



**Developing a DDoS Clearing House for Europe**  
**Pitch @ the 1<sup>st</sup> TUCCR Cyber Café**  
**Enschede, March 24, 2022**

**Cristian Hesselman (SIDN Labs)**

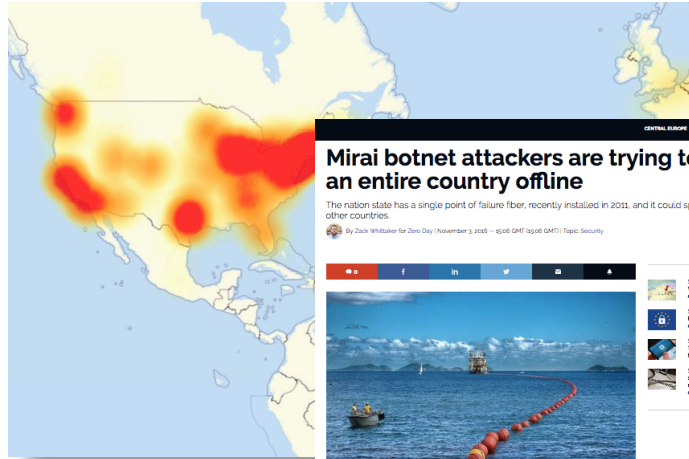
**Partners:** SIDN, University of Twente, Telecom Italia, FORTH, University of Zurich, SURF, University of Lancaster, CODE, Siemens





# High-impact DDoS Examples

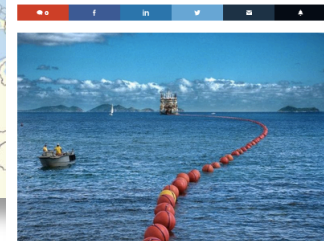
Mirai botnet, 2016



## 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 Whittaker for Zim Day | November 3, 2016 -- 10:06 GMT (10:06 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 Machtigen Veiligheid Waag en antwoord

DigiD aanvragen

DigiD activeren

Machtigen regelen

Inloggen Mijn DigiD

Handige links

- Wachtwoord vergeten?
- Nieuw mobiel nummer regelen?
- Herinstalleer ontvanger?

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

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

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

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 Waag & Aanbod Forum Camera Meet v Inloggen Registreren

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 geavanceerd 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 NSO 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

