CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Collaborative DDoS Mitigation & The DDoS Clearing House

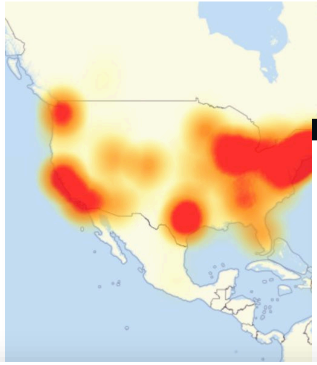
Thijs van den Hout (SIDN Labs)

Partners: SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE, Siemens

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

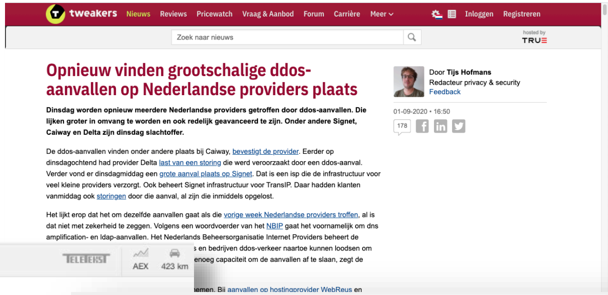
DDoS remains relevant

Mirai botnet, 2016



Estonia, 2007

The Netherlands, September 2020



Opnieuw vinden grootschalige ddos-aanvallen op Nederlandse providers plaats

Door Tijs Hofmans
Redacteur privacy & security
Feedback

01-09-2020 • 16:50

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

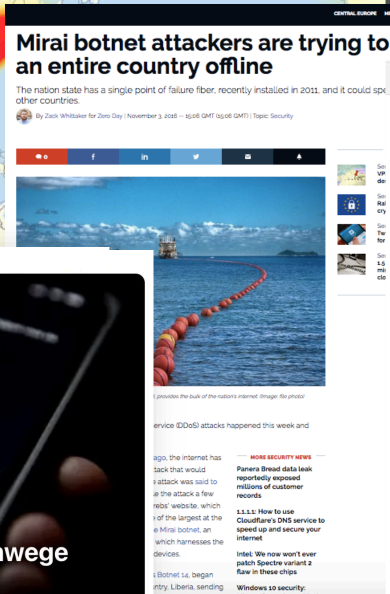
De ddos-aanvallen vinden onder andere plaats bij Caiway, bevestigt de provider. Eerder op dinsdagochtend had provider Delta last van een storing die werd veroorzaakt door een ddos-aanval. Verder vond er dinsdagmiddag een grote aanval plaats op Signet. Dat is een isp die de infrastructuur voor veel kleine providers verzorgt. Ook beheert Signet infrastructuur voor TransIP. Daar hadden klanten vanmiddag ook storingen door die aanval, al zijn die inmiddels opgelost.

Het lijkt erop dat het om dezelfde aanvallen gaat als die vorige week Nederlandse providers troffen, al is dat niet met zekerheid te zeggen. Volgens een woordvoerder van het NBIP gaat het voornamelijk om dns amplification- en ldap-aanvallen. Het Nederlands Beheersorganisatie Internet Providers beheert de
s en bedrijven ddos-verkeer naartoe kunnen loodsen om
enoeg capaciteit om de aanvallen af te slaan, zegt de

nemen. Bij aanvallen op hostingprovider WebReus en

House of Representatives of The Netherlands, Oct 2020

Tweede Kamer
DER STATEN-GENERAAL



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 spe
other countries.

By Zack Whittaker for Zero Day | November 3, 2016 -- 15:06 GMT (15:06 GMT) | Topic: Security

, provides the bulk of the nation's internet. (Image: file photo)

ervice (DDoS) attacks happened this week and

ago, the internet has
tack that would
attack was said to
e the attack a few
rebs' website, which
of the largest at the
e Mirai botnet, an
which harnesses the
devices.

s Botnet 14, began
ntry, Liberia, sending

MORE SECURITY NEWS

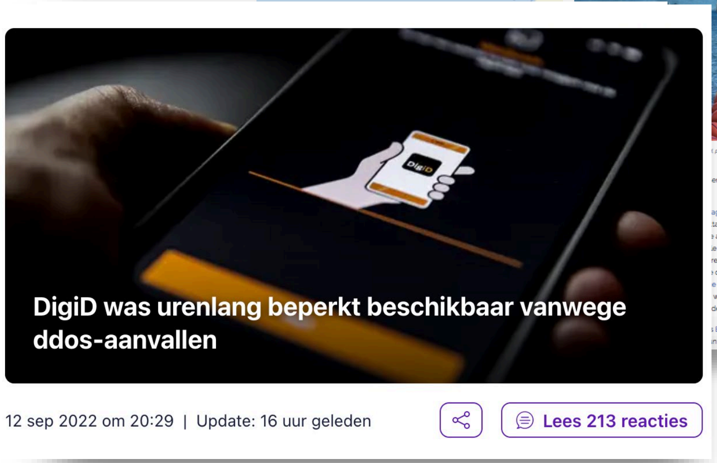
Panera Bread data leak reportedly exposed millions of customer records

