# Veelgestelde vragen over het datalek in september 2024

## Inhoud

# Maatregelen

### Welke beveiligingsmaatregelen heeft de politie genomen?

Alle maatregelen die de afgelopen dagen zijn genomen zijn gebaseerd op het scenario dat zich nu ontvouwt. Ook toekomstig te nemen maatregelen volgen die lijn. Bij maatregelen die genomen zijn kan gedacht worden aan:

**Maatregelen op gebied van bewustwording**

- Collega's zijn nogmaals gewezen op het belang van gebruik van sterke wachtwoorden
- Medewerkers is gevraagd extra alert te zijn op phishing-mails of verdachte berichten en telefoontjes, om de impact van de hack zo klein mogelijk te maken.
- Medewerkers zijn verplicht de e-learning Altijd Alert Goud te maken.

**ICT-maatregelen**

- Collega's wordt nog vaker dan gebruikelijk gevraagd in te loggen met 2-factoridentificatie.
- Verder is de politie voortdurend alert op mogelijke aanvallen. Politie monitort continu de systemen met als doel zo snel mogelijk en adequaat te kunnen handelen.

### Waarom is de politie niet open over de genomen en te nemen maatregelen?

De maatregelen zijn in stilte genomen om het lek te kunnen dichten en om te kunnen beoordelen of het naar buiten brengen van deze maatregelen niet meer kwetsbaarheden met zich mee zou brengen. We maken continu een afweging tussen transparantie en veiligheid.

Trefwoord(en)

Waarom niet open vertelt over genomen nemen maatregelen maatregel datalek acties doen

### Waarom komt dit (nu) naar buiten?

Wij maken continue de afweging tussen transparantie en veiligheid, dit heeft invloed op de momenten waarop al dan niet gecommuniceerd kan worden. Zo snel het mogelijk is om aanvullende informatie openbaar te maken, dan doen we dat. Zo ook nu. Bovendien hopen we dat dit bijdraagt aan de bewustwording en nodige weerbaarheid tegen mogelijke cyberaanvallen van statelijke actoren.

### Lopen gegevens van burgers die bij de politie liggen ook gevaar? Denk aan informatie over aangiftes?

De informatie die buit gemaakt is bestaat uit contactgegevens van politiemedewerkers. Er is geen informatie uit andere systemen gelekt, dus gegevens van burgers lopen geen gevaar.

### In Outlook staan ook gegevens van externe partners, zoals het OM, J&V en Raad van de Rechtspraak. Zijn zij ook in geïnformeerd?

Verschillende samenwerkingspartners zijn via de SGBO's geïnformeerd dat gegevens van hun medewerkers mogelijk onderdeel zijn van het datalek.

Er zijn mailadressen van externe partners waarvan we weten dat deze ook zijn gelekt,zijn per mail op de hoogte gebracht. Voor deze groep geldt hetzelfde advies: wees extra alert op phisingmails of verdachte berichten en telefoontjes.

### Ik moet mij vaker aanmelden voor Office 365, waaronder Teams, Outlook, Excel, Word. Klopt dit?

Ja, dat klopt**.** Een van de zichtbare maatregelen is dat je vanaf heden vaker met twee factor authenticatie moet aanmelden voor Teams. We snappen dat dit vervelend is, maar het is de prijs die we betalen voor meer veiligheid.

### Kunnen de Outlook-visitekaartjes niet allemaal tegelijkertijd aangepast worden?

Momenteel wordt binnen de IV-organisatie gekeken of dit automatisch voor iedereen kan worden aangepast, zodat alleen de hoogstnodige informatie op het kaartje staat.

# Meest gestelde vragen

Antwoorden bij de vragen zijn gebaseerd op de kennis van 7 oktober 2024.

