DDoS data rapport 2019

De wapenwedloop tussen aanvallers en DDoS-mitigatie nader bekeken

NBIP nationale beheersorganisatie internet providers

Colofon

Het NBIP DDoS data rapport 2019 is een uitgave van Stichting Nationale Beheersorganisatie Internet Providers.

Datum van uitgave
juni 2020, jaargang 3

Hoofdredactie
Octavia de Weerdt (NBIP)

Redactie
Gerald Schaapman (NBIP)

Bijdragen
NaWas operationeel team

Eindredactie
Wouter Pegtel (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

Vorm
Dit rapport is gemaakt in PDF-formaat

Samenvatting
DDoS-aanvallen blijven een hardnekkig probleem met een grote maatschappelijke impact. In 2019 waren aanvallen wederom groter en complexer dan het voorgaande jaar, een trend die stand lijkt te houden. Waakzaamheid blijft geboden.

Inhoudsopgave

Voorwoord

Voor u ligt alweer het derde jaaroverzicht met DDoS-data verzameld in 2019 door de Nationale DDoS Wasstraat (NaWas) van de stichting Nationale Beheersorganisatie Internet Providers (NBIP). Hierin leest u alles over de cijfers en trends rondom DDoS-aanvallen op een aanzienlijk deel van het 'Nederlandse internet'. De NaWas beschermt bijna 2,5 miljoen .nl domeinen.

De NaWas

De DDoS wasstraat is sinds 2014 operationeel en mitigeert 24/7 automatisch DDoS-aanvallen voor aangesloten deelnemers. Door gezamenlijk capaciteit, technologie en kennis en kunde in te kopen, is een uitermate effectieve bestrijding van DDoS-aanvallen mogelijk. De wasstraat 'wast' het DDoS-verkeer schoon en stuurt alleen het schone verkeer via een aparte VLAN naar de deelnemer. Zo blijven zijn systemen en diensten beschikbaar en wordt de DDoS-aanval onschadelijk gemaakt.

De NBIP en dit rapport

In 2017 is de NBIP gestart met het (half) jaarlijks publiceren van rapporten met uitgebreide informatie over DDoS-aanvallen. De rapporten geven een overzicht van het aantal DDoS-aanvallen, de grootte van de aanvallen, de duur van de aanvallen, de soorten aanvallen en de gesignaleerde trends zoals waargenomen in de NaWas. Overigens doet de NBIP veel meer dan alleen het opschonen van vervuild internetverkeer: samen met branchegenoten faciliteren we de detectie en bestrijding van online abuse zoals malware, spam, onrechtmatige content en beeldmateriaal van seksueel kindermisbruik. Ook het uitvoeren van tapvordeningen van opsporings- en veiligheidsdiensten behoren tot het takenpakket.

Het doel van dit rapport is om zoveel mogelijk kennis over DDoS-aanvallen met onze deelnemers, stakeholders en geïnteresseerden te delen. Binnen de NBIP is veel kennis over dit onderwerp aanwezig. Alleen door een gezamenlijke aanpak van alle betrokken partijen zijn we de komende jaren in staat om DDoS-aanvallen het hoofd te bieden. Want één ding is zeker: DDoS-aanvallen zijn een permanente bedreiging voor een veilig en stabiel internet en er is geen reden om te verwachten dat dit binnen enkele jaren verandert. De NBIP wil daarom met de informatie uit dit rapport zijn kennis over DDoS-aanvallen, de risico's die met dit soort aanvallen gepaard gaan, manieren van mitigatie en preventie delen met aangesloten partijen, stakeholders en geïnteresseerden. Daarbij helpt inzicht in de trends en ontwikkelingen van het afgelopen jaar.

Intensieve samenwerking geeft nieuwe inzichten en mogelijkheden

Omdat steeds meer organisaties en sectoren onderkennen dat DDoS-aanvallen een permanente dreiging zijn die ook hen raakt, zijn intensievere samenwerkingen bij de bestrijding van deze aanvallen mogelijk. Zo is in 2018 gestart met de anti-DDoS coalitie, een samenwerking tussen inmiddels 18 organisaties waaronder telecom providers, financiële instellingen, overheidsorganisaties, politie en de digitale sector.

Recent is het eerste proof of concept voor een DDoS clearinghouse afgerond, waarbij samenwerkende partijen veel informatie delen over DDoS-aanvallen. Ook worden levensechte simulaties uitgevoerd, waarbij de ene organisatie letterlijk een DDoS-aanval uitvoert op de andere. Op die manier wordt veel waardevolle kennis en ervaring opgedaan over hoe DDoS-aanvallen zijn te herkennen en mitigeren, en hoe organisaties en hun medewerkers om moeten gaan met een aanval.

De NaWas in 2020

Tot slot: 2020 is nu al een uitzonderlijk jaar door de coronacrisis en alle gevolgen die deze crisis heeft. De NBIP deelt waar mogelijk achter de schermen kennis en biedt hulp als dat nodig is. We bieden hulp aan ziekenhuizen en andere zorginstellingen als zij daar behoefte aan hebben. We onderzoeken voortdurend hoe de NaWas kan bijdragen aan de enorme inspanning die we als samenleving leveren om deze crisis de baas te kunnen.

De NaWas is ooit opgericht met het idee ‘samen sta je sterker’. Dat is op dit moment meer dan ooit zo, en we zullen die missie met grote toewijding blijven uitvoeren.

Met vriendelijke groet,

Octavia de Weerdt

Algemeen directeur NBIP

1. Inleiding

Nog niet zo lang geleden was er behoorlijk wat kennis en geduld nodig om een DDoS-aanval uit te kunnen voeren. Dat is tegenwoordig niet meer zo: je kunt met een paar muisklikken en een creditcard illegaal DDoS-aanvallen kopen op het darkweb of het reguliere internet. Je zou denken dat daarmee het aantal DDoS-aanvallen snel toeneemt, maar dat blijkt in de praktijk mee te vallen zo blijkt uit dit rapport: er was in 2019 zelfs sprake van een lichte daling van het aantal DDoS-aanvallen dat de NaWas afhandelde.

DDoS-aanvallen blijven niettemin een ernstig maatschappelijk probleem die tot grote ontwrichting kunnen leiden. Hoewel in 2019 grote aanvallen met forse impact, zoals die zich in januari 2018 voordeden, uitbleven, moeten we waakzaam blijven.

DDoS-aanvallen in het nieuws

Aan nieuws over DDoS-aanvallen was in 2019 geen gebrek. Burgers, consumenten, studenten, leerlingen en bedrijven hebben in Nederland op verschillende manieren last gehad van DDoS-aanvallen in 2019. Een kleine greep:

In de Tweede Kamer werd in februari gedebatteerd over de vraag of de wet voldoende mogelijkheden biedt om de verkoop van DDoS-aanvallen te bestrijden. In maart en ook in april was een veelgebruikte online leeromgeving voor middelbare scholen lange tijd overbelast door DDoS-aanvallen. De Nederlandstalige Wikipedia was in september 2019 urenlang onbereikbaar door een wereldwijde DDoS-aanval. In oktober werden vijf servers die een botnet aanstuurden in Amsterdam offline gehaald. En begin december moest de Radboud Universiteit Nijmegen een tentamen afblazen vanwege herhaalde DDoS-aanvallen.

> Wie een DDoS-aanval wil uitvoeren hoeft geen technische kennis te bezitten.

Het feit dat er niet veel meer van dit soort nieuws is, is te danken aan het groeiende besef dat niemand immuun is voor DDoS-aanvallen en dat het dus noodzakelijk is om voorzorgsmaatregelen te nemen. Bij de NaWas doen we dat sinds 2014 als collectief zonder winstoogmerk. Inmiddels heeft de NaWas vele duizenden DDoS-aanvallen geneutraliseerd.

Jaarlijkse rapportage

De NaWas neemt jaarlijks vele honderden DDoS-aanvallen waar. Deze waarnemingen geven inzicht in hoe DDoS-aanvallen evolueren. De NBIP deelt deze inzichten om het internet voor iedereen veiliger te maken. Daarom publiceert de NBIP ieder jaar het DDoS data rapport. We zien trends opduiken, of kunnen juist constateren dat sommige ontwikkelingen helemaal geen trends zijn. Het biedt de lezer hopelijk houvast om op basis van een substantiële hoeveelheid door de jaren heen waargenomen DDoS-aanvallen inzicht te krijgen in hoe deze dreiging zich jaar op jaar ontwikkelt.

Dit rapport richt zich op de lezer met enige basiskennis over DDoS-aanvallen en hoe zij werken. Wie nog onbekend is met bepaalde termen, kan de bijlage achter in dit rapport raadplegen.

2. DDoS - de basis

Om de impact van een DDoS-aanval te begrijpen, is het nodig om te weten hoe zo'n aanval precies werkt, wat er kan gebeuren tijdens en na een DDoS-aanval en hoe dit is tegen te gaan.