1.1.1.1: How to use Cloudflare's DNS service to speed up and secure your internet

Intel: We now won't ever patch Spectre variant 2 flaw in these chips

Windows 10 security:

Liberia, 2016

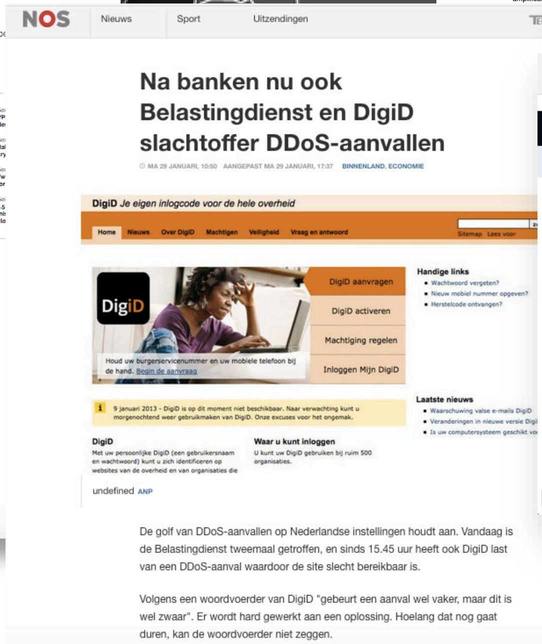


DigiD was urenlang beperkt beschikbaar vanwege ddos-aanvallen

12 sep 2022 om 20:29 | Update: 16 uur geleden

Lees 213 reacties

The Netherlands, 3 days ago!



Na banken nu ook Belastingdienst en DigiD slachtoffer DDoS-aanvallen

MA 29 JANUARI, 10:50 AANGEPAST MA 29 JANUARI, 17:37 BINNENLAND, ECONOMIE

DigiD *Je eigen inlogcode voor de hele overheid*

Houd uw burgerservicenummer en uw mobiele telefoon bij de hand. Begin de aanvraag

Handige links
- Wachtwoord vergeten?
- Nieuw mobiel nummer opgeven?
- Herstelcode ontvangen?

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

Laatste nieuws
- Waarschuwing valse e-mails DigiD
- Veranderingen in nieuwe versie Digi
- Is uw computersysteem geschikt vo

DigiD
Met uw persoonlijke DigiD (een gebruikersnaam en wachtwoord) kunt u zich identificeren op websites van de overheid en van organisaties die

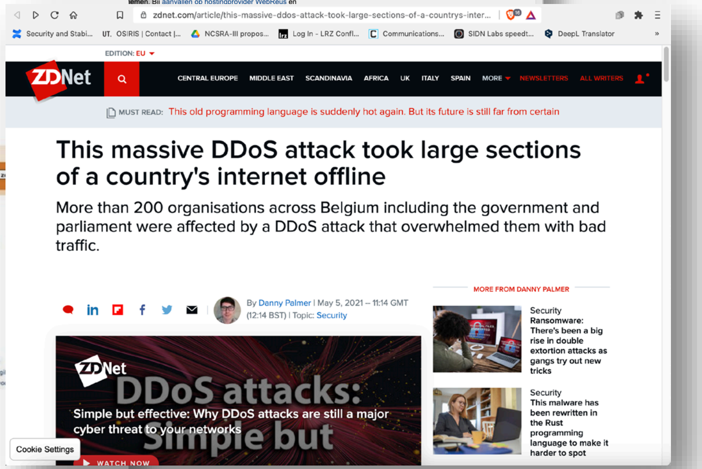
Waar u kunt inloggen
U kunt uw DigiD gebruiken bij ruim 500 organisaties.

undefined ANP

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



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

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

MORE FROM DANNY PALMER

Security
Ransomware: 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

Problem

- Mature DDoS mitigation services (e.g., scrubbing), routinely handling large numbers of DDoS attacks

