Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025 **Aanhangsel van de Handelingen**

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

551

Vragen van de leden **Kathmann** (GroenLinks-PvdA) en **Van der Werf** (D66) aan de Ministers van Justitie en Veiligheid en van Buitenlandse Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de aanval op Nederlandse apparaten door Chinese staatshackers* (ingezonden 19 september 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid), mede namens de Minister van Buitenlandse Zaken en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 14 november 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 236.

Vraag 1
Bent u bekend met het bericht «Duizenden apparaten in Nederland getroffen door Chinese staatshackers»?[1]

Antwoord 1
Ja, alle aangeschreven bewindspersonen zijn bekend met het bericht.

Vraag 2
Sinds wanneer is deze hack bij u bekend? Hoeveel tijd is er verstreken tussen de initiële aanval en het moment dat het onder uw aandacht kwam?

Antwoord 2
De Nederlandse overheid is enkele dagen voor de publicatie van de FBI op 18 september 2024 in vertrouwen geïnformeerd over deze casus door de VS. De gehackte Nederlandse apparaten waren onderdeel van een botnet dat bekend staat in open bronnen als het Raptor Train-botnet. Dit botnet is in mei 2020 geïnitieerd. Het is niet bekend wanneer de eerste apparaten in Nederland zijn besmet. Het ging hier namelijk om een wereldwijd botnet waarvan ca. 260.000 systemen onderdeel uitgemaakt hebben, waaronder ook ruim 2000 apparaten in Nederland.

[1] NU.nl, 18 september 2024, Duizenden apparaten in Nederland getroffen door Chinese staatshackers (www.nu.nl/tech/6328683/duizenden-apparaten-in-nederland-getroffen-door-chinese-staatshackers.html?referrer=https%3A%2F%2Ft.co%2F).

ah-tk-20242025-551
ISSN 0921 - 7398
's-Gravenhage 2024

Vraag 3
Bent u bekend met welk motief Nederlandse apparaten gehackt zijn, naast het kapen van deze systemen voor het uitvoeren van andere cyberaanvallen? Was deze aanval gericht of ongericht?

Antwoord 3
Bij het opzetten van een botnet worden apparaten besmet die op dat moment eenvoudig over te nemen zijn. Het doel is meestal zo veel mogelijk verschillende apparaten onder controle te krijgen om deze later gericht te kunnen inzetten. Het botnet zelf is dus ongericht. Ook de *cybersecurity advisory* van de Amerikaanse diensten geeft weer dat deze cyberoperatie ongericht was. De Chinese cyberactor, een commercieel bedrijf, hackte doorlopend en wereldwijd kwetsbare apparaten om deze toe te voegen aan het Raptor-Train botnet. Vervolgens bood deze het botnet aan als dienstverlening voor obfuscatie doeleinden. Andere Chinese cyberactoren kregen hiermee toegang tot een middel om hun cyberoperaties langs te routeren en zo de herkomst hiervan te verhullen.
Deze activiteit past binnen het normbeeld van het Chinese cyberecosysteem en de rol van commerciële bedrijven daarbinnen. Deze professionaliseerden hun operaties door gebruik te maken van gehackte infrastructuur, waaronder consumentenapparatuur, zo meldden de AIVD[2] en MIVD[3] in hun jaarverslagen over 2023.

Vraag 4
Welke gevolgen verbindt u aan het de aanval van Chinese staatshackers? Trekt u hierin gezamenlijk op met de andere getroffen landen?

Antwoord 4
De *Joint Cyber Security Advisory*[4] van de Amerikaanse, Australische, Britse, Canadese en Nieuw-Zeelandse diensten omvat een analyse van de gevolgen, schaal en motief van dit botnet. Deze analyse is in lijn met het normbeeld dat wordt geschetst in het Dreigingsbeeld Statelijke Actoren[5] en het Cybersecuritybeeld Nederland (CSBN 2024)[6]. Met de Nederlandse Cybersecurity Strategie (NLCS)[7] streeft het kabinet naar een digitaal veilig Nederland en verhoogt het de weerbaarheid tegen cyberaanvallen.
De antwoorden op vragen 5, 8, 10 en 11 hieronder geven weer welke mitigerende maatregelen zijn genomen door het National Cybersecurity Centrum (NCSC) en Digital Trust Center (DTC). Over verdere maatregelen tracht het Kabinet zoveel mogelijk naar buiten te treden, in lijn met motie Erkens, maar dit is niet altijd mogelijk. Nederland trekt hierbij zoveel mogelijk op met partners, vooral in EU- en NAVO-verband.

Vraag 5
Op welke termijn verwacht u een totaalbeeld te hebben van de gevolgen, de schaal en het motief van deze aanval? Kunt u de analyse (al dan niet vertrouwelijk) aan de Kamer doen toekomen?

