



No More DDoS

Anti-DDoS-Coalitie

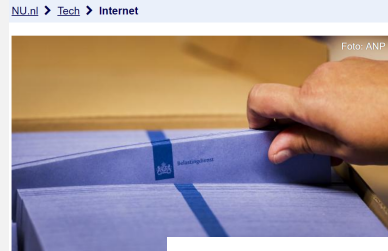
Inter-ISAC meeting NL

22 januari 2021



Achtergrond

2018



Belastingdienst en DDoS-aanvallen

Directeuren NBIP en DINL uiten kritiek op ABN Amro, ING, Rabobank en Volksbank

Banken moeten meer samenwerken om te voorkomen dat cybercriminelen hun diensten platleggen met DDoS-aanvallen. Ze zouden zich vaker moeten aansluiten bij collectieve initiatieven tegen cybercrime. Nu kiezen ze nog te vaak voor een individuele aanpak van netwerkbeveiliging bij één security-leverancier, daardoor missen ze de kennis en kunde van een grote achterban. Criminelen zijn namelijk ook in groepsverband georganiseerd.

Lees verder

op: <https://www.computable.nl/artikel/nieuws/security/6290656/250449/banken-moeten-meer-samenwerken-tegen-ddos.html>



'NaWas kan uitval van diensten door DDoS-aanvallen voorkomen'

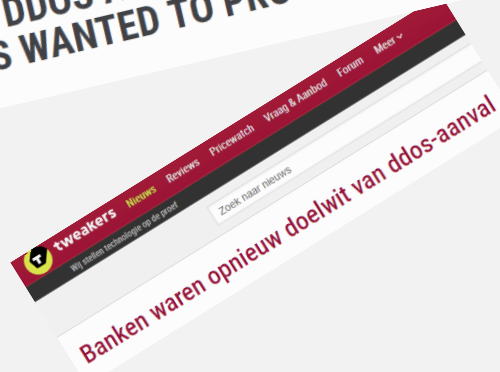
30 januari 2018 [Nieuws](#)

De DDoS aanvallen die de afgelopen dagen ABN AMRO, ING, de Rabobank en de Belastingdienst plagen hoeven niet te leiden tot uitval van diensten. Dat stelt Octavia de Weerd van de [Nationale Beheersorganisatie Internet Providers](#) (NBIP).

De NBIP is een not for profit organisatie die zich toelegt op het snel en adequaat afslaan van grootschalige en/of langdurige DDoS aanvallen.

TEEN SUSPECTED OF DDOS ATTACKS ON DUTCH FINANCIAL SERVICES WANTED TO PROVE A POINT

By Janene Pieters on February 7, 2018 - 10:09



Teenager suspected of crippling Dutch banks with DDoS attacks

A large distributed denial of service attack on banks and other organisations in the Netherlands, first thought to emanate from Russia, is now thought to have been launched by a local teenager



Deelnemers





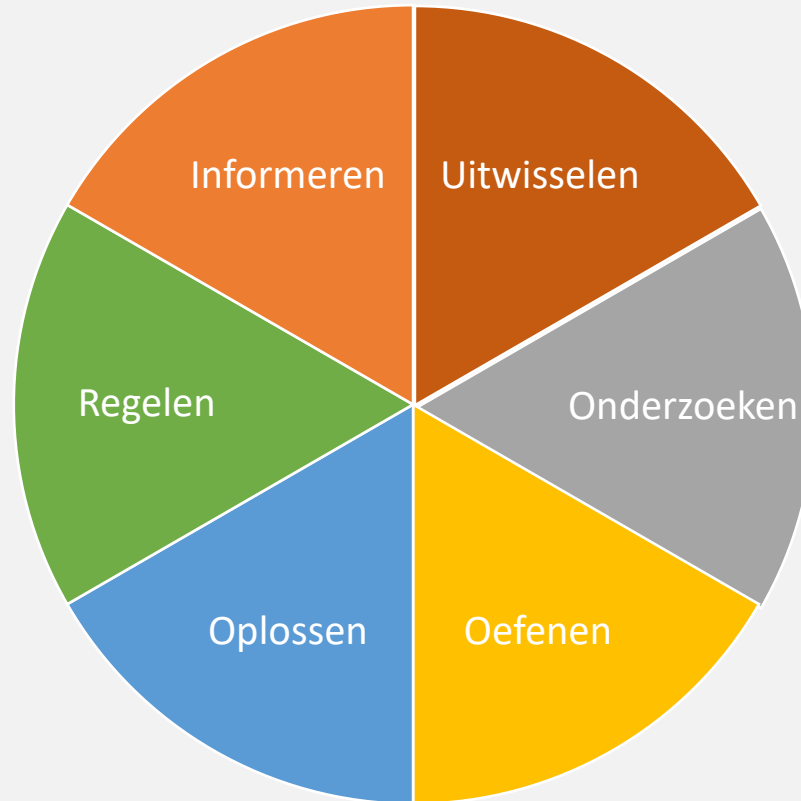
Doel

- Het verbeteren van de weerbaarheid van Nederlandse onlinediensten door DDoS-aanvallen op coöperatieve basis te bestrijden over verschillende organisaties en sectoren heen.



