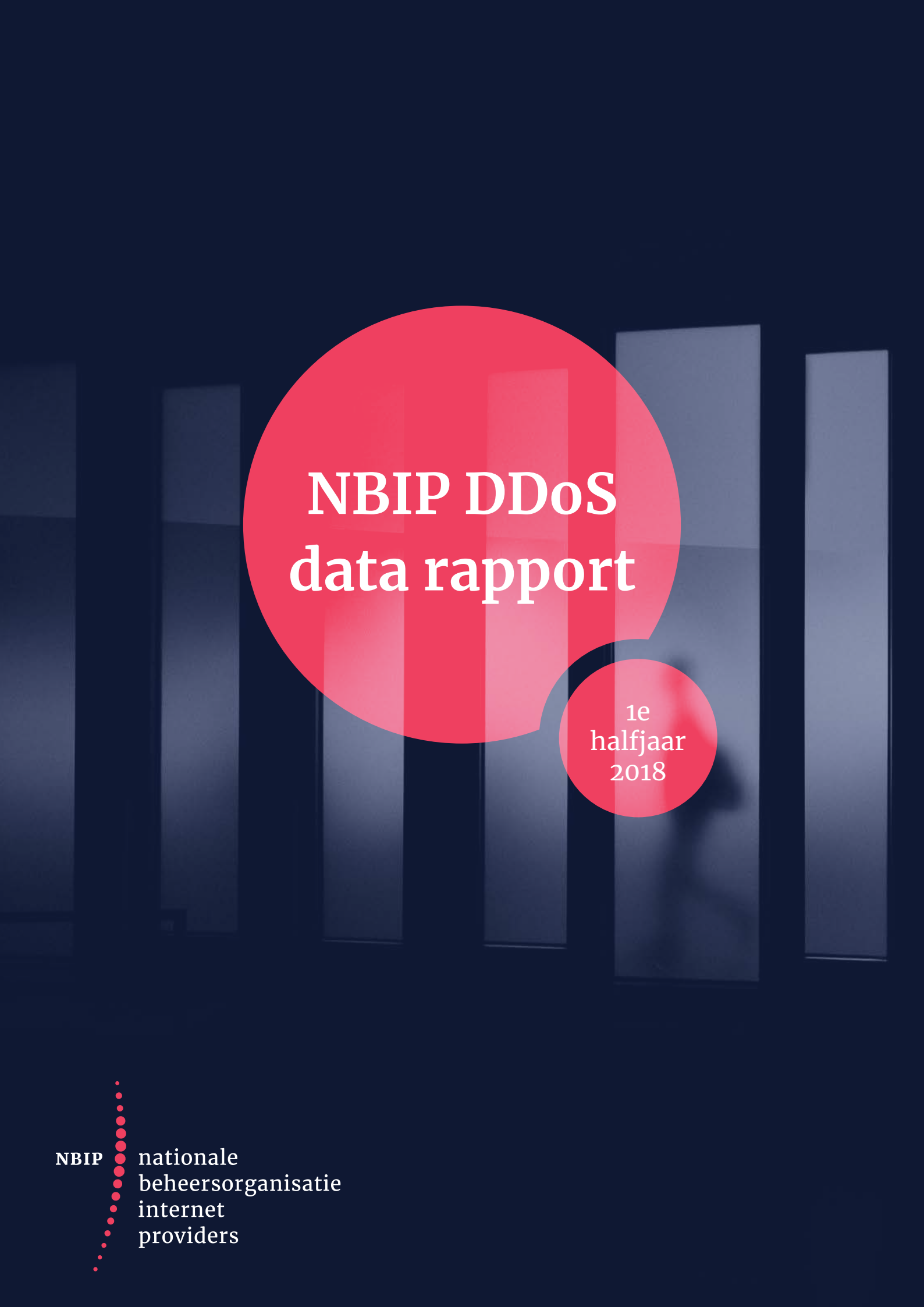


NBIP DDoS data rapport

1e halfjaar 2018

NBIP nationale beheersorganisatie internet providers

Colofon

Het ‘NBIP DDoS data rapport: 1e halfjaar 2018’ is een uitgave van Stichting Nationale Beheersorganisatie Internet Providers.