Antwoord 5
De *Joint Cyber Security Advisory* van de Amerikaanse, Australische, Britse, Canadese en Nieuw-Zeelandse diensten omvat een analyse van de gevolgen, schaal en motief van dit botnet. Deze analyse is in lijn met het normbeeld dat wordt geschetst in het Dreigingsbeeld Statelijke Actoren en het Cybersecuritybeeld Nederland (CSBN 2024). Verder geven de antwoorden op vragen 6, 7

---

[2] AIVD Jaarverslag 2023. AIVD-jaarverslag 2023 | Jaarverslag | AIVD
[3] Jaarverslag MIVD 2023. Jaarverslag MIVD 2023 | Jaarverslag | Defensie.nl
[4] National Security Agency, 18 september, 2024. «NSA and Allies Issue Advisory about PRC-Linked-Actors and Botnet Operations». NSA and Allies Issue Advisory about PRC-Linked Actors and Botnet Operations > National Security Agency/Central Security Service > Press Release View
[5] Dreigingsbeeld Statelijke Actoren 2022. Dreigingsbeeld Statelijke Actoren 2 November 2022 | Rapport | Rijksoverheid.nl
[6] Cybersecuritybeeld Nederland 2024. Cybersecuritybeeld 2024: turbulente tijden, onvoorziene effecten | Nieuwsbericht | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
[7] Nederlandse Cybersecuritystrategie 2022–2028. Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

en 8 hieronder weer wat het huidige, en naar verwachting zo volledig mogelijk nationale totaalbeeld over de gevolgen, de schaal en het vermoedelijk motief is.
Het NCSC heeft door tussenkomst van het Digital Trust Centre (DTC) van het Ministerie van Economische Zaken, waar mogelijk eigenaren van de getroffen apparatuur op de hoogte gesteld. Er is daarbij een algemeen advies meegegeven aan de eigenaren. Het NCSC en het DTC hebben ook op hun websites[8] [9] algemeen beveiligingsadvies uitgebracht met een verwijzing naar deze *Joint Cyber Security Advisory* en algemene kennisproducten over het verhogen van weerbaarheid toegevoegd.

Vraag 6
Is er kritische digitale infrastructuur geraakt door deze aanval? Zijn de volledige gevolgen voor de cyberveiligheid van Nederland in beeld?

Antwoord 6
Nee, voor zover bekend waren de in Nederland besmette systemen geen onderdeel van de Rijksoverheid of vitale infrastructuur. Het ging met name om besmetting van consumentenapparaten.

Vraag 7
Is er mogelijk staatsgeheime informatie geraakt in de aanval? Met welke zekerheid kunt u dat zeggen?

Antwoord 7
Voor zover bekend waren de besmette systemen geen onderdeel van de kritische infrastructuur, er zijn geen apparaten van de Rijksoverheid of vitale infrastructuur besmet en onderdeel geweest van het Raptor-Train botnet. Voor zover bekend is het botnet ook niet door andere Chinese cyberactoren gebruikt om cyberoperaties uit te voeren tegen Nederlandse of Europese belangen. Zeer waarschijnlijk is er vanuit het botnet geen dreiging geweest voor Nederlandse staatsgeheimen. Gezien het doel van het netwerk was om cyberoperaties te verhullen, kan echter inherent niet worden uitgesloten dat dit op enig moment het geval is geweest.

Vraag 8
Op welk detailniveau is het bekend welke personen, organisaties en apparaten getroffen zijn? Welke rol speelt het Nationaal Cyber Security Centrum (NCSC) nu bij het informeren en de verdere hulpverlening van getroffenen?

Antwoord 8
Van de Nederlandse gehackte apparaten is het bekend wat de IP-adressen en MAC-adressen waren. De gebruikers van deze apparaten hebben voor zover bekend geen problemen ondervonden van de malware, omdat deze er op gericht was om internetverkeer op heimelijke wijze via het apparaat te routeren. Voor zover bekend hebben de betreffende gebruikers ook geen problemen ondervonden door de Amerikaanse verstoringsoperatie waarbij deze malware verwijderd is van hun apparaten en waarmee het botnet werd uitgeschakeld.
Het NCSC heeft een lijst gekregen met alle IP-adressen van getroffen apparaten. Partijen zijn, waar mogelijk, via het DTC geïnformeerd. Het gaat hier om een klein deel van de totale hoeveelheid getroffen apparaten in Nederland Het NCSC heeft zelf geen getroffen organisaties geïnformeerd, aangezien het niet ging om apparaten van organisaties behorende tot de doelgroep van het NCSC (Rijksoverheid of vitale aanbieders). Wel hebben zowel het DTC en het NCSC op hun website algemeen advies gepubliceerd en verwijzingen toegevoegd naar het *Joint Cyber Security Advisory* en bestaande kennisproducten om de weerbaarheid te verhogen.

