNS_QUERY",
    "SINGLE_VECTOR_ATTACK"
  ]
}
```

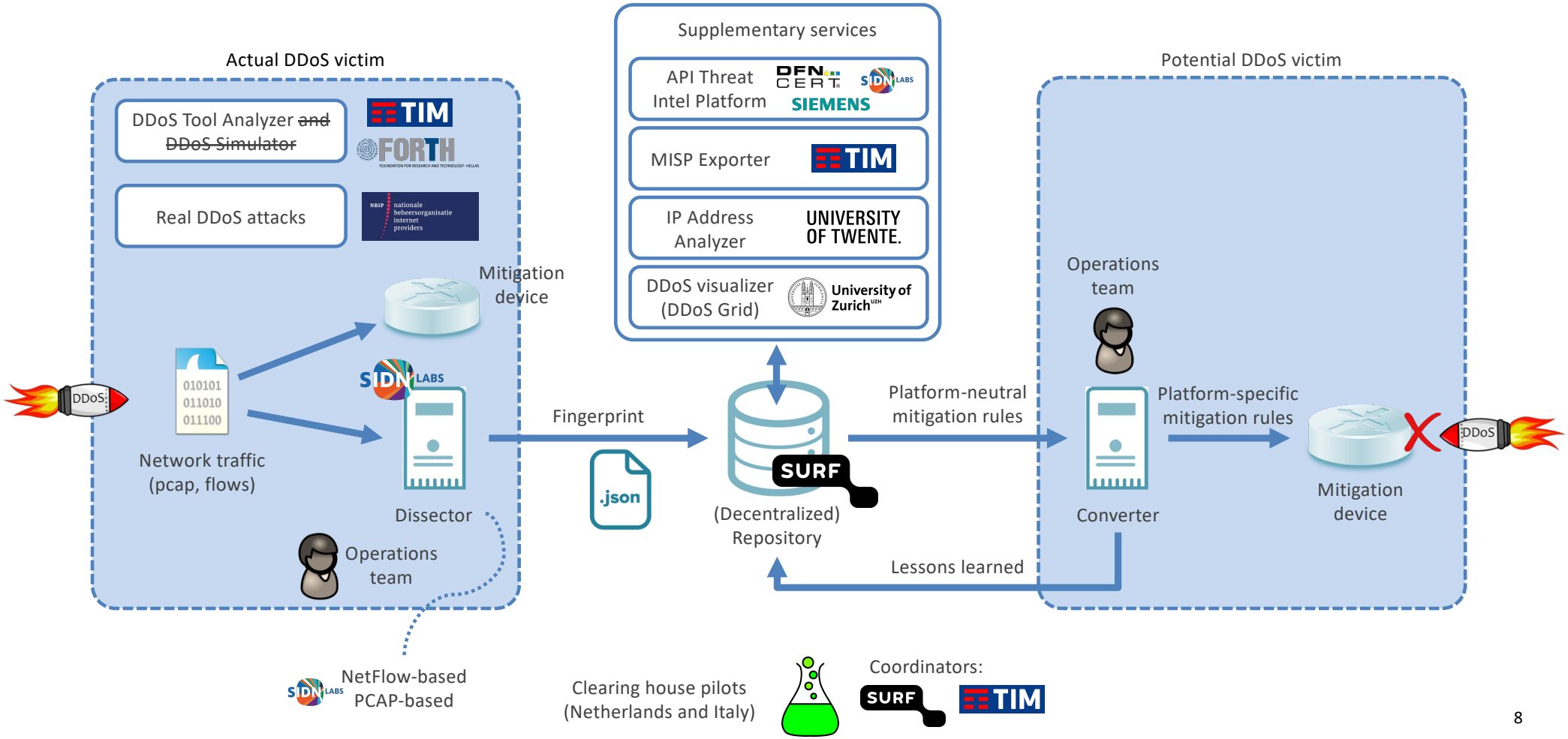
Clearing House increases Digital Autonomy

- Increased **insight** of potential victims into DDoS attacks from their own narrow view to an ecosystem-wide view

- Increased **control** because the new DDoS insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party)

