

## Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA 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  
DCS

Schedeldoekshaven 200  
2511 EZ Den Haag  
Postbus 20011  
2500 EA Den Haag  
[www.nctv.nl](http://www.nctv.nl)

**Ons kenmerk**

311172

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

Datum 29 oktober 2012  
Onderwerp Antwoorden Kamervragen over de gevaren van het spionagevirus  
Flame voor Nederland

Hierbij doe ik u, mede namens de minister van Binnenlandse Zaken en  
Koninkrijksrelaties, de antwoorden toekomen op de schriftelijke Kamervragen die  
zijn gesteld door het lid Gesthuizen (SP) over de gevaren van het spionagevirus  
Flame voor Nederland, ingezonden 19 september 2012 met kenmerk  
2012Z15995.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

**Antwoorden van de Minister van Veiligheid en Justitie op de vragen van het lid Gesthuizen (SP) over de gevaren van het spionagevirus Flame voor Nederland. (ingezonden 19 september 2012, nr. 2012Z15995)**

---

**Datum**  
29 oktober 2012

**Ons kenmerk**  
311172

**Vraag: 1**

**Wat is uw reactie op het bericht 'Flame-virus trof ook Nederlandse computers', waarin staat dat dit spionagevirus ook in Nederland slachtoffers heeft gemaakt?<sup>1</sup>**

**Antwoord: 1**

Het feit dat acht Nederlandse IP-adressen (het adres van een met het internet verbonden computer), zoals genoemd in het artikel, gebruikt zijn wil niet zeggen dat er sprake is van acht geïnfecteerde computers in Nederland. Eén geïnfecteerde computer kan meerdere IP-adressen gebruiken. Daarnaast kan het gebruik van IP-adressen ook plaatsvinden door proxies (systemen waarbij verkeer uit het buitenland via Nederlandse IP-adressen geleid wordt). Het feit dat Nederlandse IP-adressen gebruikt zijn wil dus niet per definitie zeggen dat er sprake is van infecties in Nederlandse computersystemen.

**Vraag: 2**

**Welke Nederlandse systemen zijn door het Flame-virus getroffen? Gaat het hier om een gerichte aanval op systemen die gevoelige informatie bevatten?**

**Antwoord: 2**

Er zijn vooralsnog geen aanwijzingen dat Nederlandse systemen bedoeld of onbedoeld geïnfecteerd zijn met het Flame-virus.

**Vraag: 3**

**Acht u onderzoek noodzakelijk om boven tafel te krijgen of er, naast de bekende acht besmette IP-adressen, zich meer besmette systemen in Nederland bevinden? Zo ja, hoe en door wie wilt u het onderzoek laten uitvoeren en kan de Kamer hierover worden geïnformeerd?**

**Vraag: 4**

**Welke stappen bent u bereid te nemen om zoveel mogelijk schade van dit virus te voorkomen? Welke rol speelt het Nationaal Cyber Security Centrum hierbij?**

---

<sup>1</sup> <http://tweakers.net/nieuws/84416/flame-virus-trof-ook-nederlandse-computers.html>

**Antwoord: 3 en 4**

Onderzoek naar de aard en herkomst van het Flame-virus is noodzakelijk en wordt reeds uitgevoerd door de inlichtingen en veiligheidsdiensten (I&V-diensten). De I&V diensten hebben immers in het belang van de nationale veiligheid de taak en de middelen om onderzoeken te doen naar (potentiële) digitale spionage. Indien het onderzoek van de I&V-diensten hier aanleiding toe geeft dan zal de Tweede Kamer hierover geïnformeerd worden via de geëigende kanalen. Vooralsnog is hier geen reden voor.

Het Nationaal Cyber Security Centrum (NCSC) heeft naast haar expertisefunctie en verantwoordelijkheid voor de versterking van ICT-crisisbeheersing, de rol richting Rijksoverheid en vitale sectoren om cyberincidenten te voorkomen, te verhelpen en schade te beperken. In dit kader volgt het NCSC de ontwikkelingen ten aanzien van het Flame-virus nauwlettend en heeft het NCSC in juni 2012 een Factsheet uitgebracht.<sup>2</sup>

Vanuit deze verantwoordelijkheden werken de I&V-diensten en het NCSC samen in de aanpak van kwesties als het Flame-virus.

---

<sup>2</sup> <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-afluistermalware-flamer-lang-onder-de-radar.html>