Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Prinses Irenestraat 6
Den Haag

Ministerie van Buitenlandse Zaken
Rijnstraat 8
2515 XP Den Haag
Postbus 20061
Nederland
www.rijksoverheid.nl

Onze Referentie
BZDOC-1634456041-18
Uw Referentie
2024Z05303
Bijlage(n)

Datum 26 april 2024
Betreft Beantwoording vragen van de leden Sneller (D66) en Zeedijk (Nieuw Sociaal Contract) over de Chinese cyberaanvallen op Nederlandse Kamerleden

Geachte voorzitter,

Hierbij bied ik u, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie, de antwoorden aan op de schriftelijke vragen gesteld door de leden Sneller (D66) en Zeedijk (Nieuw Sociaal Contract) over de Chinese cyberaanvallen op Nederlandse Kamerleden.
Deze vragen zijn ingezonden op 28 maart 2024 met kenmerk 2024Z05303.

De minister van Buitenlandse Zaken,

Hanke Bruins Slot

Antwoorden van de minister van Buitenlandse Zaken, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie, op vragen van de leden Sneller (D66) en Zeedijk (Nieuw Sociaal Contract) over de Chinese cyberaanvallen op Nederlandse Kamerleden

Onze Referentie
BZDOC-1634456041-18

Vraag 1
Bent u bekend met het bericht 'Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians'?[1]

Antwoord
Ja.

Vraag 2
Wat is uw reactie op de aantijgingen van de Verenigde Staten (VS) en het Verenigd Koninkrijk (VK) tegen deze zeven hackers, die volgens hen in opdracht van de Chinese Staat cyberaanvallen uitvoerden tegen journalisten, politici, activisten en bedrijven?

Antwoord
De verklaringen van de VS en het VK passen in het algemene beeld van de cyberdreiging die uitgaat van China, dat al langer wordt geschetst door de AIVD, de MIVD en de NCTV.[1] Na publicatie van de Britse verklaring op 28 februari jl. heeft Nederland, zowel nationaal als via de Europese Unie (EU), solidariteit uitgesproken met het VK. De verklaringen van de VS en het VK onderstrepen de noodzaak om de groeiende cyberdreiging, samen met de EU, VS, VK en andere partners, strategischer en proactiever tegen te gaan, zoals ook beschreven in de Internationale Cyberstrategie 2023 – 2028.[2]

Vraag 3
Deelt u de grote zorgen over de gevolgen van mogelijke Chinese cyberaanvallen?

Antwoord
Wij delen de zorgen over de gevolgen van Chinese cyberaanvallen. Die zorgen zijn overgebracht door de minister-president en de minister voor Buitenlandse Handel en Ontwikkelingssamenwerking aan de Chinese autoriteiten tijdens hun gezamenlijke bezoek aan Beijing op 26 en 27 maart jl. Daarbij is specifiek verwezen naar de recente attributie door het kabinet van een Chinese cyberaanval op het ministerie van Defensie.

Vraag 4
Is de hackgroep Advanced Persistent Threat Group 31 (APT31) bekend bij de Nederlandse inlichtingen-en veiligheidsdiensten? Wat kunt u delen over de werkwijze van deze groep en de dreiging daarvan voor Nederland?

Vraag 5
Kunt u bevestigen dat deze groep wordt aangestuurd door het Chinese ministerie van Staatsveiligheid?

[1] Zie jaarverslagen AIVD, MIVD 2022 en DBSA2.
[2] Zie ICS2, Internationale Cyber Strategie 2023 - 2028 (overheid.nl)

Vraag 6
Kunt u bevestigen dat deze groep gerichte aanvallen uitvoert op journalisten, politici (o.a. van de Inter-Parliamentary Alliance on China), activisten en bedrijven? Zo ja, hoe lang gebeurt dat al

Vraag 7
Klopt het voor zover bij u bekend dat APT31 zich ook richtte op Nederlandse Kamerleden? Zo ja, sinds wanneer en welke zijn dit?

Vraag 8
In hoeverre kan er via deze hackaanvallen staatsgeheime informatie zijn verkregen? Kunt u daarbij specifiek ingaan op informatie die eventueel van/via Nederlandse politici is verkregen?

Antwoord vraag 4 t/m 8
Er wordt in het openbaar niet ingegaan op de werkwijze en het kennisniveau van de inlichtingen- en veiligheidsdiensten.

Zoals vermeld in het Cyber Security Beeld Nederland 2022, heeft de Chinese digitale spionage actor APT31 op grote schaal en langdurig politieke doelwitten in Europa en Noord-Amerika aangevallen. Ook in Nederland waren er doelwitten van aanvallen en verkenningsactiviteiten door deze actor.[3] De interesse vanuit statelijke actoren in deze doelwitten illustreert het belang van goede beveiligingsmaatregelen en netwerkdetectiemogelijkheden voor Nederlandse overheidsnetwerken om aanvallen te detecteren, af te slaan en nader onderzoek te verrichten.

Vraag 9
Bent u tevens bekend met het bericht 'New Zealand accuses China of hacking parliament, condemns activity'?[2]

Antwoord
Ja.

Vraag 10
Is de hackgroep ATP40 bekend bij de Nederlandse inlichtingen-en veiligheidsdiensten? Wat kunt u delen over de werkwijze van deze groep en de gevolgen daarvan?

Antwoord
Zie beantwoording vraag 4 t/m 8.

[1] US Department of Justice - Office of Public Affairs, 25 maart 2024, 'Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians' (Office of Public Affairs | Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians | United States Department of Justice)

[3] Zie CSBN 2022, pagina 17.

[2] Reuters, 26 maart 2024, 'New Zealand accuses China of hacking parliament, condemns activity' (New Zealand accuses China of hacking parliament, condemns activity | Reuters)