CONCORDIA CYBERSECURITY SUMMIT

ERICSSON

RI. SE

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

T3.2: Piloting a DDoS Clearing House for Europe

Thijs van den Hout (SIDN Labs)

March 20, 2023

Stockholm

SIDN

SURF

TIM

FORTH

UT

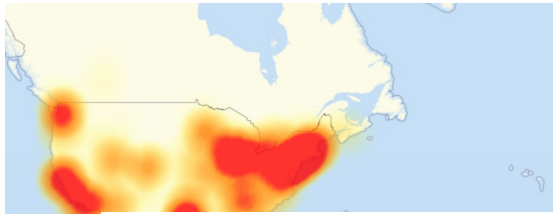
UZH

CONCORDIA
CYBERSECURITY
SUMMIT

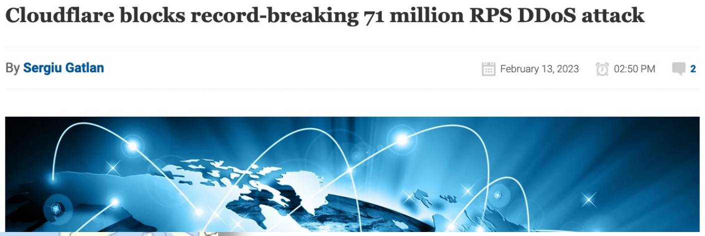
STOCKHOLM
20TH MARCH
2023

DDoS attacks remain relevant

Mirai botnet, 2016



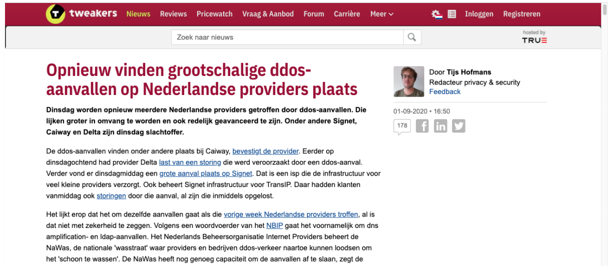
February 2023



Cloudflare blocks record-breaking 71 million RPS DDoS attack

By Sergiu Gatlan — February 13, 2023 — 02:50 PM — 2

The Netherlands, September 2020



tweakers Nieuws Reviews Pricewatch Vraag & Aanbod Forum Carrière Meer Inloggen Registreren

Zoek naar nieuws — hosted by TRUE

Opnieuw vinden grootschalige ddos-aanvallen op Nederlandse providers plaats

Door Tijs Hofmans
Redacteur privacy & security
Feedback

01-09-2020 • 16:50 — 178

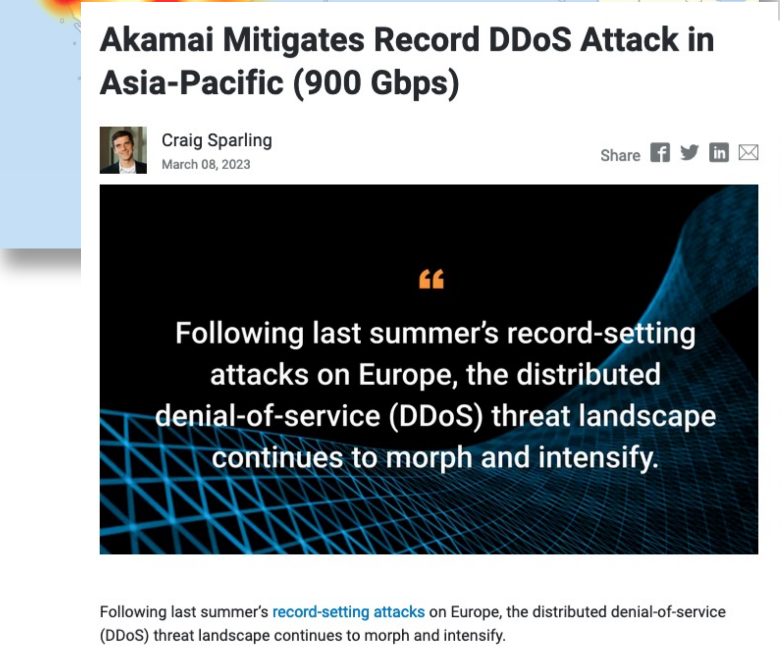
Dinsdag worden opnieuw meerdere Nederlandse providers getroffen door ddos-aanvallen. Die lijken groter in omvang te worden en ook redelijk geavanceerd te zijn. Onder andere Signet, Caiway en Delta zijn dinsdag slachtoffer.

