OPINIE

WAT GAAN WE DOEN TEGEN DE CYBERAANVALLEN?



Prof. dr. Pieter Hartel en prof. dr. Marianne Junger zijn verbonden aan de Universiteit Twente. Dr. ir. Jan van den Berg is verbonden aan de Technische Universiteit Delft. Zij houden zich bezig met onderzoek naar cyber security en zijn respectievelijk te bereiken via pieter.hartel@utwente.nl, m.junger@utwente.nl en J.vandenBerg@tudelft.nl.

Een aantal bedrijven, zoals ING, de Telegraaf, en de NS hebben de afgelopen maand last gehad van Distributed Denial of Service (DDoS) aanvallen. Enigszins gesimplificeerd zijn hierin de volgende stappen te onderscheiden: 1) de PC van een gebruiker loopt een computervirus op, bijvoorbeeld omdat de gebruiker een email aanhangsel van dubieuze herkomst opent. 2) De geïnfecteerde PC gaat daardoor deel uitmaken van een 'botnet', waarbij de PC op afstand bestuurd wordt door een crimineel, ook wel bot-herder genoemd. Hoe meer PC's er in het botnet zitten, hoe meer schade de bot-herder kan aanrichten. 3) De bot-herder besluit om het botnet in te zetten om berichten naar een bepaalde website, bijvoorbeeld van een bank, te sturen. 4) Als dat wordt gedaan, dat wordt de website door overbelasting – nagenoeg – onbereikbaar. Wereldwijd worden er per dag honderden van dergelijke DDoS-aanvallen geregistreerd [1]. Soms pakt de politie een bot-herder op, maar meestal niet, omdat ze zich goed kunnen verstoppen.

Omdat de voorbereiding voor een DDoS-aanval uit verschillenden stappen bestaat, is de bestrijding daarvan het meest kansrijk als op meer fronten preventieve maatregelen worden getroffen. Hieronder beschrijven wij een aantal maatregelen die op korte termijn mogelijk zijn om de situatie te verbeteren.

1. De ISPs gaan samen werken om botnetbesmettingen aan te pakken

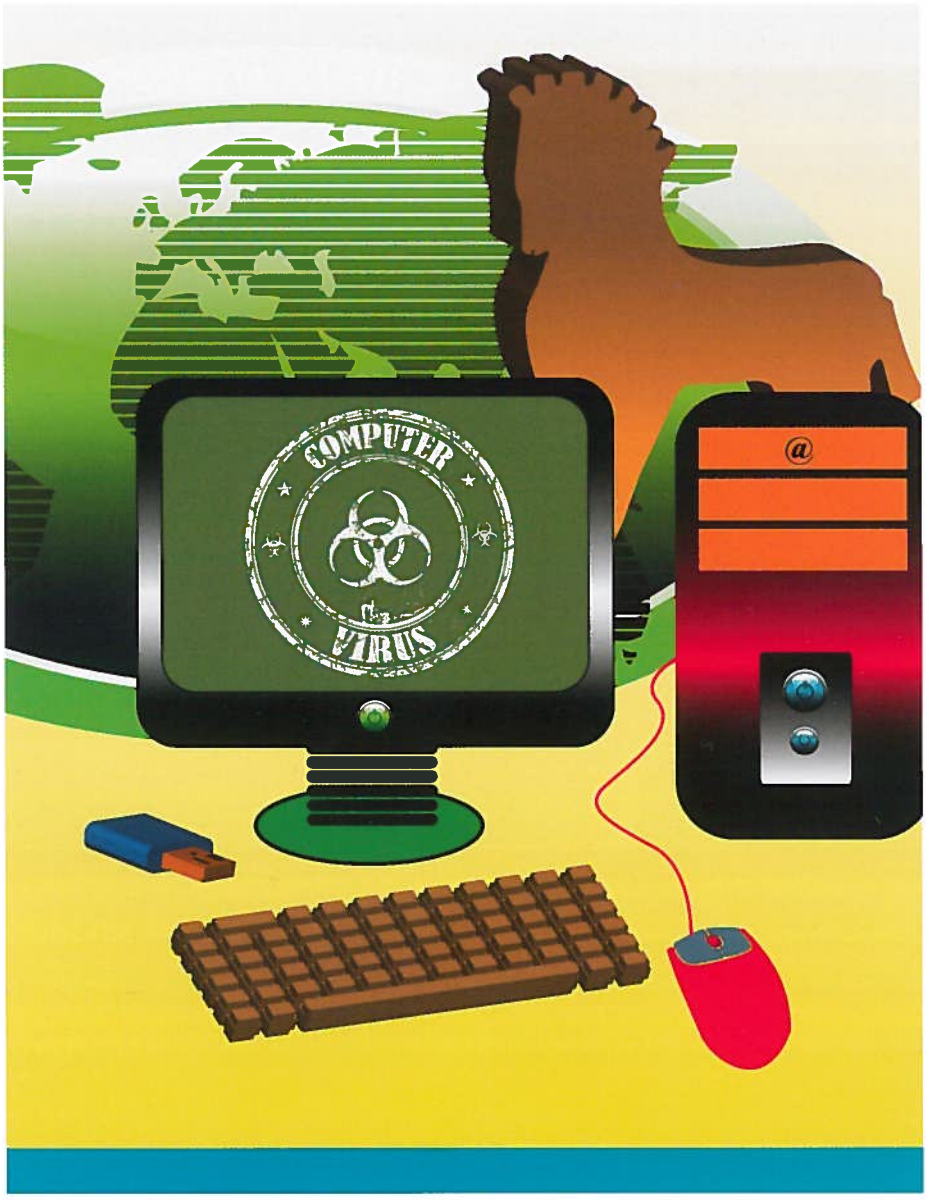
De Nederlandse Internet Service Providers gaan binnenkort op grote schaal botnetbesmettingen aanpakken via de Abuse Internet Exchange. Dat is een verzamelpunt waar allerlei informatie bijeen komt over besmette PC's in de netwerken van de providers. Die informatie wordt vervolgens doorgesluisd naar teams die contact opnemen met de getroffen klanten en hen informeren over hoe de computer opgeschoond kan worden. De providers doen dit al enkele jaren, maar onderzoek van de TU Delft toonde aan dat ze maar een beperkt deel van de besmettingen wisten op te sporen en op te ruimen. Het nieuwe initiatief gaat het probleem grootschaliger aanpakken.