### Hoe kan ik mijn gegevens in het visitekaartje wijzigen?

Als jouw privénummer gekoppeld is aan jouw visitekaartje in Outlook, neem dan contact op met de Servicedesk IV. De servicedesk is 24/7 te bereiken via 5.1.2.i (of 5.1.2.i vanaf je werkmobiel).
Om te voorkomen dat in andere systemen (zoals BluePortaal) een privénummer zichtbaar is, raden wij je aan om jouw telefoonnummers in Youforce te controleren.

5.1.2.i

### Ik heb een phishingmail ontvangen, wat moet ik doen?

Denk je dat je een (spear)phishingmail hebt gehad? Klik dan niet, maar meld dit dan. Rechtsboven in Outlook zit de knop ‘Phishing e-mail melden’. Ons security operations center zal dan de mail onderzoeken. Op het moment dat je de knop niet ziet kun je de ICT-Servicedesk bellen voor hulp hierbij. Op je werktelefoon kun je het bericht doorsturen naar 5.1.2.i @politie.nl
Trefwoord(en)
phishingmail ontvangen wat doen datalek

### Ik word gebeld door onbekende nummers uit het buitenland, bijvoorbeeld uit Irak. Ook op mijn privénummer. Heeft dit te maken met de hack bij de politie?

Toegevoegd 1 oktober - 9.00
Voor zover bekend heeft dit geen relatie met de hack. Dergelijke telefoontjes vinden helaas regelmatig plaats. Mocht je gebeld worden door een onbekend nummer uit het buitenland, neem dan niet op en meld het telefoontje bij het meldpunt van Fraudehelpdesk. Dit geldt ook voor 06-nummers waarna een bandje in het Engels start.
Trefwoord(en)
Ik word gebeld door onbekende nummers uit het buitenland, bijvoorbeeld uit Irak. Ook op mijn privénummer. Heeft dit te maken met de hack bij de politie datalek

### In de media lees ik dat de datalek door een fout van een politievrijwilliger komt. Hoe reageert de organisatie hierop?

De Telegraaf vermeldt in een artikel dat de datalek het gevolg zou zijn van een fout van een politievrijwilliger uit de eenheid Oost-Nederland. Dit is op geen enkele manier het standpunt van de organisatie. Uit onderzoeksbelang doen we geen uitspraken over de mogelijke scenario’s. Politievrijwilligers zijn een onmisbaar onderdeel van de organisatie. Er is intern geen sprake van een beschuldiging richting politievrijwilligers.
Heb je vragen of maak je je zorgen over jouw situatie? Blijf er niet meer rondlopen, maar bespreek het met je leidinggevende of een andere collega.

### Is het gebruik van mobiele applicaties nog veilig?

De veiligheid en betrouwbaarheid van de applicaties wordt continu gemonitord. Als er signalen binnenkomen van een onveilige applicatie wordt dit meteen opgepakt. Als je twijfelt over de veiligheid van een applicatie kun je dit melden bij de Servicedesk IV. Zij zijn 24/7 bereikbaar via telefoonnummer 5.1.2.i (of 5.1.2.i vanaf je werkmobiel). Het huidige lek heeft voor zover wij nu weten geen relatie heeft met andere applicaties of diensten.

### Waarom lees ik het nieuws eerst in de media?

We zetten alles op alles om eerst intern te informeren en dan pas extern. Maar het is onmogelijk om iedereen écht gelijktijdig te bereiken. Een mail aan allen bereikt alleen de mensen die net de mail open hebben staan. Voor een bericht via 5.1.1. geldt hetzelfde; als je vrij bent, zul je die waarschijnlijk niet lezen. De kans is dan gewoon groter dat het nieuws wel via sociale media, nieuwsapps en televisie of radio bij je terechtkomt. Vooral omdat ook tijdens dit incident opnieuw is gebleken dat de media beschikken over interne bronnen die het interne nieuws meteen naar buiten brengen. Qua transparantie is dat geen probleem, qua snelheid waarop we onze collega’s éérst willen bereiken wel.