- BUT no sharing of DDoS data and expertise between organizations
  - Increases response time and prevents learning because of limited view
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of DDoS mitigation providers

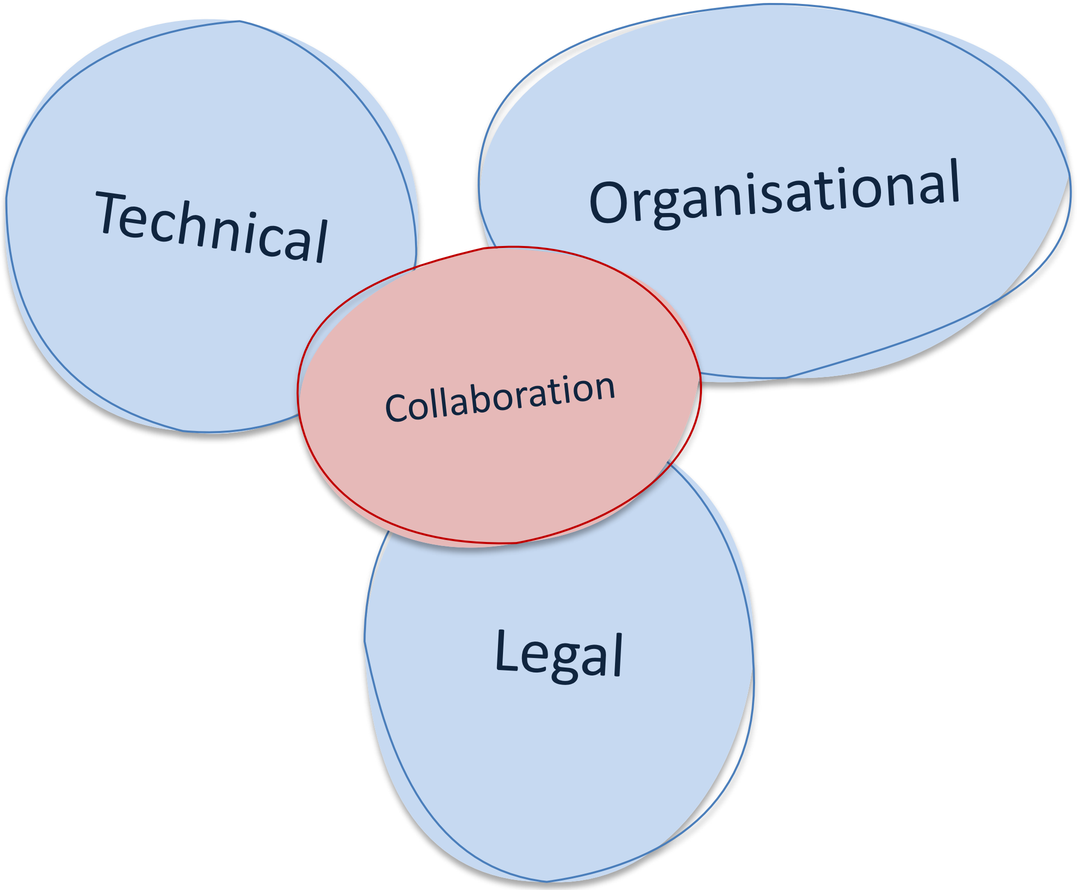
- Increases probability of societal disruptions through online services

Collaborative DDoS Mitigation

Goal: Improve collective DDoS resilience with additional activities

+ Sharing
  - DDoS metadata
  - Mitigation strategies
  - Tools and services

+ Practice together
  - DDoS drills
  - Cyber ranges



Examples

- Network playbook sharing for DNS Anycast (Tech talk II)
- IXP scrubber (Tech talk III)
- MANRS (Mutually Agreed Norms for Routing Security)
- DDoS Clearing House

