Terug-hacken als opsporingsmethode

Een juridische analyse van de terug-hack praktijk van Justitie in relatie tot het privacyrecht naar aanleiding van de Bredolab ontmanteling

M.E. Koning

September 2011

Terug-hacken als opsporingsmethode

Een juridische analyse van de terug-hack praktijk van Justitie in relatie tot het privacyrecht

g van de Bredolab ontmanteling

Universiteit van Amsterdam - Instituut voor Informatierecht

Masterscriptie Informatierecht 2011

Begeleider: prof. dr. N.A.N.M. van Eijk

INHOUD

Afkortingen V
Inleiding 1
Hoofdstuk 1 Casus Bredolab 3
1.1 Kwantitatief en kwalitatief gebruik ICT-systemen 3
1.2 Cybercriminaliteit 4
1.3 Botnetbestrijding door Justitie 5
1.3.1 Bredolab botnet: technische specificaties 6
1.3.2 Bredolab botnet: ontmanteling 8
1.4 Terug-hacken en Bredolab 13
Hoofdstuk 2 Terug-hacken en privacy 14
2.1 Terug-hacken en inmenging 14
2.1.1 Inmenging en verdachte 18
2.1.2 Inmenging en slachtoffers 19
2.2 Criteria artikel 8 EVRM 20
2.3 Terug-hacken verdachte getoetst 22
2.3.1 Relevante nationale wetgeving 22
2.3.2 Toetsing 25
2.4 Terug-hacken slachtoffers getoetst 28
2.4.1 Relevante nationale wetgeving 28
2.4.2 Toetsing 32
2.4.3 Toetsing toekomstig terug-hacken slachtoffers 34
Tussenconclusie 37
Hoofdstuk 3 Terug-hacken en de rechtstaat 38
3.1 Opsporingsdiensten en rechtstatelijke binding 38
3.2 Terug-hacken voor andere doelen 41
Conclusie 42
Verklarende woordenlijst 44
Bijlage I Beschrijving Malware: Botnet 48
Bijlage II Botnet schema 55
Bijlage III Relevante Wetgeving Paragraaf 2.3.1 56
Bijlage IV Parlementaire ontwikkelingen terug-hack bevoegdheid. 58
Bronnen 60

AFKORTINGEN

AIVD: Algemene Inlichtingen- en Veiligheidsdienst

CBS: Centraal Bureau voor de Statistiek

CERT: Computer Emergency Response Team

DDoS: Distributed Denial of Service

DNR: Dienst Nationale Recherche

EHRM: Europees Hof voor de Rechten van de Mens

EVRM: Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden

Gw: Grondwet

ICT: Informatie- en communicatietechnologie

IRC: Internet Relay Chat-channel

KLPD: Korps Landelijke Politie Diensten

NFI: Nederlands Forensisch Instituut

NHTU: Nationale High Tech Crime Unit

OM: Openbaar Ministerie

OvJ: Officier van Justitie

Polw: Politiewet 1993

Sr: Wetboek van Strafrecht

Sv: Wetboek van Strafvordering

THTC: Team High Tech Crime

Tw: Telecommunicatiewet

VPN: Virtual Private Network

Wbp: Wet bescherming persoonsgegevens

Wet RO: Wet op de Rechterlijke Organisatie

WODC: Wetenschappelijk Onderzoek- en Documentatiecentrum

INLEIDING

Eind augustus 2010 lijkt de herfst vroeg in te vallen. Het is koud en regenachtig. De ambtenaren van de High Tech Crime Unit van het Korps Landelijke Politie Diensten (KLPD) merken daar echter weinig van. Dag in dag uit zitten zij aan het beeldscherm gekluisterd te speuren naar cybercriminelen. Boeven die zich schuil houden achter namen als Dark Dante, Atata en Black_Tapir.

De cybercrime speurders weten zich dagelijks geconfronteerd met de ongelijke positie in kennis en capaciteit tussen zichzelf en de criminelen. In de strijd voor een rechtvaardige samenleving ervaren zij het recht niet aan hun zijde. In de ogen van de agenten ontbreekt het aan passende bevoegdheden om deze aan de maffia gelieerde veelplegers aan te pakken. Hopende op een zaak waarmee zij de publieke opinie en Den Haag voor zich kunnen winnen speuren ze gestaag verder, tot de dagelijkse routine abrupt wordt doorbroken. Aan de telefoon is de security officer van één van Europa's grootste datacenters. Deze nodigt het Team uit om te komen kijken naar 'verdacht verkeer' in zijn datacenter, waarschijnlijk van het mothership van een groot internationaal botnet. De security officer is bereid de politie de kans te geven de criminelen achter het botnet op te sporen alvorens de stekker uit de servers te trekken. De cyberagenten geloven hun oren niet. Dit is de zaak waar ze al jaren van droomden.

Bovenstaande is gebaseerd op het waargebeurde verhaal van het Bredolab botnet, eind oktober 2010 door de Nederlandse politie ontmanteld. Deze ontmanteling heeft veel stof doen opwaaien omdat de gehanteerde opsporingsmethode door sommigen als dubieus en schokkend zijn ervaren.[1] De verklaringen in de pers van de bij de ontmanteling betrokken partijen waren tegenstrijdig. Zo meldde de een dat het botnet door de politie was overgenomen en dat via het netwerk een waarschuwing naar de slachtoffers was gestuurd, terwijl de ander dit in alle toonaarden ontkende.[2]

Indien de botnet servers zijn overgenomen, heeft de politie feitelijk gehackt: dan heeft zij een server iets anders laten doen dan waar deze oorspronkelijk voor ingericht is. In de pers en in

1 Zie bijvoorbeeld de reactie van Ot van Daalen, directeur van digitale burgerrecht organisatie Bits of Freedom:
webwereld.nl> politie over de schreef bij botnet ontmanteling

2 Ronald Prins van ingehuurd beveiligbedrijf Fox IT geeft aan dat het botnet was overgenomen:
webwereld.nl> politie over de schreef bij botnet ontmanteling
Woordvoerder van het landelijk parket van het Openbaar Ministerie ontkent:
webwereld.nl> politie ontkent terughacken bredolab bots

wetenschappelijke artikelen zijn dergelijke handelingen van opsporingsdiensten aangeduid met de term 'terug-hacken'.[3] In deze scriptie verwijst terug-hacken naar het op elektronische wijze heimelijk toegang verschaffen, via een externe verbinding, in een geautomatiseerd werk of netwerk.[4]

Opsporing gaat vaak gepaard met inmenging op het privacyrecht. Door het effect van opsporing en beëindiging van strafbare feiten op fundamentele rechten is het van belang dat heldere bevoegdheden worden geformuleerd en dat deze met waarborgen omkleed zijn.
Deze scriptie onderzoekt in hoeverre terug-hacken vanuit het privacyrecht bezien een gelegitimeerde opsporingsmethode is. Voor de positionering in het maatschappelijk debat is de Bredolab botnet ontmanteling onderzocht.

Interviews zijn afgelegd met betrokkenen van de ontmanteling: Officier van Justitie Lodewijk van Zwieten van het Landelijk Parket bij het Openbaar Ministerie, verantwoordelijk voor de vervolging van cybercrime; Alex de Joode, security officer bij LeaseWeb hosting provider; Ronald Prins, directeur van cybersecuritybedrijf Fox IT. Met Dave Woutersen van GOVCERT.NL heeft een mailwisseling plaatsgevonden.

In het eerste hoofdstuk wordt de casus Bredolab geschetst. De rol van ICT-systemen en cybercriminaliteit zal kort worden weergegeven. Daarna worden de technische specificaties van het Bredolab botnet uiteengezet en de ontmanteling beschreven. Aan de hand van een feitenreconstructie zal worden bezien of sprake is geweest van terug-hacken.
In hoofdstuk twee wordt de casus getoetst aan het privacyrecht aan de hand van de beschermingsomvang van artikel 8 EVRM. Hierbij zal de argumentatieopbouw van het Europees Hof voor de Rechten van de Mens worden aangehouden.
In het laatste hoofdstuk wordt de houding van opsporingsdiensten naar rechtstatelijke binding bekeken en zullen enkele niet noodzakelijk juridische observaties worden gedaan.

---

3 Zie bijvoorbeeld: webwereld.nl> *pvda politie moet hackers kunnen terug hacken* en J.J. Oerlemans, 'Conceptwetsvoorstel Computercriminaliteit III: Onzorgvuldige wetgeving?', *Informatiebeveiliging*, nr. 4 2011 p. 8-11.

4 Terug-hacken kan bijvoorbeeld door gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid. Daartoe kan zonder weet van de gebruiker eerst de fysieke controle over het werk verkregen zijn.Of op afstand worden binnen gedrongen, door bijvoorbeeld tussenkomst van internet. Definitie deels ontleend aan: J. Boek, 'Hacken als opsporingsmethode', *Nederlands Juristenblad* 2000, nr. 11.

HOOFDSTUK 1 CASUS BREDOLAB

Dit hoofdstuk geeft een beschrijving van ontwikkelingen in het gebruik van ICT-systemen.
De prominente rol van ICT-systemen in het privéleven wordt beschreven aan de hand van kwantitatieve en kwalitatieve indicatoren. Tevens wordt het gebruik van ICT-systemen voor criminele doeleinden geschetst. Aan de hand van de Bredolab botnet ontmanteling wordt ingegaan op het antwoord van Justitie op cybercriminaliteit en wordt de mogelijke toepassing van terug-hacken als opsporingsmethode onderzocht.

1.1 KWANTITATIEF EN KWALITATIEF GEBRUIK ICT-SYSTEMEN

Vanaf de negentiende eeuw is de relatie tussen mens en techniek in Europa voortdurend inniger geworden. Nieuwe producten worden geïntroduceerd als bevrijder van tijd- of geldrovende bezigheden, waarna ze binnen afzienbare tijd de nieuwe standaard vormen.[5] Leve de vooruitgang. Ditzelfde geldt voor ICT-systemen. Met name de toegang tot het internet heeft ertoe bijgedragen dat het gebruik van computers is geïntensiveerd, waardoor het een kwalitatief belangrijk communicatiemiddel is geworden. Deze ontwikkeling is te vergelijken met die van de telefonie.[6] Karin Spaink beschrijft in: *Het huis uit, de wereld in: een kleine telefoongeschiedenis* hoe de telefoon in vijfentwintig jaar van een formeel communicatiemiddel op een tochtige gang is veranderd in "*ons aller-intiemste communicatiemiddel […], meer dan ooit verweven met onze alledaagse, huiselijke of juist vertrouwelijke activiteiten en gevoelens.*"[7] Bankieren, winkelen, studeren, vrijen, solliciteren en communiceren in vele varianten van intimiteit en vertrouwelijkheid en zowel privé als zakelijk: het vindt allemaal plaats op het internet. Intensief is ook het gebruik van sociale netwerken, waardoor deze over een schat aan persoonlijke informatie beschikken. Foto's, video's, interesses, loopbaan, locatiegegevens en relaties zijn, afhankelijk van privacyinstellingen, beperkt of vrij beschikbaar op het internet. Computers zelf beschikken over een nog grotere schat aan informatie, omdat deze ook de niet online geplaatste bestanden bevatten. Agenda's, dagboeken, post en vele andere persoonlijke gegevens zijn daar opgeslagen.

5 J. Gackenbach & E. Ellerman 1998.
6 B. Wilson 2002.
7 K. Spaink 2010, p. 16.

In kwantitatieve zin is het gebruik van ICT-systemen ook fors toegenomen. Van de eerste personal computers moesten de bestanden, bij gebrek aan een harde schijf, worden opgeslagen op floppy´s van 110 kilobyte.[8] De opslagruimte van de computer voor deze scriptie is 2,6 miljoen maal groter dan deze eerste floppy. De randapparatuur van het wereld wijde web bevatte in mei 2009 500 exabyte aan opgeslagen informatie.[9] Cijfers van het Centraal Bureau voor de Statistiek uit 2010 geven aan dat 92% van de totale Nederlandse bevolking thuis internet gebruikt.[10] Uit een recent onderzoek van de London School of Economics and Political Sience blijkt dat 87% van de Nederlandse kinderen tussen de 13 en 16 jaar gebruik maakt van sociale netwerken.[11] Bij de social network site Hyves.nl hebben 9,3 miljoen Nederlanders een profiel. Op Hyves.nl worden gemiddeld 815.000 foto's per dag geüpload.[12] Deze cijfers maken het aannemelijk te veronderstellen dat zowel de convergerende technologische ontwikkeling als het gebruik van ICT-systemen in de nabije toekomst nog meer zal toenemen.

1.2 CYBERCRIMINALITEIT

De toename van het computergebruik heeft een belangrijke keerzijde. Door het uitdijende scala aan applicaties en software en door de grote interconnectiviteit zijn kwetsbaarheden in de infrastructuur ontstaan. Deze worden gebruikt voor cybercriminaliteit. In de literatuurinventarisatie *High-tech crime, soorten criminaliteit en hun daders* van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) worden vier voordelen van cybercriminaliteit ten opzichte van conventionele criminaliteit aangestipt: (a) de barrières van tijd en ruimte zijn verdwenen, waardoor binnen enkele seconden direct contact mogelijk is met personen overal ter wereld; (b) het bereik ten opzichte van potentiële slachtoffers is groot (tegen minimale investering); (c) men geniet een zekere vorm van anonimiteit (met de mogelijkheid om een andere identiteit aan te nemen); (d) activiteiten kunnen relatief gemakkelijk en veelvuldig worden herhaald of gelijktijdig plaatsvinden, waardoor zelfs kleine opbrengsten per delict tot

8 Zie voor de geschiedenis van de floppy en haar rol in bestanden delen: F. Miller, *Floppy Disk*, Beau Bassin: Alphascript Publishing 2010.
9 guardian.co.uk> digial content expansion.
10 *ICT gebruik van personen naar persoonskenmerken*, Centraal Bureau voor de Statistiek, Gewijzigd op 26 oktober 2010.
11 *Social Networking, Privacy and Age, EU Kids online*, London School of Economics. S. Livingstone e.a. april 2011.
12 http://www.hyves.nl/over/facts/ laatst bezocht: 28 augustus 2011.

grote winsten kunnen leiden.[13]

Hier moet mijns inziens de relatief lage pakkans aan toegevoegd worden. [14] Ook de ontwikkeling van cybercriminaliteit is onderhevig aan groei in kwalitatieve en kwantitatieve zin. Voor een encyclopedisch overzicht van verschillende vormen, gehanteerde technieken en maatschappelijke aspecten van cybercriminaliteit wordt de *Encyclopedia of Cybercrime* van Samuel C. McQuade III aangeraden. [15] Voor een uitgebreid overzicht van verschillende soorten cybercriminaliteit en daders in Nederland wordt verwezen naar het bovengenoemde WODC rapport.[16]

1.3 BOTNETBESTRIJDING DOOR JUSTITIE

Deze scriptie spitst zich toe op het Justitiële antwoord op de malware vorm: het botnet. In bijlage I is een uitvoerige beschrijving gegeven van de techniek en exploitatie van botnets. Botnets krijgen in 2008 voor het eerst aandacht van de politie. In het *verslag van het onderzoek voor het nationaal dreigingsbeeld van 2008* van de Korps Landelijke Politie Diensten (KLPD) wordt de dreiging van botnets bij phishing genoemd.[17] In augustus 2008 ontmantelde de politie een botnet uit Friesland.[18] Daarna wordt het op strafvorderlijk handhavingsgebied stil, tot de ontmanteling van het Bredolab botnet alom in het nieuws wordt medegedeeld.[19]

---

13 *High-tech crime, soorten criminaliteit en hun daders*, WODC 2008. p.31.

14 Zie ook het *Nationaal Trendrapport Cybercrime en Digitale veiligheid, 2010.* De lage pakkans wordt in trend 1 benoemd.

15 Samuel C. McQuade III 2008.

16 *High-tech crime, soorten criminaliteit en hun daders*, WODC 2008.

17 *Actualisering van dreigingen uit 2004, verslag van het onderzoek voor het dreigingsbeeld van 2008*, KLPD dienst IPOL.

18 Nieuwsbericht over de ontmanteling van het Sneker botnet: webwereld.nl>nederlandse primeur politie waarschuwt botnetslachtoffers. De wijze waarop dit botnet is ontmanteld valt buiten het bereik van deze scriptie.

19 Zie voor verschillende online mediaberichten over de ontmanteling:
telegraaf.nl> Groot crimineel computernetwerk opgerold.
volkskrant.nl> gigantisch crimineel computernetwerk opgerold.
webwereld.nl> politie legt nederlands botnet plat.

1.3.1 BREDOLAB BOTNET: TECHNISCHE SPECIFICATIES

Alvorens op de ontmanteling in te gaan wordt de werking van Bredolab beschreven aan de hand van de infectiewijze, functionaliteit, doeleinden, businessmodel en cijfers.[20] In bijlage II is de Bredolab infrastructuur schematisch weergegeven.

Bij het botnet waren de volgende actoren betrokken: een dedicated hosting provider, een dedicated hosting afnemer, de botherder, afnemers van de botherder en slachtoffers. De zes command en control servers van Bredolab stonden in Nederland bij dedicated hosting provider LeaseWeb te Haarlem. LeaseWeb verhuurde in totaal 143 servers aan, zoals later bleek, een cybercriminele afnemer. De vermoedelijke botherder van Bredolab is een 27-jarige Armeniër, die zich destijds in Rusland en Armenië ophield. De botherder had toegang tot 13 tot 18 LeaseWeb servers. Alle onderdelen van het Bredolab botnet draaiden op deze servers, waaronder zes command en control servers. Een reeks onbekende afnemers van de botherder maakte gebruik van zijn diensten.

De botherder maakte gebruik van drive-by download infecties. Op meer dan 1200 websites had hij exploits geplaatst om beveiligingslekken te detecteren. Via een lek werd een trojan downloader op de computer van het slachtoffer geplaatst om de volledige Bredolab malware te downloaden en installeren. Na succesvolle installatie behoorde de computer tot het Bredolab botnet. Voor de verspreiding van exploits hanteerde de botherder twee methodes. Ten eerste maakte hij gebruik van malvertising. De botherder hackte de servers van online advertentiebedrijven en plaatste Bredolab exploits in bestaande legitieme advertenties. Ten tweede plaatste hij exploits op websites van reeds gemaakte slachtoffers.[21] Op deze manier groeide het botnet exponentieel, zonder al te veel inspanningen van de botherder zelf. Ten tijde van de ontmanteling had hij meer dan 11.000 gestolen credentials op zijn servers op voorraad.

---

20 De in deze paragraaf verwerkte informatie is hoofdzakelijk uit interviews afkomstig van de bij de ontmanteling betrokken personen: OvJ Lodewijk van Zwieten, van het Landelijk Parket OM; Alex de Joode, security officer bij LeaseWeb hosting provider; Ronald Prins, directeur van cyber securitybedrijf Fox IT; met Dave Woutersen van GOVCERT.NL heeft een mailwisseling plaatsgevonden. Op niet voor de juridische analyse relevante punten is informatie aangevuld uit de media.

21 Hierbij kan onder andere gedacht worden aan facebook- en twitterpagina's.

De Bredolab malware bevatte twee functionaliteiten: een keystroke logger en een download platform. De keystroke logger zond de gestolen credentials naar de command en control server. Via de tweede functionaliteit, het download platform, installeerde de botherder malware op de botclients ten behoeve van zijn afnemers. Een botclient kon verschillende malware gelijktijdig draaien. Zo werden bijvoorbeeld gelijktijdig gegevens van het slachtoffer afgetapt, man-in-the-middle- en DDoS-aanvallen uitgevoerd en een grote hoeveelheid spam verstuurd. [22] Afnemers plaatsen hun bestellingen in de Bredolab webwinkel. De wensen van de afnemer konden vrij nauwkeurig worden gedefinieerd, door opties als werelddeel, land, besturingssysteem, etc. De webwinkel was moeilijk bereikbaar voor de reguliere internet gebruiker, maar binnen het cybercriminele circuit welbekend. Bredolab werd aangeboden voor 800 dollar per bestelling. Uit de klantendatabase bleek dat sinds juli 2009 de botherder 821 opdrachten aan de botclients had gegeven.

