AIVD en MIVD onderkennen nieuwe Russische cyberactor

Dit is een gezamenlijke publicatie van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Een bijbehorend persbericht is gepubliceerd op de websites van de AIVD en het ministerie van Defensie.

1. Samenvatting

- De AIVD en MIVD hebben een tot nu toe publiek onbekende, zeer waarschijnlijk Russische staatsgesteunde cyberactor onderkend en de naam LAUNDRY BEAR gegeven.

- LAUNDRY BEAR is verantwoordelijk voor het uitvoeren van cyberoperaties tegen westerse overheden sinds 2024 en heeft een specifieke interesse in de krijgsmacht, overheden, defensie(toe)leveranciers, sociaal-maatschappelijke organisaties en digitale dienstverleners.

- Aanleiding voor het onderzoek naar deze actor was een opportunistische cyberaanval op de Nederlandse politie in september 2024. Bij deze aanval zijn werkgerelateerde contactgegevens van politiemedewerkers buitgemaakt. De diensten en de politie hebben niet kunnen vaststellen dat er andere gegevens zijn buitgemaakt. Zeer waarschijnlijk zijn ook andere Nederlandse organisaties slachtoffer geweest van deze actor.

- LAUNDRY BEAR weet onder de radar te blijven door gebruik te maken van eenvoudige aanvalstechnieken en -paden die beschikbaar zijn op de computer van een slachtoffer, die lastig te detecteren zijn voor organisaties en lastig te onderscheiden zijn van andere bekende Russische actoren.

2. Oorsprong en attributie

Op 23 september 2024 werd de politie slachtoffer van een cyberaanval waarbij de werkgerelateerde contactgegevens van alle politiemedewerkers door een cyberactor zijn buitgemaakt. Uit daaropvolgend technisch onderzoek van de diensten is gebleken dat deze cyberaanval is uitgevoerd door een tot nu onbekend gebleven, zeer waarschijnlijk Russische staatsgesteunde cyberactor.

De diensten hebben deze actor de naam LAUNDRY BEAR gegeven.[1] Uit onderzoek blijkt dat deze actor al sinds tenminste 2024 cyberaanvallen uitvoert tegen westerse overheden, bedrijven en andere organisaties. LAUNDRY BEAR lijkt hiermee een relatief nieuwe cyberactor te zijn. De diensten beschouwen LAUNDRY BEAR en diens doelwitselectie als passend binnen het reeds bekende normbeeld van het Russische offensieve cyberprogramma, gericht op het Westen en westerse belangen.

Ondanks dat de diensten nu over deze actor naar buiten treden, beschikken zij niet over volledig zicht op deze actor en zijn activiteiten. Het is de intentie van de diensten via deze publicatie de cyberactor bekend te maken en partijen in staat te stellen de juiste weerbaarheidsmaatregelen te treffen om organisaties beter te beschermen.

2.1 Activiteiten

Op basis van technisch onderzoek, in samenwerking met de politie, zijn de diensten in staat geweest om inzicht te verkrijgen in de activiteiten van LAUNDRY BEAR. Zo wordt duidelijk welke landen en sectoren de actor aanvalt.

2.1.1 Type cyberoperaties

LAUNDRY BEAR voert tot op heden enkel niet-destructieve cyberaanvallen uit, zeer waarschijnlijk voor spionagedoeleinden. Uit het technisch onderzoek van de AIVD en MIVD blijkt dat LAUNDRY BEAR succesvol toegang weet te verkrijgen tot gevoelige informatie van een groot aantal (overheids-)organisaties en bedrijven wereldwijd met een specifieke interesse voor landen uit de Europese Unie en de NAVO. LAUNDRY BEAR verkrijgt die informatie door binnen te dringen in (cloud)e-mailomgevingen, met name exchange servers. Hierbij ontvreemdt LAUNDRY BEAR op grote schaal en in hoog tempo bijvoorbeeld e-mails en informatie over mailcontacten van een organisatie

[1] De AIVD en MIVD werken samen met Microsoft in het onderzoek naar LAUNDRY BEAR. Microsoft hanteert de naam Void Blizzard voor deze actor.

zoals een *Global Address List* (GAL). Deze informatie kan de actor achterhalen via toegang tot een gebruikersaccount. De diensten hebben vastgesteld dat LAUNDRY BEAR soms ook bestanden weet buit te maken. Het gaat dan onder meer over data die is opgeslagen in de cloud.

