

## **Tech Monitor: Botnets – een dreigende ontwikkeling op het internet**

### **Maatschappelijk Overleg Betalingsverkeer, november 2008**

#### **Introductie**

De laatste jaren zijn Nederlanders het internet massaal gaan gebruiken om te internetbankieren en om online te winkelen. Volgens recente cijfers had 88 procent van de mensen in Nederland internettoegang, de meesten ( 79 procent ) breedband. 72 procent van de internetgebruikers doet aan internetbankieren en 66 procent winkelt via internet<sup>1</sup>. Nederland behoort met deze cijfers tot de koplopers in Europa. De omzet van de Nederlandse webwinkels bedroeg in de eerste helft van 2008 EUR 2,3 miljard<sup>2</sup> en zal naar verwachting over 2008 als geheel tussen de EUR 4-5 miljard bedragen. In Europa bedraagt de webwinkelomzet in 2008 in totaal naar schatting EUR 124,1 miljard<sup>3</sup>.

Bovenstaande cijfers spreken tot de verbeelding. In een periode van enkele jaren is het internet voor banken en bedrijven een belangrijk kanaal geworden om producten en diensten te leveren. Tegelijkertijd heeft het boevengilde de mogelijkheden van het internet ontdekt. Cybercrime is sterk aan het groeien. Zwakheden van computers op het internet bieden mogelijkheden voor criminelen om misbruik van te maken. Een belangrijk wapen dat criminelen in handen hebben om deze zwakheden uit te buiten zijn zogeheten *botnets*. Dit zijn netwerken van gekaapte computers op het internet die voor allerlei verschillende activiteiten kunnen worden gebruikt. Deze Tech Monitor zal de ontwikkeling van botnets toelichten.

#### **Bot en Botnet**

Een *bot* is een kwaadaardig softwareprogramma dat op een computer wordt geïnstalleerd zonder dat de computergebruiker het weet. Een *botnet* is een netwerk van computers die geïnfecteerd zijn met een dergelijk kwaadaardig softwareprogramma. Hierdoor is het mogelijk voor kwaadwillenden om deze computers massaal op afstand te besturen<sup>4</sup>.

#### **Activiteiten**

Zodra computers geïnfecteerd zijn, kunnen deze worden ingezet voor allerlei frauduleuze activiteiten op het internet, zoals spam, identiteitsfraude, massale aanvallen, klikfraude, phishing, et cetera. Daarnaast worden botnets gebruikt om meer computers te infecteren en zo het botnet uit

---

<sup>1</sup> Centraal Bureau voor de Statistiek, *De digitale Economie 2007*, maart 2008.

<sup>2</sup> Thuiswinkel.org, *Thuiswinkel markt Monitor 2008-I*, september 2008.

<sup>3</sup> Forrester Research, *The State of Retailing Online*, October 2008

<sup>4</sup> Dit stuk is mede gebaseerd op informatie uit ENISA Position paper No. 3, *Botnets – The Silent Threat*, November 2007. Kaspersky Lab, *The botnet business*, May 13 2008 en de GOVCERT.NL Trendrapporten

te breiden of om nieuwe botnets op te zetten. De meest voorkomende activiteiten worden toegelicht.

### *Spam*

Het versturen van spam is een veel gebruikte toepassing van botnets en is betrekkelijk eenvoudig te doen. Experts schatten dat tachtig procent van alle verzonden spam afkomstig is van computers die deel uitmaken van een botnet. Spam wordt overigens lang niet altijd door de beheerder van een botnet zelf verstuurd; vaak wordt capaciteit van botnets ingehuurd door spammers. Eén computer kan 3 spamberichten per seconde versturen (259.200 e-mails per dag). Miljoenen - of zelfs miljarden - spam-berichten kunnen in korte tijd worden verstuurd door computers uit het botnet. De grote botnets (met namen als Srizbi, Storm, Bobax en Ozdok/Mega-D) hebben een capaciteit van meer dan 100 miljard spam e-mails per dag.

Botnets bieden ook de mogelijkheid om e-mailadressen te verzamelen van geïnfecteerde computers. Deze adressen worden weer doorverkocht aan spammers die ze kunnen gebruiken om spam aan te sturen.