Datum van uitgave
augustus 2018, jaar 1

Hoofdredactie
Octavia de Weerdt (NBIP)

Redactie
Gerald Schaapman (NBIP)

Eindredactie
Lorenz van Gool (Splend)

Marketing en artwork
Michiel Cazemier (Splend)
Lorenz van Gool (Splend)

Vorm
Dit rapport is gemaakt in PDF-formaat
© 2018

Samenvatting
Het einde van de DDoS-malaise is nog lang niet in zicht. DDoS-aanvallen zijn nog steeds klein, complex en gericht. Hoewel de eerste helft van 2018 geen grote veranderingen kent vergeleken met 2017 (slechts kleine trendbreuken) zijn er wel een groot aantal nieuwe typen aanvallen gezien, wat aangeeft dat DDoS-aanvallen blijven evolueren.

Inhoudsopgave

Voorwoord

U leest het tweede rapport van Stichting Nationale Beheersorganisatie Internet Providers (NBIP) over DDoS-aanvallen in Nederland. Middels onze Nationale Wasstraat, de NaWas, hebben we sinds 2014 voor een groot deel van de Nederlandse internetsector elke DDoS-aanval kunnen mitigeren. Dat geeft ons natuurlijk veel inzicht in malafide cyberpraktijken die helaas de norm zijn.

Begin dit jaar publiceerden we ons eerste rapport, over heel 2017. Omdat veranderingen zich steeds sneller voordoen, zeker op het gebied van cybercrime, is besloten om onze cijfers per halfjaar bekend te maken, om zo een actueel beeld te kunnen blijven bieden. Data die we graag delen, want een veiliger internet begint bij bewustwording.

De verhoogde frequentie in rapportage staat parallel aan onze activiteiten, zowel op het gebied van DDoS-mitigatie als kennisdeling. Allereerst zijn we in, ten tijde van publicatie van dit rapport, flink bezig met de uitbreiding en gestage groei van de NaWas die continuïteit en high redundancy biedt voor onze huidige deelnemers. Daarnaast treden we als stichting meer transparant op door meer informatie te delen met onze deelnemers en geïnteresseerden. Houd daarom dus onze website in de gaten of abonneer je op onze maandelijkse ‘NBIP Notes’ - dan blijf je op de hoogte!

Wederom wil ik graag iedereen bedanken die deze rapportage een warm hart toedraagt. Niet alleen ons bestuur, bureau NBIP en onze deelnemers, maar zeker ook u als lezer.

Hartelijke groet,

Octavia de Weerdt
Algemeen directeur NBIP
octavia@nbip.nl

Inleiding

2018 begon met een knal. Eind januari begonnen de DDoS-aanvallen op Nederlandse diensten die heel het land raakten. Dit veroorzaakte veel opschudding en het onderwerp kwam ter sprake in de belangrijkste Nederlandse praatprogramma's. Men sprak van een Russische tegenaanval of iemand die structureel bezig was met het platleggen van alle internetservices. Het bleek echter een 18-jarige jongeman te zijn, die via internet gericht DDoS-aanvallen bestelde. Voor de lol.

In ons rapport over 2017 bleek dat dit soort korte, gerichte en disruptieve aanvallen steeds vaker aan het licht komen. Daar kwam nog eens bij dat volgens onze resultaten DDoS-aanvallen steeds complexer in elkaar steken.

Snelle verdienmodellen en de eenvoud van het uitvoeren van DDoS-aanvallen houden het gevaar van DDoS in stand. Toch zien we enkele kleine trendbreuken in de eerste zes maanden van dit jaar.

Dit rapport gaat uit van enige kennis van zaken bij de lezer.

In het volgende hoofdstuk bespreken we hoe we met de NaWas DDoS-aanvallen tegengaan. In hoofdstuk 3 staat hoe we dit onderzoek hebben uitgevoerd. In hoofdstuk 4 bespreken we de resultaten, waarna de conclusie volgt met verwachtingen voor de rest van het jaar.