*2.1.2 **Doelwitten***

Net als andere Russische cyberactoren voert LAUNDRY BEAR gericht cyberaanvallen uit op landen die onderdeel uitmaken van de Europese Unie of de NAVO. Vrijwel alle landen binnen deze twee internationale samenwerkingsverbanden zijn doelwit van de actor. De aanvallen van LAUNDRY BEAR richten zich op zaken die direct relevant zijn voor de Russische oorlogsinspanningen in Oekraïne: ministeries van defensie van NAVO-landen, hun vertegenwoordigers bij andere organisaties, krijgsmachtonderdelen en defensie(toe)leveranciers. Net als bij Russische actoren die cyberspionage uitvoeren in het Westen, valt LAUNDRY BEAR ook ministeries van buitenlandse zaken en diverse EU-instellingen aan. De diensten hebben naast gerichte cyberaanvallen op EU- en NAVO-lidstaten ook aanvallen van LAUNDRY BEAR waargenomen op entiteiten in andere regio's, in het bijzonder in Oost- en Centraal-Azië.

In 2024 voerde LAUNDRY BEAR cyberaanvallen uit tegen defensie-, lucht- en ruimtevaart technologiebedrijven die militair materieel produceren. Uit het technisch onderzoek uitgevoerd bij slachtoffers blijkt dat LAUNDRY BEAR zeer waarschijnlijk uit was op het verkrijgen van (gevoelige) informatie over de aanschaf en productie van militair materiaal door westerse overheden en westerse wapenleveringen aan Oekraïne. De diensten zien dat de actor enige mate van kennis lijkt te bezitten over de vervaardiging en levering van defensiematerieel en de daarvoor benodigde subonderdelen. Daarnaast heeft LAUNDRY BEAR ook cyberaanvallen uitgevoerd tegen bedrijven die hoogwaardige technologieën produceren waar Rusland door huidige westerse sancties moeilijk aan weet te komen. De exacte doelen van deze spionageaanvallen zijn met de huidige informatie niet vast te stellen.

Daarnaast zien de diensten een bredere interesse bij deze actor. Ook civiele organisaties en bedrijven zijn doelwit van deze groep. De aanvallen concentreren zich vooral op de IT- en technologiesector, inclusief digitale dienstverleners aan grote organisaties als overheden. Netwerken van dergelijke organisaties bevatten vaak niet alleen informatie over processen, maar bieden vaak ook direct of indirect toegang tot informatie of netwerken van hun klanten, zoals bijvoorbeeld overheden, en zijn zo een interessant doelwit voor cyberactoren.[2] Verder zagen de diensten ook dat non-gouvernementele organisaties, politieke partijen, media en onderwijs doelwit zijn van LAUNDRY BEAR. Tot slot hebben de diensten ook aanvallen op enkele vitale sectoren waargenomen, zeer waarschijnlijk uitsluitend voor spionagedoeleinden. LAUNDRY BEAR is, vergeleken met enkele andere Russische actoren waar de diensten onderzoek naar doen, zeer succesvol. Zie voor de meest aangevallen sectoren figuur 1.

Figuur 1: overzicht meest aangevallen sectoren.

[2] Wanneer een actor een organisatie binnendringt door eerst een vertrouwde toeleverancier te compromitteren wordt dit een supply chain-aanval genoemd.

*2.1.3 **Ook Nederlandse slachtoffers***

In september 2024 verkreeg LAUNDRY BEAR toegang tot een account van een medewerker van de Nederlandse politie. Hierbij is het de actor gelukt om via dit account de werkgerelateerde contactgegevens – de GAL – van politiemedewerkers buit te maken. Uit technisch onderzoek blijkt dat de actor zeer waarschijnlijk de politie opportunistisch heeft aangevallen via een *pass-the-cookieaanval*.[3] Dit is een techniek waarbij de actor zich voordoet als de eigenaar van een cookie. Naar aanleiding van het technische onderzoek achten de diensten het waarschijnlijk dat deze cookie is buitgemaakt via *infostealer*-malware van mogelijk een derde partij en daarna door LAUNDRY BEAR via criminele fora is aangeschaft. Met deze buitgemaakte cookie kan de actor zonder een wachtwoord of gebruikersnaam in te vullen toegang verkrijgen tot bepaalde informatie.

