DDoS data rapport 2018

Een volwassen en steeds veranderende dreiging

NBIP nationale beheersorganisatie internet providers

Colofon

Het NBIP DDoS data rapport 2018 is een uitgave van Stichting Nationale Beheersorganisatie Internet Providers.

Datum van uitgave
maart 2019, jaargang 2

Hoofdredactie
Octavia de Weerdt (NBIP)

Redactie
Gerald Schaapman (NBIP)

Bijdragen
Bureau NBIP

Eindredactie
Lorenz van Gool (Splend)

Design
Sam Zondervan (Splend)

Marketing
Splend

Vorm
Dit rapport is gemaakt in PDF-formaat

Samenvatting
Het fenomeen ‘DDoS-aanval’ is ingeburgerd in onze samenleving. Zij blijven complex in elkaar steken en de soorten aanvallen zijn continu aan verandering onderhevig. Dit maakt ze dermate lastig te bestrijden. Een DDoS-aanval is inmiddels een volwassen dreiging die serieus genomen dient te worden.

Inhoudsopgave

Voorwoord

U leest het jaarrapport 2018 van stichting Nationale Beheersorganisatie Internet Providers (NBIP) met cijfers en trends rondom de DDoS-aanvallen die door de NaWas (Nationale Wasstraat) zijn gezien, geanalyseerd en gemitigeerd. Dit 'scrubbing center' van 'vuil' internetverkeer is sinds 2014 operationeel en is in zeer korte tijd een bekende naam in de Nederlandse internetsector geworden.

Vorig jaar is de NBIP begonnen met het (half) jaarlijks publiceren van rapporten met data over DDoS-aanvallen. Dit rapport geeft inzage in het aantal DDoS-aanvallen, de grootte van aanvallen, de duur van aanvallen, de soorten DDoS-aanvallen en trends zoals opgevangen door de experts van de NaWas in 2018.

Ook zijn we actief geweest in het breder onderzoek in samenwerkingen met andere partijen, zoals het DDoS-impact onderzoek met Stichting Internet Domeinregistratie Nederland (SIDN). Hieruit bleek dat de NaWas 43% van alle .nl-domeinen in Nederland beschermt - dat zijn er meer dan 2,5 miljoen.

Tevens is de NBIP betrokken bij het DDoS Clearinghouse, een initiatief van meerdere partijen om DDoS-aanvallen beter te begrijpen en zoveel mogelijk te ontleden. Dat resulteerde tot nu toe onder andere in een aantal tools en een DDoS-database. Daarnaast is er een onderzoek naar de DDoS-aanvallen in december 2018 uitgevoerd, waarvan de resultaten aan bod kwamen in het NOS-journaal.

Deze onderzoeken en media-outreach zijn onderdeel van onze focus om zoveel mogelijk kennis te delen, niet alleen op het gebied van DDoS-aanvallen. De NBIP is namelijk ook zeer actief op het gebied van abuse-bestrijding en het uitvoeren van tapbevelen.

Want een beter en veiliger internet begint bij onszelf!

Terug naar DDoS. Onze collectieve aanpak van de NaWas (we kopen samen in en we worden alleen ingezet wanneer nodig) begint nu ook in het buitenland aandacht te krijgen. We zijn verheugd dat NBIP met vele interessante partijen uit heel Europa aan het praten is, op weg naar een pan-Europees anti-DDoS wasstraat. Inmiddels hebben we onze eerste Europese stappen al gezet. Want wij geloven erin dat hoe meer organisaties zich aansluiten, hoe beter onze dienst wordt. Ook over de grenzen.

We hopen dat u bij het lezen van dit rapport nieuwe dingen leert. Wij staan zelf nergens meer van te kijken. Daarom ook dit rapport, zodat u weet wat er speelt. DDoS-aanvallen mitigeren begint met kennis opdoen en delen, daar zijn we heilig van overtuigd.

Veel leesplezier,

Octavia de Weerdt,
Algemeen directeur NBIP

De NBIP beschermt meer dan 2,5 miljoen .nl domeinen

1. Inleiding

Begin 2018 werd Nederland wakker geschud door grote DDoS-aanvallen op verschillende instellingen in Nederland. DDoS was in één klap een hot topic. Enerzijds door het ontwrichtende effect, anderzijds door het gemak waarmee deze aanval uiteindelijk tot stand kwam. Ook zorgde een uitzending van Nieuwsuur met een DDoS-'expert' voor grote hilariteit. Gevolg: een golf van aandacht voor het fenomeen DDoS-aanval. Het zette zowel media als consumenten op scherp.

Het is gebleken dat het delen van kennis noodzakelijk is om de juiste maatregelen te kunnen nemen. Er werd in o.a. NRC en bij BNR gepleit voor een gezamenlijke aanpak van DDoS-dreigingen door banken.

Collectief optreden en data delen om ervan te leren - dat is precies ook de aanpak van NBIP met de NaWas.Dit zorgt ervoor dat wij sinds 2014 ruim 3200 aanvallen effectief hebben kunnen mitigeren.

DDoS-aanvallen zijn, helaas, dagelijkse kost voor ons. Bedrijven krijgen er steeds meer mee te maken en een aanval is steeds vaker in het nieuws. Vooral de aanleiding voor zo'n aanval blijkt vaak het onderwerp van discussie. Vorig jaar lieten we al zien dat het motief (voor de lol) wordt versterkt door het gemak waarmee een DDoS-aanval uit te voeren is.