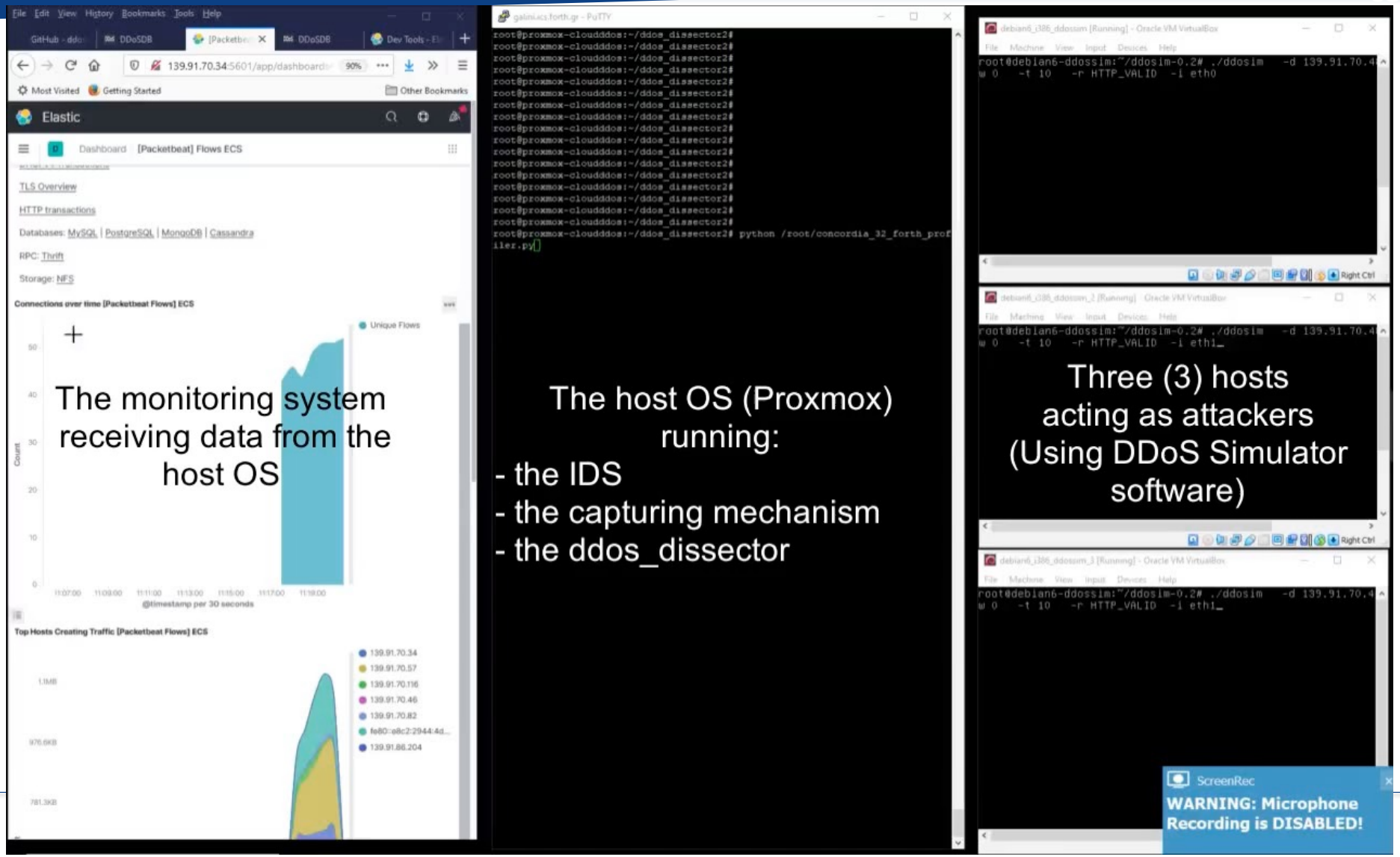
- ADCs also build up a joint **pool of expertise** independent of particular DDoS mitigation providers through drills and best common practices

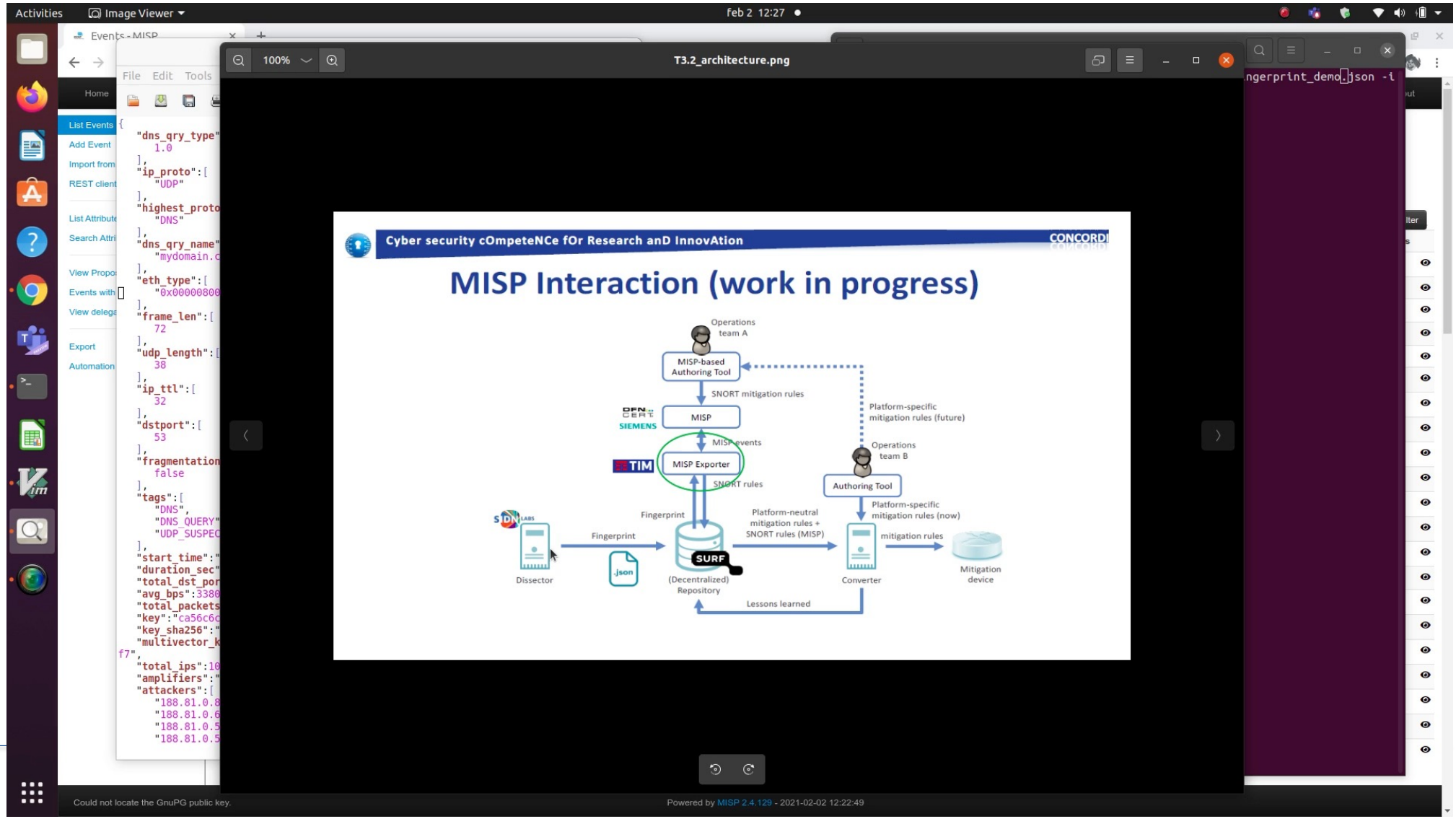
Main Components and Data Flows



Fingerprint generation, storage, enrichment

https://www.youtube.com/watch?feature=oembed&v=1QlC3SwwYAU


The monitoring system receiving data from the host OS
The host OS (Proxmox) running:
- the IDS
- the capturing mechanism
- the ddos_dissector
Three (3) hosts acting as attackers (Using DDoS Simulator software)
ScreenRec
WARNING: Microphone Recording is DISABLED!