### *Identiteitsfraude*

Naast e-mailadressen kunnen botnets worden gebruikt om allerlei identificerende gegevens zoals gebruikersnamen, wachtwoorden en creditcardgegevens te stelen die mensen gebruiken om met hun computer in te loggen op websites en voor online diensten. Deze gestolen gegevens worden ergens op internet opgeslagen (in zogeheten drop zones). Vervolgens kunnen de criminelen deze gegevens zelf misbruiken of doorverkopen aan andere criminelen. Er zijn allerlei 'marktplaatsen' op internet ontstaan waarop dergelijke gestolen gegevens worden verhandeld.

### *Massale aanvallen*

Botnets zijn tevens een gevaarlijk wapen om massale aanvallen uit te voeren door middel van zogeheten *Distributed Denial of Service (DDoS)* aanvallen. Het ene moment draait er een ogenschijnlijk onschuldige toepassing, het volgende moment opent de computer een DDoS-aanval. Computers die deel uitmaken van het botnet kunnen opdracht krijgen om massaal een website te bezoeken van een overheidsorganisatie of bedrijf. Bij een upload bandbreedte van 40Kb/s gemiddeld per computer kan een relatief klein botnet van 10.000 computers de meeste websites al plat leggen. Het aantal computers in grotere botnets kan oplopen tot honderdduizenden computers.

---

2007 en 2008. Definitie van botnets afkomstig uit de ENISA position paper. De rapporten zijn te vinden via de website [www.allesoverbetalen.nl](http://www.allesoverbetalen.nl)

De aanvallen kunnen politiek gericht zijn. Zo lagen vorig jaar allerlei (overheids)websites in Estland wekenlang plat door DDoS-aanvallen nadat een Russisch standbeeld in een Estse stad was verplaatst. Deze verplaatsing was slecht gevallen bij bepaalde Russische groeperingen en was voor hen reden om daarop de cyber-aanval te openen. Massale aanvallen kunnen ook een 'commercieel' oogmerk hebben in de vorm van afpersing. Een bepaalde website wordt dan aangevallen en er wordt meegedeeld dat de aanval pas wordt stopgezet als de eigenaar van de website een bepaald bedrag betaald aan de criminelen. Het is ook al voorgekomen dat bedrijven websites van concurrenten op deze illegale wijze platleggen om zo concurrentievoordeel te behalen. Tot slot kunnen individuen of groeperingen ook botnets inzetten in het kader van hun ideologische doelstellingen. Kortom, toegang tot botnets is niet beperkt tot alleen cybercriminelen.

### *Klikfraude*

Computers in het botnet kunnen zich voordoen als legitieme gebruikers van websites. Ze kunnen worden ingezet om muisklikken op webadvertenties te genereren. Via deze zogeheten klikfraude kan de eigenaar van de website hogere advertentie-inkomsten verkrijgen.

### *Phishing*

Phishing is een vorm van fraude waarbij mensen worden opgelicht door ze te lokken naar een valse (bank)website die een kopie is van de echte website. Op het moment dat de klant daar nietsvermoedend inlogt in de veronderstelling op de echte website te zijn, bemachtigt de fraudeur de inloggegevens van de klant. Vervolgens kunnen deze gegevens worden misbruikt. Criminelen verzinnen steeds nieuwe manieren om de phishing-aanvallen te verbeteren. Eén van de nieuwe technieken is er op gericht om de locatie van een phishing-website te verbergen. Hierbij wordt een botnet gebruikt om adressen van phishing-websites voortdurend te veranderen door computers in het botnet te gebruiken als zogeheten *proxy server* (dit is een onzichtbare tussenschakel tussen internetgebruiker en een website). Normaal gesproken worden adressen van phishing-websites snel geblokkeerd zodra deze op het internet verschijnen, maar op deze manier wordt dat bemoeilijkt. Een andere belangrijke ontwikkeling op het gebied van phishing zijn zogeheten *man-in-the-middle* of *man-in-the-browser* aanvallen. Hierbij positioneren criminelen zich tussen de aangevallen klant en de echte website van een bank.