Dat DDoS als een dreiging wordt ervaren, blijkt uit het nieuws dat Intertoys zo'n aanval zelfs als excuus gebruikte, terwijl eigenlijk sprake was van eigen overbelasting.

> Het begint nu eindelijk te dagen dat het uitvoeren van een DDoS-aanval een vorm van cybercriminaliteit is

Ook de reacties op DDoS-aanvallen worden serieuzer. Hoe eenvoudig het ook uit te voeren is, en hoe luchtig er over zo'n aanval gedaan wordt door bedrijven ("het overkomt mij toch niet"), het is en blijft een misdrijf. Het begint nu eindelijk te dagen dat het uitvoeren van een DDoS-aanval serieus is en een vorm van cybercriminaliteit. Met passende straffen.

Het is daarom noodzakelijk om onderzoek te blijven doen naar DDoS. Het begint immers bij bewustzijn en dat kunnen we niet vaak genoeg benadrukken. Ondanks het gemak waarmee ze kunnen worden uitgevoerd is een DDoS-aanval zelf, hoe deze in elkaar steekt, behoorlijk complex. Dat heeft het rapport van vorig jaar wel laten zien.

Dit rapport gaat uit van een lezer met enige kennis van zaken. In de bijlage zijn de beschrijvingen van alle soorten DDoS-aanvallen die in dit rapport worden genoemd opgenomen.

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, infecteert de aanvaller 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.

Dat klinkt heel eenvoudig, en dat is het helaas ook. Een DDoS-aanval is met zowel geringe als veel technische kennis uit te voeren. 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.

Waarom zijn DDoS-aanvallen zo populair?

Mede daarom is een DDoS-aanval 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.

> Een aanval wordt makkelijker door het stijgende aantal DDoS-diensten vanuit de cloud

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.

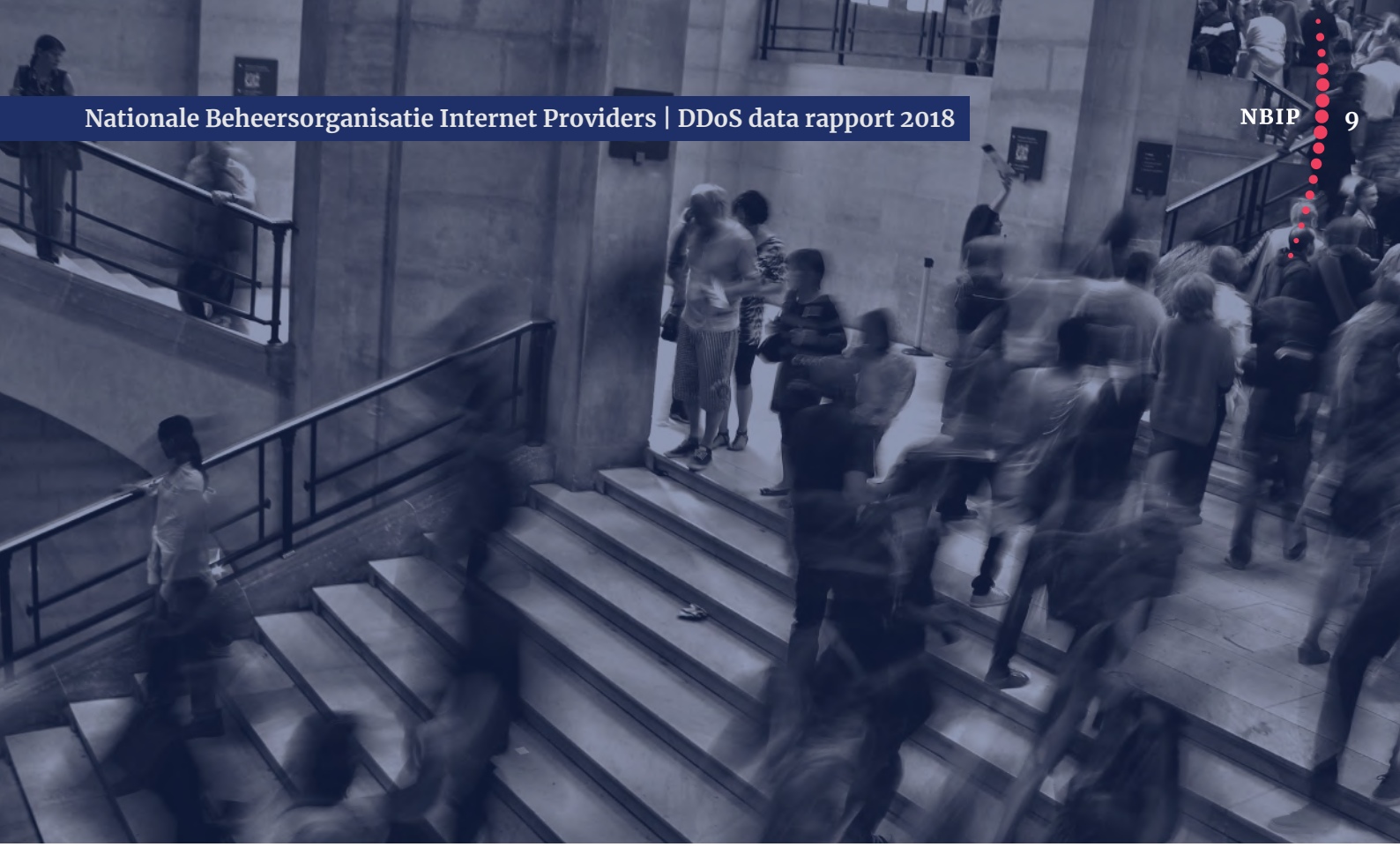
Methoden van DDoS-mitigatie

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 2017 waren dit 56 deelnemers. Eind 2018 betrof het data van 68 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 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. 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 het overzicht te bevorderen en de resultaten voor de lezer zo helder mogelijk te maken.

