



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





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



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 stop other countries.

By Zach Whitaker for Zero Day, November 3, 2016 - 10:08 GMT (10:08 GMT) Topic: Security

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 operated by L33700 - made that double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 400,000 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 2.0, began targeting a small, little-known African country, Liberia, sending

More Security News

- Parsons Broad data leak reportedly exposed millions of customer records
- LLN: How to use Cloudflare's DNS service to speed up and secure your internet
- Intel: We now won't ever patch Spectre variant 2
- Windows 10 security...

Liberia, 2016

Estonia, 2007



Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

DigiD de eigen inlogcode voor de hele overheid

Home Nieuws Over DigiD Mactingen Veiligheid Waag en erandoer

DigiD activeren
Machtiging regelen
Inloggen Mijn DigiD

Handige links

- Wachtwoord vergeten?
- Wachtwoord opnieuw opzetten?
- Herstellcode ontbreken?

Laatste nieuws

- Wachttijd voor e-mails DigiD
- Wachttijden in nieuw versie DigiD
- Is uw computer nu geschikt om

9 januari 2013 - DigiD is op dit moment niet beschikbaar. Naar verwachting komt u morgenochtend weer gebruikmaken van DigiD. Deze excuses voor het ongemak.

DigiD Het is uw persoonlijke DigiD (een gebruikersnaam en wachtwoord) wordt u ook identificeert op websites en de website van een organisatie die

Waar u kunt inloggen U kunt uw DigiD gebruiken bij ruim 500 organisaties.

undefind aap

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

Opnieuw vinden grootschalige ddoS-aanvallen op Nederlandse providers plaats

Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddoS-aanvallen. Dit is het grootste in omvang te worden en ook ruimelijk georganiseerd te zijn. Onder andere Sigmet, Calway en Delta zijn dinsdag slachtoffer.

De ddoS-aanvallen vinden onder andere plaats bij Calway, Delta, Sigmet, Calway, Delta, Sigmet, Calway en Delta zijn dinsdag slachtoffer. Eerder op donsdagochtend had provider Delta (01.01.01.01.01.01) de werkdag voorstaat door een ddoS-aanval. Verder wordt er dinsdagmiddag een grote aanval plaats op Sigmet. Dit is een tip die de infrastructuur voor veel kleine providers versorgt. Dit betreft Sigmet infrastructuur voor TransIP. Daar hadden klanten verwachting om uitgesteld door de aanval, al zijn die inmiddels opgevoerd.

Het lijkt erop dat het om dezelfde aanvallen gaat als die vorig week Nederlandse providers troffen, al is dat niet met zekerheid te zeggen. Volgens een woordvoerder van het NISII gaat het voornamelijk om drie applicatie- en top-aanvallen. Het Nederlands Belastingagentschap (Belastingdienst) bevestigt de applicatie- en top-aanvallen. Het NISII heeft ook bevestigd dat er een ddoS-aanval is geweest op de infrastructuur van de providers. Het NISII heeft ook bevestigd dat er een ddoS-aanval is geweest op de infrastructuur van de providers.

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.

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

Security Researchers: There's been a big rise in double extortion attacks as gangs try out new tricks

Security This malware has been rewritten in the Rust programming language to make it harder to spot

