CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

DDoS Clearing House for Europe (Task 3.2)

Cross-sector Pilot Demo | Update @GA4

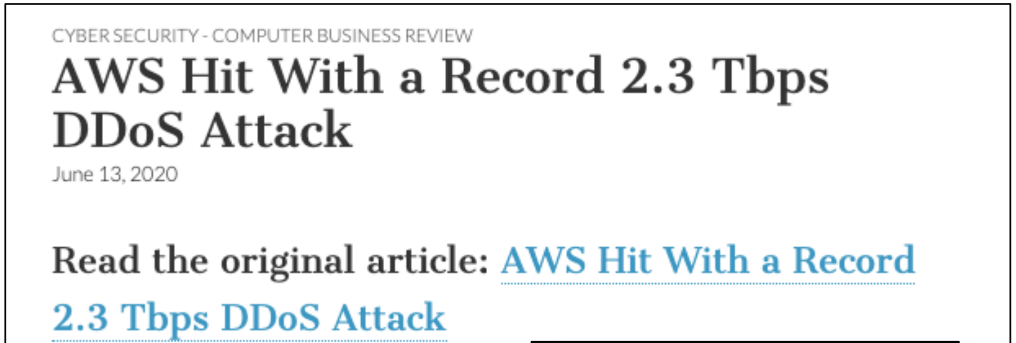
Cristian Hesselman
(SIDN Labs)

João M. Ceron
(SIDN Labs)

Partners: CODE | ERICSSON | FORTH | UT | UZH | SIDN | SNET | TI | ULANC

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

DDoS Examples

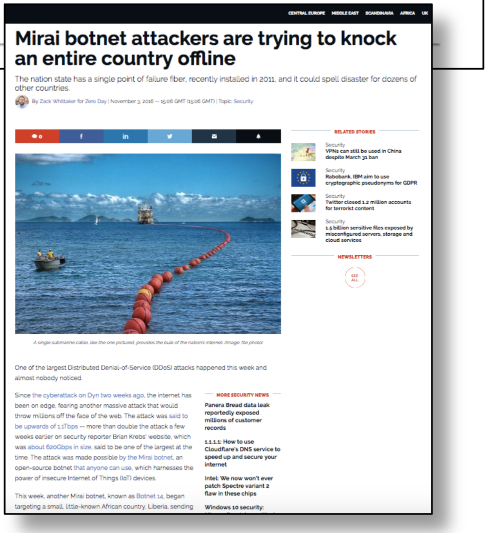


CYBER SECURITY - COMPUTER BUSINESS REVIEW

AWS Hit With a Record 2.3 Tbps DDoS Attack

June 13, 2020

Read the original article: AWS Hit With a Record 2.3 Tbps DDoS Attack



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 spell disaster for dozens of other countries.

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

RELATED STORIES

Security
VPNs can still be used in China despite March 31 ban

Security
Rabobank, IBM aim to use cryptographic pseudonyms for GDPR

Security
Twitter closed 1.2 million accounts for terrorist content

Security
1.5 billion sensitive files exposed by misconfigured servers, storage and cloud services

NEWSLETTERS

SEE ALL

A single submarine cable, like the one pictured, provides the bulk of the nation's internet. (Image: file 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 1.1Tbps -- more than double the attack a few weeks earlier on security reporter Brian Krebs' website, which was about 620Gbps 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

MORE SECURITY NEWS

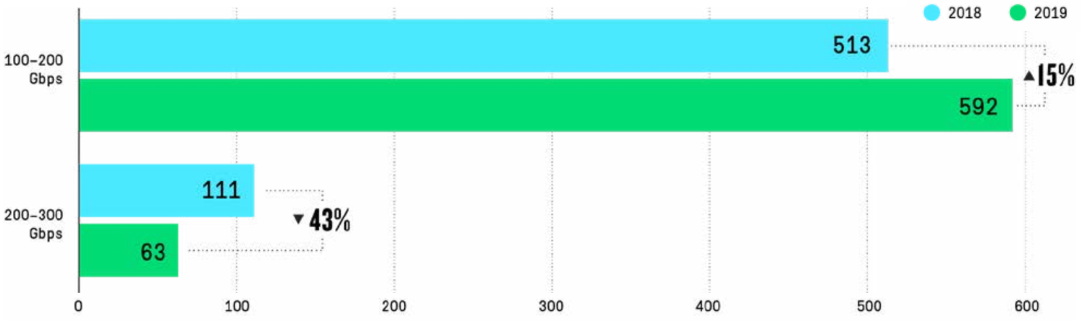
Panera Bread data leak reportedly exposed millions of customer records