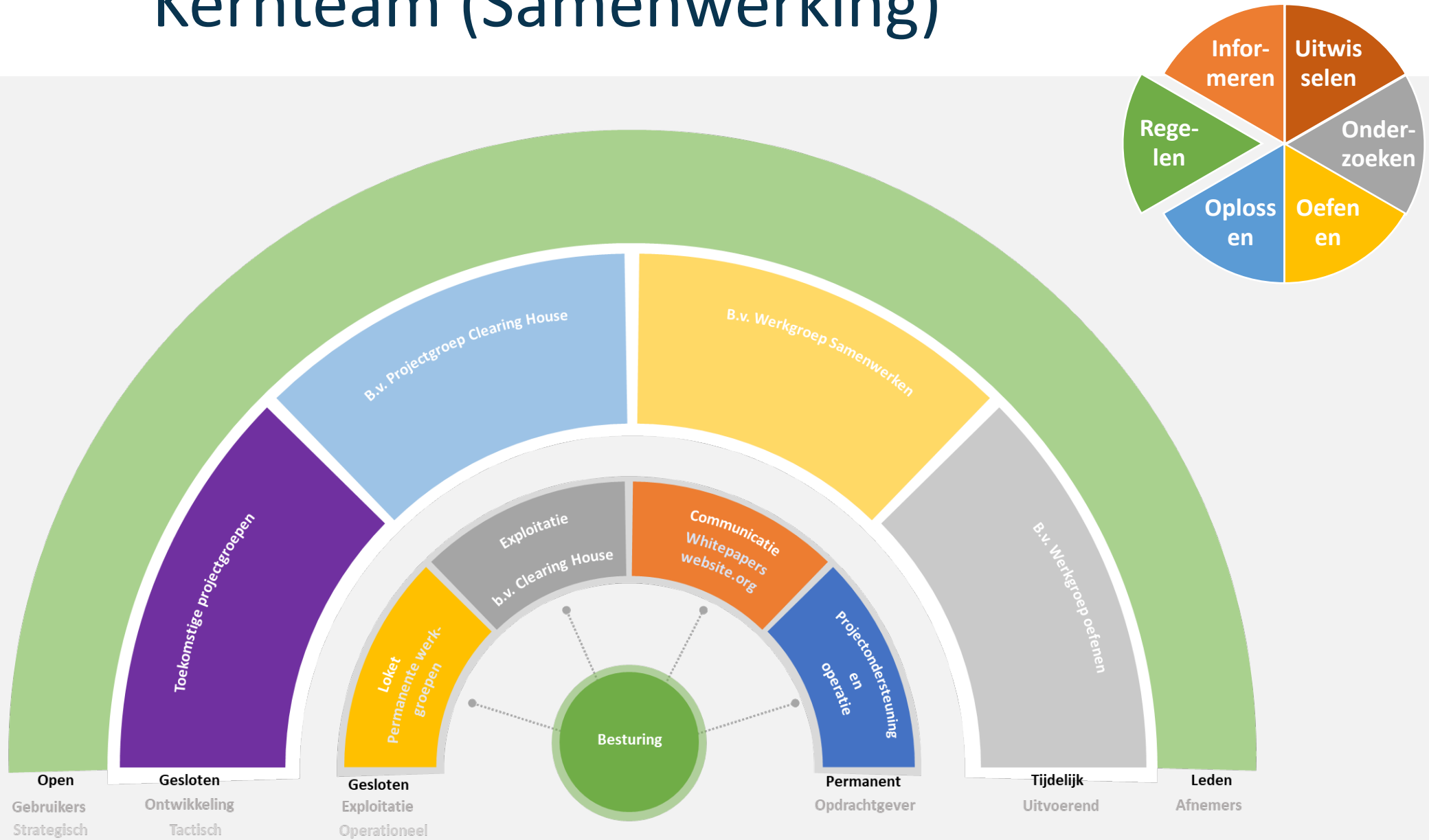


Wat doen we met de werkgroepen





Kernteam (Samenwerking)





Zichtbaarheid



No More DDoS
Anti-DDoS-Coalitie

Blog Nieuws Presentaties FAQ Partners Over de coalitie

Nationale Anti-DDoS-coalitie

De nationale anti-DDoS-coalitie is een samenwerkingsverband tegen DDoS-aanvallen. Het samenwerkingsverband bestaat uit zeventien organisaties waaronder overheden, internetproviders, internet exchanges, academische instanties, non-profitorganisaties en banken. De coalitie heeft als doel om DDoS vanuit verschillende hoeken te onderzoeken en bestrijden.

