NBIP DDoS-datarapport

1e halfjaar 2019

NBIP nationale beheersorganisatie internet providers

Colofon

Het NBIP DDoS-datarapport: eerste halfjaar 2019 is een uitgave van de Stichting Nationale Beheersorganisatie Internet Providers.

Datum van uitgave
september 2019, jaar 1

Hoofdredactie
Octavia de Weerdt (NBIP)

Redactie
Gerald Schaapman (NBIP)

Eindredactie
Stefan Penders (Splend)

Marketing en artwork
Sam Zondervan (Splend)
Michiel Cazemier (Splend)

Vorm
Dit rapport is gemaakt in PDF-formaat

Inhoudsopgave

Voorwoord

Voor u ligt het vierde rapport van de Nationale Beheersorganisatie Internet Providers (NBIP) over DDoS-aanvallen. Sinds 2017 publiceren we rapporten over DDoS-aanvallen. We constateerden in voorgaande rapporten dat DDoS-aanvallen steeds vernuftiger en frequenter worden. Helaas moet ik u melden dat die trend ook in 2019 aanhoudt.

Maar er is een lichtpuntje in dit slechte nieuws. De strijd tegen DDoS-aanvallen heeft sinds 2018 aan kracht gewonnen. De overheid en het bedrijfsleven nemen het gevaar van DDoS serieus en slaan de handen in elkaar met internet service providers. Dat leidde tot de oprichting van een anti-DDoS-coalitie, met als doel om DDoS-aanvallen beter te begrijpen en af te mitigeren.

Ook de NBIP is onderdeel van deze anti-DDoS-coalitie. De NBIP gelooft in een coöperatieve benadering van de DDoS-problematiek. Daarom heeft de NBIP er vorig jaar voor gekozen om de diensten van de NaWas ook ter beschikking te stellen van Europese internet service providers. DDoS-aanvallen houden immers niet op bij de grens. Met een gezamenlijke Europese aanpak kunnen we DDoS beter te lijf.

Bent u geïnteresseerd in dit onderwerp en wilt u graag meer weten? Houd dan onze website in de gaten, of abonneer u op onze ‘NBIP Notes’! Voor nu wens ik u in ieder geval veel leesplezier toe.

Hartelijke groet,

Octavia de Weerdt
Algemeen directeur NBIP
octavia@nbip.nl

Inleiding

De stichting Nationale Beheersorganisatie Internet Providers (NBIP) richtte in 2014 de Nationale DDoS Wasstraat (NaWas) op. NaWas beschermt deelnemers tegen zogeheten Distributed-Denial-of-Service-aanvallen. Tijdens een DDoS-aanval overspoelen computers een website met toegangsverzoeken. De website kan de grote hoeveelheid verkeer niet aan en vertraagt of gaat zelfs helemaal offline.

De NaWas zorgt ervoor dat DDoS-aanvallen worden tegengehouden voordat ze schade kunnen aanrichten. Door het dataverkeer richting een website door onze Wasstraat te halen, zorgen we dat alleen 'schone' toegangsverzoeken worden doorgelaten. De data die we over binnenkomende aanvallen verzamelen geeft ons inzicht in de methodes van cybercriminelen en veranderende trends op gebied van DDoS. In dit rapport geven we u inzicht in de ontwikkelingen voor de eerste helft van 2019. We gebruiken daarbij specifieke terminologie en gaan uit van enige voorkennis.

Clearing House

Een belangrijke ontwikkeling in het eerste halfjaar van 2019 is dat de NBIP deelneemt aan de werkgroep Clearing House, onderdeel van de nationale anti-DDoS-coalitie. Samen met bedrijven, overheden en academische instanties deelt de NBIP kennis over DDoS-aanvallen. De technische basis voor de werkgroep werd gelegd door een onderzoeksproject van de NBIP en de TU Twente. We ontwikkelden een database om de kenmerken van DDoS-aanvallen bij te houden. Met behulp van de werkgroep Clearing House kunnen we die database verder professionaliseren en uitbouwen. Dat betekent in de praktijk dat we aanvallen sneller kunnen herkennen en dus ook mitigeren. Zo staan we gezamenlijk sterker tegen DDoS.

Europa

Sinds 2018 staat de NaWas open voor Europese deelnemers. De NBIP werkt daarbij vanuit het geloof dat we samen sterker staan tegen DDoS. Door kennis uit te wisselen met Europese internet service providers kunnen we de NaWas verder verbeteren en blijven we DDoS-aanvallers een stap voor. Inmiddels beschermt de NaWas deelnemers in Duitsland, Frankrijk en het Verenigd Koninkrijk.