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:

Mirai botnet: Dyn, OVH (hosting provider), Krebs On Security (website), Deutsche Telecom (ISP)



NETSCOUT report 2019

DDoS attacks: bigger, smarter and more frequent

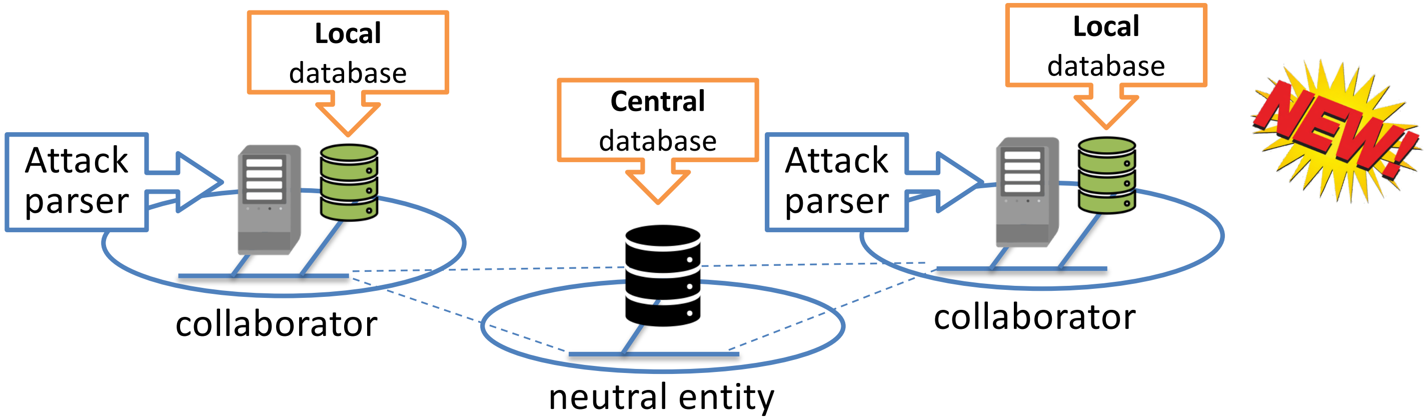
Amplification attacks

IoT

https://www.itsecuritynews.info/aws-hit-with-a-record-2-3-tbps-ddos-attack/
https://www.zdnet.com/article/mirai-botnet-attack-briefly-knocked-an-entire-country-offline/

