DDoS data rapport 2020

Aanvallen in 2020:
krachtiger, complexer en duren langer

NBIP nationale beheersorganisatie internet providers

Colofon

Het NBIP DDoS data rapport 2020 is een uitgave van Stichting Nationale Beheersorganisatie Internet Providers (NBIP).

Datum van uitgave
April 2021, jaargang 4

Hoofdredactie
Octavia de Weerdt (NBIP)

Redactie
Gerald Schaapman (NBIP)

Bijdragen
NaWas operationeel team

Eindredactie
Marc Boersma (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

Vorm
Dit rapport is gemaakt in PDF-formaat

Samenvatting
Ook in 2020 blijven DDoS-aanvallen een hardnekkig probleem die het maatschappelijke en economische leven ernstig kunnen ontregelen. In 2020 waren de DDoS-aanvallen krachtiger, complexer en duurden langer in vergelijking met voorgaande jaren. Inzet van NaWas is meer dan ooit vereist om DDoS-aanvallen het hoofd te blijven bieden.

Inhoudsopgave

Samenvatting

De DDoS-aanvallen vormen nog steeds een groot maatschappelijk probleem. Doordat ze in staat zijn om systemen plat te leggen, ontwrichten ze het economische leven voor korte tijd. Als gevolg van het massale thuiswerken door de uitbraak van corona zijn we nog meer dan voorheen afhankelijk van digitale systemen die in de cloud draaien. Dat maakt ons nog meer kwetsbaar voor DDoS-aanvallen.

In 2020 hebben we een aantal opvallende ontwikkelingen gezien. De DDoS-aanvallen werden complexer, krachtiger en duurden vooral een stuk langer in vergelijking met de aanvallen in 2019.

In het derde kwartaal heeft NBIP 307 aanvallen geconstateerd. Gemiddeld ging het om vier aanvallen per dag. De sterkste aanval had een kracht van 200 Gbps. In totaal registreerde de NaWas 38 aanvallen die langer dan vier uur duurden. Ter vergelijking: in het eerste kwartaal zagen we 11 aanvallen die langer dan vier uur duurden. In het derde kwartaal waren dat 16 aanvallen die langer dan vier uur duurden en in het vierde kwartaal van 2020 waren dat er 21. De meest voorkomende aanvallen waren DNS Amplification en LDAP Amplification. Ze waren bijzonder krachtig en waren grotendeels gericht op ISP's en grote ondernemingen in Europa.

In de laatste drie maanden van 2020 zagen we een toename van het aantal technisch complexere aanvallen: de zogeheten carpet bombing. In augustus begonnen krachtige aanvallen op de infrastructuren van ISP's die bleven voortduren. Het ging om buitengewoon krachtige aanvallen tot een capaciteit van 167 Gbit per seconde en duurden langer dan vier uur. In de laatste vier maanden zagen we ook DDoS-aanvallen na werktijd en het gemiddelde aantal aanvallen bedroeg vier per dag.

Deze trend zet ook dit jaar door. In het eerste kwartaal van 2021 hebben we al meer aanvallen geconstateerd dan in heel 2020, waarbij de krachtigste aanval een omvang van 300 Gbps had

Download infographic

Voorwoord

De NBIP presenteert alweer het vierde jaaroverzicht met DDoS-data in 2020 met cijfers afkomstig van Nationale DDoS Wasstraat (NaWas) van de stichting Nationale Beheersorganisatie Internet Providers (NBIP). In dit rapport vindt u een overzicht van alle cijfers en trends rondom DDoS-aanvallen op het Nederlandse deel van het internet. In totaal beschermt NaWas inmiddels 2,5 miljoenen .nl domeinnamen.

De NaWas

De wasstraat voor DDoS-aanvallen is sinds 2014 operationeel en zorgt voor een automatische 24/7 mitigatie van DDoS-aanvallen voor aangesloten deelnemers. Door de bundeling van capaciteit, technologie, kennis en kunde, realiseert de NaWas een uitermate effectieve bestrijding van DDoS-aanvallen. De wasstraat zorgt voor een scheiding van het besmette en schone internetverkeer. Via een apart VLAN stuurt de wasstraat het schone verkeer naar de deelnemer. Door uitschakeling van de DDooS-aanval blijven de systemen en diensten van de deelnemer beschikbaar.

De NBIP en dit rapport

Sinds 2017 publiceert de NBIP jaarlijkse rapporten met uitgebreide (achtergrond) informatie over DDoS-aanvallen. Deze rapporten geven inzicht in aantal, grootte, duur en soorten DDoS-aanvallen. In de rapporten is tevens informatie over gesignaleerde trends te lezen.