DDoS-mitigatie: hoe doe je dat?

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, 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").

> Een "wasstraat" staat voor verfijnde DDoS-mitigatie

De NaWas (Nationale Wasstraat), een initiatief van de NBIP, is zo'n wasstraat. Inmiddels is de NaWas de bekendste wasstraat van Nederland. Dat komt mede doordat de NBIP is opgericht door internet service providers zelf. Voordeel van zo'n stichting is ook dat er samen inkoop wordt gedaan. Tegelijkertijd wordt de wasstraat ook veiliger: want hoe meer deelnemers, hoe meer kennisdeling, hoe beter de NBIP in staat is DDoS-aanvallen te herkennen en te mitigeren.

Methode

In dit hoofdstuk wordt ingegaan op de onderzoeksmethode. 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. 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. Dit betreft 62 deelnemers (dd augustus 2018)

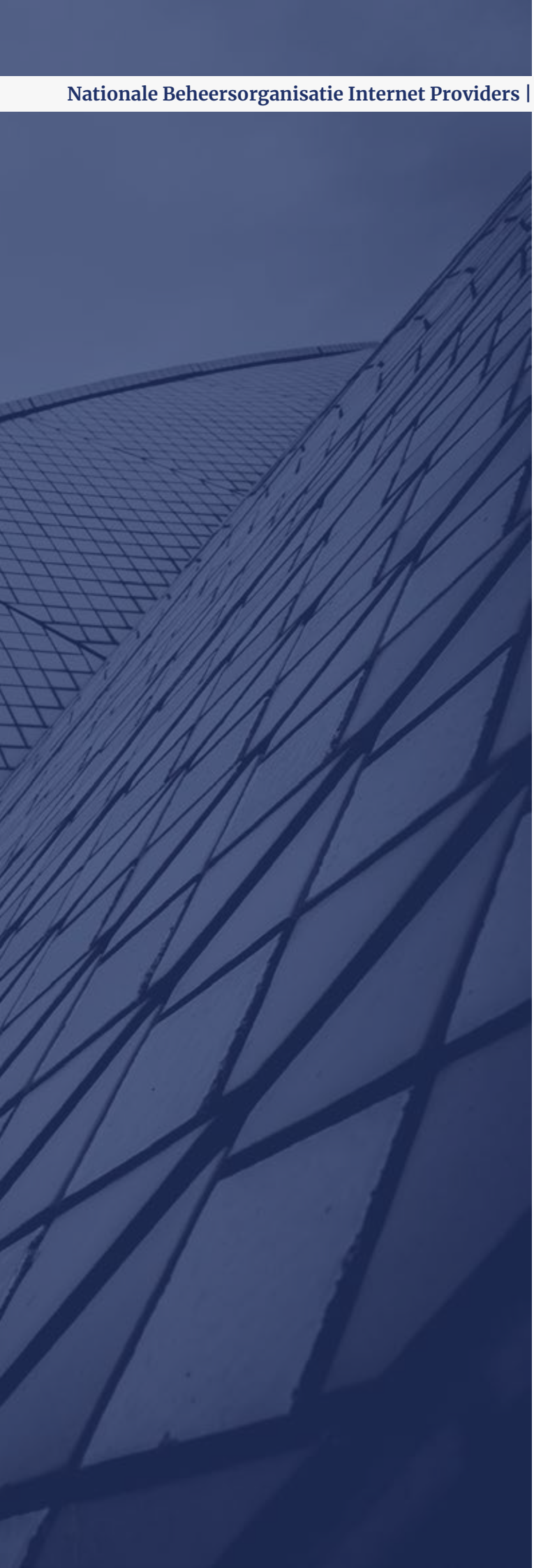
Deze deelnemers bestaan uit grotendeels internet service providers (ISP's). Met ISP wordt in dit onderzoek een bedrijf of organisatie bedoeld dat online diensten en/of toegang tot internet aan klanten biedt. In het geval van de deelnemers aan de NaWas zijn dit voornamelijk bedrijven die cloud- en hostingdiensten aanbieden.

