DDOS attack. Wat is dat eigenlijk?

Handleiding van Helpmij.nl

Auteur: leofact

juni 2018

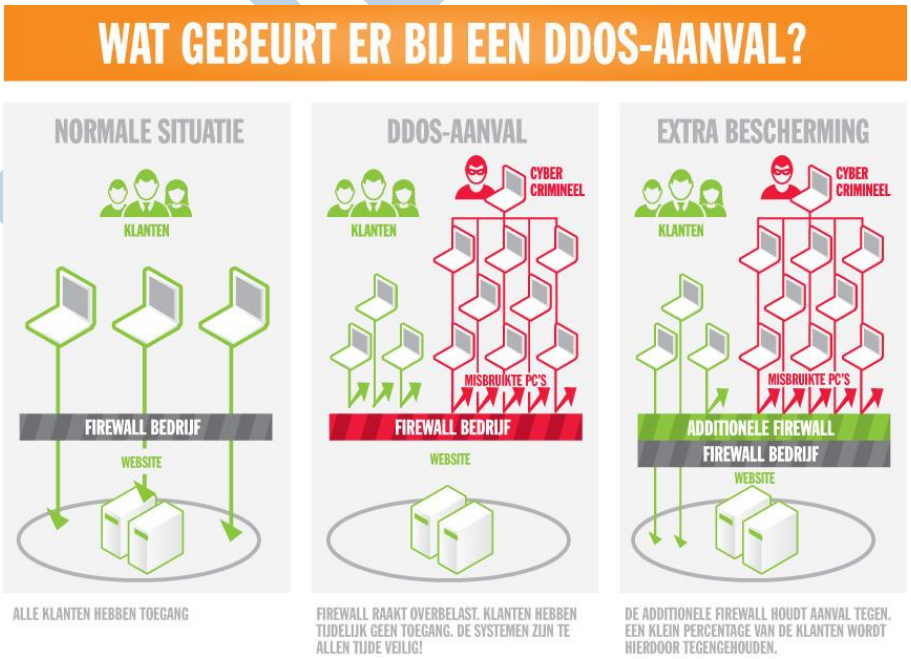
Een DDOS aanval was nog maar een paar jaar geleden een volkomen onbekend begrip voor veel mensen. De laatste tijd valt de term steeds vaker en ondertussen weten we dat er dan een internetdienst plat ligt. Over het algemeen valt dit ons het meest op wanneer het internetbankieren weer eens niet lukt. Er wordt veel over geschreven en gesproken en toch blijken veel mensen niet te weten wat een DDOS aanval nu precies is. Dit leek me een goede reden om een poging te wagen om uit te leggen waar het nu om draait bij een dergelijke digitale aanval.

Pesten

DDOS attack staat voor Distributed Denial Of Service aanval. Bij een DDOS aanval probeert de aanvaller de werking van een server van een bepaalde dienst (in ons voorbeeld; internetbankieren) te verstoren door er heel veel contact-verzoeken naar toe sturen. De bedoeling daarvan is dat de server overbelast raakt en vervolgens niet meer reageert op de inlogverzoeken van de normale gebruikers. Resultaat; de server gaat plat en de dienst ligt eruit. Daar blijft het dan ook bij. Er worden geen gebruikersgegevens buit gemaakt bij een DDOS aanval.. Het is uiteindelijk niets ander dan een vervelende manier van digitaal pesten. Niets meer en niets minder. Dit “pesten” kan overigens best grote gevolgen hebben voor de slachtoffers. De laatste tijd worden banken zo vaak getroffen door een aanval dat de klanten het vertrouwen kwijt raken in de betreffende bank en daarom aan overstappen gaan denken. De grote banken worden vaker getroffen dan de wat kleinere, maar elke dienst die gebruikt maakt van een server die met internet is verbonden kan worden getroffen door een DDOS aanval. Dat betekent dus dat iedere bank het slachtoffer kan zijn.