Belgium, May 2021

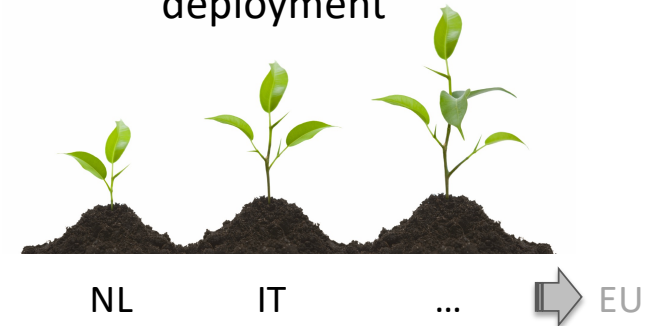


Objective

- 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**



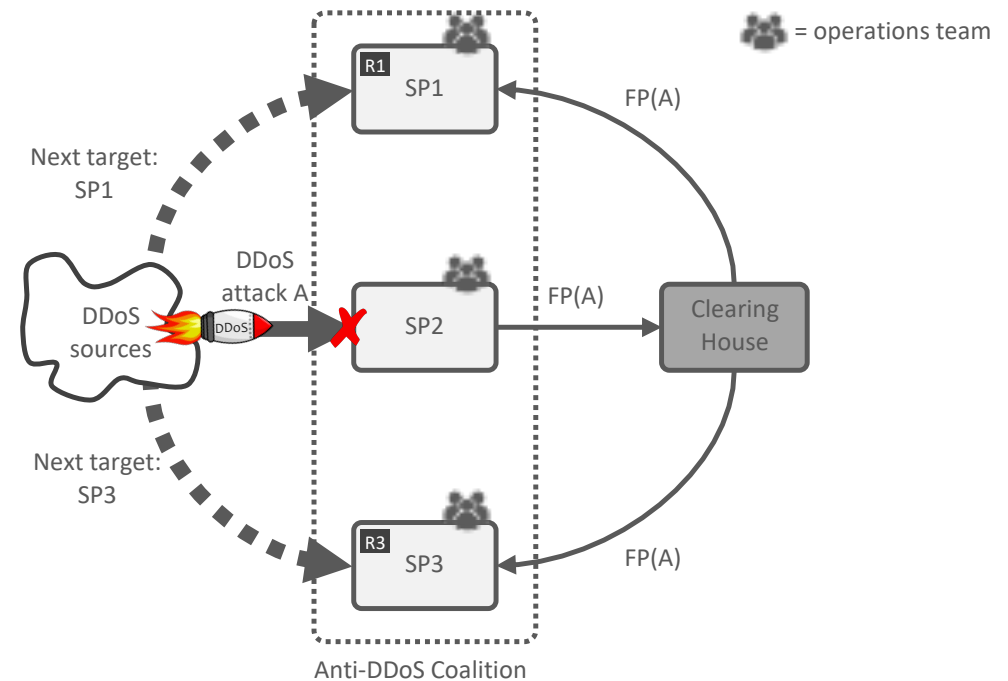
Key challenge: increase to TRL 5-7 and grow deployment





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": [
      omitted;
    ],
    "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"
  ]
}
```

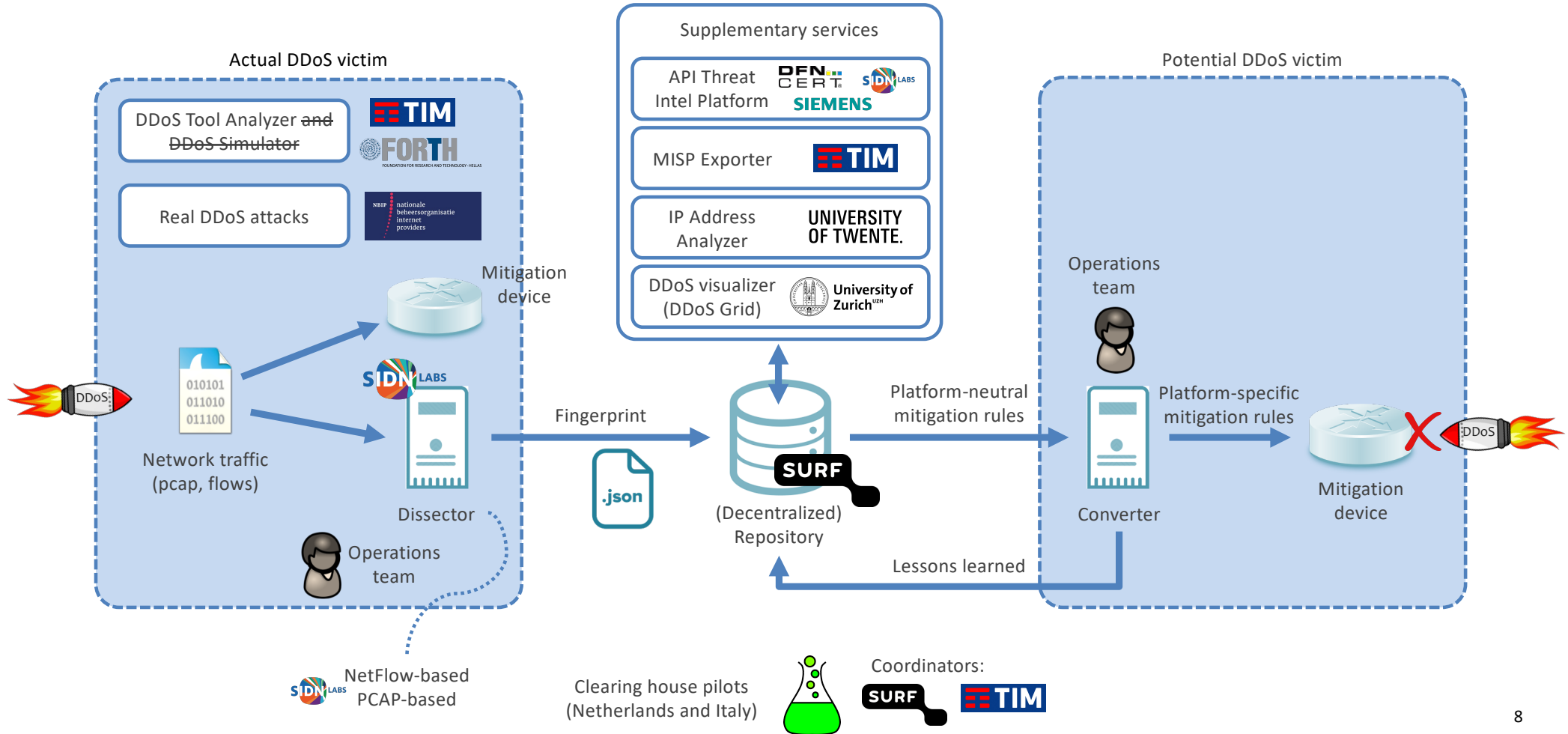


Clearing House increases Digital Autonomy

- 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





Activities Image Viewer Feb 2 12:27

Events - MISP