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

Representatief voor Nederland

Het aantal onderzochte DDoS-aanvallen op deze deelnemers zal niet direct iets kunnen zeggen over heel Nederland. Toch wordt geschat dat dit onderzoek redelijk representatief is voor de Nederlandse internetsector.

De NBIP doet namelijk samen met SIDN onderzoek naar de economische impact van de aanvallen die in onze rapporten beschreven worden. Zo is precies na te gaan in hoeverre onze cijfers representatief zijn voor de rest van Nederland. Dit onderzoek zal najaar 2018 gepubliceerd worden.



Verantwoording

Dit onderzoek toont cijfers en resultaten voor de eerste helft van het jaar 2018.

Voor dit onderzoek is gekozen om de grootte van de aanvallen in Gbps (gigabit per second) te meten.

Dit onderzoek over de eerste zes maanden van het jaar vormt een tussenstand van zaken over het hele jaar 2018. De opvallendste zaken hebben we daarom uitgelicht - een meer uitgediepte analyse zullen we daarom in het jaarrapport 2018 geven.

Zoals gemeld in het voorwoord, gaat dit rapport uit van lezers met enige kennis van zaken. In dit onderzoek wordt in de meeste gevallen geen nieuwe kennis verstrekt. Mocht dit wel het geval zijn, dan wordt dit direct uitgelegd. Vanwege de omvang van dit rapport is er daarom geen appendix met extra uitleg, zoals bij de jaarrapporten wel het geval is.

Resultaten

Allereerst is het aantal, de grootte en de duur van DDoS-aanvallen (eerste helft 2017 / eerste helft 2018) geanalyseerd. Vervolgens zijn de soorten DDoS-aanvallen geanalyseerd die tot nu toe in 2018 zijn voorgekomen. Daarnaast volgt een analyse van de gemeten resultaten.