Hoe werkt een DDoS-aanval?

Wat is een DDoS-aanval? DDoS staat voor Distributed Denial of Service. Om een DDoS-aanval uit te voeren, heeft een aanvaller verschillende opties. De meest bekende is het infecteren van een flink aantal computers of andere aan internet gekoppelde apparaten. Dit wordt gedaan met bijvoorbeeld malware of via e-mail attachments. Zo ontstaat een 'botnet', een netwerk van geïnfecteerde devices. Vervolgens wordt dit netwerk de opdracht gegeven data naar de server van het doelwit te sturen, met als doel een overbelasting van die server. Als de server het verkeer niet meer aankan, en gebruikers dus niet meer bij de servers kunnen, is de aanval geslaagd.

De meest voorkomende manier om een DDoS-aanval op te zetten is echter niet via botnets, maar via zogenaamde 'amplification'. Hierbij worden servers niet geïnfecteerd, maar worden zij wel misbruikt om een DDoS-aanval op te zetten. Daarnaast hoeft een DDoS-aanval niet altijd gericht te zijn op het overbelasten van servers, maar kan ook worden geprobeerd de bandbreedte die een server beschikbaar heeft voor inkomend verkeer te overbelasten, waardoor de server ook niet langer bereikbaar is.

Wie een DDoS-aanval wil uitvoeren hoeft geen technische kennis te bezitten. Op speciale websites (het zijn er duizenden) kunnen DDoS-aanvallen worden gekocht, en niet alleen op het darkweb. Ook kan met relatief weinig voorkennis zelf een aanval worden opgetuigd: handleidingen om een eigen botnet op te zetten zijn eenvoudig te vinden en ook kennis voor aanvallen met andere tactieken is ruim voorhanden.

> Een aanval uitvoeren is makkelijker door het stijgende aantal DDoS-diensten vanuit de cloud.

Waarom zijn DDoS-aanvallen zo populair?

Een DDoS-aanval is nog steeds de meest voor de hand liggende wijze om een website of online diensten te ontregelen. Maar er is meer aan de hand. Er zijn enkele factoren die het gemak en de aantrekkelijkheid van dit type aanvallen in stand houden.

Ten eerste wordt het uitvoeren van een aanval makkelijker door het stijgende aantal DDoS- diensten die vanuit de cloud worden geleverd. Hosting is goedkoop en er is steeds meer bandbreedte beschikbaar. Het kopen van malafide diensten op het internet wordt dus steeds eenvoudiger en betaalbaarder. Deze diensten worden via zogenaamde 'stressers' of 'booters' ingekocht. Verreweg de meeste DDoS-aanvallen komen via een dergelijke tussenpartij.

Ook profiteren booters van aantrekkelijke businessmodellen gericht op snelle winst. Aanvallen die via booters worden ingekocht zijn

niet eens heel geavanceerd, en dat is ook niet in het belang van de booter service provider. Omdat deze zo snel mogelijk geld willen verdienen met zo min mogelijk moeite, verdwijnen booters dan ook net zo snel als dat ze zijn verschenen.

Omdat aanvallen zo eenvoudig kunnen worden aangeschaft, betekent dat ook dat meer mensen met minder technische kennis een DDoS-aanval kunnen uitvoeren. Omdat het relatief eenvoudig is om met weinig moeite rumoer te veroorzaken, of om je huiswerk te ontlopen, is een DDoS-aanval een populair misdrijf.

Daarnaast is het Internet of Things (IoT) een niet te onderschatten ontwikkeling die de frequentie en de eenvoud van DDoS-aanvallen in stand houdt. Van tandenborstels tot thermostaten: meer en meer apparaten hebben een internetverbinding. Vaak gaat het om apparaten met een slechte (of geen) standaard beveiliging. En dus vormen IoT-devices een makkelijk doelwit om te dienen als pion in een botnet. Onderzoeksbureau Gartner schat dat er ruim 25 miljard van dat soort apparaten zullen circuleren in het jaar 2021.

Gevolgen van een DDoS-aanval

De gevolgen van een DDoS-aanval zijn divers. Van kleine irritatie tot grote ontregelingen,het is allemaal mogelijk. Van een aanval kan één persoon heel erg last hebben (zijn of haar persoonlijke blog ligt er bijvoorbeeld uit), of een groot deel van de samenleving (internetbankieren doet het niet).

Dat een gerichte DDoS-aanval voor financiële schade kan zorgen, heeft de NBIP vorig jaar samen met Stichting Internet Domeinregistratie Nederland (SIDN) onderzocht. Uit het rapport 'Impact van DDoS-aanvallen in Nederland' blijkt dat de economische impact enorm is: de door NBIP en SIDN onderzochte bedrijven en organisaties hebben in 2018 ongeveer 425 miljoen euro misgelopen. Betrek je heel het bedrijfsleven, dan is de schade minimaal een miljard euro.

Ook bleek uit dat onderzoek dat er veel nevenschade optreedt. Vooral als een bedrijf een shared hosting-oplossing bij een ISP heeft, waarbij er meerdere websites op 1 server gehost worden. Een website kan bijvoorbeeld ten prooi vallen aan een DDoS-aanval, terwijl het niet het doelwit is, doordat de aanval op een ander doelwit is gericht op dezelfde server.

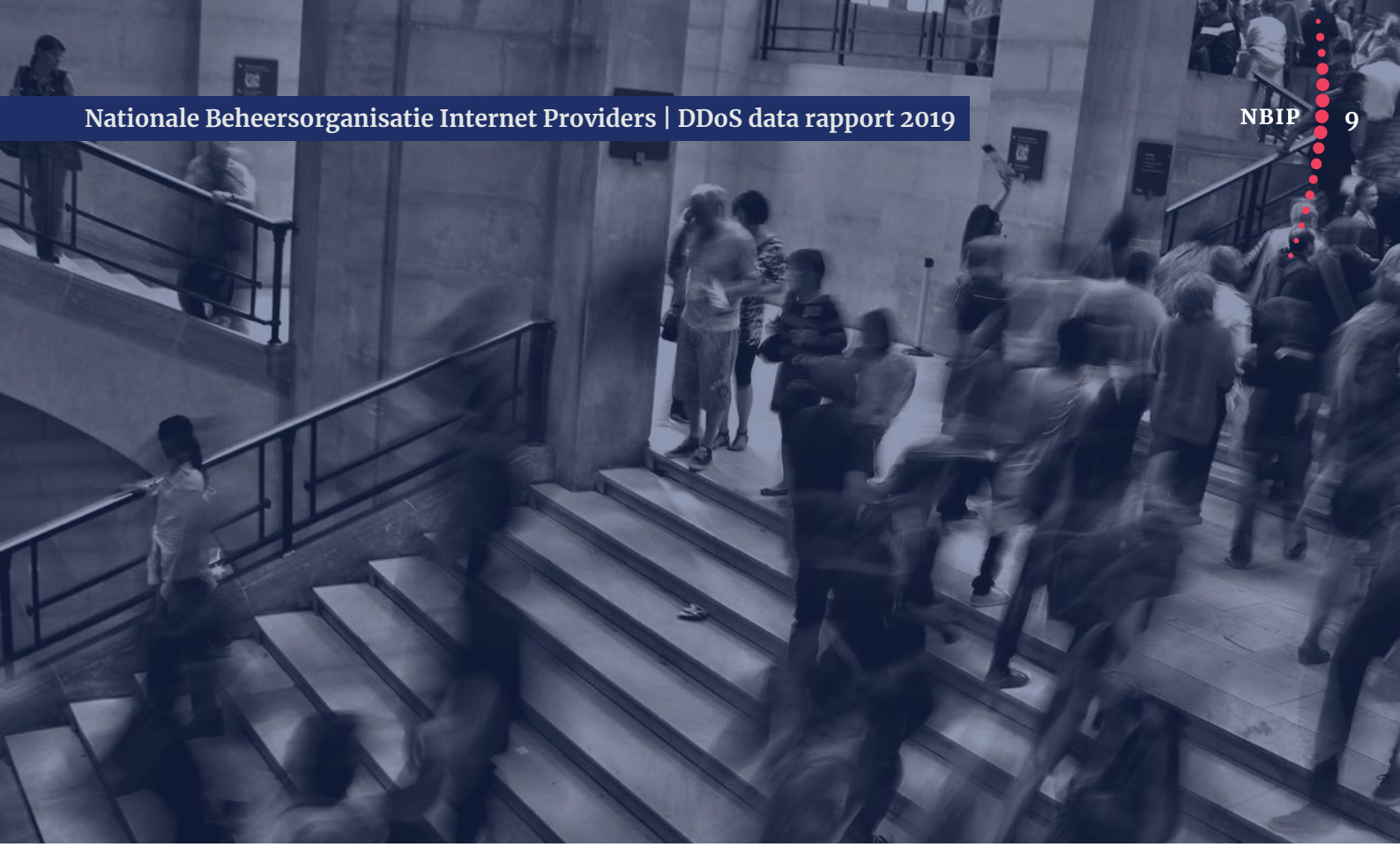
Methoden van DDoS-mitigatie

Om DDoS-aanvallen af te wenden zijn er verschillende soorten maatregelen te nemen. Deze variëren van extreem en rigoureus tot verfijnd en subtiel.

