Beste klant,

Maandag 22 maart is TransIP getroffen door een grote DDoS-aanval gericht op onze gehele infrastructuur. Hierdoor waren jouw diensten en onze website 's middags verminderd bereikbaar.

In deze post mortem leggen we uit wat er gebeurd is tijdens deze aanval, welke maatregelen wij op dat moment hebben genomen om de impact te beperken (mitigeren) en welke maatregelen wij nemen om te voorkomen dat een dergelijke aanval in de toekomst een grote impact heeft.

Achtergrond

DDoS-aanvallen en de onderdelen van de TransIP-infrastructuur die daarbij betrokken waren, zijn technisch van aard. Kennis van bepaalde termen is noodzakelijk voor het volledig kunnen volgen van de gebeurtenissen tijdens de aanval. We lichten deze termen hieronder daarom graag eerst toe.

DDoS-aanval

DDoS staat voor Distributed Denial of Service en heeft als doel het verkeer van en naar servers, computers, of netwerken onmogelijk te maken. Hiervoor wordt gebruikgemaakt van een netwerk van geïnfecteerde/kwetsbare apparaten van derden. Deze apparaten sturen een overweldigende hoeveelheid internetverkeer naar het doelwit.

Het gevolg is dat de aangevallen dienst (bijvoorbeeld een website) zeer traag gaat werken, gedeeltelijk of geheel onbereikbaar wordt. In theorie kan een DDoS-aanval zodanig opgeschaald worden dat, ongeacht de netwerkcapaciteit van de verdedigende partij, dit doel bereikt wordt.

Er zijn verschillende technieken die gebruikt kunnen worden voor een DDoS-aanval. De aanval van afgelopen maandag was dusdanig groot dat we daarbij iedere techniek wel voorbij hebben zien komen.

DDoS-scrubbing

‘Scrubbing’ is een veelgebruikte techniek om tegen DDoS-aanvallen te beschermen. Netwerkverkeer wordt ‘gescrubbed’ (schoongemaakt): DDoS-verkeer wordt tegengehouden en alleen legitiem verkeer wordt doorgelaten. Een provider kan zelf dit scrubbingproces uitvoeren, of verkeer kan naar een specialistische partij worden omgeleid. Vaak kan een dergelijke partij nog veel grotere hoeveelheden dataverkeer aan dan de provider zelf.

Het voordeel van scrubbing is dat legitiem verkeer in principe geen hinder ondervindt van de DDoS-aanval, tenzij de hoeveelheid verkeer groter is dan het netwerk van de scrubbende partij kan verwerken.

Een nadeel bij het gebruik van een externe partij voor het scrubben, is dat om technische redenen ook een stukje legitiem netwerkverkeer wordt tegengehouden. Hoewel zeer effectief bij grote aanvallen, is het scrubben via een externe partij alsof je met een geweer op een mug schiet. Als de aanval niet te groot is, heeft het daarom de voorkeur om zelf te scrubben: daarbij speelt dit nadeel niet.

Blackholing

DDoS blackhole routing, oftewel blackholing, is een techniek waarbij netwerkverkeer naar een ‘black hole’ wordt gestuurd. Al het verkeer naar een IP-adres, goed en slecht, wordt naar de black hole geleid en daar ‘gedropt’ (al het netwerkveer verdwijnt).

Het voordeel is dat de netwerkbelasting van de aanval verdwijnt. Dit geeft ook engineers de ademruimte om aanpassingen te maken om de aanval verder te bestrijden. Daarnaast zal een aanvaller ook merken dat zijn verkeer in een black hole verdwijnt. Grote DDoS-aanvallen zijn kostbaar en meestal is een black hole dan ook genoeg reden voor een aanvaller om binnen een paar minuten te stoppen met aanvallen. Het nadeel is dat ook legitiem verkeer hiermee tijdelijk wordt tegengehouden.