De botherder had 330 verschillende soorten malware op voorraad. Het Bredolab botnet kende beperkte plug-in mogelijkheden waardoor, naargelang de aard van de bestelling, andere malware op de botclient moest worden geïnstalleerd. De aan de slachtoffers onttrokken gegevens werden direct door de botclients naar de afnemers gestuurd, zonder tussenkomst van de Bredolab command en control servers.

Voor de toegang tot de command en control servers maakte de botherder middels een VPN verbinding contact met een communicatie server. De botclients waren mondiaal verspreid. De communicatie tussen de botclients en de botherder was geëncrypteerd en werd met tussenkomst van een aantal proxy servers verstuurd. Het IP-adres van de command en control server was in de broncode van de botclients opgenomen. In dit inmiddels verouderde systeem konden de botclients niet met elkaar in contact komen.[23]

De eerste Bredolab exploits zijn in mei 2009 opgemerkt door een antivirus bedrijf.[24] In september 2010 werden drie miljoen geslaagde infecties geteld. Dit is inclusief het aantal infecties van malware die door de botherder in opdracht van zijn afnemers op de botclients is geplaatst. Het

22 De Bredolab verdachte Georgy A. wordt door de Russische autoriteiten in verband gebracht met Igor G. Laatstgenoemde wordt verantwoordelijk gehouden voor het versturen van twintig procent van de spam-berichten wereldwijd per dag. sunbeltsoftware.com> arrested Bredolab mastermind also connected to spamit.com

23 Zie ook het artikel *Trend Micro: BREDOLAB Simple but Effective.*

24 *A Trend Micro White paper Bredolab, Bredolab's sudden rise in prominence.* David Sancho, October 2009.

werkelijke aantal botclients is niet bekend.[25] In de media claimden de opsporingsdiensten een botnet te hebben ontmanteld, dat vanaf 143 servers werd bestuurd en ten minste 30 miljoen slachtoffers had gemaakt.[26]

1.3.2 BREDOLAB BOTNET: ONTMANTELING

De ontmanteling van het Bredolab botnet door het KLPD heeft een hoop stof doen opwaaien. Uit verklaringen van een aantal bij de ontmanteling betrokken partijen kon namelijk worden afgeleid dat door het KLPD was terug-gehackt. Bovendien werden zelfgecreëerde persmomenten door de opsporingsdiensten gebruikt om te pleiten voor ruimere online opsporingsbevoegdheden, waaronder de terug-hack bevoegdheid.[27] Op online fora werd over het algemeen zeer kritisch gereageerd op zowel de ontmanteling als op de wenselijkheid van een terug-hack bevoegdheid.[28] Naar aanleiding van deze polemiek ontkende het KLPD te hebben terug-gehackt, maar benadrukte wel de wenselijkheid van de bevoegdheid hiertoe.[29] De komende alinea's beogen de terug-hack actie op te helderen.

Bredolab in het vizier

LeaseWeb is in 2010 haar 'Community Outreach Project' gestart. De website van LeaseWeb vermeldt dat zij: "*gratis server capaciteit en bandbreedte ter beschikking stelt aan bedrijven die, samen met LeaseWeb, de veroorzakers van cybercrime monitoren, identificeren en aanpakken.*" Op deze wijze hoopt zij beter zicht te krijgen op de aanwezigheid van cybercriminaliteit binnen het eigen netwerk en kunnen geïnfecteerde websites sneller worden geblokkeerd. [30] In augustus 2010 meldde een deelnemer van het Community Outreach Project dat een cluster LeaseWeb servers mogelijk het mothership van een botnet vormden. In de dagen na de melding

25 Het naar buiten gebrachte aantal botclients van 30 miljoen is een extrapolatie van 3 miljoen geobserveerde infecties in een maand. Deze infecties betroffen de Bredolab infecties maar ook de opdrachten van de botherder aan de individuele bots. De logfiles op de command en control servers gingen 10 maanden terug. De berekening 10*3 miljoen is gemaakt. Dit is een uiterst onbetrouwbare berekening waarmee de exponentiele groei die dit soort botnets doormaken is genegeerd. Zie in deze lijn ook de blog van Michel van Eeten: http://blog.internetgovernance.org/blog/_archives/2010/11/1/4669564.html

26 om.nl> persbericht Bredolab

27 Zie bijvoorbeeld de uitzending van het tv-programma nieuwsuur op de dag van de ontmanteling: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html

28 Zie bijvoorbeeld: http://webwereld.nl/article/comments/id/67601#

29 webwereld.nl> politie ontkent terughacken bredolab bots

30 Zie voor een uitgebreide uitleg over het community outreach programma de website van LeaseWeb: http://blog.leaseweb.com/2010/08/31/leaseweb-offers-free-web-hosting-to-fight-cybercrime/

heeft LeaseWeb onderzoek gedaan naar servers binnen het eigen netwerk en geconstateerd dat hier waarschijnlijk het Bredolab botnet bestuurd werd. De dedicated hosting afnemer van de verdachte servers stond bij hen bekend als mogelijke cyber crimineel.[31] LeaseWeb besloot alvorens stappen tegen Bredolab te nemen, tot een melding van het verdachte verkeer bij het Team High Tech Crime (THTC).[32] Het THTC valt onder de Dienst Nationale Recherche (DRN) van het KLPD. De DNR is belast met de bestrijding van zware, georganiseerde criminaliteit die qua groepering of aard een landelijk of internationaal karakter heeft.[33] Het gezag over de DNR wordt uitgeoefend door het Landelijk Parket van het Openbaar Ministerie (OM).[34]

Project Tolling

Het HTCT ging tot actie over. Met het uiteindelijk doel Bredolab te ontmantelen werd Project Tolling opgestart.[35] Deelnemende partijen waren het OM, het THTC, GOVCERT.NL, het NFI, LeaseWeb, Kaspersky antivirus lab en Fox IT. De partijen beoogden het botnet effectief neer te halen en zo een klap uit te delen aan cybercriminelen, opdat deze zich bewust worden dat Justitie wel degelijk in staat is dit soort criminaliteit tegen te gaan. Partijen hoopten aan de internationale internet gemeenschap het signaal af te geven dat "*cybercriminelen Nederland in de toekomst*

31 Het dedicated hosting contract voor de 143 servers was afgesloten op naam van John Datri. Uit onderzoek bleek LeaseWeb opgericht in 1997 en John Datri begin jaren negentig overleden in de Amerikaanse staat Florida en zodoende postuum slachtoffer van identiteitsfraude. De daadwerkelijke afnemer van de dedicated hosting servers moet worden gezocht in het criminele circuit. Deze crimineel verhuurde servers door aan andere criminelen. Deze kwam in 1/3 van de NAW-verzoeken van Justitie aan LeaseWeb voor. Al voor de ontdekking van zijn valse identiteit had de politie meerdere malen zijn NAW-gegevens opgevraagd.

32 Deze melding wijkt af van de gebruikelijke handelswijze van LeaseWeb bij het bestrijden van botnets. In de algemene voorwaarden van LeaseWeb is het beleid toegelicht. Normaliter wordt na het signaleren van mogelijk strafbare feiten melding gemaakt aan de afnemer Indien deze niet of niet afdoende reageert sluit LeaseWeb de servers van het internet af. Acceptable Use Policy Leaseweb en Algemene voorwaarden (V4.5) LeaseWeb (geldig op 17-8-2011).

33 *Kamerstukken II* 2002/03, 28 250, nr. 4 p. 2.

34 C. Cleiren e.a. 2009 p. 2273.

35 LeaseWeb is als één van de grootste datacenters in Europa betrokken bij *project Taurus,* geïnitieerd door het THTC en het OM. Deelnemende partijen beogen middels publiek privaat overleg tot een betere informatie positie voor de bestrijding van botnets te komen. In de loop van 2010 werden een aantal testmodellen gemaakt. Aanvankelijk werd gekozen voor het monitoren van meer dan 700 IRC-based botnets. Na de Bredolab melding besloten het KLPD en het OM de focus te verleggen en het onderzoek naar dit botnet groots aan te pakken. Vaste partijen van Project Taurus zijn: het THTC van het KLPD, het OM, Europol, de Duitse Federale Politie (BKA), de Amerikaanse Federal Bureau of Investigation (FBI), de United States Secret Services (USSS), de Russische Federale veiligheidsdienst (FSB vroeger KGB), Secret Service Oekraïne (SBU), het Nederlandse computer emergency response team GOVCERT.NL, het Nederlands Forensisch Instituut (NFI), de Onafhankelijke Post en Telecom Autoriteit (OPTA), Stichting Internet Domein Registratie (SIDN), de Universiteit Aacken, regionale internet coördinator RIPE, Cybercrime analist ShadowServer, virus labs Qnet Labs, Norman en Kaspersky, cyber security bedrijven VeriSign en Fox-IT en hosting provider Leaseweb.

beter links kunnen laten liggen".[36]

Effectieve botnet ontmanteling

Project Tolling besloot op drie gebieden actie te ondernemen en te zorgen dat deze acties gelijktijdig dan wel snel op elkaar volgend werden uitgevoerd. Op deze manier werd getracht te voorkomen dat het botnet elders zou worden overgenomen. De actie punten waren:

1. Het aanhouden van de verdachten.
2. Het verbreken van het communicatiekanaal tussen de command en control servers en de botclients.
3. Het waarschuwen van de slachtoffers voor de aanwezigheid van malware op hun computer.

Voorbereiding op de drie actie gebieden

Alle 143 gehuurde servers van de dedicated hosting afnemer zijn voor onderzoek in beslag genomen. Het KLPD sloot met LeaseWeb een overeenkomst tot bewaring van strafrechtelijk in beslag genomen goederen, waarin werd afgesproken dat het beheer van de servers bij LeaseWeb zou blijven en dat zij zelf geen actie tegen het botnet zou ondernemen: de afnemers zouden van de opsporing niets mogen merken. Vervolgens werd het verkeer van en naar tien vermoedelijke Bredolab servers afgetapt. De datastroom werd naar het hoofdkantoor van het KLPD geleid, waar het met behulp van Fox IT is geanalyseerd.

In de eerste plaats leverde het onderzoek weinig resultaat op, omdat de hele infrastructuur geëncrypteerd was. De encryptie was echter niet toegepast op een op de pc van de botherder opgeslagen cookie. Bij het opzetten van de VPN-verbinding werd deze cookie met het wachtwoord van de botherder verzonden naar de getapte communicatie server. Dit wachtwoord verschafte de opsporingsdiensten toegang tot de VPN verbinding, waar de overige toegang- en decryptiesleutels werden afgevangen. De handelingen van de botherder konden zo op de servers worden onderzocht en gemonitord. Op deze manier werd gedurende ongeveer tien weken over de schouder van de botherder meegekeken. De identiteit van de verdachte en de kenmerken van

36 Interview Ronald Prins. 23-6-2011, 14:00 uur. Olof Palmestraat 6, Fox IT.

Bredolab werden toegevoegd aan het procesdossier. [37]

Daarnaast bleek de aanwezigheid van een tweede botnet. De command en control servers van dit botnet stonden bij hosting provider OVH in Frankrijk en waren via de LeaseWeb communicatie server te bereiken. Het Franse botnet bestond uit minimaal 220.000 bots. Het OM diende bij de Franse opsporingsautoriteiten een rechtshulp verzoek in om de internetverbinding van de servers op een tevoren overeengekomen tijdstip te verbreken.

Uit berichten op de facebook pagina van verdachte kon het THTC opmaken dat deze op vrijdag 22 oktober 2010 voor een dancefeest naar Nederland zou komen. De actie *(aanhouden, verbreken verbinding en waarschuwen slachtoffers)* werd gepland voor deze datum.

Aanhouden verdachte

Het was de bedoeling verdachte bij aankomst op Schiphol aan te houden. Hij kwam echter niet opdagen. Daarop werd de actie uitgesteld naar de maandag en een internationaal arrestatiebevel uitgevaardigd door het OM. Verdachte is uiteindelijk aangehouden in de nacht van dinsdag 26 oktober 2010 op het vliegveld van Jerevan in Armenië. Het uitleveringsverzoek van Nederland is door Armenië niet ingewilligd en verdachte wordt in eigen land berecht.

Verbreken verbinding

Op maandag 25 oktober 2010 werd voor de ontmanteling in de directiekamer van LeaseWeb de technische set-up geïnstalleerd door de specialisten van Fox IT, het NFI, het THTC en LeaseWeb.

Voor het verbreken van het communicatiekanaal tussen de command en control servers en de botclients zou het afdoende zijn geweest om de servers uit te zetten of de internet verbinding te verbreken. Met het oog op het waarschuwen van de slachtoffers kozen het THTC en het OM echter voor een andere aanpak. Met behulp van de andere partijen kaapte het KLPD het botnet van binnenuit en kreeg op deze manier de controle in handen.

De kaping werd onmiddellijk door de verdachte opgemerkt, waardoor hij nog tijdens de operatie

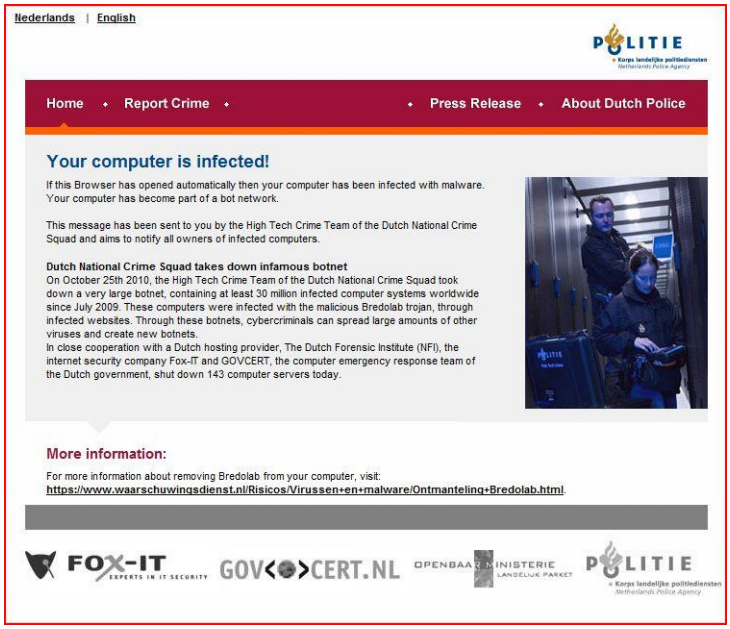
37 Uit de datastroom was de facebook-account van de vriendin van verdachte gebleken. Op een onbewaakt moment logde zij in via de VPN-verbinding met de getapte communicatie server, waardoor haar account gegevens en identiteit bekend raakten bij de het KLPD. Onderzoek leidde naar de vermoedelijke botherder.

het botnet probeerde terug te krijgen.[38] Toen deze poging faalde gaf hij zijn tweede botnet opdracht tot een DDoS-aanval op de netwerk infrastructuur van LeaseWeb.

Daar de Franse opsporingsdienst te laat reageerde op het verzoek de internetverbinding te verbreken, kon de DDoS-aanval plaatsvinden tot de door de botherder voorgeprogrammeerde eindtijd voor het commando "stop" was bereikt. De netwerk architect van LeaseWeb wist de aanval echter binnen korte tijd om te leiden, waardoor de botnet ontmanteling kon worden voortgezet.
Het KLPD verwierf controle over alle zes command en control servers, waarna LeaseWeb op last van het OM de internetverbinding verbrak van de overige 137 in beslag genomen servers.[39]

Waarschuwen slachtoffers

De slachtoffers werden gewaarschuwd via het botnet zelf. Door een opdracht vanuit de command en control servers haalde de botclient een executable file op en installeerde die op de computer. Dit bestand leidde, zodra de default brouwser geopend werd, het slachtoffer naar een waarschuwingspagina.[40] De waarschuwing zag er als volgt uit:[41]



38 Naar alle waarschijnlijkheid ging verdachte er in de eerste plaats vanuit dat hij te maken had met ordinaire botnet-hijack van een andere cybercrimineel en niet van de Nederlandse opsporingsautoriteiten.
39 Wat met deze groep servers is gebeurd, valt buiten het bereik van deze scriptie.
40 http://teamhightechcrime.nationale-recherche.nl/nl_infected.php.
41 De waarschuwing is ook in het Nederlands verspreid.

Deze website meldde de malware besmetting, en gaf een korte uitleg over Bredolab en project Tolling. Tevens waren er links naar het OM, het aangifte programma van de KLPD en naar de waarschuwingsdienst. Deze laatste bood een specifieke Bredolab desinfectie-patch. [42] Daarnaast hebben de opsporingsdiensten informatie betreffende IP-adressen, gestolen credentials en gehackte domeinnamen door GOVCERT.NL wereldwijd laten verspreiden, om ook via de CERT's en ISP's de slachtoffers te waarschuwen.

1.4 TERUG-HACKEN EN BREDOLAB

Analyse van het bovenstaande feitenkader brengt mijns inziens de constatering dat bij de Bredolab ontmanteling op twee momenten sprake is geweest van terug-hacken. De handelingen raakten zowel de verdachte als de slachtoffers van het botnet.

In de eerste plaats zijn de opsporingsdiensten middels afgevangen toegang- en decryptiesleutels op de servers van de verdachte binnengedrongen, waardoor ongeveer tien weken heimelijk de handelingen van verdachte zijn gemonitord en onderzocht. Hier hebben zij tevens voldoende informatie vergaard om de servers succesvol van binnenuit over te nemen.
In de tweede plaats zijn de servers daadwerkelijk gekaapt en werd de controle over de command en control servers en zo het botnet overgenomen. Hierdoor verwierven de opsporingsdiensten volledige toegang tot en controle over de computers van de slachtoffers en kon een bestand hieraan worden toevoegd.

42 https://www.waarschuwingsdienst.nl/Risicos/Virussen+en+malware/Ontmanteling+Bredolab.html / De desinfectie patch was in samenwerking met Kaspersky antivirus lab ontwikkeld voor Bredolab.

HOOFDSTUK 2 TERUG-HACKEN EN PRIVACY

Een juridische analyse van het terug-hacken bij de Bredolab ontmanteling in relatie tot het privacyrecht volgt in het komende hoofdstuk. Hierbij wordt onderzocht of ICT-systemen binnen de beschermingsomvang van het privacyrecht vallen. Vervolgens wordt onderzocht of terug-hacken een inmenging vormt op dit recht vormt. De geoorloofdheid van de inmenging wordt in het laatste deel van dit hoofdstuk onderzocht.

2.1 TERUG-HACKEN EN INMENGING

Over het algemeen wordt privacy gezien als een recht dat een individu kan aanwenden om zijn of haar privéleven af te schermen van anderen, inclusief de overheid.[43] Historisch gezien is de beschermingsomvang van het privacyrecht organisch gegroeid vanuit het huisrecht en de lichamelijke integriteit. Vanuit de kern van de fysieke privacy is een locatie-onafhankelijke privésfeer om de persoon heen ontwikkeld. Deze privésfeer is in twee aspecten te verdelen; de informationele en relationele privacy. De informationele privacy ziet toe op de rechten van het individu om de verwerking van persoonsgegevens te verhinderen, beperken of veranderen en verplicht tot zorgvuldige verwerking door personen of instellingen aan wie de persoonsgegevens zijn toevertrouwd.[44] De relationele privacy behelst het recht van de individu op selectieve contactlegging, met als meest extreme vorm het recht om met rust gelaten te worden.[45]

De grondwettelijke bescherming van het privacyrecht is vervat in artikel 10 Grondwet (Gw)[46]: *ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.* Bij de introductie van dit artikel achtte de wetgever het onvruchtbaar om een concrete omlijning van het privacybegrip te geven. Hij zag nadere invulling

43 E. Dommering, 2000 p. 25.

44 In Nederland is de Wet bescherming persoonsgegevens (Wbp) specifiek op deze informationele privacy toegespitst. Artikel 1 sub a Wbp definieert een persoonsgegeven als: *elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.*

45 E. Dommering 2000, p. 26 en E. Dommering, 'noot bij HR 9 januari 1987 Bespiede Bijstandsmoeder', *Computerrecht* 1987-2, p.114.
En ook: S. Warren & L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol. IV 15 December 1890, Nr.5.