"Blackholing" of het "wegsluizen" van verkeer is een vrij extreme methode van DDoS-mitigatie. Om een DDoS-aanval af te wenden, wordt er geen verkeer meer toegelaten. Hierdoor is het voor niemand mogelijk de website te bezoeken.

Een iets subtielere vorm van mitigatie is geografische IP-blocking: hierbij wordt al het verkeer buiten een bepaalde geografische locatie helemaal uitgezet. Dit is een redelijk effectieve manier, maar staat ook te boek als grof geschut. Immers, vele bezoekers worden alsnog uitgesloten.

Het concept van een "wasstraat" is op dit moment één van de meest verfijnde en intelligente bestrijdingsmiddellen. Hierbij wordt malafide verkeer langs anti-DDoS apparatuur geleid, waarna het verkeer 'schoon' teruggestuurd wordt ("scrubbing").



3. Methode

Welke manieren van dataverzameling zijn gebruikt, welke data wordt geanalyseerd, en waarom zijn bepaalde onderzoekskeuzes gemaakt?

Dataverzameling

In het vorige hoofdstuk is het principe van een 'wasstraat', zoals de NaWas, uitgelegd. De NBIP heeft de beschikking over een registratiesysteem waarin alle soorten DDoS-aanvallen die hebben plaatsgevonden op NaWas-deelnemers, worden opgeslagen. Deelnemers kunnen deze data ook zelf zien in een afgeschermd portaal.

Het registreren van een type DDoS- aanval in dat systeem is procedureel vastgelegd binnen het operationele team van de NaWas. Vervolgens werd data uit dit registratiesysteem geselecteerd ten behoeve van de rapportage.

De data is afkomstig van aanvallen op deelnemers van de NaWas. Hierbij moet opgemerkt worden dat dit niet om elke deelnemer gaat - immers niet elke deelnemer heeft te maken gehad met een DDoS-aanval. Vanwege veiligheids- en privacy maatregelen voor deze deelnemers en de contractuele verplichting die de NBIP jegens haar deelnemers heeft, is niet vrijgegeven hoe vaak een bepaalde ISP is aangevallen of welke providers dit überhaupt zijn.

Voor dit onderzoek is data van deelnemers aan de NaWas geanalyseerd. Eind 2018 betrof het data van 68 deelnemers. Eind 2019 had de NaWas 74 deelnemers.

Deze deelnemers bestaan grotendeels uit internet service providers (ISP's). Met ISP wordt in dit onderzoek een bedrijf of organisatie bedoeld dat online diensten en/of toegang tot internet aan klanten bieden.

In het geval van de deelnemers aan de NaWas zijn dit voornamelijk bedrijven die cloud- en hostingdiensten aanbieden. In heel Nederland zijn er ongeveer 1500 van dit soort bedrijven (onderzoek The METISfiles).

De NaWas heeft een groot aandeel in de Nederlandse internetsector. Uit het impact-onderzoek met SIDN blijkt dat de NBIP 43% van alle .nl-domeinen beschermt tegen DDoS-aanvallen. Dat betekent dat minstens 2,5 miljoen domeinen kunnen rekenen op DDoS-mitigatie van de NaWas. De cijfers in dit rapport zullen nooit helemaal een compleet beeld van de situatie in Nederland geven, maar bieden wel een uiterst representatief inzicht.

Deelnemers aan de NaWas zijn niet gelimiteerd tot ISPs. Er zijn ook enkele grote organisaties die meedoen, zoals banken en verzekeraars. Deelnemers kunnen dus zowel klein als groot zijn.

Verantwoording

Voor dit onderzoek is gekozen om de grootte van de aanvallen in Gbps (gigabit per second) te meten. Een uitleg van de termen en soorten aanvallen is in een bijlage opgenomen. Zoals gemeld in het voorwoord, gaat dit rapport uit van lezers met enige kennis van zaken.

In enkele grafieken is gekozen voor het maken van een top 10 in plaats van een compleet overzicht om de overzichtelijkheid te bevorderen en de resultaten voor de lezer zo helder mogelijk te maken.

4. Resultaten DDoS cijfers 2019

In dit rapport maken we een analyse van het aantal, de grootte en de duur van DDoS-aanvallen in 2019. We schenken daarnaast ook aandacht aan:

- Soorten DDoS-aanvallen
- Opvallende DDoS-aanvallen in 2019
- Nieuwe typen DDoS-aanvallen in 2019
- Trends die uit de data kunnen worden afgeleid

4.1 Aantal DDoS-aanvallen

In het jaar 2019 zijn 919 DDoS-aanvallen geregistreerd door de NaWas. Dit zijn gemiddeld ca. 2,5 DDoS-aanvallen per dag. In 2018 werden 938 DDoS-aanvallen geregistreerd. Dit betekent een lichte afname van twee procent in 2019 ten opzichte van het jaar daarvoor, gebaseerd op absolute aantallen, terwijl het aantal deelnemers van de NaWas met bijna 10% groeide. Het zou daarom mogelijk kunnen zijn dat de daling van het aantal DDoS-aanvallen in 2019 groter is dan twee procent. Zeker is in ieder geval dat de forse groei die van 2017 op 2018 zichtbaar was, niet heeft doorgezet in 2019.

Die constatering is op zichzelf verrassend, want in het halfjaar rapport over 2019 spraken we nog voorzichtig de verwachting uit dat het aantal DDoS-aanvallen in 2019 het aantal van 2018 ou overtreffen. Die uitspraak baseerden we op het feit dat we in het eerste half jaar van 2019 572 aanvallen hebben waargenomen, ruim meer dan de helft van het aantal in 2018. Die groei vlakte, zo kunnen we nu zien, al in juni 2019 af.

In geen enkele maand na juni kwam het aantal aanvallen nog boven de 100 uit, terwijl in de eerste helft van 2019 in zowel januari, april als mei meer dan 100 aanvallen werden gemitigeerd door de NaWas. In 2018 zagen we een bijna vergelijkbaar patroon: de meeste aanvallen per maand werden in maart en april waargenomen.

De rustigste maand was augustus 2019 met slechts 19 geregistreerde aanvallen. In augustus 2018 werden 49 aanvallen geregistreerd. Dit is een daling van ruim 61%. De maand met de minste aanvallen in 2018 was de maand oktober: toen werden 38 aanvallen geregistreerd. Kijken we naar de maand oktober 2019, dan zien we 66 DDoS-aanvallen: een stijging van 73%.

4.2 Grootte van een DDoS-aanval

We drukken de grootte van DDoS-aanvallen uit in gigabit per seconde, ofwel Gbps. Hieronder is in een grafiek inzichtelijk gemaakt hoe het totaal aan DDoS-aanvallen is verdeeld over de categorieën DDos-aanvallen kleiner dan 1 Gbps, tussen 1-10 Gbps, tussen 10-20 Gbps, tussen 20-40 Gbps, groter dan 40 Gbps en het totaal.

Om inzicht te geven in hoe DDoS-aanvallen zich ontwikkelen over een langere termijn, zijn ook de tabellen voor 2017 en 2018 opgenomen.

maanden	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	totaal
Jan-2017	12	53	4	1	0	70
Feb-2017	11	16	6	4	0	37
Mrt-2017	34	37	9	3	0	83
Apr-2017	20	29	8	0	0	57
Mei-2017	22	58	7	2	0	89
Jun-2017	34	41	8	1	0	84
Jul-2017	17	17	2	0	0	36
Aug-2017	12	16	2	1	0	31
Sep-2017	14	33	6	1	0	54
Okt-2017	44	50	9	6	0	109
Nov-2017	34	31	5	4	0	74
Dec-2017	40	56	5	1	0	102
Eindtotaal	**294**	**437**	**71**	**24**	**0**	**826**