Normaal

Om de werking van een DDOS aanval nader te bekijken, gaan we kort in op de normale situatie. We pakken daarvoor een infographic van de ING erbij:



Links zie je hoe een gezellig groepje groene klanten ongehinderd kunnen inloggen om hun dagelijkse banktaken te kunnen verrichten. De server doet het eigenlijke werk en de Firewall draagt er zorg voor dat er geen oneigenlijk verkeer de server kan bereiken. Belangrijk, want we willen dat niemand met zijn digitale vingers aan ons eveneens digitale geld kan zitten. De Firewall heeft dus een belangrijke

taak. De IT-afdelingen van de verschillende banken zorgen er daarom dan ook voor dat deze verdedigingsmuur goed op zijn taak berekend is.

Overbelasting

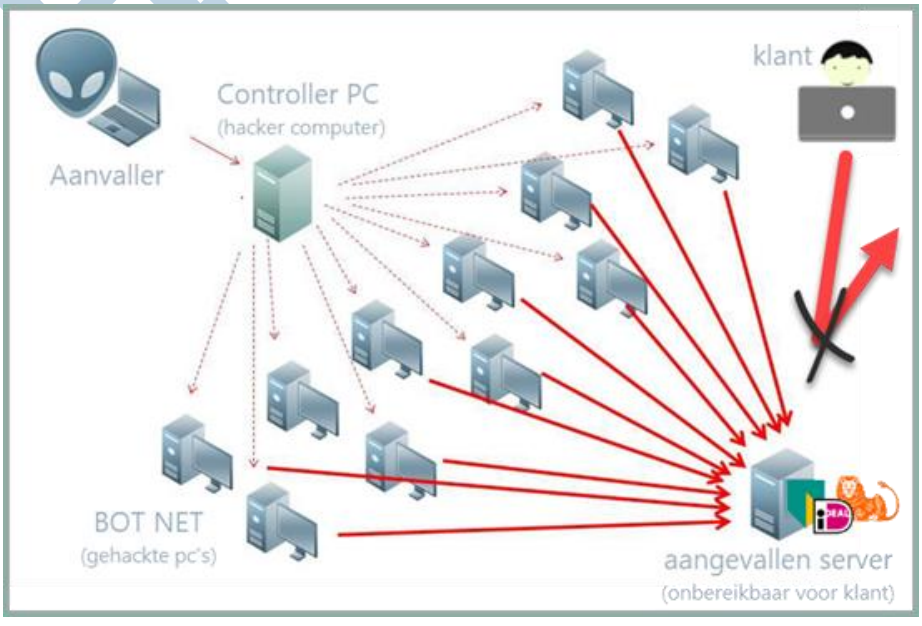
Om de Firewall goed zijn werk te laten doen is er bandbreedte en veel rekenkracht nodig. Dit is een keerzijde van de medaille die de DDOS aanvaller misbruiken kan zoals we zien in de middelste afbeelding. De aanvaller stuurt ontelbaar veel valse verzoeken aan de server en op het moment dat de Firewall al deze verzoeken niet allemaal apart meer kan behandelen, gaat hij alle verzoeken weigeren met als resultaat dat de dienst niet meer bereikbaar is. De klanten worden nu groen van ergernis als ze, in de rij voor een drukke kassa, net hun saldo nog even snel van de spaar- naar de lopende rekening moeten overschrijven, omdat de boodschappen toch weer duurder uit vielen dan gedacht. Dit lukt nu niet en de rij achter de goedwillende klant begint te morren. Er zit dan niets anders op dan uit te rij te stappen en afwachten tot de internetpesters stoppen met hun vervelende gesar en je internetbank je weer toegang geeft tot jouw eigen geld.

Tip; soms weet je niet wat er aan de hand is wanneer een bepaalde dienst niet werkt op je computer of telefoon. Om te voorkomen dat je er zelf onnodig tijd in steekt, kun je op allestoringen.nl checken of het een probleem is van de dienst zelf. Het enige wat je dan nog kunt doen, is afwachten tot het probleem is opgelost. Allestoringen.nl vind je als app en als website (zie de link onderaan dit artikel).