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

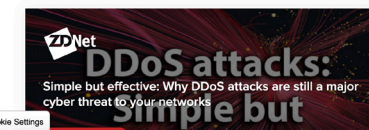
ZDNet

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



Belgium, May 2021

House of Representatives of The Netherlands, Oct 2020

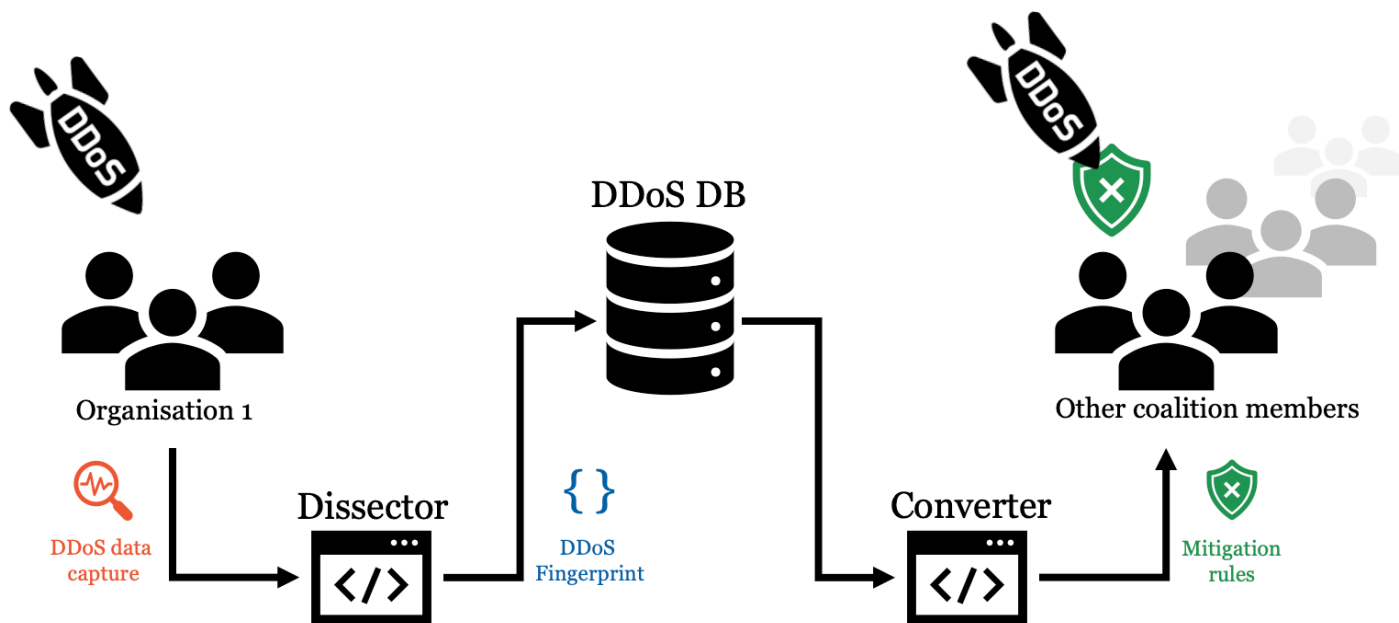




# Problem

- Mature DDoS mitigation services (e.g., scrubbing), routinely handling large numbers of DDoS attacks
- **BUT no sharing of DDoS data and expertise across organizations**
  - Longer responses: same learning curve multiple times, errors under pressure
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of (US-based) DDoS mitigation providers
- Increases probability of societal disruptions, reduces digital autonomy

# DDoS Clearing House Concept



```

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: [
        ...
      ]
    }
  ]
  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
}
  
```

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

# DDoS Clearing House: Use-inspired research



<https://www.nomoreddos.org/en/>

- DDoS clearing house **R&D**
- Clearing house distributed testbed
- Technical evaluation through pilots in the Netherlands and Italy
- DDoS clearing house cookbook
- **Using** CONCORDIA's results
- Sharing of operational experience
- Large-scale multi-party DDoS drills
- DDoS clearing house operations
- Operational ADC organization

# Dutch Anti-DDoS Coalition (NL-ADC)



CONCORDIA partner

CONCORDIA partner

CONCORDIA partner



# NL-ADC Overview

- Objective: further improve the resilience of Dutch critical services
- Strategies: sharing of DDoS measurements (clearing house), large scale collaborative drills, sharing expertise
- Organization: structure of WGs, clearing house operator and software developer, “core team” governing the initiative

# DDoS Clearing House Testbed (5 mins)







# From testbed to pilot to production

- DDoS fingerprint experiment at next NL-ADC DDoS drill
  - A-B testing with different blue teams
  - Collaborate with UT for methodological support
- Scale up testbed to pilots in the Netherlands and Italy
- Transition to production
  - Hire product owner using Dutch gov't subsidy
  - Move s/w engineering from CONCORDIA to NL-ADC
  - DDoS-DB operation from SIDN Labs to NBIP



# Further reading

<https://www.sidnlabs.nl/en/news-and-blogs/reducing-the-economic-impact-of-ddos-attacks-through-anti-ddos-coalitions>

<https://www.sidnlabs.nl/en/news-and-blogs/developing-and-running-a-testbed-for-the-ddos-clearing-house>

<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](mailto:contact@concordia-h2020.eu)

### Follow us



[www.concordia-h2020.eu](http://www.concordia-h2020.eu)



[www.twitter.com/concordiah2020](https://www.twitter.com/concordiah2020)



[www.facebook.com/concordia.eu](https://www.facebook.com/concordia.eu)



[www.linkedin.com/in/concordia-h2020](https://www.linkedin.com/in/concordia-h2020)



[www.youtube.com/concordiah2020](https://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](mailto:cristian.hesselman@sidn.nl)  
[@hesselma](https://twitter.com/hesselma)  
+31 6 25 07 87 33

Thijs van den Hout  
[thijs.vandenhout@sidn.nl](mailto:thijs.vandenhout@sidn.nl)  
[@thijsvandenhout](https://twitter.com/thijsvandenhout)