46 *Grondwet voor het Koninkrijk der Nederlanden* van 24 augustus 1815 laatstelijk gewijzigd op 22 augustus 2008, Stb. 2008, 348.

van de term 'persoonlijke levenssfeer' als een taak van de rechter en gaf de toevoeging dat het begrip ruim dient te worden opgevat.[47]

In de bescherming van grondrechtelijke en fundamentele mensenrechten speelt de grondwet slechts een beperkte rol: het is de rechter verboden om internationale en nationale wet- en regelgeving te toetsen aan de grondwet, ex art. 120 Gw. Wel spelen grondrechtelijke bepalingen een rol bij de parlementaire totstandkoming van de wetgeving, al is deze in de praktijk vaak beperkt tot die van figurant.[48]

Het privacy-recht ligt verankerd in internationale mensenrechtelijke verdragen. Artikel 17 van het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten voorziet in de bescherming tegen willekeurige of onwettige inmenging in het privéleven. Artikel 7 van het Handvest van de Grondrechten van de Europese Unie[49] omschrijft haar privacy bepaling als volgt: *"Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie."* Deze bepaling toont grote overeenkomsten met artikel 8 lid 1 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM): *"Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie."* De preambule en art. 52 lid 3 jo. art. 53 van het Handvest van de Grondrechten van de Europese Unie erkent de positie en waarde die het EVRM heeft ingenomen in de bescherming van fundamentele mensenrechten en instrueert de lidstaten en de Europese Unie om hier zo nauw mogelijke aansluiting bij te zoeken.

In 1987 legde de Hoge Raad uit dat het privacyrecht in Nederland moet aansluiten bij ontwikkelingen over de grens en dat de inhoud mede moet worden bepaald door artikel 8 EVRM.[50]

Deze scriptie zal de beschermingsomvang van het privacyrecht behandelen aan de hand van dit artikel en de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM).

---

47 *Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties.*1976 p. 21 en *Kamerstukken II* 1978/79, 13 872, nr. 3 p. 40.
48 J. Peters 2003.
49 Handvest van de Grondrechten van de Europese Unie, 2000/C 364/01.
50 HR 9 januari 1987, *NJ* 1987, 928.

Artikel 8 EVRM luidt als volgt:

> Artikel 8 - Recht op eerbiediging van privéleven, familie- en gezinsleven
> 1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
>
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

Een strikte conceptuele scheidslijn tussen de drie begrippen - *privéleven, woning en correspondentie* - is door het EHRM in de uitspraak *Klass vs. Germany* opgeheven. [51] Het concept privéleven dekt mede de fysieke en psychologische integriteit.[52] In de zaak *Peck vs. The UK* benadrukt het Hof dat het recht op persoonlijke ontwikkeling en het aangaan en ontwikkelen van relaties met anderen en de wereld, ook in een publieke of formele context, wel degelijk onder artikel 8 EVRM kan worden beschermd. [53] In een reeks uitspraken heeft het EHRM geoordeeld dat een individu niet automatisch het recht op bescherming van zijn privéleven verliest als hij zijn persoonlijke eigendommen in een meer publieke omgeving brengt.[54] In veel zaken bij het EHRM is naast een inmenging op het respect voor privéleven ook een inmenging op het recht voor respect van de woning of correspondentie aangenomen.

In casu gaat het om ICT-systemen. De rol die deze vervullen en het gebruik voor persoonlijke ontwikkeling maken het goed verdedigbaar dat alle ICT-systemen onder de beschermingsomvang van het begrip privéleven uit art. 8 EVRM vallen. Het is aannemelijk dat een deel van de computers van de slachtoffers in woningen stonden en dat deze opgeslagen correspondentie bevatten.[55] Het begrip privéleven staat echter centraal in de verdere analyse van het recht op eerbiediging van de persoonlijke levenssfeer.

---

51 EHRM 6 september 1978, nr. *5029/71(Klass and others v. Germany).*
52 EHRM 22 juli 2003, nr. 24209/94 *(YF v. Turkey)*.ro. 33.
53 EHRM 16 december 1992, nr. 13710/88 *(Niemietz v. Germany)* en EHRM 28 januari 2003, nr. 44647/98 *(Peck v. the United Kingdom).*
54 Zie bijvoorbeeld EHRM 28 januari 2003, nr. 44647/98 *(Peck v. the United Kingdom).ro.* 57-63
55 Emails, chatberichten, concept brieven etc.

Het ontbreekt aan jurisprudentie betreffende het online toegang verschaffen of doorzoeken van ICT-systemen.[56] Het doorzoeken van harde schijven van verschoningsgerechtigden (meestal na inbeslagname) is wel meermaals onderwerp geweest in een geschil voor het EHRM.[57] Echter, bij het vaststellen van de inmenging en de aard hiervan (relevant voor de verdere weging van de criteria gegeven in lid twee van artikel 8 EVRM) wordt in dergelijke zaken terecht zwaar getild aan de bijzondere positie van verschoningsgerechtigden. Hierdoor blijft de vraag naar de aard van de inmenging bij het doorzoeken onbeantwoord.

Uit bovenstaande kan worden afgeleid dat het aan concrete aanknopingspunten binnen de rechtspraak van het EHRM ontbreekt. Terug-hacken is wel in de Duitse rechtspleging besproken in een zaak voor het Constitutioneel Hof.[58] Alhoewel het formeel rechtelijke kader van deze uitspraak afwijkt van de onderhavige casus, is het materieel rechtelijke vraagstuk van overeenkomstige aard. Hierdoor kunnen de overwegingen van het Bundesverfassungsgericht over het vaststellen van de inmenging en haar aard richting geven in de onderhavige casus. In de *Online Durchsuchung-uitspraak* stond de vraag centraal of het heimelijk op afstand doorzoeken van een ICT-systeem een geoorloofde opsporingsmethode is. Het antwoord op deze vraag werd gevormd door *het recht op integriteit en vertrouwelijkheid van ICT-systemen,* een afgeleide van het uit artikel 2 van de Duitse Grondwet voortvloeiende Algemeen Persoonlijkheidsrecht.[59] Met betrekking tot het vaststellen van de aanwezigheid en de aard van de inmenging oordeelt het Bundesverfassungsgericht dat uit het relevante gebruik van informatiesystemen ten behoeve van persoonlijkheidsontplooiing en uit de gevaren voor de persoonlijkheid die verbonden zijn aan dit gebruik, een nood tot grondrechtelijke bescherming volgt.[60] Vervolgens stelt het Bundesverfassungsgericht dat een computer waarschijnlijk meer dan enkel een bulk aan persoonsbetreffende informatie en communicatie bevat. Een derde die zich

56 Een uitvoerige reeks jurisprudentie van het EHRM betreft het aftappen van telefoongesprekken en het doorzoeken van woningen Bijvoorbeeld:
EHRM 25 maart 1998, nr 44787/98 *(Halford v. the United Kingdom).*
EHRM 16 februari 2000, nr. 27798/95 *(Amman v. Swiss).*
EHRM 24 april 1990, nr. 11801/85 *(Kruslin v. France).*
EHRM 24 april 1990, nr. 11105/84 *(Huvig v. France).*

57 EHRM 16 december 1992, nr. 13710/88 *(Niemietz v. Germany).* en EHRM 2 september 2008, Decision nr. 15301/04 *(Tamm v. Estonia).*

58 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07.

59 Zie voor een heldere Engelstalig inleiding tot het Duitse grondwettelijke recht: S. Michalowski & L. Woods, *German constitutional law. The protection of civil liberties*, Ashgate: Brookfield 1999.

60 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07. Ro. 181.

toegang verschaft tot een ICT-systeem, kan zich potentieel een uiterst groot en veelzeggend databestand verschaffen, zonder op verdere dataverzamelings- en dataverwerkingsmethoden te zijn aangewezen. Dergelijke toegang weegt vele malen zwaarder dan toegang tot afzonderlijke databestanden.[61]

2.1.1 INMENGING EN VERDACHTE

Hieronder zal het omschreven toetsingskader worden toegepast op het terug-hacken naar de verdachte.

De kwantitatieve en kwalitatieve ontwikkeling van het gebruik van ICT-systemen leidt ertoe dat geautomatiseerde werken en persoonlijke gegevens zich buiten de directe fysieke omgeving van de gebruiker en in een meer publieke omgeving kunnen bevinden.[62] Externe opslag- en werkruimte wordt aangeboden door derden, het gebruik van cloud-computing neemt snel toe.[63] Ondanks de afstand is het gebruik van het ICT-systeem hetzelfde. In casu gebruikte verdachte dedicated hosting servers. Deze stonden exclusief tot zijn beschikking.[64]

De fysieke afstand tussen gebruiker en ICT-systeem is niet van doorslaggevende aard, waardoor de servers mijns inziens onder de beschermingsomvang vallen van artikel 8 EVRM. Het heimelijk binnendringen van een dedicated hosting server staat daarom gelijk aan het binnendringen van een geautomatiseerd werk in de directe fysieke omgeving van de gebruiker.

De opsporingsdienst is middels de afgevangen toegang- en decryptiesleutels op de servers van de verdachte binnengedrongen en heeft ongeveer tien weken heimelijk de handelingen van verdachte gemonitord en onderzocht. Gezien het relevante gebruik van de informatiesystemen, het uiterst groot en veelzeggend databestand dat het KLPD tot haar beschikking kreeg, en het heimelijk monitoren is mijn inziens te stellen dat, door het terug-hacken, sprake is van een

61 Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07. Ro. 198-207.
62 Zoals de H-schijf binnen het UvA netwerk.
63 Bij virtualisering van een server heeft de gebruiker via internet toegang tot het besturingssysteem. Hij behoudt daarbij de normale toegang tot het besturingssysteem van zijn fysieke apparaat. Zie voor uitleg over cloud computing: Jeroen Horlings, *Cloud Computing*, Den Haag: SDU 2011.
64 Contractueel heeft LeaseWeb de toegang tot de servers voorbehouden, maar gebruik van encryptie is toegestaan. In geval van vermoeden van strafbare feiten kan LeaseWeb binnen het eigen netwerk onderzoek doen en indien nodig de servers afsluiten. Acceptable Use Policy Leaseweb (geldig op 17-8-2011) en Algemene voorwaarden (V4.5) LeaseWeb (geldig op 17-8-2011).

zwaarwegende inmenging op de persoonlijke levenssfeer van de verdachte. [65]

2.1.2 INMENGING EN SLACHTOFFERS

Het kader zal hieronder worden getoetst op het terug-hacken naar de slachtoffers.

Door de Bredolab servers te kapen verkreeg Justitie toegang tot alle bij het botnet aangesloten computers, zonder dat de rechthebbende gebruiker hiervan op de hoogte was. Gesterkt door de bevestiging van het Bundesverfassungsgericht van de nood tot bescherming en door de rol van ICT-systemen in het dagelijks leven is het goed verdedigbaar te stellen dat zonder toestemming toegang tot en controle over een computer verwerven en hier gegevens aan toevoegen, een inmenging vormt op het privacyrecht.

Het waarschuwingsbericht meldde niets over de overname van het botnet of over de technische betekenis hiervan. Een Duits Bredolab slachtoffer postte op de website van zijn ISP na confrontatie met de waarschuwing: *"De politie kon er zelfs achter komen wie bij mij illegaal files download. Ik zie dit als een grote bedreiging. De politie moet garanderen dat er geen gegevens van mij aan derden worden doorgespeeld. Waar krijg ik überhaupt nog veiligheid voor mijn data?"*. [66] Door de technische betekenis van de kaping kon het KLPD beschikken over een potentieel uiterst groot en veelzeggend databestand van de slachtoffers. De dreiging van dit potentieel is ook terug te lezen in de reactie van het Duitse slachtoffer. Toegang tot dit databestand en het nalaten van een melding leidt mijns inziens tot de constatering dat bij de verdere toetsing van de inmenging de aard hiervan zwaar meegewogen dient te worden.

65 Het tijdens de opbouw van het procesdossier heimelijk meekijken met de botherder staat mogelijk op gespannen voet met andere fundamentele rechten. Onderzoek hiernaar valt buiten het bereik van deze scriptie.

66 http://computer.t-online.de/bredolab-polizei-warnt-via-botnetz-vor-trojaner/id_43266956/index entry op 28 oktober 2010 om 17:30:13. Naam: Gläserner Bürger: *"Polizei könnte dabei sogar herausbekommen, wer unerlaubt bei mir schnüffeln will. Dies sehe ich als größere Gefahr an. Die Polizei müßte mir aber garantieren, dass keine Daten unerlaubt an Dritte weitergegeben werden. Diese Verantwortung möcht ich dann auch zugesichert bekommen. Denn wo könnte ich eine größere Sicherheit für meine Daten übeerhaupt noch erhalten. Jede EC-Karten Bezahlung wird doch an Dritte weitergegeben und dann benutzt."*

2.2 CRITERIA ARTIKEL 8 EVRM

Wanneer aan de drie cumulatieve criteria van het tweede lid van artikel 8 EVRM is voldaan, kan inmenging zoals hierboven beschreven, gerechtvaardigd zijn en levert het niet per definitie een privacyschending op. In de deze paragraaf zal het door het EHRM uitgewerkte leerstuk van toegestane inmengingen per criterium worden uitgewerkt.

Ten eerste moet sprake zijn van een legitiem doel, welke uitputtend zijn opgenomen in het tweede lid van artikel 8 EVRM. Het Hof pleegt in haar jurisprudentie weinig aandacht te besteden aan de omlijning en reikwijdte van deze doelen.

Het tweede criterium behelst de voorzienbaarheid bij wet en is gekoppeld aan drie cumulatieve toetsstenen. 1. De maatregel moet in de nationale wetgeving zijn vastgelegd. 2. Ze moet voldoende toegankelijk zijn voor het publiek.[67] 3. Ze moet voldoen aan de *voorzienbaarheid.* Daar het gebruik van vage termen onontkoombaar is,[68] bestaat de voorzienbaarheid in het strafrecht slechts uit een voldoende mate van helderheid en niet uit absolute duidelijkheid.[69] Het Hof eist echter strenge, heldere en gedetailleerde wettelijke bepalingen in geval de inmenging plaatsvindt ter voorkoming van strafbare feiten en in geval gebruik wordt gemaakt van geavanceerde technologie.[70] Het is belangrijk dat de effecten van de maatregel door de burger kunnen worden ingeschat, zodat het gedrag hierop kan worden aangepast.[71]

Tevens wordt een kwalitatief vereiste gesteld: in overeenstemming met de algemene beginselen van de rechtsstaat moet de beperkende maatregel waarborgen bevatten tegen willekeur en misbruik. Uit vaste jurisprudentie volgen drie waarborgen: notificatie van de inmenging, beperking van de effecten van de maatregel en toekenning van meer gewicht aan de voorzienbaarheid, naarmate de aard van de inmenging zwaarder is.[72]

---

67 EHRM 2 augustus 1984, nr. 8691/79 *(Malone v. the United Kingdom).*
68 EHRM 24 mei 1988, nr. 10737/84 *(Müller and others v. Switzerland).* ro. 29.
69 EHRM 24 april 1990, nr. 11105/84 *(Huvig v. France).*ro. 26.
70 EHRM 30 juli 1998, nr. 27671/95 *(Valenzuela v. Spain)* en EHRM 24 april 1990, nr. 11801/85 *(Kruslin v. France).*
71 EHRM 1 juli 2008, nr. 58243/00 *(Liberty and others v. the United Kingdom).*
72 EHRM 26 september 1995, nr. 17851/91 *(Vogt v. Germany)* ro. 48
Daarnaast in bijvoorbeeld EHRM 25 maart 1983, nr. 5947/72, *(Silver and others. v. the United Kingdom).*ro. 88.

Het laatste criterium van artikel 8 lid 2 betreft *de noodzakelijkheid in een democratische samenleving*. Noodzakelijkheid staat hierbij niet synoniem voor nodig, wenselijk of nuttig.[73] Om ten koste van het recht op bescherming van de persoonlijke levenssfeer een legitieme doel te verwezenlijken vereist de noodzakelijkheid een dringende maatschappelijke behoefte. Daarnaast moet de maatregel proportioneel zijn en dient een belangenafweging te worden gemaakt tussen het effect van de inmenging op recht en rechtsbeleving van de burger en het nagestreefde doel. Hierbij moeten de effectiviteit en subsidiariteit worden meegewogen alsmede maatregelen die zijn genomen ter beperking van de inmenging.[74] Aanwezigheid van less restrictive means maakt de inmenging discutabel.

In de belangenafweging komt de Staat een bepaalde margin of appreciation toe, een zekere beoordelingsvrijheid om de effectiviteit, proportionaliteit en noodzakelijkheid van de maatregel te beoordelen. Het Hof heeft in de zaak *S. and Marper v. The United Kingdom* de reikwijdte van de margin of appreciation uitgelegd aan de hand van vier factoren: het recht, het belang van het recht voor het individu, de aard van de inmenging en het doel van de inmenging.[75] Voorts dienen de gronden die lidstaten aanvoeren "*relevant and sufficient*" te zijn. De uiteindelijke beslissing komt toe aan het EHRM.[76]

73 EHRM 7 december 1976, nr. 5493/72, *(Handyside v. The United Kingdom).*
74 EHRM 25 maart 1983, nr. 5947/72, *(Silver and others. v. the United Kingdom)* ro. 97.
75 EHRM 4 december 2008, nr. 30562/04, *(S. and Marper v. the United Kingdom)* ro. 102.
76 EHRM 4 december 2008, nr. 30562/04, *(S. and Marper v. the United Kingdom)* ro.101.

2.3 TERUG-HACKEN VERDACHTE GETOETST

In de komende paragraaf wordt de relevante nationale wetgeving beschreven en de inmenging op het privacyrecht van de verdachte getoetst aan de criteria uit art. 8 lid 2EVRM.

2.3.1 RELEVANTE NATIONALE WETGEVING

In casu werd de botherder verdacht van computervredebreuk in gekwalificeerde vorm.[77] Alsmede van het opzettelijk en wederrechtelijk toevoegen van gegevens, en het opzettelijk en wederrechtelijk ter beschikking stellen of verspreiden van gegevens die zijn bestemd om schade aan te richten aan een geautomatiseerd werk.[78] Bij de opsporing is gebruik gemaakt van de tap- en inbeslagname bevoegdheid. Volledigheidshalve zijn de relevante wetsartikelen in bijlage III opgenomen.

Bij de invoering van de wet Computercriminaliteit I is onderscheid gemaakt tussen onderzoek naar stromende en opgeslagen gegevens.[79] Artikel 126m Sv schept de bevoegdheid tot het onderzoeken van stromende gegevens, de tapbevoegdheid. De wetsgeschiedenis laat zien dat deze bevoegdheid zich heden expliciet richt op het opnemen van telecommunicatie. In de voorloper van dit artikel werd slechts de bevoegdheid tot het aftappen van gesprekken gegeven.[80]

---

77 Strafbaar gesteld in artikel 138ab lid 1-3 Sr De gekwalificeerde vormen zijn in het tweede en derde lid gegeven en luiden: 138ab lid 2: *Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.*
138ab lid 3: *Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens: a. met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk; b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.*

78 Strafbaar gesteld in artikel 350a lid 1 en lid 3 Sr
De exacte definiëring van de twee artikelen staat momenteel ter discussie. De Hoge Raad heeft een opmerkelijke uitspraak gedaan: Hoge Raad van 22 februari 2011 *LJN* BN9287. Hierin stelde zij dat het doen verspreiden of doen installeren van een virus (350a Sr.) computervredebreuk (138ab) oplevert. Zie voor een analyse van deze uitspraak: J.J. Oerlemans en B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *Nederlands Juristenblad* 2011, 914.

79 *Rapport commissie Computercriminaliteit, Informatietechniek en Strafrecht* april 1987 en ook: *Kamerstukken II* 1998/99, 26 671, nr. 3 Voor bepaalde communicatie geldt een ander regime, afhankelijk van de fase waarin gegevens zich bevinden. Een e-mail onderweg is stromend. Een e-mail in een inbox online of op een harde schijf is opgeslagen. *Kamerstukken II* 1999/00, 25530, nr. 40 p. 6.