De diensten en de politie hebben niet kunnen vaststellen dat er door LAUNDRY BEAR via dit account andere gegevens dan de GAL zijn buitgemaakt. Technisch onderzoek wijst uit dat LAUNDRY BEAR zeer waarschijnlijk ook andere Nederlandse slachtoffers heeft gemaakt.

2.2 Impact van techniek op snelheid en succesvolle aanvallen

LAUNDRY BEAR voert in hoog tempo cyberoperaties uit. De diensten achten het zeer waarschijnlijk dat de actor enige mate van automatisering in de aanvalsketen heeft aangebracht. Deze automatisering lijkt dusdanig efficiënt ingericht dat dit resulteert in veel aanvallen in korte tijd. De door de actor daarbij gekozen aanvalsmethoden resulteren in een hoog aantal succesvolle compromitteringen.

LAUNDRY BEAR maakt gebruik van relatief eenvoudige technieken die in sommige gevallen ook lastig te detecteren kunnen zijn. LAUNDRY BEAR beschikt voor zover de diensten hebben waargenomen niet over eigen malware en LAUNDRY BEAR weet te profiteren van *Living Of The Land*-mogelijkheden[4] om succesvol te opereren, wat het opportunistische karakter van de actor benadrukt.

De actor poogt via phishing of authenticatietokens of -cookies die verkregen zijn via (criminele) fora accounts binnen te dringen bij doelwitten.[5] Daarnaast maakt LAUNDRY BEAR gebruik van *password spraying*, waarbij enkele wachtwoorden op verschillende accounts worden uitgeprobeerd om zo in te loggen. Kenmerkend aan deze techniek is dat het aantal inlogpogingen per account gespreid wordt over tijd door eerst hetzelfde wachtwoord bij andere accounts te proberen, om daarna een ander wachtwoord te proberen. Dit voorkomt vaak dat netwerk- en systeembeheerders notificaties krijgen van foute inlogpogingen en zo kan de actor onopgemerkt blijven. Hierin verschilt het dus van een zogeheten *brute force*-aanval waarbij veel inlogpogingen in korte tijd op hetzelfde account worden gedaan. De lijst met wachtwoorden die gebruikt worden in een *password spray*-aanval bestaan bijvoorbeeld uit bekende gelekte wachtwoorden (naar aanleiding van datalekken die online gepubliceerd zijn). In dit soort overzichten staan bijvoorbeeld wachtwoorden als ‘wachtwoord123’, ‘welkom123’, en ‘qwerty’. Deze wachtwoorden lijken nog opvallend vaak te werken.

Na succesvolle authenticatie benadert LAUNDRY BEAR slachtoffers via Microsoft Exchange Web Services (EWS) en Outlook Web Access (OWA) om een of meerdere acties uit te voeren op het slachtoffernetwerk. Zo gaat LAUNDRY BEAR op zoek naar welke rechten het account van het slachtoffer heeft. De diensten achten het zeer waarschijnlijk dat LAUNDRY BEAR eerst probeert om de GAL te downloaden. Informatie uit die GAL wordt vervolgens gebruikt voor *password spraying*-aanvallen om toegang te verkrijgen tot andere accounts. Onderzoek wijst uit dat de actor ook kijkt naar mailaccounts die accounts voor anderen beheren (zogenoemde *delegates*). Bij succesvolle aanvallen weet

[3] Een cookie is een klein tekstbestand dat door een website op de computer of mobiel apparaat van een gebruiker wordt geplaatst om informatie over die gebruiker te verzamelen en op te slaan, zoals surfgedrag of inloggegevens. Zo kan je bijvoorbeeld ingelogd blijven op een bepaalde website.

[4] Living-off-the-Land (LOTL) verwijst naar een tactiek waarbij een aanvaller gebruik maakt van bestaande systemen en tools op de computer of het netwerk van het slachtoffer om zijn aanval uit te voeren, in plaats van zijn eigen malware te introduceren. Hierdoor laat de aanvaller minder sporen achter. Omdat de activiteiten eruitzien alsof ze door een legitieme gebruiker worden uitgevoerd, is het moeilijker voor beveiligingssystemen om de aanval te detecteren.

[5] Phishing is het misleiden van een beoogd doelwit via een e-mail (of andere berichten systemen) die wat anders doet of bevat dan op eerste oog duidelijk is. Het is waarschijnlijk dat LAUNDRY BEAR in de phishingmail aan hun doelwitten thema’s gebruikt die bij hun interessegebieden aansluiten.

