Een proactieve en collectieve DDoS-bestrijdingsstrategie voor de Nederlandse vitale infrastructuur

Cristian Hesselman[1], Jeroen van der Ham[2], Roland van Rijswijk[3], Jair Santanna[2], Aiko Pras[2]
[1]SIDN, Arnhem
[2]Universiteit Twente, Enschede
[3]SURFnet, Utrecht
Contactpersoon: cristian.hesselman@sidn.nl

4 april 2018

Banken en overheidsinstellingen hadden de afgelopen maanden regelmatig last van storingen door relatief kleine DDoS-aanvallen. Dit is zorgwekkend, want deze aanvallen worden alleen maar groter en complexer, bijvoorbeeld door het opkomende 'internet of things'. Wij pleiten daarom voor een proactieve en collectieve DDoS-bestrijdingsstrategie voor de Nederlandse vitale infrastructuur. Hierbij verzamelen vitale aanbieders voortdurend informatie over potentiële en actieve DDoS-bronnen en delen deze geautomatiseerd met andere aanbieders als onderdeel van een nog te ontwikkelen systeem, de 'nationale DDoS-radar'.

Internet in 2018: onmisbaar, maar kwetsbaar

Het internet heeft ons dagelijks leven enorm vergemakkelijkt en verrijkt en is er een onmisbaar onderdeel van geworden. Steeds meer diensten die we gebruiken zijn afhankelijk van het internet, waaronder diensten die de overheid tot 'vitaal' heeft verklaard, omdat hun "uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid". Voorbeelden zijn elektronisch betalen, internettoegang, energievoorziening en hulpdiensten.

Helaas maakt het internet vitale diensten ook kwetsbaar voor verstoringen als gevolg van DDoS-aanvallen op de aanbieders van die diensten, zoals ISP's, banken, overheden en DNS-beheerders. Zij moeten steeds grotere aanvallen opvangen, die inmiddels op het niveau van terabits per seconde hebben bereikt. Zo kregen Github en Dyn beide te maken met aanvallen van meer dan 1 terabit per seconde, twee orde van groottes meer dan de aanvallen op de banken en overheden eerder dit jaar (geschat op 40 gigabit per seconde) en vier orde van groottes meer dan de aanvallen op Estland in 2007 (geschat op 90 megabit per seconde). Daarnaast worden DDoS-aanvallen steeds complexer, omdat ze van steeds meer soorten bronnen afkomen die overal ter wereld kunnen staan en meerdere doelen tegelijk kunnen treffen. Voorbeelden van DDoS-bronnen zijn onveilige apparaten in het 'Internet of Things' (IoT), open 'memcached' servers, of 'booter-sites' die DDoS-aanvallen voor enkele tientjes aanbieden.

Reactief en individueel optreden is onvoldoende

Onze positie is dat de Nederlandse vitale infrastructuur op dit moment onvoldoende in staat is om steeds grotere en complexere DDoS-aanvallen duurzaam het hoofd te bieden. Dit komt omdat vitale aanbieders vooral reactief DDoS-aanvallen bestrijden, meestal door het DDoS-verkeer dat ze te verwerken krijgen door te sturen naar een commercieel DDoS-verwerkingsbedrijf dat het legitieme verkeer scheidt van het aanvalsverkeer. Daarnaast

werken vitale aanbieders vaak individueel en hebben ze geen actueel inzicht in DDoS-aanvallen bij andere vitale aanbieders. Deze reactieve en individuele strategie vergroot de kans dat aanbieders onvoldoende voorbereid zijn op een aanval en dat er daardoor een verstoring van hun dienstverlening optreedt. Daarnaast hebben commerciële DDoS-verwerkingsbedrijven er een financieel belang bij dit model te handhaven, wat betekent dat een verandering van de vitale aanbieders zelf zal moeten komen.

Naar een proactieve en collectieve strategie

Wij stellen daarom voor dat de Nederlandse vitale infrastructuur een *proactieve en collectieve* DDoS-bestrijdingsstrategie introduceert op basis van de 'nationale DDoS-radar', een nog te ontwikkelen systeem dat voortdurend 'fingerprints' maakt van potentiële en actieve DDoS-bronnen en die automatisch deelt met aangesloten vitale aanbieders. De fingerprints representeren bijvoorbeeld de internetadressen van DDoS-bronnen, identifiers van de netwerken waar ze staan en gedetailleerde verkeerspatronen van het DDoS-verkeer dat ze genereren. De DDoS-radar maakt fingerprints op basis van sensoren van vitale aanbieders, zoals DDoS-logs, 'crawlers' die het internet afzoeken naar booter-sites, en 'honeypots' die besmette IoT-apparaten aantrekken en in kaart brengen.