4. Resultaten DDoS cijfers 2018

Allereerst is het aantal, de grootte en de duur van DDoS-aanvallen (2017/2018) geanalyseerd. Vervolgens zijn de soorten DDoS-aanvallen geanalyseerd die in 2018 zijn voorgekomen, waarbij we kort de resultaten bespreken. Een analyse van de gemeten getallen vindt u in de conclusie.

4.1 Aantal DDoS-aanvallen

In 2018 heeft de NBIP in Nederland wederom meer aanvallen geregistreerd, namelijk 938 DDoS-aanvallen, een stijging van 13,6 procent. Dat zijn ongeveer 2,6 aanvallen per dag.

In 2017 was er nog sprake van 826 DDoS-aanvallen en in 2016 was het aantal 680. De groei vlakt dus wel af, daar de groei vorig jaar (2016-2017) 21,5 procent betrof.

Het aantal deelnemers van de NaWas steeg in 2018 van 56 naar 68.

Het enige rooskleurige aan deze cijfers is dat de voorspelling van het NBIP in het halfjaarrapport 2018 over het totale aantal aanvallen niet is gehaald: namelijk 'over de 1000'.

4.2 Grootte van een DDoS-aanval

De grootte van een DDoS-aanval is gemeten in Gbps (gigabit per second).

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
Mar-2018	33	57	20	3	0	113
Apr-2018	44	55	9	2	0	110
May-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
Oct-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**

Wat meteen opvalt bij het bestuderen van beide tabellen, is dat de grote aanvallen van meer dan 40 Gbps weer terug zijn, nadat ze vorig jaar ontbraken. In 2016 waren het er overigens slechts 2.

Ook is het opvallend te noemen dat oktober in 2017 nog de maand was met de meeste DDoS-aanvallen, terwijl dat vorig jaar juist de rustigste maand was. Een mogelijke verklaring is dat er in 2018 een aantal grote botnets wereldwijd uit de lucht zijn gehaald. Maar dit is niet met zekerheid te zeggen. Juli en augustus blijven, waarschijnlijk vanwege de zomervakantie, relatief rustige periodes.

De verdeling van de grootte van aanvallen bleef nagenoeg hetzelfde, al is er een lichte verschuiving te zien naar de uiterste waarden:

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%

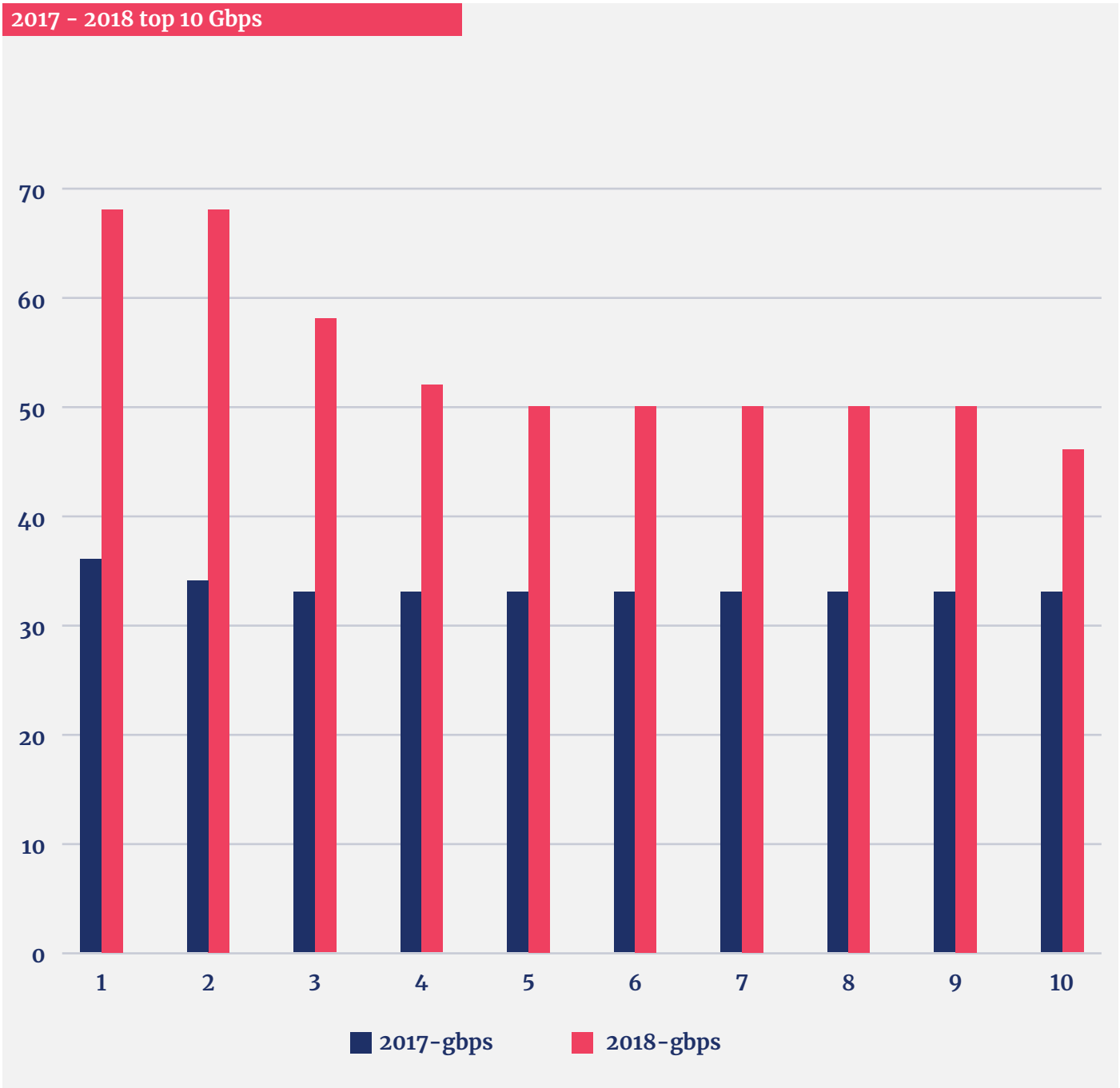
DDoS-aanvallen in 2018 werden dus zowel kleiner als groter in Gbps. Van een verschuiving naar de uitersten is vooralsnog geen sprake. Nog steeds is het gros van de aanvallen niet groter dan 10 Gbps.