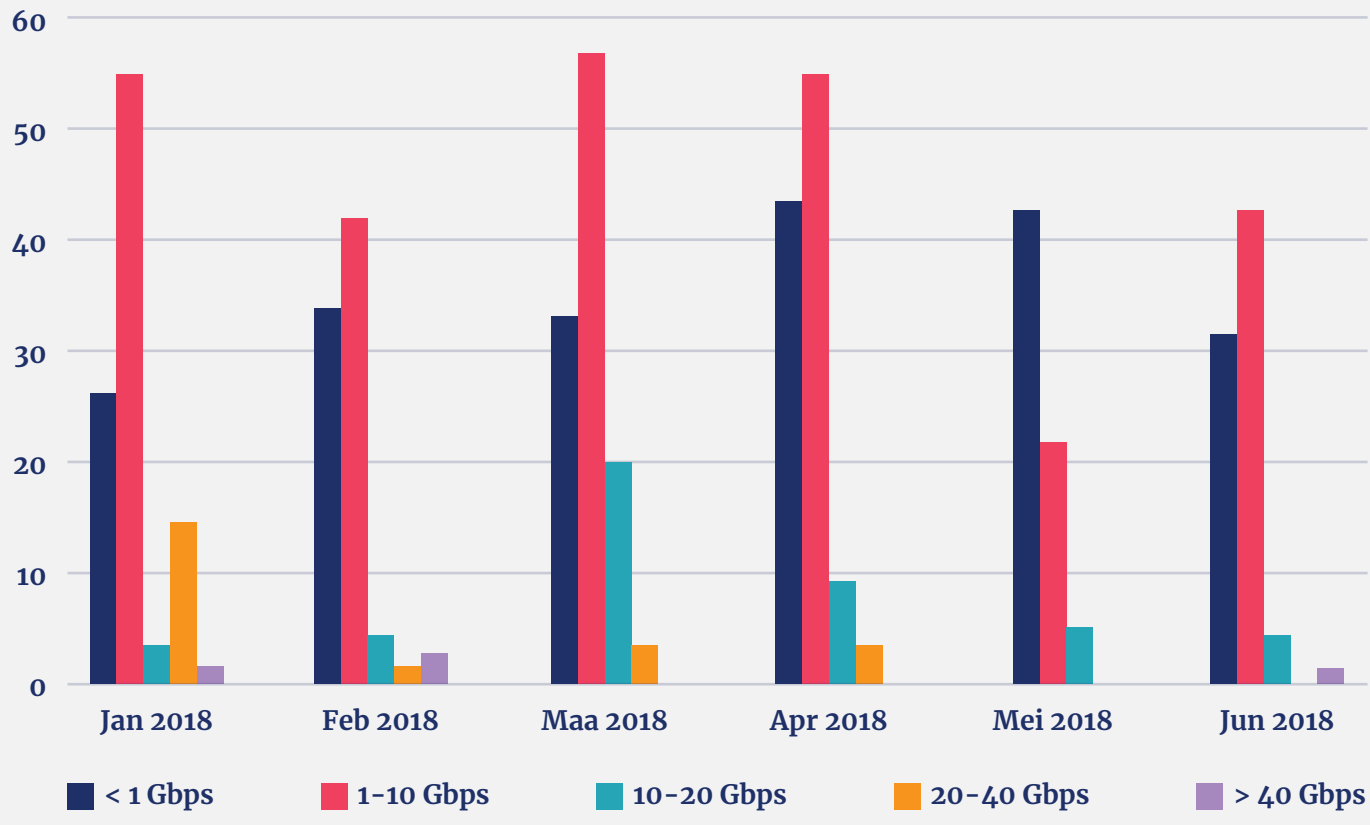
Aantal DDoS-aanvallen

In de eerste helft van 2017 heeft de NBIP 420 DDoS-aanvallen geregistreerd - dat zijn ongeveer 2,3 aanvallen per dag. In de eerste zes maanden van 2018 was dit aantal al 555, wat neerkomt op ruim 3 aanvallen per dag. Een stijging van 32 procent. De NBIP heeft geen aanleiding om te vermoeden dat de aanvallen minder worden in de komende zes maanden - wat betekent dat het record van aantal DDoS-aanvallen per jaar hoogstwaarschijnlijk wederom gebroken wordt, en ongeveer boven de 1000 uit zal komen. Vorig jaar waren er 826 aanvallen gemeten.

Grootte van een DDoS-aanval

De NBIP zag geen bijzondere, complexe aanvallen in deze periode. Wel werden er een aantal grote aanvallen gezien (van meer dan 40 Gbps), wat een trendbreuk is met dezelfde periode daarvoor. Over heel 2017 zelfs werden er geen DDoS-aanvallen van deze grootte gespot. De laatste keer was in 2016.