80 De voorloper was art. 125g Sv. *Stb.* 1971, 180.

De Hoge Raad oordeelde destijds dat een tapbevoegdheid nauw geïnterpreteerd dient te worden.[81] In reactie hierop is het bestanddeel *gesprekken* door de wetgever vervangen door het bestanddeel *telecommunicatie*.[82] Ingevoerde gegevens die niet via een netwerk verzonden worden vallen hierbuiten.[83] Getapte communicatie mag door opsporingsambtenaren ontsleuteld worden. Deze decryptiebevoegdheid wordt geacht te zijn 'ingebakken' in de tapbevoegdheid.[84]

De bevoegdheid komt de opsporingdiensten toe in geval van verdenking van een misdrijf als omschreven in art. 67, eerste lid Sv, dat in aard of samenhang met andere misdrijven een ernstige inbreuk op de rechtsorde oplevert. Indien het onderzoek dit dringend vordert, kan de officier van justitie met een machtiging van de rechter-commissaris bevelen dat, met een technisch hulpmiddel niet voor publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen.

Met invoering van de wet Computercriminaliteit I en II geeft de wetgever specifieke bevoegdheden voor onderzoek naar opgeslagen gegevens. De aard van gegevens leent zich in beginsel niet voor de algemene inbeslagname, daar het geen goederen in strafrechtelijke zin zijn.[85]

De lex specialis van inbeslagname is de bevoegdheid tot doorzoeking van een plaats ter vastlegging van relevante gegevens ex. artikel 125i Sv. Dit artikel is mede ingevoerd om disproportionaliteit tegen te gaan tussen de verdenking en de toegepaste dwangmiddelen. De nadruk ligt daardoor op relevante gegevens.[86] Alleen indien er omstandigheden zijn die ertoe nopen dat de gehele gegevensdrager wordt verkregen, kunnen de algemene inbeslagname bevoegdheden worden toegepast.[87] In de memorie van Toelichting bij artikel 125i Sv wordt als dergelijke omstandigheid "het originele document veilig stellen" als voorbeeld genoemd.[88]

81 HR 26 mei 1992, *NJ* 1992, 753.
82 *Stb.*1993, 33.
83 *Kamerstukken II*, 1996/97 25 403 nr. 3.
84 Koops, 2008 p. 126.
85 *Rapport commissie Computercriminaliteit, Informatietechniek en Strafrecht,* april 1987, en HR 3 december 1996, *NJ* 1997, 574.
86 *Kamerstukken II* 2003/04, 29 441, nr. 3p. 1-12.
87 *Kamerstukken II* 2003/04, 29 441, nr. 3 p. 13.
88 *Kamerstukken II* 2003/04, 29 441, nr. 3p. 13.

Artikel 134 lid 1 Sv definieert algemene inbeslagname als het onder zich nemen of gaan houden van enig voorwerp ten behoeve van de strafvordering. [89] Het voorwerp komt in de macht van de beslaglegger waardoor de beslagene de vrije beschikking verliest.[90] Wanneer fysieke ontneming niet mogelijk is, dient het beslag duidelijk te worden gecommuniceerd middels notificatie of verzegeling. [91] Vatbaar voor inbeslagneming zijn alle voorwerpen die kunnen dienen om de waarheid aan de dag te brengen, ex art. 94 Sv. Het ontsleutelen van gegevens is daarvoor toegestaan.[92] In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid Sv, is de opsporingsambtenaar tot in beslagname bevoegd, ex. art. 96 Sv.

In casu rustte de verdenking op de strafbare feiten omschreven in artikel 138ab en 350a Sr. Beide artikelen zijn omschreven in artikel 67 lid 1 Sv. Het OM stelt dat een botnet vanwege de uitstraling naar andere delicten een ondermijnende werking op de rechtsorde heeft, en Bredolab derhalve een ernstige inbreuk op de rechtsorde maakte. De OvJ zag het doorbreken van de encryptie als dringende noodzaak om de taps bij LeaseWeb te plaatsen. [93] Hij heeft hiertoe een schriftelijke machtiging van de rechter-commissaris ontvangen. In totaal zijn 6 taps geplaatst.
Hoewel LeaseWeb haar medewerking aan het onderzoek bood wilde zij niet verantwoordelijk zijn voor de verdachte servers. De servers bevatte veel informatie voor de opsporing. Om dit veilig te stellen is voor klassieke inbeslagname gekozen. [94]

89 HR 6 april 1936, *NJ* 1936, 813.
90 R. Vennix 1998, p. 57.
91 R. Vennix 1998, p. 57.
92 Koops 2008, p.126.
93 LeaseWeb is een aanbieder van een communicatiedienst in de zin van artikel 126la Sv. In de uitoefening van haar bedrijf verwerkt zij gegevens en/of slaat deze op ten behoeve van een communicatiedienst of diens gebruikers. LeaseWeb is echter geen aanbieder van een openbaar elektronisch telecommunicatie netwerk of een openbare elektronische telecommunicatie dienst in de zin van artikel 1.1 sub g en h Tw. Er rust derhalve geen meewerk verplichting op LeaseWeb ex art. 126m lid 3 Sv. juncto art. 13.2 lid 1 Tw. Tenzij het niet mogelijk is of het belang van strafvordering zich daartegen verzet, wordt de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel. Art. 126m lid 4 Sv. In het geval van Bredolab heeft LeaseWeb volledige medewerking gegeven aan het tappen van de servers.
94 Het is onduidelijk of in casu rekening gehouden is met de positie die LeaseWeb toekomt als geregistreerde ingevolge artikel 2.1, vierde lid, van de Tw. LeaseWeb is ingevolge artikel 2.1 Tw ingeschreven bij de OPTA onder registratienummer 941165 en 941642 per 7-6-2007. Uit de Memorie van Toelichting van de partiële wijziging van het Wetboek van Strafvordering blijkt dat een bevel tot uitlevering ex. artikel 96a lid 1 Sv. nooit aan één van de ingeschreven instellingen gericht mag worden. *Kamerstukken II* 1992/93, 23 251, nr.3. Het is aannemelijk dat op de server communicatie berichten waren opgeslagen. Het bevel tot uitlevering dient in een dergelijk geval te geschieden op basis van art. 100 lid 1 jo. art. 96 jo. 96a lid 5. De bevoegdheid komt de OvJ toe onder art. 94 Sv.

2.3.2 TOETSING

In paragraaf 2.1.1 is vastgesteld dat terug-hacken een inmenging op het privacyrecht behelst. Vraag is of een verdachte tijdens de voorbereiding of uitvoering van een strafbaar feit een beroep op het privacyrecht kan doen. Door de uitspraak van het EHRM in de zaak *Lüdi v. Switzerland* scheen dit beroep slechts beperkt mogelijk, maar het Hof lijkt hier in latere zaken op te zijn teruggekomen.[95] In de zaak *A. v. France* en *Peck v. The United Kingdom* heeft het Hof geoordeeld dat ondanks de strafbare feiten sprake was van inmenging op het privacyrecht en dat de overheid de bescherming van dit recht had moeten waarborgen.[96]

1. Het legitieme doel.

Het OM kwalificeert een botnet als een gevaarlijk netwerk, welke de nationale veiligheid kan bedreigen.[97] Daarnaast heeft het OM de maatregelen genomen ter voorkoming van strafbare feiten. Dit zijn beide gelegitimeerde doelen onder artikel 8 lid 2 EVRM. Gezien de geringe aandacht die het EHRM pleegt te besteden aan de vaststelling van de legitieme doelen volstaat deze constatering.

2. Voorzienbaarheid bij wet.

Het OM maakte in haar onderzoek gebruik van art. 96 juncto art. 126m Sv. Deze artikelen maken deel uit van het wetboek van strafvordering en zijn middels websites en publicaties in het Staatsblad voldoende toegankelijk voor het publiek.[98] Vanwege de technische mogelijkheden bij terug-hacken en de potentieel grove inbreuk die opsporing op het privacyrecht maakt, worden strenge eisen aan de voorzienbaarheid gesteld.

In casu had de toepassing van art. 126m en 96 Sv het effect: *dat de opsporingsdienst middels afgevangen toegang- en decryptiesleutels op de servers zijn binnengedrongen, waardoor gedurende ongeveer tien weken heimelijk de handelingen van de verdachte werden gemonitord en onderzocht.*

---

95 EHRM 15 juni 1992, nr. 12433/86 *(Lüdi v. Switzerland)* ro. 39.
96 EHRM 23 november 1993, nr. 14838/89 *(A. v. France)* ro. 34 en EHRM 28 januari 2003, nr. 44647/98 *(Peck v. the United Kingdom).*
97 OvJ van Zwieten stelde dat een bedreiging van de nationale veiligheid de zwaarste categorie bedreiging is van de openbare orde.
98 Artikel 96 Sv *Stb.* 2006, 330 en Artikel 126m Sv *Stb.* 2006, 300.

De voorzienbaarheid vereist dat burgers bij kennisneming van de artikelen het hierboven omschreven effect moeten kunnen inschatten, opdat zij hun gedrag hierop kunnen aanpassen.

Het in te schatten effect op de privacy van art. 126m Sv is dat door aftappen en onderzoek de inhoud van de telecommunicatie, ook al is deze versleuteld, bij opsporingsdiensten bekend wordt en mogelijk als bewijs zal dienen. Het in te schatten effect op de privacy van art. 96 Sv is dat door inbeslagname beslagene de beschikking over de gegevensdrager verliest en dat de in het verleden opgeslagen gegevens en daarmee het privéleven bij de opsporingsdiensten bekend wordt en mogelijk als bewijs zal dienen.

Het effect van de inmenging in casu komt mijns inziens niet overeen met bovengenoemde effecten. Heimelijk observeren en onderzoeken van handelingen wijkt significant af van onderzoek aan telecommunicatie en opgeslagen gegevens, waardoor art. 96 en 126m Sv niet voorzien in het effect van een dergelijke inmenging.[99] Het technisch effect van terug-hacken op de privacy is de totaalsom van het doorzoeken, aftappen, heimelijk volgen, observeren en infiltreren.

Daarnaast brengt de inbeslagname nog een complicatie met zich mee. Ter wille van het onderzoek werd beslag gelegd op de gegevensdragers, waardoor LeaseWeb de juridisch beschikkingsmacht over de servers verloor. Het onderzoek richtte zich vervolgens op de aanwezige gegevens en handelingen van de botherder, terwijl deze vrije beschikking behield over de servers.[100] LeaseWeb werd over de inbeslagname geïnformeerd; de inbeslagname is welbewust niet aan de gebruiker gemeld. De vereiste notificatie is daarmee uitgebleven. Tevens is het is uit literatuur en jurisprudentie niet duidelijk op te maken hoe, de verhoudingen liggen tussen de eigenaar van een gegevensdrager, de eigenaar/gebruiker van de gegevens en de opsporingsdiensten, alsmede welk gewicht aan de notificatieplicht moet worden toegekend.

---

99 Door het meekijken op de servers van de botherder worden niet alleen zijn communicatieve handelingen bekeken maar zijn gehele doen en laten. Het totaal aan handelingen die de botherder op de servers uitvoerde betreffen niet-stromende gegevens. Slechts het gedeelte van de gegevens dat nodig is voor het uitvoeren van de commando's wordt als stromende gegevens naar de computer van de botherder of naar andere adressen gestuurd.
De overige gegevens maken geen deel uit van het telecommunicatie verkeer en zijn derhalve geen stromende gegevens.

100 LeaseWeb geeft aan volledige medewerking aan opsporingsdiensten te verlenen. Art. 4.2 *Acceptable Use Policy Leaseweb*. Deze medewerking is privaatrechtelijk vastgelegd tussen huurder en LeaseWeb en geeft geen bevoegdheden voor opsporingsdiensten.

Bovenstaande leidt mijns inziens tot de conclusie dat art. 96 en 126m Sv in casu geen strenge, heldere en gedetailleerde regels vormen die in de effecten van de inmenging voorzien. Het is derhalve goed verdedigbaar te stellen dat aan het vereiste criterium van artikel 8 lid 2 EVRM *voorzienbaarheid bij wet* niet is voldaan, waardoor terug-hacken een schending van het privacyrecht oplevert.

2.4 TERUG-HACKEN SLACHTOFFERS GETOETST

In deze paragraaf wordt de juridische verantwoording van het OM ten aanzien van het terug-hacken naar de Bredolab slachtoffers weergegeven en achtergrondinformatie gegeven betreffende artikel 2 Politiewet (Polw). Daarna wordt de inmenging getoetst aan de criteria van artikel 8 lid 2 EVRM.

2.4.1 RELEVANTE NATIONALE WETGEVING

In een interview ten behoeve van deze scriptieis het terug-hacken naar de slachtoffers door het OM op basis van de volgende argumenten binnen het wettelijk systeem geplaatst:[101]

1. De verrichtte handelingen bevinden zich binnen de grenzen van artikel 2 Polw.
Officier van Justitie van het Landelijk Parket Lodewijk van Zwieten zegt hierover: *"[...] Artikel 2 Politiewet is voldoende. Het is een stukje bescherming van de rechtsorde en bescherming van de openbare orde. Het gevaarlijke systeem bedreigde zowel de rechtsorde als de openbare orde. [...]. Het [Art. 2 Polw - red.] is omgrensd wanneer opsporend optreden door de politie een meer dan geringe inbreuk maakt op de privacy van de betrokkenen. Het begrenzend criterium van artikel 2 Politiewet geldt niet als het om de bescherming van de openbare orde gaat. Dit criterium geldt heel nadrukkelijk voor opsporingshandelingen, dus niet voor handhaving."*

2. Het versturen van de executable is een schending van de privacy, maar de minst inbreukmakende die het OM en de KLPD konden verzinnen.
OvJ van Zwieten stelt hierover: "*Onthoofden botnet, opsporing en slachtoffer waarschuwen zou zo veel mogelijk in gezamenlijkheid moeten gebeuren, dan kun je effectief een botnet bestrijden. De meest directe infrastructuur naar de slachtoffers was het botnet zelf. [...] Ja, je maakt een inbreuk op de privacy want je stuurt iets naar iemand en een aantal van de geïnfecteerde computers zal zich in huizen bevinden in ruimtes waar mensen onbevangen zichzelf moeten kunnen zijn. En als je mensen daar benadert dan kunnen ze op dat moment niet even onbevangen zichzelf zijn, want ze worden geconfronteerd met de politie en dat is een privacyschending. Maar die privacyschending is niet meer dan gering, want wat er via het botnet gebeurt [doorsturen van wachtwoorden, creditcardgegevens etc. naar criminelen - red.] is vele malen privacy inbreukmakender dan dat wij met de politie doen.*"

3. Artikel 350a lid 4 Sr geeft het OM en het KLPD een strafuitsluitingsgrond. OvJ van Zwieten: "*Meest effectieve is dat wij een .exe naar de computers sturen over het botnet. [...]. Wat we dus feitelijk hebben gedaan is het toevoegen van gegevens aan een geautomatiseerd werk ex. artikel 350a strafrecht. De*

101 Interview L. van Zwieten Landelijk Parket 23 juni 2011. Locatie: Posthumalaan 74, Rotterdam. Tijd: 10:30
In tegenstelling tot eerdere uitspraken in de media stelde het OM in dit interview dat zij strafvorderlijk is opgetreden. Zie bijvoorbeeld de reactie in *Future of Copy Right*> botnets zijn het zwitserse zakmes van cybercriminelen: "*Het versturen van de waarschuwing zien wij niet als het inzetten van een opsporingsmethode. Het is eerder een maatregel in het algemeen belang, ter bescherming van de openbare orde op het internet, zo je wilt. En bovendien ter voorkoming van verdere schade. Het versturen van de maatregel heeft aan het vergaren van het bewijs in deze zaak niets bijgedragen.*"

strafbaarheid vervalt als je dat doet om schade te voorkomen ex. artikel 350a lid 4. Dit staat in de wet om überhaupt het desinfecteren van de computer mogelijk te maken. Het is een uitsluiting van de strafbaarheid."

Artikel 350a Sr bevat de strafbaarstelling van het onbevoegd aanpassen van digitale gegevens en het verspreiden van malware.

> Artikel 350a Wetboek van Strafrecht[102]
> 1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
> 2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.
> 3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
> 4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.

In artikel 2 Polw is de taakstelling van de politie gegeven.

> Artikel 2 Politiewet 1993[103]
> De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.

Artikel 2 Polw behelst een tweeledige taakstelling: handhaving van de openbare orde en daadwerkelijke handhaving van de rechtsorde. Met deze laatste wordt handhaving in strafrechtelijk zin bedoeld.[104] Het onderscheid tussen deze taken is in zowel de rechtspraak als in de dogmatiek ontwikkeld en is bepalend voor de verdeling van het gezag over en de bevoegdheden van de politie. Echter de scheidslijn is niet altijd even duidelijk. OvJ van Zwieten stelt dat artikel 2 Polw het terug-hacken - om de slachtoffers waarschuwen - voldoende legitimeert. Deze handeling zou zowel ter bescherming van de rechtsorde en als ter handhaving

102 Wet van 3 maart 1881, tot vaststelling van een nieuw Wetboek van Strafrecht, *Stb.* 1881, 35. Laatstelijk gewijzigd op 31 maart 2011 *Stb.* 2011, 171.
103 Wet van 9 december 1993, tot vaststelling van een nieuwe Politiewet, *Stb.* 1993, 724. Laatstelijk gewijzigd op 13 december 2010, *Stb.* 2011, 4.
104 C. Cleiren e.a. 2009 p. 2241.

van de openbare orde zijn geschied.

In de Nederlandse wet is geen definitie van het begrip *openbare orde* opgenomen. In de Memorie van Toelichting bij de vaststelling van de Politiewet 1993 wordt openbare orde beschreven als de zorg voor de naleving van regels, waarvan bij niet-naleving de orde als rust in het openbare leven wordt verstoord.[105] Handhaving van de openbare orde wordt gedefinieerd als het daadwerkelijk voorkomen en beëindigen van zich concreet voordoende of dreigende verstoringen, alsmede het bestuurlijk voorkomen van strafbare feiten die invloed hebben op de orde en rust in de gemeentelijke samenleving.[106] Hieronder wordt mede het veiligheidsbeleid verstaan, waartoe ook bestuurlijke criminaliteitspreventie wordt gerekend.

In beginsel is de burgemeester verantwoordelijk voor handhaving van de openbare orde.[107] De rol van het OM is beperkt tot op dader gerichte criminaliteitspreventie, binnen de bestuurlijke driehoek.[108] Bij zich concreet voordoende of dreigende verstoringen maakt het OM vervolging opportuun en instrueert de politie hiertoe alle verdachten/daders van openbare orde schending aan te houden, in de hoop de potentiële wetsovertreders hiermee af te schrikken.[109]

De tweede politietaak, handhaving van de rechtsorde in strafrechtelijke zin, bestaat uit het daadwerkelijk voorkomen, opsporen en beëindigen van strafbare feiten.[110] Bij de uitvoering van de strafrechtelijke handhaving staat de politie onder het gezag van het OM ex art. 13 Polw. In concrete opsporingsonderzoeken heeft de Officier van Justitie de leidende positie en is verantwoordelijk voor de legitimiteit van het optreden van opsporingsambtenaren.[111]

Artikel 2 Polw is door de tijd heen gebruikt als grondslag voor bepaalde strafvorderlijke bevoegdheden. Zo werden opsporingstechnieken als het observeren van verdachten in de

105 *Kamerstukken II* 1991/92, 22 562, nr. 3 p. 7.
106 Zoals het bekeuren van overtreders van de Algemene plaatselijke verordening.
107 Art. 12 Politiewet. In geval van een minder plaatselijke openbare orde schending is de commissaris van de koningin of de minister van binnenlandse zaken bevoegd om de burgemeester instructies te geven.
108 *Kamerstukken II* 1991/92, 22 562, nr. en *Kamerstukken II* 1986/87, 19 535, nr. 4 en *Kamerstukken II* 1987/88, 19 403, nr. 15. Bestuurlijke driehoek: Burgemeester, korpschef Politie en hoofdofficier van Justitie.
109 Het bovenstaande komt terug in het persbericht in het Zero Tolerance beleid bij de Gay Pride 2011. http://www.om.nl/@156307/zero-tolerance/. Of in het beleid voor risico voetbalwedstrijden. Zie: Aanwijzing bestrijding van voetbalvandalisme en -geweld (2010A023).
110 *Kamerstukken II* 1985/86, 19 535, nr. 3 p. 5-7.
111 *Kamerstukken II* 1996/97, 25 392, nr. 3 p.11.

openbare ruimte[112] (inmiddels art 126g Sv) en infiltreren in een crimineel netwerk[113] (inmiddels art 126h Sv.) in de jaren zeventig en tachtig door de Hoge Raad geacht voldoende rechtsgrond te hebben middels dit artikel.