DNS

Domeinnamen maken gebruik van DNS, wat staat voor Domain Name System. Voor je domeinnaam kun je zogenaamde DNS-records instellen. DNS-records vertellen systemen, bijvoorbeeld je internetbrowser en e-mailprogramma, op welke servers diensten zoals de website en e-mail van jouw domeinnaam gehost staan.

Nameserver

De DNS-records van je domeinnaam worden in nameservers opgeslagen. Zodra je bijvoorbeeld een domeinnaam in de adresbalk van je browser invoert, wordt er een verzoek gedaan naar de nameservers die voor het domein zijn ingesteld. De nameservers geven vervolgens, door te kijken naar de DNS-records, aan op welke server de bijbehorende website staat. Nameservers zijn een soort telefoonboek van het internet.

Packet loss

Netwerkverkeer wordt in kleine stukjes data oftewel ‘packets’ gesplitst. Wanneer een of meer packets niet bij de bestemming aankomen spreek je over packet loss. Je ervaart dit als een trage verbinding, een gehele of gedeeltelijke onderbreking van je verbinding naar onze website en diensten die bij TransIP gehost worden.

Tijdlijn van de DDoS-aanval

13:30: Op dit tijdstip ontvangen onze engineers een melding van een DDoS-aanval. Het is al snel duidelijk dat deze gericht is op onze nameservers, en dat de aanval vrij fors is. Onze DDoS-bescherming kan middels scrubbing het verkeer opschonen waardoor de impact minimaal is.

We krijgen gelijktijdig melding dat mensen die gebruikmaken van internet via Ziggo onze website en domeinen die onze nameservers gebruiken niet kunnen bereiken. We starten direct een onderzoek naar de oorzaak hiervan.

14:00: Het volume van de aanval neemt af, maar de problemen van mensen die gebruikmaken van een Ziggo-verbinding houden aan. In een poging deze te verhelpen, zetten we onze automatische scrubbing uit. Dit lost echter de problemen niet op.

14:30: We komen erachter dat het probleem met de Ziggo-verbindingen veroorzaakt wordt door blackholing van de IP-adressen van onze nameservers door een van onze internetproviders, die voornamelijk verkeer van Ziggo-verbindingen naar TransIP verwerkt.

Het gevolg daarvan is dat iedereen die gebruikmaakt van een Ziggo-verbinding onze website, en domeinen die gebruikmaken van onze nameservers niet kunnen bereiken. Onze engineers nemen contact op met de betreffende provider en de black hole van onze nameservers wordt ongedaan gemaakt. We zetten de automatische scrubbing weer aan, omdat DDoS-verkeer anders onbelemmerd doorkomt.

Een tweede, aanzienlijk zwaardere aanval begint gelijktijdig. Dit is een bredere aanval, niet alleen gericht op onze nameservers maar ook op andere delen van onze infrastructuur. De hoeveelheid verkeer tijdens deze aanval is groter dan ons netwerk kan verwerken. Het gevolg hiervan is dat nu iedereen die verbinding maakt naar diensten die bij TransIP gehost worden problemen ervaart in de vorm van packet loss.

16:20: Onze engineers hebben het internetverkeer van enkele van onze providers tijdelijk uitgeschakeld: een groot deel van het DDoS-verkeer blijkt namelijk vooral via de verbindingen van enkele van onze providers te verlopen. Door deze providers tijdelijk uit te schakelen, vangen we een zeer groot deel van het DDoS-verkeer af. Legitiem verkeer dat via deze providers verloopt, wordt hiermee ook tijdelijk tegengehouden.

Daarnaast blackholen we diverse van onze eigen IP-adressen die aangevallen worden maar geen cruciale taak vervullen op dat moment. Het doel hiervan is om de aanvallers te laten zien dat het DDoS-verkeer nergens meer naartoe gaat. Dit is bij bijna alle DDoS-aanvallen voldoende motivatie om de aanval te stoppen en al na enkele minuten zien we dat dat ook hier het geval is: de DDoS-aanval neemt af en onze diensten worden weer bereikbaar.

17:45: De situatie is nu geruime tijd stabiel. We houden de situatie de rest van de avond en nacht nauwlettend in de gaten.