Het schoonschrobben van een DDoS-aanval

DDoS-aanvallen komen in vele soorten en maten. Zo ook de maatregelen om organisaties te beschermen tegen DDoS-aanvallen.

De meeste anti-DDoS-maatregelen zijn redelijk rigorous van aard. “Blackholing” bijvoorbeeld sluist al het verkeer weg van een website. Een uiterst effectieve methode, maar met één groot nadeel: ook onschuldige bezoekers kunnen we website niet meer bezoeken. IP-blocking werkt op soortgelijke wijze, maar gericht op regio’s. De server weigert toegang aan het dataverkeer afkomstig van een bepaalde geografische locatie. Maar wederom met als gevolg dat onschuldige bezoekers de website niet kunnen bereiken.

Een centrale ‘wasstraat’ is een flinke stap voorwaarts. Dataverkeer wordt door specialistische apparatuur geleid en - bij een DDoS-aanval - schoongeboend (“scrubbing”). De wasstraat houdt DDoS-aanvallen tegen maar laat onschuldig dataverkeer gewoon door, in tegenstelling tot blackholing en IP-blocking. Het grote nadeel van een wasstraat is echter de grote capaciteit die nodig is om de wasstraat effectief in te zetten. Voor individuele internet service providers zijn de kosten van het onderhouden van die capaciteit erg hoog.

> Een “wasstraat” staat voor verfijnde DDoS-mitigatie

Met die reden heeft de NBIP in 2014 de Nationale Wasstraat (NaWas) opgezet. In plaats van individuele service providers die hun eigen bescherming regelen, werken de deelnemers van de NaWas samen. Ze delen de kosten van de aanschaf en het onderhoud van de wasstraat-apparatuur. En ze delen kennis over DDoS-aanvallen, waardoor de NaWas steeds up-to-date blijft.

Hoe wij onze data verzamelen

DDoS-aanvallen veranderen voortdurend. In intensiteit, grootte en samenstelling. Regelmatig duiken nieuwe vormen van DDoS-aanvallen op. Om DDoS-aanvallen effectief af te slaan, nu en in de toekomst, verzamelen we data. De NBIP beheert een registratiesysteem voor DDoS-aanvallen. Alle DDoS-aanvallen op onze deelnemers komen in dit registratiesysteem terecht, waaruit we vervolgens onze data putten.

De deelnemers aan de NaWas bestaan voor een groot deel uit internet service providers, maar ook banken en verzekeraars doen mee. Niet elke deelnemer krijgt te kampen met DDoS-aanvallen, en de intensiteit van de aanvallen verschilt van deelnemer tot deelnemer. Om veiligheidsredenen, privacy-overwegingen en contractuele verplichtingen jegens onze deelnemers doen wij geen uitspraken over het aantal aanvallen per deelnemer. Ook maken wij geen namen bekend van getroffen organisaties.

De data in dit rapport is verzameld over de periode januari tot en met juni 2019. De cijfers en analyses in dit rapport zijn samengesteld op basis van data van 70 deelnemers. Deze cijfers tonen alleen de DDoS-aanvallen die zijn geregistreerd door de NaWas, niet het totaal van DDoS-aanvallen op Nederlandse organisaties. Gegeven onze grote groep deelnemers en de grote hoeveelheid gemeten aanvallen, zijn wij van mening dat onze data representatief is voor bredere trends op het gebied van DDoS-aanvallen.

Representatief voor Nederland

Hoewel de NaWas niet alle bedrijven en organisaties in Nederland beschermt tegen DDoS-aanvallen, zijn de cijfers in de rapport representatief. Dat komt onder andere door het grote aantal .nl domeinnamen dat wordt beschermd door de NaWas: bijna 50%.

DDoS: cijfers en aantallen

Het aantal DDoS-aanvallen stijgt, zo suggereren de cijfers voor de eerste helft van 2019. Gedurende het jaar 2018 vonden er 938 aanvallen plaats. Oftewel, ongeveer 2,6 aanvallen per dag. Medio 2019 staat de teller al op 572, een gemiddelde van 3,2 aanvallen per dag. Of deze stijgende lijn doorzet naar de tweede helft van 2019 is moeilijk te voorspellen. Op basis van data uit 2017 en 2018 lijkt het echter onwaarschijnlijk dat de hoeveelheid DDoS-aanvallen zal afnemen in de tweede helft van dit jaar.

