

Botnets

Is uw computer onderdeel
van een crimineel netwerk?



Regelmatig duiken er berichten op in de media over websites van bedrijven die worden aangevallen en uit de lucht raken. Maar wist u dat ook uw computer misbruikt kan worden om deze aanvallen uit te voeren? Uw computer maakt in dat geval (zonder dat u het weet) deel uit van een grootschalig en wereldwijd netwerk, oftewel een botnet.

Maar wat is nou precies een botnet? Hoe loopt u een besmetting op en vooral, wat kunt u er tegen doen? Deze folder geeft u een beknopt antwoord op deze vragen.



Wat is een botnet?

Het woord 'bot' komt van robot. Een bot is een programma dat zelfstandig geautomatiseerd werk kan uitvoeren. Een bot kan heel onschuldig zijn. Zo worden bots gebruikt door zoekmachines om websites in kaart te brengen. Maar helaas kan een bot ook worden gebruikt om criminele handelingen uit te voeren op computers.

Een computer die besmet is met een bot wordt ook wel een zombie genoemd. Een botnet is een netwerk van een groot aantal willoze zombiecomputers die allemaal besmet zijn met dezelfde bot. Vanuit een centraal punt kan één kwaadwillend persoon al deze bots in het netwerk opdracht geven om dezelfde taak uit te voeren.



Botnets worden verkocht aan criminele organisaties en vervolgens voor diverse illegale activiteiten gebruikt. Zo kan een bot gebruikt worden om (samen met alle andere bots in een botnet) zoveel verkeer naar een website te sturen dat deze bezwijkt. Ook worden botnets ingezet om spam te versturen en reacties daarop te verwerken. Hierdoor wordt het bijna onmogelijk om de spammer te achterhalen.

Maar een bot kan ook direct tegen u worden gebruikt. Zo kan een bot bijvoorbeeld uw creditcard- of bankgegevens onderscheppen of een achterdeur openen op uw computer, zodat anderen ongemerkt toegang hebben tot uw persoonlijke informatie.



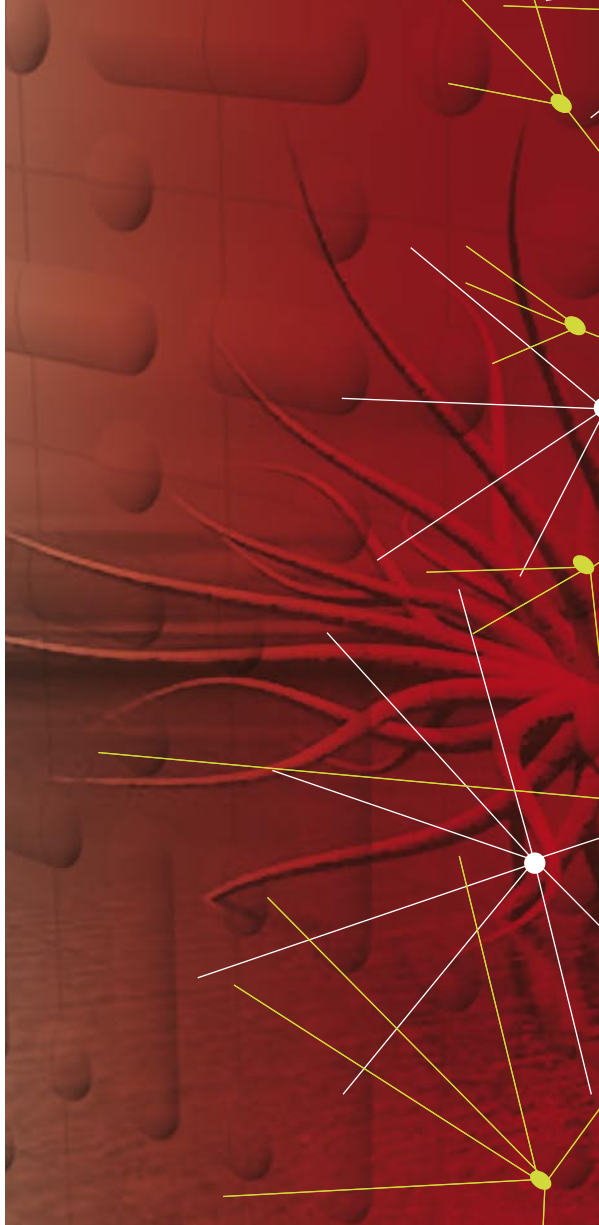
Hoe loopt u een besmetting met een bot op?