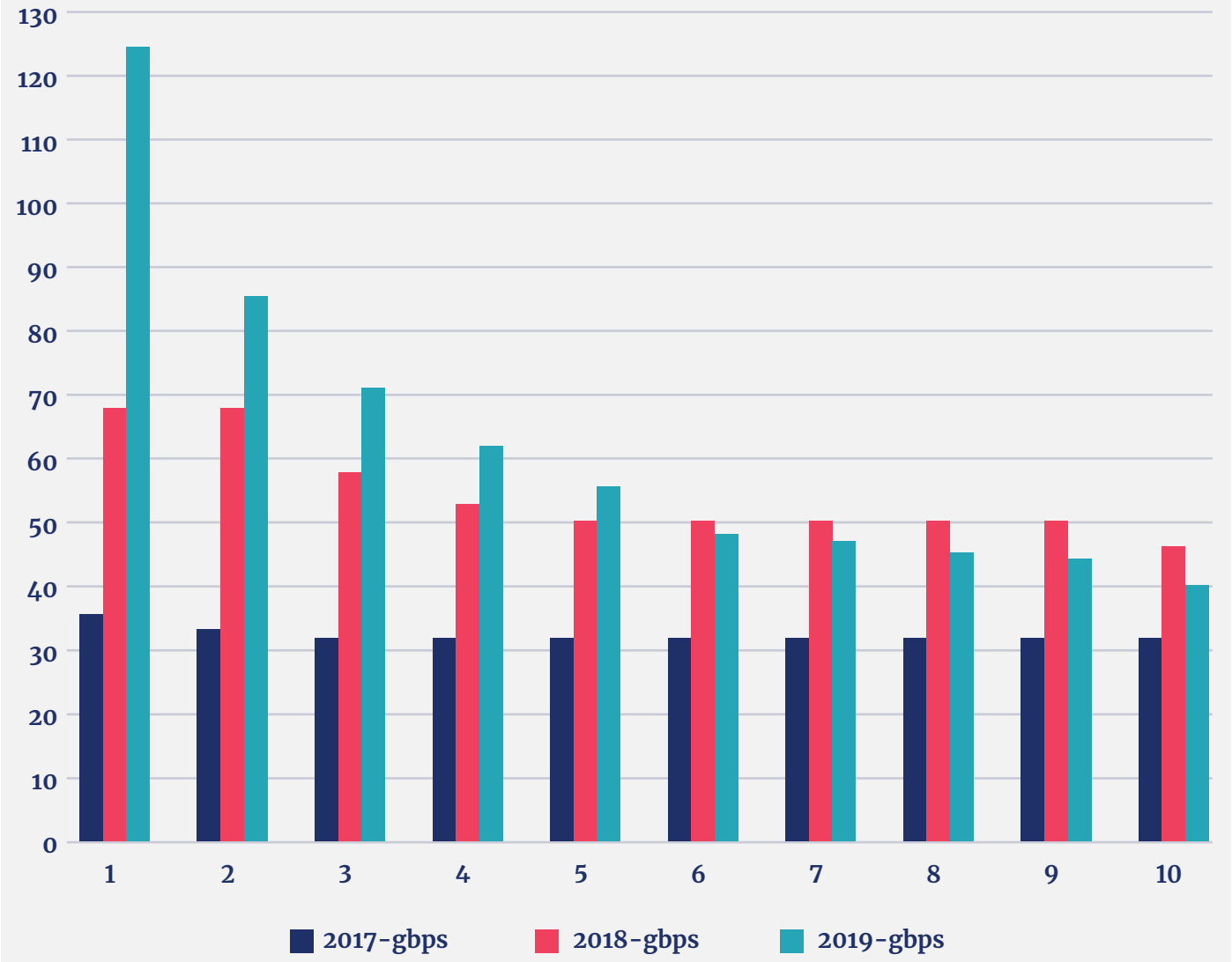
maanden	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	totaal
Jan-2018	26	55	3	14	1	99
Feb-2018	34	42	4	1	2	83
Mrt-2018	33	57	20	3	0	113
Apr-2018	44	55	9	2	0	110
Mei-2018	43	22	5	0	0	70
Jun-2018	32	43	4	0	1	80
Jul-2018	18	32	2	3	1	56
Aug-2018	22	20	2	4	1	49
Sep-2018	33	38	3	4	1	79
Okt-2018	10	27	0	1	0	38
Nov-2018	32	53	6	2	3	96
Dec-2018	35	25	4	0	1	65
Eindtotaal	**362**	**469**	**62**	**34**	**11**	**938**

maanden	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	totaal
Jan-2019	32	70	9	4	1	116
Feb-2019	18	39	8	3	3	71
Mrt-2019	42	35	1	0	1	79
Apr-2019	25	72	15	5	2	119
Mei-2019	40	61	4	5	0	110
Jun-2019	26	41	3	0	1	71
Jul-2019	12	25	2	1	0	40
Aug-2019	7	9	0	0	0	16
Sep-2019	24	57	3	1	0	85
Okt-2019	13	49	2	2	0	66
Nov-2019	14	51	5	1	2	73
Dec-2019	20	40	9	3	1	73
Eindtotaal	**273**	**549**	**61**	**25**	**11**	**919**

jaar	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps
2017	35,6%	52,9%	8,6%	2,9%	0%
2018	38,6%	50%	6,6%	3,6%	1,2%
2019	29,7%	59,7%	6,6%	2,7%	1,2%

Ten opzichte van 2018 zien we in 2019 een daling aandeel van aanvallen kleiner dan 1 Gbps, maar er is een flinke stijging van het aantal aanvallen tussen de 1 en 10 Gbps. Het aandeel in het totaal aantal aanvallen van aanvallen tussen de 10 en 20 Gbps blijft gelijk aan 2018. Alleen bij de aanvallen met een kracht tussen 20-40 Gbps zien we in 2019 een kleine daling. Het aantal grote aanvallen van 40 Gbps of groter bleef gelijk.

2017 - 2019 top 10 Gbps



4.3 Duur van een DDoS-aanval

Ten opzichte van 2018 zien we in 2019 het aantal aanvallen korter dan 15 minuten van 323 naar 405 toenemen. Het aantal aanvallen met een tijdsduur tussen de 15 en 60 minuten daalt in dezelfde periode van 430 naar 378. Het aantal aanvallen met een tijdsduur tussen 1 en 4 uur daalt van 156 naar 107. In 2019 werden net als in 2018 29 aanvallen geregistreerd die langer dan 4 uur duurden.

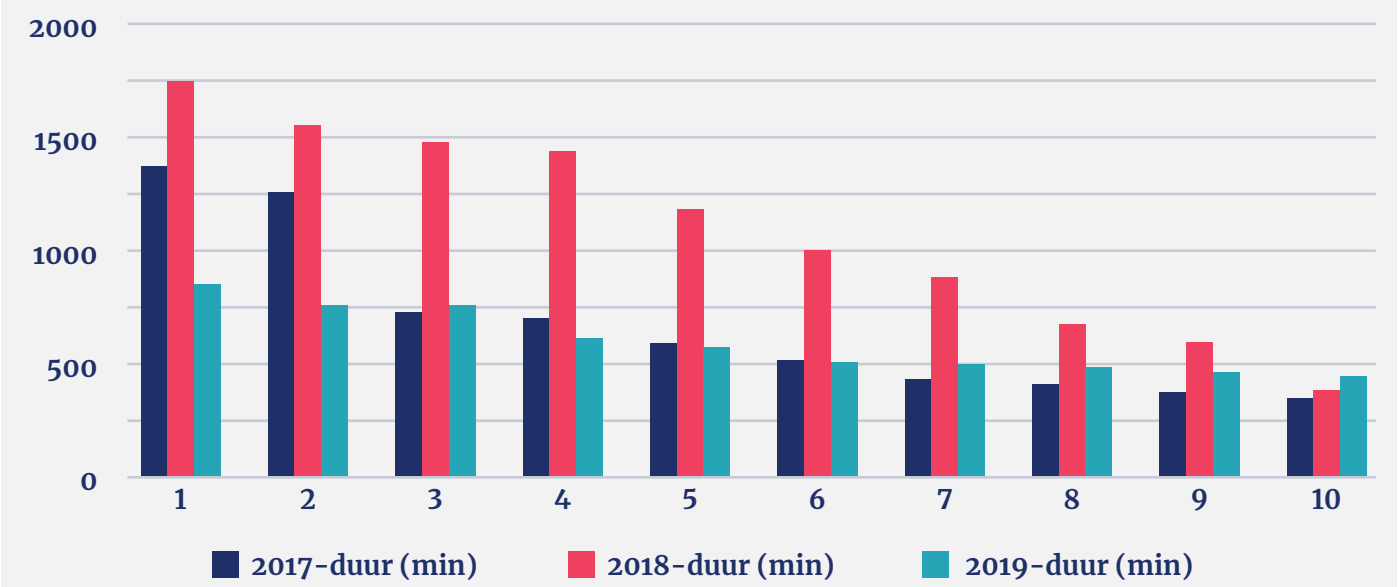
maanden	< 15 min	15-60 min	1-4 uur	> 4 uur	totaal
Jan-2017	29	29	7	5	70
Feb-2017	18	9	7	3	37
Mrt-2017	34	23	21	5	83
Apr-2017	28	24	4	1	57
Mei-2017	46	28	14	1	89
Jun-2017	36	36	9	3	84
Jul-2017	12	14	8	2	36
Aug-2017	12	12	7	0	31
Sep-2017	15	31	8	0	54
Okt-2017	18	58	32	1	109
Nov-2017	18	34	17	5	74
Dec-2017	43	42	15	2	102
Eindtotaal	**309**	**340**	**149**	**28**	**826**