[Over de coalitie](#)

Nieuwe versie van de basiscomponenten van het DDoS-clearinghouse

20 september 2020

SIDN Labs en SURF hebben een nieuwe versie uitgebracht van de DDoS-Clearinghouse-In-Box, een systeem waarmee netwerkovertuilers door middel van 'DDoS-fingerprints' automatisch informatie kunnen...

[Lees meer >](#)

DDoS-coalitie heeft handvol aan huidige DDoS-aanvallen

14 september 2020

Klanten hebben er tot nu toe weinig last van daarbij gezamenlijk cotreden. De laatste weken worden tientallen bedrijven en organisaties aangevallen door middel van een...

[Lees meer >](#)

Nationale anti-DDoS-coalitie lanceert website over voortgang

11 juni 2020

Site weerspiegelt inspanningen van de coalitie afgelopen twee jaar. Na zo'n twee jaar in relatieve stilte te hebben gewerkt, heeft de nationale anti-DDoS-coalitie recent de...

[Lees meer >](#)

Partners

[FAQ](#)
[Partners](#)
[Over de coalitie](#)

No More DDoS
Anti-DDoS-Coalitie

Over de coalitie
De nationale anti-DDoS-coalitie is een samenwerkingsverband dat als doel heeft om het verschijnsel DDoS vanuit maatschappelijk en economische oogpunt te onderzoeken en kennis aan te dragen om de aanvallen terug te dringen of te stoppen. Het samenwerkingsverband bestaat uit vijftien organisaties waaronder overheden, internetproviders, internet exchanges, academische instanties, non-profitorganisaties en banken.

info@nomoredos.org

Contact

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.



Basismaatregelen



[Docs] [txt|pdf]

Network Working Group P. Ferguson
 Request for Comments: 2827 Cisco Systems, Inc.
 Obsoletes: 2267 D. Senie
 BCP: 38 Amaranth Networks Inc.
 Category: Best Current Practice May 2000

**Network Ingress Filtering:
 Defeating Denial of Service Attacks which employ
 IP Source Address Spoofing**

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

Recent occurrences of various Denial of Service (DoS) attacks which have employed forged source addresses have proven to be a troublesome issue for Internet Service Providers and the Internet community overall. This paper discusses a simple, effective, and straightforward method for using ingress traffic filtering to prohibit DoS attacks which use forged IP addresses to be propagated from 'behind' an Internet Service Provider's (ISP) aggregation point.

Table of Contents

1.	Introduction	2
2.	Background	3
3.	Restricting forged traffic	3
4.	Further capabilities for networking equipment.	6
5.	Liabilities.	6
6.	Summary.	7
7.	Security Considerations.	8
8.	Acknowledgments	8
9.	References	8
10.	Authors' Addresses	10
11.	Full Copyright Statement	10





Oefenen



[Blog](#) [Nieuws](#) [Presentaties](#) [FAQ](#) [Partners](#) [Over de coalitie](#) 

“Deze oefeningen zijn uniek in de wereld.”

6 april 2020

Gezamenlijke DDoS-oefeningen door Nederlandse anti-DDoS-coalitie

DDoS-aanvallen worden steeds groter en complexer. Reactief en individueel actie ondernemen is vaak onvoldoende. Daarom richtten we met enkele andere partijen de **Nederlandse anti-DDoS-coalitie** op. Deze coalitie deelt de karakteristieken van DDoS-aanvallen via een DDoS-clearinghouse en kennis over DDoS-aanvallen. Daarnaast houden de deelnemende partijen samen DDoS-oefeningen. Karl Lovink, Technical Lead Security Operations Center van de Belastingdienst, en Marc Groeneweg, Infrastructure & Security Architect bij SIDN, organiseren deze oefeningen. “Wij kunnen elk moment op de ‘rode knop’ drukken.”

Waarom is het zo belangrijk om samen in actie te komen tegen DDoS-aanvallen?

Lovink: “Iedereen heeft met DDoS-aanvallen te maken. Het is nooit slechts één partij die last heeft. Als DigiD niet werkt, kunnen mensen ook niet inloggen op de website van de Belastingdienst. Als Ziggo eruit ligt, kunnen hun klanten ook geen domeinnamen registreren. Daarom is samenwerken zo belangrijk. Samen hebben we enorm veel kennis. Als we die kennis delen en acties op elkaar afstemmen, zijn we weerbaarder en daar profiteert iedereen in Nederland van”.



Karl Lovink, Technical Lead Security Operations Center van de Belastingdienst

Zijn er meer landen waar gezamenlijk geoefend wordt?