```
File Edit Tools
```

Home

- List Events
- Add Event
- Import from REST client
- List Attributes
- Search Attributes
- View Properties
- Events with View delegations
- Export
- Automation

```
{ "dns_gry_type": 1.0, "ip_proto": ["UDP"], "highest_protocols": ["DNS"], "dns_gry_name": "mydomain.com", "eth_type": ["0x00008000"], "frame_len": 72, "udp_length": 38, "ip_ttl": 32, "dstport": 53, "fragmentation": false, "tags": ["DNS", "DNS_QUERY", "UDP_SUSPECT"], "start_time": "2021-02-02T12:22:49", "duration_sec": 1.0, "total_dst_ports": 1, "avg_bps": 3380, "total_packets": 1, "key": "ca56c6c6c6c6c6c6c6c6c6c6c6c6c6c6", "key_sha256": "f7...", "total_ips": 10, "amplifiers": ["188.81.0.8", "188.81.0.6", "188.81.0.5", "188.81.0.5"] }
```

T3.2_architecture.png

MISP Interaction (work in progress)

The diagram illustrates the MISP interaction workflow. It shows the following components and their interactions:

- Operations team A:** Uses a **MISP-based Authoring Tool** to create **SNORT mitigation rules** based on **MISP events**.
- Operations team B:** Uses an **Authoring Tool** to create **Platform-specific mitigation rules (now)** based on **MISP events** and **Platform-specific mitigation rules (future)**.
- Data Sources:** **SIDN LABS** and **Dissector** provide **Fingerprints** to the **(Decentralized) Repository**.
- Repository:** The **(Decentralized) Repository** (containing **SURF**) stores **Fingerprints** and provides **SNORT rules** to the **MISP Exporter**.
- MISP:** The **MISP** system (powered by **TIM**) receives **MISP events** and provides **SNORT rules** to the **MISP Exporter**.
- Export and Conversion:** The **MISP Exporter** exports **SNORT rules** to a **Converter**. The **Converter** outputs **mitigation rules** to a **Mitigation device**.