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



T3.2 Objectives

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

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

- Build on existing components

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

P-NL P-IT … EU

Starting Point: Pilot in the Netherlands

amsix

kpn

POLITIE

SURF
CONCORDIA partner

DNB

SIDN
CONCORDIA partner

National Cyber Security Centre
Ministry of Justice and Security

Betaalvereniging
Nederland

UNIVERSITY
OF TWENTE.
CONCORDIA partner

NLix
The Interconnect Exchange

Belastingdienst

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

DINL Stichting
Digitale Infrastructuur
Nederland

NBIP nationale
beheersorganisatie
internet
providers

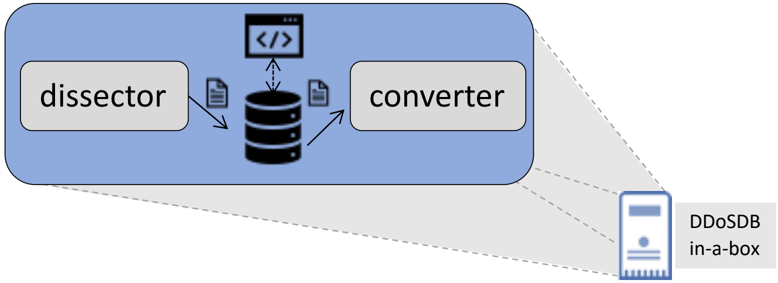
vodafone Ziggo

Plus NoMoreDDoS and Dutch Continuity Board

https://nomoreddos.org/

Advance #1: DDoS Clearing House-in-a-Box

- All-the-components together (ready-to-deploy)
- First step towards more distributed deployment model
- Enables quick prototyping
  - Shared development
  - Easy to test/audit
  - Attack samples [1]
- Improvements will be merged into our repository [2]

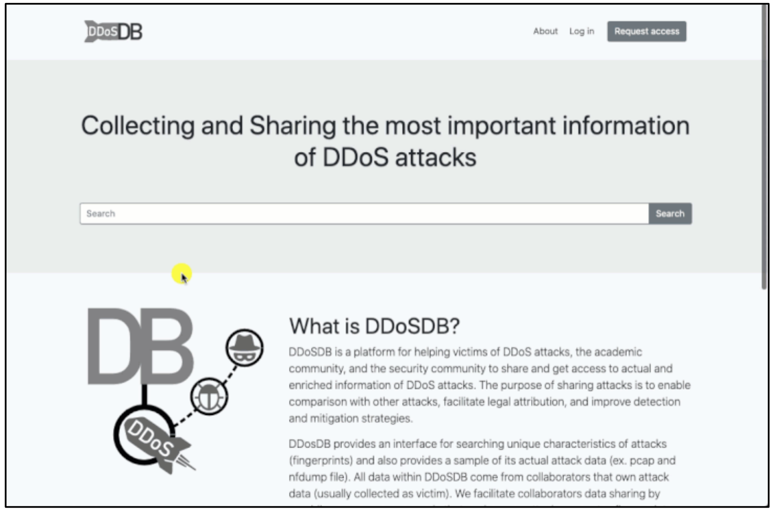


[1] https://www.simpleweb.org/wiki/index.php/Traces#Booters_-_An_analysis_of_DDoS-as-a-Service_Attacks
[2] https://github.com/ddos-clearing-house/

Advance #2: Pilot in the Netherlands

- Basic sharing of FPs through ddosdb.nl (non-production) ✓
- Improved software (Dissector and Converter) ✓
- Processing DDoS attacks on a regular basis ✓
- Translated data sharing agreement from Dutch to English ✓

```
ddosdb@ddosdb:~$
```



Collecting and Sharing the most important information of DDoS attacks

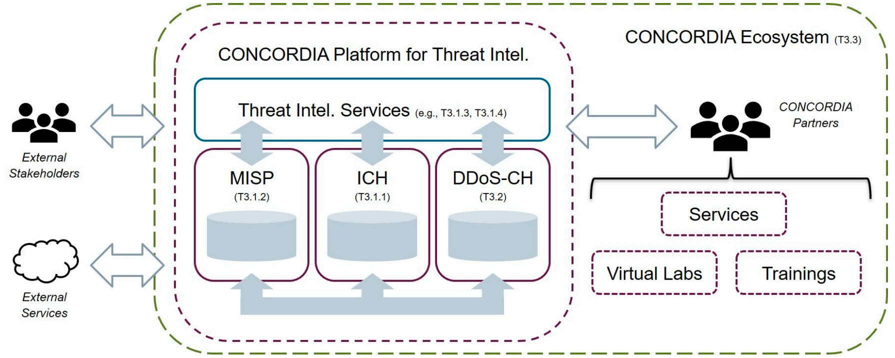
What is DDoSDB?

DDoSDB is a platform for helping victims of DDoS attacks, the academic community, and the security community to share and get access to actual and enriched information of DDoS attacks. The purpose of sharing attacks is to enable comparison with other attacks, facilitate legal attribution, and improve detection and mitigation strategies.

