Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2204

Vragen van het lid **Gesthuizen** (SP) aan de minister van Veiligheid en Justitie over *het bericht dat de overheid laks is geweest na een aanval door een botnet*. (ingezonden 18 februari 2013).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) (ontvangen 8 mei 2013). Zie Aanhangsel Handelingen, vergaderjaar 2012–2013, nr. 1584.

Vraag 1
Wat is uw reactie op het artikel «Overheid laks na aanval door botnet» waarin wordt belicht dat de overheid niet adequaat heeft opgetreden nadat zij was ingelicht dat duizenden bedrijven en overheidsinstellingen slachtoffer zijn geworden van cybercriminelen?[1]

Antwoord 1
Het artikel «Overheid laks na aanval door botnet» suggereert dat er door de overheid niets is en wordt gedaan aan de aanval door een botnet. Deze suggestie is onjuist.
Het NCSC heeft Digital Investigation verzocht om het gedeelte van de dataset te leveren dat nodig is om respons naar zijn achterban van overheid en vitale sectoren mogelijk te maken. Deze gegevens zijn op 8 december 2012 aangeleverd. Dit gedeelte van de dataset betrof de IP-adressen, de computernamen en de tijdstippen waarop de geïnfecteerde computers actief waren binnen het botnet. Dit heeft het NCSC gedaan op grond van haar bestaande taken en bevoegdheden, het NCSC heeft geen rechtsbasis om deze inhoudelijke en mogelijk gevoelige gegevens in te zien en te verwerken. De informatie was immers oorspronkelijk afkomstig van een misdrijf en bevatte persoonlijke gegevens en informatie waarvan de betrouwbaarheid en herkomst niet kon worden vastgesteld. Tevens stond niet vast stond hoe Digital Investigation deze informatie had verkregen.
De van Digital Investigation ontvangen IP-adressen zijn in december 2012 gecontroleerd op aanwezigheid in de bij het NCSC bekende IP-ranges (reeksen van door het departement of de instelling gebruikte IP-adressen) van departementen en instellingen binnen de doelgroep van het NCSC: de overheid en de vitale sectoren. Naar aanleiding van de resultaten hiervan zijn een zestiental departementen en instellingen actief geïnformeerd over een

[1] http://nos.nl/artikel/474184-overheid-laks-na-aanval-door-botnet.html

ah-tk-20122013-2204
ISSN 0921 - 7398
's-Gravenhage 2013

mogelijke besmetting omdat een match met mogelijk besmette IP-adressen werd vastgesteld in de IP-range.

Vraag 2
Wat zijn de risico's nu blijkt dat cybercriminelen informatie hebben buitgemaakt van instellingen die deel uitmaken van de vitale infrastructuur zoals energie- en waterleidingmaatschappijen? Hoe treedt u op tegen deze gevaren?

Antwoord 2
Zie antwoord 8

Vraag 3
Waarom heeft de politie besloten geen verder onderzoek te doen naar de melding van deze aanval? Waarom heeft de politie niet gevraagd om een leesbare kopie van de harddisk met de gestolen informatie? Deelt u de mening dat het verloop van deze kwestie niet bijdraagt aan het vergroten van het besef bij bedrijven en instellingen dat het melden van cybercrime van groot belang is?

Antwoord 3
Door de Politie wordt permanent onderzoek gedaan naar botnets. Begin augustus 2012 werd een groot aantal, voornamelijk Nederlandse bedrijven en (overheids)-instellingen getroffen door de uitbraak van een computervirus met de naam Dorifel. Gelet op de impact van de virusuitbraak, werd daar een onderzoek naar ingesteld door het Team High Tech Crime (THTC) van de Landelijke Eenheid van de Politie.
In dit onderzoek bleek dat het Dorifel-virus werd verspreid middels een botnet dat gebruik maakt van de zogenaamde Citadel-malware. Het onderzoek richt zich (tevens) op de identificatie van het criminele samenwerkingsverband achter het specifieke Citadel-botnet waarmee het Dorifel-virus werd verspreid. In oktober 2012 kreeg het IT-beveiligingsbedrijf Digital Investigation via Leaseweb de beschikking over de inhoud van een command & controlserver van een Citadel-botnet (met de naam Pobelka). Omdat vermoed werd dat deze command & controlserver gerelateerd was aan de uitbraak van het Dorifel-virus, werd door Digital Investigation contact opgenomen met THTC en werd aangeboden om de gegevens van de command & control-server aan THTC te verstrekken. Op 16 oktober 2012 is door medewerkers van THTC een bezoek gebracht aan Digital Investigation. Door Digital Investigation is een kopie van de data op een harde schijf aan THTC overhandigd. Naar later bleek was deze schijf niet leesbaar. Daarna is op 20 november 2012 door medewerkers van THTC wederom een bezoek gebracht aan Digital Investigations. In dat gesprek kwam naar voren dat er geen directe relatie gelegd kon worden met de uitbraak van het Dorifel-virus. Derhalve is door THTC niet om een nieuwe kopie van de data verzocht. Wel bleek uit het onderzoek van Digital Investigation dat een groot aantal Nederlandse bedrijven besmet was met de Citadel-malware, hierop is door het THTC geadviseerd om contact op te nemen met het NCSC.
Ik ben met u van mening dat het melden van cybercrime van groot belang is. Naar mijn oordeel doet deze casus geen afbreuk aan het besef bij bedrijven dat het melden van cybercrime van groot belang is.