Activities
Image Viewer
feb 2 12:27
Events - MISP
File Edit Tools
Home
List Events
Add Event
Import from
REST client
List Attribute
Search Attri
View Propo
Events with
View delega
Export
Automation
"dns_qry_type"
1.0
"ip_proto":[
"UDP"
"highest_proto
"DNS"
"dns_qry_name"
"mydomain.c
"eth_type":[
"0x00000800
"frame_len":[
72
"udp_length":[
38
"ip_ttl":[
32
"dstport":[
53
"fragmentation
false
"tags":[
"DNS",
"DNS_QUERY"
"UDP_SUSPEC
"start_time":"
"duration_sec"
"total_dst_por
"avg_bps":3380
"total_packets
"key":"ca56c6c
"key_sha256":"
"multivector_k
f7",
"total_ips":10
"amplifiers":"
"attackers":[
"188.81.0.8
"188.81.0.6
"188.81.0.5
"188.81.0.5
100%
T3.2_architecture.png
ngerprint_demo.json -i
Cyber security cOmpeteNCe fOr Research anD InnovAtion
CONCORDI
MISP Interaction (work in progress)
Operations team A
MISP-based Authoring Tool
SNORT mitigation rules
MISP
SIEMENS
Platform-specific mitigation rules (future)
MISP events
Operations team B
TIM
MISP Exporter
SNORT rules
Authoring Tool
Platform-specific mitigation rules (now)
Fingerprint
Platform-neutral mitigation rules + SNORT rules (MISP)
Fingerprint
mitigation rules
SURF
.json
Dissector
(Decentralized) Repository
Converter
Mitigation device
Lessons learned