### Welke precieze gegevens zijn nu buitgemaakt bij het datalek?

Het gaat om gegevens van alle politiecollega's. Wil je weten welke gegevens bij het datalek betrokken zijn? Een eenvoudige manier om dit voor jezelf te controleren is door het visitekaartje in Outlook te bekijken. De gegevens die op dat visitekaartje te vinden zijn, zijn buitgemaakt.

### Zijn er privégegevens gelekt?

We weten dat de gegevens uit de Global Adress List uit Outlook zijn buitgemaakt. In een aantal gevallen staan hier privé-gegevens in van collega's. Er bestaat dan de kans dat deze gegevens ook zijn buitgemaakt. Dat privégegevens in de Global Adress List staan, kan te maken hebben met verschillende zaken. In het verleden heeft het veld bijvoorbeeld opengestaan en kon je deze gegevens zelf bewerken. Het kan ook mogelijk zijn dat je gegevens niet goed hebben gestaan in een HR-systeem. Wanneer je privégegevens in je visitekaartje staan, kun je dit melden bij de Servicedesk IV: telefoonnummer 5.1.2.i (of 5.1.2.i vanaf je werkmobiel). De Servicedesk IV is 24/7 te bereiken.

# Politiemedewerker

**Wat betekent dit voor de veiligheid van politiemedewerkers? Lopen politiemedewerkers (nog steeds) een risico?**
De politie doet onderzoek naar de aard, omvang en gevolgen van het datalek. Vragen over hoe het lek heeft kunnen ontstaan, maken deel uit van dat onderzoek, dat nog in volle gang is. Daarbij zijn veel specialisten uit onze organisatie betrokken. In het belang van dat onderzoek kunnen we er verder geen uitspraken over doen.

**Zijn er al gevallen bekend van collega's die te maken hebben gekregen met phishing/intimidatie/doxing?**
Nee, die zijn ons niet bekend. We zetten alles op alles om dat te voorkomen. Politiemensen moeten veilig hun werk kunnen doen. Dat is nu de hoogste prioriteit.

**Ik maak me zorgen om doxing, waar kan ik terecht?**
Op het Bluethemapagina Doxing vind je werkinstructies.

**Welke politiemedewerkers lopen hierdoor extra risico?**
De veiligheid van alle politiemedewerkers heeft hoge prioriteit van de korpsleiding. Bij het onderzoek naar de omvang en gevolgen van de hack wordt uiteraard ook de impact voor specifieke doelgroepen nauwlettend bekeken.

**Wat betekent deze hack voor doelgroepen binnen de politie die mogelijk extra risico lopen, zoals de ME, het arrestatieteam of de medewerkers die werken onder dekmantel?**
De veiligheid van alle politiemedewerkers heeft de prioriteit van de korpsleiding. Dat geldt uiteraard ook voor deze medewerkers. Bij het onderzoek naar de omvang en gevolgen van de hack wordt uiteraard ook de impact voor deze doelgroepen nader bekeken.
Net als alle andere medewerkers zijn medewerkers uit deze doelgroepen op de hoogte gesteld en hebben een mail ontvangen van de korpschef. Met vragen en zorgen kunnen zij terecht bij hun leidinggevende, bij de Servicedesk IV (5.1.2.i ) of de Servicedesk HR 5.1.2.i . De Servicedesk IV is 24/7 bereikbaar, de Servicedesk HR is van maandag tot en met vrijdag van 7.30 uur tot 17.30 uur te bereiken.

**Worden alle dienstnummers veranderd?**
Nee, daar is geen sprake van.

**Krijgen we nu allemaal nieuwe telefoonnummers en/of mailadressen?**
Nee, dit is op dit moment niet aan de orde.

**Kunnen mensen nu ook meelezen met 5.1.1.b, 5.1.2.c, 5.1.2.i**
Nee, dit is niet het geval.

**Hoe wordt er met de vragen/zorgen van collega's omgegaan?**
Met vragen en zorgen kunnen medewerkers terecht bij hun leidinggevende, of bij de Servicedesk HR via het telefoonnummer telefoonnummer 5.1.2.i (of 5.1.2.i vanaf je werkmobiel). De Servicedesk HR is van maandag tot en met vrijdag van 7.30 uur tot 17.30 uur te bereiken.