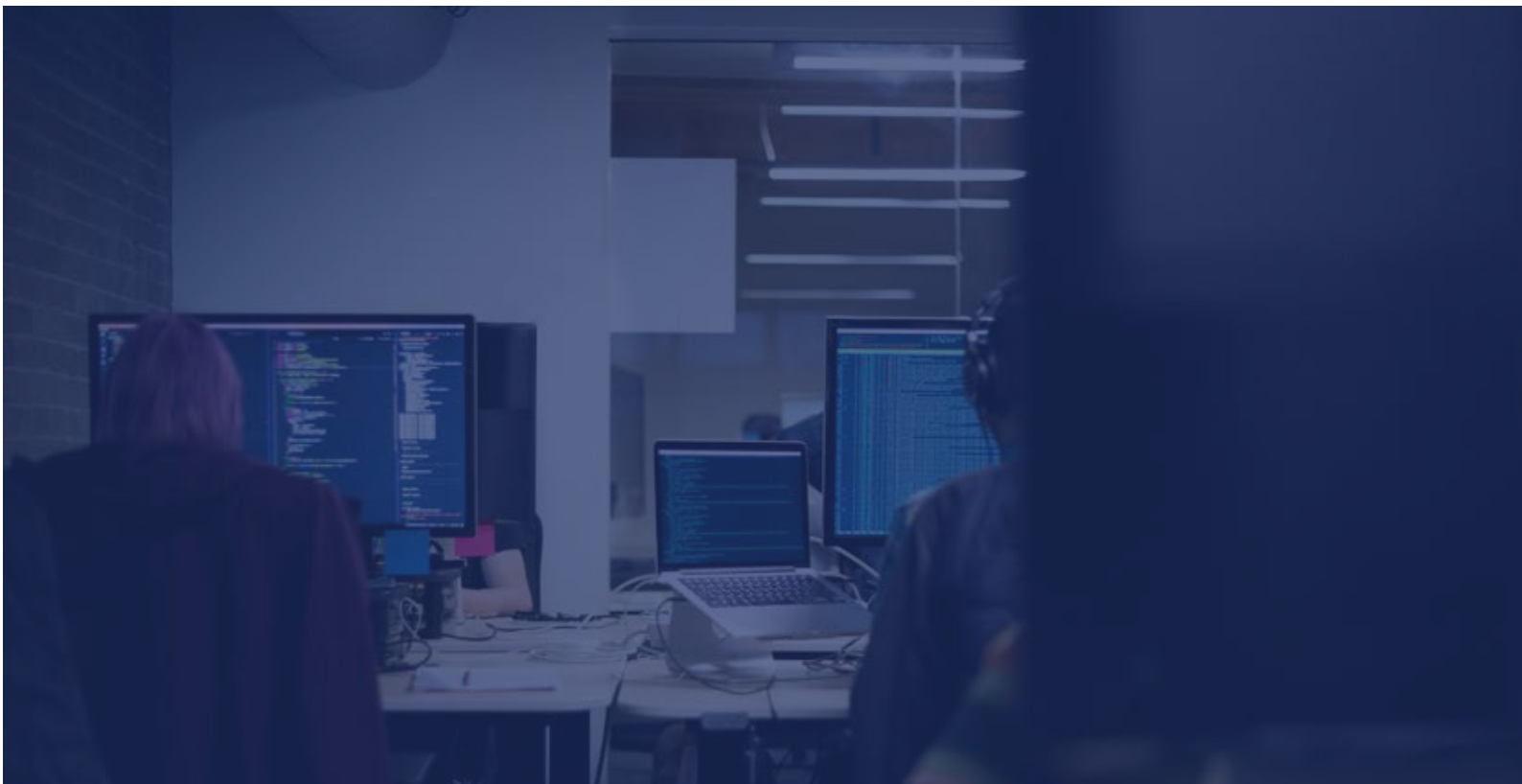
DDoS-aanvallen - grootte (Jan-2018 t/m Jun-2018)