Lovink: “Voor zover ik weet, zijn deze oefeningen uniek in de wereld. Het is vooral bijzonder dat publieke en private organisaties samenwerken binnen de anti-DDoS-coalitie. Hoort misschien ook bij de Nederlandse cultuur, waar we gewend zijn samen te werken voor het algemeen belang.”



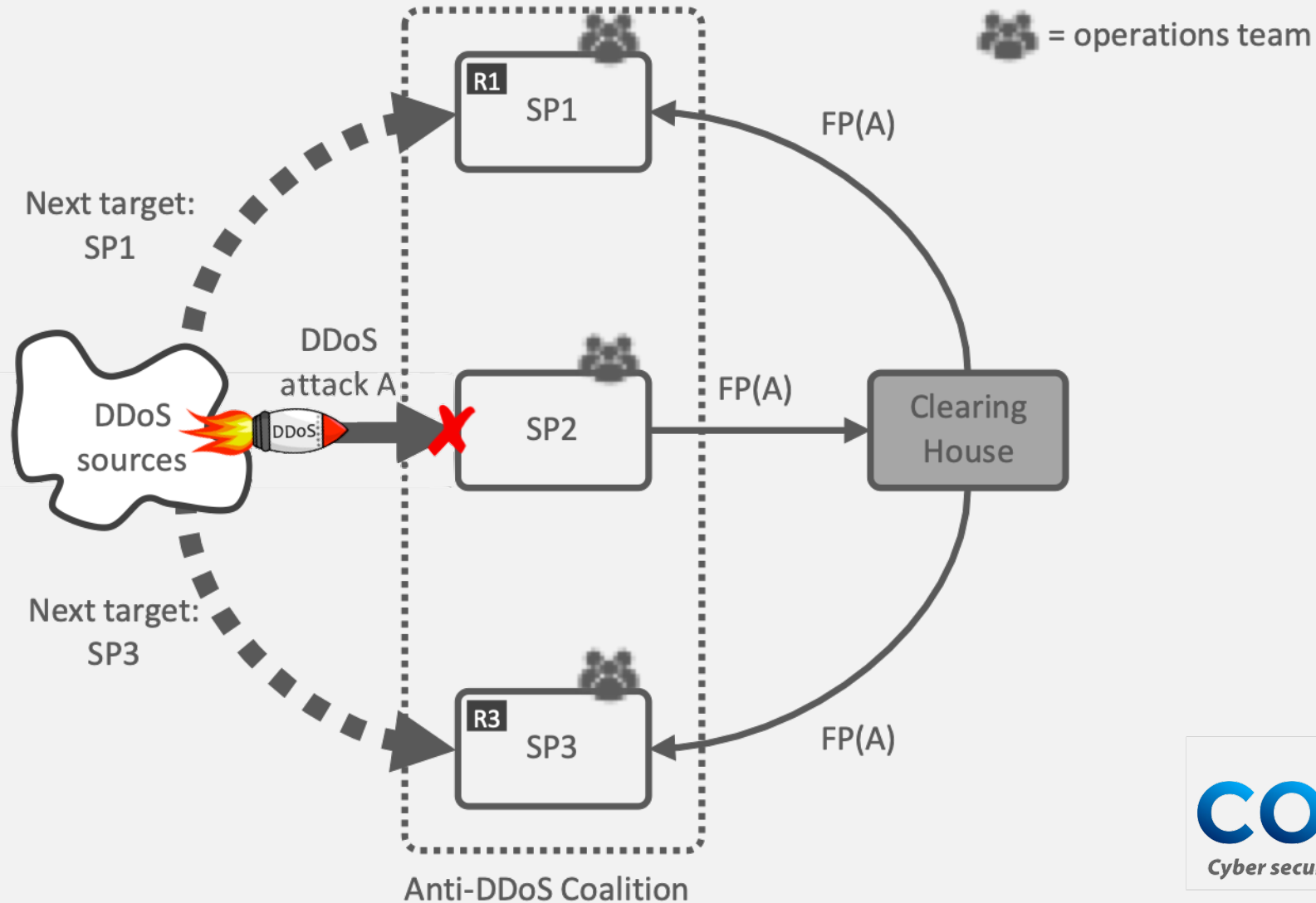
Juridisch



- 🎯 Vrijwaringsovereenkomst oefenen
- 🎯 Datasharing agreement oefenen
- 🎯 Overeenkomst Coalitie



Clearinghouse





Contactgegevens

Kernteam: Remco Ruiters
r.ruiters@betaalvereniging.nl

Clearinghouse: Cristian Hesselman
cristian.hesselman@sidn.nl

Secretaris: Mieke van Ulden
info@nomoreddos.org

www.nomoreddos.org

SIDN, SURFnet, and the University of Twente were partly funded by the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 830927. Project website: <https://www.concordia-h2020.eu/>