maanden	< 15 min	15-60 min	1-4 uur	> 4 uur	totaal
Jan-2018	40	37	20	2	99
Feb-2018	30	41	11	1	83
Mrt-2018	44	47	20	2	113
Apr-2018	41	46	19	4	110
Mei-2018	20	39	9	2	70
Jun-2018	30	38	11	1	80
Jul-2018	15	26	11	4	56
Aug-2018	10	27	9	3	49
Sep-2018	19	44	15	1	79
Okt-2018	12	17	8	1	38
Nov-2018	32	43	17	4	96
Dec-2018	30	25	6	4	65
Eindtotaal	**323**	**430**	**156**	**29**	**938**

maanden	< 15 min	15-60 min	1-4 uur	> 4 uur	totaal
Jan-2019	53	54	9	0	116
Feb-2019	40	24	7	0	71
Mrt-2019	41	28	7	3	79
Apr-2019	33	38	34	14	119
Mei-2019	46	42	18	4	110
Jun-2019	34	28	7	2	71
Jul-2019	14	24	2	0	40
Aug-2019	10	4	2	0	16
Sep-2019	36	41	7	1	85
Okt-2019	28	33	5	0	66
Nov-2019	37	31	4	1	73
Dec-2019	33	31	5	4	73
Eindtotaal	**405**	**378**	**107**	**29**	**919**

jaar	< 15 min	15-60 min	1-4 uur	> 4 uur
2017	37,4%	41,2%	18,3%	3,4%
2018	34,4%	45,9%	16,6%	3,1%
2019	44,1%	41,2%	11,6%	3,2%

2017 - 2019 top 10 duur (min)



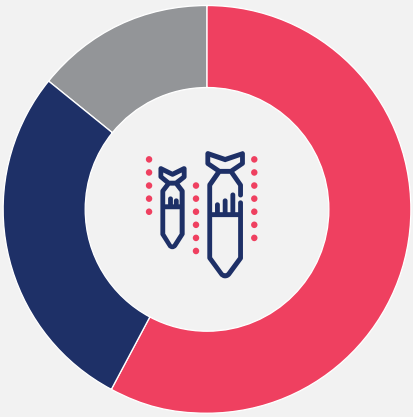
4.4 Soorten DDoS-aanvallen

In 2018 hebben we 56 soorten DDoS-aanvallen waargenomen. In 2019 is dit aantal gedaald naar 49 soorten aanvallen. De NBIP maakt in dit verband een onderscheid tussen drie DDoS-hoofdtypen met daaronder verschillende subtypen: TCP flood, UDP flood en UDP amplification.

Ten opzichte van het jaar 2018 zien we in 2019 een toename van het aanvalstype UDP amplification en een afname van het type TCP flood. Deze percentages bedroegen in 2018 nog respectievelijk 51% en 33%, waar dit in 2019 56% en 28% was. Afgezet tegen de cijfers van 2017 lijkt er jaarlijks sprake te zijn van een kleine schommeling in de populariteit van UDP amplification en TCP flood aanvallen, terwijl het aandeel van het type UDP flood in het totaal jaar op jaar in mindere mate schommelt.

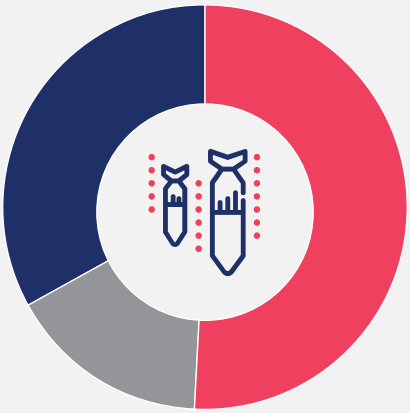
> Ten opzichte van het voorgaande jaar zien we in 2019 een duidelijke toename van het aanvalstype UDP amplification.

DDoS-type hoofdgroep verdeling 2017



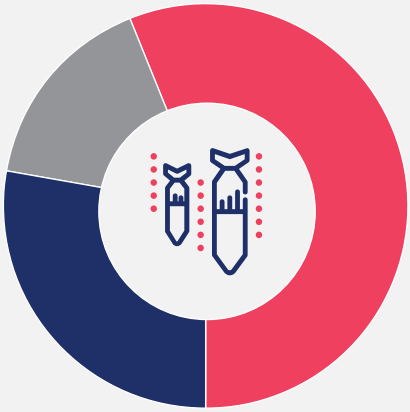
28% TCP flood
58% UDP amplification
14% UDP flood

DDoS-type hoofdgroep verdeling 2018



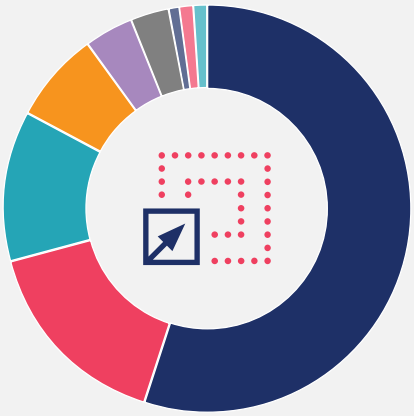
33% TCP flood
51% UDP amplification
16% UDP flood

DDoS-type hoofdgroep verdeling 2019



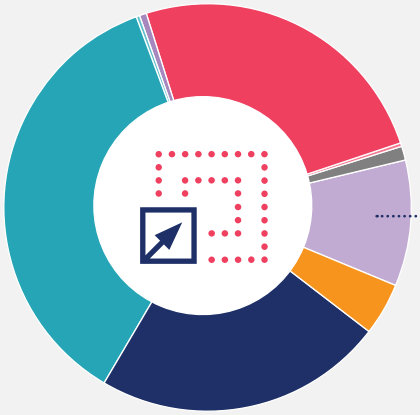
28% TCP flood
56% UDP amplification
16% UDP flood

UDP amplification DDoS-types 2017



55% DNS
16% NTP
12% LDAP
7% Chargen
4% Netbios
3% SSDP
1% RIPv1
1% RPC port
1% SNMP

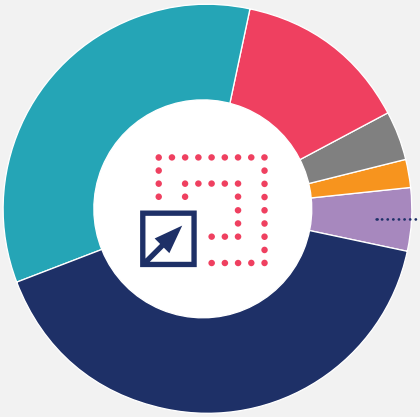
UDP amplification DDoS-types 2018



- 36% LDAP
- 25% NTP
- 23% DNS
- 10% Overig
- 4% Chargen
- 1% RPC port
- 0,5% Netbios
- 0,4% MS SQL monitor
- 0,1% RIPv1