- Feedback Loop:** **Lessons learned** are fed back from the **Mitigation device** to the **(Decentralized) Repository**.

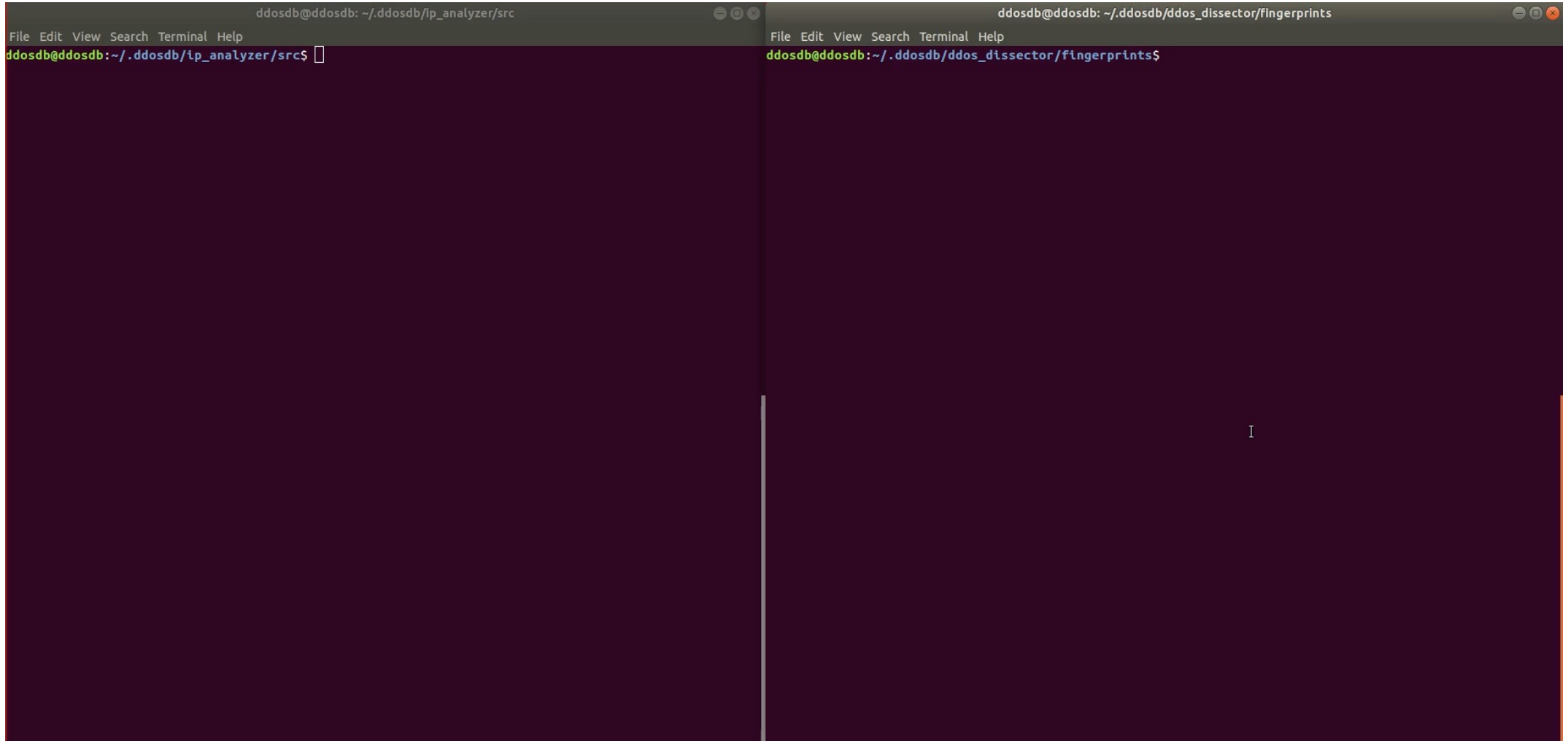
Powered by MISP 2.4.129 - 2021-02-02 12:22:49



The image shows a desktop environment with two windows. On the left is a terminal window with the following text:

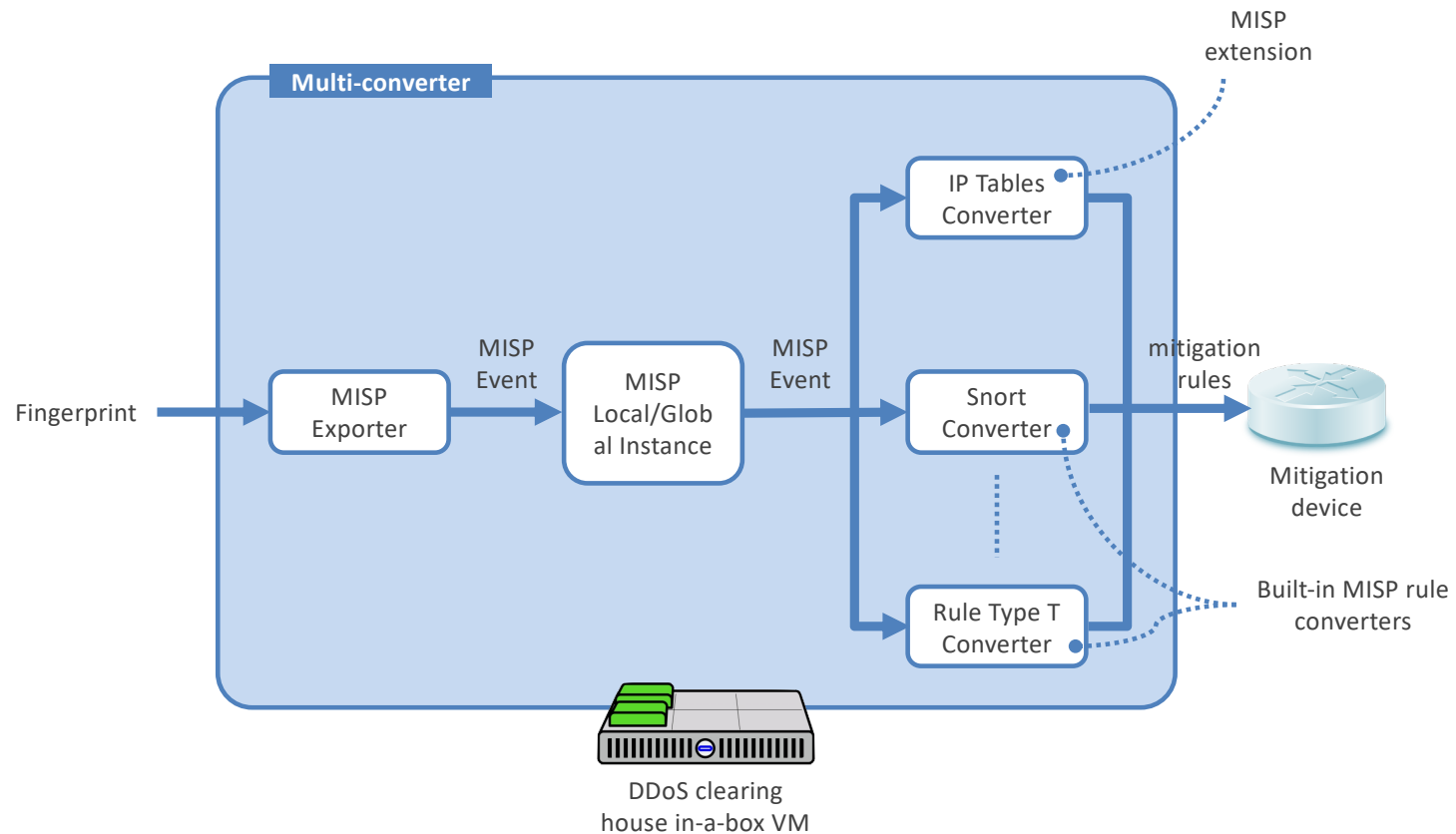
```
jan@tpj: ~/ddos_dissector  
λ tpj ddos_dissector → λ git 3.0* → ./ddos_dissector.py -f ./pcap_samples/sample3.pcap --upload --host https://www.csg.uzh.ch/ddosgrid/ddosdb/ --user jan --passwd gg
```

On the right is a Mozilla Firefox Private Browser window. The browser title is "Mozilla Firefox (Private Browsing)". The address bar contains "Search with Google or enter address". The main content area displays the Firefox logo and the text "Firefox". Below the logo