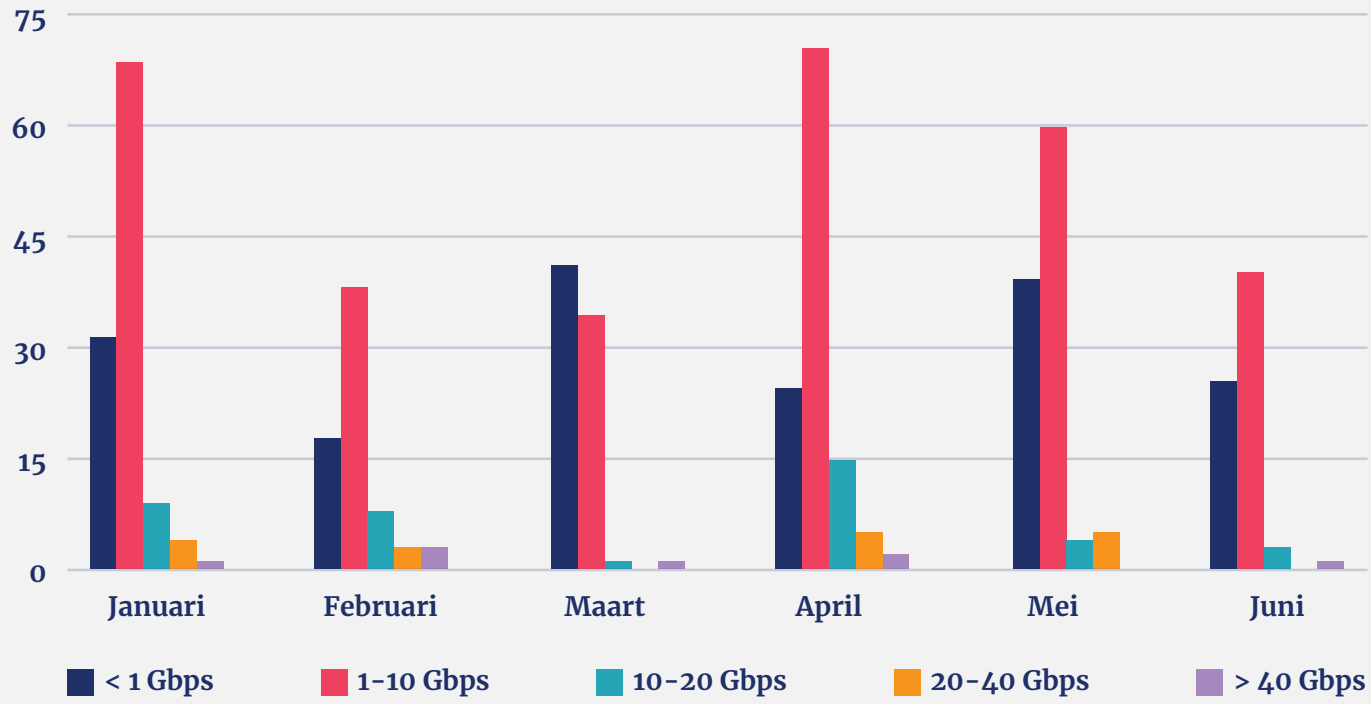
> De eerste helft van 2019 zag een voorlopige piek met een DDoS-aanval van 71 Gbps

Naast het aantal aanvallen groeit ook de maximale grootte van aanvallen. De eerste helft van 2019 zag een voorlopige piek met een DDoS-aanval van 71 Gbps. Een record dat past binnen een bredere trend. Het vorige record stamt uit 2018, toen we een aanval van 68 Gbps maten. Toch moet hierbij vermeld worden dat het merendeel van de aanvallen van beperkte grootte is, minder dan 10Gbps. Kwaadwillenden maken voornamelijk gebruik van aanvallen die net groot genoeg zijn om een server of dienst onbereikbaar te maken.

Ten slotte stijgt ook de duur van de aanvallen. In 2019 registreerden we 23 aanvallen die langer dan vier uur duurden. Dat staat in contrast met 2018, waar gedurende het hele jaar ‘slechts’ 22 van dergelijke langdurige aanvallen plaatsvonden.