LAUNDRY BEAR zijn toegang binnen de Microsoftomgeving van het slachtoffer uit te breiden waarmee LAUNDRY BEAR zeer waarschijnlijk e-mails en andere informatie binnen deze omgeving weet te verzamelen. Uit technisch onderzoek is gebleken dat LAUNDRY BEAR in staat is geweest om op grote schaal emailverkeer van slachtoffers buit te maken. Ook hebben de diensten vastgesteld dat LAUNDRY BEAR in enkele gevallen data heeft buitgemaakt van de Sharepoint-omgeving van slachtoffers. De diensten hebben vastgesteld dat de actor gebruikmaakt van bekende kwetsbaarheden voor het verzamelen van inloggegevens voor vervolgoperaties. Doordat LAUNDRY BEAR zich zeer waarschijnlijk beperkt tot de reeds bestaande toegang tot (Microsoft-)accounts en niet zijn toegang poogt te vergroten tot achterliggende netwerken of systemen, lijkt de actor langer en eenvoudig onder de radar van systeem- en netwerkbeheerders te blijven.

De diensten werken samen met Microsoft in het onderzoek naar LAUNDRY BEAR om misbruik van Microsoftsystemen te mitigeren.

2.2.1 LAUNDRY BEAR en APT28

Veel van de aanvalstechnieken waar LAUNDRY BEAR gebruik van maakt, worden ook door andere cyberactoren gebruikt. Dit gebeurt zeer waarschijnlijk omdat de technieken niet al te complex en daardoor makkelijker te gebruiken zijn. Bijkomend voordeel voor de actor is dat het lastig is om de aanval aan een specifieke actor toe te kennen.

Gedurende het onderzoek van de diensten naar LAUNDRY BEAR constateerden de diensten met enige regelmaat dat aanvallen van LAUNDRY BEAR overlap vertonen met de *modus operandi* van APT28. Deze Russische statelijke actor wordt door de MIVD toegeschreven aan eenheid 26165 van de Russische militaire inlichtingendienst GRU. Naast een overeenkomende doelwitselectie overlapt ook het gebruik van *password spraying*-aanvallen. LAUNDRY BEAR en APT28 zijn wel twee verschillende actoren.

2.3 De toekomst van LAUNDRY BEAR

De diensten beschouwen LAUNDRY BEAR als een actor in opbouw en achten het mogelijk dat de cyberactor in de toekomst andere, meer complexe manieren van aanvallen aan zijn arsenaal zal toevoegen. Ook kan de buitgemaakte informatie uit de GAL gebruikt worden voor vervolgaanvallen, zoals spearphishing. Doordat LAUNDRY BEAR een vrij nieuwe actor is, is het lastig om de toekomst van de actor in te schatten. Door de geautomatiseerde wijze waarop LAUNDRY BEAR op grote schaal impact weet te maken, beoordelen de diensten dat er een verhoogde spionagedreiging uitgaat van deze actor.

3. Weerbaarheidsbevorderende maatregelen

Om verder inzicht te bieden in de werkwijze van LAUNDRY BEAR, kiezen de diensten ervoor om informatie vrij te geven over de aanvalstechnieken van de actor. Hiervoor wordt gebruik gemaakt van het zogenoemde MITRE ATT&CK raamwerk.[6] Daarbij delen de diensten welke weerbaarheidsbevorderende maatregelen getroffen kunnen worden.

Tactic	Technique ID	Technique name
Initial Access / privilege escalation	T1078	Valid accounts
Persistence / privilege escalation	T1098.002	Account manipulation
Credential access	T1539	Steal web session cookie
Credential access	T1110.003	Password spraying
Discovery	T1087	Account discovery
Collection	T1114.002	Remote email collection
Command and Control	T1090	Proxy
Exfiltration	T1048.003	Exfiltration over alternative protocol (non-C2 protocol)

3.1 Verkrijgen van toegang via geldige accounts (T1078)

Actoren kunnen bestaande accountgegevens verkrijgen en misbruiken om initiële toegang te verkrijgen, persistentie te behouden, verkrijgen van verhoogde rechten of detectie te omzeilen.

Mitigatie en aanbevelingen:

- **Gebruik Least Privilege-principes** Gebruikers en services krijgen hierbij alleen de minimale rechten die nodig zijn om hun taken uit te voeren, zo wordt de potentiële schade geminimaliseerd.

- **Implementeer Privileged Access Management (PAM)** om het gebruik van accounts met verhoogde privileges te controleren, te monitoren en te beperken. Dit kan helpen bij het detecteren en voorkomen van ongeautoriseerde verhoogde rechten te verkrijgen.