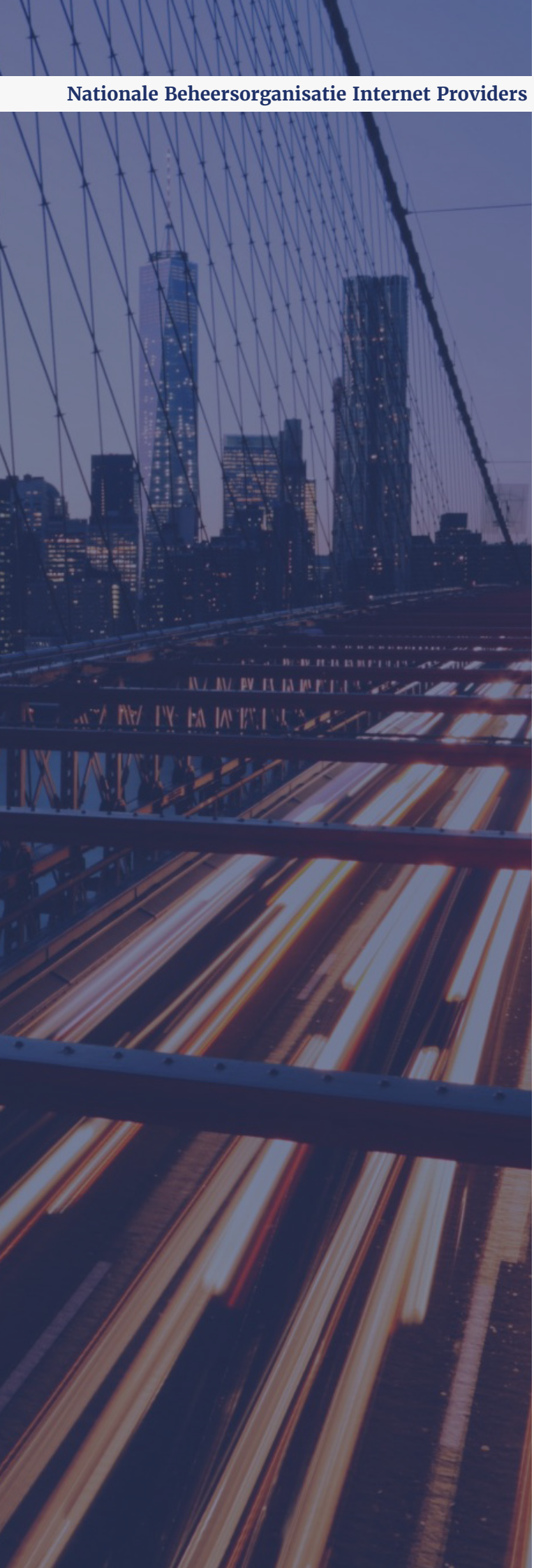
Naast het opschonen van vervuild internetverkeer met de NaWas doet de NBIP nog veel meer: in samenwerking met branchegenoten faciliteren we detectie en bestrijding van online abuse, zoals malware, spam en kwetsbaarheden. Het uitvoeren van tapvorderingen van opsporings- en veiligheidsdiensten behoren tot het takenpakket.

Met dit DDoS Data rapport 2020 willen we zoveel mogelijk kennis en achtergrondinformatie delen over DDoS-aanvallen met onze deelnemers, stakeholders en geïnteresseerden. Binnen onze organisatie is veel diepgaande kennis over dit onderwerp aanwezig. Om de komende jaren het toenemende aantal DDoS-aanvallen het hoofd te kunnen bieden, is een gezamenlijke aanpak van alle betrokkenen noodzakelijk. DDoS-aanvallen zijn inmiddels een veel voorkomende en permanente bedreiging voor een veilig en stabiel internet en de verwachting is dat dit niet zal veranderen. Met dit rapport deelt de NBIP kennis over DDoS-aanvallen en hiermee samenhangende risico's en methoden voor preventie en mitigatie. Dit rapport geeft inzicht in de trends en ontwikkelingen van het afgelopen jaar.

Intensieve samenwerking geeft nieuwe inzichten en mogelijkheden

Doordat steeds meer organisaties en sectoren zich bewust zijn dat DDoS-aanvallen een permanente dreiging vormen, ontstaan ook intensievere samenwerkingen bij de bestrijding ervan. Zo is in 2018 een start gemaakt met de anti-DDoS coalitie, een samenwerking tussen inmiddels 18 organisaties waaronder telecomproviders, financiële instellingen, overheidsorganisaties, politie en de digitale sector.

Via het DDoS clearinghouse, waarvoor



momenteel een proof of concept loopt, delen samenwerkende partijen relevante informatie over DDoS-aanvallen. Ook voeren ze levensechte simulaties uit, waarbij organisaties DDoS-aanvallen op elkaar uitvoeren met als doel hun kennis en ervaring op dit gebied te vergroten. Zo leren ze hoe ze een aanval kunnen herkennen en mitigeren en hoe medewerkers van organisaties hierop moeten reageren.

De NaWas in 2020

Door de coronacriss hebben we in 2020 een uitzonderlijk jaar beleefd. De aanvallen duurden het afgelopen jaar een stuk langer - soms wel vier uur achter elkaar - en waren een stuk krachtiger en complexer van opzet. Dat zien we ook in het eerste kwartaal van 2021, waarin we al meer aanvallen hebben gemeten dan in heel 2020. Deze ontwikkelingen laten zien dat we als NBIP niet stil moeten blijven zitten en de komende jaren een krachtig beleid moeten ontwikkelen om de DDoS-aanvallen met NaWas het hoofd te kunnen blijven bieden.

Ondanks de toename van het aantal, de duur en de complexiteit van de DDoS-aanvallen in het afgelopen jaar doen we het in Nederland nog niet zo heel slecht in vergelijking met andere landen. Met de NaWas zijn we heel goed in staat om zelfs hele krachtige en complexe DDoS-aanvallen op een adequate manier af te slaan. We hebben hierdoor veel economische schade weten te beperken doordat bedrijven en thuiswerkers ongestoord hebben kunnen doorwerken.

De NaWas hebben we ooit opgericht vanuit de gedachte **samen sta je sterker**: dit uitgangspunt is vandaag de dag meer dan ooit van toepassing in de huidige crisistijd. Onze missie zullen we ook het komende jaar met de grootste passie en toewijding blijven uitvoeren.

Met vriendelijke groet,

Octavia de Weerdt

Algemeen directeur NBIP

1. Inleiding

DDoS-aanvallen in het nieuws

Aan nieuws over DDoS-aanvallen was in 2020 geen gebrek. Burgers, consumenten, studenten, leerlingen en bedrijven hebben in 2020 op verschillende manieren last ondervonden van DDoS-aanvallen. Een kleine greep uit het nieuws van het afgelopen jaar:

- In februari werd in de Tweede Kamer gedebatteerd over de vraag of de wet voldoende mogelijkheden biedt om het online bestellen van 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.
- In oktober werden vijf servers die een botnet aanstuurden in Amsterdam offline gehaald.
- In december 2020 moest de Radboud Universiteit Nijmegen een tentamen afblazen vanwege herhaalde DDoS-aanvallen.

Omdat niemand immuun is voor DDoS-aanvallen is het noodzakelijk 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.

De toename van het aantal DDoS-aanvallen zagen we ook in het eerste kwartaal van 2021, waarin er al meer dan DDoS-aanvallen dan in het jaar 2020.