**Wat kunnen politiemedewerkers nu doen?**
We blijven alles op alles zetten om samen met veiligheidspartners politiemedewerkers te beschermen en verdere schade te voorkomen. Met collega's van ons Security Operations Center die onze cybersecurity continu aanscherpen en het Team High Tech Crime, dat strafrechtelijk onderzoek doet. Maar collega's kunnen ook zelf helpen. Door de komende tijd extra alert te zijn op phishingmails of verdachte berichten en telefoontjes.

### Hoe herken ik phisingmails of verdachte berichten en telefoontjes?

Specifieke (groepen) collega's kunnen gericht benaderd worden met op de persoon toegeschreven phishingberichten. Dat noemen we spearphishing. Dergelijke berichten zijn vaak urgent. Ze lijken afkomstig van een betrouwbaar iemand, maar deze persoon vraagt om ongebruikelijke informatie. Of de afzender vraagt je iets te downloaden of om op een link te klikken.
Denk je dat je een (spear)phishingmail hebt gehad? Klik dan niet, maar meld dit dan. Rechtsboven in Outlook zit de knop 'Phishing e-mail melden'. Ons security operations center zal dan de mail onderzoeken. Op het moment dat je de knop niet ziet kun je de ICT-Servicedesk bellen voor hulp hierbij. Op je werktelefoon kun je het bericht doorsturen naar 5.1.2.i @politie.nl
Ontvang je een phishingtelefoontje? Neem dan ook contact op met de ICT-Servicedesk.
Moet je een wachtwoord wijzigen? Zorg dan altijd voor een sterk wachtwoord. Neem contact op met de servicedesk ICT als je andere verdachte dingen tegenkomt. Ook als je niet kunt inloggen met je gebruikelijke wachtwoord.

### Waar kan ik verdachte situaties melden?

Politiemedewerkers kunnen verdachte situaties melden bij de Servicedesk IV: telefoonnummer 5.1.2.i (of 5.1.2.i vanaf je werkmobiel). De Servicedesk IV is 24/7 te bereiken.
Trefwoord(en)
Waar meldt politiemedewerkers politiemedewerker operationele operatie verdachte situaties situatie melden doorgeven datalek politie meldpunt 088 nummer

### Is mijn profielfoto in Outlook ook gelekt?

Het onderzoek loopt nog. Eerder waren er onvoldoende aanwijzingen dat de profielfoto's ook gelekt waren. Volgens de laatste informatie uit het onderzoek blijkt dat dit vermoedelijk wel het geval is.

### Hoe kan ik mijn foto verwijderen of wijzigen?

Je foto kan gekoppeld zijn aan BluePortaal. Deze foto wijzigen/verwijderen doe je door in het BluePortaal op je profielfoto te klikken (rechtsboven in de hoek) en deze dan in het menu dat verschijnt te wijzigen/verwijderen.
Mocht dit niet het juiste resultaat opleveren, kun je gaan inloggen op de 5.1.1.b, 5.1.2.c, 5.1.2.i en daar dan je profielfoto wijzigen. Mocht dit niet lukken, dan kun je contact opnemen met de Servicedesk ICT (5.1.2.i).
Update 2 oktober: er zijn verschillende manieren waarop je de profielfoto zou kunnen aanpassen of verwijderen. Welke daarvan precies de jusite is, is nog niet helemaal zeker. Er wordt door de SGBO IV onderzocht hoe de profielfoto's precies zijn opgeslagen. Het verwijderen van het bestand op bovengenoemde manier geeft dus geen 100% garantie. Als hierover meer duidelijk is, updaten we uiteraard deze Q&A.