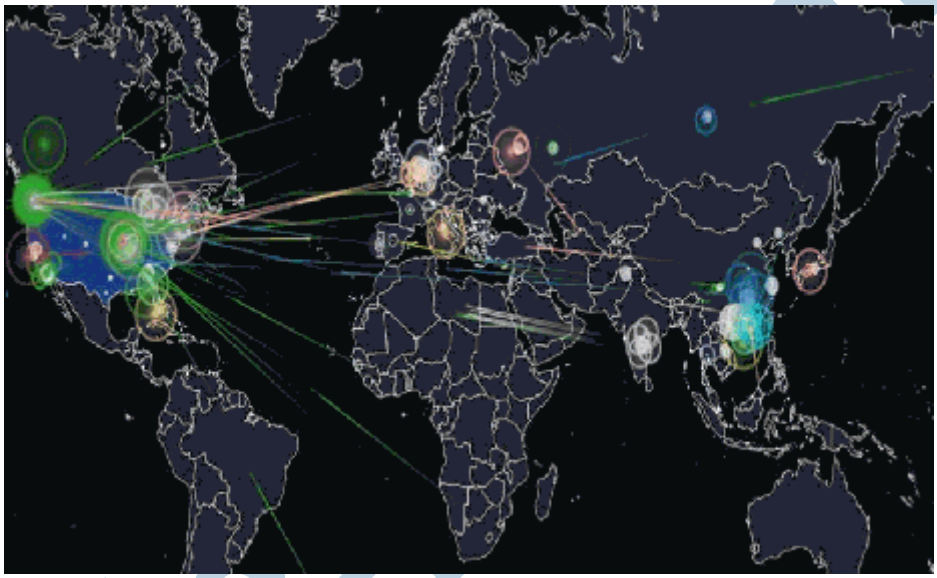
Machteloos?

In het meest rechtse plaatje zie je dat de bank dit probeert op te lossen door een extra Firewall in te stellen, die in ieder geval deels nog in gebruik blijft. Waarom nu zo'n lapmiddel? Kan de aanval niet gewoon worden afgeslagen? Voor het antwoord hierop is het goed om te beseffen dat Internetdiensten geen enkele mogelijkheid hebben om het aantal verzoeken te beperken dat de Firewall bereikt. De bandbreedte kan worden vergroot en de server kan sneller worden gemaakt, maar de intensiteit van de aanval kan door de aanvaller net zo eenvoudig worden vergroot. Hierdoor is er een digitale wapenwedloop ontstaan die nog lang niet teneinde is.

Krachten bundelen



Banken en andere diensten hebben veelal flink geïnvesteerd in hun apparatuur om dit soort ongemakken zoveel mogelijk te beperken. Daar kun je echt niet tegenop met je laptopje vanaf een donker zolderkamertje. Om deze uitdaging het hoofd te bieden, zetten de aanvallers een andere criminele praktijk in; de inzet van een botnet. Dit is een groep computers van willekeurige gebruikers die ooit gehackt zijn en waarop software is geïnstalleerd waarmee de aanvaller de controle overneemt van de gehackte PC's. De aanvaller bundelt de rekenkracht en de bandbreedte van de computers om een gecombineerde aanval uit te voeren. Deze gecoördineerd uitgevoerde aanval kan dan alsnog de versterkte server van de internetdienst overwinnen. Wanneer er een botnet wordt ingezet spreek je van een DDOS aanval: een Distributed Denial Of Service attack. Distributed betekent hier dat de aanval verdeeld wordt over meerdere (gekaapte) computers. De aanval kan ook door een groep aanvallers uitgevoerd worden. De eerste D wordt dan weggelaten; men spreekt dan van een DOS aanval. De hackersgroep Anonymous heeft wel dergelijke aanvallen uitgevoerd.



Tip; een besmetting met malware kan iedereen overkomen en ook jouw PC kan onderdeel uitmaken van een botnet. Een besmetting kun je soms merken doordat de PC trager gaat werken en je met browsen onverwachte sites ziet. Of de PC daadwerkelijk besmet is en wat je eraan doet, lees je onder meer op de site van Computer Totaal!. Volg daarvoor de link onderaan dit artikel.

Moeilijk?

Is het nu moeilijk om een aanval op te zetten? Helaas niet. Wanneer je bekend bent met het criminele, duistere deel van het internet, dat beeldend dan ook het Darkweb heet, kun je zo'n aanval gewoon kopen. Voor nog geen 10 euro kun je al je eigen DDOS aanval opzetten. Let op; dit is beslist géén oproep om dat ook te doen!