- **Implementeer Zero Trust-architectuur** Overweeg het implementeren van een Zero Trust-beveiligingsmodel, waarbij alle gebruikers en apparaten binnen of buiten het netwerk als potentieel onbetrouwbaar worden behandeld en alleen toegang krijgen op basis van strikte autorisatie- en verificatieprocessen.

- **Gebruik sterke authenticatie** Implementeer multifactorauthenticatie (MFA) om te voorkomen dat cyberactoren toegang krijgen tot accounts met alleen een wachtwoord, zelfs als ze het wachtwoord kennen.

3.2 Account manipulatie via veranderen permissies (T1098.002)

Bij accountmanipulatie via het veranderen van toegangsrechten, proberen cyberactoren de machtigingen of rechten van bestaande e-mail accounts te wijzigen, zodat ze meer toegang krijgen tot gevoelige informatie of systemen. Het wordt ook ingezet om toegang te kunnen behouden. Dit kan op verschillende manieren gebeuren, zoals bijvoorbeeld door het toewijzen van extra rechten, wijzigen van groepslidmaatschap en verandering van gebruikersrechten.

Dit type aanval kan gevaarlijk zijn omdat het moeilijk kan zijn deze te detecteren. Cyberactoren kunnen bestaande accounts gebruiken die al vertrouwd zijn door het systeem, waardoor de activiteit minder opvallend is dan het maken van een compleet nieuwe account met verdachte machtigingen.

[6] Meer informatie over het MITRE ATT&CK raamwerk is te vinden op de website attack.mitre.org.

Mitigatie en Aanbevelingen:

- **Audits** Voer regelmatig audits uit op gebruikersaccounts en hun respectievelijke machtigingen.

- **Toegangsbeheer** Controleer het toegangsbeheer strikt met principes als "minimale bevoegdheid" (*least privilege*), waarbij gebruikers alleen de rechten krijgen die absoluut noodzakelijk zijn voor hun taken.

- **Logging en monitoring** Stel logging en monitoring van accountactiviteiten in om ongebruikelijke wijzigingen in gebruikersrechten of gedrag snel op te merken.

3.3 Stelen web-sessie cookie (T1539)

Actoren verkrijgen toegang tot netwerken door het bemachtigen van bestaande cookie-sessies van gebruikers. Een actor weet zo op een legitieme manier toegang te verkrijgen tot het netwerk. Waarschijnlijk worden deze cookies aangeboden op (criminele) fora nadat deze via malware zoals *infostealer*-malware, van een andere (criminele) actor zijn buitgemaakt.

Mitigatie en aanbevelingen:

- **Beheer apparaten** Maak geen gebruik van bring-your-own-devices (BYOD, laptop of telefoon) of beperk dit zoveel mogelijk. Zorg dat de organisatie alle apparaten beheert die toegang hebben tot zijn IT-systemen. Hiermee verkleint de organisatie de kans dat apparaten met geïnstalleerde malware in het netwerk worden opgenomen. Bovendien heeft de organisatie dan beter zicht op het gedrag van deze apparaten. Het risico voor het stelen van een sessiecookie is groter in een organisatie waar gebruik wordt gemaakt van apparaten die niet worden beheerd.

- **Beheer systemen** Maak daarnaast alleen gebruik van beheerde systemen voor toegang tot gevoelige omgevingen als Sharepoint en Exchange online. Sta inlogpogingen voor belangrijke accounts alleen toe vanuit de IP-adressen die bij de organisatie bekend zijn.

- **Levensduur cookies** Stel de levensduur van een sessie zo kort als praktisch mogelijk in. Dit verkleint de periode die een actor kan gebruiken om zich toegang te verschaffen. Het vermindert direct de bruikbaarheid van gestolen cookies met een access-token. De juiste levensduur is een risicoafweging tussen gebruikersgemak en veiligheid.

- **Browsercookies** Dwing in het beveiligingsbeleid af dat browsercookies regelmatig worden verwijderd en zie erop toe dat dit wordt geïmplementeerd.

- **Sessieherbinding** Schakel sessieherbinding uit, zodat slechts één IP-adres een sessiecookie mag gebruiken. Dit bemoeilijkt aanzienlijk het gebruik van gestolen sessiecookies.