Could not locate the GnuPG public key.
Powered by MISP 2.4.129 - 2021-02-02 12:22:49

Demo: DDoS Grid (01:17)

jan@tpj: ~/ddos_dissector

jan@tpj: ~ | jan@tpj: ~/ddos_dissector

```
λ tpj ddos_dissector → λ git 3.0* → ./ddos_dissector.py -f ./
pcap_samples/sample3.pcap  --upload --host https://www.csg.uz
h.ch/ddosgrid/ddosdb/ --user jan --passwd gg
```

Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

Private Browsing

Search with Google or enter address

Firefox

Search the Web

You're in a Private Window

Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

Need more privacy?

Try Mozilla VPN

Oct 7 11:42

Demo: IP Address Analyzer (02:08)

ddosdb@ddosdb: ~/.ddosdb/ip_analyzer/src

File Edit View Search Terminal Help

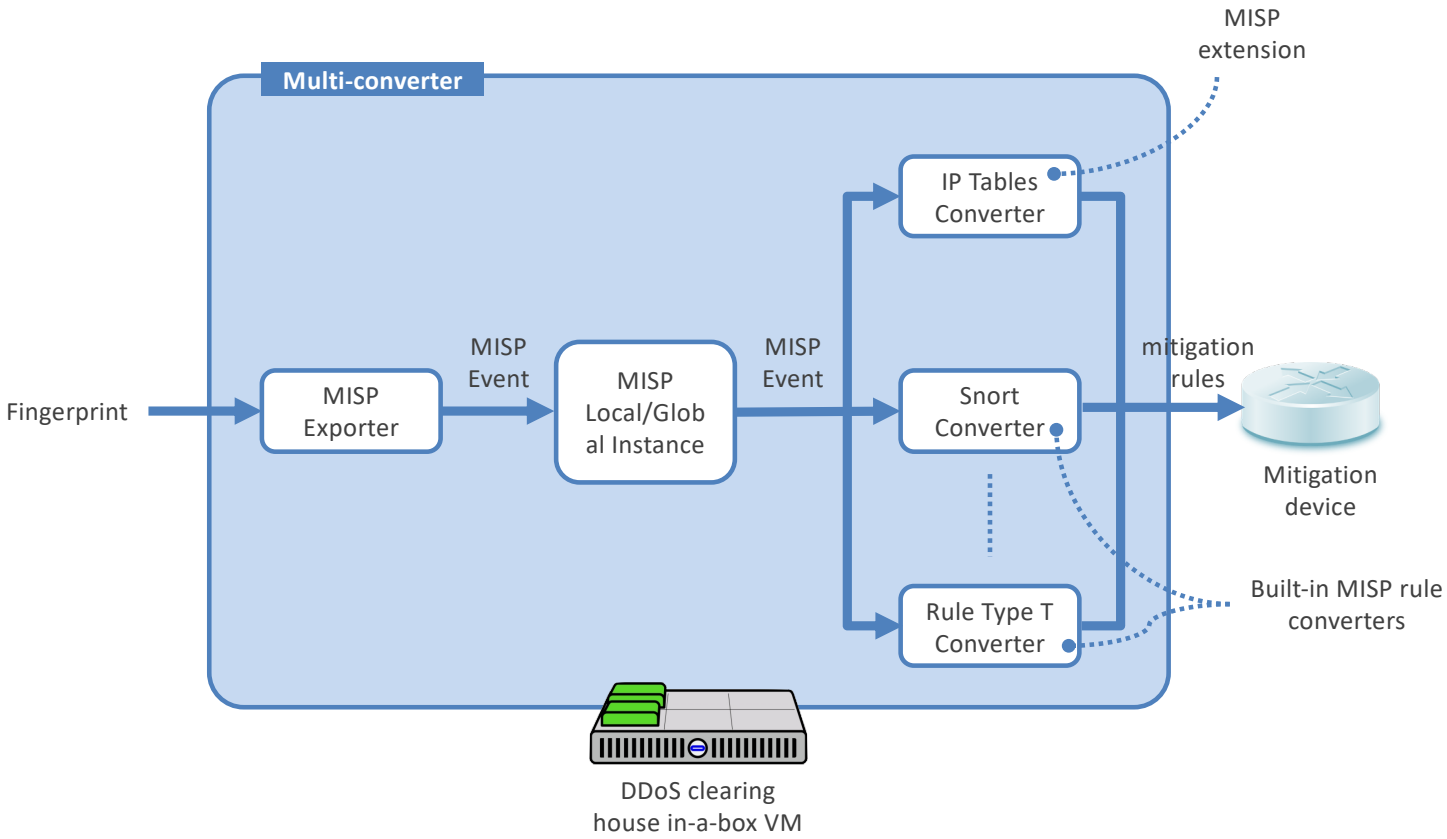
```
ddosdb@ddosdb:~/.ddosdb/ip_analyzer/src$
```

ddosdb@ddosdb: ~/.ddosdb/ddos_dissector/fingerprints

File Edit View Search Terminal Help

```
ddosdb@ddosdb:~/.ddosdb/ddos_dissector/fingerprints$
```

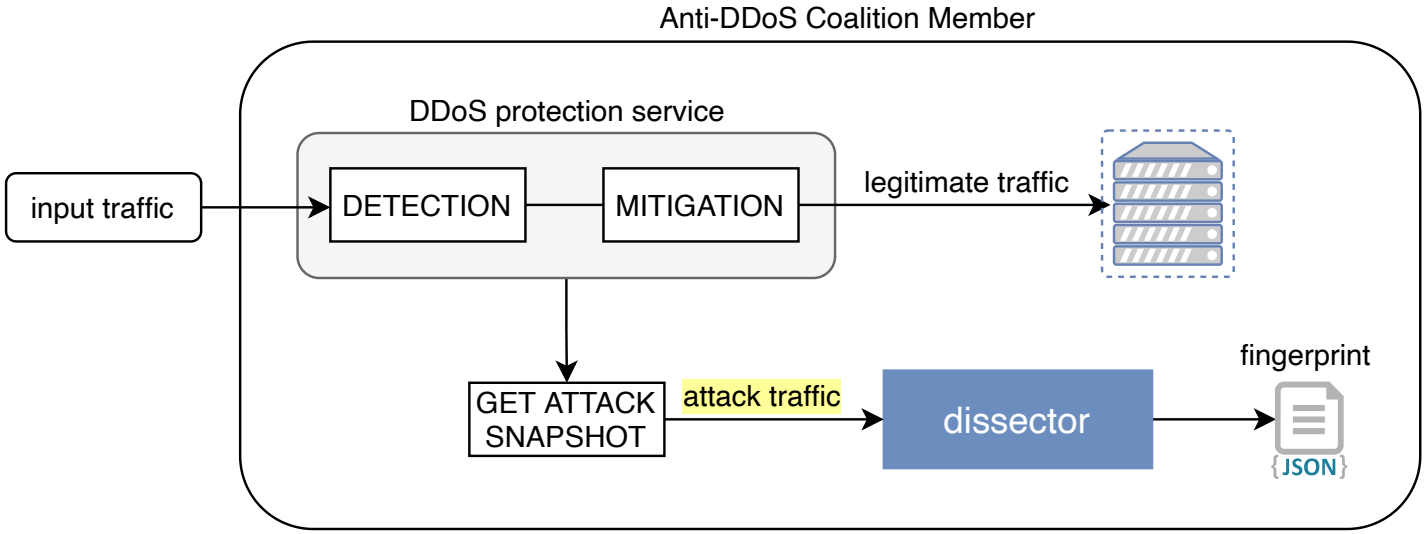
Multi-converter



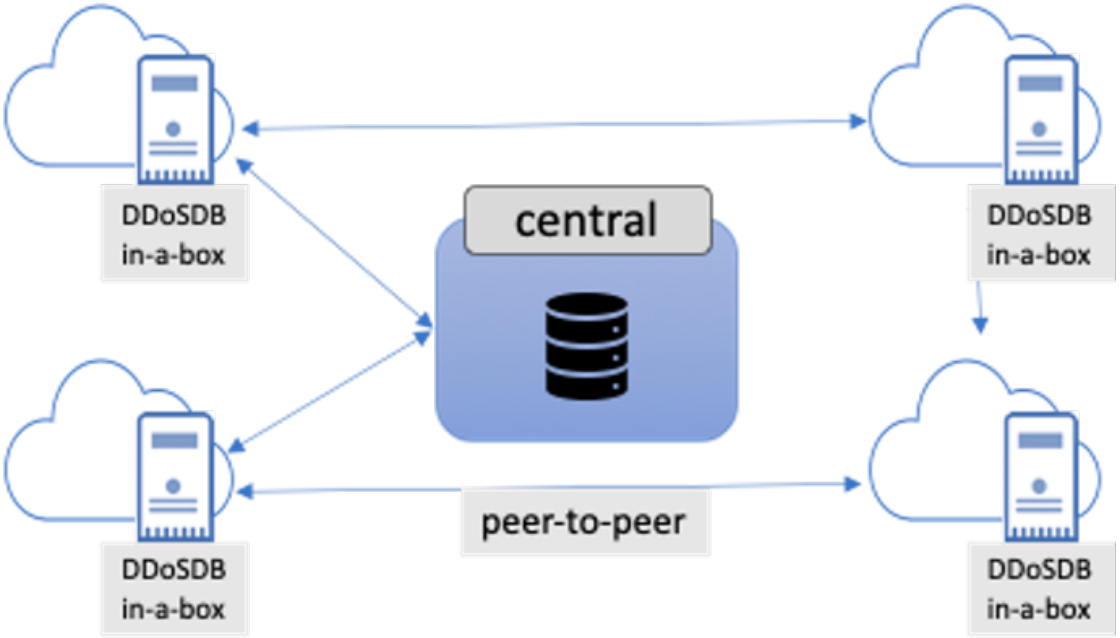
Component Maturity Indication

Name	Function	Maturity
Dissector	Generate DDoS fingerprints based on PCAP files and flows data	High