> De kans bestaat dat u medeplichtig bent aan een van de recente DDoS-aanvallen

2. De gebruiker gaat de thuis PC beter onderhouden

Als gebruikers maken wij zelf deze kans op besmetting groter wanneer we onzorgvuldig omgaan met onze PC, bijvoorbeeld als we niet de laatste versie van de programma's gebruiken, of als we de virusscanner

of de firewall uitzetten. Uit onderzoek van de TU Delft is gebleken dat ongeveer één op de twintig PC's besmet is. Dit betekent dat de kans bestaat dat u, lezer, 'medeplichtig' bent aan één van de recente DDoS-aanvallen op onze banken of - op dit moment - meedoet aan de DDoS-aanval op een bedrijf elders in de wereld. Daarom lijkt het ons verstandig dat gebruikers nadrukkelijk op hun verantwoordelijkheid wordt gewezen om hun PC en daarmee het Internet gezond te houden. Vanzelfsprekend geldt dit ook voor PC's en computersystemen van bedrijven en andere organisaties.



3. Bedrijven gaan de thuis PC gebruiker beter helpen

De banken vertellen ons al sinds jaar en dag hoe je je thuis PC zo gezond mogelijk kan houden [2]. De benodigde software kun je kopen bij bedrijven zoals Symantec, Microsoft en Kaspersky. Maar die software kan beter; zo kost het vaak te veel tijd om nieuwe virussen te analyseren en de software zodanig bij te werken dat die virussen worden herkend en onschadelijk gemaakt.

4. De overheid gaat werken aan een APK voor PC's

Gebruikers moeten aanvullende hulp kunnen krijgen in de vorm van extra kennis en hulpmiddelen. De overheid zou bijvoorbeeld een veiligheidspakket (à la het Duitse veilige e-mail encryptiepakket) kunnen aanbieden, waarmee de gebruiker een simpele "APK-controle" op zijn of haar PC, MAC, én smartphone (en eerdaags ook de digitale TV) kan uitvoeren. Vindt het APK pakket geen problemen, dan ben je grotendeels gevrijwaard van digitale onveiligheden.

5. Er komt een internationaal certificeringssysteem voor software

Virussen maken misbruik van fouten in computerprogrammatuur. Het opzetten van een certificeringssysteem voor programmatuur kan helpen om fouten te voorkomen en daarmee het probleem kleiner te maken, want hoe minder fouten hoe beter.

Succes tegen botnets kan bereikt worden, indien de Nederlandse overheid samen met private partijen bovenstaande punten voortvarend aanpakt. Daarmee is de kous zeker niet af. Het ligt in de lijn der verwachting dat DDoS aanvallen ook steeds vaker gaan gebeuren via de smartphone (waar zijn de veiligheidspakketten?) en de digitale TV. De overheid zal zijn sturende en wetgevende rol rond cyberspace nog serieuzer moeten nemen en bovenstaande initiatieven op elkaar moeten afstemmen, mede in de internationale context. Dit klemt des te meer daar criminelen niet stilzittend zullen afwachten wat wij gaan doen, maar, als reactie op bovenstaande, hun tegenmaatregelen nemen. Kortom, we zullen alert moeten blijven om cyberspace ook in de toekomst voldoende veilig te houden, door inspanningen van ons allen. ●

De overheid zal zijn sturende en wetgevende rol rond cyberspace nog serieuzer moeten nemen

Links

[1] *Atlas Global DDoS Summary Report: http://atlas.arbor.net/summary/dos*

[2] *NVB campagne Veilig Bankieren: http://www.veiligbankieren.nl*