Software

De software die je voor een aanval nodig hebt, is overal te vinden. Vaak slecht geprogrammeerd, maar wel in staat om de gevraagde taak uit te voeren. Deze software is in feite vaak omgebouwde software die ooit is ontwikkeld om een stresstest uit te voeren op een server, om te onderzoeken of deze op zijn taak berekend is. De server gaat bij een DDOS aanval dus in feite onderuit door de test sterk te overdrijven. Er zijn verschillende methodes om de server over te belasten. Het resultaat is steeds hetzelfde; de server wordt trager en reageert uiteindelijk niet meer.

Gevaarlijk?

Is een DDOS aanval nu gevaarlijk? Daar is geen eenduidig antwoord op te geven. In eerst instantie is de aanval niet gevaarlijk. Er worden geen gegevens gestolen en als de aanval over is, kan de aangevallen dienst gewoon weer zijn werk doen. Een DDOS aanval wordt echter ook wel ingezet als afleidingsmanoeuvre. Het IT-personeel richt zijn aandacht op het weer online krijgen van de server. Aanvallers kunnen van deze verwarring gebruik trachten te maken om in te breken in de server om dan via deze omweg alsnog bij de gegevens van de gebruikers te komen. Zover mij bekend is dit bij het bankwezen nog nooit gelukt.

Het wordt ook een ander verhaal als er vaak langdurige aanvallen worden gelanceerd. Dit kan dan ontregelend werken in het betalingsverkeer. In het hypothetische geval dat er heel grootscheepse aanvallen zouden worden opgezet, kan het internet zodanig worden verstoord dat het onbruikbaar wordt. Als een dergelijk probleem langer zou bestaan, werkt dat ontwrichtend voor onze samenleving, omdat watervoorziening, energie-opwekking en voedseldistributie in theorie in gevaar kunnen komen. Gelukkig wordt hier rekening mee gehouden en worden er allerlei tegenmaatregelen genomen. Zo staan de twee kerncentrales in Nederland helemaal los van het internet. Het is en blijft echter een wedloop tussen de aanvallers en verdedigers. Er zijn speciale diensten in het leven geroepen die tot doel hebben om de cybercriminaliteit te bestrijden. In Nederland is dat het Nationaal CyberCrime Centrum. Als land is Nederland maar een kleine speler in dit spel. Door de krachten te bundelen kan er meer bereikt worden. Hiervoor is er in Europees verband een digitale politie opgericht; The European CyberCrime Centre. Gelukkig begint het bij de verschillende overheden steeds meer door te dringen hoe belangrijk het is om internetcriminaliteit te bestrijden.

Ten slotte

In dit artikel heb je kunnen lezen dat een DDOS aanval een manier is om een internetdienst plat te leggen door onder meer gebruik te maken van een botnet. De gevolgen van een aanval zijn irritant, maar leveren in beginsel geen gevaar op. Wel is er sprake van een wedloop en het is daarom zaak om de aanvallers voor te blijven.

Volg de link voor informatie bij dit artikel over de volgende onderwerpen:

DDOS Attack (https://nl.wikipedia.org/wiki/Distributed_denial-of-service)
Wat is een botnet (https://nl.wikipedia.org/wiki/Botnet)
Web server (https://nl.wikipedia.org/wiki/Webserver)
Firewall (https://nl.wikipedia.org/wiki/Firewall)
Anonymous groep (https://nl.wikipedia.org/wiki/Anonymous_(groep))
Nationaal CyberCrime Centrum (https://nl.wikipedia.org/wiki/Nationaal_Cyber_Security_Centrum)
European CyberCrime Centre (https://nl.wikipedia.org/wiki/European_Cybercrime_Centre)
Hoe weet ik of mijn PC besmet is? (Computer Totaal!) (https://computertotaal.nl/artikelen/apps-software/de-5-tekenen-van-malware-zo-ontdek-je-of-je-de-dupe-bent-64131/)
Allestoringen.nl (http://www.allestoringen.nl/overzicht/)

De gebruikte afbeelding zijn deels bewerkt en afkomstig van Wikimedia en Pixelbay