- **Voorwaardelijke toegang** Overweeg het implementeren van voorwaardelijke toegang (conditional access) om het inloggen van gebruikers te beperken vanaf specifieke IP-locaties, IP-bereiken of afkomstig van specifieke hardware.

- **Multifactorauthenticatie** Implementeer phishingresistente MFA door middel van een (FIDO2-) hardwaretoken.

- **ID protection** Overweeg gebruik te maken van Microsoft Entra ID Protection of vergelijkbare oplossingen van Amazon Web Services (AWS) of Google. Dit soort oplossingen maakt detectie van pass-the-cookie of soortgelijke aanvallen mogelijk.

3.4 Brute Force: Password spraying (T1110.003)

Password spraying is een type cyberaanval waarbij een cyberactor probeert om ongeautoriseerd toegang te krijgen tot een groot aantal accounts door een klein aantal veelvoorkomende wachtwoorden uit te proberen tegen veel

verschillende gebruikersnamen. In tegenstelling tot traditionele *brute-force*-aanvallen, die zich richten op het uitproberen van een groot aantal wachtwoorden tegen één gebruikersnaam, houdt *password spraying* in dat een beperkte set wachtwoorden (vaak zwakke of gemakkelijk te raden wachtwoorden) worden uitgeprobeerd bij meerdere gebruikersnamen. In sommige gevallen voert een actor *password spraying*-aanvallen uit in een zeer laag tempo van slechts enkele inlogpogingen per uur.

Mitigatie en aanbevelingen:

Organisaties kunnen een aanval detecteren door de logbestanden van de applicatie-, netwerk- of cloudomgeving te controleren op een relatief hoog aantal mislukte inlogpogingen voor meerdere accounts. Omdat deze inlogpogingen vanaf verschillende IP-adressen worden uitgevoerd is het verstandig om detectielogica te ontwikkelen die meerdere foutieve inlogpogingen in een vooraf gedefinieerd tijdframe opmerkt. De grootte van dit tijdframe is afhankelijk van het normale verkeer binnen de organisatie. Traditionele detectie op basis van IP-locatie is vaak ineffectief wegens het gebruik van *residential proxies*[7]. De volgende maatregelen kunnen aanvullende bescherming bieden tegen *password spraying*-aanvallen.

- **Authenticatielogs** Monitor authenticatielogs op mislukte aanmeldpogingen bij systemen en applicaties van geldige accounts.

- **Monitor de inlogpogingen** op regelmatige basis en implementeer beveiligingstools die verdachte patronen kunnen detecteren, zoals snel achter elkaar geplaatste inlogpogingen vanaf één IP-adres.

- **Verouderde accounts** Schakel verouderde of inactieve gebruikers-en beheeraccounts uit. Actoren richten zich op dergelijke accounts om initiële toegang te verkrijgen.

- **Maximeer aanmeldpogingen** Stel beleid in voor accountvergrendeling na een bepaald aantal mislukte aanmeldpogingen om te voorkomen dat wachtwoorden worden geraden.

- **Multifactorauthenticatie** Gebruik MFA met methoden zoals authenticatorapps en hardwaretokens.

- **Uitsluiten** Blokkeer IP-adressen tijdelijk of permanent waar meerdere inlogpogingen van zijn gedaan.

- **Conditional access** Overweeg om voorwaardelijke toegang (*conditional access)* te implementeren op meer dan alleen de IP-locatie. Door middel van *conditional access* kunnen gebruikers alleen inloggen met valide inloggegevens als ook voldaan wordt aan andere voorwaarden zoals lidmaatschap van bepaalde groepen, apparaatspecificaties en gebruik van bepaalde applicaties. Alleen de IP-locatie gebruiken voor *conditional access* biedt onvoldoende bescherming tegen password spraying. Dit komt doordat cyberactoren kunnen verhullen vanwaar zij inloggen.

- **ID protection** Overweeg gebruik te maken van Microsoft Entra ID Protection of vergelijkbare oplossingen van AWS of Google. Dit soort oplossingen kan uw organisatie helpen bij het detecteren van malafide inlogpogingen.

3.5 Account verkenning (T1087)

Binnen een gecompromitteerde omgeving kunnen cyberactoren systematisch proberen geldige accounts, gebruikersnamen en e-mailadressen te inventariseren. Het verkrijgen van deze informatie stelt actoren in staat om gerichte acties te ondernemen, zoals brute-force aanvallen, spearphishing campagnes en ongeautoriseerde accountovernames.