De maximale grootte van een enkele DDoS-aanval lag in 2018 op 68 Gbps

De maximale grootte van een enkele DDoS-aanval lag in 2018 op 68 Gbps. In 2017 zagen we een maximale grootte van 36 Gbps. Het jaar daarvoor, in 2016, zagen we nog een enkele aanval van 53 Gbps voorbij komen, maar verder niets boven de 40 Gbps.

Hoe anders is dat in 2018, waar de top 10 bestaat uit alleen maar grotere aanvallen dan het jaar ervoor.

2017 - 2018 top 10 Gbps



4.3 Duur van een DDoS-aanval

Het gros van de aanvallen duurde niet langer dan een uur, net als in 2017.
Er waren 29 DDoS-aanvallen in 2018 die langer duurden dan 4 uur, tegen 28 in 2017.

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**

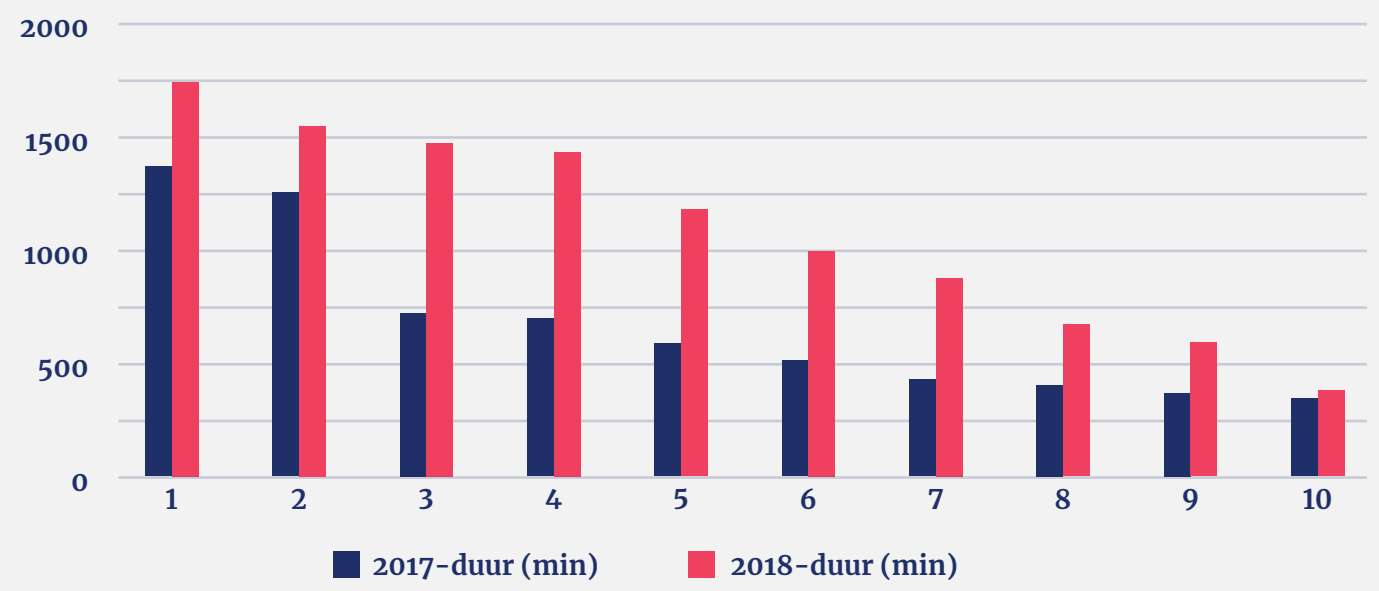
maanden	< 15 min	15-60 min	1-4 uur	> 4 uur	totaal
Jan-2018	40	37	20	2	99
Feb-2018	30	41	11	1	83
Mar-2018	44	47	20	2	113
Apr-2018	41	46	19	4	110
May-2018	20	39	9	2	70
Jun-2018	30	38	11	1	80
Jul-2018	15	26	11	4	56
Aug-2018	10	27	9	3	49
Sep-2018	19	44	15	1	79
Oct-2018	12	17	8	1	38
Nov-2018	32	43	17	4	96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