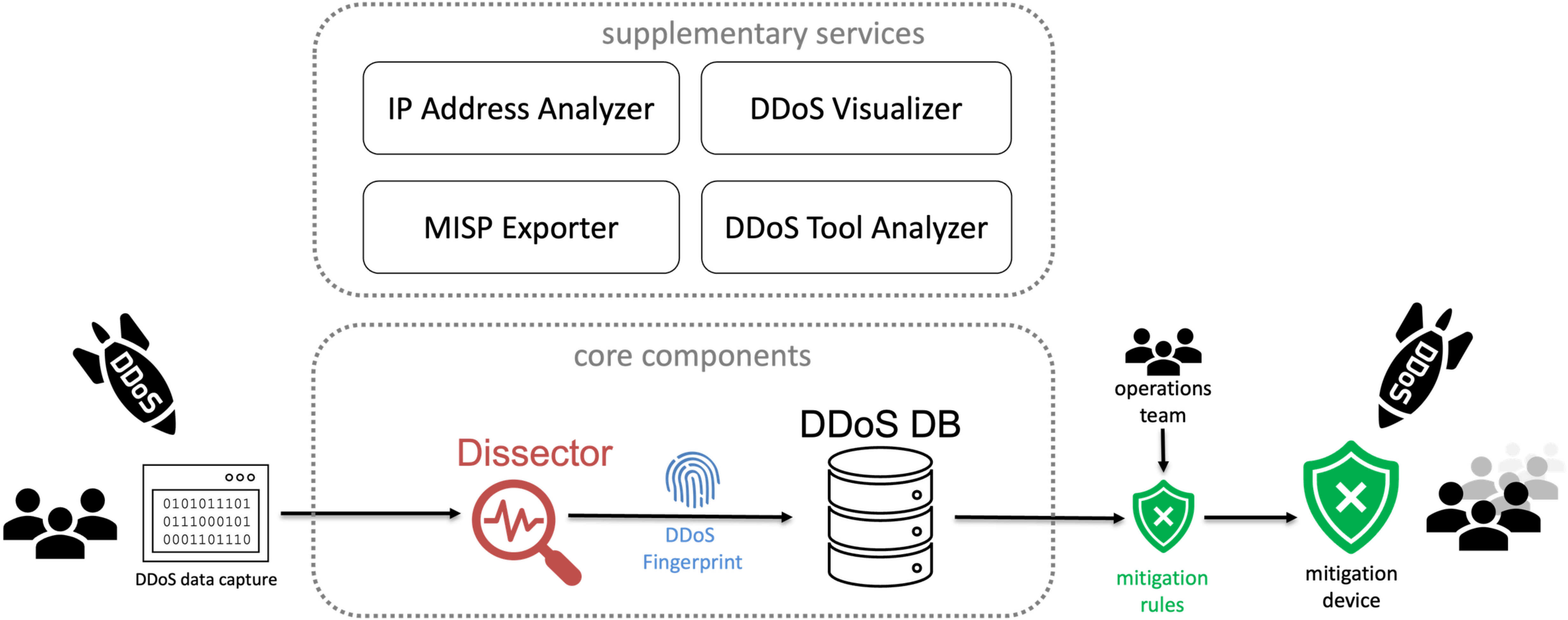
DDoS Clearing House

- Sharing of **DDoS fingerprints** between organizations

- Generic concept: **Anti-DDoS Coalitions** across sectors, Member States, business units, etc.

- **Extends DDoS protection services** that service providers use and does not replace them