Conclusies en maatregelen

Allereerst vinden wij het heel vervelend dat je als gevolg van deze DDoS-aanval overlast hebt ervaren. De eerste aanval was in eerste instantie gericht op onze nameservers en de tweede daarnaast ook op onze interne infrastructuur. De impact van deze aanvallen was echter veel groter: een groot deel van de domeinen die gebruikmaken van onze nameservers waren getroffen door deze aanval. De oorzaak hiervan zit hem in twee punten:

- Tijdens de eerste aanval waren onze nameservers onbereikbaar voor mensen met een Ziggo-verbinding. Dit komt doordat een van onze providers een black hole had ingesteld voor de IP-adressen van onze nameservers. Deze provider verwerkt hoofdzakelijk Ziggo-verbindingen naar ons netwerk. Dat de impact daarvan zo groot bleek, is het gevolg van hoe DNS-systemen werken:
  Domeinen maken gebruik van DNS-records om aan te geven op welke server(s) een domein

staat gehost, bijvoorbeeld voor de website en e-mail van dat domein.
Een belangrijk onderdeel van DNS-records, is de zogeheten 'TTL', oftewel de Time To Live. De TTL geeft aan hoe lang het duurt voor DNS-records verlopen. Nadat DNS-records verlopen, worden die opnieuw opgevraagd bij de nameservers die voor dat domein zijn ingesteld. Als nameservers onbereikbaar worden, zoals in dit geval door het blackholen van onze IP-adressen en later door de omvang van de DDoS-aanval, kunnen die DNS-records niet opgevraagd worden. Het gevolg daarvan is dat bijvoorbeeld je computer niet weet met welke server die moet verbinden wanneer je een website bezoekt waarvan het domein onze nameservers gebruikt.

- De tweede aanval was dusdanig groot dat ons eigen netwerk de hoeveelheid verkeer niet meer aan kon en er aanzienlijke packet loss optrad. Hierdoor kon je ook hinder ondervinden bij het gebruiken van diensten die op servers van TransIP gehost worden, zonder dat die servers het primaire doel van de aanval waren.

Op basis van deze conclusies, nemen we een aantal maatregelen om de impact van een grote DDoS-aanval in de toekomst drastisch te beperken of zelfs te voorkomen.

- We sluiten een contract met een partij die gespecialiseerd is in scrubbing. Bij DDoS-aanvallen waar ons eigen netwerk de hoeveelheid verkeer niet meer aankan, wordt netwerkverkeer via deze partij omgeleid en opgeschoond.
- De provider die een black hole voor onze nameservers had ingesteld, heeft de IP-adressen van onze nameservers aan een whitelist toegevoegd, waardoor dit niet meer zal voorkomen.
- Er komen meerdere fysieke en logische scheidingen in onze nameserver-setup. Dit maakt onze nameservers beter bestand tegen gerichte DDoS-aanvallen.
- We onderzoeken of we met een aanpassing van de TTL van zowel onze domeinen als die van onze klanten, voor zover het DNS-beheer daarvan automatisch via ons verloopt, de impact van dit soort aanvallen kunnen beperken.

Daarnaast onderzoeken we nog enkele aanvullende opties om verschillende aspecten van onze infrastructuur beter bestand tegen DDoS-aanvallen te maken.

Tot slot bieden we onze excuses aan dat wij je niet tijdig over deze DDoS-aanval per e-mail konden informeren. Het mailen van al onze klanten neemt zeer veel tijd in beslag (langer dan deze aanval duurde). Hierom maken we gebruik van de pagina https://transnoc.nl die gescheiden is van ons eigen netwerk. Bij problemen met ons netwerk kunnen wij je daardoor alsnog informeren over de status daarvan.

Mocht je naar aanleiding van deze post mortem nog vragen hebben, aarzel dan niet om contact met ons op te nemen via een bericht vanuit je TransIP-controlepaneel.

Met vriendelijke groet,

TransIP B.V.