Ook qua duur waren er geen grote verschillen in de verdeling te zien, vergeleken met het jaar daarvoor. Wel neemt het aantal zeer korte aanvallen (minder dan 15 minuten) af, en nemen aanvallen iets langer dan een kwartier tot een uur juist toe.

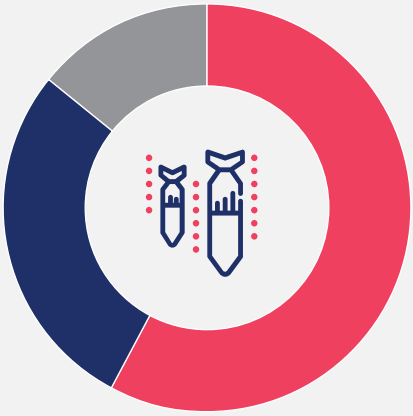
jaar	< 15 min	15-60 min	1-4 uur	> 4 uur
2017	37,4%	41,2%	18,3%	3,4%
2018	34,4%	45,9%	16,6%	3,1%

De maximale duur van een DDoS-aanval in 2018 was ruim een dag, deze duurde namelijk 29 uur. In 2017 was de maximale duur nog 23 uur. Meerdaagse aanvallen zijn sinds 2016 niet meer geconstateerd.

2017 - 2018 top 10 duur (min)

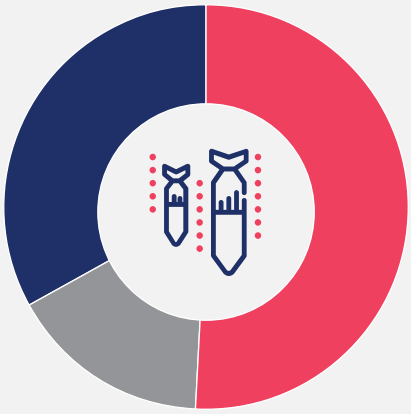


DDoS-type hoofdgroep verdeling 2017



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

DDoS-type hoofdgroep verdeling 2018



23% TCP flood
51% UDP amplification
16% UDP flood

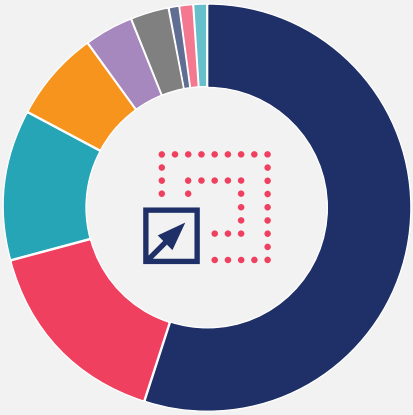
4.4 Soorten DDoS-aanvallen

In 2017 hebben we 46 soorten DDoS-aanvallen waargenomen. In 2018 is dit aantal gestegen naar 56 soorten aanvallen. We maken doorgaans onderscheid in drie hoofdgroepen DDoS-typen: TCP flood, UDP flood en UDP amplification.

Nog steeds bestaat meer dan de helft van de aanvallen uit UDP amplification, al daalde dat aantal wel flink met 7 procentpunt. De percentages van de rest van de aanvallen (TCP floods en UDP floods) zijn in 2018 dus gestegen.

In 2018 bestaat meer dan de helft van de aanvallen uit UDP amplification

UDP amplification DDoS-types 2017

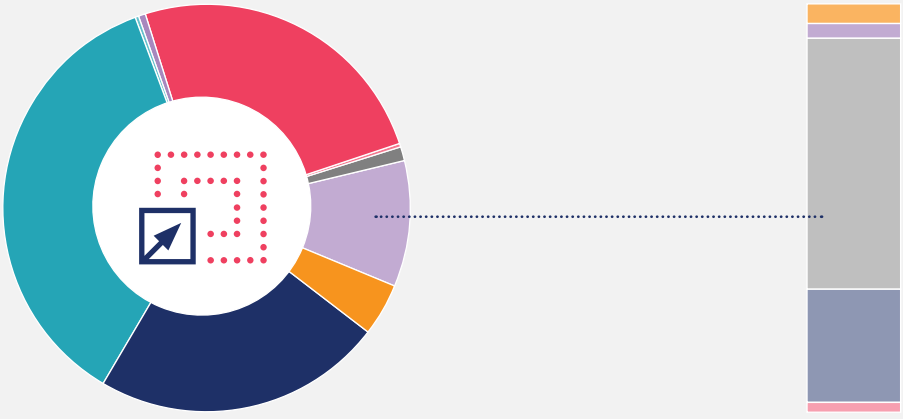


55%	DNS	3%	SSDP
16%	NTP	1%	RIPv1
12%	LDAP	1%	RPC port
7%	Chargen	1%	SNMP
4%	Netbios		

Binnen UDP amplification is er een grote verscheidenheid aan aanvallen, zoals te zien is in de grafieken op deze pagina.

