Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 268

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 maart 2013

De commissie voor Veiligheid en Justitie heeft mij in haar procedurevergadering d.d. 27 februari verzocht om een reactie te geven op het bericht van de NOS dat de overheid laks is geweest na een aanval door een botnet. Dit in aanvulling op de reeds door de leden Gesthuizen (SP), Oosenbrug en Recourt (beiden PvdA) gestelde vragen. Met deze brief informeer ik u zowel over het handelen van de overheid ten aanzien van het Pobelka-botnet als over de ondernomen acties om botnets te bestrijden en dergelijke aanvallen eerder te detecteren.

In de berichtgeving van de NOS wordt met nadruk aangegeven dat de overheid laks is geweest in de bestrijding van het Pobelka-botnet. Deze kwalificatie acht ik onjuist. De overheid zet meerdere middelen in om botnets, zoals het Pobelka-botnet te bestrijden, en heeft dat ook in dit geval gedaan.

Het Pobelka-botnet is onderdeel van de bredere familie van citadel-botnets. In de afgelopen Cyber Security Beelden is dan ook ingegaan op de problematiek rond botnets. Nederland bezit een uitgebreide ICT-infrastructuur die deels de aanwezigheid van botnets in Nederland verklaart. Deze komt het Nationaal Cyber Security Centrum (NCSC) in haar werk vaker tegen, het informeren hierover is dagelijkse praktijk van het NCSC. Op de website van het NCSC is daarom eerder al de factsheet «Verlos me van een botnet» gepubliceerd. Hierin wordt beschreven wat gebruikers kunnen doen als zij besmet zijn met malware en daardoor mogelijk onderdeel zijn van een botnet.

Verloop van de gebeurtenissen en het optreden van de overheid

In eerste instantie kreeg het IT-beveiligingsbedrijf Digital Investigation via Leaseweb de beschikking over de inhoud van een command & control-server van een Citadel-botnet (met de naam Pobelka). Omdat vermoed werd dat deze command & controlserver gerelateerd was aan de uitbraak van het Dorifel-virus, waar door het Team High Tech Crime (THTC) van de

kst-26643-268
ISSN 0921 - 7371
's-Gravenhage 2013

Landelijke Eenheid van de Politie al onderzoek naar werd gedaan, 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.

Op 20 november 2012 is door medewerkers van THTC wederom een bezoek gebracht aan Digital Investigation. In dat gesprek kwam naar voren dat er geen directe relatie kon worden gelegd 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 heeft THTC geadviseerd deze informatie te delen met het NCSC.

Op 26 november 2012 heeft de teamleider van THTC de directeur van Digital Investigation in contact gebracht met het NCSC. Hierna heeft het NCSC met Digital Investigation overlegd. Naar aanleiding van dit overleg heeft het NCSC verzocht om het gedeelte van de dataset dat nodig is om respons naar haar achterban van Rijksoverheid en vitale sectoren mogelijk te maken. 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 had geen rechtsbasis om de resterende 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 na het verkrijgen door het NCSC 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 mogelijke besmetting omdat een match met mogelijk besmette IP-adressen werd vastgesteld in de IP-range. Het NCSC beschikt niet over de IP-range van andere bedrijven of gebruikers.

De overige IP-adressen zijn vervolgens en eveneens in december 2012 aangeboden aan de Internet Service Providers (ISP) om hen in staat te stellen hun klanten te informeren wanneer zou blijken dat deze mogelijk besmet zouden zijn. De reden hiervoor is onder meer dat ISP's hierin een sleutelrol kunnen vervullen. Zij beschikken over de gegevens van de klanten, hebben de vertrouwensrelatie en kunnen ook problemen gericht oplossen.

Onderzoek

Naar aanleiding van de uitzending van het NOS-journaal d.d. 14 februari zijn onderdelen van de dataset in de openbaarheid gekomen en daarmee is het risico van misbruik groter geworden. Daarnaast 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 om de potentiële impact van gegevens in de dataset in te schatten.