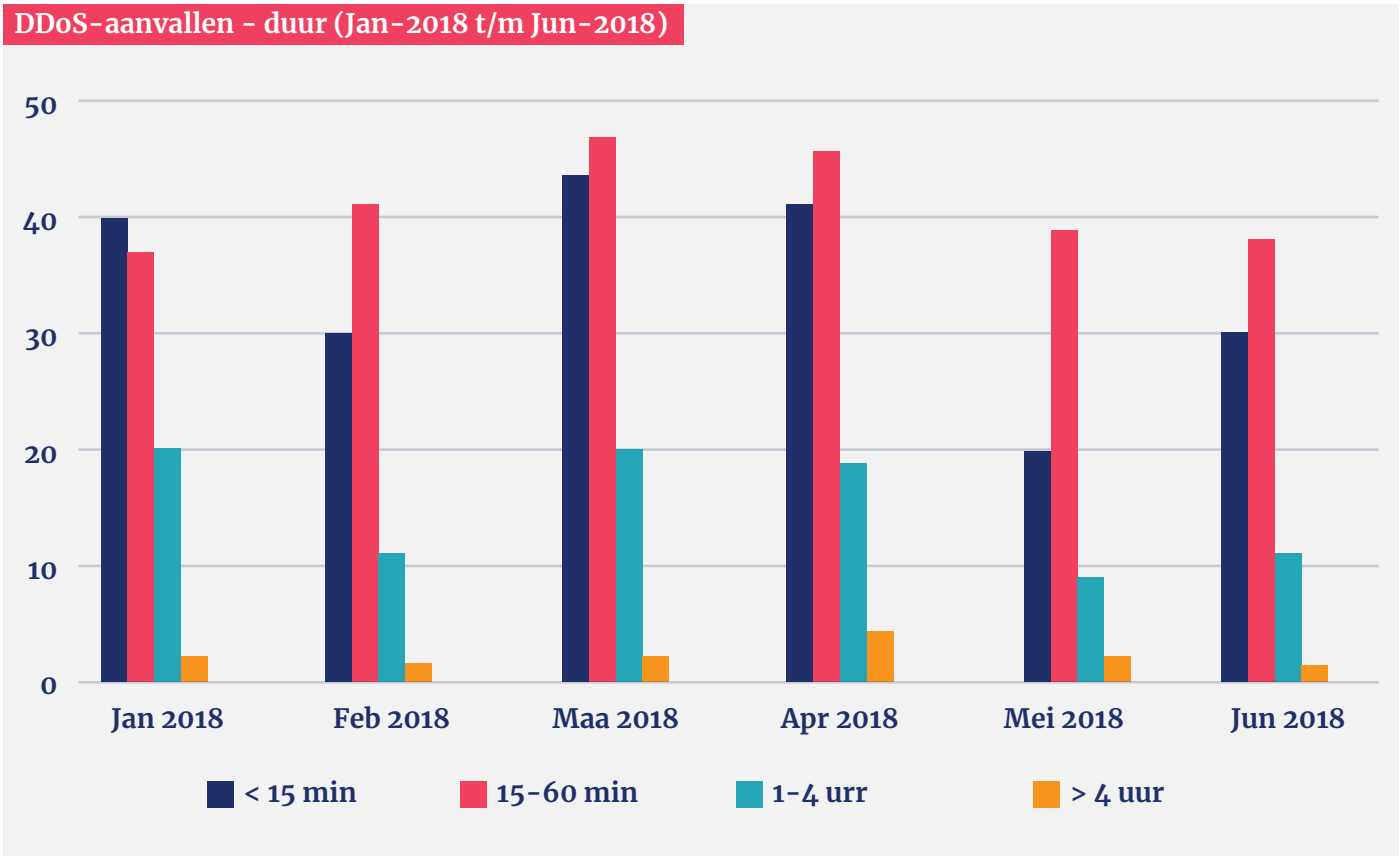
Er zijn voor het eerst sinds 2016 weer enkele grote aanvallen van meer dan 40 Gbps gezien

In juni is de grootste DDoS-aanval tot nu toe verwerkt; 68 Gbps. Dit was een gecombineerde aanval van een SSDP en DNS amplification en deze duurde ongeveer 10 minuten. Dit betrof 1 aanval, en met de 3 aanvallen in januari en februari van meer dan 40 Gbps erbij, waren er ondanks deze trendbreuk met vorig jaar nauwelijks grote aanvallen. In de eerste helft van 2018 bestond de overgrote meerderheid van 486 DDoS-aanvallen (87,6 procent) uit grootten van minder dan 10 Gbps. Dit verschilt nauwelijks met het percentage in de eerste helft van 2017: 87,3 procent.

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
Maa-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
Eindtotaal	**212**	**274**	**45**	**20**	**4**	**555**



Duur van een DDoS-aanval
453 (81,6 procent) aanvallen duurden minder dan 1 uur, met 205 (37%) minder dan een kwartier.



Wederom verschilt dit niet veel met dezelfde periode in 2017: 80,9 procent van de DDoS-aanvallen duurde minder dan 1 uur. Vorig jaar waren er wel iets meer korte aanvallen van minder dan een kwartier: 43 procent.

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
Maa-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
Eindtotaal	**205**	**248**	**90**	**12**	**555**

Soorten DDoS-aanvallen

Uit het jaarrapport 2017 bleek de belangrijkste conclusie qua soorten DDoS-aanvallen het vernuft van multivector-aanvallen (een combinatie van meerdere typen DDoS). Ook dit halfjaar blijft deze trend zich stevig voortzetten. De NBIP heeft 200 van deze multivector-aanvallen in het eerste halfjaar van 2018 gezien - 36 procent van het geheel.

