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
304996

Uw kenmerk
2012Z15016

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

Datum 21 september 2012
Onderwerp Antwoorden kamervragen van het lid Heijnen (PvdA) over het bericht dat een computervirus heeft toegeslagen

Hierbij bied ik u mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties de antwoorden aan op schriftelijke Kamervragen die zijn gesteld door het lid Heijnen (PvdA) over het bericht dat een computervirus bij zeker 20 instellingen heeft toegeslagen (2012Z15016 van 13 augustus 2012).

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Antwoorden op de vragen (2012Z15016) van het lid Heijnen (PvdA) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat een computervirus bij zeker 20 instellingen heeft toegeslagen (ingezonden 13 augustus 2012)

Vraag 1
Kent u de berichtgeving dat een computervirus bij vele instellingen, waaronder gemeenten, bedrijven en universiteiten, heeft toegeslagen? 1)

Antwoord
Ja.

Vraag 2
Wat zijn de gevolgen van infectie door dit virus voor belangrijke gegevens, documenten en privacygevoelige informatie?

Antwoord
De inhoud van belangrijke gegevens, documenten en privacygevoelige informatie die geïnfecteerd is door het Dorifel virus wordt versleuteld. De inhoud wordt niet vernietigd.

Vraag 3
Welke andere gemeenten en publieke instellingen, dan de in de media gemelde, zijn er nog meer getroffen?

Antwoord
In antwoord op vragen van de Vaste Commissie voor Veiligheid en Justitie is reeds 14 augustus door het kabinet geantwoord (KST 26643, 251) dat bekend is dat vanaf woensdag 8 augustus in ieder geval 30 instellingen waaronder gemeenten, bedrijven en universiteiten zijn getroffen door het Dorifel virus. Hierbij zijn de instellingen genoemd, die de ministeries aan de RijksCIO hadden gerapporteerd.

Bij NCSC en koepelorganisaties is bekend dat er meerdere gemeenten en twee provincies zijn getroffen. Aangezien er nog geen meldplicht bestaat kan geen compleet beeld worden gegeven.

Vraag 4
Hoe snel na de eerste melding van het virus is het Nationaal Cyber Security Centrum (NCSC) in actie gekomen? Op welke wijze heeft het NCSC gereageerd?

Antwoord
Op woensdagmiddag 8 augustus jl. heeft het NCSC de eerste meldingen van dit virus binnen gekregen via verschillende private- en overheidspartijen. In reactie op de eerste meldingen van het virus is het NCSC een uitgebreid onderzoek gestart om de karakteristieken van het virus in kaart te brengen en meer inzicht te krijgen in de verspreidingsgraad van de malware en de mate waarin organisaties zijn getroffen. Naar aanleiding van de eerste meldingen van het Dorifel virus heeft het NCSC op dezelfde dag een waarschuwing uitgestuurd binnen de overheid en richting de vitale sectoren. Daarnaast zijn ook de aangesloten partijen binnen het NCSC geïnformeerd. Toen verdere verspreiding zichtbaar werd is vervolgens ook actief via de media gecommuniceerd.

Getroffen partijen zijn gedurende het onderzoek actief geïnformeerd en het NCSC heeft op de website handelingsperspectieven gepubliceerd. Tevens is een lijst met

**Nationaal Coö
Terrorismebe
Veiligheid**
Directie Cyber

Datum
21 september

Ons kenmerk
dj

veelgestelde vragen gepubliceerd. Uiteindelijk heeft dit onderzoek geresulteerd in de factsheet: 'Verlos me van een botnet'. Deze factsheet is actief verspreid en gepubliceerd op de website www.ncsc.nl. Tevens is in samenwerking met de industrie gewerkt aan het bieden van handelingperspectief voor getroffen organisaties.

Vraag 5
Is het waar dat het Nationaal Cyber Security Centrum de problemen naar aanleiding van het virus in kaart brengt en de meldingen onderzoekt? Zo ja, kunt u de resultaten zo snel mogelijk met de Kamer delen?

Antwoord
Ja, het NCSC heeft een uitgebreid onderzoek uitgevoerd om de karakteristieken van het virus in kaart te brengen en meer inzicht te krijgen in de verspreidingsgraad van de malware en de mate waarin organisaties zijn getroffen.