Een bot-programma kan uw computer besmetten via een virus of via een beveiligingslek in uw browser of besturingsstelsel. Wanneer een bot een computer heeft besmet, kan deze computer gebruikt worden om de bot verder te verspreiden.

Hoe kunt u een besmetting met een bot herkennen?

Wanneer uw computer besmet is met een bot, kunt u dit herkennen aan een aantal 'symptomen':

- Een bot op uw computer kan de opdracht hebben gekregen om bijvoorbeeld een website aan te vallen of spamberichten te versturen. Uw computer zal daarvoor intensief gebruik maken van uw internetverbinding. Wanneer u bijvoorbeeld een emailbericht wilt versturen of een website wilt bezoeken, zult u merken dat dit allemaal **zeer traag** verloopt.
- Zodra een bot op uw computer is geïnstalleerd, zal deze vaak **proberen** uw anti-virusprogramma of uw firewall **uit te schakelen**.
- U kunt door middel van een poortscan controleren of vreemden toegang hebben tot uw computer. Dit kan erop wijzen dat uw computer besmet is met een bot. Meer informatie hierover leest u op www.surfopsafe.nl/scans.



Wat kunt u doen?

- **Installeer een antivirus-programma** en een **firewall** en houd deze up-to-date. Aan de hand van een antivirus-programma kunt zien of u al besmet bent met een bot en deze vervolgens verwijderen. Een firewall houdt indringers buiten de deur en kan voorkomen dat uw computer misbruikt wordt. Goede programma's zijn verkrijgbaar bij computerwinkels of uw internetprovider.
- Zorg ervoor dat uw **browser en besturings-systeem altijd up-to-date** zijn, bij voorkeur door middel van automatische updates. Indringers komen meestal binnen via fouten in de oudere versies. Ga naar www.surfop-safe.nl of www.waarschuwingsdienst.nl voor meer informatie.
- **Let op met downloaden** van bestanden via zogenaamde '**peer-to-peer**' netwerken waarmee u bijvoorbeeld gratis muziekbestanden kunt uitwisselen met andere gebruikers. Virussen doen zich vaak voor als aantrekkelijke bestanden zoals muziek, programma's en filmpjes. Hierin kan ook een bot verborgen zitten.
- **Verwijder direct e-mail** van personen of bedrijven die u niet kent, zonder deze te openen.
- Wees voorzichtig met het openen van **bijlagen** in e-mails. Deze kunnen een bot bevatten, waardoor uw computer besmet raakt. Open dus geen bijlagen in e-mails die u niet vertrouwt!

Voor meer informatie en vragen over botnets en andere internetrisico's kunt u terecht bij:

De Waarschuwingsdienst

Meld u aan op www.waarschuwingsdienst.nl en blijf op de hoogte van de allerlaatste computerdreigingen, zoals phishing-aanvallen, computervirussen, wormen en lekken in software.

Surf op Safe

Ga naar www.surfopsafe.nl voor meer informatie over veilig internetten of vraag gratis de brochure 'Veilig Internetten' van Surf op Safe aan via www.postbus51.nl of telefoonnummer 0800 8051.

Deze uitgave van het Ministerie van Economische Zaken, Directoraat-Generaal Telecommunicatie en Post (DGTP) is met grote zorgvuldigheid opgesteld in samenwerking met de Waarschuwingsdienst. Desondanks kunnen aan de tekst geen rechten worden ontleend.

Gratis exemplaren van deze folder kunt u telefonisch bestellen bij Postbus 51, telefoon 0800 8051, elke werkdag van 9.00 uur tot 21.00 uur, of opvragen via www.minez.nl (onder publicaties).

November 2005

Publicatienummer: 05TP29



Ministerie van Economische Zaken

 **WAARSCHUWINGSDIENST**