Ministerie van Veiligheid en Justitie

> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Oranjebuitensingel 25
2511 VE Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
378477

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 7 mei 2013
Onderwerp Antwoorden kamervragen over de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum

Hierbij bied ik u de antwoorden aan op schriftelijke Kamervragen die zijn gesteld door de leden Oosenbrug en Recourt (beiden PvdA) over de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum. (2013Z03400 van 20 februari 2013)

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

2013Z03400

Vragen van de leden Oosenbrug en Recourt (beiden PvdA) aan de minister van Veiligheid en Justitie over de reactie op een grote botnet-infectie door het Nationaal Cyber Security Centrum (ingezonden 20 februari 2013)

Vraag 1
Heeft u kennisgenomen van de kritiek van enkele beveiligingsbedrijven op de reactie van de politie en het Nationaal Cyber Security Centrum (NCSC) toen zij op de hoogte gesteld werden van een grootschalige infectie in Nederland door een botnet? 1) Zijn de gegevens in het genoemde artikel over de aangeleverde informatie aan het NCSC en de politie en hun reactie daarop juist? Zo nee, wat is dan de juiste beschrijving van de gebeurtenissen rond deze grote cyber-inbraak?

Antwoord 1
Op hoofdlijnen is de in het artikel geschetste tijdslijn juist. Naar mijn mening is er echter wel degelijk geacteerd door de Politie en het NCSC. 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 & control-server gerelateerd was aan de uitbraak van het Dorifel-virus, waar door het Team High Tech Crime (THTC) van de Landelijke Eenheid van de Politie al onderzoek naar werd gedaan werd door Digital Investigations 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 Investigations. Door DI is een kopie van de data op een harde schijf aan THTC overhandigd. In de publiciteit is deze harde schijf aangeduid als “de 750 GB”. Naar later bleek was deze schijf niet leesbaar.

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 overheid 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

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

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 Rijksoverheid 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.

Vraag 2
Is het correct dat het NCSC de afgelopen week de wens uitgesproken heeft om de ip-adressen van vitale organisaties te krijgen om een betere reactie te kunnen geven bij informatie over inbreuken op de beveiliging? Zo ja, waarom komt dit verzoek juist nu en op welke wijze is dit verzoek aan de betrokken sectoren gedaan?

Antwoord 2
Het NCSC heeft inderdaad gezien de publiciteit rondom dit onderwerp een herhaalde oproep aan haar achterban van Rijksoverheid en vitale sectoren gedaan om IP-adressen met het NCSC te delen om het NCSC in staat te stellen om partijen gericht te kunnen alerteren als het NCSC kennis heeft van mogelijke infecties van bepaalde IP-adressen. Ook in de komende periode zal door het NCSC actief aandacht worden gevraagd voor het volledig en up-to-date houden van de bij het NCSC beschikbare informatie over IP-adressen van partijen 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.

Vraag 3
Is in dit geval een "notice-and-take-down procedure" gestart door het bedrijf Digital Investigation voor de centrale servers van het botnet? Is het gebruikelijk dat deze procedure in gang gezet wordt door een privaat bedrijf? Welke gevolgen heeft deze procedure gehad voor het traceren van de daders en de schade door het botnet?

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

Antwoord 3
De notice and take down procedure (NTD) is een procedure waarbij aan providers een notificatie, ofwel een verzoek, wordt gedaan om een server uit te schakelen. Ook een private partij kan een dergelijk verzoek doen en dat gebeurt ook. Doel van de NTD-procedure is primair het beëindigen van de functionaliteit van de server en dient daarmee ook geen opsporingsdoeleinden.

Vraag 4
Wordt er op dit moment onderzoek gedaan naar de verantwoordelijken voor dit botnet? Zo ja, wat is de voortgang en de slagingskans van dit onderzoek? Zo nee, waarom niet?

Antwoord 4
Ja, naar aanleiding van de uitbraak van het dorifel-virus in augustus 2012 is reeds een onderzoek ingesteld door het THTC. Tevens is op 18 februari 2013 een tweede 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 (gevoelige) data. Gegeven het feit dat het onderzoek nog loopt is het niet mogelijk om uitspraken te doen over de slagingskans.

Vraag 5
Bent u van mening dat het blokkeren van verkeer naar de "command-and-control servers" van botnets een effectieve manier is om deze netwerken te belemmeren? Zo ja, ziet u mogelijkheden om deze werkwijze toe te staan zonder schending van de netneutraliteit?

Antwoord 5
Ja, het blokkeren van verkeer naar command en conrol-server (C&C-servers) is een van de effectieve opties in het bredere palet aan mogelijkheden om botnets te bestrijden. Toepassing van deze werkwijze zonder schending van de netneutraliteit is mogelijk binnen de uitzonderingsbepalingen in artikel 7.4a , eerste lid sub b en d van de Telecommunicatiewet (Tw). Deze bepalingen hebben betrekking op het blokkeren van verkeer dat de veiligheid of integriteit van het netwerk of het randapparaat van de eindgebruiker aantast (bijvoorbeeld verkeer afkomstig van computers die onderdeel uitmaken van een botnet) dan wel ter uitvoering van een wettelijk voorschrift of rechterlijk bevel.

Vraag 6
Wat is de rolverdeling en afbakening tussen het NCSC en de nieuwe Integrale Beveiligingsdiensten (IBD) en het centrum Abuse Information Exchange (Abuse-IX) van respectievelijk de gemeenten en enkele grote internetbedrijven? Met welke vergelijkbare diensten werkt het NCSC samen?

