2012D33226

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

De vaste commissie voor Veiligheid en Justitie heeft een aantal vragen voorgelegd aan de minister van Veiligheid en Justitie over de brief inzake het Dorifelvirus bij (overheids)instellingen (Kamerstuk 26 643, nr. 251).

De voorzitter van de commissie,
De Roon

Adjunct-griffier van de commissie,
Van Doorn

Inhoudsopgave

I. Vragen en opmerkingen vanuit de fracties

1. Vragen en opmerkingen vanuit de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de brief van de minister van Veiligheid en Justitie (hierna: de minister) over het Dorifelvirus (Kamerstuk 26 643, nr. 251). Zij hebben hierover enige vragen. Doet de minister al het nodige om het Dorifelvirus te bestrijden en wat doet hij om de kans op een toekomstig uitbreken van een virus, vergelijkbaar met het Dorifelvirus, tot een minimum te beperken?

Deze leden merken op dat in de onderhavige brief staat dat er geen aanwijzingen zijn dat persoonsgegevens van burgers zijn gelekt. Is hier nu meer zekerheid over? Kan de minister inderdaad garanderen dat er geen persoonsgegevens zijn gelekt? Het virus lijkt zich pas te manifesteren bij het opstarten van systemen. Het is dus mogelijk dat het virus in de komende weken, als mensen terugkomen van vakantie, weer de kop zal opsteken. Wat is de inzet van de minister om een eventuele tweede uitbraak van het Dorifelvirus voor te zijn? Kan de minister tevens nader ingaan op de samenwerking met private partijen en gemeenten?

De aan het woord zijnde leden merken op dat de minister aangeeft dat hij nieuwe wetgeving wil introduceren voor ruimere strafrechtelijke opsporingsbevoegdheden op het internet. Doel hiervan is om te voldoen aan de gesignaleerde behoeften van de diensten die zijn belast met opsporing en vervolging van cybercrime. Kan de minister allereerst concreet uiteenzetten wat de gesignaleerde behoeften zijn in relatie tot het Dorifelvirus en vergelijkbare virussen? Wat is de stand van zaken als het gaat om de aanpak van het onderliggende probleem, namelijk wereldwijde botnets?

2. Vragen en opmerkingen vanuit de PvdA-fractie

De leden van de PvdA-fractie hebben kennisgenomen van de brief van de minister inzake het Dorifelvirus. Zij vragen hoe kan het dat vooral infecties bij overheden aan het licht kwamen. Was de overheid een gericht doelwit dan wel extra kwetsbaar voor dit virus? Hoeveel infecties van computersystemen in het bedrijfsleven zijn er bekend en wat is de schade die de besmettingen hier veroorzaakt hebben? Heeft de minister de indruk dat bedrijven besmettingen open gedeeld hebben of zijn bedrijven terughoudend met het melden van inbreuken in hun computersysteem? Kan een ruimere meldplicht de aanpak van computercriminaliteit verbeteren? Betekent de infectie van computers bij overheidsinstellingen door het Dorifelvirus ook dat deze systemen al langer deel uitmaakten van het Citadel-botnet? Zo ja, hoe kan het dat deze eerdere infecties onopgemerkt zijn gebleven en hoe kunnen deze besmettingen alsnog opgeschoond worden om nieuwe activiteit van dit botnet te voorkomen? Tonen de latent aanwezige botnet-besmettingen aan dat er tekortkomingen zijn in de

beveiliging van overheidsnetwerken? Wat wordt er gedaan om deze beveiliging te verbeteren? Hoe effectief is de bestrijding van het Citadel-botnet door de toegang tot de bekende C&C-servers te blokkeren? Werken alle Internet Serviceproviders (ISP's) hier aan mee, of wordt er ook gebruik gemaakt van blokkering op een hoger niveau? Zijn alle servers bekend, of verandert het botnet snel van servers?