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 NaWas, de nationale 'wasstraat' waar providers en bedrijven ddos-verkeer naartoe kunnen loodsen om het 'schoon te wassen'. De NaWas heeft nog genoeg capaciteit om de aanvallen af te slaan, zegt de

House of Representatives of The Netherlands, Oct 2020

Tweede Kamer
DER STATEN-GENERAAL



Akamai Mitigates Record DDoS Attack in Asia-Pacific (900 Gbps)

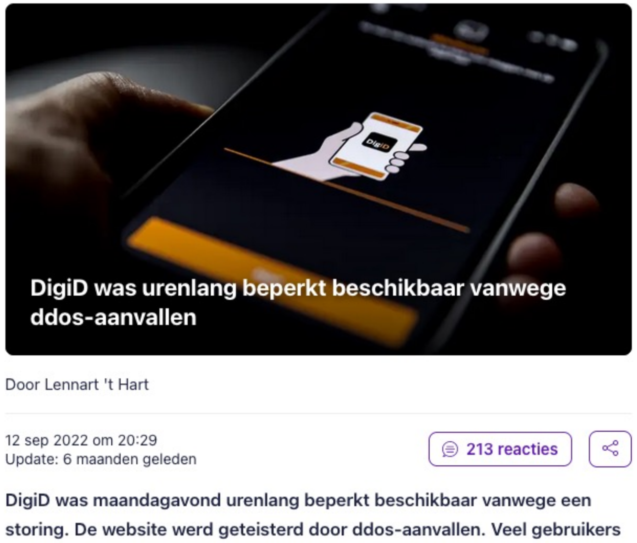
Craig Sparling
March 08, 2023

Share

> Following last summer's record-setting attacks on Europe, the distributed denial-of-service (DDoS) threat landscape continues to morph and intensify.

Following last summer's record-setting attacks on Europe, the distributed denial-of-service (DDoS) threat landscape continues to morph and intensify.

March 2023



DigiD was urenlang beperkt beschikbaar vanwege ddos-aanvallen

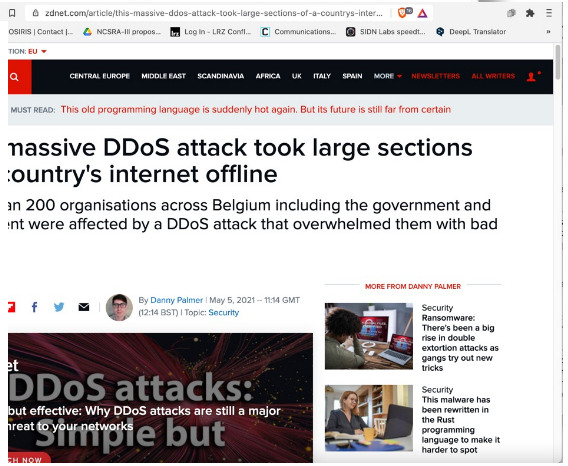
Door Lennart 't Hart

12 sep 2022 om 20:29
Update: 6 maanden geleden

213 reacties

DigiD was maandagavond urenlang beperkt beschikbaar vanwege een storing. De website werd geteisterd door ddos-aanvallen. Veel gebruikers

The Netherlands, September 2022



zdnet.com/article/this-massive-ddos-attack-took-large-sections-of-a-countrys-inter...