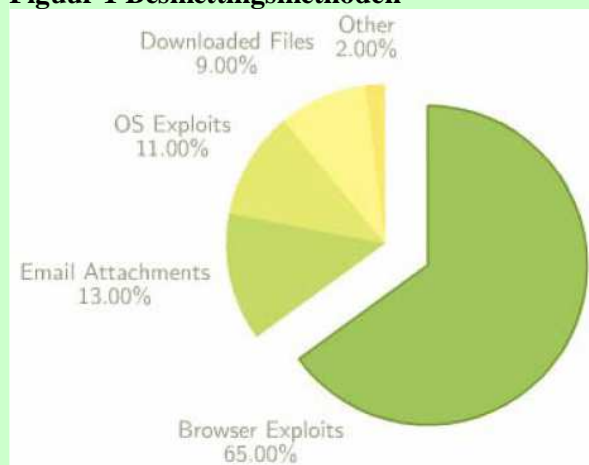
In Nederland pakt GOVCERT.NL - het Computer Emergency Response Team van de Nederlandse overheid - samen met de Nederlandse banken phishing aan via het *Notice and Take Down* project. Na een melding van een bank worden de servers waarop de phishing-website staat door GOVCERT.NL opgespoord en uit de lucht gehaald. Eén op de drie gemelde phishing-

websites wordt dezelfde dag afgesloten; de volgende dag is de helft niet meer actief. Hoewel uiteindelijk alle websites verdwijnen, kan in een enkel geval ook GOVCERT.NL niets uitrichten<sup>5</sup>.

### Een botnet in drie stappen

1. Het misbruiken van een kwetsbaarheid is de eerste stap voor het opzetten van een botnet. Tegenwoordig gebeurt besmetting van een computer vooral via zogeheten *browser exploits*. Hierbij wordt door het klikken op een link op een website een kwaadaardig programma geïnstalleerd.

**Figuur 1 Besmettingsmethoden**



Bron: ENISA Position paper No. 3, *Botnets – The Silent Threat*, November 2007

Besmetting op andere manieren, zoals via e-mail bijlagen, zwakheden in het *operating system*, of het downloaden van bestanden komt naar verhouding minder vaak voor. Zie figuur 1.

2. Zodra een kwetsbaarheid is benut wordt een klein programma in uitvoerbare vorm (een zogeheten *executable file*) gedownload en op de computer uitgevoerd.

3. Het nieuwe proces dat via dit computerbestandje is opgestart, zoekt verbinding met het botnet. Het meldt dat de computer gecompromitteerd is en klaar is om opdrachten uit te voeren in het botnet. Hierbij kunnen ook nieuwe programma's worden geladen die weer andere ongewenste dingen doen.

Schattingen over het aantal computers wereldwijd dat deel uit maakt van een botnet lopen uiteen. Eén van de grondleggers van het internet, Vint Cerf, schatte op het World Economic Forum in 2007 dat wereldwijd een kwart van de computers op het internet behoorde tot een botnet. In een recente uitgave van PC Magazine (oktober 2008) wordt een schatting van 11 procent genoemd.

### Botnet = business

Vroeger konden hackers worden gekarakteriseerd als slimme mensen die graag hun technische vaardigheden via luidruchtige virussen zichtbaar wilden maken aan de rest van de wereld. Bij deze hackers was geldelijk gewin geen doel; het ging hen hoofdzakelijk om de 'eeuwige roem'. Enkele jaren geleden realiseerden ook criminelen zich dat het internet allerlei kansen biedt om geld te verdienen. Ze leerden hoe ze misbuik konden maken van de zwakheden van het internet. De hackers van nu handelen voornamelijk uit crimineel oogmerk en zijn erop gericht hun technische vaardigheden zo onzichtbaar mogelijk te houden in hun 'producten'. Tegenwoordig dus geen luidruchtige virussen meer, maar stille botnets.

<sup>5</sup> GOVCERT Trendrapport 2008



## **Wat te doen tegen botnets?**

Er kan een aantal maatregelen worden genomen om de dreiging van botnets af te wenden<sup>6</sup>. Het is zaak voor makers van operating systems, browsers en softwaretoepassingen om de kwaliteit van hun producten te verbeteren aangezien vaak kwetsbaarheden in deze producten leiden tot misbruik. Veel mensen blijken verouderde productversies te gebruiken en dit verhoogt de risico's op besmetting aanzienlijk. Dit probleem komt deels doordat sommige gebruikers de mogelijkheid om computerprogramma's automatisch te repareren tegen lekken niet aan hebben staan. Terwijl deze automatische updates er juist voor zorgen dat de computer zelf zorgt dat deze actueel beschermd blijft. Mensen hiervan bewuster maken, is daarom een belangrijk punt voor alle partijen.