De leden van de PvdA-fractie vragen voorts of er al zicht is op de personen en organisaties die achter het Citadel-botnet en het Dorifelvirus zitten. Hoe verloopt hierin de samenwerking met buitenlandse opsporingsdiensten? Is er hierin behoefte aan meer en passender opsporingsmiddelen? Hoe verhoudt de diefstal van bankgegevens, die aan het licht kwam na de Dorifeluitbraak, zich tot het Citadel-botnet en Dorifel? Wat is het risico van deze inbreuk?

Ten slotte vragen deze leden hoe de bestrijding van met botnets geïnfecteerde computersystemen vordert bij particulieren? Worden deze computereigenaren door hun ISP's al geïnformeerd over geconstateerde besmettingen?

3. Vragen en opmerkingen vanuit de PVV-fractie

De leden van de PVV-fractie merken op dat in de onderhavige brief staat dat het Dorifelvirus zich in eerste instantie heeft verspreid via systemen die al met het Citadelvirus waren besmet. Waren het overheidscomputers die met dit Citadelvirus waren besmet? Zo ja, is er nader onderzoek gedaan naar eventuele andere virussen die deze (of andere) overheidscomputers tegelijkertijd besmet kunnen hebben? Waren de besmette computers op het moment van besmetting allemaal up-to-date waar het beveiligingsupdates, softwareversies en antivirusprogramma's betreft? Denkt u dat deze besmetting te voorkomen was geweest? Zo ja, op welke wijze en waarom is daar niet voor gekozen? Zo nee, waarom is dan slechts een beperkt aantal computers besmet?

De aan het woord zijnde leden vragen wat de minister gaat doen om in de toekomst te voorkomen dat virussen of wellicht cyberaanvallen (delen van) de overheid plat leggen. Ziet hij hierbij een grotere taak voor de Rijksoverheid of blijft het aan gemeenten zelf om individueel voorbereidingen te treffen?

Voornoemde leden vragen of er tijdens het onderzoeken en bestrijden van het Dorifelvirus gebleken is dat er momenteel strafrechtelijke opsporingsbevoegdheden werden gemist waarmee -indien deze er wel waren geweest- effectiever optreden mogelijk was geweest? De Zo ja, kunt u dan aangeven welke strafrechtelijke bevoegdheden dit zijn of diende deze passage in de brief alleen om een beeld van de ontwikkelingen aan de kant van het ministerie te schetsen? De leden van de PVV-fractie vragen dit gezien de aandacht die hier aan wordt besteed in de slotpassage van de onderhavige brief.

4. Vragen en opmerkingen vanuit de CDA-fractie

De leden van de CDA-fractie hebben naar aanleiding van de brief van de minister nog aan aantal vragen die hieronder aan bod zullen komen.

Deze leden vragen welke risico's er op dit moment nog zijn. Hoe kunnen bedrijven, overheidsinstellingen en burgers zich hiertegen wapenen, naast het uitvoeren van virusscans en het updaten van antivirusprogramma's? Heeft het Nationaal Cyber Security Centrum (NCSC) daarover informatie

beschikbaar? Zo ja, hoe wordt die gedeeld met overheidsinstellingen en met het bedrijfsleven?

Voornoemde leden vragen of het Dorifelvirus alleen in Nederland actief (is geweest), of dat dit virus ook buiten Nederland is verspreid?