OSIRIS | Contact |... NCSRA-III propos... Log In - LRZ Confl... Communications... SIDN Labs speedt... DeepL Translator

TION: EU

CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE NEWSLETTERS ALL WRITERS

MUST READ: This old programming language is suddenly hot again. But its future is still far from certain

massive DDoS attack took large sections country's internet offline

an 200 organisations across Belgium including the government and nt were affected by a DDoS attack that overwhelmed them with bad

By Danny Palmer | May 5, 2021 -- 11:14 GMT (12:14 BST) | Topic: Security

DDoS attacks: Simple but effective: Why DDoS attacks are still a major 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

CONCORDIA CYBERSECURITY SUMMIT — STOCKHOLM 20TH MARCH 2023

Problem statement

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

- **BUT no sharing of DDoS data and expertise across organizations**
  - Limited victim-specific view worsens response time and learning
  - Reduces innovation of mitigation processes and systems at ecosystem level
  - DDoS data “stuck” in systems of (US-based) DDoS mitigation providers

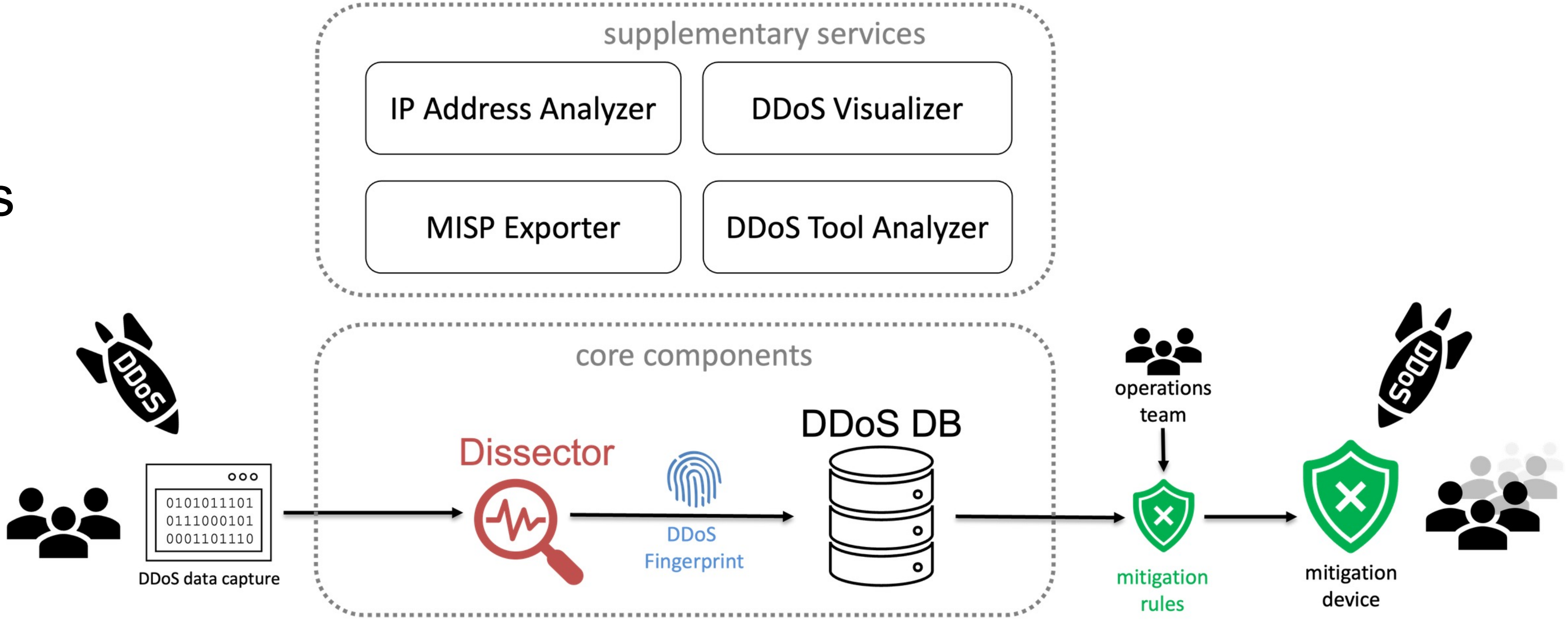
- Increases probability of societal disruptions, especially through critical (cyberphysical) systems (cf. WP2)

