# Tweede Kamer der Staten-Generaal

**2**

Vergaderjaar 2014–2015

**Aanhangsel van de Handelingen**


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

## 725

Vragen van de leden **Schouw** en **Verhoeven** (beiden D66) aan de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over *de geheime malware die aangetroffen is binnen de systemen van de Europese Unie en bedrijven in Europese lidstaten* (ingezonden 27 november 2014).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 2 december 2014)

Vraag 1
Kent u de berichten «Secret malware in European Union attack linked to U.S. and British intelligence»[1] en «Researchers uncover government spy tool used to hack telecoms and Belgian Cryptographer»?[2]

Antwoord 1
Ja.

Vraag 2
Was u, of een van uw diensten zoals de AIVD of het NCSC, op de hoogte van het bestaan en functioneren van de specifieke malware, ook wel «Regin» genoemd, die kennelijk wordt gebruikt voor infecties van ICT-systemen? Zo ja, wanneer was u hier van op de hoogte?

Antwoord 2
Zoals ik heb aangegeven richting uw Kamer op 14 oktober 2013, bij de beantwoording van Kamervragen van de leden Schouw en Verhoeven, naar aanleiding van berichtgeving van de Duitse krant Der Spiegel en de Belgische krant de Standaard, heeft de AIVD onderzoek verricht en destijds geen aanwijzingen aangetroffen dat Nederland een direct doelwit was van deze aanval (Aanhangsel Handelingen, vergaderjaar 2014–2015, nr. 254).

[1] The Intercept, 24-11-2014, https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/
[2] Wired, 24-11-2014, http://www.wired.com/2014/11/mysteries-of-the-malware-regin/


ah-tk-20142015-725
ISSN 0921 - 7398
's-Gravenhage 2014

Vraag 3
Kunt u bevestigen of het in de gevallen van de Europese Unie en Belgacom, gaat om de specifieke malware «Regin», zoals beschreven in het artikel van The Intercept?

Antwoord 3
Daarover kunnen in het openbaar geen mededelingen worden gedaan.

Vraag 4
Kunt u garanderen dat ICT-systemen van de Nederlandse overheid niet geïnfecteerd zijn door schadelijke malware van buitenlandse inlichtingendiensten of veiligheidsdiensten? Zo nee, welke stappen onderneemt u ter beperking van het risico op aanvallen met malware?

Antwoord 4
In het algemeen zijn geen garanties te geven. Nederland heeft een nationale cyber security strategie, waarbij diverse organisaties samenwerken om dreigingen op het gebied van digitale veiligheid tegen te gaan. In dit kader is ook de pilot Nationaal Detectie Netwerk gestart, waar de AIVD aan deelneemt.

Vraag 5
Kunt u verifiëren of «Regin» malware of vergelijkbare malware afkomstig is van Amerikaanse of Britse inlichtingen- of veiligheidsdiensten zoals wordt gesuggereerd in de genoemde artikelen? Zo nee, gaat u hierover contact zoeken met betrokken Amerikaanse en Britse overheidsinstanties?

Antwoord 5
In het algemeen zullen Nederlandse inlichtingen- en veiligheidsdiensten buitenlandse diensten aanspreken indien sprake is van geconstateerde inbreuken op Nederlandse belangen. Over de inhoud van dergelijke contacten kan ik in het openbaar geen mededelingen doen.

Vraag 6 en 7
Kunt u aangeven of Nederland werkt aan het aanpakken van dit soort malware en het achterhalen van de makers van de genoemde en vergelijkbare malware? Zo ja, wordt hierbij samengewerkt met andere landen of in Europees verband?
Gaat u dit aankaarten in internationaal verband, bijvoorbeeld op een internationale top over cyber security, nu de mogelijkheid bestaat dat deze malware is gemaakt door inlichtingendiensten van westerse landen waar Nederland een goede verstandhouding mee heeft?

Antwoord 6 en 7
Heimelijk uitgevoerde inlichtingenactiviteiten in en tegen Nederland zijn niet toelaatbaar. Er zijn nationaal en internationaal initiatieven ontplooid om digitale dreigingen tegen te gaan.
Vanuit de EU is er de Working Group on data protection. Ook is er aansluiting gezocht bij het acht-punten-programma van de Duitse Bondskanselier Merkel.