Echter met het Zwolsmans-arrest uit 1995 heeft de Hoge Raad een nauw criterium gesteld ter begrenzing van de strafvorderlijke bevoegdheden uit artikel 2 Polw.[114] De voortschrijdende ontwikkeling van het privacyrecht en de toenemende technische verfijning en intensivering van onderzoeksmethoden en -technieken verlangen een meer precieze legitimatie in de wet. Indien bij opsporing slechts een beperkte inbreuk op de persoonlijke levenssfeer wordt gemaakt, biedt de globale taakomschrijving van art. 2 Polw hiervoor een toereikende wettelijke grondslag, aldus de Hoge Raad.

In casu is het zonder een apocalyptisch visie op het effect van cybercriminaliteit, mijns inziens moeilijk om in de aanwezigheid van de Bredolab command en control servers in Gemeente Haarlem een concreet voordoende of dreigende verstoring van de openbare orde te zien. Terug-hacken kan derhalve niet als handeling in de uitvoering van de openbare handhavingstaak worden gezien.
De kans is groot dat ten tijde van de Bredolab ontmanteling op de botclients nog lopende opdrachten ten behoeve van de afnemers in uitvoering waren. Met het doel deze criminele activiteiten te beëindigen stuurde de politie over het botnet zelf een waarschuwing naar de slachtoffers. Als deze daarop zouden reageren en de door Kaspersky beschikbaar gestelde patch zouden downloaden, zou de waarschuwing bijdragen aan de beoogde doelstelling: de beëindiging van strafbare feiten.

112 HR 14 oktober 1986, *NJ* 1988, 551.
113 HR 4 december 1979, *NJ* 1980, 356.
114 19 december 1995, *NJ* 1996, 249.

2.4.2 TOETSING

1. Het legitieme doel.

Toetsing van dit criterium biedt in wezen dezelfde uitkomst als het in paragraaf 2.3.2 gestelde. Het OM kwalificeert een botnet als een gevaarlijk netwerk, welke de nationale veiligheid kan bedreigen.[115] Zij besloot om deze reden terug te hacken. Daarnaast heeft het OM de maatregelen genomen ter voorkoming van strafbare feiten. Dit zijn beide gelegitimeerde doelen onder artikel 8 lid 2 EVRM. Gezien de geringe aandacht die het EHRM pleegt te besteden aan de vaststelling van de legitieme doelen volstaat ook hier deze constatering.

2. Voorzienbaarheid bij wet.

Artikel 2 Polw en art 350a lid 4 Sr maken deel uit van de Nederlandse wetgeving en zijn middels websites en publicaties in het Staatsblad voldoende toegankelijk voor het publiek. De vraag is echter of bij het kennisnemen van deze artikelen de inmenging voorzienbaar is en als zodanig voor de burger is in te schatten: *terug-hacken via het botnet en daarbij de volledige controle over de computer en toegang tot een potentieel uiterst groot en veelzeggend databestand van het slachtoffer verwerven. Vervolgens deze controle aanwenden om gegevens toe te voegen en het slachtoffer te waarschuwen.*

Artikel 2 Polw omschrijft de taakstelling van de politie en verleent beperkte bevoegdheden. De zwaarwegende aard van de inmenging, zoals in paragraaf 2.1.2 gesteld, staat mijns inziens in de weg aan bevoegdheidsverlening van art. 2 Polw.

Artikel 350a lid 4 Sr vormt een strafuitsluitingsgrond voor de persoon die opzettelijk en wederrechtelijk gegevens bedoeld om schade aan te richten (malware) in een geautomatiseerd werk *verspreidt* of *beschikbaar stelt,* met het oog op de beperking van de schadelijke gevolgen van deze gegevens.[116] Schulduitsluiting ziet toe op gronden die de strafbaarheid van de dader wegnemen. De wederrechtelijkheid van de handeling blijft evenwel onverlet.[117] In een rechtsstaat komt het vaststellen van het ontbreken van strafbaarheid toe aan de rechtsprekende macht en niet

115 OvJ van Zwieten stelde dat een botnet een gevaarlijk netwerk is. In situaties van gevaarlijke netwerken is de nationale veiligheid in beding.
116 *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 36.
117 C. Cleiren e.a. 2010 p. 321-340.

aan de uitvoerende macht. Daarnaast is de schulduitsluitingsgrond niet gericht op het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk (computervredebreuk, art. 138ab Sr) en ook niet op het opzettelijk en wederrechtelijk toevoegen van gegevens (art 350a lid 1 Sr). Vraag is of een schulduitsluitingsgrond voor het verspreiden of beschikbaar stellen van malware (art. 350a lid 3 Sr) terugslaat op de straffeloosheid van de persoon die zich zonder toestemming toegang tot de computer van het slachtoffer verwerft (binnendringen) en gegevens daaraan toevoegt.

Bij art. 2 Polw en 350a lid 4 Sr ontbreekt het aan waarborgen tegen willekeur en misbruik. Bij het terug-hacken zijn voor zover bekend geen alternatieve maatregelen getroffen tegen willekeur of misbruik.[118] In het waarschuwingsbericht maakte het KLPD geen melding van de overname van het botnet, noch van de toegang die zij zich verschafte tot de computer van het slachtoffer. Ook werd geen melding gemaakt van het toevoegen van gegevens.[119]

In casu vormen art. 2 Polw en 350a lid 4 Sr geen strenge, heldere en gedetailleerde wetgeving. Hierdoor kan mijns inziens worden gesteld dat het effect van de inmenging voor de burger niet is in te schatten. Het is goed verdedigbaar te stellen dat aan het vereiste criterium van artikel 8 lid 2 EVRM *voorzienbaarheid bij wet* niet is voldaan en terug-hacken derhalve een schending van het privacyrecht oplevert.

Daar de inmenging op het privacyrecht meer dan gering kan worden genoemd, zal art. 2 Polw geen strafvorderlijke bevoegdheid tot terug-hacken verlenen.

118 Mogelijk levert het terug-hacken ook spanningen op met andere grondrechten waaronder het recht tot een daadwerkelijk rechtsmiddel ex art 13 EVRM. Aangifte en de klachten procedure bij het KLPD zijn de enige rechtsmiddelen open voor de slachtoffers. Aanwending lijkt mijns inziens vruchteloos, nu bij de bepaling van de ontvankelijkheid van de klacht gekeken wordt naar de grondslag van de aangewende bevoegdheid. Naar alle waarschijnlijkheid zal art. 2 Polw toereikend worden geacht, wat zal resulteren in onontvankelijkheid van de klacht. Eenzelfde valkuil schuilt in de aangifte.

119 Het slachtoffer zag de melding in de browser maar hoe de browser op die pagina is gekomen is waarschijnlijk net zo mysterieus voor het slachtoffer als de besmetting met Bredolab zelf.

2.4.3 TOETSING TOEKOMSTIG TERUG-HACKEN SLACHTOFFERS

3. Noodzakelijkheid in een democratische samenleving

De ontwikkelingen van het computergebruik enerzijds en die van de cybercriminaliteit anderzijds, maken het begrijpelijk (en wenselijk) dat Justitie de online omgeving graag onder haar controle heeft. Ook al is met het vaststellen van de privacyschending de art. 8 EVRM toets afgerond, met het oog op de toekomst kan het een interessante exercitie zijn om het terug-hacken ter voorkoming van strafbare feiten te toetsen aan het laatste criterium *de noodzakelijkheid in een democratische samenleving.*[120]

OvJ van Zwieten stelde bij de ontmanteling van Bredolab dat de snelste en makkelijkste weg naar het slachtoffer via het botnet zou gaan. Deze veronderstelling was medebepalend voor het besluit terug te hacken. Daarnaast speelde het argument dat het verlies van vertrouwen in online diensten negatieve gevolgen zou hebben voor de 24-uurs-informatie-economie in Nederland. Project Tolling wilde onder meer op basis van deze argumenten bereiken dat cybercriminelen Nederland zouden mijden. Volgens de opsporingsdiensten is dit doel inmiddels gedeeltelijk gerealiseerd, met de ontmanteling van Bredolab.[121] Hoe legitiem deze argumenten en doelstellingen ook mogen zijn, zij zullen in het licht van de noodzakelijkheid binnen een democratische samenleving gewogen moeten worden.

Het kost weinig verbeeldingskracht om substituten te bedenken voor het voorkomen van de strafbare feiten. In de eerste plaats konden de opsporingsdiensten de infecties voor de afnemers van Bredolab zien. Zowel het IP adres van de bestelling, als het afleveradres en de klantendatabases waren zichtbaar. In samenwerking met buitenlandse opsporingsdiensten konden aan de hand van deze gegevens de verdachte afnemers of hun servers worden opgespoord. In de tweede plaats waren tijdens het tappen de IP adressen van alle nieuwe en grotendeels ook van de oudere slachtoffers bekend geworden. GOVCERT.NL heeft deze wereldwijd doorgegeven om de slachtoffers te waarschuwen.[122] Het is niet bekend of deze meldingen het slachtoffer

120 Deze stap ontbreekt bij de eerdere lid 2 toets. Een theoretische exercitie op dit punt bij de verdachte lijkt weinig toe te voegen aan de voorliggende argumentatie daar de aard en kenmerken van strafbare feiten uiteenlopend zijn.
121 Zie bijvoorbeeld het rapport van Kaspersky antivirus lab, zijdelings betrokken bij de ontmanteling: KasperskyHome, www.securelist.com>Analysis>11 Aug 2011>IT Threat Evolution: Q2 2011
122 Het is niet bekend of deze meldingen in casu het slachtoffer hebben bereikt.

hebben bereikt.

In vergelijking met het terug-hacken vormen bovengenoemde maatregelen slechts een beperkte inmenging op de persoonlijke levenssfeer van de slachtoffers. Met andere woorden: het zijn *less restrictive means*.

OvJ van Zwieten legitimeerde de inmenging mede op de effectiviteit daarvan en stelde dat door de directe communicatie tussen opsporingsinstantie en slachtoffers onbetrouwbare of niet welwillende derden de beëindiging van de strafbare feiten niet konden beïnvloeden. De OvJ doelde hiermee op ISP's met een belang in het voortduren van malware op het netwerk of op buitenlandse opsporingsdiensten zonder prioriteit op het tegengaan van cybercriminaliteit.

Mijns inziens rechtvaardigt het OM de inmenging op oneigenlijke gronden en ontkent het territorium waaraan zij gebonden is.[123] De oneigenlijke grond bestaat uit de kennelijke overtuiging dat het KLPD en het OM in geval van cybercriminaliteit bevoegd zijn de rechtsorde wereldwijd daadwerkelijk te handhaven. In een adem noemt de OvJ de onbetrouwbaarheid van ISP's in het buitenland en de welwillendheid van de Nederlandse en stelt dat cybercriminaliteitsbestrijding op nationaal niveau goed mogelijk is met genoemde substituten.

Het OM heeft tot taak handhaving van de strafrechtelijke rechtsorde.[124] De taak van de politie is de daadwerkelijke handhaving van de rechtsorde, in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels.[125] De omvang van de strafrechtelijke rechtsorde wordt door de werking van het Wetboek van Strafrecht gedefinieerd.[126] Strafvorderlijk optreden is gebonden aan het territorialiteitsbeginsel: de Nederlandse strafwet is toepasbaar op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.[127]

---

123 Takkenberg en Van Zwieten benoemen het probleem: "*Onze jurisdictie houdt feitelijk op bij de landsgrens… Maar omdat het gevaar zo groot was, hebben we deze stap gezet om de schade te beperken."* Er wordt echter niet naar deze uitspraken gehandeld. http://www.softbrix.nl/page1551597.aspx

124 Art. 124 wet RO

125 Art. 2 Polw

126 Wetboek van Strafrecht, eerste boek, titel 1.

127 Artikel 2 Sr. Daarnaast is binding middels het universaliteitsbeginsel art. 4 sub13 en 14 Sr. Dit beginsel betreft specifiek omschreven omstandigheden voor de toepasbaarheid van de Nederlandse strafwet. Het wetboek is van toepassing indien artikel 350a Sr. (verspreiden van malware en aanpassen gegevens op een geautomatiseerd werk) met een terroristisch oogmerk of ten doel van de financiering van terrorisme geschied. De casus geeft geen aanleiding om aan te nemen dat deze situatie zich voordeed.

In casu is het strafbare feit niet direct verbonden aan het Nederlands grondgebied. Het betreft een buitenlandse botherder die voor buitenlandse afnemers malware op de computers van vooral buitenlandse slachtoffers heeft geplaatst. De afgetapte gegevens zijn direct naar buitenlandse afnemers gestuurd. Aanwijzingen die duiden op effecten binnen de Nederlandse rechtsorde bij het niet prompt waarschuwen van de slachtoffers wereldwijd ontbreken.[128]

Het is mijns inziens onwenselijk voor de privacy van de internetgebruiker als activiteiten op internet die ooit via een inmiddels onschadelijke server in Nederland zijn geïnitieerd, zonder dat zij verdere effect op de rechtsorde hebben, onder de Nederlandse strafwet zouden vallen.[129]

Daarnaast is het zeer de vraag of inmenging als in casu noodzakelijk is met het oog op het mogelijke effect. Het lijkt niet handig als internet gebruikers gewend raken aan malware waarschuwingen van vreemde partijen. Cybercriminelen passen deze truc namelijk toe om gegevens aan slachtoffers te ontfutselen, zich voordoend als bijvoorbeeld antivirus bedrijf of software leverancier. Nog even en ze stellen zich voor als opsporingsautoriteit.

Binnen het eigen territorium was het met minder beperkende maatregelen goed mogelijk geweest om de strafvorderlijke handhavingstaken effectief uit te voeren. Er waren een less restrictive means, waardoor aan de eis van proportionaliteit niet is voldaan.[130]

Ook de aanwezigheid van een expliciete terug-hack bevoegdheid zou het terug-hacken niet in overeenstemming hebben gebracht met art. 8 EVRM, daar aan de eis van noodzakelijkheid in een democratische samenleving niet is voldaan.

---

128 Het OM stelt dat alleen een rigoureus optreden internet in Nederland voor een catastrofe kan behoeden. Bij grote internationale botnets kan de nationale veiligheid in gevaar komen, omdat mensen het vertouwen in diensten verliezen. Tevens kunnen criminele netwerken die middels internet informatie uitwisselen een dermate verontrustende uitwerking op de samenleving hebben, dat het voortbestaan van die netwerken een ernstige inbreuk op de rechtsorde betekent.
Er zijn geen aanwijzingen dat bovenstaande zich heeft voorgedaan bij het Bredolab botnet.

129 Het gegeven dat het THTC deel uitmaakt van de Dienst Nationale Recherche en laatstgenoemde zich specifiek richt op de opsporing en bestrijding van zware (inter)nationale misdrijven doet niet af aan de territoriale binding van de politie.

130 Hier dient te worden opgemerkt dat het direct waarschuwen van de slachtoffers via de ISP's alleen kan plaatsvinden als de IP-adressen voor of vlak na een daadwerkelijke ontmanteling bekend zijn.

TUSSENCONCLUSIE

Voor wat betreft de Bredolab ontmanteling kan worden geconcludeerd dat terug-hacken naar zowel de verdachte als naar de slachtoffers een privacyschending heeft opgeleverd. De doelen en technische specificaties waren dermate uiteenlopend, dat mijns inziens kan worden gesteld dat terug-hacken per definitie dient te worden getoetst aan artikel 8 EVRM.

HOOFDSTUK 3 TERUG-HACKEN EN DE RECHTSTAAT

In dit hoofdstuk worden enkele observaties gedeeld betreffende de houding van de opsporingsdiensten tegenover rechtstatelijke binding en de wens voor een brede terug-hack bevoegdheid.

3.1 OPSPORINGSDIENSTEN EN RECHTSTATELIJKE BINDING

Uit het tweede hoofdstuk is gebleken dat de gehanteerde opsporingsmethode bij het Bredolab botnet in strijd is met fundamentele mensenrechten en derhalve ongeoorloofd. De inmenging op het privacyrecht was bij het OM bekend, terwijl de waarde van het EVRM onderbelicht bleef.

Het OM ging uit van een privacy inmenging bij het terug-hacken naar de slachtoffers omdat " *je iets stuurt naar iemand en een aantal van de geïnfecteerde computers zich in huizen zal bevinden. In ruimtes waar mensen onbevangen zichzelf moeten kunnen zijn. En als je mensen daar benadert kunnen ze op dat moment niet even onbevangen zichzelf zijn, want ze worden geconfronteerd met de politie en dat is een privacy schending."*[131]

De beschermingsomvang van artikel 8 EVRM inclueert niet alleen de woning maar ook het ICT-systeem.[132] Bij het terug-hacken naar de verdachte is enkel naar de aard en onderzoekbijdrage van de bevoegdheid gekeken. Het te verwachten effect van de bevoegdheid en van de inmenging had moeten worden meegewogen.[133]

Het optreden was niet *bij wet voorzien*. Dit criterium behelst de binding aan rechtstatelijke beginselen door de overheid. In het geval van de Bredolab ontmanteling ontbrak deze binding.

---

131 Interview L. van Zwieten Landelijk Parket 23 juni 2011. Locatie: Posthumalaan 74, Rotterdam. Tijd: 10:30.

132 Zie paragraaf 2.1.

133 Over de grenzen van strafvorderlijk optreden stelt Corstens dat *"strafvorderlijke wetgeving geen overzicht geeft van opsporingsmethodes maar de kern aangeeft van de grenzen die aan de overheid zijn opgelegd bij het maken van inbreuk op rechten en vrijheden van burgers. De overheid mag, zolang zij geen inbreuk maakt, dezelfde handelingen uitvoeren als iedere gewone burger. Voor zover de overheid meer zou willen doen en dit meerdere zou bestaan uit inbeuk op rechten omschreven in de grondrechtelijke of fundamentele rechten verdragen, moet zij daarvoor een uitdrukkelijke legitimatie in de wet in formele zin aanwijzen. Als die er niet is dient zij zich van zo'n inbreuk te onthouden, hoe respectabel haar oogmerk ook mag zijn."* G. Corstens. 2008 p. 275.
Simmelink stelt*: "de aard van de betrokken bevoegdheid is niet doorslaggevend maar het effect dat de handeling teweeg brengt is noodzakelijk voor de vraag of een bevoegdheid een formeel wettelijke grondslag betreft"*J.Simmelink 1987 p. 43.

Uitspraken in de media van THTC en OM kunnen verleiden tot de conclusie dat rechtstatelijke binding in meerdere gevallen ontbreekt.

Peter Zinn, senior advisor van THTC laat weten dat, ondanks de ontstane commotie rond de legitimiteit van het optreden bij de Bredolab ontmanteling, zijn team niettemin op de ingeslagen weg voortgaat *"al mag het misschien niet van de rechter".*[134] Dat een zaak door dergelijke beslissingen kapot kan gaan neemt hij voor lief.