Verder heeft het NCSC in de periode van 10 tot 16 augustus jl. actief de infrastructuur van een achterliggend Citadel botnet verstoord. In het totaal zijn op dit moment circa 60 domeinnamen die het botnet gebruikt aangepakt. Er zijn verder 10 Notice and Take Down verzoeken uitgegaan naar servers in Oostenrijk, VS, Vietnam en Rusland. Daarbij is samengewerkt met publieke en private organisaties om analyses en take downs uit te voeren. Daarnaast zijn slachtoffers binnen en buiten Nederland geïnformeerd. Voor meer gedetailleerde informatie verwijs ik u naar de reactie op het Verslag Schriftelijk Overleg Dorifel.

Vraag 6
Wat zijn de kosten voor de overheid als gevolg van het toeslaan van dit virus?

Antwoord
Voor zover bekend zitten de kosten in het de doen van onderzoek naar de besmetting, het blokkeren van de bronservers en het herstellen van de besmette bestanden. Dit maakt deel uit van reguliere bedrijfsvoering. Directe kosten zijn daarmee niet te kwantificeren.
Vanuit de contacten met gemeenten is duidelijk geworden dat de kosten sterk samenhangen met hoe zwaar de gemeente is getroffen en welke maatregelen men heeft kunnen nemen. Enkele eerste schattingen lagen tussen de 10.000 en 50.000 euro.

Vraag 7
Wordt de dienstverlening voor de burger beïnvloed door het toeslaan van dit virus? Zo ja, hoe?

Antwoord
Met name bij gemeenten is de dienstverlening aan burgers tijdelijk geraakt. De zwaarte hiervan was afhankelijk van de lokale situatie. Bij enkele gemeenten heeft de e-dienstverlening stilgelegen, variërend van enkele uren tot twee dagen. Enkele gemeenten hebben de dienstverlening aan de fysieke balie circa een halve dag stilgelegd. Enkele gemeenten hebben preventief hun e-mailverkeer tijdelijk stilgelegd.

Vraag 8
Was de uitbraak van dit virus te voorkomen? Zo nee, waarom niet? Zo ja, waarom is dit niet gebeurd?

**Nationaal Coö
Terrorismebe
Veiligheid**
Directie Cyber

Datum
21 september

Ons kenmerk
dj

Antwoord
Nee, de malware, zowel Dorifel als de Citadel variant, werden door anti-virus scanners niet herkend. Door de sterk wisselende verschijningsvormen van deze malware is het lastig om nieuwe besmettingsvormen nu en in de nabije toekomst snel te herkennen.

Vraag 9
Hoe verklaart u dat dit virus alleen bij (semi-) overheidsinstellingen lijkt te hebben toegeslagen?

**Nationaal Coö
Terrorismebe
Veiligheid**
Directie Cyber

Datum
21 september

Ons kenmerk
dj

Antwoord
Het virus heeft zowel overheid als bedrijfsleven getroffen, vermoedelijk evenredig. Er is op basis van de huidige informatie en signalen uit de community geen indicatie dat publiek zwaarder getroffen is dan privaat of andersom.

Vraag 10
Zou het kunnen zijn dat bedrijven dergelijke ICT-incidenten niet melden?

Antwoord
Zie antwoord op vraag 3.

Vraag 11
Gaat het NCSC ook bij het bedrijfsleven inventariseren of, en in welke mate, dit virus daar heeft toegeslagen? Zo nee, waarom niet? Zo ja, wilt u de Kamer van de resultaten daarvan op de hoogte stellen?

Antwoord
Zie antwoord op vraag 5.

Vraag 12
Wat is de stand van zaken met betrekking tot de voorbereiding van de meldplicht voor bedrijven van ICT-incidenten, waarvoor in diverse moties is gepleit?

Antwoord
In de brief 'Meldplicht en interventiemogelijkheden' d.d.6 juni is de Tweede Kamer geïnformeerd over de uitwerking van de in de motie Hennis-Plasschaert voorgestelde security breach notification. Op dit moment wordt door de Minister van Veiligheid en Justitie gewerkt aan de wettelijke regeling meldplicht security breaches. In de voortgangsbrief Cyber Security van 2013 zal de Kamer worden geïnformeerd over de voortgang.

Vraag 13
Deelt u de mening dat het vertrouwen van de burger in de overheid niet wordt bevorderd als alleen van cybercriminaliteit bij de (semi-)overheid sprake lijkt te zijn?

Antwoord
Zie antwoord op vraag 9

1) NOS-journaal, 9 augustus 2012