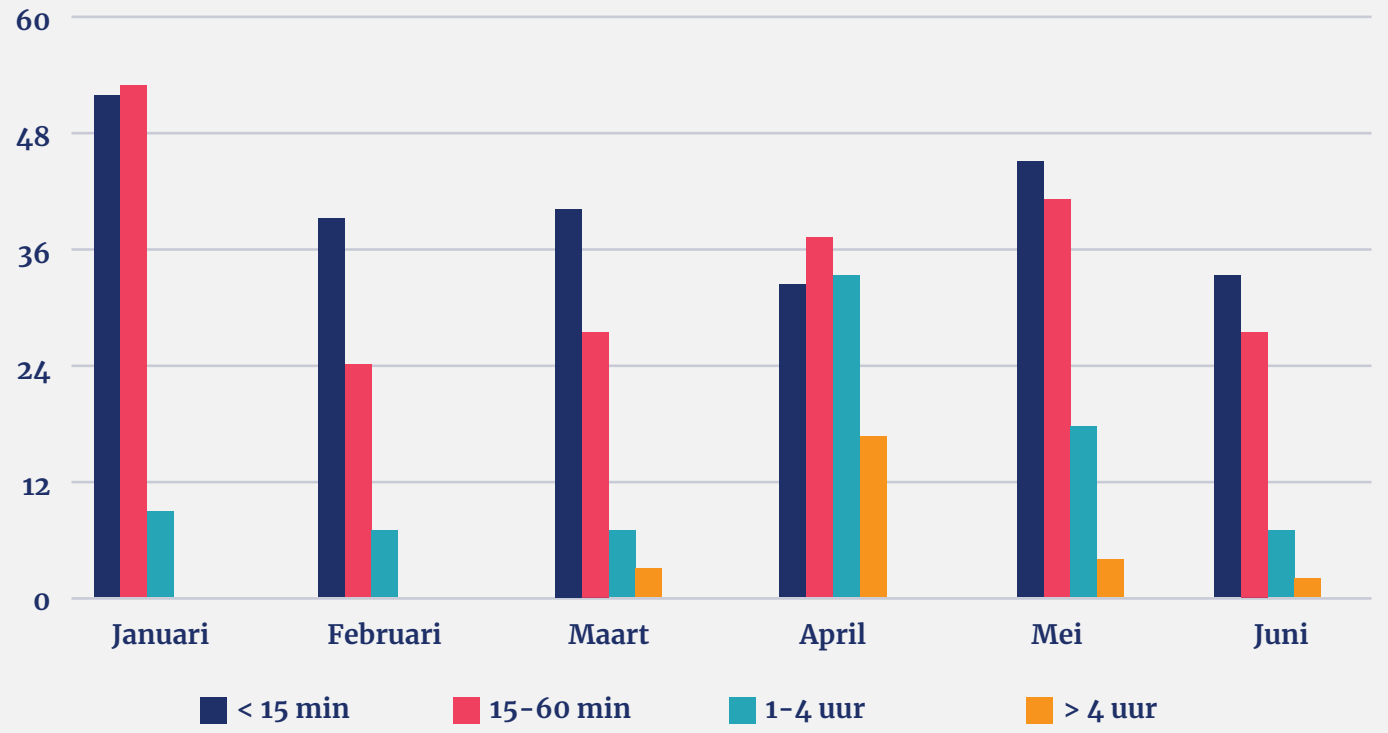
Op de volgende pagina’s zijn deze waarnemingen gevat in twee grafieken.

DDoS-aanvallen - grootte (januari t/m juni 2019)



Maand (2019)	< 1 Gbps	1-10 Gbps	10-20 Gbps	20-40 Gbps	>40 Gbps	totaal
Januari	32	70	9	4	1	116
Februari	18	39	8	3	3	71
Maart	42	35	1	0	1	79
April	25	72	15	5	2	119
Mei	40	61	4	5	0	110
Juni	26	41	3	0	1	71
Eindtotaal	**183**	**318**	**40**	**17**	**8**	**566**

DDoS-aanvallen - duur (januari t/m juni 2019)



Maand (2019)	< 15 min	15-60 min	1-4 uur	> 4 uur	totaal
Januari	53	54	9	0	116
Februari	40	24	7	0	71
Maart	41	28	7	3	79
April	33	38	34	14	119
Mei	46	42	18	4	110
Juni	34	28	7	2	71
Eindtotaal	**247**	**214**	**82**	**23**	**566**

DDoS: types en trends

De eerste stap in het succesvol afslaan van een DDoS-aanval is het tijdig herkennen van de aanval. Op basis van de data van onze deelnemers, analyseert de NBIP DDoS-trends en verzamelt informatie over de kenmerken van verschillende types DDoS-aanvallen. Hieronder delen we de belangrijkste inzichten voor de eerste helft van 2019.

DDoS-types

De NBIP houdt een top tien bij van de meest gebruikelijke DDoS-aanvallen. Gedurende de eerste helft van 2019 bleek DNS amplification de meest voorkomende variant. In 2018 was dit nog de LDAP amplification, die nu als tweede eindigt. Een opvallend verschijnsel is dat nog slechts 8% van alle DDoS-aanvallen gebruik maakt van NTP amplification. Daarmee komt NTP amplification op de zesde plaats terecht. In 2018 maakten nog 15% van alle DDoS-aanvallen gebruik van NTP amplification. Hoewel het vooralsnog gissen blijft naar de precieze oorzaak van deze daling, is het waarschijnlijk dat de betere beveiliging van veel NTP services een grote rol speelt.