- 0,5% UDP memcached
- 0,4% UDP flood
- 6% SSDP
- 3% SNMP
- 0,1% Sentinel

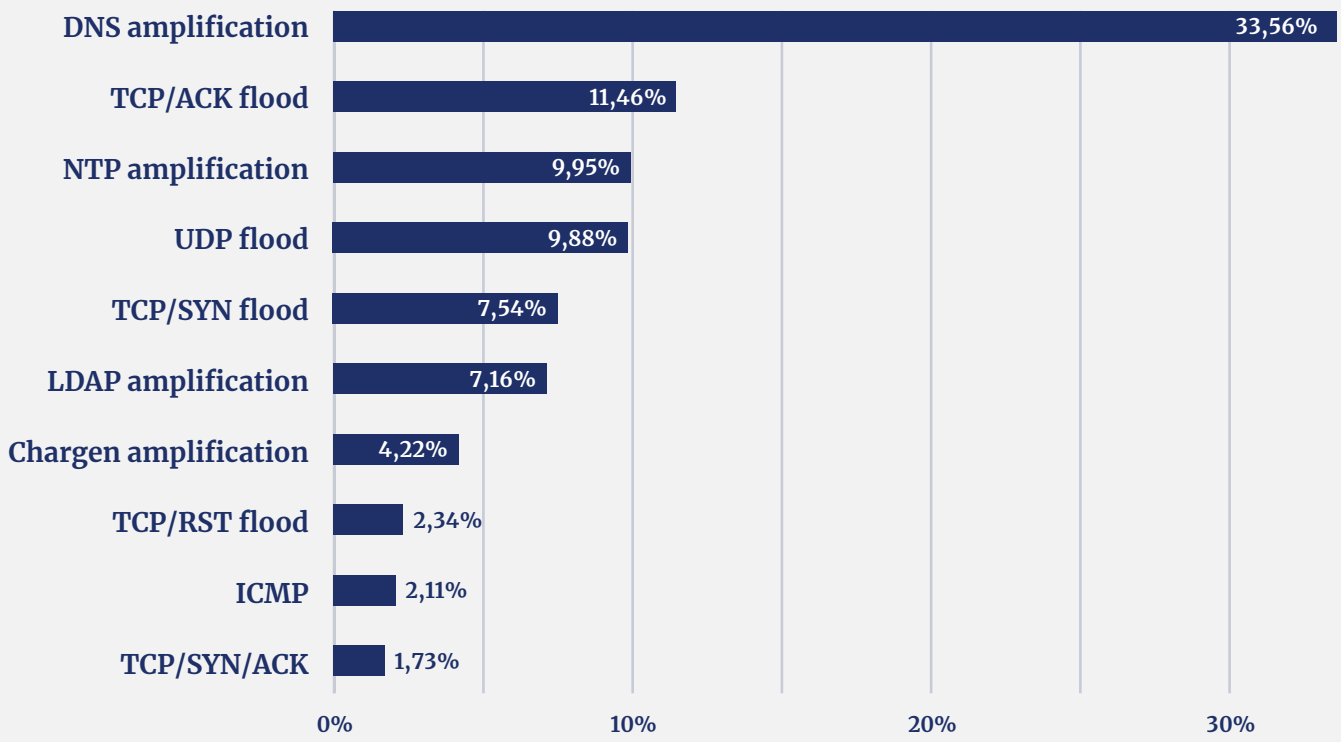
UDP amplification DDoS-types 2019



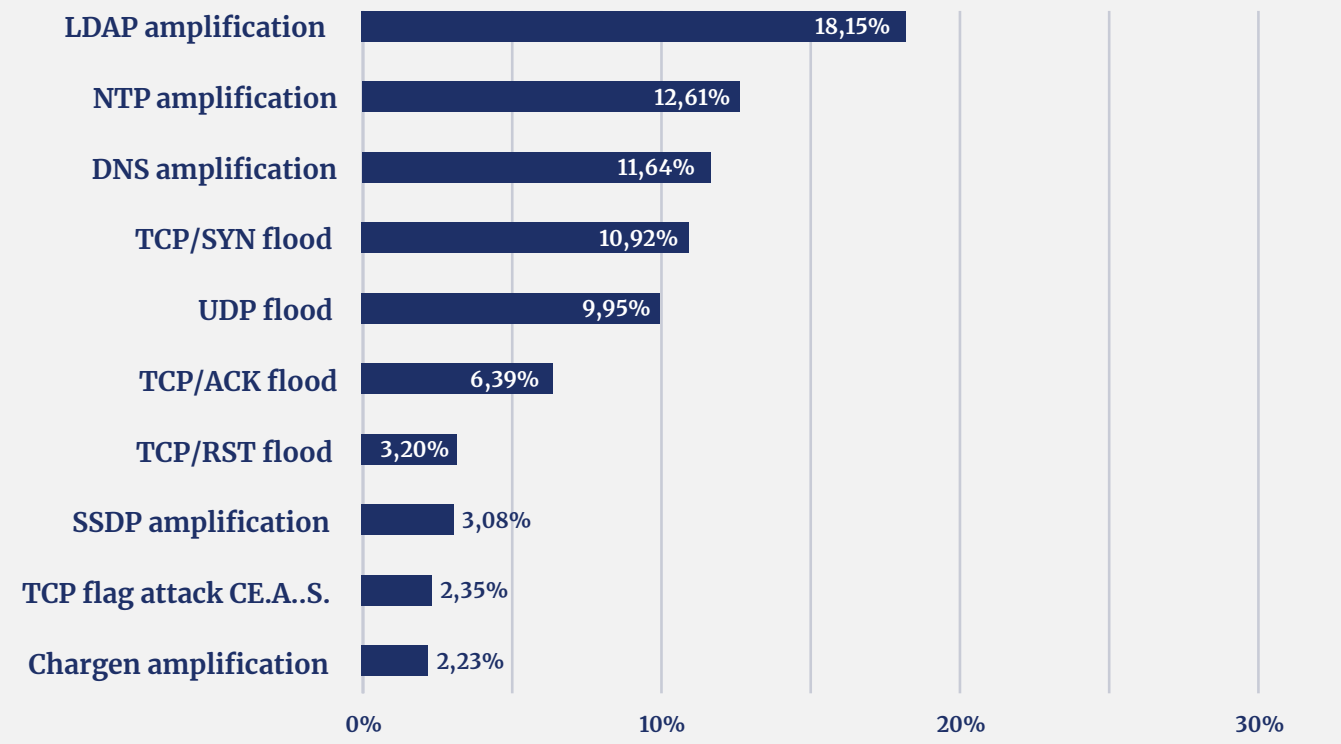
- 41% DNS
- 34% LDAP
- 14% NTP
- 4% SSDP
- 2% Chargen
- 5% Overig

- 1,4% MS SQL monitor
- 1% RPC port
- 0,8% ARMS
- 0,6% SNMP
- 0,6% UDP memcached
- 0,2% IPMI
- 0,2% NBNS
- 0,2% Netbios

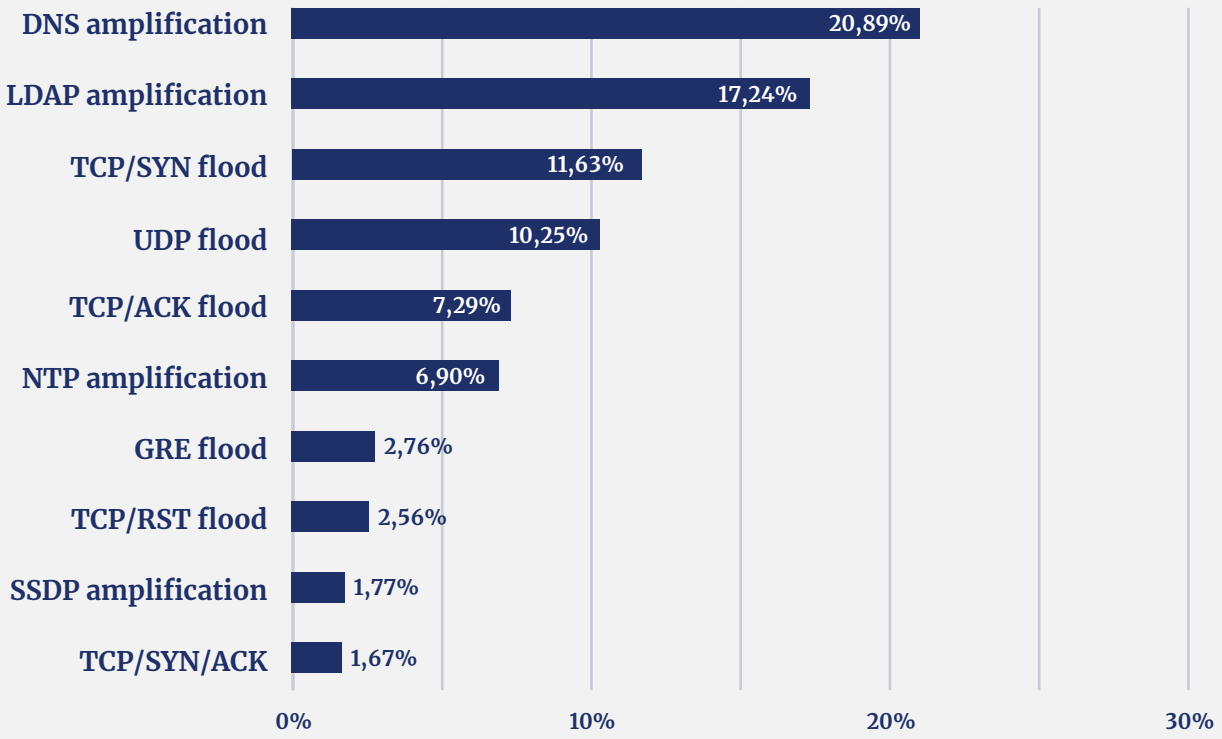
DDoS-type top 10 2017



DDoS-type top 10 2018



DDoS-type top 10 2019



In 2018 stond de LDAP amplification met een aandeel van 18,15% bovenaan in de lijst DDoS-type top 10 2018. In 2019 is DNS amplification met een aandeel van ruim 20% het meest voorkomende DDoS-type aanval. In 2017 scoorde DNS amplification ook hoog met een percentage van 33,56%. LDAP amplification blijft overigens ook populair. Opvallend is dat NTP amplification, vorig jaar nog op de tweede plek, flink is gedaald: van 12,61% in 2018 naar 6,9% in 2019.

4.5 Multivector aanvallen

Ook in 2019 blijven multivector aanvallen populair. Hierbij is sprake van meerdere aanvalssoorten die worden gebundeld. Het kan gaan om zowel een 'simpel', zwaar aanvalstype met daarbij een klein, geavanceerd type aanval maar ook om twee 'simpele' aanvallen die relatief eenvoudig zijn om op te zetten. De meest complexe aanval die in de NaWas is waargenomen maakte gebruik van maar liefst 30 verschillende vectoren, hoewel dit in het totaal wel een uitzondering is. Aanvallen met 8, 9 of 10 vectoren zijn ook met enige regelmaat waargenomen.

