Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

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

802

Vragen van de leden **Rebel** en **Oosenbrug** (beiden PvdA) aan de Minister van Veiligheid en Justitie over *het bericht dat een computervirus kinderpornografie verspreidt* (ingezonden 1 november 2013).

Antwoord van Minister **Opstelten** (Veiligheid en Justitie) (ontvangen 18 december 2013) Zie ook Aanhangsel Handelingen, vergaderjaar 2013–2014, nr.661

Vraag 1
Kent u het bericht «Computervirus toont kinderpornografie»?[1]

Antwoord 1
Ja.

Vraag 2
Acht u het mogelijk dat personen van wie de computer door het genoemde «politievirus» wordt geblokkeerd, vanwege angst voor strafvervolging in verband met kinderporno zullen afzien van het doen van melding of aangifte tegen de verspreiders van deze ransomware? Zo ja, betekent dit dat dit «politievirus» meer dan de genoemde honderden mensen kan hebben getroffen? Zo nee, waarom niet?

Antwoord 2
Net zoals bij slachtofferschap van andere misdrijven kunnen er tal van redenen zijn waarom mensen afzien van het doen van aangifte. De angst om te maken te krijgen met strafvervolging in verband met kinderporno zou ook zo'n reden kunnen zijn. Ik kan mede daarom niet uitsluiten dat het aantal mensen dat aangifte heeft gedaan lager is dan het aantal mensen dat daadwerkelijk door dit virus getroffen is.

Vraag 3
Hoe kan de politie onderscheiden of kinderporno die op een computer wordt aangetroffen afkomstig is van een «politievirus» of door de gebruiker zelf is gedownload?

[1] http://www.bnr.nl/nieuws/tech/853537–1310/computervirus-toont-kinderpornografie

ah-tk-20132014-802
ISSN 0921 - 7398
's-Gravenhage 2013

Antwoord 3
Er zijn allerlei onderzoeksmethodes om te achterhalen wat de herkomst is van kinderporno die op een computer wordt aangetroffen. Over de vraag welke methode(s) in het geval van een dergelijk virus aangewezen zijn kunnen geen algemene uitspraken worden gedaan, want dit hangt af van de specifieke situatie en kan ook veranderen in de tijd. Van belang voor betrokkenen is dat de politie heeft aangegeven dat zij onderscheid kan maken tussen de gevallen waarin kinderporno door middel van een virus op de computer is geplaatst en de gevallen waarin kinderporno op andere wijze op de computer terecht is gekomen.

Vraag 4
Acht u het mogelijk dat computerbezitters op wiens computer kinderporno wordt aangetroffen zich zullen trachten te verschuilen achter de bewering dat die kinderporno door ransomware is achtergelaten? Zo nee, waarom niet?

Antwoord 4
Ik acht het mogelijk dat mensen het argument van de ransomware, waar of onwaar, gebruiken als verklaring voor kinderporno die op hun computer wordt aangetroffen. Dit zal altijd worden onderzocht door de politie. Ik verwijs verder naar mijn antwoord op vraag 3.

Vraag 5 en 6
Zijn de genoemde vouchers enkel voor het doel van het vermeend deblokkeren van computers bedoeld of zijn die breder aan te wenden? Kunnen de verkopers van de vouchers weten dat de vouchers bedoeld zijn voor het deblokkeren van een computer die getroffen is door malafide ransomware? Zo ja, maakt dat die verkopers in aanleg vatbaar voor strafrechtelijke vervolging? Zo nee, waarom weten die verkopers dat niet?
Kan het bedrijf dat de vouchers uitgeeft en via winkels distribueert, op enig moment weten dat vouchers gebruikt worden voor strafbare doeleinden? Zo ja, hoe oordeelt u over de rol en de betrokkenheid van een dergelijk bedrijf bij deze malafide praktijken van ransomware? Zo nee, waarom niet?

Antwoord 5 en 6
Deze vouchers worden gebruikt voor betalingen via het internet en zijn breed verkrijgbaar en te gebruiken. Normaal gesproken is het niet zo dat verkopers en producenten de motieven voor de aanschaf van deze vouchers door hun klanten weten. Ik dicht verkopers en producenten van deze breed toepasbare betalingsmethode dus geen betrokkenheid bij malafide ransomewarepraktijken toe. Gezien de actualiteit van ransomewarevirussen heeft de politie wel het initiatief genomen om posters te ontwikkelen en te verspreiden waarop gewaarschuwd wordt niet te betalen als de computer is besmet met ransomeware.[2] Daarnaast adviseert de politie winkeliers om hun eigen personeel goed voor te lichten. Als er een indicatie is dat zij te maken hebben met een slachtoffer van ransomware, kan winkelpersoneel het slachtoffer inlichten over de opties.

Vraag 7
Hoe kunnen computergebruikers zich beschermen tegen het zogenaamde «politievirus» of andere ransomware die strafbare content op computers kan achterlaten? Voldoet een standaard en up-to-date virusscanner hiertegen?

Antwoord 7
Computergebruikers moeten er in ieder geval voor zorgen dat zij voldoende maatregelen op hun computer treffen, zoals het gebruik van een up-to-date virusscanner. Maar ook dan is een infectie niet helemaal uit te sluiten. Mocht een computer geïnfecteerd raken met ransomeware dan bieden bijvoorbeeld de websites waarschuwingsdienst.nl of fraudehelpdesk.nl soelaas. Op deze sites staan instructies en stappenplannen over voor het verwijderen van ransomware.

[2] Zie de website http://www.politie.nl/onderwerpen/ransomware.html