### Wat kan ik zelf doen op het gebied van training en verdere informatie rond cybersecurity en digitale weerbaarheid?

Maak de e-learning Altijd Alert Goud. Je leert in deze training over onder andere statelijke actoren, cyberaanvallen, cyberdreigingen en social engineering. Door het maken van de e-learning leer je nog beter hoe je veilig om kunt gaan met informatie en zo kunt voorkomen dat kwaadwillenden toegang krijgen tot vertrouwelijke informatie.
Maak de e-learning Altijd Alert Zilver. Deze training bevat alle informatie om jouw kennis over informatiebeveiliging up-to-date te houden. Bijvoorbeeld over het rubriceren van informatie, het melden van incidenten en het gebruik van een wachtwoordmanager. Heb je deze training al gemaakt, dan maak je Goud nog.
Op de pagina van Altijd Alert vind je ook meer informatie.
Binnen de politie maken we sinds een paar jaar gebruik van het Cybersecurity Portaal, wat een trainingsplatform is dat sterk de nadruk legt op Cybersecurity. Dit portaal biedt direct toegang tot trainingen, instructievideo`s, securitychallenges en tests van een gerenommeerde externe partij op dit gebied. Je leert bijvoorbeeld welke risico`s je nu echt loopt online en hoe je jezelf en jouw collega`s online het best kan beschermen.
Hier vind je de instructies om in te loggen.

**Ik heb familieleden toegevoegd aan mijn adresboek in Outlook. Zijn die gegevens ook betrokken bij de hack?**
Als je deze zelf hebt toegevoegd aan je persoonlijke lijst contactpersonen, dan zijn die gegevens nog steeds veilig.

**Wat kan ik verwachten, nu mijn werkgegevens gelekt zijn, als ik naar het buitenland ga voor werk (of privé)?**
De informatie die je met je meedraagt (zowel fysiek als digitaal) kan interessant zijn voor anderen. Zorg dus dat je goed voorbereid op reis gaat. Op de pagina van de Sector Informatiebeveiliging vind je handige tips die je kunnen helpen om (informatie) veilig op reis te gaan.

**Ik heb een eenmanszaak en mijn bezoekadres is zichtbaar bij de KVK. Wat kan ik doen?**
Als je bij de KVK geregistreerd staat als eenmanszaak, kun je jouw bezoekadres wijzigen naar een postadres. Deze wijzigingen worden met spoed doorgevoerd. Als je geen postadres hebt kan het momenteel niet aangepast worden. Wel wordt nog gekeken naar wat hier de mogelijkheden voor zijn voor politiemedewerkers.

# Update 3/11/2024: "hack door statelijke actor"

### Wat is er nu bekend geworden over de hack?
Wij zijn door de 5.1.1.b, 5.1.2.c, 5.1.2.i geïnformeerd dat het zeer waarschijnlijk is dat een statelijke actor verantwoordelijk is voor het cyberincident.  Met andere woorden: we gaan ervan uit dat een ander land of daders in opdracht van een ander land verantwoordelijk is. In het belang van het onderzoek kan er geen aanvullende informatie worden verstrekt.
Op basis van die informatie zijn in stilte meteen forse beveiligingsmaatregelen ingezet tegen deze aanval. Er is voor gekozen niet te noemen wie erachter zit en hoe ze te werk zijn gegaan om de daders niet wijzer te maken en verder onderzoek niet te schaden.

### Om wie/welk land gaat het?
Daarover is afgesproken dat er geen uitspraken over gedaan kunnen worden.

### Hoe lang is dit al bekend?
In het belang van het onderzoek kunnen we daar geen uitspraken over doen.

### Hoe is de politie hierachter gekomen?
Wij zijn door de 5.1.1.b, 5.1.2.c, 5.1.2.i in geïnformeerd dat het zeer waarschijnlijk is dat een statelijke actor verantwoordelijk is voor het cyberincident.

### Hebben de aanvallers nog steeds toegang tot het systeem?
We hebben geen aanleiding om aan te nemen dat dit risico nu nog bestaat. De monitoring van de omgeving is echter geïntensiveerd en nader onderzoek loopt nog.