4.6 Opvallende DDoS-aanvallen

SIPvicious attack

SIPvicious behoort tot een toolset voor het testen van op Session Initiation Protocol (SIP) gebaseerde VoIP-systemen. Hackers kunnen deze toolset ook misbruiken voor een flood gericht op deze systemen met uitschakeling als doel.

SIPvicious is een auditing tool die wordt ingezet bij aanvallen gericht op IP-telefoons, VoiP-telefoons en PBX-systemen. Het is daarom aan te bevelen om de IP/VoIP-apparatuur achter een firewall te plaatsen.

4.7 Nieuw waargenomen DDoS-aanvallen

WS-Discovery amplification

In 2019 hebben we voor het eerst een WS-discovery DDoS-aanval waargenomen in de NaWas. Het WS-Discovery protocol is niet ontworpen om via het internet vindbaar te zijn. Aanvallen die via dit protocol worden uitgevoerd zijn dan ook alleen mogelijk doordat dit protocol verkeerd is ingesteld.

WS-Discovery is bedoeld voor lokale, afgesloten netwerken waarbij devices het protocol kunnen gebruiken om te 'ontdekken' welke andere devices zich in het netwerk bevinden. Het gaat dan om printers, maar ook IoT-devices. Hoewel het voor apparaten buiten het netwerk niet mogelijk zou moeten zijn om apparaten op een intern netwerk uit te vragen via dit protocol, is dit vaak toch mogelijk omdat deze apparaten verkeerd zijn geconfigureerd en vindbaar zijn op het internet. Aanvallers kunnen zo in korte tijd grote hoeveelheden apparaten 'bevragen' waarbij ze als retouradres het eigenlijke doeladres van de DDoS-aanval meesturen. In potentie sturen daardoor vele duizenden apparaten hun antwoord naar één doeladres, waardoor deze overbelast raakt.

GRE flood

De Generic Routing Encapsulation (GRE) flood is een type DDoS-aanval waarmee netwerk packets in grote hoeveelheden data worden ingepakt. Deze packets worden vervolgens naar het doelnetwerk gestuurd, dat bij het uitpakken van de packets overbelast raakt. Er zijn ook GRE-floods waargenomen waarbij alleen gebruik wordt gemaakt van header informatie voor de packets. GRE floods werden breed bekend na de aanval van 665 Gbps door het Mirai-botnet op een bekende internationale security specialist in 2016. Het type aanval is dan ook niet nieuw, maar werd tot 2019 weinig waargenomen in de NaWas. De groei van dit type aanval is daarom opmerkelijk.

De meest complexe aanval in 2019 maakte gebruik van maar liefst 30 verschillende vectoren.

5. Trends

Op het eerste gezicht lijkt 2019 veel overeenkomsten te hebben met 2018 als het gaat om het aantal DDoS-aanvallen die door de NaWas zijn waargenomen. Er zijn echter ook belangrijke verschillen. Zo is een daling van het aantal aanvallen zichtbaar. Tegelijkertijd nam de grootte van aanvallen over de hele breedte toe.

Aanvallen blijven snel groeien qua omvang

De grootste aanval die is waargenomen was bijna twee keer zo groot als de grootste aanval in 2018: 124 Gbps in 2019 ten opzichte van 68 Gbps in 2018. In 2017 was de maximale grootte 36 Gbps. We zien dat de grootste DDoS-aanvallen sterker worden, maar geen groter procentueel aandeel hebben in het totaal. De conclusie moet hier dan ook luiden dat de grootste door de NaWas waargenomen DDoS-aanvallen jaar op jaar in omvang toenemen waarbij de aanvallen in de top 3 vooral flink groter zijn dan in 2018, maar dat hun aantal niet evenredig toeneemt.

Ook valt op de het aantal kleine (< 1Gbps) aanvallen langzaam afneemt. Het aandeel van aanvallen met een grootte tussen de 1 en 10 Gbps blijft het grootst en is ten opzichte van 2018 flink gegroeid.

Duur en moment van DDoS-aanvallen

De duur van DDoS-aanvallen lijkt gemiddeld iets af te nemen. Het aantal kortdurende aanvallen (<15 minuten) nam de afgelopen drie jaar toe, terwijl het aantal aanvallen met een duur tussen de 1 en 4 uur afnam in dezelfde periode. Het aantal zeer langdurige aanvallen blijft ongeveer gelijk de afgelopen 3 jaar. Wel duurden 9 van de top 10 langste aanvallen in 2019 (veel) korter dan de langste aanvallen in 2018.

> Het aantal aanvallen daalde in 2019, maar de grootte nam toe.

Opvallend is, dat net als in 2018, in de eerste jaarhelft meer DDoS-aanvallen worden uitgevoerd dan de tweede jaarhelft. Het is gissen welke redenen hieraan ten grondslag liggen, als die er al zijn. Wel ligt het in de rede dat de hogere frequentie in de eerste jaarhelft is te relateren aan bepaalde variabelen, in het kader van preventie zou het kunnen lonen om hier onderzoek naar te doen.

Top 10 aanvallen wisselt jaarlijks

Ook in 2019 valt weer op dat de typen aanvallen die veel worden gebruikt snel veranderen. Was in 2018 LDAP amplification nog het meest populair, in 2019 was dat DNS amplification, waar dit in 2017 ook het geval was. In 2017 nam bijvoorbeeld TCP/ACK flood een tweede plek in, waar dat anno 2019 een vijfde plek is. Het type Chargen amplification stond in 2017 en 2018 bijvoorbeeld nog in de top 10 van meest voorkomende aanvallen, maar is in 2019 uit de top 10 verdwenen.

6. Conclusie

Op basis van de onderzoeksresultaten over het jaar 2019 trekt de NBIP een drietal conclusies.

We zien een daling van het aantal DDoS-aanvallen in het jaar 2019. In 2019 werden 919 aanvallen geregistreerd, in 2018 waren dat er 938. Het aantal deelnemers aan de NaWas groeide daarnaast, waardoor de daling relatief sterker is. Aangezien in 2018 het aantal DDoS-aanvallen nog groeide ten opzichte van 2017, is het goed mogelijk dat de lichte daling in 2019 geen trend zal zijn. Wel lijkt het erop dat in de eerste helft van ieder jaar meer DDoS-aanvallen worden uitgevoerd dan de tweede jaarhelft. Daarom zal pas nadat 2020 ten einde is kunnen worden overzien of het aantal aanvallen stijgt of daalt.

In 2019 namen DDoS-aanvallen in omvang toe, net als in 2018. De maximale grootte van een DDoS-aanval bedroeg in 2019 ca. 124 Gbps, tegenover 68 Gbps in 2018. In 2017 is geen enkele DDoS-aanval van boven de 40 Gbps geregistreerd door de NaWas. Het is dan ook raadzaam dat alle partijen die met DDoS-aanvallen te maken hebben zich voorbereiden op een verdere groei van de omvang van deze aanvallen en de juiste maatregelen treffen om daarmee om te kunnen gaan.

> De voortdurende evolutie van DDoS-aanvallen wijst op een wapenwedloop die waarschijnlijk niet snel zal stoppen.

Tot slot is uit de data die de NaWas verzamelde in 2019 duidelijk geworden dat de multivector aanval, waarbij meerdere typen DDoS-aanvallen worden gecombineerd in één aanval, een populaire manier blijft om toe te slaan. Dat betekent ook dat nog steeds zowel op een groei in omvang als complexiteit van DDoS-aanvallen moet worden geanticipeerd.

Er moet voortdurend rekening gehouden worden met een groei van zowel de omvang als complexiteit van DDoS-aanvallen. De voortdurende evolutie van DDoS-aanvallen wijst op een wapenwedloop die waarschijnlijk niet snel zal stoppen. Gelukkig kan door samenwerking een voorsprong worden opgebouwd. Zo wordt de impact van DDoS-aanvallen kleiner en wordt het internet veiliger.

Bijlage
Typen DDoS-aanvallen

Hoofdcategorieën

Er zijn twee hoofdcategorieën binnen DDoS-aanvallen: (UDP-based) amplification en flood.

Amplification (UDP-based)

Bij een DDoS amplification aanval wordt er een (niet beveiligde) server misbruikt. Het bericht dat wordt toegestuurd, wordt met een factor X vergroot. Daarmee kan een aanvaller met kleine en eenvoudige berichten zorgen voor een enorm aantal berichten richting een server. In het eenvoudige bericht vervalst (spoofed) de afzender het return address naar die van het doelwit. De aanvaller stuurt als het ware een kaartje naar het postkantoor, en het doelwit ontvangt honderden telefoonboeken terug.