Jaarlijkse rapportage

De NaWas registreert jaarlijks vele honderden DDoS-aanvallen, die inzicht geven in de manier waarop DDoS-aanvallen evolueren. De NBIP deelt deze inzichten met als doel het internet voor iedereen veiliger te maken. Daarom publiceert de NBIP ieder jaar het DDoS Data rapport. We zien trends ontstaan of kunnen juist constateren dat sommige ontwikkelingen helemaal geen trends zijn. Het biedt de lezer hopelijk houvast om op basis van een substantiële hoeveelheid data 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 de werking ervan. Wie nog onbekend is met bepaalde termen, kan de bijlage achter in dit rapport raadplegen. In dit onderdeel geven we uitleg van van de meest voorkomende begrippen.

2. DDoS - de basis

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

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, IoT-devices of andere aan internet gekoppelde apparaten. Dit doen aanvallers door injecteren met bijvoorbeeld malware of via e-mail attachments. Aanvallers injecteren computers met malware door e-mails met besmette attachments te versturen. Zo ontstaat een botnet', een netwerk van geïnfecteerde devices. Vervolgens krijgt dit botnet de opdracht om veel 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 te organiseren, gebeurt 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 het doel kan ook zijn om beschikbare bandbreedte voor inkomend verkeer te overbelasten, waardoor de server ook niet langer bereikbaar is.

Wie een DDoS-aanval wil uitvoeren, hoeft geen technische kennis in huis te hebben. Op speciale websites (het zijn er duizenden) kan iedereen met een creditcard of bitcoins DDoS-aanvallen bestellen, en niet alleen op het darkweb. Ook is het mogelijk om met relatief weinig voorkennis zelf een aanval op te tuigen: handleidingen om een eigen botnet op te zetten zijn eenvoudig te vinden en ook kennis voor aanvallen met andere tactieken is ruim voorhanden.

Wie een DDoS-aanval wil uitvoeren, hoeft geen technische kennis in huis te hebben.

Waarom zijn DDoS-aanvallen zo populair?

Een DDoS-aanval is nog steeds de meest voor de hand liggende manier 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 gemakkelijker door het toenemend aantal DDoS-diensten die vanuit de cloud beschikbaar zijn. Hosting is goedkoop en er is steeds meer bandbreedte beschikbaar. Het kopen van malafide diensten op het internet is dus dus steeds eenvoudiger en goedkoper. Deze diensten worden via zogenaamde 'stressers' of 'booters' ingekocht. Verreweg de meeste DDoS-aanvallen worden gefaciliteerd 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 veel 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 zijn verbonden met het internet. Vaak gaat het om apparaten met een slechte (of geen) standaardbeveiliging. Zo vormen IoT-devices een makkelijk doelwit om te dienen als pion in een botnet. Volgens onderzoeksbureau Gartner zullen er in het jaar 2021 ruim 25 miljard van dat soort apparaten beschikbaar zijn.

Gevolgen van een DDoS-aanval

De gevolgen van een DDoS-aanval zijn divers. Van kleine irritatie tot grote ontregelingen: het behoort allemaal tot de mogelijkheden. Van een aanval kan één persoon heel erg last hebben (zijn of haar persoonlijke webblog is niet beschikbaar), maar ook een groot deel van de samenleving (internetbankieren doet het niet) kan worden gedupeerd..

Dat een gerichte DDoS-aanval voor financiële schade kan zorgen, heeft de NBIP eerder 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 een enkele server worden gehost. Een website kan bijvoorbeeld getroffen worden door een DDoS-aanval, terwijl het niet het doelwit is, omdat de aanval zich richt op een andere site die op dezelfde server is gehost.

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: al het internetverkeer buiten een bepaalde geografische locatie krijgt geen toegang. Dit is een redelijk effectieve manier, maar staat ook te boek als grof geschut. Immers, de bezoekers uit het geblockte gebied hebben geen toegang meer tot de diensten.

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 bekijken 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 privacymaatregelen 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 2020 betrof het data van 97 deelnemers. Eind 2020 had de NaWas 97 deelnemers.

Deze deelnemers bestaan grotendeels uit Internet Service Providers (ISP’s). Met een ISP bedoelen we in dit onderzoek een bedrijf of organisatie 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. 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. Onder de deelnemers zijn ook enkele grote organisaties, zoals banken en verzekeraars, te vinden. 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) uit te drukken. Een uitleg van de termen en soorten aanvallen is de bijlage te lezen. Zoals gemeld in het voorwoord, gaat dit rapport uit van lezers met enige voorkennis op het gebied van DDoS-aanvallen.

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

4. Resultaten DDoS cijfers 2020

In dit rapport maken we een analyse van het aantal, de grootte en de duur van DDoS-aanvallen in 2020. We schenken daarnaast ook aandacht aan:

- Soorten DDoS-aanvallen
- Opvallende DDoS-aanvallen in 2020
- Nieuwe typen DDoS-aanvallen in 2020
- Trends die uit de data kunnen worden afgeleid

4.1 Aantal DDoS-aanvallen

In het jaar 2020 zijn maar liefst 1.610 DDoS-aanvallen geregistreerd door de NaWas. Omgerekend zijn dit 4,4 DDoS-aanvallen per dag. In 2019 werden 919 DDoS-aanvallen geregistreerd. Dit betekent een stijging van maar liefst 75% ten opzichte van 2019, gebaseerd op absolute aantallen die toenamen als het gevolg van een stijging van het aantal deelnemers van de NaWas.

De meeste aanvallen zagen we in de maand november. In die maand verwerkte de NaWas maar liefst 213 aanvallen. December 2020 was met 190 de één na drukste maand.

De maanden juni, juli en augustus 2020 waren met respectievelijk 94, 87 en 67 aanvallen relatief het rustigst. Na de zomer namen het aantal aanvallen weer toe: in september en november waren er respectievelijk 153 en 137 aanvallen. In januari van 2020 werden 133 aanvallen geregistreerd, gevolgd door 118 aanvallen in februari. In maart zagen we weer een stijging van het aantal aanvallen: maar liefst 158 werden er deze maand geregistreerd. In april en mei namen de aantallen iets af met achtereenvolgens 121 en 94 geregistreerde aanvallen.

