Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

DNS-amplificatie

Laat uw deur niet wagenwijd openstaan

Factsheet FS-2013-03
versie 1.0 | 4 oktober 2013

DNS-amplificatie blijft een populaire methode om (distributed) denial-of-service ((D)DoS)-aanvallen uit te voeren. Aanvallers maken misbruik van openstaande DNS-resolvers op het internet, waarmee zij hun doelwit bestoken met grote hoeveelheden dataverkeer. De eigenaren van die openstaande DNS-resolvers zijn daardoor onbedoeld en vaak ook ongemerkt betrokken bij deze aanvallen. Dit probleem speelt wereldwijd, maar het grote aantal internetaansluitingen in Nederland gaat gepaard met een groot aantal open DNS-resolvers. Dit betekent dat ook als de aanvaller en het uiteindelijke slachtoffer van de (D)DoS-aanval zich in andere landen bevinden, deze aanvallen alsnog kunnen plaatsvinden via Nederlandse infrastructuur.

De oplossing lijkt eenvoudig; eigenaren van kwetsbare DNS-systemen kunnen deze systemen met weinig moeite beveiligen tegen deze vorm van misbruik. Toch staat er een aanzienlijke hoeveelheid DNS-servers in Nederland open. Misschien ook die van u. In dit factsheet leest u wat DNS-amplificatie is, waar u het aan herkent en wat u daartegen kunt doen.

De belangrijkste feiten

- DNS-amplificatie blijft een populaire methode om (distributed) denial-of-service ((D)DoS)-aanvallen uit te voeren.
- Aanvallers maken misbruik van openstaande DNS-resolvers op het internet, waarmee zij hun doelwit bestoken met grote hoeveelheden dataverkeer.
- Netwerkbeheerders (maar ook eindgebruikers) kunnen controleren of er sprake is van een open DNS-resolver.
- Het NCSC adviseert om te zorgen dat uw DNS-resolvers niet misbruikt kunnen worden voor het uitvoeren van aanvallen met DNS-amplificatie.

Wat is DNS-amplificatie?

Bij een (D)DoS-aanval wordt een systeem of netwerk van het slachtoffer (tijdelijk) onbeschikbaar gemaakt door het te overbelasten met een grote hoeveelheid dataverkeer.[1] Een aanvaller zou deze grote hoeveelheid dataverkeer zelf kunnen uitsturen naar het slachtoffer, wat een grote capaciteit van zijn eigen netwerk/systeem zou vereisen. Een betere mogelijkheid is dat hij de overbelasting veroorzaakt via een of meerdere servers van derden. Door dit slim te doen, kan een grote versterking (amplificatie) worden bereikt van het uitgestuurde verkeer dat naar het slachtoffer wordt gestuurd. Een voorbeeld van een dergelijke aanval is DNS-amplificatie. Hierbij worden een of meerdere 'onschuldige' DNS-servers misbruikt om verkeer dat naar een slachtoffer wordt gestuurd te versterken.

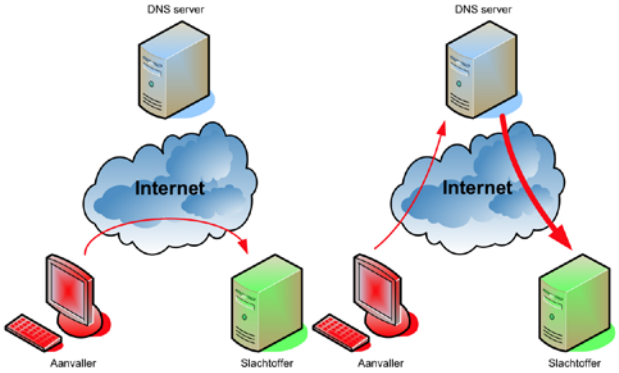
DNS staat voor Domain Name System. Dit 'systeem' vormt een essentieel onderdeel van het internet, omdat deze de vertaling doet van de domeinnaam in een URL naar een IP-adres. Wanneer bijvoorbeeld in een browser www.example.nl wordt ingetypt, wordt dit door een DNS-server vertaald naar het IP-adres dat nodig is om datapakketten over het internet te routeren. Overigens is het met DNS niet alleen mogelijk om het IP-adres dat bij een domeinnaam hoort op te vragen. Ook andere informatie kan worden opgevraagd met een DNS-verzoek, bijvoorbeeld wat de mailservers zijn die bij een domein horen of digitale handtekeningen die de authenticiteit van het domein garanderen.