DDoS Clearing House concept

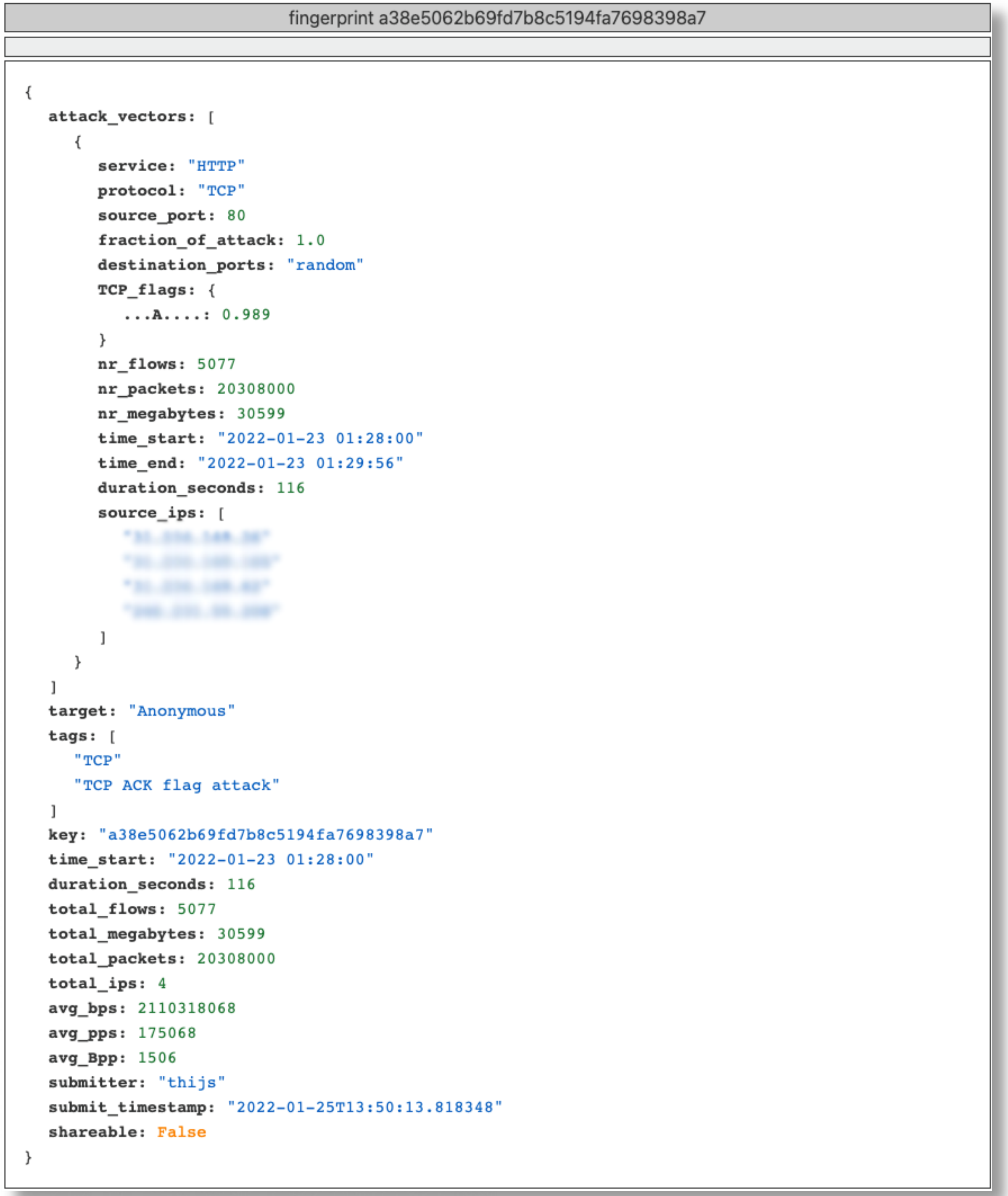
- Continuous and automatic sharing of **DDoS fingerprints**, buys providers time (proactive)

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

- Generic concept: across sectors, Member States, business units, etc.