Diverse technieken worden benut om accountgegevens bloot te leggen, waaronder het misbruik van bestaande beheertools, ingebouwde systeemcommando's en het uitbuiten van configuratie(-fouten) die ongewenste blootstelling van accounts, rollen en rechten veroorzaken.

[7] Een residential proxy is een type proxyserver dat gebruik maakt van IP-adressen die zijn toegewezen door een echte internetprovider aan een particulier huishouden. Dit betekent dat het IP-adres dat via de proxy wordt gebruikt, eruitziet als een regulier thuisnetwerk, waardoor het moeilijker is om het als een proxy te detecteren.

Cloudomgevingen kunnen bijzonder kwetsbaar zijn, omdat ze vaak interfaces bieden waarmee gebruikerslijsten relatief eenvoudig toegankelijk zijn. Daarnaast kunnen aanvallers op endpoints standaard PowerShell-functionaliteiten en andere opdrachtregeltools inzetten om accounts te identificeren. Ook kunnen e-mailadressen en accountgegevens worden geëxtraheerd door malafide zoekopdrachten uit te voeren op bestanden binnen een geïnfecteerd systeem.

Mitigatie en aanbevelingen:

Voor een effectieve verdediging is een proactieve strategie vereist die zich richt op het minimaliseren van accountdetectierisico's, het monitoren van afwijkend gedrag en het versterken van toegangscontroles. Zo kunnen de onderstaande maatregelen het risico verkleinen:

- **Multifactorauthenticatie** Zorg ervoor dat alle accounts extra authenticatielagen hebben om ongeautoriseerde toegang te voorkomen, zelfs als inloggegevens worden blootgelegd.

- **Least Privilege Access** Beperk gebruikersrechten tot het absolute minimum dat nodig is voor hun functies, zodat aanvallers minder toegang krijgen bij een compromittering.

- **Security Information and Event Management** (SIEM) Implementeer een SIEM-oplossing om inlogpogingen en accountgerelateerd gedrag real-time te monitoren en afwijkingen snel te detecteren.

- **Beperking van accountenumeratie** Configureer systemen en applicaties zo dat accountnamen en e-mailadressen niet worden blootgesteld aan cyberactoren via openbare interfaces of foutmeldingen.

- **Bewustwordings- en trainingprogramma's** Zorg ervoor dat medewerkers phishingpogingen, social engineering en accountmisbruik herkennen en rapporteren.

- **Security audits en misconfiguratiecontroles** Voer periodiek controles uit om ongewenste blootstelling van accounts, permissies en rollen te identificeren en direct te corrigeren.

3.6 E-mail collectie via mail servers (T1114.002)

Actoren kunnen e-mails stelen via externe toegang tot e-mailservers of cloudgebaseerde e-mailplatforms zoals Microsoft Exchange Online (Office 365). Cyberactoren maken doorgaans gebruik van gestolen inloggegevens, toegangstokens of ongeautoriseerde API-toegang om directe toegang te krijgen tot inboxen en e-mailarchieven.

Dit type aanval kan bijzonder schadelijk zijn voor een organisatie, aangezien e-mails vaak gevoelige bedrijfsinformatie bevatten. Bovendien worden cyberactoren steeds geavanceerder in het filteren en automatiseren van hun zoekopdrachten binnen e-mailomgevingen om snel relevante gegevens te verzamelen.

Mitigatie en aanbevelingen:

- **Multifactorauthenticatie** Vereis MFA voor toegang tot e-mailplatforms, met voorkeur voor hardware- of applicatiegebaseerde methoden in plaats van SMS.

- **Toegangslimieten** Controleer en beperk API-toegang en maak gebruik van contextgevoelige toegangscontroles.

- **Detectie van anomalieën** Implementeer monitoringtools die ongebruikelijke inlogpogingen en dataverkeer detecteren.

- **Bewustwordings- en trainingprogramma's** Zorg ervoor dat medewerkers phishingpogingen herkennen en dat toegangscodes regelmatig worden vernieuwd.

- **Encryptie en DLP** Beveilig gevoelige e-mails met encryptie en *Data Loss Prevention* (DLP)-beleid.

3.7 Proxy (T1090)

Actoren maken gebruik van verbindingsproxy's om netwerkverkeer om te leiden en indirect te communiceren met command-and-control-servers (C2-servers). Dit helpt om directe verbindingen met de eigen infrastructuur te vermijden en detectie te compliceren. Deze strategieën worden ingezet om de controle over command-and-control-communicatie (C2-communicatie) te behouden, het aantal zichtbare uitgaande netwerkverbindingen te beperken, veerkracht te bieden bij netwerkstoringen en het vertrouwen in bestaande communicatiepaden te benutten om verdachte activiteiten te maskeren.