Het record qua verschillende DDoS-typen in een aanval, namelijk 13, werd niet verbroken. Toch waren de aanvallen nog steeds ongekend complex: het hoogste aantal in een DDoS-aanval (eerste helft 2018) bestond uit 11 verschillende DDoS-typen.

Memcached

Ook heeft de NBIP in het jaarrapport 2017 gewaarschuwd voor de opkomst van zogenoemde memcached-aanvallen. Dit zijn DDoS-aanvallen waarin kleine pakketjes met data flink worden vergroot ('amplifiication') - waardoor enorme verkeerspieken ontstaan en de server het uiteindelijk begeeft.

Vanaf eind februari heeft de NBIP regelmatig dit soort aanvallen waargenomen, ongeveer drie per maand. De grootste was 41 Gbps, de kleinste slechts 230 Mbps. De aanvallen duurde relatief kort: gemiddeld ongeveer 15 minuten.

Nieuwe typen DDoS-aanvallen

Er zijn door de NBIP in deze periode maar liefst 13 nieuwe type DDoS-aanvallen gezien. Hoewel amplification-aanvallen het vaakst voorkomen, heeft de NBIP vooral nieuwe flood-aanvallen gezien. Dit zijn soorten DDoS-aanvallen waarbij meerdere computers tegelijk 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'.

> De NBIP heeft deze periode maar liefst 13 nieuwe typen DDoS-aanvallen gezien

In dit eerste helft van 2018 zag de NBIP bijvoorbeeld de volgende flood-aanvallen, waarbij misbruik wordt gemaakt van (oude) protocollen: een UDP CHAOS flood, een Authentication Header flood en een Encapsulating Security Payload flood.

Voor het overzicht van vorig jaar van alle soorten DDoS-aanvallen, download ons volledige jaarrapport 2017. In het jaarrapport over heel 2018 zullen we een uitgebreid overzicht van alle nieuwe aanvallen geven.

Conclusie

De NBIP ziet op basis van de resultaten over de eerste helft van 2018 geen grote veranderingen vergeleken met 2017. Wel wordt duidelijk dat DDoS-aanvallen blijven evolueren.

Dat DDoS-aanvallen kleiner en complexer worden, klopt nog steeds. Opvallend is dat de grote aanvallen van meer dan 40 Gbps wel terug zijn in 2018, maar voor het gemiddelde van de grootte en duur niet veel uitmaken. De toename aan het aantal aanvallen zorgt hiervoor.

Ook is de duur van DDoS-aanvallen niet veranderd. Het blijven korte, disruptieve aanvallen - al zijn minder aanvallen binnen het kwartier voltooid vergeleken met de eerste helft van 2017. Het gros is nog steeds binnen het uur voltooid.

In het jaarrapport 2017 heeft de NBIP twee grote verwachtingen genoemd, namelijk een groter aantal aanvallen in 2018 - en de opkomst van memcached aanvallen.

Met de huidige groei verwachten we dat dit jaar weer meer DDoS-aanvallen te zien, over de duizend. Hierdoor kunnen we vrijwel zeker stellen dat deze voorspelling is uitgekomen. Ook hebben we de in eind 2017 voorspelde memcached aanvallen dit jaar in actie gezien.

Er zijn in de eerste zes maanden van 2017 geen grote trendbreuken gezien. De voorspellingen die zijn uitgekomen, aanvallen blijven complex door het grote aantal multivector-aanvallen en het feit dat er weer 13 nieuwe typen DDoS-aanvallen zijn waargenomen door de de NBIP, laten wel zien dat zulke aanvallen blijven veranderen.

Continue evolutie van soorten DDoS-aanvallen maakt het voor ISP's lastiger om hierop in te spelen. Een speelveld dat zich constant aanpast dient daarom constant gemonitord te worden.

NBIP nationale beheersorganisatie internet providers

Voor meer informatie:

www.nbip.nl