Kwartaalupdate over DDoS-aanvallen: Q4 2020

Alles over de recente DDoS-aanvallen in 11 vragen en antwoorden.

Wat is er gebeurd in het vierde kwartaal van 2020?

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. Sinds de oprichting van NBIP hebben we in de laatste maanden van 2020 dagelijks meer aanvallen dan ooit geregistreerd.

Wat zijn de kenmerken van deze aanvallen?

Deze aanvallen waren buitengewoon krachtig (tot 167 Gbit per seconde) en duurden soms langer dan vier uur. De aanvallen zijn in te delen in vijf verschillende categorieën: DNS amplification (43%), LDAP amplification (26%), UDP flood (14%), NTP amplification (10%), TCP flood (7%).

Wat is carpet bombing?

Carpet bombing bestaat uit een groot aantal individuele aanvallen die tegelijkertijd worden uitgevoerd. In plaats van een bepaald IP-adres (doorgaans een /32) aan te vallen, richten de aanvallers zich op een geheel subnet met als gevolg dat honderden of duizenden bestemmingen in het netwerk datapakketjes ontvangen.

Staat uw vraag hier niet tussen?
In het geval uw vraag hier niet tussen staat, kunt u altijd via e-mail contact met de vakspecialisten van NBIP opnemen. We zijn van harte bereid om uw vragen te beantwoorden. Ook voor persvragen inzake alle DDoS-gerelateerde onderwerpen kunt u contact met ons opnemen.

bureau@nbip.nl
nbip.nl/en/nawas

Wat is LDAP amplication?

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".

Wat is 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 DNSveiligheidsextensie (DNSSEC) misbruiken om het bericht groter te maken.

Wat is 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.

Wat is NTP amplication?

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 één 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.

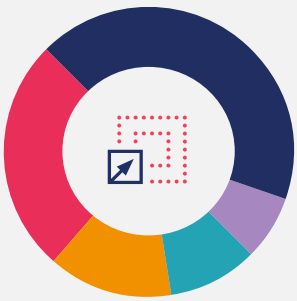
Wie zitten er achter deze DDoS-aanvallen?

Het is lastig om te bepalen wie precies de daders zijn. Het daderprofiel varieert van scriptkiddies tot landen die de boel willen ontregelen met een DDoS-aanval.

Wat zijn de motieven bij een DDoS-aanval?

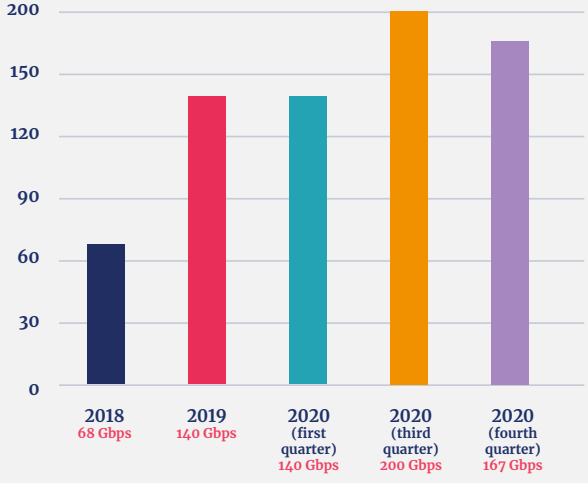
Aanvallers kunnen verschillende motieven hebben. Een DDoS-aanval kan bedoeld zijn om een bijvoorbeeld een website van een organisatie onbereikbaar te maken. In sommige gevallen organiseren jonge mensen een DDoS-aanval puur uit baldadigheid.

Types of DDoS Attacks



- 43% DNS amplification
- 26% LDAP amplification
- 17% UDP flood
- 14% NTP amplification
- 10% TCP flood

Maximum size of DDoS Attacks



Hoe kun je een DDoS-aanval afwenden?

Het afwenden van DDoS-aanval is door een individueel bedrijf vrijwel niet te doen. Voor het afslaan van een DDoS-aanval is een stevige infrastructuur vereist die veel geld kost. Door de bundeling van krachten en expertise biedt NBIP de NaWas waar internetserviceproviders een aansluiting op kunnen krijgen. De NaWas is in staat om 'goed' en 'fout' internetverkeer van elkaar te scheiden. Het gebeurt soms dat cybercriminelen bedrijven benaderen en zeggen dat ze tegen betaling zullen afzien van een DDoS-aanval. NBIP adviseert altijd om niet te betalen. Kiezen voor de NaWas van NBIP is een betere oplossing. In het geval uw bedrijf slachtoffer is van een DDoS-aanval, adviseert NBIP om altijd een melding bij de politie te doen. Als organisaties bij de NaWas zijn aangesloten, doet NBIP namens haar deelnemers een gezamenlijke melding.

Wat is NaWas?

De NaWas is een wasstraat waarmee een DDoSaanval kan worden afgeslagen. De NaWas is een initiatief van de NBIP. Deelnemers van de NBIP kunnen in het geval ze worden aangevallen, het verkeer laten omleiden via de NaWas, die het goede en foute internetverkeer filtert. De aangesloten deelnemer ontvangt alleen het schone verkeer. NaWas van NBIP is een non-profit community driven Scrubbing Center uit Nederland dat via AMS-IX, LINX en andere grote internet exchanges is aangesloten. NaWas is aanwezig op Amsterdam Internet Exchange (AMS-IX), NL-IX en DCspine en biedt meerdere manieren om ISP's in Europa met elkaar te verbinden.

Wie is de NBIP?

De Nationale Beheersorganisatie Internet Providers (NBIP) is een Nederlandse nonprofitorganisatie die ondersteunende diensten aan internetserviceproviders levert. NBIP levert momenteel een tweetal diensten aan internetserviceproviders vanuit een collectieve gedachte: de tapdienst, om wettelijke tapverplichtingen en -vorderingen uit te voeren, en de NaWas, een anti-DDos-dienst voor deelnemers. In de loop van 2021 zal de NBIP de dienst Clean Networks platform introduceren waarmee internetserviceproviders actief en realtime geïnformeerd worden over kwetsbaarheden of exploits in hun netwerk. Tegelijkertijd helpt de NBIP de internetserviceprovider om deze problemen in hun netwerken op te lossen.

	Q1	Q2	Q3	Q4
Amount of /24 prefixes	24.796	32.581	34.725	**34.915**
IP addresses	6.347.776	8.340.736	8.889.600	**8.938.240**
Number of attacks	409	354	307	**540**
Maximum size	140 gbps	75 gbps	200 gbps	**167 gbps**