DDosDB provides an interface for searching unique characteristics of attacks (fingerprints) and also provides a sample of its actual attack data (ex. pcap and nfdump file). All data within DDoSDB come from collaborators that own attack data (usually collected as victim). We facilitate collaborators data sharing by

Advance #3: Cross-dataset Platform

- Layer that combines
  - MISP and Incident Clearinghouse (T3.1)
  - DDoS Clearinghouse (T3.2)

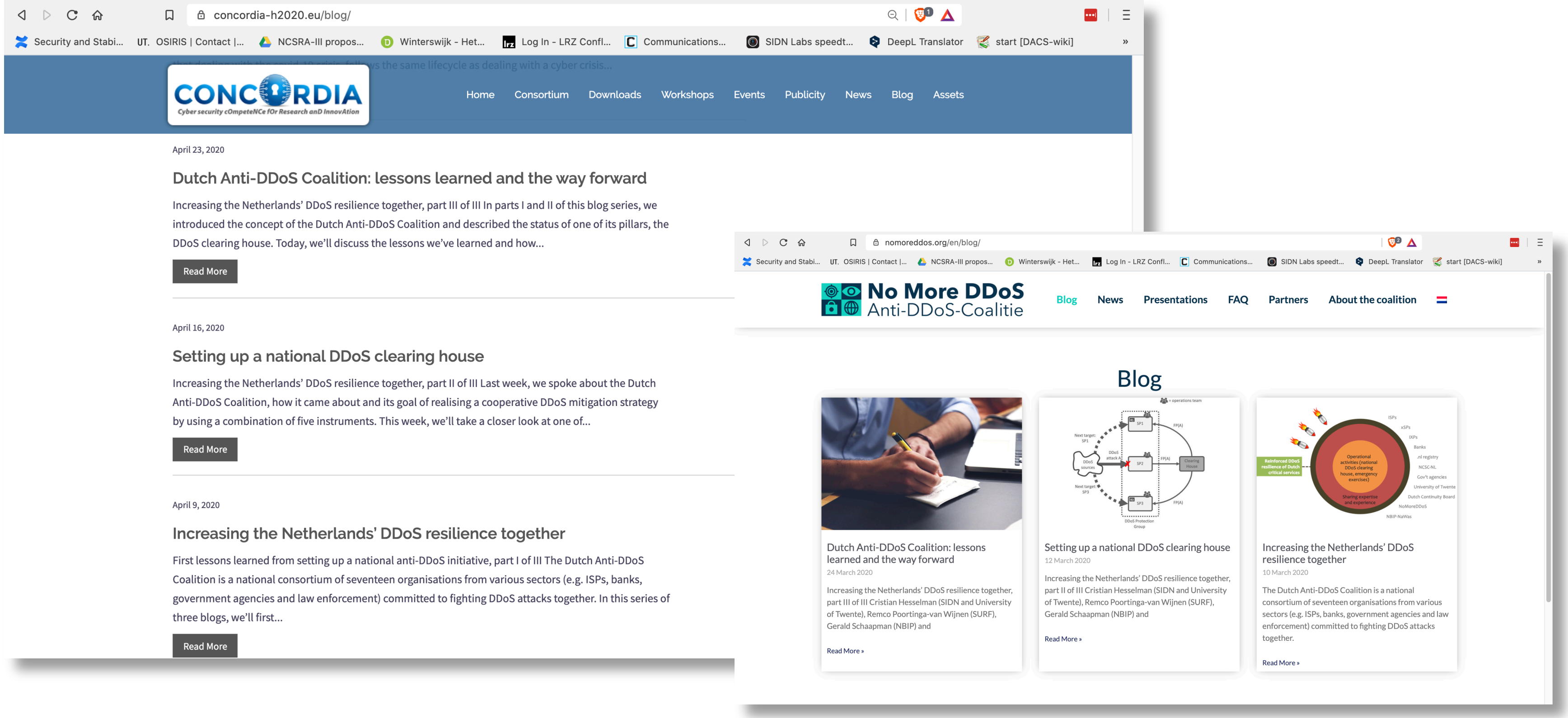


- Defined several use cases, such as
  - Booter detection
  - Incident response automation

- Work in progress

One pager on our T3.1/T3.2 “Liaison” Page:
https://confluence.lrz.de/pages/viewpage.action?pageId=159886496

Advance #4: Blog Series



April 23, 2020

Dutch Anti-DDoS Coalition: lessons learned and the way forward

Increasing the Netherlands' DDoS resilience together, part III of III In parts I and II of this blog series, we introduced the concept of the Dutch Anti-DDoS Coalition and described the status of one of its pillars, the DDoS clearing house. Today, we'll discuss the lessons we've learned and how...