In een artikel over de bestrijding van cybercriminaliteit in Vrij Nederland van 28 Juni 2011 vertelt OvJ van Zwieten *"Soms doen we dingen waarvan we niet weten hoe de rechter ertegenaan kijkt. En zoeken we creatief naar mogelijkheden die de wet biedt voor dit nieuwe speelveld."* Over het opsporen van een aantal hackers die zich uitgaven onder de naam Antisec NL[135] stelt de leider van het THTC Pim Takkenberg*"We zijn niet geïnfiltreerd, we hebben slechts meegekeken bij Anonymous."* Hoe de mogelijkheid tot het meekijken op het niet openbare chat kanaal is ontstaan noemt OvJ van Zwieten *"het geheim van de smid".*[136] In een recent item van het NOS journaal, over het oprollen van een internationaal kinderporno netwerk, kwam de OvJ met een opmerkelijke vergelijking: *"Hacken is een misdrijf. Wat wij hebben gedaan is het betreden van computersystemen waarbij we een beveiliging hebben doorbroken. Eigenlijk vergelijkbaar met een huiszoeking waarbij we ook wel eens een deur moeten doorbreken".*[137]

Naar aanleiding van een uitzending van het tv-programma van *Nieuwsuur,*[138] waarin van Zwieten een toelichting gaf op de Bredolab ontmanteling, stelde PvdA-parlementariër Recourt Kamervragen die zich toespitsten op de totstandkoming van een terug-hack bevoegdheid. In reactie op deze vragen gaf de minister aan dat Nederland een terughoudend beleid zal voeren inzake het grensoverschrijdend terug-hacken.[139] Mijns inziens sluit dit niet aan met de realiteit, daar is geconstateerd dat het terug-hacken naar de slachtoffers onnodig grensoverschrijdend was.

134 30 april 2011 http://www.bndestem.nl/algemeen/internet/8611463/KLPD-zoekt-grenzen-op-internet-op.ece.
135 Zie voor algemene informatie over Anonymous: http://en.wikipedia.org/wiki/Anonymous_%28group%29. Het persbericht van de arrestatie is middels de volgende link beschikbaar: http://www.om.nl/actueel-0/nieuws-persberichten/@155993/vier-verdachte/.
136 Online op te vragen via: *http://www.vn.nl/Standaard-Media-Pagina/Hackersjacht.htm* .
137 NOS journaal 20:00 uur. 31-8-2011.
138 Maandag 25 oktober 2010 http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html.
139 Ah-tk-20102011-578 2010/2011 nr. 578.

Over de legitimiteit van de Bredolab ontmanteling en positie van de minister ten opzichte hiervan werden in de Kamer overigens geen vragen gesteld.[140] Parlementaire controle op terug-hacken heeft tot op heden ontbroken.

In casu is het privacyrecht geschonden van zowel een grote groep slachtoffers als de verdachte. Het effect van deze privacy schending is van een andere aard dan het doorzoeken van een woning. Het is dan ook vreemd dat de analogie met huiszoeking wordt gemaakt om het terug-hacken te legitimeren. Feitelijk is het zo dat het eerste inderdaad legitiem is en met waarborgen omkleed maar het tweede niet.

Deze ontwikkelingen leiden tot de verwachting dat toekomstig optreden evenmin zal plaatsvinden in lijn met de rechtstaatgedachte.

Daarnaast heeft het THTC in de voorbereiding van de ontmanteling belangrijke hoeveelheden malware door de botherder op de bots laten plaatsen, waarbij niet werd ingegrepen. Dit werd uitgesteld om een zo succesvol mogelijke ontmanteling te bewerkstelligen, waardoor de internationale internetgemeenschap de slagkracht van het THTC zou ervaren.

Het is curieus om de significante overeenkomst met de IRT-affaire te signaleren. Het schenden van de privacy en het doorlaten van grote partijen drugs om het internationale drugscircuit een klap toe te brengen gaven destijds aanleiding tot het instellen van de Parlementaire enquêtecommissie van Traa. De commissie concludeerde dat voor de verwezenlijking van het rechtstatelijk gedachtegoed opsporingsmethoden een uitdrukkelijk wettelijke grondslag behoeven.[141] Het uiteindelijke rapport heeft geresulteerd in de implementatie van de Wet Bijzondere opsporingsbevoegdheden. In deze wet zijn een groot aantal opsporingstechnieken van een expliciet wettelijke bevoegdheid voorzien.[142] Mijns inzien is er geen aanleiding om in geval van cybercriminaliteit van rechtstatelijke beginselen af te wijken.[143]

---

140 *Aanhangsel handelingen II* 2010/11, nr. 453.

141 *Kamerstukken II* 1995/96, 24 072, nr. 10-20 Rapport van Traa p. 452.

142 Tevens is na de IRT affaire in artikel 126ff Sv opgenomen dat de opsporingsambtenaar in het algemeen is verplicht om voorwerpen die een gevaar kunnen vormen in beslag te nemen. In casu gaat het om gegevens en geen voorwerpen. In de geest der wet zou malware niet doorgelaten mogen worden.

143 Kennelijk denken de opsporingsambtenaren daar anders over. Op de European Police Chiefs Convention 2011 van Europol werd door workinggroup on Organised Crime gepleit voor: *"more creative approach to combatting*

3.2 TERUG-HACKEN VOOR ANDERE DOELEN

In de *Nieuwsuur* uitzending over de Bredolab ontmanteling meent OvJ van Zwieten dat een terug-hack bevoegdheid *"een heel effectief middel zou kunnen zijn in de bestrijding van deze criminaliteit"* […] *"een groot voordeel van het op afstand kunnen benaderen van computers is dat je rechtstreeks en zonder de vertragende factor van collegiaal overleg criminele systemen kunt aanpakken, ook ver in het buitenland."* De OvJ erkent dat de wet moet worden aangepast om deze bevoegdheid te realiseren.[144]

THTC- leider Pim Takkenberg deelt deze opvatting en pleit in de media voor een terug-hack bevoegdheid. In Vrij Nederland zegt hij hierover: *"Eigenlijk heb ik behoefte aan een wet waarin dat expliciet is geregeld."*

Met de terug-hack bevoegdheid wordt meer bedoeld dan alleen een techniek ter bestrijding van botnets. Analyse van het interview dat voor deze scriptie met OvJ van Zwieten is gedaan, levert vier doelen voor de terug-hack bevoegdheid:

a) vaststelling van de locatie van de cybercrimineel
b) bemachtiging van een decryptiesleutel
c) manipulatie van het systeem
d) vergaring van bewijs

Een concreet wetsvoorstel is tot op heden niet ingediend. De minister erkent wel de behoefte aan een terug-hack bevoegdheid en belooft onderzoek te doen naar de haalbaarheid. De parlementaire ontwikkelingsgang van terug-hacken als opsporingstechniek is in Bijlage III uitgewerkt.

---

criminality, that looks beyond traditional law enforcemenet investigations, procecutions and survaillance methods (...).".Europol 2011, *European police chiefs convention, the future of Organised crime. Challenges and recommended actions*. p. 3

144 http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html *5:47min.*

CONCLUSIE

Reflecterend op deze Bredolab botnet studie kan worden geconstateerd dat het feitelijke kader minder spectaculair was dan aanvankelijk werd voorgesteld. Zo werd naar de media melding gemaakt van 143 command en control servers en bleek het uiteindelijk om 6 stuks te gaan. Ook werden dubieuze berekeningen gemaakt om tot een aantal van 30 miljoen botclients te komen, en bleek later dat het eigenlijke aantal onbekend is gebleven en waarschijnlijk lager lag. Er is niet veel fantasie voor nodig om te veronderstellen dat het feitenkader van deze zaak is opgepoetst om de noodzaak van door Justitie gewenste bevoegdheden te onderbouwen.

Aan de andere kant is daar het in mijn ogen wel vrij spectaculaire juridische kader.
Justitie besloot het botnet te ontmantelen in de hoop daarmee een klap uit te delen aan het internationale cybercriminele circuit. Zij maakte voor deze ontmanteling gebruik van de discutabele opsporingsmethode terug-hacken. Met gebruikmaking van valse signalen en valse sleutels werd binnengedrongen op de botnet servers om daar gedurende tien weken verdachte te monitoren en observeren. Daarnaast werd via het botnet toegang verworven tot alle aangesloten computers van de slachtoffers om daarop bestanden toe te voegen. Vanwege de belangrijke rol van ICT-systemen op het dagelijks leven en de toegang tot een potentieel uiterst groot en veelzeggend databestand, vormt terug-hacken een inmenging op het privacyrecht ex. art. 8 EVRM, ook wanneer de systemen zich buiten de directe fysieke omgeving van de gebruiker bevinden en zelfs voor verdachten.

Justitie creëerde de mogelijkheid tot terug-hacken naar de verdachte door gebruik te maken van de tap- en inbeslagnamebevoegdheid. Het te verwachten effect op de privacy van deze bevoegdheden: inzage in telecommunicatie en vroeger opgeslagen gegevens, wijkt significant af van het effect van de inmenging bij terug-hacken: het heimelijk monitoren en onderzoeken van handelingen. Daarnaast is het bij inbeslagname onduidelijk hoe de verhoudingen liggen tussen de eigenaar van een gegevensdrager, de eigenaar/gebruiker van de gegevens en de opsporingsdiensten.

Middels de algemene taakstelling van de politie en een schulduitsluitingsgrond meende Justitie bevoegd te zijn tot het terug-hacken van de slachtoffers. De taakstelling voorziet slechts in een

bevoegdheid wanneer een niet meer dan geringe inbreuk op de privacy speelt. In een rechtsstaat komt echter het vaststellen van straffeloosheid toe aan de rechtsprekende macht en niet aan de uitvoerende macht. Daarnaast slaat de strafuitsluiting op het verspreiden of beschikbaar stellen van malware om schade te voorkomen, terwijl in casu via het botnet toegang is verworven en gegevens zijn toegevoegd.
Deze handelingen zijn strafbaar gesteld in art. 138ab en 350a Sr en zonder bijzondere strafuitsluitingsgrond.

Door de afwezigheid van strenge, heldere en gedetailleerde wetgeving is het effect van de inmenging niet in te schatten, waardoor de voorzienbaarheid bij wet ontbreekt en terug-hacken een schending van het privacyrecht oplevert.

Daarnaast verkeerde Justitie in de kennelijke veronderstelling wereldwijd geroepen te zijn cybercriminaliteit te bestrijden, waardoor de less restrictive means voor de inmenging op het privacyrecht van de slachtoffers niet afdoende zijn overwogen.

Uitspraken gedaan in de media leiden tot verwarring. Vreemde formuleringen en subjectieve waardetoekenning veroorzaken een rookgordijn voor de feitelijke handelingen en lijken de grenzen van bevoegdheden op te rekken.

Het onderzoek naar de vraag in hoeverre terug-hacken vanuit het privacyrecht bezien een gelegitimeerde opsporingsmethode is, leidt tot de volgende conclusie:

Terug-hacken onder huidig recht is geen gelegitimeerde opsporingsmethode. Justitie ontbeert de bevoegdheid om terug te hacken. Het technisch effect van terug-hacken op de privacy is de totaalsom van het doorzoeken, aftappen, heimelijk volgen, observeren en infiltreren. Hierdoor is het onmogelijk om terug-hacken onder een reeds bestaande bevoegdheid te schuiven. De inmenging op het privéleven is schrikbarend groot.

Mocht de wetgever een terug-hack bevoegdheid wenselijk achten, is het mijns inziens noodzakelijk strikte doelen te formuleren en voldoende waarborgen en toetsen in te bouwen. Daarnaast zal toepassing van een eventuele terug-hack bevoegdheid altijd de art. 8 EVRM toets moeten doorstaan.

VERKLARENDE WOORDENLIJST

Afnemers van de botherder: cybercriminelen die tegen betaling gebruik maken van de mogelijkheden van het botnet.

Botherder: de malware exploitant (cybercrimineel).

Botclient/bot: een geïnfecteerde computer die deel uit maakt van een botnet.

Botnet: een groep computers geïnfecteerd met malware. Door de malware verkrijgt de botherder de controle over het besturingssysteem van de computers, zonder dat de rechtmatige gebruikers dit weten.

Botnet-hijacking: het kapen van een botnet door middel van hacken, waardoor de kaper de controle krijgt over de botclients.

Botnet ontmanteling: het uitschakelen van een botnet.

Bredolab botnet: naam van het botnet, ontmanteld door het KLPD op 25 oktober 2010. Andere botnets die gebruik maken van dezelfde Bredolab malware, worden niet in deze scriptie geadresseerd.

Broncode: programmacode van software of malware.

Cloud computing: ICT gebruik waarbij een computer, smartphone o.i.d. verbinding maakt met een (dienst van een) server en zo de gebruiker in staat stelt om de dienst of server te gebruiken of te besturen.

Command en control server: server met de besturingssoftware van het botnet. Vanaf deze server krijgen de bots commando's.

Community Outreach Project Leaseweb: project van LeaseWeb waarbij gratis server capaciteit en bandbreedte ter beschikking wordt gesteld aan bedrijven die samen met LeaseWeb de veroorzakers van cybercriminaliteit monitoren, identificeren en aanpakken.

Cookie: kleine hoeveelheid data die een server via de browser naar de harde schijf van een computer stuurt met de bedoeling deze op te slaan en bij een volgend bezoek weer op te vragen. Zo kan de server de computer herkennen.

Credentials: informatie benodigd om toegang te krijgen tot randapparatuur of diensten. Vaak is dit de combinatie username en password.

Cybercrimineel: pleger van klassieke misdrijven middels geautomatiseerde netwerken of werken, ook pleger van specifiek digitale misdrijven.

Datacenter: de faciliteit waar kritische ICT-apparatuur (servers) wordt ondergebracht.

DDoS-aanval: aanval waarbij een grote groep botclients contact zoekt met één specifiek IP-adres. Door de grote hoeveelheid contactverzoeken is de ontvangende server overbelast en is de website of dienst tijdelijk voor reguliere gebruikers onbereikbaar.

Dedicated hosting: type internet hosting waarbij de provider een gehele server verhuurt, waardoor het besturingssysteem van de server door de afnemer wordt bepaald en beheerd. De hosting provider heeft beperkte controle over de server.

Decryptiesleutel: sleutel om encryptie ongedaan te maken.

Dedicated hosting afnemer: afnemer van dedicated hosting dienst.

Download platform: malware functie die toeziet op het plaatsen van andere malware of plug-ins op de botclient.

Drive-by downloads: malware infecties die zonder nadrukkelijke handeling van de gebruiker tijdens het surfen op internet plaats vinden.

Encryptie: versleuteling van digitale bestanden.

.exe/ Exexutable file: bestand dat door een computer uit te voeren is. Bijvoorbeeld installatiebestanden van een programma.

Exploit: software die de computer scant op beveiligingslekken in het besturingssysteem of in de programmasoftware. Bij aanwezigheid van een dergelijk lek installeert de exploit malware op de computer.

Fast Flux networks: communicatietechniek waarbij de botclient een tiental domeinnamen benadert om commando's van de botherder te ontvangen, door middel van een bepaald algoritme. In de broncode van de botclient zijn de domeinnamen en het algoritme door de botherder geprogrammeerd. Met gestolen creditcard gegevens huurt de botherder de domeinnamen bij wisselende domeinaanbieders.

Hosting provider: een aanbieder van webruimte, webdiensten en server faciliteiten.

IP-adres: een adres waarmee een apparaat op internet wordt geïdentificeerd. De functie van IP-adressen is te vergelijken met die van telefoonnummers en leiden direct naar het land van herkomst.

IRC: Internet Relay Chat-channel. Een afgesloten chat kanaal.

ISP: Internet Service Provider. Bijvoorbeeld toegangsproviders als XS4ALL of KPN.

Keystroke logger: een malware functie die de toetsaanslagen van het slachtoffer registreert en doorstuurt naar de command en control servers.

Man-in the middle-attack: een aanval waarbij communicatie tussen twee partijen heimelijk onderschept wordt. De afgevangen gegevens worden voor andere criminele doeleinden gebruikt.

Malvertising: een Drive-by download techniek waarbij malware exploits via online advertenties worden verspreid. De cybercrimineel biedt besmette advertenties aan bij advertentiebedrijven of hackt de servers en infecteert bestaande advertenties.

Malware: verzamelnaam voor kwaadaardige software en programmacodes. Malware is de afkorting van *malicious software*.

Mothership: alle command en control servers van een botnet.

NAW gegevens: naam, adres, woonplaats - gegevens zoals bekend bij de aanbieders van telecommunicatiediensten. Deze gegevens kunnen door Justitie ex art. 126na Sv. worden opgevraagd.

Opgeslagen gegevens: statische gegevens opgeslagen op computer of gegevensdrager.

Patch: software om malware onschadelijk te maken en te verwijderen.

Phishing: is een vorm van internetfraude die slachtoffers naar een valse (bank)website lokt. De op deze manier verkregen gegevens worden naar de phishing-cybercrimineel gestuurd.

Plug-in: klein bestand dat extra functionaliteiten aan malware toevoegt.

Proxy server: wordt ingezet om begin- en eindpunt van de route die gegevens op het internet afleggen lastiger traceerbaar te maken.

Project Taurus: publiek privaat project geïnitieerd door KLPD en OM voor een verbeterde informatie positie met betrekking tot de bestrijding van botnets.

Project Tolling: projectnaam voor de Bredolab ontmanteling. Bij dit project waren betrokken: OM, THTC van de KLPD, GOVCERT.NL, NFI, LeaseWeb, Kaspersky antivirus lab en Fox IT.

Server: een computer die diensten verleent. Vaak kan de server via een netwerk worden bereikt.

Slachtoffer: rechtmatige gebruiker van een met malware geïnfecteerde computer.

Spam: ongewenste email in bulk verzonden.

Stromende gegevens: maken op het moment van onderzoek deel uit van het telecommunicatieverkeer.

Terug-hacken: op elektronische wijze heimelijk toegang verschaffen of binnendringen in een geautomatiseerd werk of netwerk. Dit kan met gebruikmaking van technische hulpmiddelen, valse signalen, valse sleutels of valse hoedanigheid, door zonder weet van de gebruiker eerst de fysieke controle over het geautomatiseerd werk te verkrijgen of op afstand, door bijvoorbeeld tussenkomst van internet.

Trojan downloader: een klein bestand dat de computer opdracht geeft een server te benaderen en de daar aangetroffen malware te downloaden.

VPN-verbinding: beveiligde tunnel verbinding naar een server. Het IP adres van de server is wel te zien, het IP-adres van de gebruiker niet.

BIJLAGE I BESCHRIJVING MALWARE: BOTNET

Botnets

Een botnet is een groep computers geïnfecteerd met malware die het besturingssysteem van de computers onder controle van de malware exploitant brengt, zonder dat de gebruikers hier weet van hebben.
De term malware is de afkorting van *malicious software* en de verzamelnaam voor vormen van kwaadaardige software en programmacodes.
Aan de hand van actoren, besmetting, functionaliteit, gebruiksmodellen, businessmodellen, aantallen en omvang zal in deze bijlage inzicht worden gegeven in het gebruik en de complexiteit van botnets.

1 Actoren

Bij een botnet zijn meerdere actoren betrokken: de botherder, afnemers van de botherder, botclients en slachtoffers. De botherder is de malware exploitant, deze heeft de controle over het botnet. De afnemers van de botherder maken (tegen betaling) gebruik van de mogelijkheden van het botnet.
Een geïnfecteerde computer die deel uit maakt van het botnet wordt botclient of bot genoemd. Onder de term slachtoffer zal naar de rechtmatige gebruiker van een geïnfecteerde computer worden verwezen.

2 Besmetting

De meest voorkomende besmettingswijzen zullen hier worden besproken.
Infectie vindt plaats doordat de botherder ‘slim’ gebruik maakt van beveiligingslekken, zogeheten drive-by downloads, of omdat het slachtoffer een ‘domme’ handeling uitvoert, en zodoende opdracht geeft tot het installeren van de malware.

2.1 Drive-by downloads

Drive-by downloads refereren aan infecties die worden opgedaan tijdens het surfen op internet zonder nadrukkelijke handeling van het slachtoffer. De botherder besmet internetlocaties met exploits. Een exploit intendeert in deze scriptie de software die de computer van een

websitebezoeker scant op beveiligingslekken in het besturingssysteem of in de programmasoftware. Als een beveiligingslek is gedetecteerd verschaft de exploit toegang tot de computer en installeert hier een trojan downloader, een klein bestand dat de computer opdracht geeft een bepaalde server te benaderen om de daar aangetroffen malware te downloaden. De malware installeert zichzelf. Na installatie van de malware is de infectie geslaagd en maakt de computer deel uit van het botnet. Dit alles geschiedt zonder weet van het slachtoffer. Er zijn drie verspreidingsvarianten voor drive-by download exploits.