Zie antwoord op vraag 7

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

Vraag 7
Op welke wijze is de relatie georganiseerd tussen het NCSC en vitale sectoren? Welke informatie wordt hierin uitgewisseld en hoe frequent is dit contact? Welke sectoren zijn aangemerkt als vitale sectoren? Herkent u het beeld dat in dit informatietijdperk de informatiesystemen van steeds meer sectoren vitaal zijn?

Antwoord op vraag 6 en 7
Het NCSC werkt samen met een grote diversiteit aan partijen. In het huidige informatietijdperk neemt het belang van informatiesystemen in vitale sectoren toe. Vanuit het belang van de continuïteit van deze sectoren voor onze maatschappij werkt het NCSC dan ook nauw samen met bedrijven en organisaties uit deze sectoren.

Een belangrijk georganiseerd verband binnen deze samenwerking zijn de Information Sharing and Analysis Centers (ISAC's), georganiseerd door partijen uit het bedrijfsleven en aangesloten bij het NCSC. Dit zijn overlegorganen waarbij bedrijven uit vitale sectoren samen met relevante overheidsorganisaties werken aan het verhogen van de digitale weerbaarheid. Tijdens reguliere overleggen worden, trends, ontwikkelingen en dreigingen op het gebied van cyber security uitgewisseld.

De lijst van vitale sectoren beslaat 12 sectoren (Energie, Telecommunicatie/ICT, Drinkwater, Voedsel, Gezondheid, Financieel, Keren en Beheren Oppervlaktewater, Openbare Orde en Veiligheid, Rechtsorde, Openbaar Bestuur, Transport en de Chemische en Nucleaire Industrie) met daarbinnen 31 vitale producten en of diensten. Uitgangspunt bij deze vitale sectoren is dat uitval of verstoring van vitale producten of diensten van deze sectoren een (potentieel) maatschappelijk ontwrichtend effect heeft; de lijst van vitale sectoren sluit aan bij dit criterium.

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 doelgroep 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. Het is de ambitie om dit netwerk in stappen uit te bouwen. 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. Het NCSC werkt nauw met hen samen.

Een ander belangrijk initiatief, is het door de Minister van Economische Zaken gesubsidieerde initatief. Binnen Abuse Information Exchange werken

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

internetproviders samen en wordt informatie verzamelt en verwerkt over botnetbesmettingen. Op die manier worden besmette computers sneller opgemerkt en kunnen klanten beter en sneller geholpen worden. Abuse Information Exchange heeft de ambitie om in de loop van 2013 operationeel zijn. Deze ontwikkelingen juich ik toe.

Vraag 8
Welke plicht hebben bedrijven om aan hun klanten te melden dat hun gegevens mogelijk gestolen zijn, waardoor zij een groot veiligheidsrisico kunnen lopen? Weet u of alle bedrijven die getroffen zijn door het Pobelka-botnet hun klanten ingelicht hebben?

Antwoord 8
Hierop is geen eenduidig antwoord te geven omdat er nog onderzoek uitgevoerd wordt welke bedrijven mogelijk getroffen zijn, daarmee is ook nog niet te zeggen onder welk juridisch regime de getroffen bedrijven opereren en of zij op grond daarvan verplicht zijn hun klanten in te lichten.

Vraag 9
Deelt u de mening dat de beveiliging van de infrastructuur van vitale sectoren op dit moment nog teveel afhankelijk is van de bereidheid van bedrijven om gegevens te delen en alert te reageren op informatie over beveiligingsproblemen? Zo nee, waarom bent u van mening dat de huidige situatie voldoet? Zo ja, wat ziet u als de beste richting om dit gebrek aan regie op te lossen?

Antwoord 9 en 10
Als coördinerend bewindspersoon voor het onderwerp cyber security ben ik het met u eens dat regie belangrijk is op het onderwerp. Juist in dit licht heeft het kabinet in maart 2011 de Nationale Cyber Security Strategie gepubliceerd. Hiermee is ingezet op publiek-private, civiel-militaire en internationale samenwerking om de digitale veiligheid verder te verhogen. Met deze lijn is het fundament gelegd voor een integrale aanpak van cyber security. Uiteraard is het veld van cyber security voortdurend aan verandering onderhevig. Juist in dit licht zullen wij nog dit jaar komen met een geactualiseerde versie van de Nationale Cyber Security Strategie, het door u gevraagde plan is er dus. Daarbij is er nadrukkelijk aandacht voor de balans tussen veiligheid en digitale grondrechten.

De Pobelka-casus onderstreept 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. Ook zal vóór de zomer juridisch worden verkend hoe het NCSC op een zorgvuldige wijze kan blijven omgaan met de beschikbare informatie die het

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Directie Cyber Security

Datum
7 mei 2013

Ons kenmerk
378477

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.

Ten aanzien van het melden van inbreuken op de veiligheid van informatiesystemen binnen vitale sectoren kan ik u aangeven dat ik hiervoor al wetgeving in een vergaand stadium van voorbereiding heb. Deze wetgeving zal spoedig in consultatie worden gebracht.

Vraag 10
Herkent u de verwachting dat het NCSC of een onafhankelijke partij een actievere rol op zich neemt bij de melding van inbreuken op de veiligheid van Nederlandse computersystemen? Zo ja, bent u bereid een plan te ontwikkelen waarin een dergelijke partij de digitale veiligheid in Nederland vergroot, zonder de grondrechten van bedrijven en burgers aan te tasten?

Zie antwoord 9

1) http://webwereld.nl/nieuws/113408/politie-en-ncsc-laks-na-hack-duizenden-bedrijven.html

Toelichting:
Deze vragen dienen ter aanvulling op eerdere vragen **van het lid Gesthuizen (SP), ingezonden 18 februari 2013 (vraagnummer 2013Z03273)**