DDoS Clearing House for Europe

ICANN71 vTechDay

June 14, 2021

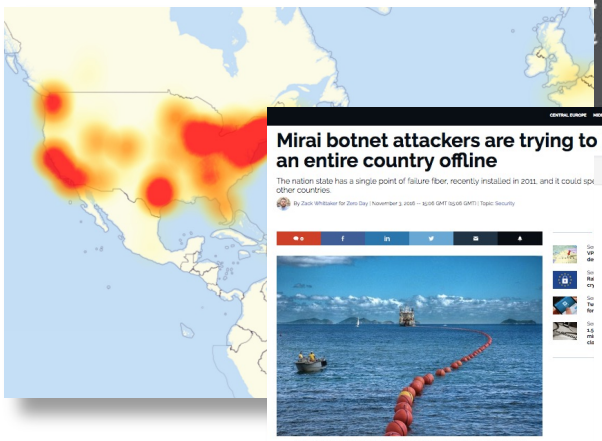
Cristian Hesselman
(SIDN Labs)

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.

High-impact DDoS Examples

Mirai botnet, 2016



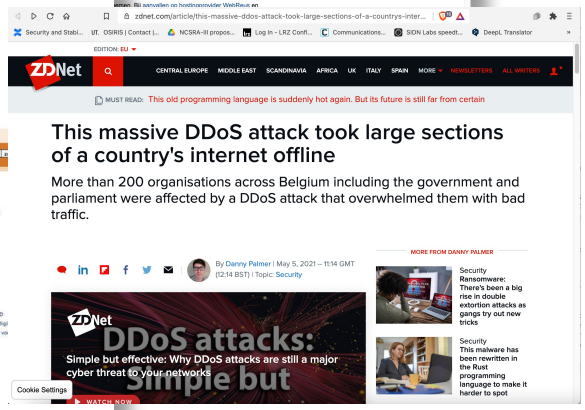
Liberia, 2016

Estonia, 2007

The Netherlands, January 2018

The Netherlands, September 2020

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

- Enable European critical infrastructure to proactively and collaboratively protect themselves against DDoS attacks

- Pilot a DDoS Clearing House with European industry for Europe that can also be used elsewhere

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

- Key outputs: pilots in the Netherlands and Italy, DDoS clearing house blueprint

Key innovations

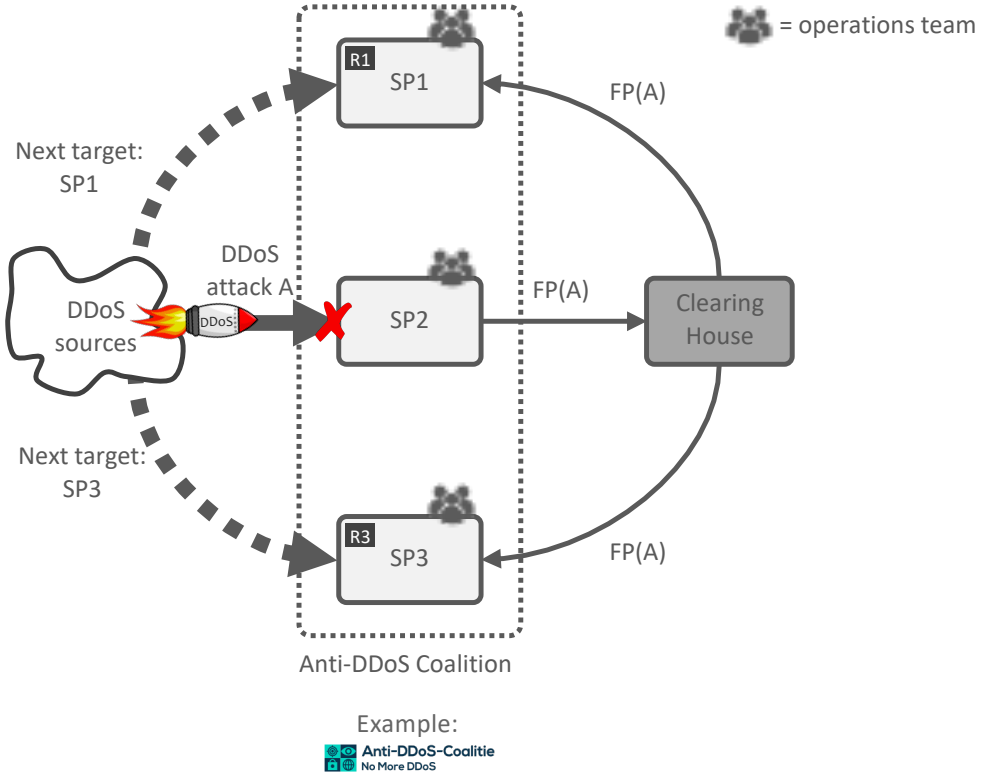
- Bridge **multidisciplinary gap** to deployment, more than tech!

- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, experiences, lessons learned
  - Main use case is Dutch Anti-DDoS Coalition
  - Enable other groups of organizations to set up their clearing house

- Can operate across **heterogeneous networks**

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"
  ]
}
```

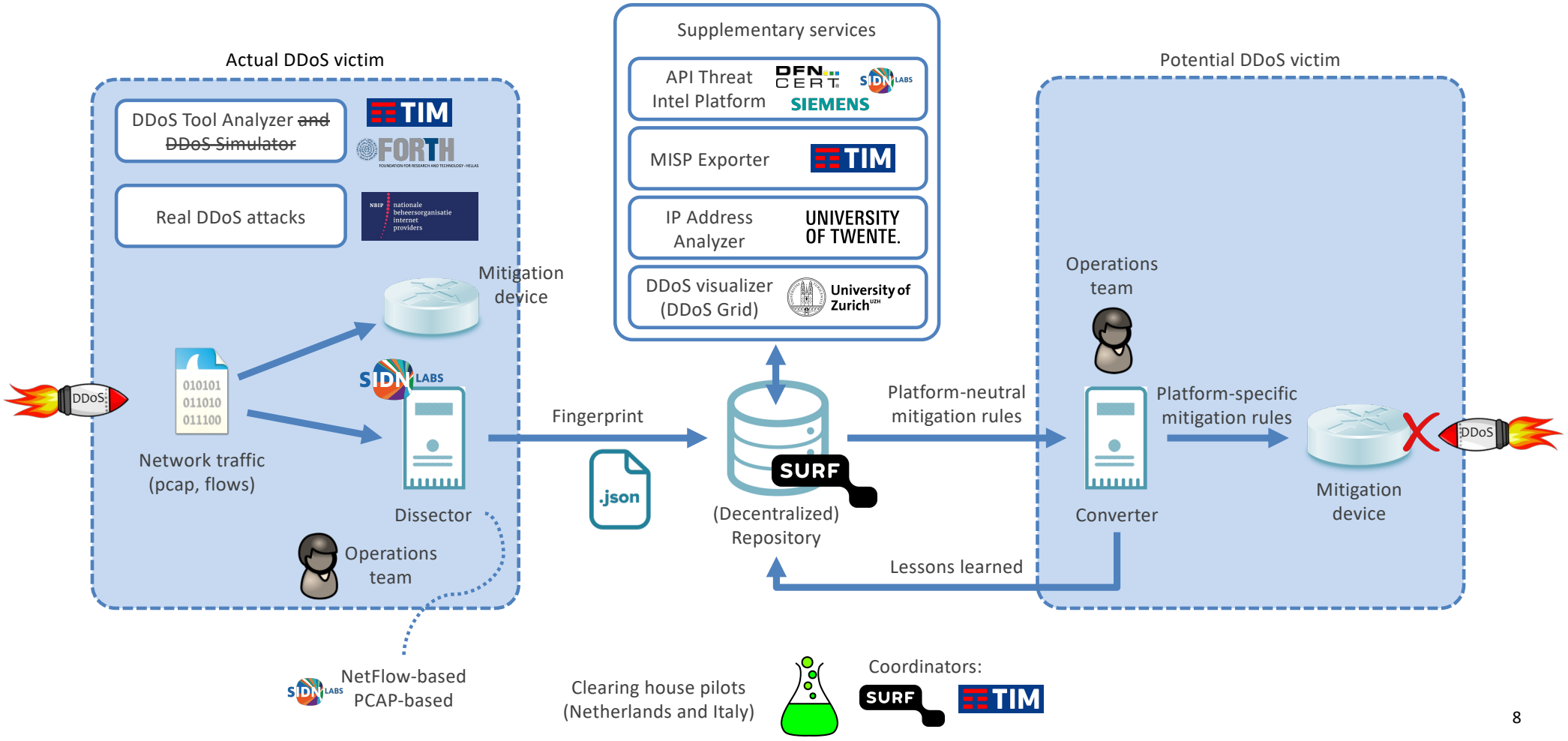
Clearing House increases Digital Autonomy

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