DDoSDB	Insert, update, search, and retrieve DDoS fingerprints	High
Converter	Generate mitigation rules based on DDoS fingerprints	Medium
DDoS Grid	Dashboard for the visualization of DDoS fingerprints	High
IP Address Analyzer	Enriches fingerprints with details about IP addresses involved in an attack, based on measurements	Low
DDoS Tool Analyzer	Generate DDoS fingerprints of tools used to launch DDoS attacks	Low
MISP Exporter	Generate MISP events based on DDoS fingerprints	Medium

Dissector deployment models



DDoS-DB deployment model



Outlook 2021

- Couple with **production systems** of partners in the Dutch ADC, initially at our partner NBIP (Dutch ADC)

- Further **mature the clearing house's components**, such as
  - Extend the Dissector with additional fingerprint generation modules
  - Develop a MISP extension for authoring and distributing DDoS filtering rules

- First published version of the DDoS clearing house **cookbook** (e.g., as a paper for the Journal on Internet Services and Applications)

Details in D3.2, "2nd year report on community building and sustainability", Dec 2020

Dutch National Anti-DDoS Coalition

Betaalvereniging Nederland

SURF
CONCORDIA partner

VNO NCW

SIDN
CONCORDIA partner

NBIP NaWas

UNIVERSITY OF TWENTE.