### Waarom komen jullie nu met deze informatie? Veroorzaakt dit niet alleen maar meer onrust?
Wij maken continue de afweging tussen transparantie en veiligheid, dit heeft invloed op de momenten waarop al dan niet gecommuniceerd kan worden. Zo snel het mogelijk is om aanvullende informatie openbaar te maken, dan doen we dat. Zo ook nu.

### Hebben de aanvallers nog steeds toegang tot politiesystemen?
We hebben geen aanleiding om aan te nemen dat dit risico nu nog bestaat. De monitoring van de omgeving is geïntensiveerd en nader onderzoek loopt nog.

### Wat betekent ‘statelijke actor’?
Statelijke actoren vertegenwoordigen een regering van een land. Het betreft dus individuen of entiteiten die geassocieerd zijn met een regering of een staat vertegenwoordigen.

### Welke dreiging volgt hieruit? Wat zou ‘deze actor’ met deze data kunnen?
De politie doet onderzoek naar de aard, omvang en gevolgen van het datalek. Vragen over hoe het lek heeft kunnen ontstaan, maken deel uit van dat onderzoek, dat nog in volle gang is. Daarbij zijn veel specialisten uit onze organisatie betrokken. In het belang van dat onderzoek kunnen we er verder geen uitspraken over doen.

### Heeft de phishing mail die recentelijk naar alle medewerkers van de Politieacademie is gestuurd te maken met deze hack?
Nee, dit is niet het geval.

# Update 9/11/2024: "Mogelijk foto's buitgemaakt"

### Bestaat het risico dat er nog meer gegevens zijn buitgemaakt?
Met de kennis van nu hebben we geen aanwijzingen dat er naast de gegevens uit de Global Address List nog andere gegevens zijn buitgemaakt. Voor zover nu bekend is, zijn de gegevens buitgemaakt die vermeld staan in het visitekaartje. We doen uitvoerig onderzoek en krijgen elke dag meer zicht op welke gegevens het precies betreffen. We informeren collega's zo snel mogelijk over de informatie die beschikbaar is, zonder daarbij het onderzoek te schaden.

### We begrijpen dat mogelijk ook data uit andere systemen is gelekt. Klopt dat?
Met de kennis van nu hebben we geen aanwijzingen dat er naast de gegevens uit de Global Address List nog andere gegevens zijn buitgemaakt.

### Hoeveel foto's zijn er gelekt?
Van een deel van de collega's zijn mogelijk foto's buitgemaakt. Het gaat vermoedelijk om foto's of afbeeldingen, die in het visitekaartje worden gebruikt, maar dit is niet 100% zeker. Bij afbeeldingen kan gedacht worden aan bijvoorbeeld avatars of cartoons die door medewerkers aan hun visitekaartje toegevoegd zijn.

### Hoe is mijn foto of afbeelding in het visitekaartje terecht gekomen?
Medewerkers hebben deze handmatig toegevoegd aan hun visitekaartje

### Hoe kom ik erachter of en zo ja welke foto gelekt is?
Wil je weten welke afbeelding(en) mogelijk bij het datalek betrokken zijn? Een eenvoudige manier om dit voor jezelf te controleren is door het visitekaartje in Outlook te bekijken. De afbeelding die op dat visitekaartje te vinden is, is mogelijk buitgemaakt.

### Ik maak me zorgen over het lekken van mijn foto. Wat kan ik doen?
Je kunt jezelf en de organisatie weerbaarder helpen maken om de kans op een vervolg te verkleinen. Bekijk de Menukaart Maatregelen Datalek die online staatop BlueThema Datalek en volg de e-learning Altijd Alert Goud.