In 2017 waren er 9 soorten UDP amplification te zien, in 2018 is dit aantal gestegen naar 11 soorten. Niet vreemd, gezien het aantal soorten over de hele linie is gestegen (van 46 naar 56). Binnen UDP amplification is LDAP amplification de DDoS-aanval die het meeste voorkomt met 36%.

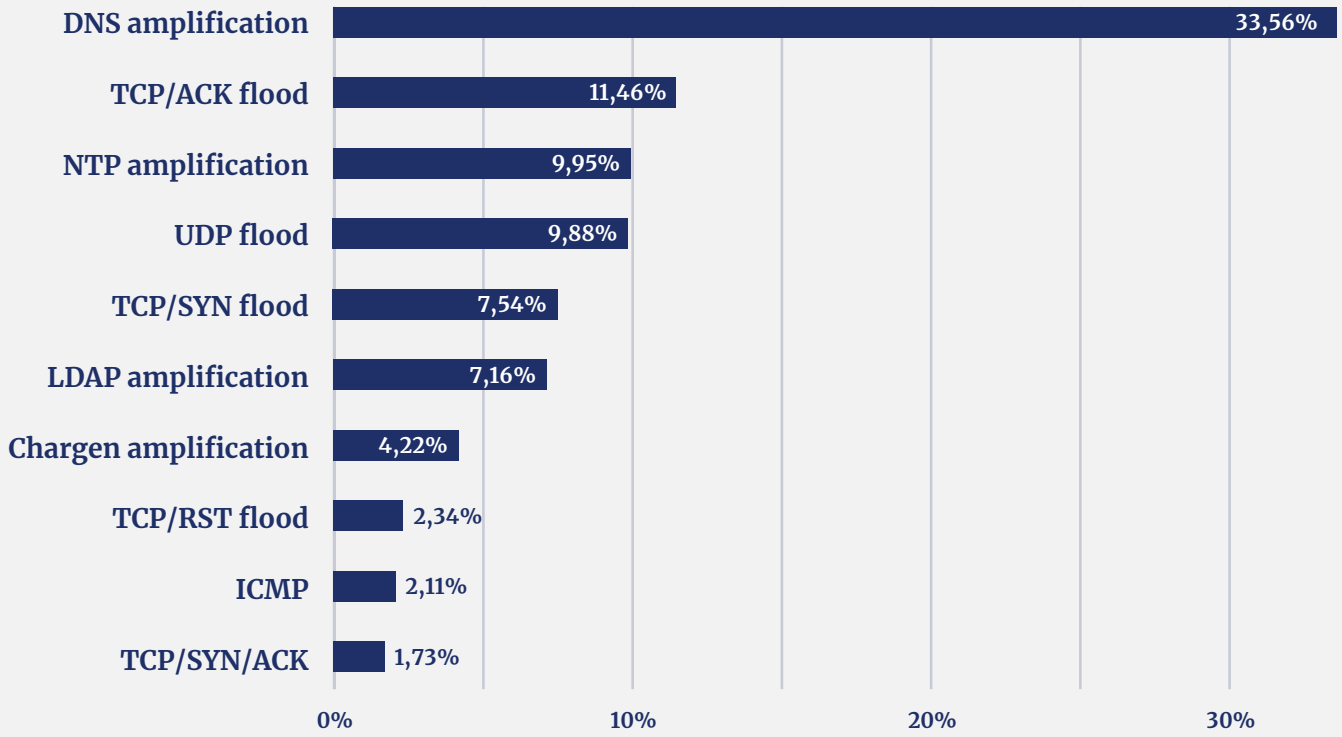
UDP amplification DDoS-types 2018



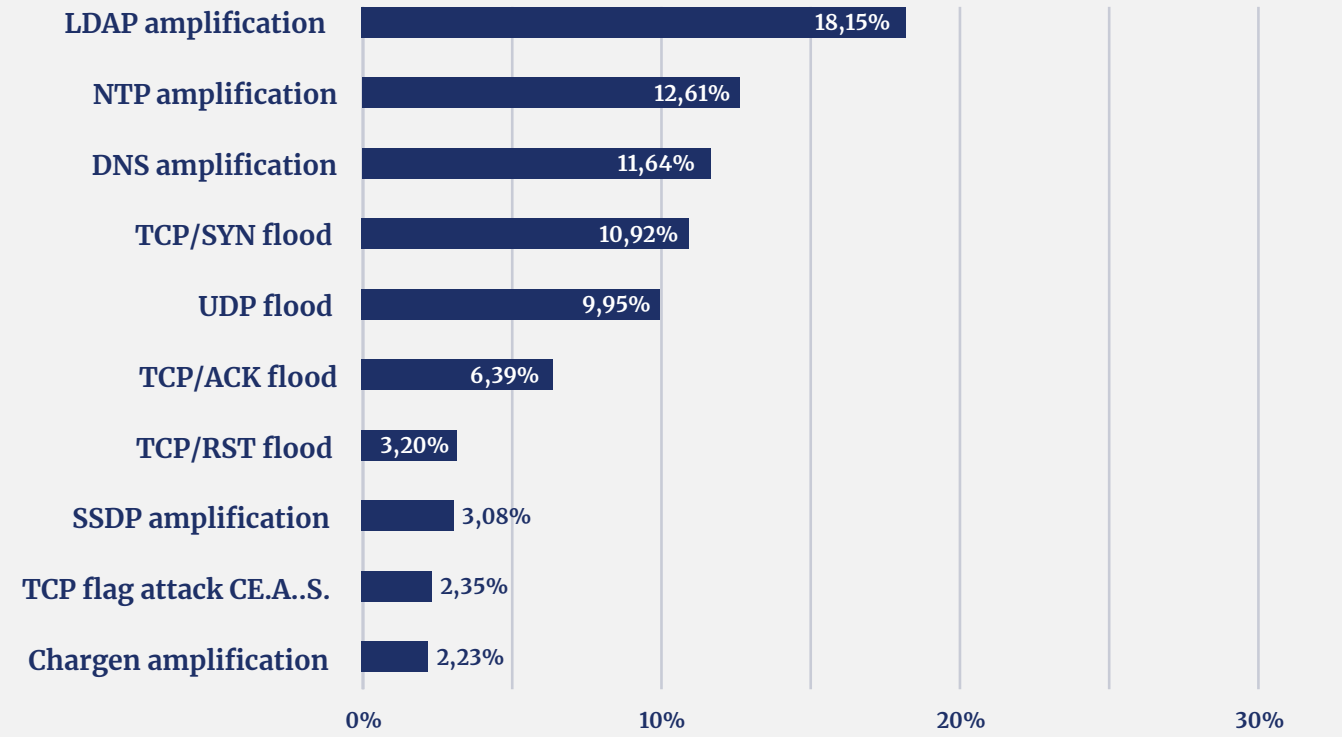
36%	LDAP	1%	RPC port	0,5%	UDP memcached
25%	NTP	0,5%	Netbios	0,4%	UDP flood
23%	DNS	0,4%	MS SQL monitor	6%	SSDP
10%	Overig	0,1%	RIPv1	3%	SNMP
4%	Chargen			0,1%	Sentinel

Dit betekent ook dat LDAP amplification DNS amplification van de troon heeft gestoten:

DDoS-type top 10 2017



DDoS-type top 10 2018



DNS amplification stond in 2017 nog fier aan kop met een aandeel van 33% in alle DDoS-aanvallen. In 2017 stond LDAP amplification zelfs nog op plaats 6.

Multivector-aanvallen, waarbij er meerdere aanvalsoorten bij elkaar worden verpakt, zijn nog immer aanwezig. Meestal is dit een 'simpel', zwaar aanvalstype met daarbij een klein, geavanceerd type aanval. De NBIP verwacht dat deze vorm van DDoS-aanval niet snel zal verdwijnen - integendeel, er is zelfs sprake van een trend (zie paragraaf 4.6).

4.5 Opvallende DDoS aanvallen

Naast de veelvoorkomende typen aanvallen hebben we ook enkele interessante en opvallende DDoS-aanvallen gezien in 2018.

STUN servers

Het viel op dat bij één van de deelnemers aan de NaWas opmerkelijk veel verschillende IP's contact maakten met een STUN server, dit gebeurde op onregelmatige tijden. Dit verkeer werd niet gefilterd door onze systemen maar maakte ons desalniettemin nieuwsgierig.

Na wat speurwerk van de deelnemer bleek dat de STUN server werd gebruikt door een cryptomunt om publieke IP adressen te valideren. Cryptomunten gebruiken doorgaans een aantal websites om dit te doen (showmyip.com bijvoorbeeld). In verband met privacy en decentralisatie worden open STUN servers hiervoor gebruikt. De verzoeken zijn op zichzelf legitiem.