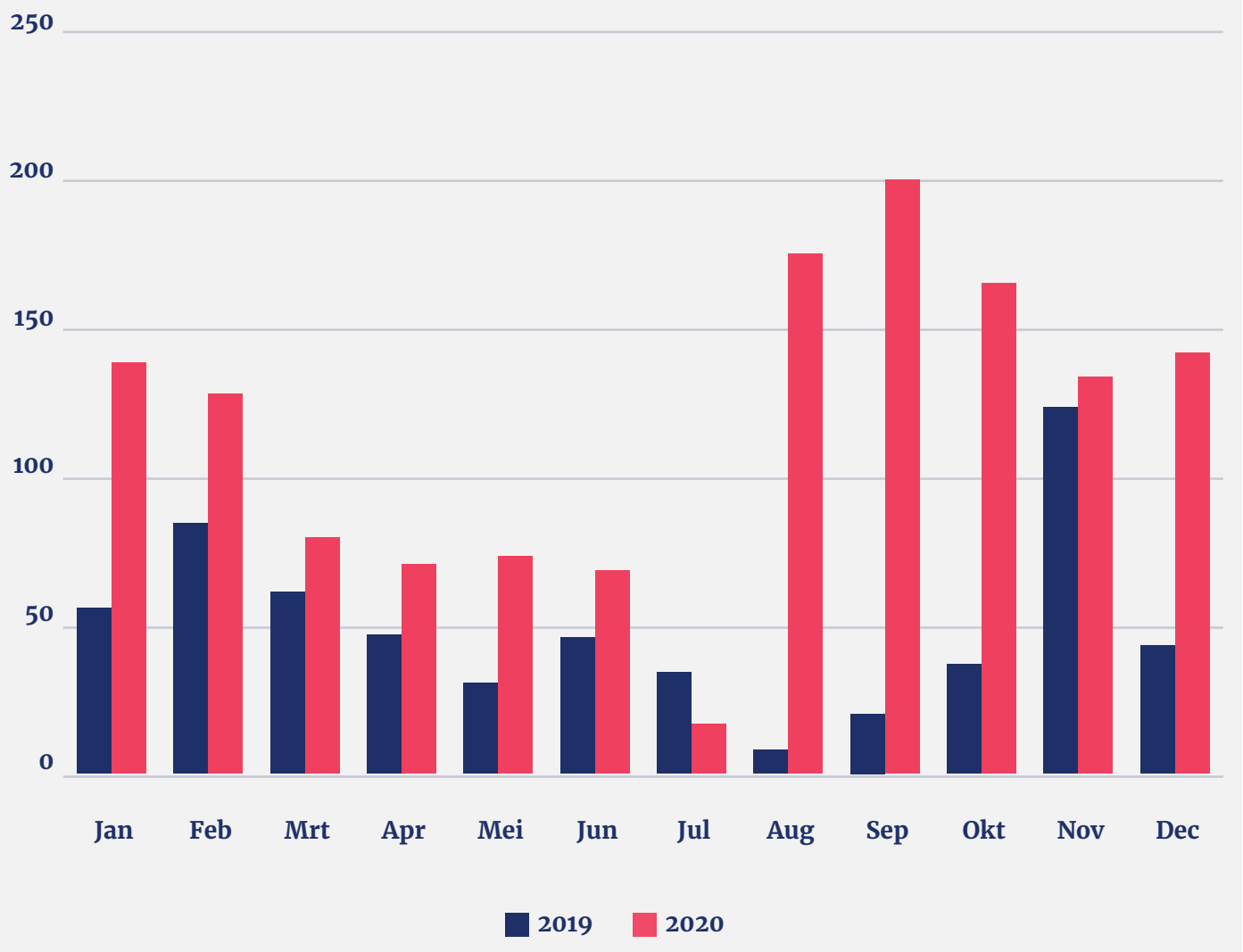
4.2 Grootte van een DDoS-aanval

De grootte van een DDoS-aanval drukken we uit in gigabit per seconde, ofwel Gbps. In de onderstaande grafiek is het aantal DDoS-aanvallen verdeeld in vijf categorieën: kleiner dan 1 Gbps, tussen 1-10 Gbps, tussen 10-20 Gbps, tussen 20- 40 Gbps en groter dan 40 Gbps. Om ook inzicht te geven in de ontwikkeling van de DDoS-aanvallen in de afgelopen jaren, hebben we ook de tabellen voor 2019 opgenomen.

2020	Kwartaal 1	Kwartaal 2	Kwartaal 3	Kwartaal 4
< 1 Gbps	89	116	120	182
1 - 10 Gbps	265	201	141	257
10 - 20 Gbps	33	15	21	56
20 - 40 Gbps	11	11	6	22
> 40 Gbps	11	11	19	23