Read More

April 16, 2020

Setting up a national DDoS clearing house

Increasing the Netherlands' DDoS resilience together, part II of III Last week, we spoke about the Dutch Anti-DDoS Coalition, how it came about and its goal of realising a cooperative DDoS mitigation strategy by using a combination of five instruments. This week, we'll take a closer look at one of...

Read More

April 9, 2020

Increasing the Netherlands' DDoS resilience together

First lessons learned from setting up a national anti-DDoS initiative, part I of III The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together. In this series of three blogs, we'll first...

Read More

Blog

Dutch Anti-DDoS Coalition: lessons learned and the way forward

24 March 2020

Increasing the Netherlands' DDoS resilience together, part III of III Cristian Hesselman (SIDN and University of Twente), Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBIP) and

Read More »

Setting up a national DDoS clearing house

12 March 2020

Increasing the Netherlands' DDoS resilience together, part II of III Cristian Hesselman (SIDN and University of Twente), Remco Poortinga-van Wijnen (SURF), Gerald Schaapman (NBIP) and

Read More »

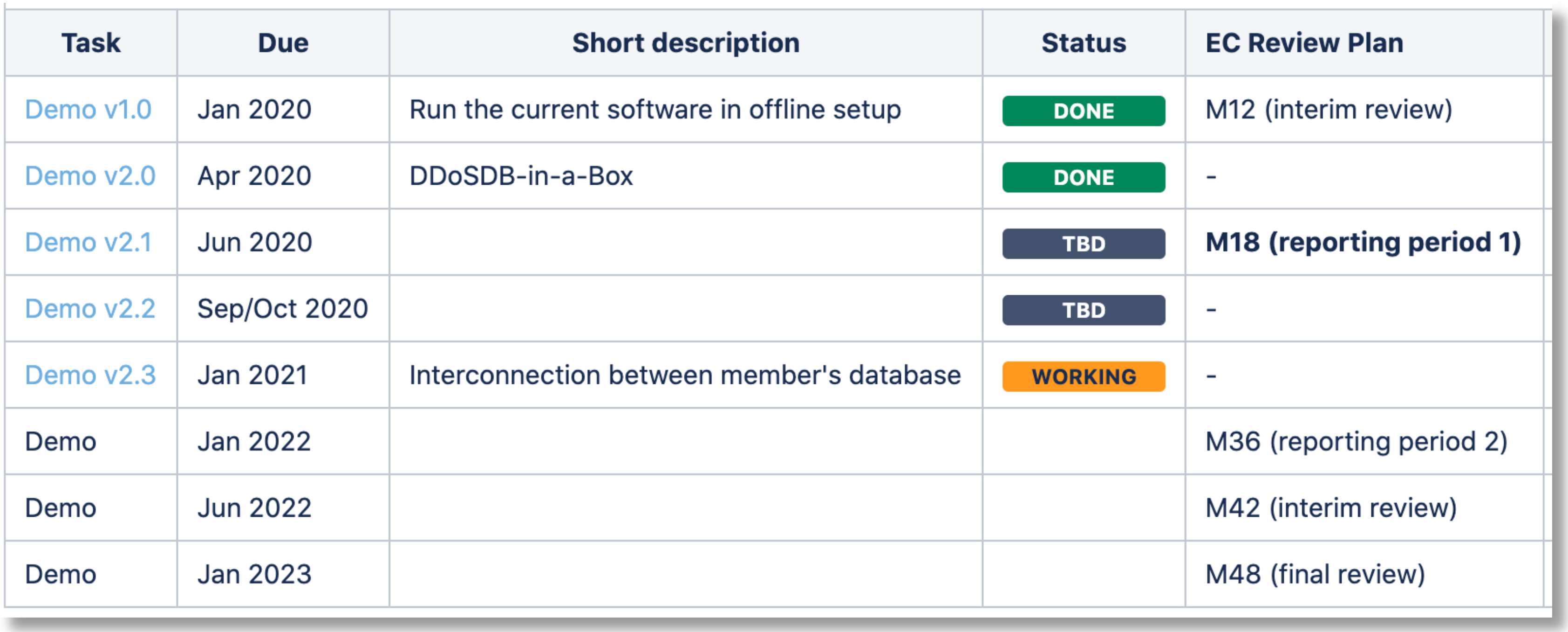
Increasing the Netherlands' DDoS resilience together