Ook bedrijfsleven en overheid kunnen bijdragen aan het verbeteren van de veiligheid van hun websites en toepassingen op het internet. Banken doen dit bijvoorbeeld door bij het internetbankieren gebruik te maken van identificatiefuncties met wachtwoorden die klanten slechts één keer kunnen gebruiken- zogeheten *one time passwords*. Internet service providers vervullen een sleutelfunctie in het internetverkeer en zij kunnen bepaalde technische maatregelen nemen tegen botnets. De OPTA bij de overheid is actief in het bestrijden van spam.

Of een beheerder van een botnet strafbaar is en kan worden vervolgd, hangt mede af van de activiteit van een botnet en of de wetgeving daarop kan worden toegepast. Overheden in de EU kunnen regelgeving om botnets te bestrijden meer harmoniseren dan nu het geval is. Cybercrime kent letterlijk geen grenzen en is bij uitstek een internationaal probleem waarbij activiteiten van cybercriminelen zich in een oogwenk kunnen verplaatsen naar andere landen - of continenten. Opsporing en vervolging van cybercriminelen wordt mede hierdoor internationaal bemoeilijkt en kan wereldwijd verder worden verbeterd.

De onwetende gebruiker - bij overheid, in het bedrijfsleven, of de consument - is vaak de zwakste schakel op het internet. Het is belangrijk om de bewustwording bij gebruikers te vergroten over wat zij kunnen doen om veilig internet te gebruiken. Vanuit verschillende partijen zijn hiervoor initiatieven opgestart in Nederland. Het Digibewust programma - een samenwerkingsverband tussen overheid en bedrijfsleven in Nederland - is bijvoorbeeld opgezet om te werken aan het vergroten van het digitale bewustzijn op het internet. Recent is voor webwinkeliers in dit verband een document gepubliceerd waarin een aantal criteria zijn geformuleerd om webwinkels beter te beveiligen<sup>7</sup>. Dit is niet alleen in het belang van de webwinkel zelf, maar ook van de klanten. In de

---

<sup>6</sup> Voor een compleet overzicht wordt verwezen naar de ENISA position paper *Botnets*, 2008.

<sup>7</sup> Digibewust, ECP.nl, Hoofdbedrijfschap Detailhandel, Thuiswinkel.org, *Criteria voor een veilige webwinkel*, augustus 2008.

financiële sector hebben banken gezamenlijk het initiatief genomen voor de campagne ‘Drie Keer Kloppen’ om de bewustwording van klanten te vergroten over hoe ze veilig kunnen internetbankieren. Enkele jaren geleden is ook de website [www.veiligbankieren.nl](http://www.veiligbankieren.nl) opgezet. Daarnaast heeft iedere individuele bank informatie op de website staan om de klant te helpen bij het veilig uitvoeren van transacties.

### **Slot**

Botnets worden door criminelen gebruikt voor een grote verscheidenheid aan criminele activiteiten. Het is niet bepaald waarschijnlijk dat criminelen dit machtige wapen zomaar uit handen zullen geven. Sterker nog, veiligheidsexperts verwachten dat botnet-technologieën geavanceerder worden. Zo kunnen botnets steeds meer gebruik maken van nieuwe kanalen en toepassingen zoals Instant messaging, Bluetooth en door infecties uit te breiden naar mobiele apparaten, spelcomputers en thuisssystemen. Botnets worden steeds onzichtbaarder doordat de kwaadaardige programma's dieper binnendringen in computers. Daarnaast worden door criminelen ook beveiligingsmaatregelen toegepast om hun 'producten' beter te beschermen - tegen bestrijders maar vooral ook tegen concurrerende botnets.

Botnets worden niet alleen technisch geavanceerder, maar tegelijkertijd ook gebruiksvriendelijker gemaakt voor de beheerder ervan. Hierdoor worden ze toegankelijk voor een grotere groep criminelen. Toegang tot een botnet wordt niet zozeer bepaald door technische kennis, maar door de prijs die ervoor moet worden betaald. Sterke concurrentie tussen makers van botnets zorgen ervoor dat botnets tegen lage prijzen beschikbaar zijn.

Bovengenoemde trends wijzen erop dat de dreiging van botnets naar alle waarschijnlijkheid zal toenemen. Het is voor iedereen – bij de overheid, in het bedrijfsleven en de consument - zaak hier alert op te zijn en te zorgen voor een adequate bescherming.