CONCORDIA partner

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

amsix

DeNederlandscheBank
EUROSYSTEEM

vodafone ziggo

POLITIE

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Belastingdienst

NLIX
The Interconnect Exchange

kpn

DINL
Stichting Digitale Infrastructuur Nederland

Status Dutch Anti-DDoS Coalition

- Members committed to a more sustainable model (Dec 2020)
- Approved fee-based budget (EUR 114K total)
- Structure of WGs, **clearing house** operator and software developer
- Consortium agreement under development
- Core team governing the Dutch ADC

No More DDoS
Anti-DDoS-Coalitie

DDoS Clearing House Planning @Dutch ADC

- Phase 0: pilot, March through ~July 2021
  - Development by CONCORDIA T3.2 team
  - Operations with CONCORDIA and Dutch ADC partners

- Phase 1: basic production, July 2021 through ~Dec 2021
  - Development by CONCORDIA T3.2 team
  - Operations with Dutch ADC partners

- Phase 2: full production, Jan 2022 and onward
  - Development and operations with Dutch ADC partners

Phase 0 (Pilot)

- Operations
  - 3+ partners use Dissector in their networks and share fingerprints ◉◉
  - Initial set of fingerprints in ddosdb.nl ◉
  - SIDN Labs is the DDoS-DB operator ◉◉
  - Data sharing based on existing agreement with SIDN ◉

- Development
  - Further improved clearing house software ◉
  - BCOP to connect ADC members and operate the clearing house ◉◉
  - BCOP and other learnings captured in DDoS clearing house cookbook ◉

◉ CONCORDIA T3.2 responsibility ◉ Dutch ADC responsibility

Phase 1 (Basic Production)

- Operations
  - NBIP is the DDoS-DB operator (to be OK'ed by Dutch ADC members) ◉
  - Additional ADC members connected ◉

- Development
  - CONCORDIA s/w updates regularly transitioned into production ◉◉
  - DDoS clearing house cookbook updated ◉
  - Contracted software company to replace CONCORDIA T3.2 in phase 2 ◉

◉ CONCORDIA T3.2 responsibility ◉ Dutch ADC responsibility

Phase 2 (Full Production)

- Operations
  - NBIP is the DDoS-DB operator (see Phase 1)
  - Additional ADC members connected (continued from Phase 1)

- Development
  - Software development company improves s/w (open source)
  - DDoS clearing house cookbook updated
  - CONCORDIA T3.2 focuses on development for pilot in Italy

CONCORDIA T3.2 responsibility Dutch ADC responsibility

Outlook 2022 (project end)

- Pilot in the Netherlands: 3+ member organizations of the Dutch ADC sharing fingerprints (inter-organization)

No More DDoS
Anti-DDoS-Coalitie

- Pilot in Italy: 3+ TI departments sharing fingerprints (intra-organization)
  - Security Lab, internal SOC, anti-DDoS team
  - Optionally with other orgs in Italy (e.g., universities)

TIM

- Cookbook and tech report combined in a peer-reviewed paper

Further reading

https://www.sidnlabs.nl/en/news-and-blogs/new-ddos-classifiers-for-the-ddos-clearing-house

https://www.sidnlabs.nl/en/news-and-blogs/work-in-progress-the-concordia-platform-for-threat-intelligence

https://www.sidnlabs.nl/en/news-and-blogs/new-version-of-the-ddos-clearing-house-core-components

https://www.sidnlabs.nl/en/news-and-blogs/dutch-anti-ddos-coalition-lessons-learned-and-the-way-forward

https://www.sidnlabs.nl/en/news-and-blogs/setting-up-a-national-ddos-clearing-house

https://www.sidnlabs.nl/en/news-and-blogs/increasing-the-netherlands-ddos-resilience-together

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020

Dutch Anti-DDoS Coalition:
https://www.nomoreddos.org/en/

Clearing house on GitHub:
https://github.com/ddos-clearing-house/

Cristian Hesselman (T3.2 lead)
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

This work was funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: https://www.concordia-h2020.eu/