Bij DNS-amplificatie maken aanvallers handig gebruik van het feit dat een DNS-antwoord vaak groter is dan een DNS-verzoek. Soms maken de aanvallers misbruik van domeinnamen die uit zichzelf grote antwoorden geven, bijvoorbeeld omdat ze beveiligd zijn met DNSSEC en digitale handtekeningen moeten meesturen met het antwoord. Er is dus sprake van een versterkingsfactor. Omdat de grootte van het verzoek klein is en het antwoord relatief groot kan

1 Voor meer informatie over (D)DoS-aanvallen, zie het factsheet Continuïteit van onlinediensten van het NCSC.

zijn, is een versterkingsfactor van meer dan 50 niet ongebruikelijk. Een groot aantal van de DNS-servers op internet staan, soms zonder dat beheerders zich daar bewust van zijn, open voor dergelijke verzoeken.

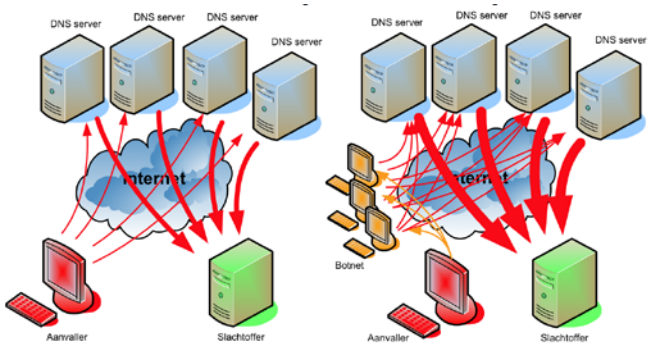
100 Mb/s kan worden versterkt tot 5 Gb/s. Als een aanvaller een botnet van 100 pc's gebruikt die elk een bandbreedte van 1 Mb/s hebben, is dat voldoende om een bedrijfswebsite uit de lucht te halen.



DoS-aanval zonder (links) en met (rechts) amplificatie.

Om de pakketten vanuit de DNS-server bij het slachtoffer aan te laten komen, is het noodzakelijk dat de aanvaller in de IP-pakketten het bronadres aanpast naar het adres van het slachtoffer. Dit wordt ook wel 'IP spoofing' genoemd (zie kader). Hierdoor wordt het mogelijk om de antwoorden van de DNS-server naar het slachtoffer sturen.

Door veel verzoeken, met een gespooft IP-bronadres, naar een of meerdere servers te sturen wordt uiteindelijk een grote datastroom richting het slachtoffer verkregen. Het gevolg daarvan is dat een systeem, of zelfs het netwerk van het slachtoffer overbelast kan raken. Aanvullend kan een aanvaller een botnet gebruiken om de DNS-verzoeken te versturen naar de DNS-servers om zo de hoeveelheid verkeer richting een slachtoffer te vergroten.



DDoS-aanval met amplificatie (links) en amplificatie met botnet (rechts).

Wie zijn de aanvallers?

Een (D)DoS-aanval wordt regelmatig gebruikt als aanvals(hulp) middel door de volgende actoren[2]:

- Hacktivisten
- Criminele organisaties
- Statelijke actoren
- Scriptkiddies

IP-spoofing

- IP-pakketten, de datapakketten op het internet, bevatten een bronadres, waar het IP-pakket vandaan komt en een doeladres, waar het IP-pakket naar toe gestuurd wordt.
- Bij IP-spoofing vervangt een aanvaller het bronadres, zijn eigen IP-adres, door een ander adres. Dit doet hij bijvoorbeeld om moeilijker traceerbaar te zijn of omdat het een essentieel onderdeel van een aanval vormt.
- Bij DNS-amplificatie is IP-spoofing noodzakelijk om de DNS-server te laten denken dat verzoeken niet van de aanvaller afkomstig zijn, maar van het slachtoffer. De (grote) antwoorden op de verzoeken worden door de DNS-server dus gericht aan het slachtoffer.

Bij het uitvoeren van een (D)DoS-aanval kunnen zij van tijd tot tijd omschakelen tussen verschillende aanvalstechnieken, waarbij DNS-amplificatie een veelgemaakte keuze is.

Afhankelijk van de intentie die deze aanvallers hebben spelen de volgende motieven een rol:

- Geldelijke en/of materiële motieven.
- Ideologische motieven en angst zaaien.
- Politieke, statelijke motieven en/of cyber offense.
- Wraak en/of vergelding.
- Kijken of iets kan, voor de lol.
- Afleiding, verhullen en/of ontduiken.[3]
- Het testen van botnets.[4]

2 Meer informatie over actoren is te vinden in andere publicaties van het NCSC, onder andere het factsheet Continuïteit van onlinediensten en het Cybersecuritybeeld Nederland 3.