is a search bar with the text "Search the Web". A message box states "You're in a Private Window" and explains that Firefox clears search and browsing history. At the bottom of the message box, there is a link: "Common myths about private browsing". Below the message box, there are two links: "Need more privacy?" and "Try Mozilla VPN". The system tray at the bottom shows the date "Oct 7 11:42" and various icons.





Multi-converter



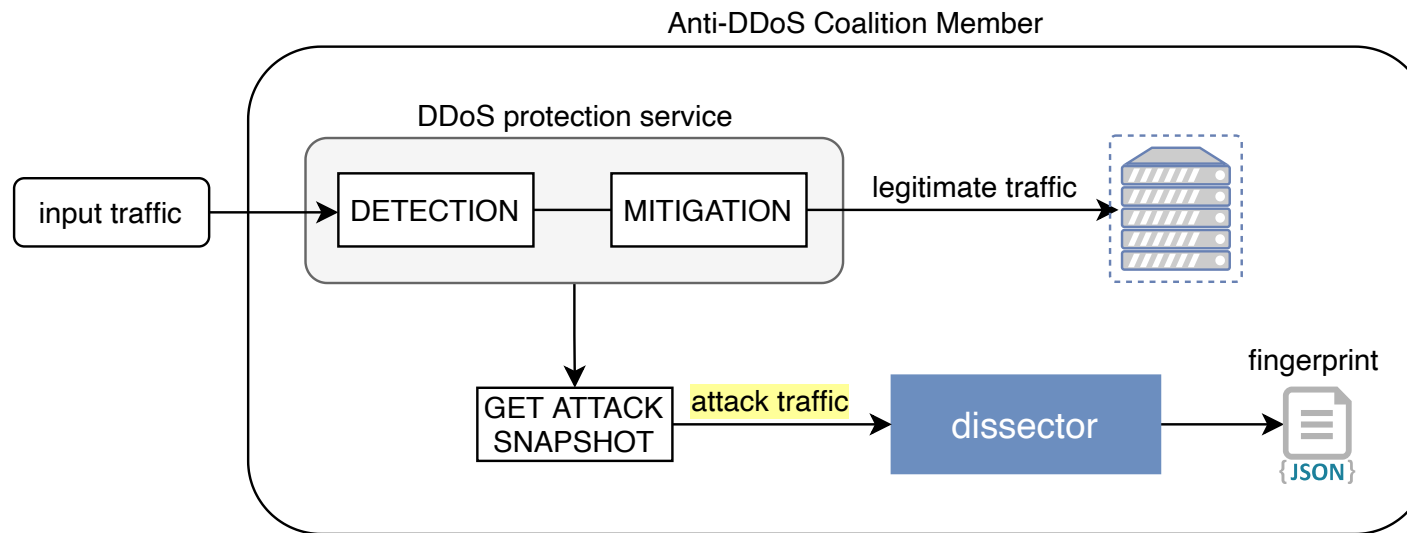


Component Maturity Indication

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

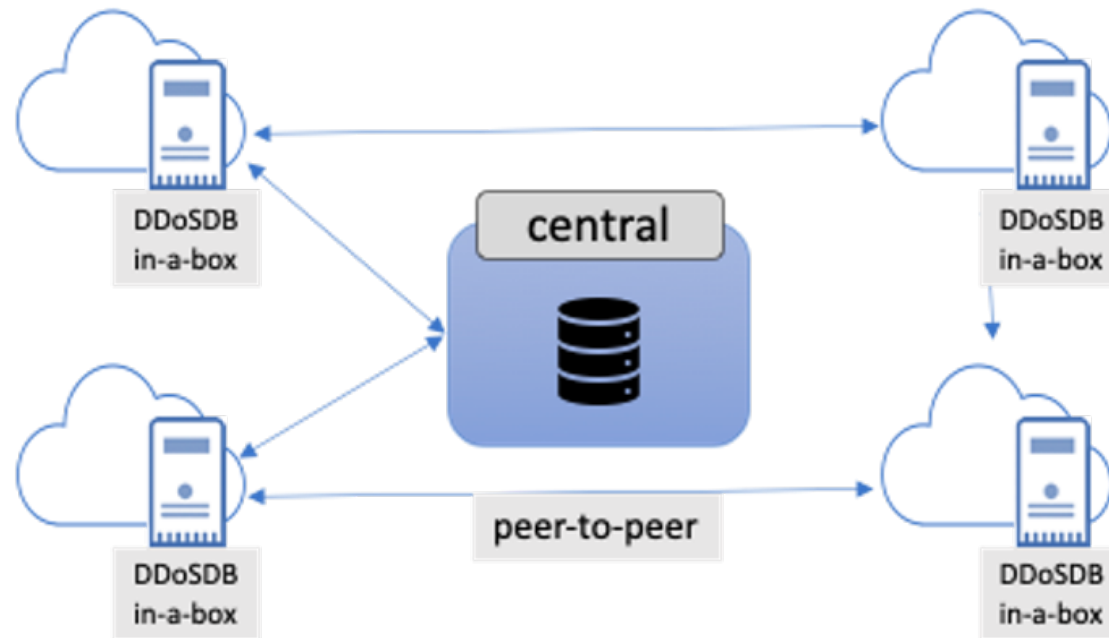


Dissector deployment models





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



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner





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





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