Vanuit zijn coördinerende rol heeft de NCTV partijen zoals het OM, de Politie, AIVD, MIVD en het NFI die, vanuit eigen mandaat en verantwoordelijkheid, aan de analyse meedoen bij elkaar gebracht. De eerste resultaten van dit onderzoek zullen naar verwachting in de 2e helft van maart beschikbaar zijn.

Tevens 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 data bij getroffen partijen.

Acties in de komende periode

Ook in de komende periode zal een aantal acties worden ondernomen om blijvend adequaat te kunnen optreden tegen digitale dreigingen zoals botnets. Daarbij gaat het om: 1) het uitvoeren van een juridische verkenning, 2) het op- en uitbouwen van een Nationaal Detectie en Response Netwerk, 3) het i.s.m. de vitale sectoren onverminderd up-to-date houden van IP-ranges en 4) het actualiseren van de Nationale Cyber Security Strategie.

Ten eerste zal er vóór de zomer juridisch worden verkend 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. Het betreft daarbij informatie die mogelijk de persoonlijke levenssfeer raakt. Op deze wijze wil ik er voor zorgen dat het NCSC onder meer haar rol als Computer Emergency Response Team (CERT) blijvend adequaat kan vervullen. Hiermee wil ik de taken en bevoegdheden van het NCSC helder duiden, zodat men dit belangrijke werk ook in de toekomst effectief kan blijven doen.

Ten tweede onderschrijft de Pobelka-casus het in het AO d.d. 6 december aangegeven belang van het versterken van de detectiecapaciteit bij de Rijksoverheid en de vitale sectoren. Op deze wijze kunnen incidenten zo snel mogelijk gedetecteerd worden en van een gepaste response worden voorzien. Het NCSC is op het gebied van cyber security het centrale punt in Nederland en daarmee de spin in het web. Om organisaties buiten de eigen achterban van Rijksoverheid en vitale sectoren te kunnen bedienen wanneer dit nodig is werkt het NCSC samen met schakel- en partnerorganisaties. Niet alleen kunnen langs deze weg verschillende sectoren binnen de eigen verantwoordelijkheid zelfstandig digitale weerbaarheid vergroten, ook wordt hiermee de uitrol van een effectief landelijk netwerk van sectorale informatiebeveiligingsorganisaties gestimuleerd. Zo is met ondersteuning van het NCSC door VNG/KING met de oprichting van de Informatiebeveiligingsdienst voor gemeenten (IBD), een belangrijke stap gezet in de ontwikkeling van sectorale capaciteiten voor mede-overheden op het gebied van ICT-response. Door nauw samen te werken met partnerorganisaties wordt een zo groot mogelijk deel van de Nederlandse samenleving bestreken. Hiermee worden ook organisaties buiten de primaire doelgroep van het NCSC, de Rijksoverheid en de vitale sectoren, bereikt. Dit netwerk zal in stappen verder worden op- en uitgebouwd.

Ten derde zal het NCSC actief aandacht blijven vragen voor het volledig en up-to-date houden van de bij het NCSC beschikbare informatie over IP-adressen van organisaties en instellingen binnen de doelgroep van het

NCSC: de Rijksoverheid en de vitale sectoren. Naar aanleiding van het genoemde incident heeft een groot aantal partijen zich reeds bij het NCSC gemeld om informatie over de door deze partijen gebruikte IP-ranges te verstrekken.

Tot slot zal ik na het zomerreces komen met een geactualiseerde versie van de Nationale Cyber Security Strategie. Dit is juist van belang in het dynamische veld van cyber security dat voortdurend aan verandering onderhevig is en waarbij technologische ontwikkelingen consequent een gepast antwoord van publieke en private partijen vergen.

Met de aanvullende acties zal nu en in de toekomst effectiever gereageerd kunnen worden op dreigingen in het digitale domein.

De minister van Veiligheid en Justitie,
I.W. Opstelten