---

[8] Nationaal Cyber Security Centrum, 18 september, 2024. «Nederlandse apparaten onderdeel van Chinees botnet». Nederlandse apparaten onderdeel van Chinees botnet | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl)

[9] Digital Trust Center, 18 september 2024. «Botnet bevat duizenden Nederlandse kleine apparaten.» Botnet bevat duizenden Nederlandse kleine apparaten | Digital Trust Center (Min. van EZ)

Vraag 9
Kunt u vaststellen of de getroffen apparaten een gedeelde kwetsbaarheid hadden? Hoe kan deze kwetsbaarheid worden afgedekt? Zou de Cyber Resilience Act (CRA) voorkomen dat dergelijke hacks in de toekomst weer plaatsvinden?

Antwoord 9
De *Joint Cyber Security Advisory* van de Amerikaanse, Australische, Britse, Canadese en Nieuw-Zeelandse diensten spreekt over misbruikte kwetsbaarheden in meer dan 70 verschillende typen apparaten, van meer dan 40 fabrikanten. Het betrof zowel apparaten die *end-of-life*zijn als apparaten die nog door de fabrikant ondersteund worden.
Aangezien het botnet vat heeft gekregen op veel verschillende type kwetsbare apparaten is er waarschijnlijk sprake van meerdere uitgebuite kwetsbaarheden. De *Cyber Resilience Act*(CRA) schrijft voor dat producten met digitale elementen (hard- en software) vanaf eind 2027 aan cybersecurityvereisten moeten voldoen om in de EU op de markt te mogen worden aangeboden. Vanaf 1 augustus 2025 gelden er bovendien op grond van de radioapparatenrichtlijn al cybersecurityeisen voor het op de Europese markt aanbieden van draadloos verbonden apparatuur. De Rijksinspectie voor Digitale Infrastructuur (RDI) zal toezien op de naleving van deze eisen. De kans op kwetsbaarheden in apparatuur wordt met deze cybersecurity-producteisen aanzienlijk verkleind. Toch zullen kwetsbaarheden en hacks die daar misbruik van maken nooit volledig kunnen worden voorkomen. Om die reden krijgen fabrikanten op grond van de CRA ook een zorgplicht voor de cybersecurity van de producten gedurende de verwachte gebruiksduur, waarbij zij een gratis veiligheidsupdate moeten verstrekken zodra er een kwetsbaarheid wordt geïdentificeerd, die in beginsel automatisch wordt geïnstalleerd. Hierdoor zal de impact van een eventuele hack zo veel mogelijk worden beperkt.

Vraag 10
Welke rol hebben uw verschillende ministeries bij het verder afhandelen van de gevolgen van deze aanval?

Antwoord 10
Het NCSC heeft door tussenkomst van het DTC, waar mogelijk, eigenaren van de getroffen apparatuur op de hoogte gesteld. Er is door het DTC een algemeen advies meegegeven aan de eigenaren. Het NCSC heeft zelf geen getroffen organisaties geïnformeerd, aangezien het voor zover bekend niet ging om apparaten van organisaties binnen de Rijksoverheid of van vitale aanbieders. Ook hebben het NCSC en het DTC op hun websites algemeen beveiligingsadvies uitgebracht om dergelijke apparaten veiliger te kunnen maken. Tevens hebben het DTC en het NCSC organisaties geattendeerd op de *Joint Cyber Security Advisory* en algemene kennisproducten die weerbaarheid tegen digitale aanvallen verhogen.
Het Ministerie van Buitenlandse Zaken onderhoudt contact met partners over mogelijke aanvullende maatregelen. Mochten diplomatieke vervolgstappen t.a.v. het incident in beeld komen, dan zal het Ministerie van Buitenlandse Zaken daarover de coördinatie voeren.

Vraag 11
Met welke organisaties en partijen werken uw ministeries en de NCSC samen, zowel landelijk als internationaal, om de aanval verder af te handelen?

Antwoord 11
De verdere afhandeling van deze cyberoperatie binnen Nederland is beperkt. Er zijn voor zover bekend geen vitale of overheidsbelangen getroffen waar verdere mitigatie nodig is. Door de Amerikaanse verstoringsoperatie is de malware verwijderd van de gehackte Nederlandse apparaten in het botnet. Het kabinet heeft in de communicatie rondom dit incident gewezen op de beschikbare adviesproducten op de website van het NCSC en DTC over cyberdreigingen voor kwetsbare apparaten van particulieren en midden- en kleinbedrijf om eventuele mitigatie van kwetsbaarheden.

Vraag 12
Kunt u deze vragen afzonderlijk van elkaar en op zo kort mogelijke termijn beantwoorden?

Antwoord 12
Deze antwoorden zijn in samenwerking van de Ministers van Justitie en Veiligheid, Economische Zaken, Buitenlandse Zaken en Binnenlandse Zaken opgesteld en zijn op een zo kort mogelijk termijn beantwoord.