Een in het oog springende nieuwkomer in de top tien is de zogeheten GRE flood. We achten het waarschijnlijk dat de opkomst van GRE floods samenhangt met het gebruik van GRE-tunnels in netwerknodes. Die vormen een nieuw doelwit voor kwaadwillenden. Een bijkomend voordeel vanuit het oogpunt van een DDoS-aanvaller is dat GRE-verkeer versleuteld is. Doordat de data niet inhoudelijk bekeken kan worden, is het lastiger om een DDoS-aanval tijdig te herkennen.

Een bijkomend verrassend verschijnsel waren de zogeheten DNS water torture attacks, die we aan het begin van dit jaar registreerden. Die macabere naam verwijst naar een aanval op DNS services waarbij gericht DNS-bevragingen worden gedaan in de vorm van ‘<prefix>.<victim domain>’. In de <prefix> wordt een willekeurige string opgenomen van zestien of meer tekens die voortdurend veranderen. Hierdoor moet de authoritative nameserver worden bevraagd, die vervolgens zoveel verzoeken krijgt dat de nameserver onderuit gaat. Wanneer dit lang genoeg duurt, verdwijnen de domeinen uit de cache DNS services. Er is geen vertaling naar IP meer mogelijk, met als resultaat dat de domeinen van de authoritative nameserver onbereikbaar zijn. Door slim gebruik van filters was de NaWas deze vorm van DDoS een stap voor, waardoor we de aanvallen konden mitigeren.

Trends

Twee belangrijke trends in de eerste helft van 2019 werd hierboven al kort genoemd: het aantal aanvallen groeit, evenals de maximale grootte van aanvallen. Maar ook het aantal grote aanvallen neemt toe. Hoewel het merendeel van de DDoS-aanvallen onder de grens van 10Gbps blijft, zien we desalniettemin een stijgende lijn in het aantal aanvallen boven die grens. Overigens is dit geen volledig nieuwe ontwikkeling: ook in 2018 zagen we een gestage toename van het aantal grote DDoS-aanvallen. Toch wijzen deze verontrustende cijfers wederom op het groeiende gevaar van DDoS-aanvallen.

Conclusies

De cijfers in dit rapport hebben slechts betrekking op de eerste helft van 2019. De conclusies die getrokken kunnen worden op basis van deze data zijn beperkt. Toch zijn er een aantal trends te benoemen die aansluiten op de ontwikkelingen van de afgelopen jaren.

In ons jaarrapport over 2018 concludeerden we al dat de duur, grootte en de complexiteit van aanvallen toenneemt. Die conclusies zien we ook terug in de eerste helft van 2019. Het totaal aantal aanvallen stijgt. Gemiddeld vinden er elke dag meer dan drie aanvallen plaats. De aanvallen groeien ook in tijdsduur. Aanvallen van meer dan vier uur komen steeds vaker voor. En de omvang neemt toe, met steeds meer grote aanvallen van boven de 10 Gbps. En hoewel 'kleine' aanvallen nog steeds de hoofdmoot vormen, moet het gevaar niet onderschat worden: ook een kleine aanval kan een server of dienst uit de lucht halen.

Een tweede belangrijke conclusie is dat DDoS-aanvallen steeds slimmer worden. We zien dat kwaadwillenden snel reageren op verbeteringen in de beveiliging (zoals bij de NTP services) en kiezen voor nieuwe aanvalsroutes. Zwakke plekken, zoals GRE-tunnels, kunnen gemakkelijk worden uitgebuit. Vernuftige nieuwe DDoS-aanvallen, zoals GRE floods en DNS water torture, zijn lastig (maar niet onmogelijk) om af te weren. Dit vereist een actieve houding in DDoS-bescherming, die snel kan reageren op nieuwe soorten aanvallen.

Beide ontwikkelingen tonen aan dat de dreiging van DDoS actueler is dan ooit. We zien al enkele jaren een stijgende lijn in het aantal, de duur en impact van DDoS-aanvallen. De eerste cijfers van 2019 laten zien dat die stijgende lijn zich ook in dit jaar voortzet. En de opkomst van nieuwe soorten DDoS-aanvallen wijst op de noodzaak van voortdurende oplettendheid en onderzoek. Reden genoeg voor de NBIP om zich actief in te blijven zetten voor de bescherming van haar deelnemers.

NBIP nationale beheersorganisatie internet providers

Voor meer informatie:

www.nbip.nl