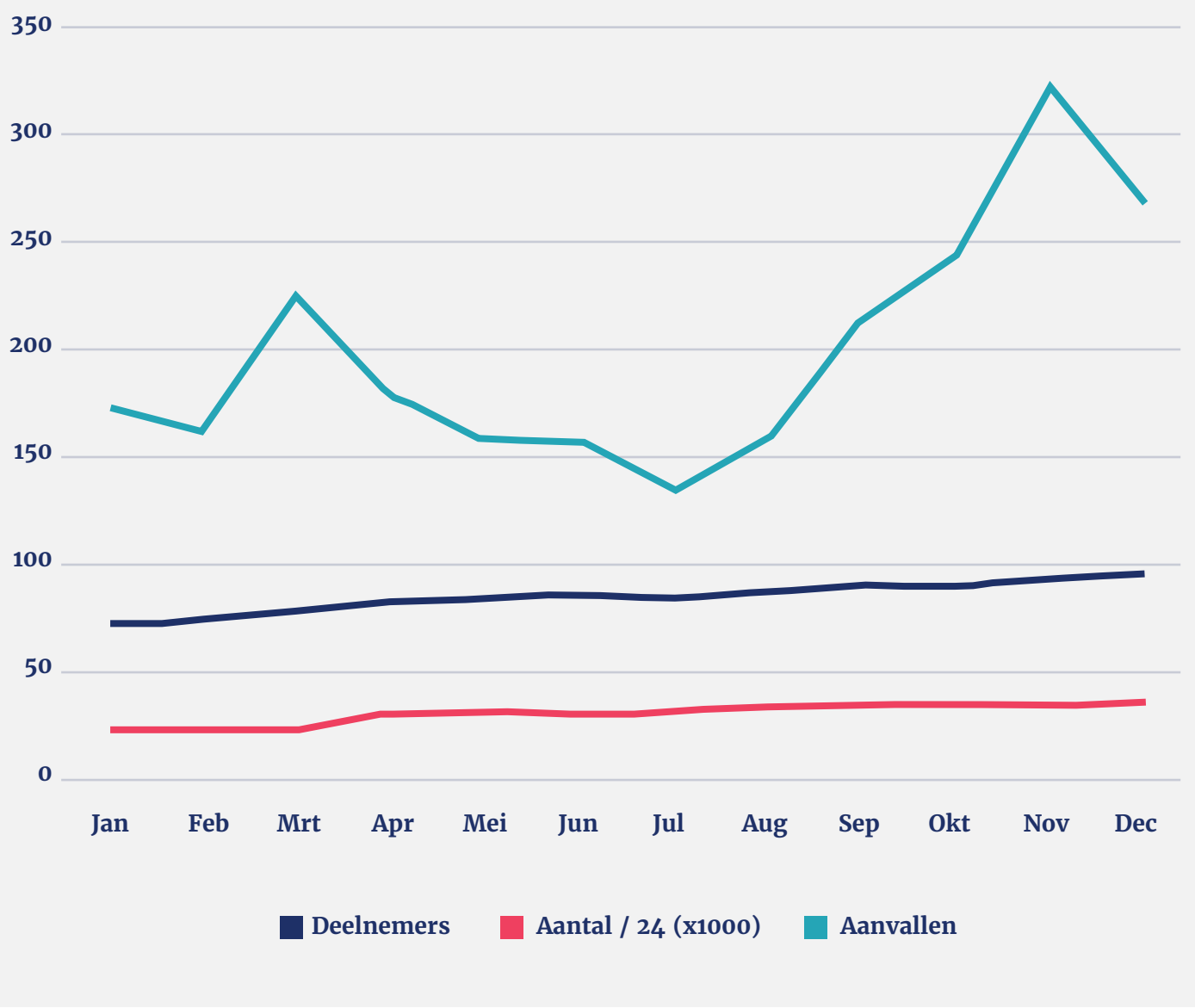
2019	Kwartaal 1	Kwartaal 2	Kwartaal 3	Kwartaal 4
< 1 Gbps	92	91	43	47
1 - 10 Gbps	144	174	91	140
10 - 20 Gbps	18	22	5	16
20 - 40 Gbps	7	10	2	6
> 40 Gbps	5	3	0	3

Max Gbps per maand



	Jan	Feb	Mrt	Apr	Mei	Jun	Jul	Aug	Sep	Okt	Nov	Dec
Deelnemers	74	77	80	84	86	87	86	89	91	91	94	97
Aantal / 24	24,5	24,7	24,7	31,9	32,4	32,5	32,5	34,3	34,7	34,7	34,8	34,9
(x1000)	54	8	96	69	49	81	14	44	25	25	38	15
Aanvallen	175	164	228	181	160	159	138	161	217	246	324	269

Deelnemers versus aanvallen en beschermde prefixen



Ten opzichte van 2019 zien we in 2020 een duidelijke toename van het aantal aanvallen kleiner dan 1 Gbps. In het derde kwartaal van 2020 zagen we 120 aanvallen met deze kracht, tegenover 43 aanvallen in 2019. Dat gold ook voor het vierde kwartaal van 2020. Toen werden er 182 aanvallen met een kracht van 1 Gbps geregistreerd. In het vierde kwartaal van 2019 waren dat er 47.

Bij de aanvallen met een kracht tussen de 1 en 10 Gbps zien we ook in 2020 ook een duidelijke toename. In het vierde kwartaal van 200 waren dat er 257, tegenover 140 in dezelfde periode van 2019. Deze toename was ook te zien in het eerste kwartaal van 2020. Het ging toen om 265 aanvallen met deze kracht. In 2019 waren dat in het eerste kwartaal 144.

In absolute aantallen gemeten waren er in 2020 niet zoveel aanvallen met een kracht tussen de 10 en 20 Gbps. In het eerste kwartaal waren dat er 33. Kijken we naar het eerst kwartaal van 2019, dan waren dat er 18. In het laatste kwartaal van 2020 waren dat er 56, tegenover 16 in dezelfde periode in 2019.

Voor de aanvallen met een kracht tussen 20 en 40 Gbps zagen we in 2020 een duidelijke toename ten opzichte van het jaar daarvoor. In het derde kwartaal van 2020 waren dat er 19, terwijl we in 2019 daarvan slechts twee aanvallen zagen. In het vierde kwartaal van 2020 werden 23 aanvallen met deze kracht, tegenover zes van deze aanvallen in 2019.

Ook voor aanvallen groter dan 40 Gbps gold in 2020 een duidelijke toename ten opzichte van 2019. In het laatste kwartaal registreerde de NaWas 23 aanvallen, tegenover drie aanvallen in 2019. In het derde kwartaal van 2020 waren dat er 19 tegenover nul in het derde kwartaal van 2019.

4.3 Duur van een DDoS aanval

Met betrekking tot de maximale duur van een DDoS-aanval zien we ten opzichte van de voorgaande jaren een duidelijke stijging. In 2018 bedroeg de maximale duur van een DDoS-aanval 1 dag en 5 uur. Het daaropvolgende jaar zagen we een toename van de totale tijdsduur naar 1 dag en 12 minuten. Een duidelijke stijging is te zien in 2020: de maximale duur van een DDoS-aanval duurt maar liefst 20 dagen en 6 uur.