Bij de eerste variant beheert een botherder zelf een website en probeert hier zo veel mogelijk bezoekers naartoe te lokken. Omdat naast het beheer van het botnet de botherder ook het nodige aan marketing moet doen, is dit een relatief ineffectieve verspreidingsvariant.[1]
De tweede variant is effectiever. De botherder hackt een goedbezochte website en plaatst exploits in een verborgen laag onder de site. Hij doet dit door ofwel gebruik te maken van een beveiligingslek in het besturingssysteem of programmasoftware van de server dan wel middels gestolen credentials.[2]
De derde en meest geavanceerde drive-by download variant wordt *malvertising* genoemd, afkorting van *malicious advertising.* De exploits worden via online advertenties verspreidt. Veel populaire websites tonen advertenties, waarbij het beheer is uitbesteed aan specialisten. Deze vullen de advertentieruimte door alleen advertenties te tonen die aansluiten bij het gedrag en de interesse van de individuele website bezoeker.[3] De advertenties zijn niet afkomstig van de server van de bezochte website maar van een server van het online advertentiebedrijf.

Men kan twee infiltratietechnieken voor malvertisement onderscheiden.
a) de botherder breekt via een beveiligingslek in op de advertentie server. Vervolgens verbergt hij zijn exploits in aanwezige advertenties. Op deze manier kan een grote hoeveelheid advertenties worden besmet en op verschillende websites worden getoond. Het bereik naar potentiële slachtoffers is hierdoor groot. Echter zodra de hack is opgemerkt worden maatregelen genomen tegen de verspreiding van de exploits.
b) De botherder maakt een of meer schijnadvertenties waarin hij exploits verbergt. Hij doet zich voor als marketeer en levert de schijnadvertenties aan bij de online adverteerder, die ze laten rouleren op verschillende websites. De advertenties worden betaald met gestolen creditcard gegevens.

2.2 Infectie door handeling slachtoffer

De methoden van de botherder om een ‘infecterende’ handeling uit te lokken zijn dermate geraffineerd dat het slachtoffer zich zelden bewust is dat hij door middel van een meer actieve handeling een infectie veroorzaakt.

Veel voorkomende valkuil is het openen van email bijlagen waarvan de file extensie, waarmee het type bestand, wordt aangeduid niet is onderzocht. De botherder zorgt voor betrouwbaar ogende bijlagen. De file extention '.doc.exe' zal niet snel worden gewantrouwd, terwijl dit wel degelijk malware is. De .doc.exe bestanden bevatten een trojan downloader.

Een tweede voorbeeld is het afspelen van een online videofragment. Met gehackte accounts wordt de video aangeprezen. De opdracht tot afspelen behelst in dergelijke gevallen ook de opdracht tot het installeren van malware. Gebruik van beveiligingsmaatregelen, zoals een firewall en virusscanner, kan het risico op infectie verminderen.

3 Functionaliteit botnet

Na infectie staat de botclient onder controle van de botherder. Op de command en control server beheert en bestuurt hij het botnet.
In veel gevallen bevat de basis malware een download platform en een keystroke logger. Als de botherder een kwantitatief groot botnet nastreeft, bevat de door hem geëxploiteerde malware een functionaliteit (keystroke logger) die erop toeziet hij alle credentials aan het slachtoffer onttrekt. Op deze manier kan de botherder zich toegang verschaffen tot social network pagina’s en andere websites van het slachtoffer, om ook hier exploits verbergen.

Op het download platform kunnen overige malware of plug-ins geïnstalleerd worden. De plug-in is een klein bestand dat extra functionaliteiten aan de malware toevoegt. Recente botnet ontwikkelingen laten zien dat het installeren van plug-ins een lucratieve methode is.[4]

4 Gebruiksmodellen

Een botclient kan op verschillende manieren worden gebruikt:
a) voor opslagcapaciteit.
b) voor netwerkcapaciteit.
c) als doorzendcapaciteit voor afgetapte of opgeslagen gegevens van het slachtoffer.

4.1 Opslagcapaciteit

De botherder geeft de botclient opdracht een verborgen map op de harde schijf te creëren en deze te vullen met aangeleverde (illegale) content. Deze content staat veelal gefragmenteerd op de harde schijf van meerdere slachtoffers en is bijvoorbeeld via een peer-to-peer netwerk te bereiken. Dit wordt bijvoorbeeld voor het hosten van kinderporno gebruikt.

4.2 Netwerkcapaciteit

Netwerkcapaciteit wordt voornamelijk gebruikt voor het verzenden van spam en uitvoeren van DDoS-aanvallen. Bij een DDoS-aanval zoekt een grote groep botclients contact met één specifiek IP-adres. Door de grote hoeveelheid contactverzoeken is de ontvangende server overbelast en is de website of dienst tijdelijk voor reguliere gebruikers onbereikbaar. Dit wordt bijvoorbeeld ingezet als pressie- en intimidatiemiddel, als afweermechanisme of als wapen bij een aanval van een andere hacker. Soms wordt de techniek ook gebruikt door hacktivists om hun ideologisch gedachtegoed onder de aandacht te brengen.[5]

4.3 Doorzendcapaciteit voor afgetapte of opgeslagen gegevens van het slachtoffer

Veruit de meest veelzijdige toepassingsmogelijkheid is de doorzendcapaciteit voor afgetapte of opgeslagen gegevens van het slachtoffer.

Naast de algemene keystroke logger voor het aftappen van credentials zijn er tal van gespecialiseerde technieken die voornamelijk worden gebruikt voor E-spionage en het onttrekken van financiële en persoonlijke gegevens voor verdere fraude.

E-spionage vindt vooral plaats bij bedrijven of overheidsinstellingen. Middels de botclient kan de botherder de opgeslagen bestanden van het slachtoffer doorzoeken, kopiëren, doorzenden, wissen, aanpassen en verwijderen. Daarnaast kan de computer op afstand worden bestuurd en kan bijvoorbeeld de microfoon en webcam aan en uit worden gezet.

Fraude betreft vooral de identiteit- en financiële gegevens van individuele slachtoffers. Daarnaast vormen de banken zelf een gewild doelwit. Door infiltratie in het banksysteem kunnen de identificatie, accordatie, authenticatie systemen gemanipuleerd worden en ontstaat een digitale witwas-straat.

5 Businessmodellen

De lezer zal intussen mogelijk zijn afgedwaald naar de legio exploitatie modellen van botnets. Bij E-spionage en een witwas-straat zijn de kwaliteit en locatie van de geïnstalleerde botnets van belang. De infectie is moeilijk omdat deze is gericht op personen in een specifieke positie. De complexiteit van de infectie en de malware maakt dat er veel geld voor kan worden gevraagd.

Bij willekeurige infectie via drive-by downloads zit de kracht in de kwantiteit. Deze infectie is gemakkelijker en heeft sneller resultaat, waardoor meer structurele inkomsten kunnen worden gegenereerd. De botherder kan ofwel inspringen op een bestaande vraag dan wel een specifieke opdracht voor een afnemer uitvoeren, waarbij hij het botnet als het ware verhuurd. [6]

Geavanceerd botnet

Bij de meer geavanceerde botnets, zoals het TDL-4 botnet,[7] past de botherder de malware middels plug-ins aan op het benodigd aantal botclients. Deze sturen de afgevangen gegevens direct door naar de afnemers/opdrachtgevers. Middels goed afgeschermde beveiligingsbarrières kan de botherder de opslag- of netwerkcapaciteit van het botnet ook zodanig verhuren, dat zijn tussenkomst overbodig is.

Verouderd botnet

Oude botnet malware, zoals bijvoorbeeld het Bredolab botnet, is geschreven op het installeren van meer malware programma's en niet op het installeren van plug-ins. Voor het versturen van spam en het uitvoeren van DdoS-aanvallen verhuurt de botherder delen bandbreedte. Om te voorkomen dat zijn afnemers het botnet kapen stuurt hij de aanvallen zelf aan. De botherder installeert de malware voor een overeengekomen tijd op overeengekomen botclients. De malware zendt de afgevangen gegevensstroom direct door aan de afnemers. Vóór de installatie zal de botherder de malware goed moeten onderzoeken om de risico's van kaping uit te sluiten.

6 Omvang botnets

Onderzoek naar aantal en omvang van botnets blijkt een lastige opgave.[8]
In de meeste gevallen ontbreek een wetenschappelijke verantwoording over de gehanteerde onderzoekstechniek en -methode.[9] De aantallen die door opsporingsinstanties of virus labs worden genoemd missen vaak precisie en zijn grotendeels onbetrouwbaar.

Een rapport van het European Network and Information Security Agency reuslteert in de constatering dat in bepaalde gevallen de omvang geen indicatie is voor de dreiging van het botnet, omdat de kwaliteit van de bots zwaarder weegt dan de kwantiteit. [10]

Uit een analyse van de University of California blijkt dat het tellen van IP-adressen resulteert in 6,5 keer meer botclients dan het tellen van unieke botclients die contact maken met de command en control servers.[11]

Tussen januari 2009 en zomer 2010 is door TU Delft een schatting gemaakt met als uitkomst dat 450.000 tot 900.000 computers in Nederland besmet en onderdeel is van een botnet.[12]

7 Complexiteit botnets

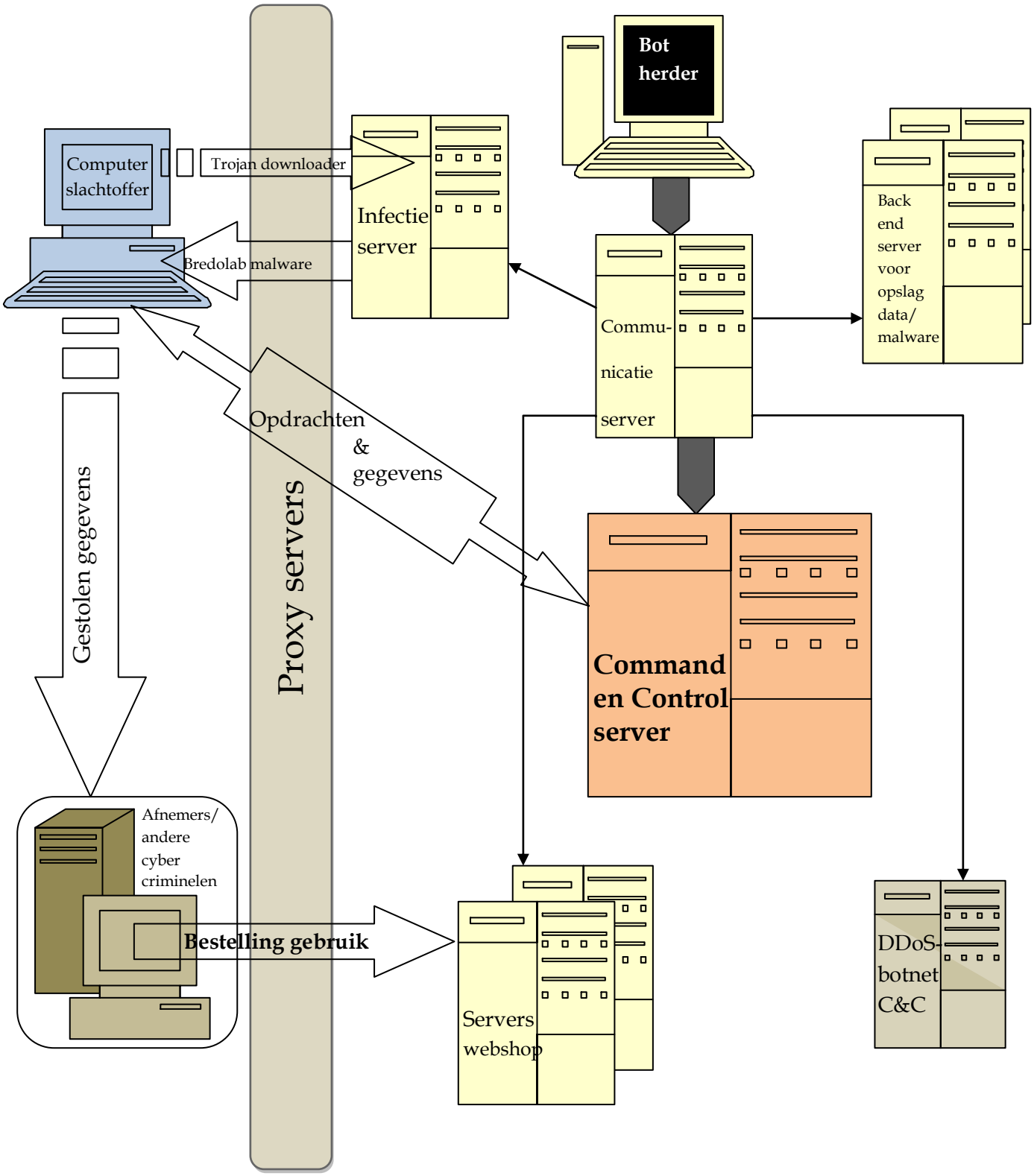
De technische ontwikkeling van botnets zit in een stroomversnelling. Vooral 'botnet- hijacking' (het kapen door een andere hacker) komt erg veel voor, waardoor malware schrijvers continu de beveiliging verbeteren en de botnets steeds onzichtbaarder worden. Detectie door gebruikers en opsporingsinstanties is dus zeer lastig.

Kenmerk van een geavanceerd botnet is het gebruik van de communicatietechniek Fast Flux, waarbij de botclient door middel van een algoritme een aantal domeinnamen benadert voor opdrachten. In de broncode van de botclient zijn de domeinnamen en het ritme door de botherder geprogrammeerd. Met gestolen creditcard gegevens huurt hij de domeinnamen bij wisselende aanbieders.

De botclients en de botherder communiceren met elkaar in IRC of peer to peer channels over https-protocol. Er zijn zelfs botnets die communiceren via social media zoals Twitter. De verbinding wordt via versleutelde kanalen opgezet en de informatie uitwisseling is geëncrypteerd. Door tussenkomst van proxy servers is de route die de informatie volgt lastig te traceren. [13] Daarbij worden vrijwel alle botnets vanaf meerdere command en control servers met een mondiale spreiding aangestuurd.

1 Vaak zijn de domeinnamen van dergelijke websites minimaal afwijkend van veelbezochte websites, waardoor gebruikers door een typefout de website bezoeken.
2 Credentials: informatie benodigd om toegang te krijgen tot randapparatuur of tot een afgesloten gedeelte van een website. Vaak is dit de combinatie: username wachtwoord.
3 Deze vorm van adverteren wordt behavirourl advertising genoemd. Voor meer informatie over dit onderwerp: A. McStay, *Mood of Information: A Critique of Online Behavioural Advertising*, New York: Continuum 2011.
4 Zowel wat betreft de beveiliging naar andere cybercriminelen als naar virusscanners.
5 Hacktivist is de verkorte samenvoeging van het woord hacker en activist. Zie bijvoorbeeld de oproep om DDoS-aanvallen uit te voeren op de infrastructuur van overheidsinstellingen in Orlando, na arrestatie van vrijwilligers in een soup kitchen. http://www.indymedia.nl/nl/2011/06/77027.shtml
6 Bijvoorbeeld een bulk creditcard gegevens uit een land. Nederland is erg in trek.
7 Een technische specificatie van dit botnet: http://www.securelist.com/en/analysis/204792180/TDL4_Top_Bot
8 *Botnets 10 thoug questions*, Enisa 2011.
9 *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Enisa 2011.*
10 *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Enisa 2011.*
11 B. Stone-Gross e.a., 'Your Botnet is My Botnet: Analysis of a Botnet Takeover', *Proceedings of the ACM CCS*, Chicago, IL, November 2009.
12 *Internet Service Providers and Botnet Mitigation, A Fact-Finding Study on the Dutch Market*, Report prepared for the Netherlands Ministry of Economic Affairs, Agriculture and Innovation . TU Delft 2011.
13 Voor een meer technische beschrijving van botnets en de communicatie tussen bot en command en control servers: http://www.honeynet.org/papers/bots

BIJLAGE II BOTNET SCHEMA



BIJLAGE III RELEVANTE WETGEVING PARAGRAAF 2.3.1

Artikel 94 Wetboek van Strafvordering

1. Vatbaar voor inbeslagneming zijn alle voorwerpen die kunnen dienen om de waarheid aan de dag te brengen of om wederrechtelijk verkregen voordeel, als bedoeld in artikel 36e van het Wetboek van Strafrecht, aan te tonen.

2. Voorts zijn vatbaar voor inbeslagneming alle voorwerpen welker verbeurdverklaring of onttrekking aan het verkeer kan worden bevolen.

3. Van de inbeslagneming van een voorwerp wordt, ook in geval de bevoegdheid tot inbeslagneming toekomt aan de rechter-commissaris of de officier van justitie, door de opsporingsambtenaar een kennisgeving van inbeslagneming opgemaakt. Zoveel mogelijk wordt aan degene bij wie een voorwerp is inbeslaggenomen, een bewijs van ontvangst afgegeven.

Artikel 96 Wetboek van Strafvordering

1. In geval van ontdekking op heterdaad van een strafbaar feit of in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, is de opsporingsambtenaar bevoegd de daarvoor vatbare voorwerpen in beslag te nemen en daartoe elke plaats te betreden.

2. De opsporingsambtenaar kan, in afwachting van de komst van de rechter of ambtenaar die bevoegd is ter inbeslagneming de plaats te doorzoeken, de maatregelen nemen die redelijkerwijs nodig zijn om wegmaking, onbruikbaarmaking, onklaarmaking of beschadiging van voor inbeslagneming vatbare voorwerpen te voorkomen. Deze maatregelen kunnen de vrijheid van personen die zich ter plaatse bevinden beperken.

126m Wetboek van Strafvordering

1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, aan een opsporingsambtenaar bevelen dat met een technisch hulpmiddel niet voor het publiek bestemde communicatie die plaatsvindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst, wordt opgenomen.

2. Het bevel is schriftelijk en vermeldt:

a het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;

b de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;

c zo mogelijk het nummer of een andere aanduiding waarmee de individuele gebruiker van de communicatiedienst wordt geïdentificeerd alsmede, voor zover bekend, de naam en het adres van de gebruiker;

d de geldigheidsduur van het bevel;

e een aanduiding van de aard van het technisch hulpmiddel of de technische hulpmiddelen waarmee de communicatie wordt opgenomen.

3. Indien het bevel betrekking heeft op communicatie die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst in de zin van de Telecommunicatiewet, wordt - tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet - het bevel ten uitvoer gelegd met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst en gaat het bevel vergezeld van de vordering van de officier van justitie aan de aanbieder om medewerking te verlenen.

4. Indien het bevel betrekking heeft op andere communicatie dan bedoeld in het derde lid, wordt - tenzij zulks niet mogelijk is of het belang van strafvordering zich daartegen verzet - de aanbieder in de gelegenheid gesteld medewerking te verlenen bij de tenuitvoerlegging van het bevel.

5. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. Artikel 126l, vijfde tot en met achtste lid, is van overeenkomstige toepassing.

6. Voor zover het belang van het onderzoek dit bepaaldelijk vordert, kan indien toepassing is gegeven aan het eerste lid tot degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van versleuteling van de communicatie, de vordering worden gericht medewerking te verlenen aan het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.

7. De in het zesde lid bedoelde vordering wordt niet gericht tot de verdachte.

8. Op de in het zesde lid bedoelde vordering zijn artikel 96a, derde lid, en artikel 126l, vierde, zesde en zevende lid, van overeenkomstige toepassing.

9. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de wijze waarop het in het eerste lid bedoelde bevel en de in het derde en zesde lid bedoelde vorderingen kunnen worden gegeven en over de wijze waarop daaraan wordt voldaan.

Artikel 134 Wetboek van Strafvordering

1. Onder inbeslagneming van eenig voorwerp wordt verstaan het onder zich nemen of gaan houden van dat voorwerp ten behoeve van de strafvordering.
2. Het beslag wordt beëindigd doordat hetzij
a. het inbeslaggenomen voorwerp wordt teruggegeven, dan wel de waarde daarvan wordt uitbetaald;
b. het openbaar ministerie de last geeft als bedoeld in artikel 116, tweede lid, onder c;
c. de machtiging als bedoeld in artikel 117 is verleend en het voorwerp niet om baat is vervreemd;
d. de bewaring ingevolge artikel 118, derde lid, door tijdsverloop is beëindigd en het voorwerp niet om baat is vervreemd.
3. Onder teruggave van inbeslaggenomen voorwerpen wordt begrepen het verrichten van de in verband met de beëindiging van het beslag vereiste formaliteiten.

