Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

AIVD – kenmerk
9e77515d-or1-1.12

MIVD – kenmerk
DIS2025012979

Uw kenmerk

Bijlagen
1

Datum 27 mei 2025
Betreft Attributie nieuwe Russische cyberactor

De Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst (AIVD en MIVD, tezamen de diensten) hebben middels inlichtingenonderzoek een nieuwe Russische cyberactor onderkend. Zij brengen hierover een technisch rapport uit. Aanleiding voor het onderzoek was een cyberaanval bij de politie op 23 september 2024. U bent hierover per brief geïnformeerd op 27 september, 2 oktober, 9 oktober en 8 november jl.[1] Uit onderzoek van de diensten is gebleken dat deze cyberaanval is uitgevoerd door een nieuwe, tot dusver onbekende Russische cyberactor: *Laundry Bear*. Het betreft een zeer waarschijnlijk staatsgesteunde actor.

De actor voert sinds tenminste 2024 cyberaanvallen uit tegen Westerse overheden, bedrijven en andere organisaties. Naast buitenlandse organisaties zijn er zeer waarschijnlijk ook andere Nederlandse organisaties getroffen, die hierover in een eerder stadium geïnformeerd zijn. De actor voert non-destructieve cyberaanvallen uit, zeer waarschijnlijk voor spionagedoeleinden. De diensten beschouwen deze actor en diens activiteiten als passend binnen het reeds bekende normbeeld van het Russische offensieve cyberprogramma gericht op het Westen en westerse belangen. Zowel de AIVD als de MIVD hebben dit normbeeld over Russische cyberdreiging uiteengezet in hun openbare jaarverslagen.[2]

Vanuit het belang van het verhogen van de weerbaarheid, wil het kabinet publieke en private organisaties in staat stellen om mitigerende maatregelen te kunnen treffen. De diensten publiceren daarom een technisch rapport met de belangrijkste aspecten van de werkwijze van de actor. Het technisch rapport is als bijlage bijgevoegd bij deze Kamerbrief. Het rapport bevat handelingsperspectief voor publieke en private organisaties in Nederland, en wereldwijd, om hun weerbaarheid te verhogen en onderzoek mogelijk te maken naar deze cyberactor. Hiermee wordt de slagingskans van de actor ingeperkt en kunnen digitale netwerken beter worden beschermd. Aanvullend op het rapport van de diensten zal het Nationaal Cyber Security Centrum (NCSC) zijn doelgroepen informeren over welke maatregelen ze kunnen treffen.

[1] Kamerstukken II 2024-25, 29 628, nrs. 1221, 1222, 1223, 1236.
[2] Kamerstukken II 2025-26, 30 977, nr. 174, Kamerstukken II 2025-26, 29 924, nr. 282.

Met deze publieke attributie wordt invulling gegeven aan de motie Erkens om indien mogelijk vaker cyberaanvallen en bijbehorende technische werkwijzen openbaar te maken om het bewustzijn en de weerbaarheid in Nederland op het gebied van cyberveiligheid te vergroten.[3]

Mede namens de minister van Justitie en Veiligheid,

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.J.M. Uitermark

De minister van Defensie,

Ruben Brekelmans

[3] Kamerstukken II 2023-24, 36 410-X, nr. 46.