Als we kijken naar de duur van de DDoS-aanvallen over de verschillende maanden van 2020, dan zien we in de maanden september en oktober een duidelijke piek. In september duurde de langste aanval maar liefst 20 dagen en 6 uren. Voor de maand oktober is deze duur 13 dagen en 14 uren. In de overige maanden van dat jaar duren de DDoS-aanvallen tussen de één en zeven dagen.

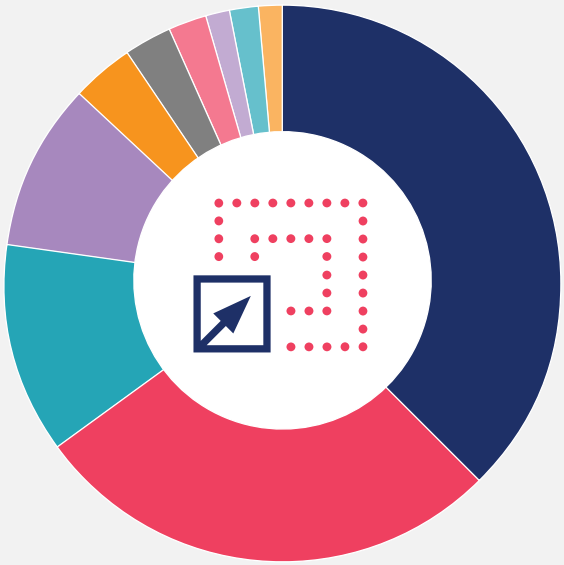
4.4 Soorten DDoS-aanvallen

In 2019 hebben we 49 soorten DDoS-aanvallen waargenomen. In 2020 is dit aantal gedaald naar 34 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 2019 zien we in 2020 een toename van het aanvalstype UDP amplification en een afname van het type TCP flood. Deze percentages bedroegen in 2019 nog respectievelijk 50% en 32%, waar dit in 2020 71% en 12% was. Afgezet tegen de cijfers van 2018 en 2019 zien we in 2020 een duidelijk dalende trend van de TCP flood. Kijken we naar UDP amplification dan zien we ten opzichte van 2018 een duidelijke opgaande trend in 2020. Het percentage UDP flood is de laatste drie jaren min of meer stabiel gebleven. In vergelijking met 2019 is in 2020 de top drie met meest voorkomende soorten DDoS-aanvallen gelijk gebleven: DNS amplification, LDAP amplication en UDP flood. Het aandeel DNS amplification is 2020 met een percentage van 32,12% bijna verdubbeld ten opzichte van 2019 (16,6%). Bij LDAP amplification zien we een in 2020 een duidelijke stijging naar 23,57%, terwijl dat percentage in 2019 nog 13,8% bedroeg. Op de derde plaats van meest voorkomende type DDoS-aanvallen in 2020 staat UDP flood met 10,45%. In 2019 bedroeg dit percentage 10,3% en dat betekent dat het aandeel van dit type aanval vrijwel gelijk is gebleven. Op de vierde plek met meestvoorkomende type DDoS-aanvallen staat NTP amplifcation met 8,38%. In 2019 bedroeg dit percentage 8,6% en het aandeel is hiermee ongeveer even groot als in 2020.

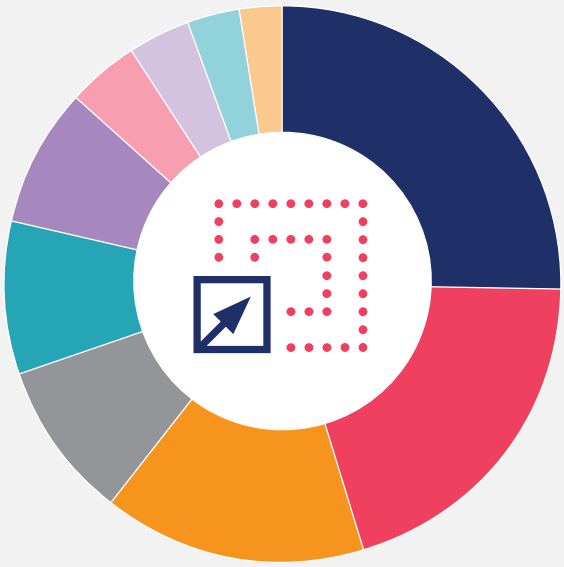
Jaar	< 15 min	15-60 min	1-4 uur	> 4 uur
2017	37,4%	41,2%	18,3%	3,4%
2018	34,4%	45,9%	16,6%	3,1%
2019	44,1%	41,2%	11,6%	3,2%
2020	47,40%	40,20	9%	3,30

DDoS-type (top 10) 2020



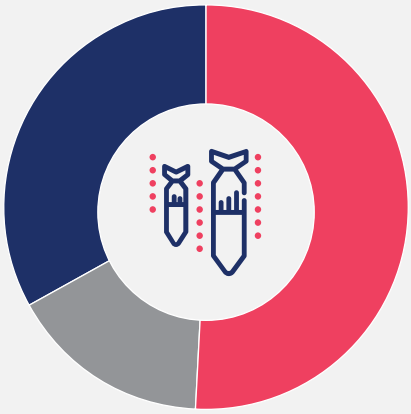
- 37,6% DNS amplification
- 27,6% LDAP amplification
- 12,2% UDP flood
- 9,8% NTP amplification
- 3,6% TCP/SYN flood
- 2,6% TCP/ACK flood
- 2,2% UDP memcached
- 1,6% SNMP amplification
- 1,5% TCP/SYN/ACK
- 1,3% WS-Discovery amplification

DDoS-type (top 10) 2019



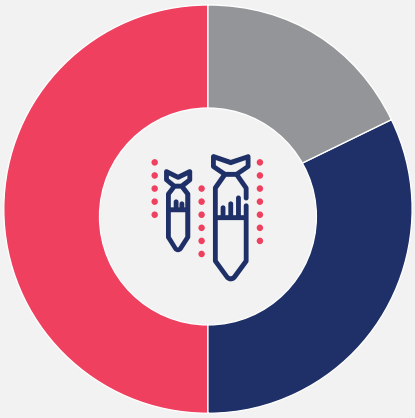
- 25,3% DNS amplification
- 20,2% LDAP amplification
- 15,2% TCP/SYN flood
- 9,2% TCP/ACK flood
- 8,7% UDP flood
- 8,2% NTP amplification
- 4,2% UDP flood 2
- 3,5% GRE flood
- 3,0% TCP/RST flood
- 2,4% TCP/ACK flood; flags AP