De leden van de CDA-fractie brengen in herinnering dat de Landelijk Officier van Justitie Cybercrime enkele maanden geleden een oproep heeft gedaan. De Nederlandse recherche blijkt bij de opsporing van cybercriminelen soms de soevereiniteit van andere landen te schenden door buitenlandse computers te kraken. Dat is verboden, maar de Landelijk Officier verklaarde dat het in de opsporing van cybercrime soms onvermijdelijk is. Volgens hem schiet de wet tekort als het gaat om de online jacht op bijvoorbeeld pedofielen. Kan de minister hier nader op ingaan? Ook de Nationale Recherche heeft gepleit voor meer specifieke, juridische kaders voor online opsporing. Wat is de reactie hierop van de Minister? Heeft hij hierover contact met andere landen in de EU? Graag ontvangen deze leden een reactie op dit punt. Is de minister er gerust op dat in de opsporing de snelheid van de digitale ontwikkelingen bijgehouden kunnen worden? Kan hij voorts reageren op de stelling van de Nationale Recherche dat er behoefte is aan wetgeving die de snelheid van deze ontwikkelingen kan bijhouden, omdat er anders constant als opsporingsdiensten achteraan wordt gejaagd?

De aan het woord zijnde leden merken op dat de beveiligingsproblemen van vorig jaar bij de certificeringsonderneming DigiNotar al bekend waren ver voordat dit bedrijf aan de bel trok. Hoe lang speelde het probleem met het Dorifelvirus al voordat het in het nieuws kwam? Zijn alle betrokken (publieke en private) partijen voldoende op de hoogte over waar zij terecht kunnen met probleemmeldingen?

De leden van de CDA-fractie merken op dat het Dorifelvirus kennelijk al een tijd op de getroffen computersystemen aanwezig was voordat het actief werd. Richt het onderzoek van NCSC bij de door het Dorifelvirus getroffen bedrijven zich ook op eventuele andere, op dit moment nog verborgen virussen die op een later moment actief kunnen worden?

Deze leden vragen of het Dorifelvirus ook in andere landen is aangetroffen? Zo ja, hoe is de aanpak daar geweest en is er vanuit Nederland contact geweest met het desbetreffende land?

Voornoemde leden lezen in de brief dat het Dorifelvirus de inhoud van originele bestanden heeft gewijzigd waardoor deze bestanden niet meer leesbaar zijn. Hebben publieke of private instellingen te maken gehad met wijziging door het virus van bepaalde vitale bestanden? Kan de minister meer zeggen over de door het virus veroorzaakte schade?

Ten slotte merken deze leden op dat het Openbaar Ministerie is begonnen met een strafrechtelijk onderzoek naar de dader(s) achter het Dorifelvirus en het Citadel-botnet. Kan de minister informatie verstrekken over de vorderingen van dit onderzoek? Klopt het dat het virus zijn oorsprong heeft bij servers in Oekraïne? Welke verwachtingen heeft de minister van strafrechtelijke aanpak van de mogelijke dader(s)? Is hierover contact met de betreffende autoriteiten?

5. Vragen en opmerkingen vanuit de SP-fractie

De leden van de SP-fractie hebben met interesse kennisgenomen van de brief van de minister over het Dorifelvirus bij (overheids)instellingen. Graag complimenteren zij de minister voor het keurig op tijd versturen

van de brief. De leden vinden de reactie van de minister echter te summier. Graag stellen zij hier dan ook een aantal vragen over.

Het verbaast deze leden dat de brief geen duidelijkheid geeft over de zaken die burgers, bedrijven en instellingen op het moment van uitbreken van het virus dienen te doen dan wel moeten verwachten. De leden zijn van mening dat de minister iedere gelegenheid die zich voordoet om burgers, bedrijven en instellingen te kunnen informeren over de te nemen stappen met beide handen moet aanpakken. Op de website van het NCSC is een duidelijke handleiding te vinden over hoe om te gaan met het Dorifelvirus. Op welke wijze is aan burgers, bedrijven en instellingen gecommuniceerd dat deze handleiding beschikbaar is? Heeft de minister een persbericht uit laten gaan om aandacht te vragen voor de beschikbare handleiding op de website van het NCSC? Is de minister van mening dat bij een volgende cyberaanval van dergelijk formaat er op een actievere wijze gecommuniceerd dient te worden over de stappen die ondernomen dienen te worden?