10 March 2020

The Dutch Anti-DDoS Coalition is a national consortium of seventeen organisations from various sectors (e.g. ISPs, banks, government agencies and law enforcement) committed to fighting DDoS attacks together.

Read More »

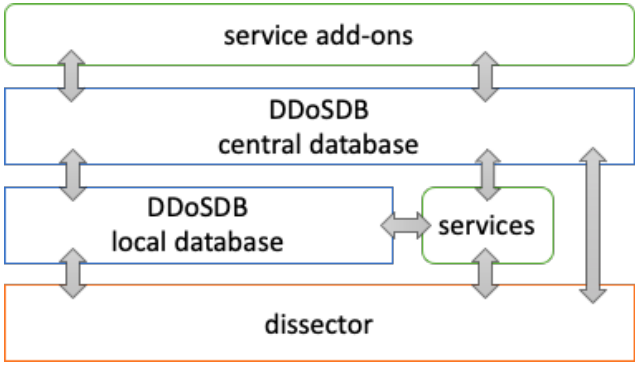
Advance #5: Demo-driven Way of Working

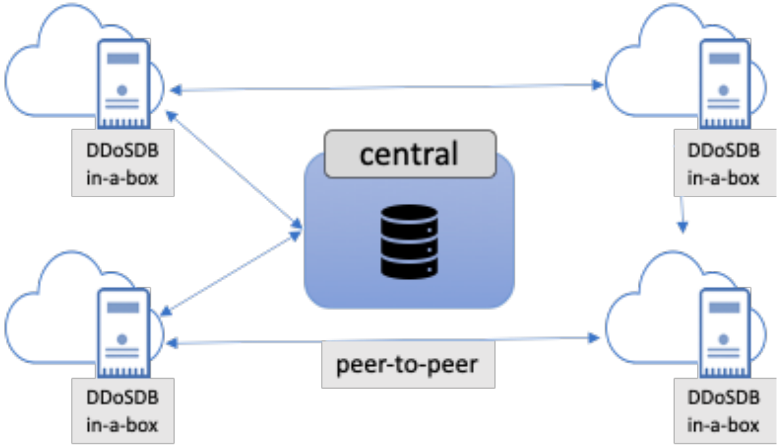


Task	Due	Short description	Status	EC Review Plan
Demo v1.0	Jan 2020	Run the current software in offline setup	DONE	M12 (interim review)
Demo v2.0	Apr 2020	DDoSDB-in-a-Box	DONE	-
Demo v2.1	Jun 2020		TBD	**M18 (reporting period 1)**
Demo v2.2	Sep/Oct 2020		TBD	-
Demo v2.3	Jan 2021	Interconnection between member's database	WORKING	-
Demo	Jan 2022			M36 (reporting period 2)
Demo	Jun 2022			M42 (interim review)
Demo	Jan 2023			M48 (final review)

Next steps: demo v2.2 (Sep/Oct)

- Deploy system at other partners
- Establish fingerprint exchange in a regular basis
- Improve software components
  - Dissector – improve DDoS characteristics fingerprints
  - Add-ons components on the top of database





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

in ™

www.linkedin.com/in/concordia-h2020

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