DDoS Clearing House



supplementary services

IP Address Analyzer

DDoS Visualizer

MISP Exporter

DDoS Tool Analyzer

core components

DDoS data capture

0101011101
0111000101
0001101110

Dissector

DDoS Fingerprint

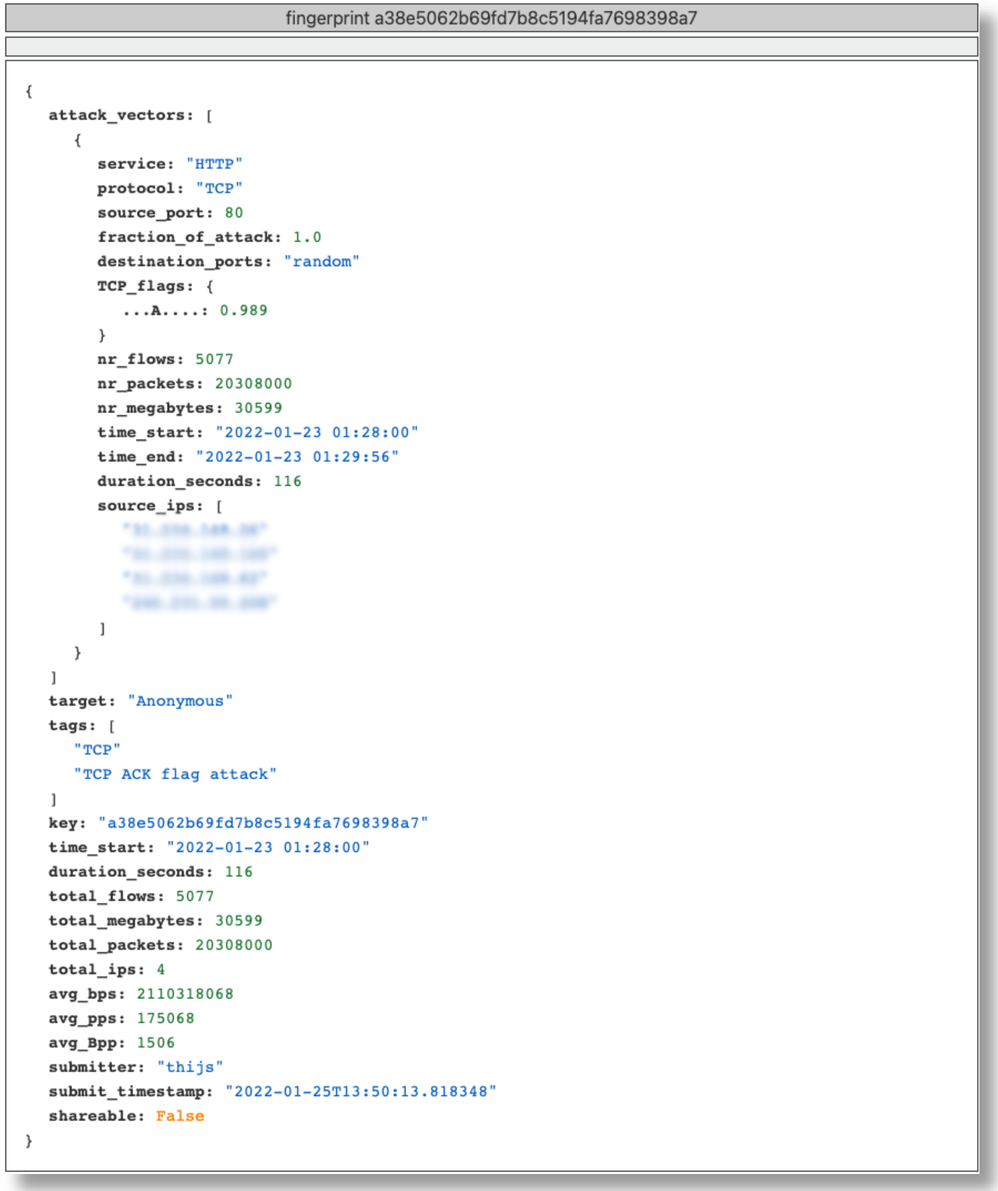
DDoS DB

operations team

mitigation rules

mitigation device

DDoS Fingerprint Example



fingerprint a38e5062b69fd7b8c5194fa7698398a7

```
{
  attack_vectors: [
    {
      service: "HTTP"
      protocol: "TCP"
      source_port: 80
      fraction_of_attack: 1.0
      destination_ports: "random"
      TCP_flags: {
        ...A....: 0.989
      }
      nr_flows: 5077
      nr_packets: 20308000
      nr_megabytes: 30599
      time_start: "2022-01-23 01:28:00"
      time_end: "2022-01-23 01:29:56"
      duration_seconds: 116
      source_ips: [
        [redacted]
      ]
    }
  ]
  target: "Anonymous"
  tags: [
    "TCP"
    "TCP ACK flag attack"
  ]
  key: "a38e5062b69fd7b8c5194fa7698398a7"
  time_start: "2022-01-23 01:28:00"
  duration_seconds: 116
  total_flows: 5077
  total_megabytes: 30599
  total_packets: 20308000
  total_ips: 4
  avg_bps: 2110318068
  avg_pps: 175068
  avg_Bpp: 1506
  submitter: "thijs"
  submit_timestamp: "2022-01-25T13:50:13.818348"
  shareable: False
}
```