Deze leden vragen voorts of de minister kan aangeven hoe het kan dat een vermoedelijk in april opgelopen besmetting pas in augustus aan het licht kwam. Wat zegt dit over de mogelijkheden van Nederlandse overheidsdiensten om besmettingen op overheidscomputers te ontdekken? Betekent dit dat de minister niet kan uitsluiten dat er ook op dit moment mogelijk geheel andere virussen en malware aanwezig zijn op computers binnen de overheid? Wat is de minister van plan te doen om hierover duidelijkheid te verkrijgen? Wanneer kan hij de Kamer daarover informeren? Wanneer verwacht de minister te kunnen zeggen dat het virus zich niet via de websites van de betroffen organisaties verder heeft verspreid en dat er geen persoonsgegevens van burgers zijn gelekt? Ook willen deze leden graag vernemen welke risico's er op dit moment nog zijn. Zijn er sinds 10 augustus 2012 nog nieuwe meldingen van besmetting bij het NCSC binnengekomen? Heeft het Dorifelvirus zich de afgelopen weken nog ergens gemanifesteerd? Zo ja, kunt u de Tweede Kamer op de hoogte brengen om hoeveel gevallen dit gaat?

Tot slot vragen deze leden wanneer zij de uitkomst van de inventarisatie naar noodzakelijke nieuwe strafrechtelijke opsporingsbevoegdheden op het internet kunnen verwachten, gelet op de urgentie van de problemen rond cyberaanvallen. Is de minister van mening dat de Nederlandse overheid voldoende kennis, capaciteit en middelen beschikbaar stelt om dergelijke aanvallen in de toekomst eerder op te merken en te voorkomen?

6. Vragen en opmerkingen vanuit de D66-fractie

De leden van de D66-fractie hebben naar aanleiding de brief van de minister een aantal vragen.

Deze leden vragen of de minister bekend is met het weblog van Rickey Gevers?[1] Is de minister van mening dat het hacken van de server door een veroordeelde hacker uiteindelijk ergere problemen heeft voorkomen nu door het hacken van de server de hacker er achter kwam dat het virus uiteindelijk bankaccounts zou aanvallen?

Kent de minister het radio-interview met de staatssecretaris van Veiligheid en Justitie, waarin hij aangaf dat het Dorifelvirus maar een komkommerverhaal was?[2] Hoe kan het dat het politieke bewustzijn ten aanzien van de gevaren van ICT na alle incidenten nog steeds lijkt te ontbreken?

[1] http://rickey-g.blogspot.nl/2012/08/more-details-of-dorifel-servers.html
[2] www.bnr.nl/?player=archief&fragment=20120810170200600

Deze leden vragen of het waar is dat het ministerie van OCW getroffen is door het Dorifelvirus? Zo ja, was dit op het netwerk van de Haagse Ring of op een apart netwerk van het ministerie. De leden van de D66-fractie merken op dat het Dorifelvirus is geïnstalleerd door computers die onderdeel waren van het Citadel-botnet. Hoe lang zijn de computers van het ministerie van OCW onderdeel geweest van dat botnetwerk? Is de minister mening dat de beveiliging van het ministerie van OCW adequaat was? Draait er op het interne netwerk van de Haagse Ring een zogenaamd Intrusion Detection System? Zo ja, is dit in eigen beheer en intern ontwikkeld of van een derde partij?

Voornoemde leden vragen of de minister van mening is dat bij de uitbraak van een virus dat gebruik maakt van «zero day» lekken, de overheid voldoende kennis in huis heeft om de uitbraak te neutraliseren en de digitale samenleving voldoende te ondersteunen om de impact minimaal te houden?

Deze leden vragen tot welke gegevens/systemen dit virus toegang heeft gehad. Wat is de maximale schade die het virus aan had kunnen richten vanuit de systemen waar het toegang toe had? Hoe beoordeelt u de «Incident response» van overheidsinstellingen? Welke verbeterpunten ziet u? Zijn alle systemen inmiddels schoon?

II. Reactie van de minister