DDoS-type hoofdgroep verdeling 2018



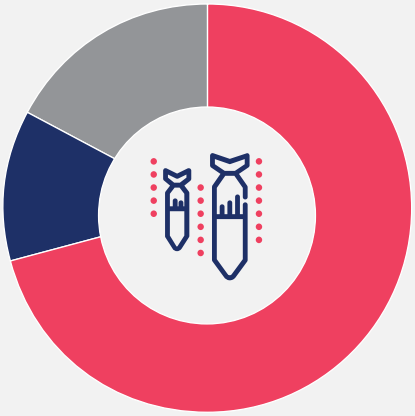
33% TCP flood
51% UDP amplification
16% UDP flood

DDoS-type hoofdgroep verdeling 2019



32% TCP flood
50% UDP amplification
18% UDP flood

DDoS-type hoofdgroep verdeling 2020



12% TCP flood
71% UDP amplification
17% UDP flood

4.5 Multivector aanvallen

Ook in 2020 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. In 2020 zijn aanvallen met 11, 12 of 13 vectoren zijn ook met enige regelmaat waargenomen.

4.6 Opvallende DDoS-aanvallen

Bij DNS water torture gaat het om aanvallen op niet-bestaande subdomeinen van een bestaande domeinnaam. Deze subdomeinen worden willekeurig en automatisch door de aanvaller aangemaakt. Door de bevraging van willekeurige subdomeinen kan de hoogste authority server niet aan deze verzoeken voldoen omdat deze informatie niet in het cache staat. Het resultaat is dat de authority server onderuit gaat.

4.7 Nieuw waargenomen DDoS-aanvallen

Cybercriminelen zijn voortdurend op zoek naar nieuwe protocollen en/of services die ze kunnen inzetten voor DDoS-aanvallen. Het gaat dan met name over protocollen en/of service die kunnen zorgen voor een multiplier. In 2020 zijn de protocollen Microsoft Remote Desktop protocol, 4talk amplification en Quote of the Day (QOTD) gebruikt.

5. Trends

In 2020 zien we een aantal duidelijke trends ten opzichte van voorgaande jaren. In de eerste plaats zien we een duidelijke stijging van het aantal aanvallen. Dat zijn er 1.610 in 2020 tegen respectievelijk 919 en 928 in 2019 en 2018. Ook worden de DDoS-aanvallen steeds krachtiger: 200 Gbps in 2020, terwijl in de twee voorgaande jaren deze 124 Gbps (2019) en 68 Gbps (2018) bedroegen. Als we kijken naar de duur van de aanvallen is ook een stijgende lijn zichtbaar: de langste aanval duurde in 2020 maar liefst 20 dagen en 6 uren. In 2018 (1 dag en 4 uren) en 2019 (1 dag en 12 uren) duurden deze aanvallen een stuk korter. Met een kracht van 200 Gbps vond de grootste aanval plaats november 2020. In 2019 was de grootste aanval 124 Gbps. De kleinste aanval van 18,1 Gbps zagen we in juli 2019.

In 2020 werden 763 aanvallen geconstateerd die korter dan 20 minuten duurden. In 2019 waren dat 405 aanvallen. Ook het aantal aanvallen die tussen de 15 en 60 minuten duurden, namen toe: in totaal ging dat om 648 aanvallen. In 2019 waren dat er 378. Kijken we naar het aantal aanvallen die tussen de een en vier uur duurden, dan waren dat er 146. Een jaar daarvoor waren dat er 107. In 2020 constateerde de NaWas 53 aanvallen die langer dan vier uur duurden. In 2019 waren dat er slechts 23: dat betekent in 2020 meer dan een verdubbeling van het aantal aanvallen die langer dan vier uur duurden.

Drempelwaarde verhogen

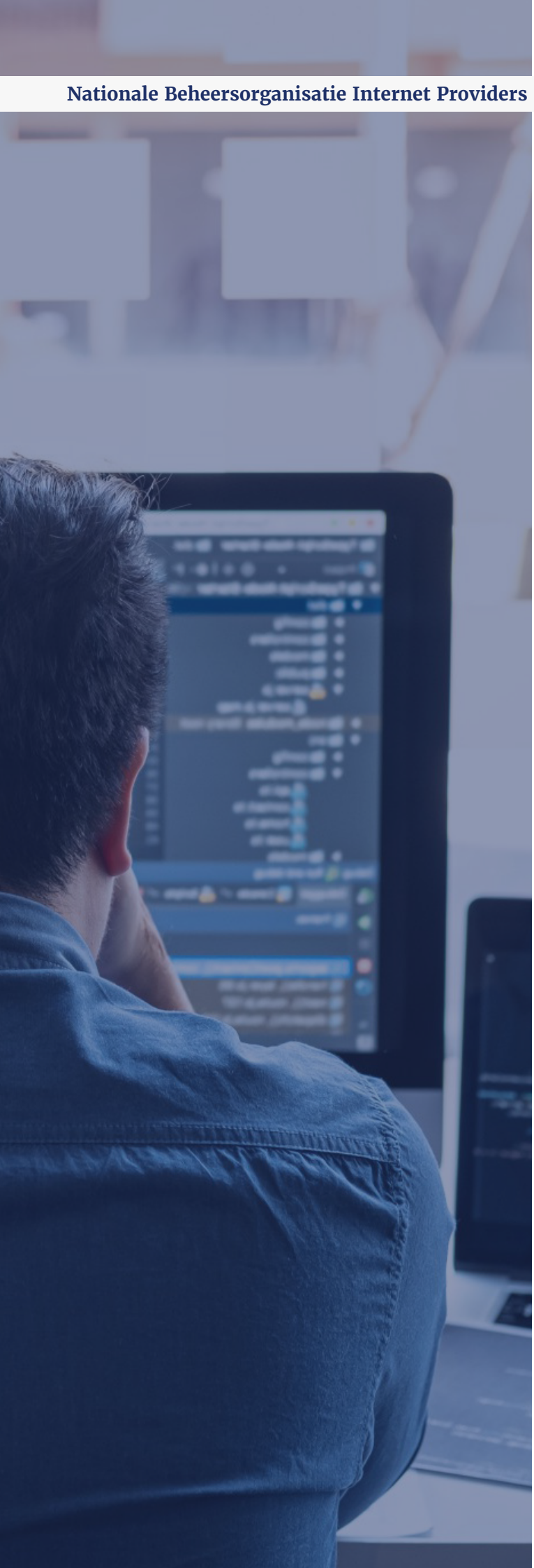
Voor het coronatijdperk hanteerde de NaWas een bepaalde drempelwaarde. Komt deze waarde boven een bepaald niveau, dan checkt de anti-DDos-apparatuur of het om een aanval gaat. Doordat het thuiswerken is toegenomen, betekent dat ook meer verkeer op de poorten. Het is voorgekomen dat duizenden werkplekken werden gezien als een soort DDoS-aanval. Dat had tot gevolg dat er meer gefilterd werd, wat niet de bedoeling was. De NaWas heeft de drempelwaardes moeten ophogen om te zorgen dat het toenemende verkeer op poorten niet meer als aanval werd gezien.