BIJLAGE IV PARLEMENTAIRE ONTWIKKELINGEN TERUG-HACK BEVOEGDHEID.

In de tweede kamer is de mogelijke terug-hack bevoegdheid voor Justitie voor het eerst besproken op 21 mei 2008 in het notaoverleg *rechtshandhaving bij cybercrime en internetmisbruik*.[1]

Parlementariër Teeven[2] formuleerde de vraag als volgt: "*naar het oordeel van de VVD-fractie kan het bij bepaalde vormen van criminaliteit – wij denken niet alleen aan terrorisme en georganiseerde misdaad, maar ook aan kindermisbruik – nodig zijn om regelmatig te kunnen hacken om criminele en terroristische activiteiten te onderzoeken, zonder dat de betrokkenen daarvan al direct op de hoogte worden gesteld. Door de trojans wordt de communicatie zichtbaar. Sterker nog, het kan zo zijn dat een tap op een communicatiemiddel voor de politie volstrekt waardeloos is als de encryptie niet kan worden ontcijferd. Is de minister van oordeel dat een verruiming van de opsporingsbevoegdheden op dit terrein wenselijk is?*"[3]
De minister van Justitie beloofde de juridische mogelijkheden te onderzoeken.[4]

In een brief van 26 juni 2009 schrijft de minister dat een samenwerkingsverband is opgestart voor een verkenning van de juridische instrumenten en een inventarisatie van knelpunten in wet- en regelgeving.[5] Bij een eerste inventarisatie is gebleken dat binnen het opsporingsveld behoefte bestaat aan de mogelijkheid van het op afstand doorzoeken van computers. De minister benadrukt de complexiteit van het traceren van cybercriminaliteit, omdat het eenvoudig voorkomen kan worden dat sporen worden gevolgd. Hij verwijst hierbij naar de *discussienotitie over cybercrime en internetjurisdictie, ten behoeve van het project cybercrime* van de Raad van Europa. De minister onderstreept de noodzaak van een snelle veiligstelling van gegevens en daarmee een terug-hack bevoegdheid voor de opsporingsdiensten.

In het Concept Wetsvoorstel Versterking Bestrijding Computercriminaliteit van Juli 2010 wordt vermeld dat de behoefte naar een bevoegdheid voor het online doorzoeken of terug-hacken nader zal worden onderzocht en om die reden niet in het wetsvoorstel wordt geadresseerd.[6]

Naar aanleiding van de Bredolab ontmanteling stelde de PvdA -parlementariër Recourt Kamervragen over een wetswijziging [7] Deze vragen richtten zich op de goedkeuring van de minister voor een terug-hack bevoegdheid voor Justitie. De Minister antwoordde dat *"de door de officier van justitie in de uitzending geuite wens overeenkomt met de in het kader van de consultatieronde ter voorbereiding van het wetsvoorstel Computercriminaliteit III geuite wens van het College van procureurs-generaal om een wettelijke grondslag te creëren voor het binnendringen in en betreden op afstand van een geautomatiseerd werk. Na afloop van de consultatieronde zal ik de daarin naar voren gebrachte punten nader bezien."*

Voor wat betreft de internationale dimensie merkte hij op dat veel bevoegdheden nationaal zijn vast te leggen. Het grensoverschrijdende gebruik zal echter mede afhangen van de rechtsmacht die gelegd wordt op de opsporing en vervolging van misdrijven die internationaal of buiten Nederland plaatsvinden en van de mate van internationale acceptatie van die rechtsmacht.[8]

---

1 *Kamerstukken II* 2007/08, 28 684, nr. 149 p. 9.
2 Ten tijde van dit onderzoek is de heer Teeven Staatssecretaris van Veiligheid en Justitie in het kabinet Rutte.
3 *Kamerstukken II* 2007/08, 28 684, nr. 144 en *Kamerstukken II* 2007/08, 28 684, nr. 149.
4 Hierbij zegt de minister toe te kijken naar de uitspraak van het Bundesverfassungsgericht over de Online Durchsuchung. Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07
5 *Kamerstukken II* 2007/08, 28 684, nr. 232 p. 1.
6 *Kamerstukken II* 2007/08, 28 684, nr. 232 p. 2.
7 *Aanhangsel handelingen II* 2010/11, nr. 45.
8 *Aanhangsel handelingen II* 2010/11, nr. 578.

BRONNEN

Parlementaire stukken

Kamerstukken II 1967/68, 9419, nr. 3
Kamerstukken II 1975/76, 13 872, nr. 3
Kamerstukken II 1978/79, 13 872, nr. 3
Kamerstukken II 1985/86, 19 535, nr. 3
Kamerstukken II 1986/87, 19 535, nr. 4
Kamerstukken II 1987/88, 19 403, nr. 15
Kamerstukken II 1990/91, 21 551, nr. 7
Kamerstukken II 1990/91, 21 551, nr. 8
Kamerstukken II 1990/91, 21 551, nr. 11
Kamerstukken II 1991/92, 21 551, nr. 12
Kamerstukken II 1991/92, 22 562, nr. 3
Kamerstukken II 1992/93, 23 251, nr.3
Kamerstukken II 1995/96, 24 072, nr. 10-20
Kamerstukken II 1996/97, 25 392, nr. 3
Kamerstukken II 1996/97, 25 403, nr. 3
Kamerstukken II 1998/99, 26 671, nr. 3
Kamerstukken II 1999/00, 25 530, nr. 40
Kamerstukken II 2001/02, 28 366, nr. 1
Kamerstukken II 2002/03, 28 250, nr. 4
Kamerstukken II 2003/04, 29 441, nr. 3
Kamerstukken II 2004/05, 26 671, nr. 7
Kamerstukken II 2007/08, 28 684, nr. 144
Kamerstukken II 2007/08, 28 684, nr. 149
Kamerstukken II 2007/08, 28 684, nr. 232
Aanhangsel handelingen II 2010/11, nr. 453
Aanhangsel handelingen II 2010/11, nr. 578
Bijlage bij Kamerstukken II 2010/11, 32 653 nr. 1

Jurisprudentie

EHRM 30 mei 1974 decision nr. 5488/74 *(X v. Belgium).*

EHRM 13 mei 1976, nr. 6825/74, *(X v. Iceland).*

EHRM 7 december 1976, nr. 5493/72, *(Handyside v. The United Kingdom).*

EHRM 6 september 1978, nr. *5029/71(Klass and others v. Germany).*

EHRM 25 maart 1983, nr. 5947/72, *(Silver and others. v. the United Kingdom).*

EHRM 2 augustus 1984, nr. 8691/79 *(Malone v. the United Kingdom).*

EHRM 24 mei 1988, nr. 10737/84 *(Müller and others v. Switzerland).*

EHRM 24 april 1990, nr. 11801/85 *(Kruslin v. France).*

EHRM 24 april 1990, nr. 11105/84 *(Huvig v. France).*

EHRM 25 februari 1992,nr. 12963/87 *(Margareta and Roger Andersson v. Sweden).*

EHRM 15 juni 1992, nr. 12433/86 *(Lüdi v. Switzerland).*

EHRM 16 december 1992, nr. 13710/88 *(Niemietz v. Germany).*

EHRM 23 november 1993, nr. 14838/89 *(A. v. France)*

EHRM 26 september 1995, nr. 17851/91 *(Vogt v. Germany).*

EHRM 25 maart 1998, nr 44787/98 *(Halford v. the United Kingdom).*

EHRM 30 juli 1998, nr. 27671/95 *(Valenzuela v. Spain).*

EHRM 16 februari 2000, nr. 27798/95 *(Amman v. Swiss).*

EHRM 28 januari 2003, nr. 44647/98 *(Peck v. the United Kingdom).*

EHRM 22 juli 2003, nr. 24209/94 *(YF v. Turkey).*

EHRM 24 januari 2006, nr. 62617/00, *(Copland v. the United Kingdom).*

EHRM 4 december 2008, nr. 30562/04, *(S. and Marper v. the United Kingdom).*

EHRM 1 juli 2008, nr. 58243/00 *(Liberty and others v. the United Kingdom).*

EHRM 2september 2008, Decision nr. 15301/04 *(Tamm v. Estonia).*

Bundesverfassungsgericht 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07.

HR 14 februari 1916, *NJ* 1916, 681

HR 6 april 1936, *NJ* 1936, 813

HR 2 juni 1936, *NJ* 1936, 1015

HR 4 december 1979, *NJ* 1980, 356

HR 29 september 1981, *NJ* 1982, 258

HR 14 oktober 1986, *NJ* 1988, 551

HR 9 januari 1987, *NJ* 1987, 928

HR 19 februari 1991, *NJ* 1992, 50

HR 19 december 1995, *NJ* 1996, 249

HR 3 december 1996, *NJ* 1997, 574

HR 9 oktober 2009, *NJ* 2010, 213

HR 22 februari 2011 *LJN* BN9287

Pres. Rb Roermond 12-9-1985, KG 1985, 299

Literatuur

P. Balkema e.a. 1995

P. Balkema e.a., *Dynamisch strafrecht, opstellen ter gelegenheid van het afscheid van G.J.M. Corstens*, Arnhemn: Quint Gouda 1995.

Y. Burema e.a. 1998

Y. Burema e.a., *Buitengewone opsporingsmethoden*, Deventer: Tjeenk Willink 1998.

M. Burkens e.a. 2001

M. Burkens e.a., *Beginselen van de Democratische Rechtsstaat. Inleiding tot de grondslagen van het Nederlands Staats- en Besuursrecht*, Deventer: Tjeenk Willink 2001.

C. Cleiren e.a. 2009

C. Cleiren e.a., *Tekst en commentaar Strafvordering*, Deventer: Kluwer 2009.

C. Cleiren e.a. 2010

C. Cleiren e.a., *Tekst en commentaar Strafrecht*, Deventer: Kluwer 2010.

G. Corstens 2008

G. Corstens, *Het Nederlands Strafprocesrecht*, Deventer: Kluwer 2008.

H. den Dolder e.a. 1994

H. den Dolder e.a., *Taak en functioneren van het OM*, SI-EUR-reeks, deel 4, Arnhem: Gouda Quint 1994.

E. Dommering 2000

E. Dommering, *Informatierecht. Fundamentele rechten voor de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2000.

J. Gackenbach & E. Ellerman 1998

J. Gackenbach & E. Ellerman, *Introduction to psychological Aspects of Internet Use in Psychology and the Internet*, J, gackenbach (red.), New York: Academic Press, 1998.

M. Hoekendijk 1985

M. Hoekendijk, *Dwangmiddelen in het strafprocesrecht*, Arnhem: Gouda Quint 1985

J. de Hullu 2009

J. de Hullu, *Materiaal Strafrecht*, Deventer: Kluwer 2009.

M. Klang en A. Murray 2005

M. Klang en A. Murray (ed.), *Human Rights in the digital age*, New York: Routledge-Cavendish 2005.

B.J. Koops 2002

B.J. Koops, *Strafvorderlijk onderzoek van (tele) communicatie 1838-2002: het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002.

B.J. Koops 2007

B.J. Koops, *Strafrecht en ICT*, Den Haag: SDU uitgevers 2007.

W. Koopstra e.a. 2004 (1)

W. Koopstra e.a., *Kernuitgave Opsporingspraktijk. Specifieke onderzoeken en bijzondere opsporingsbevoegdheden*, Den Haag: SDU uitgevers 2004.

W. Koopstra e.a. 2004 (2)

W. Koopstra e.a., *Kernuitgave Opsporingspraktijk. Dwangmiddelen - goederen en plaatsen*, Den Haag: SDU uitgevers 2004.

E. Leukfeldt 2011

E. Leukfeldt, *Verkenning cybercrime in Nederland 2009*, Den Haag: Boom uitgevers 2011.

A. McStay 2001

A. McStay, *Mood of Information: A Critique of Online Behavioural Advertising*, New York: Continuum 2011.

S. McQuade III 2008

S. McQuade III, *Encyclopedia of Cybercrime*, London: Greenwood Press 2008.

P. Mevis 2009

P. Mevis, *Capita Strafrecht*, Nijmegen: Ars Aequi Libri 2009.

S.Michalowski en L.Woods 1999

S. Michalowski & L. Woods, *German constitutional law. The protection of civil liberties*, Ashgate: Brookfield 1999.

F. Miller 2010

F. Miller, *Floppy Disk*, Beau Bassin: Alphascript Publishing 2010.

J. Peters 2003

J. Peters, *Wie beschermd omze grondwet?*, Rede uitgesproken bij de aanvaarding van het ambt van hoogleraar Staats- en bestuursrecht aan de Universiteit van Amsterdam op vrijdag 14 maart 2003. Amsterdam: Vossius pers 2003

J. Simmelink 1987

J. Simmelink, *De Rechtsstaatgedachte achter art. 1 Sv.*, Arnhem: Gauda Quint B.V. 1987.

A. Smits 2006

A. Smits, *Strafvorderlijk onderzoek van Telecommunicatie*, Nijmegen: Wolf Legal publishers 2006.

K. Spaink 2010

K. Spaink, Het *huis uit, de werled in: een kleine telefoongeschiedenis,* in *Wie is U?*, K. Spaink (red.), Amsterdam: Nijgh & van Ditmar, 2010.

B. Wilson 2002

B. Wilson, *Media Technology an Society: A History: From the Telegraph to the Internet*, New York: Routledge 2002.

R. Vennix 1998

R. Vennix, *Boef en Beslag, De strafvorderlijk inbeslagneming van voorwerpen*, Nijmegen: Ars Aequi Libri, 1998.

Artikelen

J. Boek, 'Hacken als opsporingsmethode', *Nederlands Juristenblad* 2000, 11

J. Dommering, 'noot bij HR 9 januari 1987 Bespiede Bijstandsmoeder', *Computerrecht* 1987-2, p.114

M. Groothuis en T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk? Een verkenning', *Privacy & Informatie*, nr. 6- 245, december 2010 p. 278-283

P. de Hert e.a., 'Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online Dursuchung) in breder perspectief", *Computerrecht* 5/2009, p. 200-21

J.Johnson, 'a theory of the nature and value of privacy', *Public affairs Quarterly*, vol. 6 issue 3, 1992 p. 271-288.

B.J. Koops & M.M. Prinsen, 'Glazen woning, transparant lichaam. Een toekomstblik op huisrecht en lichamelijke integriteit', *Nederlands Juristenblad* 12 maart 2005, p. 624-630.

B.-J. Koops & P. De Hert, 'Constitutional Rights and New Technologies. A Comparative Study' *Information Technology & Law Series*, vol. 15, T.M.C. Asser Press: Den Haag 2008, p. 137-158

J.J. Oerlemans en B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *Nederlands Juristenblad* 2011, 914

J.J. Oerlemans, 'Conceptwetsvoorstel Computercriminaliteit III: Onzorgvuldige wetgeving?', *Informatiebeveiliging*, nr. 4 2011 p. 8-11

B. Stone-Gross e.a., 'Your Botnet is My Botnet: Analysis of a Botnet Takeover', *Proceedings of the ACM CCS*, Chicago, IL, November 2009

C.J. Sykes, in: R. Whitaker, *The End of Privacy: How Total Surveillance Is Becoming a Reality*, New Press 1998, nr.33

S. Warren en L. Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol. IV 15 December 1890, Nr. 5

Onderzoek rapporten

Botnets 10 thoug questions. Enisa 2011.
beschikbaar via: http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Enisa 2011. beschikbaar via: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence

Position statement on botnets prepared for the Ministerial Conference on CIIP organised by the Hungarian EU Presidency in Balatonfüred on 14-15 April 2011. Enisa 2011. beschikbaar via: http://www.enisa.europa.eu/act/res/botnets

Botnets: Overview and Case Study , the history of the botnet. Mahathi Kiran.Kola, 2008. beschikbaar via: https://www.mercy.edu/ias/kola.pdf

Internet Service Providers and Botnet Mitigation, A Fact-Finding Study on the Dutch Market, Report prepared for the Netherlands Ministry of Economic Affairs, Agriculture and Innovation . TU Delft 2011.

A Trend Micro White paper Bredolab, Bredolab's sudden rise in prominence. David Sancho, October 2009.beschikbaar via: http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/bredolab_final.pdf

Trend Micro: BREDOLAB Simple but Effective. beschikbaar via: http://threatinfo.trendmicro.com/vinfo/articles/securityarticles.asp?xmlfile=031610-BREDOLAB.xml

Actualisering van dreigingen uit 2004, verslag van het onderzoek voor het dreigingsbeeld van 2008, KLPD dienst IPOL. Beschikbaar via: http://www.politie.nl/KLPD/Images/2008actualiseringdreigingenuit2004_tcm35-425012.pdf

Social Networking, Privacy and Age, EU Kids online, London School of Economics. S. Livingstone e.a. april 2011. Beschikbaar via: www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf

ICT gebruik van personen naar persoonskenmerken, Centraal Bureau voor de Statistiek, Gewijzigd op 26 oktober 2010, Verschijningsfrequentie: eenmaal per jaar. beschikbaar via: http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=71098ned&D1=0-14&D2=0-2&D3=a&HD=080506-1314&HDR=G1,G2&STB=T

High-tech crime, soorten criminaliteit en hun daders, WODC 2008. beschikbaar via: http://wodc.nl/onderzoeksdatabase/1477a-high-tech-crime.aspx?cp=44&cs=6798

Nationaal Trendrapport Cybercrime en Digitale veiligheid, 2010. Beschikbaar via: http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/trendrapporten/trendrapport-2010.html

Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties. 's-Gravenhage : Staatsuitgeverij, 1976

Rapport commissie Computercriminaliteit, Informatietechniek en Strafrecht, april 1987

Europol 2011, *European police chiefs convention, the future of Organised crime. Challenges and recommended actions.*

Afgekorte nieuwsbronnen

guardian.co.uk> digial content expansion
http://www.guardian.co.uk/business/2009/may/18/digital-content-expansion

om.nl> persbericht Bredolab
http://www.om.nl/algemene_onderdelen/uitgebreid_zoeken/@154337/nationale_recherche_0/

sunbeltsoftware.com> arrested Bredolab mastermind also connected to spamit.com
http://www.sunbeltsoftware.com/About/Security-News/?title=Arrested-Bredolab-mastermind-also-connected-to-Spamit-com--800218888

telegraaf.nl> groot crimineel computernetwerk opgerold
http://www.telegraaf.nl/digitaal/8028538/__Groot_crimineel_computernetwerk_opgerold__.html

volkskrant.nl> gigantisch crimineel computernetwerk opgerold
http://www.volkskrant.nl/vk/nl/2694/Internet-Media/article/detail/1039303/2010/10/25/Gigantisch-crimineel-computernetwerk-ontmanteld.dhtml

webwereld.nl> politie over de schreef bij botnet ontmanteling
http://webwereld.nl/nieuws/67621/politie-over-de-schreef-bij-botnetontmanteling---update.htm

webwereld.nl> politie ontkent terughacken bredolab bots
http://webwereld.nl/nieuws/67649/politie-ontkent-terughacken-bredolab-bots.html

webwereld.nl> politie legt nederlands botnet plat
http://webwereld.nl/nieuws/67594/politie-legt-nederlands-botnet-plat---update3.html

webwereld.nl> pvda politie moet hackers kunnen terug hacken
http://webwereld.nl/nieuws/67731/pvda--politie-moet-hackers-kunnen-terughacken.html

webwereld.nl> nederlandse primeur politie waarschuwt botnetslachtoffers
http://webwereld.nl/nieuws/52187/nederlandse-primeur--politie-waarschuwt-botnetslachtoffers.html

Future of Copy Right> botnets zijn het zwitserse zakmes van cybercriminelen
http://www.futureofcopyright.com/nc/nl/home/blog-post/2010/11/28/botnets-zijn-het-zwitserse-zakmes-van-cybercriminelen.htm