Daarnaast maken actoren vaak gebruik van meerdere gekoppelde proxy's (multi-hop proxy) om hun activiteiten verder te verhullen. Ook maken zij soms misbruik van routeringsmechanismen binnen Content Delivery Networks (CDN's) om C2-verkeer te maskeren en via vertrouwde routes te laten verlopen.

Mitigatie en aanbevelingen:

- **Netwerksegmentatie** Zorg ervoor dat gevoelige systemen en netwerken gescheiden zijn van minder vertrouwde omgevingen. Dit beperkt de bewegingsvrijheid van cyberactoren.

- **Firewallregels en toegangscontrole** Stel strikte regels in om ongeautoriseerde proxy- en poortomleidingsverkeer te blokkeren. Gebruik toegangscontrolelijsten (*Access Control List*—ACL's) om verkeer te beperken tot alleen vertrouwde bronnen.

- **Detectie van afwijkend netwerkverkeer** Gebruik *intrusion detection/prevention systems* (IDS/IPS) en netwerkmonitoringtools om afwijkend verkeer te identificeren, zoals ongebruikelijke verbindingen of meerdere proxy-hopketens.

- **Versleuteling en authenticatie** Implementeer sterke versleuteling en authenticatie voor netwerkcommunicatie om te voorkomen dat cyberactoren verkeer onderscheppen.

- **Content Delivery Network monitoring** Monitor het verkeer dat via CDN's verloopt om misbruik door cyberactoren te detecteren.

- **Loganalyse en monitoring** Analyseer netwerk- en systeemlogboeken om verdachte activiteiten te identificeren, zoals pogingen om proxytools te gebruiken.

- **Beperking van externe tools** Beperk het gebruik van niet-goedgekeurde software en tools binnen de organisatie om te voorkomen dat cyberactoren proxytools gebruiken.

3.8 Exfiltratie via alternatieve protocollen (non-C2 protocol) (T1048.003)

Actoren kunnen gegevens stelen door deze te exfiltreren via een niet-versleuteld netwerkprotocol dat verschilt van het bestaande *command-and-control*-kanaal. De gestolen gegevens kunnen ook worden verzonden naar een alternatieve netwerkbestemming die niet overeenkomt met de hoofd-*command-and-control*-server (c2-server).

De actor kan ervoor kiezen om deze gegevens te verhullen zonder gebruik te maken van versleuteling, binnen netwerkprotocollen die van nature niet-versleuteld zijn (zoals HTTP, FTP of DNS). Dit kan onder andere door gebruik te maken van op maat gemaakte of openbaar beschikbare codering- en compressie-algoritmen (zoals base64), of door gegevens in te bedden in protocolheaders en -velden.

Mitigatie en aanbevelingen:

- **Netwerkmonitoring en -analyse** Implementeer geavanceerde netwerkmonitoringtools die in staat zijn om ongebruikelijke netwerkactiviteit te detecteren, inclusief het gebruik van ongewone protocollen of poorten voor datatransfers. Deze tools kunnen *machine learning*-algoritmen gebruiken om normale netwerkactiviteit te leren en afwijkingen hierin te signaleren.

- **Protocolbeperking** Beperk de toegang tot niet-essentiële protocollen en poorten op het netwerk. Door alleen de strikt noodzakelijke protocollen toe te staan, wordt het aanvalsoppervlak verkleind voor aanvallers die alternatieve protocollen willen gebruiken.

- **Gegevensverliespreventie** Implementeer DLP-oplossingen om gevoelige data te identificeren en te voorkomen dat deze ongeoorloofd het netwerk verlaat. DLP-systemen kunnen zijn geconfigureerd om specifieke soorten gevoelige informatie te detecteren, zoals creditcardnummers of persoonlijk identificeerbare informatie (PII), en alarm te slaan wanneer dergelijke data via ongebruikelijke kanalen wordt getransporteerd.

- **Encryptie** Zorg ervoor dat alle gevoelige data die over het netwerk wordt verzonden, goed is versleuteld. Dit maakt het moeilijker voor aanvallers om de geëxfiltreerde data te gebruiken, zelfs als ze erin slagen deze te verzenden.