Key innovations

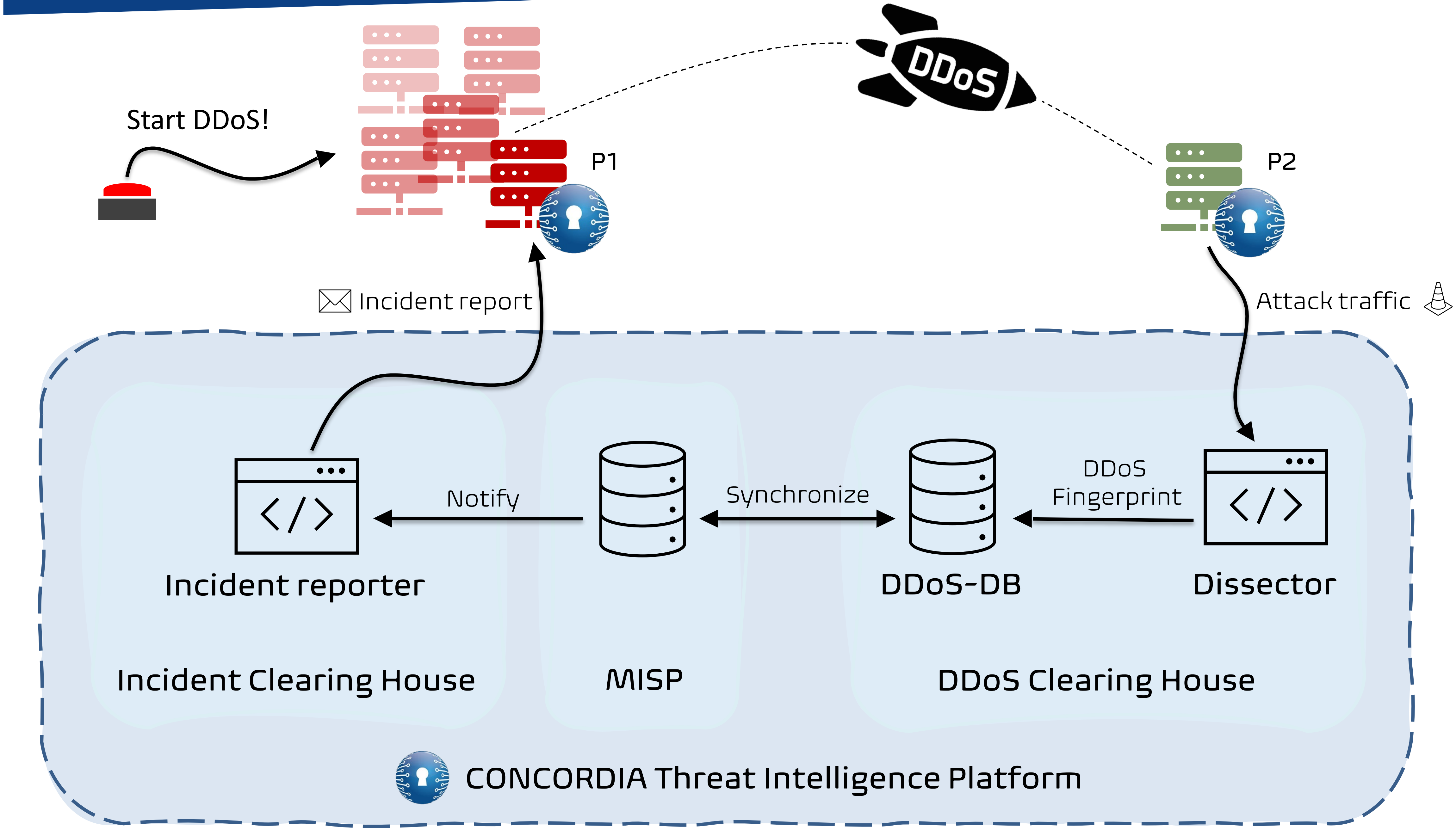
- Bridge **multidisciplinary gap** to deployment, more than tech!
- **Opensource design** that we make available through a “cookbook”
  - Technology, legal, organizational, lessons learned based on pilots
  - Enable federations of organizations to set up their own anti-DDoS coalition
  - Main use case is the Dutch Anti-DDoS Coalition (NL-ADC)
- Operates across **heterogeneous networks** and offers rich set of services

DDoS Clearing House pilots

- The Netherlands
  - In the existing Dutch Anti-DDoS Coalition (17 partners)
  - Cross-sectoral
  - One producer of fingerprints
- Italy
  - Smaller scale: Telecom Italia SOC & Security Lab + University of Turin
  - Intra-organizational
  - MISP

DDoS Testbed

- Representative environment used to
  - Test the technical developments of the Clearing House
  - Demonstrate our work
  - Cyber range for practicing DDoS
- DDoS traffic simulator
  - Small scale
  - Dashboard for attack customization


Start DDoS!
DDoS
P1
P2
✉ Incident report
Attack traffic
Notify
Synchronize
DDoS
Fingerprint
Incident reporter
DDoS-DB
Dissector
Incident Clearing House
MISP
DDoS Clearing House
CONCORDIA Threat Intelligence Platform

What’s next?

- DDoS Clearing House Cookbook
- Production phase at the NL-ADC
- Wrap up CONCORDIA with demonstration & reports

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/

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/