De DDoS-radar maakt een proactieve aanpak van DDoS-aanvallen mogelijk, omdat de fingerprints vitale aanbieders meer inzicht geven in potentiele DDoS aanvallen. Dit stelt hen in staat sneller DDoS-bronnen te herkennen en te filteren, wat de kans op een verstoring van hun dienstverlening verlaagt. Daarnaast stelt het collectieve karakter van de DDoS-radar vitale bieders in staat hun blikveld te verbreden van alleen hun eigen DDoS-sensoren en netwerkverkeer naar de hele Nederlandse vitale infrastructuur. Een bank kan via de DDoS-radar bijvoorbeeld meteen de fingerprints delen van een verzameling Mirai-DDoS-bronnen waar het mee te maken heeft, waarna de ISP's waar zich de met Mirai besmette IoT-devices bevinden contact opnemen met hun klanten om de besmetting ongedaan te maken. Overige aanbieders gebruiken deze informatie om hun detectiesystemen en filters in te stellen op een mogelijke aanval. Een ander voorbeeld is dat een vitale aanbieder die via de DDoS-radar informatie deelt over een booter-site die het heeft gevonden in het .nl-domein, waarna SIDN samen met hosting providers die informatie gebruiken om de site offline te halen.

Bij extreem grote en gedistribueerde aanvallen helpt de DDoS-radar ook om gezamenlijk te besluiten 'Nederlandse' netwerken in stappen en tijdelijk van het mondiale internet los te koppelen en deze beslissing in samenwerking met de partijen achter het voormalige Trusted Network Initiative en de Dutch Continuity Board te realiseren.

De DDoS-radar draagt verder bij aan het verzamelen van meer data over daders (attributie), zodat de overheid hen beter en sneller kan opsporen en vervolgen. Dit ontmoedigt potentiële nieuwe aanvallen op de Nederlandse vitale infrastructuur.

Anti-DDoS-manifest

Wij stellen voor de DDoS-bestrijdingsstrategie vast te leggen in een anti-DDoS-manifest, waarin deelnemende vitale aanbieders verklaren dat ze voortdurend informatie over DDoS-bronnen verzamelen en die delen als onderdeel van de nationale DDoS-radar.

Netwerkbeheerders gebruiken de constructie van een manifest om het routeren van internetverkeer veiliger te maken.

In het anti-DDoS-manifest staan ook operationele afspraken, zoals welke soorten informatie aanbieders via de DDoS-radar delen, hoe ontvangers die gegevens dienen te gebruiken, hoe er wordt samengewerkt met opsporingsinstanties en welke berichtenformaten de DDoS-radar ondersteunt (bijv. IODEF). Ook het gebruik van 'best practice' anti-DDoS-maatregelen hoort daarbij, zoals BCP38.

Borging
We stellen voor het manifest te verankeren in een nationale anti-DDoS-organisatie die het manifest opstelt, beheert en zorgt voor de naleving ervan. Deze organisatie heeft daarvoor het mandaat van een breed scala aan vitale aanbieders nodig, zoals ISP's, mobiele operators, internet exchanges, hostingproviders, banken, DNS-operators en overheidsinstellingen.

De anti-DDoS-organisatie kan bestaan uit een klein bestuur van onafhankelijke experts ondersteund door mensen uit operationele securitycommunities. Zij kijken ook samen naar nieuwe DDoS-ontwikkelingen om zo toekomstige grotere of andere aanvallen het hoofd te kunnen blijven bieden. Ook de wetenschappelijke onderzoekgemeenschap zal hierbij een actieve rol moeten spelen.

Een belangrijke voorwaarde is dat de anti-DDoS-organisatie zo transparant mogelijk werkt door het manifest te publiceren en zo open mogelijk te communiceren over aangesloten aanbieders, details van aanvallen en genomen anti-DDoS-acties te delen. Dit vergroot het vertrouwen van burgers, bedrijven en de politiek dat vitale aanbieders het probleem van DDoS-aanvallen zelf aankunnen.

Hoe verder?
Onze oproep is dat de partners uit het Trusted Networks Initiative, de leden van de Dutch Continuity Board, de NAWAS, banken, de wetenschap en de overheid met elkaar om de tafel gaan om te spreken over de haalbaarheid van het anti-DDoS-manifest en zo de weg te openen naar een proactief en collectief niveau van DDoS-weerbaarheid voor de Nederlandse vitale infrastructuur en onze online samenleving.

Bio's
Cristian Hesselman werkt bij SIDN, de beheerder van het nationale top-level-domein van Nederland, .nl. Hij leidt SIDN Labs, het researchteam van SIDN.

Jeroen van der Ham is gastonderzoeker bij de Universiteit Twente. Hij is assistant professor op het gebied van Internet security en ethiek in de groep 'Design and Analysis of Communication Systems' (DACS).

Roland van Rijswijk werkt bij SURFnet, de beheerder van het nationale onderzoeks- en onderwijsnetwerk in de rol van Innovator Internet Security.

Jair Santanna werkt bij de Universiteit Twente. Hij is assistant professor op het gebied van Internet security in de groep 'Design and Analysis of Communication Systems' (DACS).

Aiko Pras werkt bij de Universiteit Twente. Hij is professor op het gebied van Internet security in de groep 'Design and Analysis of Communication Systems' (DACS).

== EINDE