3 Een (D)DoS die specifiek een andere operatie verhult of zorgt dat de aanvaller onder verplichtingen uit kan komen (bijvoorbeeld studenten die onder een examen proberen uit te komen)

4 Er zijn botnets te huur voor onder andere het uitvoeren van DDoS. Een beheerder van een botnet test regelmatig zijn 'dienstverlening'.

Wie zijn het slachtoffer?

Een (D)DoS-aanval met behulp van DNS-amplificatie kent twee (groepen) slachtoffers. Aan de ene kant het beoogde doelwit; aan de andere kant de tussenpartij die de DNS-server in beheer heeft. Beide partijen zien dat door het versterkte dataverkeer uiteindelijk de continuïteit van zijn of haar dienstverlening in gevaar komt.

De tussenpartij hoeft dit niet eens in de gaten te hebben. De aanvaller is er per slot van rekening niet op uit om daar diensten te verstoren, maar heeft er juist belang bij dat hij zelf ongestoord kan doorgaan. Om die reden hoeft deze partij niet zozeer gedupeerd te worden. Toch is er sprake van slachtofferschap. Niet alleen vanwege enig materieel ongemak zoals verhoogd data- en energieverbruik, maar ook bestaat er een kans op imagoschade. Immers, het versterkte verkeer is van de tussenpartij afkomstig en die wordt daar op aangekeken. Kwetsbaar zijn voor DNS-amplificatie wordt gezien als het niet op orde hebben van de eigen infrastructuur, en het niet oplossen ervan kan gezien worden als het verzaken van de zorgplicht.

Ben ik kwetsbaar?

Netwerkbeheerders (maar ook eindgebruikers) kunnen met behulp van (web)tools controleren of er sprake is van een open DNS-resolver.

Is mijn DNS-server vatbaar voor misbruik?

- Gebruik de aangeboden tools op één van de volgende websites:
  - http://www.openresolverproject.org/
  - http://www.thinkbroadband.com/tools/dnscheck.html
  - http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl
- Deze tools kunnen ten onrechte een open resolver aangeven. Laat de resultaten daarom nogmaals controleren door een netwerkbeheerder of met behulp van netwerktool NMAP.
- Let op dat beveiligingssoftware deze controles kan aanmerken als een poging tot aanval.

Wat kan ik doen?

Er zijn drie factoren die bijdragen aan (D)DoS aanvallen op basis van DNS-amplificatie. Hieronder staan de bijbehorende tegenmaatregelen genoemd:

- **Breng open resolvers in kaart en sluit ze af.** Een open resolver is een resolver die voor de gehele wereld uitvraagbaar is, wat in de regel onverstandig is. Kwaadwillenden misbruiken deze op grote schaal. Beheerders die resolvers installeren, moeten hierop bedacht zijn. Zeker als deze resolvers bereikbaar zijn via het internet. Het advies is om de resolver alleen voor een beperkte doelgroep toegankelijk te maken, bijvoorbeeld alleen voor de eigen gebruikers. Bij de meeste nameserversoftware kan dit eenvoudig worden ingesteld. Waar dit niet mogelijk is kan een firewall uitkomst bieden. Bedenkelijke software (zoals de firmware in sommige modellen breedbandrouters) of slecht gekozen standaardwaarden, zorgen er dikwijls voor dat sprake is van open resolvers waar men zich niet van bewust is.

- **Beheer authoritative name servers adequaat.** Ook authoritative name servers kunnen worden misbruikt voor DNS-amplificatie. Door middel van goede monitoring kan dit worden opgemerkt. Steeds meer leveranciers van name servers bieden zogenaamde Response Rate Limiting-functionaliteit aan in hun software (BIND, Knot en NSD).[5] Deze beperkende maatregel zorgt ervoor dat er in bepaalde kenmerkende gevallen geen antwoord (of alleen een verkort antwoord) wordt gegeven op een DNS-vraag, waardoor de DNS-amplificatie aan effectiviteit inboet. Soortgelijke, maar minder 'intelligente' limiteringen kunnen worden bewerkstelligd met bepaalde firewallregels. Dit is echter niet zonder risico en vereist een zorgvuldige aanpak. Voorkomen moet worden dat legitiem verkeer ten onrechte wordt geblokkeerd, of dat de firewallregels anderszins hun doel missen.