### Waarom krijg ik in eerste instantie te horen dat er alleen naam, functie en telefoonnummer zijn gelekt. Maar blijkt later toch dat er privégegevens en profielfoto's zijn gelekt?
We doen uitvoerig onderzoek en krijgen elke dag meer zicht op welke gegevens zijn buitgemaakt. We informeren collega's zo snel mogelijk over de informatie die beschikbaar is, zonder daarbij het onderzoek te schaden.
Uit nieuwe informatie blijkt dat het vermoedelijk ook gaat om foto's of afbeeldingen, die in het visitekaartje worden gebruikt, maar dit is niet 100% zeker.

### Wat kunnen de daders met de buitgemaakte foto's? Wat zijn de gevolgen?
Dit is onderdeel van het onderzoek en kunnen we op dit moment geen mededelingen over doen.

### Zijn er ook foto's van ketenpartners (OM, Belastingdienst, etc.) onderdeel van de buitgemaakte gegevens?
In de gevallen waarbij medewerkers van ketenpartners over een politie account beschikken én zelf handmatig een foto hebben toegevoegd aan hun visitekaartje, is het mogelijk dat deze foto's buitgemaakt zijn. Voor medewerkers van ketenpartners zonder politieaccount geldt dit niet.

# Voor leidinggevende

**Waar vind ik als leidinggevende aanvullende informatie?**
Op deze BlueThema-pagina vind je meer informatie, vragen & antwoorden en instructies voor leidinggevenden rondom het datalek.

# Update 27/05/2025: "Werkwijze van de cyberactor"

### Waarom wordt dit nieuws op dit moment naar buiten gebracht?

De diensten kiezen er bewust voor om de werkwijze van deze cyberactor bloot te leggen, door middel van publicatie van een technisch advies. Zo kunnen niet alleen overheden maar ook fabrikanten, leveranciers en andere doelwitten zich wapenen tegen deze vorm van spionage. Hiermee wordt de slagingskans ingeperkt en kunnen digitale netwerken beter worden beschermd. Dit vergroot de weerbaarheid.

### Was de hack gericht op de politie?

Uit technisch onderzoek blijkt dat de actor zeer waarschijnlijk de politie opportunistisch heeft aangevallen. Dat wil zeggen, dat de actor zich niet alleen op de politie heeft gericht. Deze actor voerde sinds tenminste 2024 cyberaanvallen uit bij bedrijven en organisaties in ruim 40 Westerse landen. Ze richten zich specifiek op krijgsmachten, overheden, defensie(toe)leveranciers, sociaal-maatschappelijke organisaties en IT- en digitale dienstverleners. Veel slachtoffers werden op een vrij generieke manier gemaakt.

### Is deze nieuwe informatie (over de daders) van invloed op de voorbereidingen/maatregelen m.b.t. de NAVO-top?

Cyberaanvallen waren al één van de scenario's waar we rekening mee houden. Ook vorige NAVO-Toppen kregen ermee te maken. Deze nieuwe informatie stelt ons – maar ook andere organisaties – in staat om de weerbaarheid verder te vergroten. Over concrete maatregelen kunnen we echter geen uitspraken doen.

### Destijds werd bekend gemaakt dat er alleen zakelijke contactgegevens werden buitgemaakt. Is dat nu nog steeds het beeld?

Toen en ook nu hebben zowel de AIVD en MIVD, als de politie, niet kunnen vaststellen dat er door deze cyberactor andere gegevens dan de Global Address List (GAL) zijn buitgemaakt. In enkele gevallen waren het ook privé (contact)gegevens die personen met een politieaccount zelf in hun visitekaartje hebben toegevoegd.
Trefwoord(en)

### Wordt er weer een meldpunt ingericht waar politiemensen met vragen terecht kunnen?

Sinds vandaag (27 mei) is er weer een meldpunt ingericht waar politiemensen hun zorgen en vragen kwijt kunnen. Dit is te bereiken via 5.1.2.i . Of via 5.1.2.i @politie.nl