DDoS Fingerprint



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 the **multidisciplinary gap** to deployment
- **Open-source** design: proven in pilots, documented in a *cookbook*
- Operates across **heterogeneous networks**, offers extensible services
- ⭐ EC Innovation radar 2021
- ⭐ Key CONCORDIA results

github.com/ddos-clearing-house

Dutch Anti-DDoS Coalition

nomoreddos.org

- 18 cross-sectoral critical infrastructure operators in NL
- Sharing DDoS expertise and knowledge
- Sharing DDoS data through Clearing House
- Large-scale DDoS drills (Red teaming)
- Small-scale DDoS drills (Testbed)

Two coalitions – two and a half pilots

- Dutch Anti-DDoS Coalition (TRL 8)
  - Shared 270 *real* fingerprints through DDoS-DB
  - External collaboration
  - Iteratively improve the platform

- Italian Anti-DDoS Coalition (TRL 7)
  - Telecom Italia + university of Torino
  - Internal and external collaboration
  - Share fingerprints via MISP

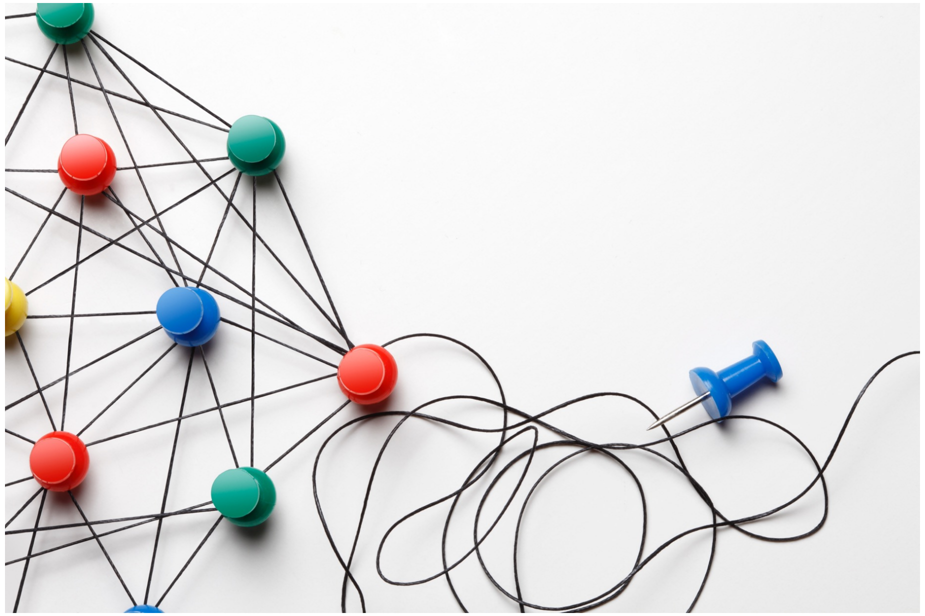
- Testbed (TRL 6)
  - pilot with simulated data

DDoS Clearing House Cookbook

- Documentation of the DDoS Clearing House
- Template agreements / contracts
- Description of pilots
- Notes on implementation
- Lessons learned
- ddosclearinghouse.eu/cookbook

Connecting the Threat Intel Platform

- CONCORDIA Threat Intelligence Platform
  - T3.1 Incident Clearing House
  - T3.2 DDoS Clearing House
  - MISP



- MISP DDoS Fingerprint object

- DDoS-DB – MISP connection

- Demo video coming soon

Looking ahead: beyond CONCORDIA

- Production-level services for Dutch ADC
  - DDoS Clearing House (at NBIP)
  - Testbed for small-scale drills (at Tax & Customs Admin)
  - Contracts currently being finalized
- Dissemination of the DDoS Clearing House Cookbook
- Submit a paper to IEEE Communications Magazine

Thank you!

Q&A

Thijs van den Hout
SIDN Labs
thijsvandenhout@sidn.nl
+31 6 12380234

CONCORDIA CYBERSECURITY SUMMIT
STOCKHOLM 20TH MARCH 2023

concordia-h2020.eu

twitter.com/**concordiah2020**

linkedin.com/in/concordia-h2020

This project has received funding from
the European Union's Horizon 2020 Research and
Innovation program under Grant Agreement No 830927.

CONCORDIA DELIVERS