Vraag 4
Deelt u de mening dat met de gestolen gegevens heel Nederland platgelegd kan worden? Kunt u uw antwoord toelichten?

Antwoord 4
Zie antwoord 8

Vraag 5
Wat is de reden dat besmette bedrijven niet actief zijn gealarmeerd? Zijn inmiddels alle getroffen bedrijven ingelicht?

Antwoord 5 en 6
Het NCSC heeft op 8 december direct actie ondernomen door na overleg met Digital Investigation dat gedeelte van de dataset in ontvangst te nemen dat noodzakelijk is voor de respons. Dit gedeelte van de dataset betrof de IP-adressen, de computernamen en de tijdstippen waarop de geïnfecteerde computers actief waren binnen het botnet. Dit heeft het NCSC gedaan op grond van haar bestaande taken en bevoegdheden. Op basis van deze gegevens heeft het NCSC voor de partijen waar zij verantwoordelijk voor is, de Rijksoverheid en de vitale sectoren, onderzocht of er, in de bij het NCSC bekende IP-ranges, IP-adressen aanwezig waren. Zo konden deze, wanneer zij getroffen waren, gericht worden geïnformeerd. Het NCSC heeft daarnaast partners als Internet Service Providers (ISP) gewezen op de informatie over het botnet, zodat zij konden nagaan of klanten en andere partijen waar zij een vertrouwensrelatie mee hebben uit hun achterban getroffen waren. In 16 gevallen is er door het NCSC gericht gealerteerd; dit betrof partijen waarvan de zogeheten IP-ranges (de reeksen van IP-adressen die door deze partijen worden gebruikt) bekend waren bij het NCSC. Indien deze IP-adressen niet bekend zijn bij het NCSC, is het onmogelijk om gericht te kunnen alerteren.

Vraag 6
Hoe kan het dat het Nationaal Cyber Security Centrum (NCSC) zegt dat de organisaties uit de vitale infrastructuur door hen zijn gewaarschuwd, terwijl uit de steekproef van de NOS blijkt dat dit niet het geval is?

Antwoord 6
Zie antwoord 5

Vraag 7
Op basis waarvan heeft het NCSC besloten de gestolen informatie niet aan te mogen nemen? Bent u van mening dat bij directe dreiging de NCSC de bevoegdheid moet hebben om informatie te kunnen inzien? Zo ja, bent u voornemens dit mogelijk te maken?

Antwoord 7
In zijn algemeenheid ben ik van mening dat de overheid op terughoudende wijze dient om te gaan met onrechtmatig verkregen informatie, zeker als dit informatie betreft die de persoonlijke levenssfeer raakt. Het NCSC kon op grond van haar bestaande taken en bevoegdheden de informatie niet in ontvangst nemen en heeft daar ook geen rechtsbasis voor. Daarbij stond niet vast hoe Digital Investigation deze informatie had verkregen. Om dit belangrijke werk nu en in de toekomst effectief te kunnen blijven doen, zal nog dit jaar gewerkt worden aan het helder duiden van de taken en bevoegdheden van het NCSC. Juridisch verkend zal worden hoe het NCSC op een zorgvuldige wijze kan omgaan met de informatie die het NCSC vanuit de ICT-community bereikt. Daarbij zal worden gekeken hoe en op welke rechtsbasis het NCSC gegevens kan verwerken om de impact van dreigingen in het digitale domein op de nationale veiligheid te beperken. Hiermee wil ik er onder meer voor zorgen dat het NCSC haar rol als Computer Emergency Response Team (CERT) blijvend adequaat kan invullen.

Vraag 8
Bestaat het risico dat de verkregen gegevens gebruikt kunnen worden voor het afpersen van bij kritieke bedrijfsprocessen betrokken personen? Kunt u uw antwoord toelichten?

Antwoord 8
Nu onderdelen van de dataset in de openbaarheid zijn gekomen en daarmee het risico van misbruik groter is geworden, is door een aantal partijen de suggestie gewekt dat hierbij mogelijk grote belangen geschaad zouden zijn. Om deze reden is het van belang om de dataset in een brede context te analyseren en de potentiële impact van gegevens in de dataset in te schatten. Vanuit zijn coördinerende rol heeft de NCTV partijen die, vanuit eigen mandaat en verantwoordelijkheid, aan de analyse meedoen bij elkaar gebracht. De eerste resultaten van dit onderzoek zullen naar verwachting in de 2^{e} helft van maart beschikbaar zijn. In afwachting van de resultaten van het onderzoek is het niet mogelijk om een gefundeerd antwoord te geven op

vragen over de potentiële impact van de gegevens en de handelingen die actoren hiermee zouden kunnen verrichten. Ook is een strafrechtelijk onderzoek opgestart. De doelstelling van dit onderzoek is om tot een identificatie te komen van de beheerders van het Pobelka-botnet, die tevens verantwoordelijk moeten worden gehouden door het wegnemen van de 750 GB aan data.