### Wat kunnen politiemedewerkers doen?

Wees extra alert op phishingmails of verdachte berichten en telefoontjes. Specifieke (groepen) collega's kunnen gericht benaderd worden met op de persoon toegeschreven phishingberichten. Dat noemen we spearphishing. Dergelijke berichten zijn vaak urgent. Ze lijken afkomstig van een betrouwbaar iemand, maar deze persoon vraagt om ongebruikelijke informatie. Of de afzender vraagt je iets te downloaden of om op een link te klikken. Denk je dat je een (spear)phishingmail hebt gehad? Klik dan niet, maar meld dit dan. Rechtsboven in Outlook zit de knop 'Phishing e-mail melden'. Ons security operations center zal dan de mail onderzoeken. Op je werktelefoon kun je het bericht doorsturen naar 5.1.2.i @politie.nl
Moet je een wachtwoord wijzigen? Zorg dan altijd voor een sterk en uniek wachtwoord.
Neem contact op met de servicedesk ICT als je andere verdachte dingen tegenkomt. Ook als je niet kunt inloggen met je gebruikelijke wachtwoord. Ben je ongerust of heb je vragen over dit incident, neem dan contact op met je leidinggevende.

### Welke (aanvullende/nieuwe) maatregelen treft de politie?

Direct na de hack heeft de politie verschillende aanvullende veiligheidsmaatregelen genomen en we monitoren continu op mogelijke cyberaanvallen. Bij de verschillende veiligheidsmaatregelen die zijn genomen, is ook rekening gehouden met deze mogelijke actor. Over specifieke maatregelen kunnen wij geen uitspraken doen. Het is belangrijk voor organisaties – dus ook voor ons – om zich goed te blijven wapenen tegen dergelijke cyberaanvallen en deze vorm van spionage. Buitgemaakte data van slachtoffers kan bovendien gebruikt worden om vervolgaanvallen mee te plegen. Het is daarom belangrijk om alert te zijn, en te blijven. De informatie die nu door de diensten is vrijgegeven helpt bij het vergroten van die weerbaarheid.

### Hoe voorkom je dat je slachtoffer wordt van infostealer-malware?

5.1.2.i

### Is het onderzoek van het THTC al afgerond? Zo ja, wat zijn de conclusies?

De resultaten van het opsporingsonderzoek van de politie ondersteunen de bevindingen uit het vandaag gepubliceerde rapport van de inlichtingendiensten. We hebben vanuit het opsporingsonderzoek zicht gekregen op de werkwijze van deze criminelen. Ook hebben we eerder deze week een deel van de digitale infrastructuur die door deze hackersgroep werd gebruikt ontoegankelijk gemaakt. Dit deden we door accounts van de diensten die zij gebruiken, te blokkeren.

### Wat houdt een ‘pass-the-cookie-aanval’ in?

Het doel van een pass-the-cookie-aanval is om een actieve sessie van een gebruiker over te nemen. Zo kan een aanvaller toegang krijgen tot een website of applicatie, zonder het inlogproces te hoeven doorlopen. Dit is vooral relevant als die toegang beveiligd is met 2-factor authenticatie (zoals dat ook bij de politie het geval was) en de aanvaller geen toegang heeft tot een van de toegangsmiddelen (5.1.1.b, 5.1.2.c, 5.1.2.i

Voor een pass-the-cookie aanval heeft de aanvaller een sessie-token nodig (de cookie). Zo’n sessie-token wordt normaal gesproken opgeslagen op de computer van een gebruiker, nadat die via het inlogproces heeft ingelogd. Als de gebruiker dezelfde computer nogmaals wil gebruiken om toegang te krijgen tot zijn applicatie hoeft hij niet opnieuw het inlogproces te doorlopen. De applicatie gebruikt in plaatst daarvan automatisch het opgeslagen sessie-token om de toegang te verkrijgen.

Een aanvaller kan een sessie-token van een legitieme gebruiker op verschillende manieren verkrijgen. In het geval van de politiehack is uit het onderzoek gebleken dat de sessie-token (cookie) 5.1.1.b, 5.1.2.c, 5.1.2.i

.