Geoblocking

Bij één zeer kleine aanval met een zeer laag bps (bits per second) konden de standaard anti-DDoS maatregelen niet goed worden ingezet. Dit kwam doordat het onderscheid tussen DDoS en legitiem verkeer te klein was. Op dat moment is effectieve filtering toegepast op basis van geografische IP-blocking of geoblocking. Deze manier van mitigeren is efficiënt, maar niet subtiel, zoals we besproken hebben in hoofdstuk 2. Met geoblocking wordt het verkeer namelijk tegengehouden op basis van de (IP) locatie waarvandaan het gestuurd wordt. Soms is het dus noodzakelijk voor een wasstraat om deze manier van mitigatie in te zetten.

4.6 Nieuwe types DDoS-aanvallen

In 2018 zijn er bijna 40 DDoS-aanval types bij gekomen. Dit betreft echter in de meeste gevallen een bestaande aanval die een andere specifieke poort aanvalt. Filteren we deze aanvallen, dan was er sprake van een toename van 10 nieuwe typen DDoS-aanvallen.

> In 2018 zijn er bijna 40 DDoS-aanval types bijgekomen

De meest opvallende nieuwkomers ten opzichte van 2017:

MS SQL monitor amplification; 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 opduikt, 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'.

ESP flood is een aanval waarbij het UDP Encapsulating Security Payload protocol 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.

5. Trends

Ook hebben we enkele trends gespot buiten de geanalyseerde data.

Kleinere DDoS-aanvallen en memcached

Ondanks dat er enkele grote DDoS-aanvallen (> 40 Gbps) voorbij kwamen, was de tendens voornamelijk kleinere aanvallen (ook in pps, packets per second). We zagen dus kleinere hoeveelheden packets die er nét voor zorgden dat een webserver onderuit ging.