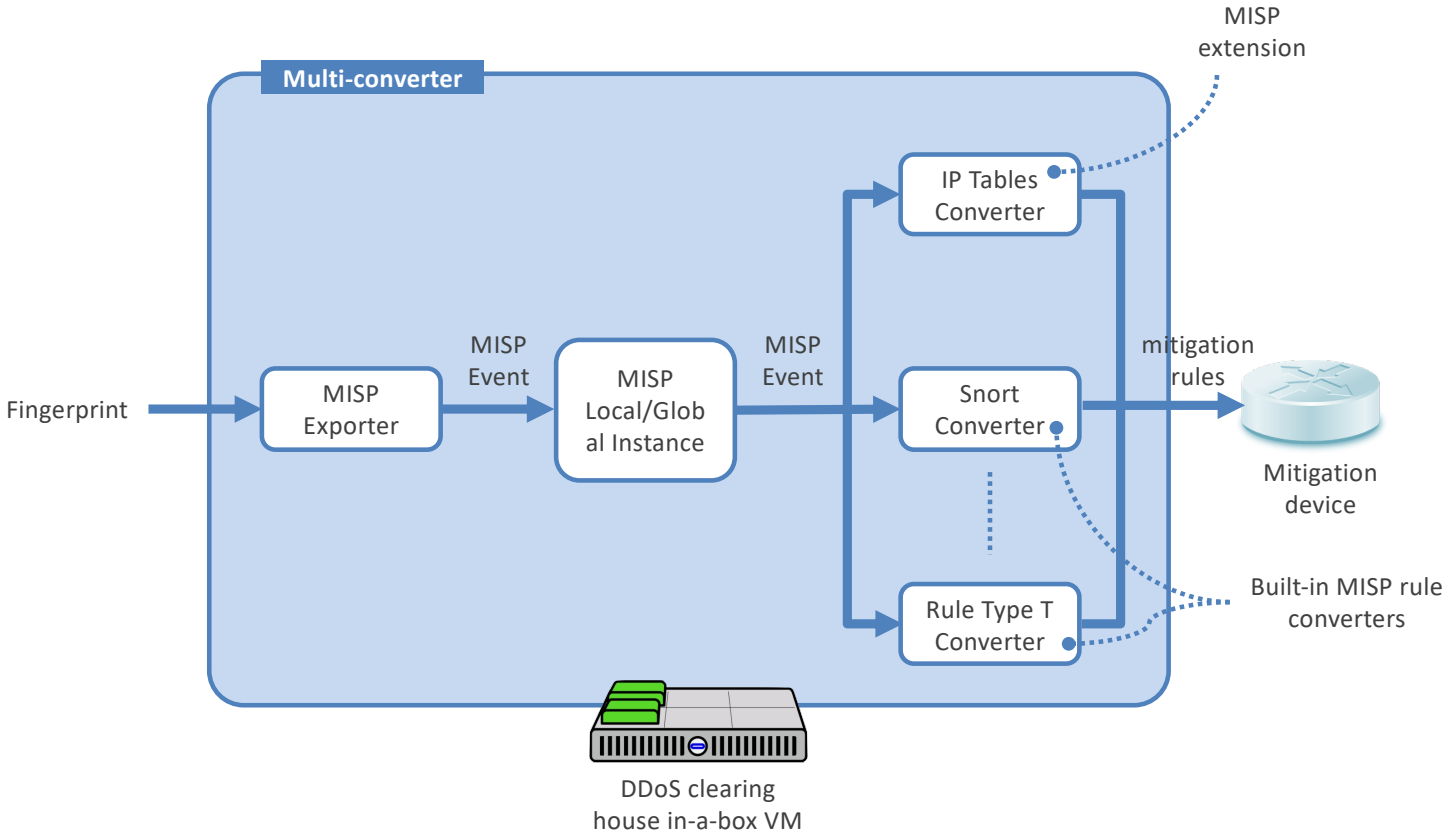
- Increased **control** because the new DDoS insights give organizations more grip on how to handle DDoS attacks and the requirements for their DDoS mitigation facilities (their own or those of a contracted third party)

- 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

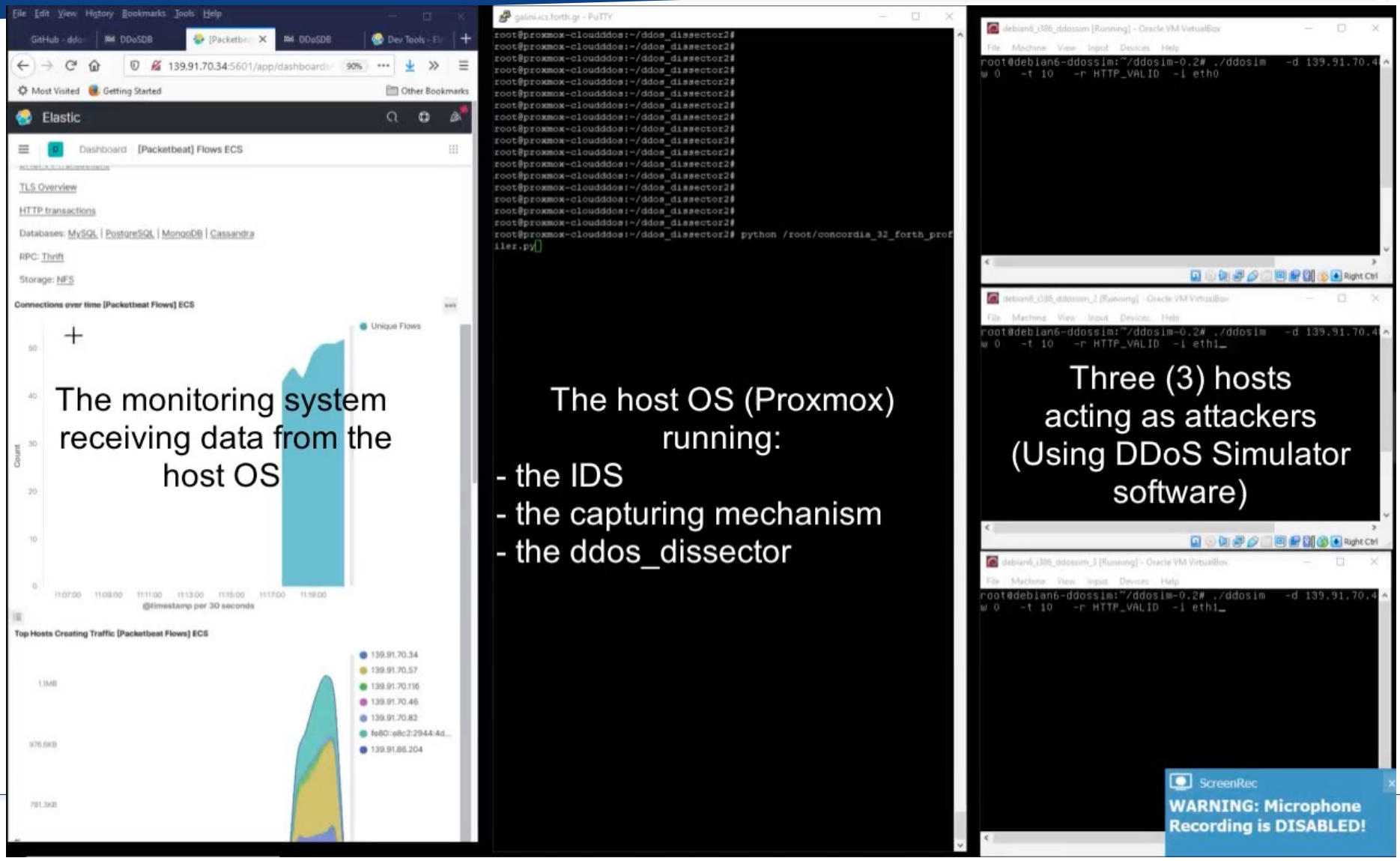


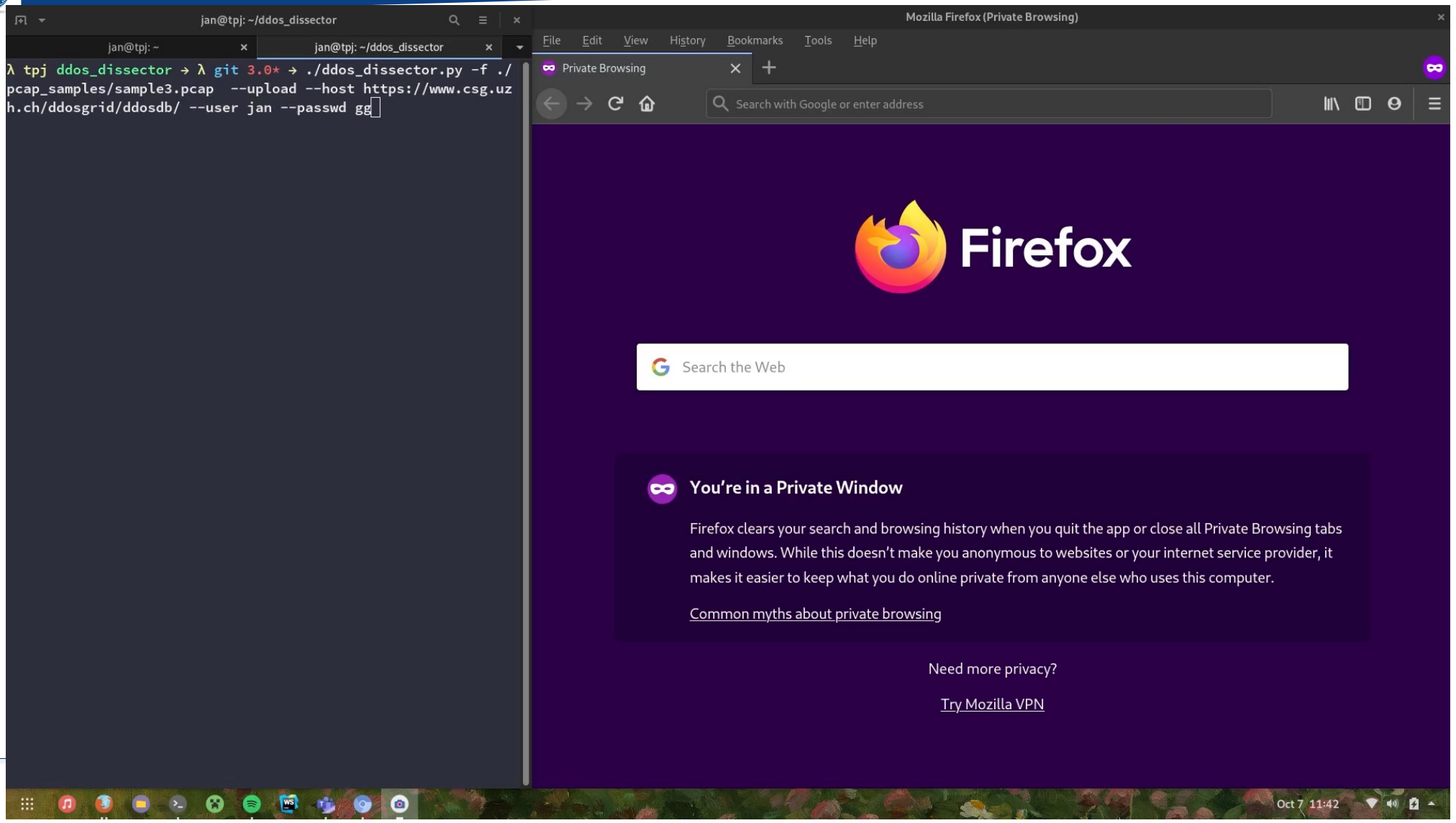
Multi-converter



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


Elastic
