DDoS-aanvallen: de stand van zaken in september 2020

Alles over de recente DDoS-aanvallen in 13 vragen en antwoorden

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/nawas

Wat is er recentelijk gebeurd?

Het afslaan van DDoS-aanvallen via de NaWas is voor NBIP dagelijkse kost, maar de aanvallen die in augustus en september hebben plaatsgevonden op de infrastructuren van internetserviceproviders waren van een hele andere orde. 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.

Wat waren de kenmerken van deze aanvallen?

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%).

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.

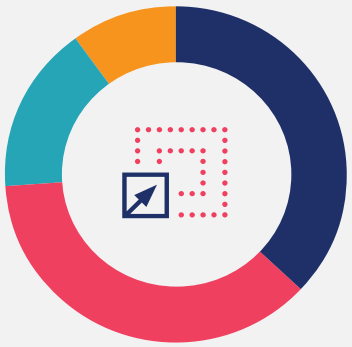
Wat is NTP amplication?

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.

Welke internetserviceproviders werden getroffen?

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.

DDoS-types



Zijn er ook internetserviceproviders buiten de Benelux getroffen?

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).

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.

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 DDoS-aanval 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 non-profitorganisatie 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.

DDoS-aanval - aantal per Gbps (top 20)