> In de eerste plaats zien we een duidelijke stijging van het aantal aanvallen in 2020.

Aanvallen op internetserviceproviders

In 2020 zagen we in de maanden augustus en september aanvallen op de infrastructuren van internetserviceproviders. De DDoS-aanvallen waren gericht op routers en DNS infrastructuren van de types DNS amplification, LDAP amplification en NTP amplification. De aanvallen waren zeer heftig, tot 260 Gbit per seconde en als een aanval was afgeslagen, begon de volgende alweer een half uur later.

De aanvallen waren bijzonder krachtig (tot 260 Gbit per seconde) en duurden soms langer dan vier uur. Ze waren gericht op internetserviceproviders in de Benelux. De aanvallen zijn in te delen in vier verschillende categorieën: LDAP amplification, DNS amplification , NTP amplification en DNS request flood. Uit metingen van NBIP is de volgende onderverdeling gebleken: LDAP amplification (37%), DNS amplification (37%), NTP amplification (18%) en DNS request flood (10%).



Aanvallen op isp's

De DDoS-aanvallen waren onder meer gericht op Caiway. Op dinsdagochtend 1 september had de provider last van een grote DDoS-aanval. Verder vond op dinsdagmiddag een grote aanval op Signet plaats. Signet beheert ook de infrastructuur voor TransIP en hun klanten hadden ook storingen door die aanval. Het forum van de Belgische ISP EDPNet spreekt zelfs over aanvallen tot 200 Gbit per seconde. Deze provider heeft al vijf dagen achter elkaar DDoS-aanvallen gehad.

Ook bedrijven buiten de Benelux werden aangevallen en kregen te maken met uitval van de internetdiensten. NaWas was in staat om in korte tijd meerdere nieuwe deelnemers aan te sluiten om DDoS te bestrijden en het internet veiliger te maken. Onlangs heeft NaWas zijn aanwezigheid uitgebreid naar Londen op de London Internet Exchange (LINX), Italië met de aansluiting van IT.Gate op Top-IX en de Vienna Internet Exchange (VIX).

Profielen voor deelnemers

Voor deelnemers heeft NaWas afhankelijk van het type aanval een aantal profielen ontwikkeld die in verschillende situaties kunnen worden ingezet. Op deze manier kan snel een bepaald type DDoS-aanval worden tegengehouden en daardoor hoeven niet adhoc instellingen worden gemaakt.

Bij een DDoS-aanval wordt de NaWas ingeschakeld met een commando. Dat doet de NaWas door het instellen van een prefix. Deelnemers die meer last hebben van DDoS-aanvallen laten de prefixen, ook wel de routes via de NaWas genoemd, langer staan. Ze laten de prefixen in stand omdat ze nieuwe aanvallen vrezen. Dat komt omdat er meer DDoS-aanvallen achter elkaar worden uitgevoerd.

De toename van het aantal aanvallen zien we ook in het eerste kwartaal van 2021, waarin al meer aanvallen zijn geconstateerd dan in heel 2020. De krachtigste aanval had in het eerste kwartaal van 2021 een kracht van maar liefst 300 Gbps.

6. Conclusie

Op basis van de onderzoeksresultaten over het jaar 2020 trekt de NBIP een aantal conclusies: meer aanvallen, die langer duren en tegelijkertijd krachtiger en complexer zijn.

Als we de cijfers over 2020 bestuderen, dan zien we in de eerste plaats een significante stijging van het aantal aanvallen. Dat waren er in 2020 maar liefst 1610 tegen 919 en 928 in 2019 en 2018. Naar de oorzaak van deze toename hebben we geen onderzoek gedaan. De toename is in elk geval opvallend te noemen.

Ook met betrekking tot de kracht van de aanvallen zien we in 2020 een duidelijke stijging ten opzichte van voorgaande jaren. De krachtigste aanval in 2020 had een omvang van 200 Gbps. Ter vergelijking: in 2018 en 2019 waren de krachtigste aanvallen respectievelijk 68 Gbps en 124 Gbps groot.

Ondanks de toename van het aantal, de duur en de complexiteit van de DDoS-aanvallen doen we het in Nederland nog niet zo heel slecht in vergelijking met andere landen. Met het geavanceerde anti-DDos platform NaWas, dat samen met de deelnemende internetserviceproviders en een aantal andere grote organisaties is opgezet, zijn we heel goed in staat om zelfs hele krachtige en complexe DDoS-aanvallen op een adequate manier af te slaan. Hierdoor hebben we al veel economische schade weten te beperken doordat bedrijven en thuiswerkers ongestoord hebben kunnen doorwerken.

> De aanvallen duren langer en zijn tegelijkertijd krachtiger en complexer.

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 basisbeveiliging 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 monitoringdienst 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