Flood

Bij een zogenaamde DDoS flood aanval worden er meerdere computers tegelijk gebruikt die pakketjes sturen naar een server. Veelal worden 'halve' berichten gestuurd die ervoor zorgen dat de server verstoord raakt. Er wordt bijvoorbeeld wel een 'start communicatie' gestuurd, maar vervolgens geen vervolgbericht wanneer het doelwit reageert met 'ok, start de vervolgcommunicatie'.

Amplification

Op alfabetische volgorde

CharGEN amplification

CharGEN is een oud protocol dat uitgebuit wordt voor amplification-aanvallen. Bij een dergelijke aanval worden kleine pakketjes met een

vervalst IP-adres naar een server verstuurd, via apparaten met een internetverbinding die nog gebruik maken van CharGEN. De meeste printers en kopieerapparaten met een internetverbinding hebben dit oude protocol standaard ingeschakeld. De server krijgt vervolgens een UDP flood te verwerken. De server raakt 'uitgeput' en gaat offline of doet een reboot.

DNS amplification

De aanvaller stuurt een DNS look-up request naar kwetsbare DNS-servers met het gespoofte IP-adres. Meestal zijn dit DNS-servers die open recursive relay ondersteunen.

De aanvraag wordt vaak via een botnet doorgegeven zodat de aanval groter uitvalt en beter verborgen blijft. Het DNS-verzoek wordt verzonden met behulp van de EDNS0-extensie van het DNS- protocol, want die laat grote DNS-berichten toe. Het verzoek kan ook de cryptografische functie van de DNS-veiligheidsextensie (DNSSEC) misbruiken om het bericht groter te maken.

LDAP amplification

Bij LDAP amplification wordt een specifieke zwakte misbruikt bij oudere, nog steeds in gebruik zijnde LDAP servers - namelijk het CLDAP-protocol. Origineel bedoeld om te bekijken welke services beschikbaar zijn op een server van een intern netwerk, hebben sommige servers de UDP-poort 389 open naar de "buitenkant".

MS SQL monitor amplification

Dit betreft misbruik van een Microsoft SQL server omgeving - een oude vorm, vooral populair rond 2015. Veel SQL-servers waren 'internet-facing' waardoor deze kwetsbaar waren voor o.a. botnets. Dat deze aanval weer terug is, geeft aan dat bedrijven basic security nog steeds niet op orde hebben. MS SQL is alweer een oudere techniek. Het is een gebruikelijke gang van zaken bij DDoS-aanvallen: legacy die niet meer geüpdatet of gepatcht is, is kwetsbaar, en er wordt dus afgetast of er iets te halen valt. Het bekende 'kloppen op de deur'.

Netbios amplification

NetBIOS is een protocol dat gebruikt wordt in software om applicaties met elkaar te laten communiceren via LAN-netwerken. Doelwitten van Netbios amplifications waren vooral doel in de gaming en hosting sector.

NTP amplification

NTP amplification is een type DDoS-aanval waarbij de aanvaller publiek toegankelijke Network Time Protocol-servers gebruikt om de doelserver te bestoken met UDP-verkeer. NTP is een van de oudste netwerkprotocollen en wordt gebruikt door connected devices om hun klok te synchroniseren.

Oudere versies van NTP ondersteunen een monitoring dienst die beheerders een telling van het verkeer laat doen. Dit commando heet monlist en het stuurt de aanvrager een lijst van de laatste 600 hosts die verbinding hebben gemaakt met de server. Aangezien de afzender gespoofed is, krijgt het doelwit van de aanval dus een enorme hoeveelheid data te verwerken.

RIPv1 amplification

Het Routing Information Protocol (RIP), helpt kleine netwerken met het delen van netwerkroute-informatie. Het bestaat al sinds 1988, maar het is ook al sinds 1996 hopeloos verouderd. Verkeer wordt naar een IP-adres verstuurd die overeenkomt met een IP-adres waarvan het gerucht gaat dat deze staat op een lijst van bekende RIPv1-routers op het internet. Op basis van recente aanvallen geven aanvallers de voorkeur aan routers die een verdacht groot aantal routes in hun RIPv1- routing-tabel lijken te hebben.

RPC Portmapper amplification

RPC Portmapper is een Open Network Computing Remote Procedure Call (ONC RPC)-service die is ontworpen om RPC-servicenummers te koppelen aan netwerkpoort nummers. Wanneer RPC-clients verbinding willen leggen met internet, vertelt portmapper hen welke TCP- of UDP-poort ze moeten gebruiken. Wanneer Portmapper wordt opgevraagd, kan de vergrootfactor van de reactie oplopen tot 20, afhankelijk van de RPC-services die op de host aanwezig zijn. Kwaadwillenden kunnen Portmapper- verzoeken voor DDoS-aanvallen gebruiken omdat de dienst op TCP- of UDP-poort 111 draait.

SNMP amplification

Een SNMP (Simple Network Management Protocol) amplification aanval werkt net als een CharGEN-aanval, maar dan worden connected devices die SNMP runnen gebruikt. Het grote verschil met een CharGEN-aanval is dat de amplification met SNMP vele malen groter is.

SSDP

SSDP (Simple Service Discovery Protocol) is een netwerkprotocol dat wordt gebruikt voor het ontdekken van netwerkdiensten. SSDP maakt het mogelijk dat universele plug-and-play-apparaten informatie verzenden en ontvangen via UDP op poort 1900. SSDP is aantrekkelijk voor DDoS-aanvallers door de open 'state', waardoor spoofing en amplification mogelijk wordt.

(UDP) memcached

Vorig jaar zag de NBIP memcached aanvallen opkomen. Dit zijn zeer kleine DDoS-aanvallen die ook zeer kort duren die het memcached protocol misbruiken. Normaal hoort poort UDP/11211 niet open te staan naar het internet, maar als dit wel het geval is, dan zijn de aanvallen flink te vergroten.

Floods

ESP flood

ESP flood is een aanval waarbij het UDP Encapsulating Security Protocol (ESP) misbruikt wordt. Een Encapsulating Security Payload (ESP) is een protocol voor het verstrekken van authenticatie, integriteit en vertrouwelijkheid van data- en payload netwerkpakketten in IPv4 en IPv6 netwerken.

GRE flood

In een GRE flood wordt een groot aantal pakketjes van het Generic Routing Encapsulation protocol naar een server gestuurd. Normaal gesproken moet een firewall deze opvangen, maar de hoeveelheid van GRE-pakketjes is dermate hoog dat de server het niet aankan. Werd vooral gebruikt door het bekende Mirai-botnet.

TCP flood

TCP/ACK, TCP/SYN, TCP/RST, TCP/SYN/ACK

TCP/SYN floods zijn een van de oudste maar nog steeds zeer populaire Denial of Service (DoS)-aanvallen. De meest voorkomende aanval is het verzenden van een groot aantal SYN pakketten naar het slachtoffer. De aanval zal het SRC IP spoofen, wat betekent dat het antwoord (een SYN+ACK pakket) niet naar de oorspronkelijke bron gaat, maar naar het doelwit .

In de meeste gevallen is de bedoeling van deze aanval om de firewall te overbelasten.

Servers moeten een ‘state’ openen voor elk SYN-pakket dat binnenkomt en deze state opslaan in tabellen met een beperkte grootte. Hoe groot deze tabel ook is, het is gemakkelijk om voldoende SYN-pakketten te versturen

die de tabel zullen vullen, en als dit eenmaal gebeurt begint de server een nieuw verzoek in te dienen, inclusief legitieme verzoeken. In tegenstelling tot andere TCP-aanvallen hoeft de aanvaller geen echt IP-adres te gebruiken; dit is misschien wel de grootste kracht van de aanval.

UDP flood

UDP flood is een type aanval waarin willekeurige poorten van een host (het doelwit) overspoeld worden met IP-pakketjes waar UDP-datagrammen inzitten. De host checkt applicaties die bij deze datagrammen horen - vindt niets - en stuurt een ‘Destination Unreachable’-pakket terug.

ICMP flood

Internet Control Message Protocol (ICMP) is een verbindingsloos protocol. Bij een ICMP flood aanval worden ICMP-pakketjes (in het bijzonder netwerk latency-pakketjes die de ‘ping’ testen) verstuurd, die de server probeert te verwerken.

DNS request flood

Deze versie van een UDP-aanval is een van de bekendste DDoS-aanvallen. Deze richt zich specifiek op DNS-servers om onder andere webservers aan te vallen. Het is ook een van de moeilijkste aanvallen om op te sporen en te voorkomen. Om uit te voeren stuurt een aanvaller een grote hoeveelheid gespoofte DNS-verzoekpakketjes die er niet anders uitzien dan echte verzoeken. Deze komen van een zeer groot aantal IP-adressen.

Dit maakt het voor de doelserver onmogelijk om onderscheid te maken tussen legitieme DNS-verzoeken en DNS- verzoeken die legitiem lijken. De server raakt overbelast in de poging om alle verzoeken te behandelen - alle bandbreedte wordt verbruikt.

NBIP nationale beheersorganisatie internet providers

Voor meer informatie:
www.nbip.nl