Dashboard [Packetbeat] Flows ECS
TLS Overview
HTTP transactions
Databases: MySQL | PostgreSQL | MongoDB | Cassandra
RPC: Thrift
Storage: NFS
Connections over time [Packetbeat Flows] ECS
Unique Flows
@timestamp per 30 seconds
Top Hosts Creating Traffic [Packetbeat Flows] ECS
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!


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.uzh.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

DDoS clearing house in the Netherlands

- 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/

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

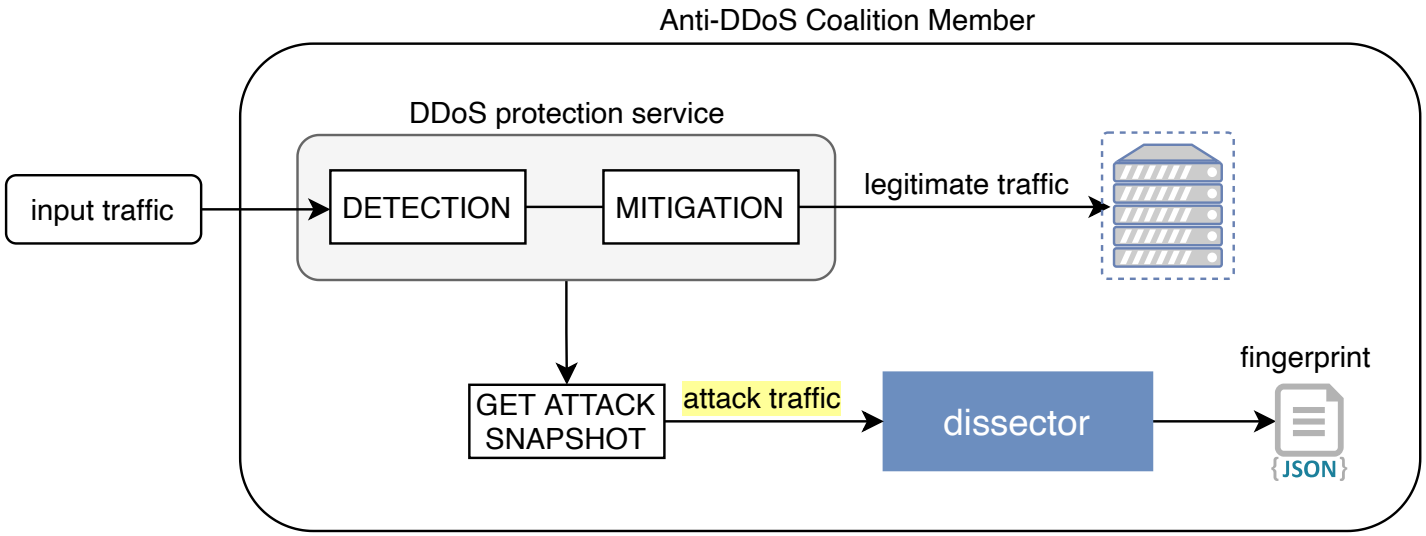
Anti-DDoS-Coalitie
No More DDoS

- Core team governing the Dutch ADC

DDoS Clearing House Planning @Dutch ADC

- Phase 0: pilot, Q2 and Q3 2021
  - Development by CONCORDIA T3.2 team
  - Operations with CONCORDIA and Dutch ADC partners
- Phase 1: basic production, Q4 2021
  - Development by CONCORDIA T3.2 team
  - Operations with Dutch ADC partners
- Phase 2: full production, Q1 2022 and onward
  - Development and operations with Dutch ADC partners

Key challenge: deployment in networks



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)

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
cristian.hesselman@sidn.nl
@hesselma
+31 6 25 07 87 33

Thijs van den Hout
thijs.vandenhout@sidn.nl
@thijsvandenhout

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/