Het Virusdilemma*

Herbert Bos Maarten van Steen Dennis Andriesse
Christian Rossow

November 24, 2012

Er is nogal wat ophef ontstaan over de conceptbrief van minister Opstelten waarin hij voorstelt om politie en justitie in sommige gevallen het recht te geven om in te breken in de computers van criminelen. Het hacken van criminelen lijkt aantrekkelijk, maar om welke computers gaat het nou eigenlijk? Cybercriminelen maken vaak gebruik van zogeheten /botnets/: netwerken van met virussen besmette computers. Een fundamenteel probleem bij Opsteltens voorstel is dat deze computers niet alleen van criminelen zijn, maar ook van onschuldige gebruikers.

De beheerders van een botnet zijn in staat om alle geïnfecteerde computers op afstand te besturen, om op die manier bijvoorbeeld bankgegevens te stelen van eindgebruikers, en de computers te misbruiken om websites aan te vallen of spam te versturen. Botnets zijn al jaren een lucratieve business. In 2010 ontdekte de FBI een misdaadnetwerk dat meer dan 70 miljoen dollar had verdiend aan het stelen van bankgegevens met behulp van een botnet. De hiervoor benodigde botnetsoftware was in de onderwereld te koop voor 4000 dollar. Afgelopen 15 September werd in het VARA-programma Kassa duidelijk dat ook Nederlandse burgers duizenden euro's verliezen aan cybercriminelen die dit soort botnets gebruiken.

Er zijn minstens twee redenen om bedenkingen te hebben bij Opsteltens voorstel en die nopen tot een brede maatschappelijke discussie.

Ten eerste zijn er ethische bezwaren. Zo noemt burgerrechtenbeweging Bits of Freedom de plannen "zeer risicovol" voor de privacy van burgers. Een soortgelijk voorstel is in Duitsland gerealiseerd in de vorm van de "Bundestrojaner", een computerprogramma waarmee de Duitse politie kan spioneren op computers van verdachten. Deze Bundestrojaner, blijkt uit een analyse door de Duitse Chaos Computer Club, opent op de bespioneerde computers achterdeuren die ook door criminelen misbruikt kunnen worden om op diezelfde computers in te breken.

In Nederland is in 2010 met een vergelijkbare benadering het zogenaamde Bredolab botnet uitgeschakeld door het Team High Tech Crime van de Nationale Recherche. De politie informeerde hierbij de geïnfecteerde gebruikers door hen een bericht te sturen via een achterdeur die door het botnet zelf was geopend. Dit

*Article originally published in NRC Handelsblad, on November 24, 2012.

stuitte op een storm van kritiek, en leverde het KLPD een “Big Brother Award” op. Het doel mocht dan goed zijn, het middel was erg controversieel.

Ten tweede zijn er juridische bezwaren: hoe ver mogen beveiligingsonderzoekers en justitie gaan om botnets uit te schakelen en wat zijn de consequenties als het misgaat?

Het is niet ongewoon dat botnets honderdduizenden, soms zelfs miljoenen geïnfecteerde computers bevatten. Zo’n geïnfecteerde computer, een zogenaamde bot, behoort doorgaans toe aan een gewone eindgebruiker die zonder het te weten een (soms moeilijk te bestrijden) virus heeft geïnstalleerd. Technisch is het mogelijk om deze infecties op te ruimen door de computers te hacken—maar wat als het misgaat? Wat als een computer met een belangrijke taak (een ziekenhuis, een industrieel proces, of misschien gewoon een webserver) crasht door een foutje in de schoonmaaksoftware?

Ach, wat is nou de kans dat dat gebeurt? De hackers bij de politie weten heus wel wat ze doen—is dit geen bangmakerij? Niet noodzakelijk. En het is ook niet de eerste keer dat men het probeert. In 2003 werden veel Windows computers geplaagd door het Blaster virus . Al snel werd een /goede/ computerworm het Internet opgestuurd om de infectie te verwijderen. Helaas richtte de goede worm bijna net zoveel schade aan als het Blastervirus zelf.

Dit juridische moeras wordt nog ondoorgrondelijker doordat botnets zich uitstrekken voorbij de grenzen van een rechtsgebied van waaruit beveiligingsonderzoekers opereren. Botnets bevatten honderdduizenden tot miljoenen bots, die toebehoren aan gebruikers bij verschillende internetproviders en in verschillende landen. Dat betekent dat veel partijen bij een tegenaanval betrokken moeten worden. Lokale bestrijding is in veel gevallen ontoereikend en een bredere aanpak is juridisch gezien nodig.

Slecht idee, dus? Dat is nog maar de vraag. Hoewel er grote bezwaren kleven aan de plannen van onze minister, zijn de alternatieven ook niet aantrekkelijk. Sommige botnets zijn op dit moment al dusdanig geavanceerd dat ze zeer moeilijk zijn uit te schakelen. Bij een aantal zijn slechts kleine aanpassingen nodig om ze geheel resistent te maken tegen conventionele tegenmaatregelen. Die kunnen we dan alleen nog maar opruimen door precies datgene te doen wat de minister voorstelt: het hacken van andermans computer. Maar dan gaat het zeker om computers van onschuldige gebruikers!

Dit roept een fundamentele vraag op: is het beter om een botnet toe te staan, dan een tegenaanval te openen met alle onwenselijke gevolgen van dien? Om weerbaar te blijven tegen de criminelen die onze computers misbruiken is het dringend nodig om door maatschappelijke en wettelijke discussie te bepalen welke middelen geoorloofd zijn in de strijd tegen botnets. Wij doen hierbij een oproep aan de Nationale Cyber Security Raad, het Openbaar Ministerie, het Nationaal Cyber Security Centrum, politici, burgerrechtenbewegingen en wetenschappers om deze discussie /nu/ te starten.