Spamhaus

The Spamhaus Project is een non-profitorganisatie die o.a. verantwoordelijk is voor het beheer van databases en 'zwarte lijsten' van IP-adressen en domeinnamen die gebruikt zijn of kunnen worden om spam te versturen. De gegevens van Spamhaus, zoals de 'Spamhaus blacklist', worden veel door e-mailproviders gebruikt in hun spamfilter om e-mail afkomstig van daarin geregistreerde domeinen te blokkeren. In maart 2013 werd de website van Spamhaus met een DNS-amplificatie aangevallen. De aanval werd achteraf getypeerd als de grootste DDoS-aanval die tot dan toe had plaatsgevonden. De aanval begon op 18 maart 2013 waarbij in het begin 10 Gbps aan verkeer werd gemeten met uitschieters tot 100 Gbps in de avond. Nadat Spamhaus een externe leverancier van anti-DDoS-diensten had ingeschakeld, waren de diensten op 20 maart weer beschikbaar. Toen de aanvallers onderkenden dat de maatregelen van de leverancier effect hadden, verplaatsten zij de aanval van Spamhaus naar de internetexchangepunten via welke de leverancier zijn diensten levert en die ook grote ISP's gebruiken voor hun communicatie. Deze aanval haalde waarden tot 300 Gbps en had in een aantal Europese en Aziatische landen zelfs merkbare gevolgen voor de performance van het internet. Volgens de leverancier waren door de aanvallers ongeveer 30.000 open DNS-resolvers ingeschakeld om de DDoS-aanval uit te voeren.

5 Zie http://www.redbarn.org/dns/ratelimits en http://www.sidnlabs.nl/laatste-berichten/nieuwsdetail/article/nieuwe-kwetsbaarheden-in-dns-maken-dnssec-validatie-noodzakelijk/ en http://www.nlnetlabs.nl/blog/2013/09/16/rrl-slipand-response-spoofing/ en https://lists.isc.org/pipermail/bind-users/2012-July/088220.html (rate limiting met behulp van IPtables)

» **Blokkeer de mogelijkheid om bronadressen te spoofen.** De essentie van DNS-amplificatie-aanvallen is dat kwaadwillenden de bron-IP-adressen in pakketten veranderen naar het IP-adres van hun slachtoffers. Netwerkbeheerders kunnen dit voorkomen door filtering te configureren in (delen van) hun netwerk. In de beroepspraktijk staat dit bekend als 'BCP38'. Deze Best Current Practice is omgezet in RFC2827.[6] Leveranciers van netwerkapparatuur bieden hier ondersteuning voor (soms aangeduid als Unicast Reverse Path Forwarding of uRPF). Met deze filtering wordt voorkomen dat er vanuit een netwerk aan adres-spoofing kan worden gedaan richting slachtoffers in andere netwerken.

Handelingsperspectief:

1. Draai niet onnodig (of onwetend) open resolvers naar het internet en wees erop voorbereid dat deze op onverwachte plekken kunnen opduiken.
2. Overweeg Response Rate Limiting (RRL) op authoritative name servers, maar hou er rekening mee dat dit met firewalls niet triviaal is. Beter is de RRL-functionaliteit die tegenwoordig beschikbaar is in name server software van bepaalde leveranciers (BIND, NSD, Knot) te gebruiken.
3. Implementeer filters tegen address-spoofing vanuit uw netwerk (BCP38).

Tot slot

De Spamhaus-aanval in maart 2013 heeft nog eens duidelijk gemaakt wat de gevolgen kunnen zijn van DNS-amplificatie, en hoe talrijk de wereldwijd openstaande DNS-resolvers en authoritative name servers nog altijd aanwezig zijn. Wanneer eigenaren en beheerders hun verantwoordelijkheid nemen door hun netwerk te beschermen tegen deze vorm van misbruik, wordt het voor de aanvaller minder aantrekkelijk en hebben de slachtoffers van (D)DoS-aanvallen één zorg minder. «

Laat anderen geen slachtoffer worden van uw DNS-infrastructuur.

Bescherm uw netwerk tegen misbruik.

6 Zie http://www.bcp38.info/ en http://dnssec.nl/cases/dns-amplificatie-aanvallen-straks-niet-meer-te-stoppen-zonder-bcp-38.html en http://tools.ietf.org/html/bcp38 en http://tools.ietf.org/html/rfc2827

Uitgave van Nationaal Cyber Security Centrum
met medewerking van SIDN, NBV en Ministerie van Defensie
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl
T 070 888 75 55 | F 070 888 75 50
Publicatienr: FS2013-03 v1.0 | Aan deze informatie kunnen geen rechten worden ontleend.