De aanval die met geoblocking opgelost moest worden, zoals besproken in paragraaf 4.5, is een vorm van zo'n zeer kleine aanval. Dit is een memcached-aanval, een trend die we vorig jaar ook al zagen opkomen maar die nu richting gemeengoed gaat.

Opvallend was ook dat enkele relatief kleine aanvallen, die normaliter door een webserver (farm) afgehandeld moeten kunnen worden, toch zorgden voor het verstoren van de webserver.

Multivector

Multivector-aanvallen blijven in aantal toenemen. Het maximaal aantal gelijktijdige type DDoS-aanvallen (multivector) van 2017 is in 2018 gelijk gebleven met 13 soorten. In 2018 waren 358 van 938 (38%) multivector-aanvallen. In 2017 was dit nog 262 van de 826 (31%).

DDoS-aanvallen wereldwijd

Onderzoek van Kaspersky Lab naar DDoS-aanvallen in 2018 laat zien dat het aantal aanvallen wereldwijd is gedaald met 13% - terwijl wij in Nederland juist een stijging van 13% hebben waargenomen.

> Wereldwijd daalde het aantal DDoS-aanvallen; in Nederland steeg het juist

Kaspersky Lab stelt dat dat vooral aan langere DDoS-aanvallen ligt.

Wij hebben dat in Nederland niet significant kunnen constateren. Een voorzichtige verklaring voor deze wereldwijde trend in 2018 is volgens ons dat er een flink aantal botnets uit de lucht zijn gehaald.

Ondanks dat DDoS-aanvallen door bedrijven serieuzer werden behandeld en cybercriminelen of verveelde jongeren door overheden strenger werden bestraft, is het aantal in Nederland dus niet gedaald. Wel was de groei minder, en vooral in de tweede helft van 2018 zette die groei niet door. Dat past in het plaatje dat er begin 2018 veel aandacht voor kwam, andere jongeren werden aangespoord om het ook eens te proberen, maar dat ze al gauw van een koude kermis thuis kwamen door goed ingrijpen. In ons eerste halfjaar rapport stelden we niet voor niets dat we over de duizend DDoS-aanvallen in 2018 zouden zien. Dat aantal is dus gelukkig niet gehaald.

6. Conclusie

Op basis van de onderzoeksresultaten trekt de NBIP vier conclusies, die we laten samenkomen in één overkoepelende conclusie over de staat van DDoS-aanvallen in Nederland.

Grote aanvallen (> 40Gbps) zijn terug, maar het grootste aantal van de aanvallen betreft nog steeds kleinere aanvallen. Dat grote aanvallen terug zijn is niet vreemd: het aantal aanvallen steeg, qua elke grootte en duur.

De tendens is nog steeds dat aanvallen nét groot genoeg 'gemaakt' zijn om disruptief te zijn. Het percentage aantal aanvallen onder de 1 Gbps steeg namelijk het hardst.

De duur van de langste aanval is iets gestegen. In 2017 was er geen enkele aanval over 24 uur, in 2018 waren er vier DDoS-aanvallen die langer dan een etmaal duurden. Hier is niet direct een verklaring voor te geven, anders dan dat deze langere aanvallen aan het begin van het jaar effectief bleken. Een aantal partijen had hun systemen niet op orde waardoor ze voor langere tijd "uitgeschakeld" konden worden.

Ook is er een nieuw soort DDoS-aanval het populairst onder cybercriminelen: LDAP amplification. In 2017 was DNS amplification het meest populair - en dat heeft mogelijk geleid tot actie bij bedrijven. "Open" DNS servers, die misbruikt worden voor een aanval, worden beter beveiligd. Al een aantal jaren wordt er door diverse partijen zoals NBIP en SIDN veel aandacht gegeven aan het beveiligen van de DNS-infrastructuur. Zo is hoogstwaarschijnlijk de "open" LDAP server boven komen drijven als een makkelijk doelwit.

> Het blijvend veranderen van DDoS-aanvallen laat zien dat de dreiging volwassen is

Vorig jaar stelden we nog dat DNS nog wel even aan kop zal blijven, omdat het de meest makkelijk uit te voeren DDoS-aanval is. Nu oude LDAP servers het grootste doelwit lijken te zijn, hopen we dat er ook voor het beveiligen van LDAP servers dezelfde aandacht komt als voor DNS servers.

Daarnaast stijgt het aantal en ook het percentage van multivector-aanvallen weer. De trend van complexe aanvallen zet door en dat maakt het verdedigen, ondanks alle aandacht voor DDoS-aanvallen, lastiger.

DDoS: een volwassen dreiging

De techniek van de DDoS-aanvallen verandert continu. Ze worden steeds kleiner, zijn net groot genoeg om te werken, en steken daarmee vaak professioneel in elkaar. Multivector-aanvallen zetten de trend van complexe aanvallen door. Dat samen maakt het verdedigen nog steeds erg moeilijk. Het blijvend veranderen van DDoS-aanvallen laat zien dat de dreiging volwassen is. Een volwassen dreiging dus die ironisch genoeg vaak niet van volwassen mensen komt. Gelukkig wordt er steeds meer strenger opgetreden. Een teken dat een DDoS-aanval eindelijk serieus genomen wordt.

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