Operatie POSITRON aflevering 6 – Control Panel

ANOUK

Da's een hele lastige afweging, want als ze hun malware veranderen, dan kunnen wij ze dus ook niet meer onderscheppen als die actor weer aanvallen gaat uitvoeren op die sector in Nederland.

LIESBETH

Wat me blijft verbazen, is dat het allemaal een gevecht is tegen een onzichtbare tegenstander op een onzichtbaar strijdtoneel. Op dit moment zitten misschien ergens ter wereld vijf mannen te bedenken hoe groot de kans is dat er in mijn MacBook informatie te vinden is over de werkelijke identiteit van hacker David. Kan het zo zijn dat ik ooit naast zo iemand heb gezeten in een vliegtuig of aan een bar ergens in de wereld? Ik zou zo graag willen weten wie er aan de andere kant op zijn toetsenbord zit te rammen. En het lijkt mij heel lastig dat werken bij de AIVD betekent dat die vraag maar zelden wordt ingelost. Ook al zijn de vermoedens nog zo sterk.

FANNEKE

Welke landen zouden er überhaupt baat bij hebben om de infrastructuur in Nederland of andere Europese landen aan te vallen?

LIESBETH

Mijn naam is Liesbeth Rasker. Dit is aflevering 6 van de podcast van de AIVD. Welkom bij De Dienst. Vandaag is mijn laatste dag, ik krijg te horen of de hack is gelukt, of we in de server zitten en of daar iets te vinden was. Ik loop meteen naar de kamer van Tom.

TOM

Laatste berichtje van de hacker. Om drie uur 's nachts exact. En er stond gewoon: succes. We zijn binnen.

LIESBETH

Het is gelukt.

TOM

Het is absoluut gelukt.

LIESBETH

En wat heeft ie dan gevonden?

TOM

Nou, laten we gewoon voor de grap even zeggen hoe het gegaan is, want het is gewoon een mooi verhaal. Dus we hadden dat dat gesloten verkeer tussen Pannenkoeken Palazzo en die tweede laag C2 server en die hebben we toen weten te ontsleutelen met die sleutel. Ja, nou, daar zat gewoon de crux in. Dat bleek een of ander zelfgemaakt protocolletje te zijn van een van de hackers zelf. Nou, vol met obvious gaten, dus door daar misbruik van te maken, is ie naar binnen kunnen gaan.

LIESBETH

Oké, dus prutswerk als ik het zo hoor.

TOM

Dat was niet heel goed, moeten we zeggen. Nee. Een kleine lichte teleurstelling daar toch wel. Maar uiteindelijk telt gewoon resultaat voor ons. En dat was gewoon dat we binnen zaten op hun tweede laag C2 server. Daar draaide gewoon het dashboardje waarmee ze al hun implants bij alle slachtoffers aanstuurden.

LIESBETH

En hoe ziet dat er nou uit? Wat voor een informatie kun je daar dan vanaf halen?

TOM

Ja, je moet je voorstellen, het is gewoon een webappje. Je hebt gewoon letterlijk een lijst met alle implants die ze hebben draaien en ook waar die dan draaien. Dus je zag bijvoorbeeld twee implants bij Elektron BV. Er stond wel bij: niet actief. Ja, dus wat stond er...Volgens mij stond er: last beacon een hele tijd geleden. Dus die hebben we inderdaad allemaal kunnen vinden.

LIESBETH

Ja, geeft dat dan ook meer informatie over wie de potentiële actor is?

TOM

Mogelijk. Mogelijk. Ik had natuurlijk stiekem gehoopt dat het controler panel in een of andere duidelijk te herkennen taal gemaakt zou zijn. Helaas was alles gewoon in het Engels, maar er zaten her en der wat zinsconstructies waar ik toch een beetje aan twijfel.

LIESBETH

Precies, want hebben jullie dan ook een soort van taalspecialisten die kunnen kijken: o, deze grammaticastructuur is kenmerkend voor die en die...

TOM

Zeker. Die hebben we absoluut. Dus ik zou ook echt willen voorstellen: daar moet ook wel even een linguïst naar gaan kijken. Of we daar misschien nog iets uit kunnen halen. Het zijn wel dat soort kleine stukjes, kleine brokjes, waar we wat mee moeten gaan doen. Maar er stonden ook beacons bij andere energiebedrijven, in het buitenland. En dat brengt wel een nieuwe wending en een stukje nieuwe dynamiek aan deze casus.

LIESBETH

Want?

TOM

Het ging om grote energiebedrijven in Duitsland. Ja, en dan komt bij ons toch wel het vermoeden op dat het wel belangrijk gaat zijn om contact op te nemen met de Duitsers. Maar dat moeten we doen in strikte samenwerking met de afdeling buitenlandse relaties.

LIESBETH

Ja, want dat zijn toch ook weer gevoelige dingen waarschijnlijk.

TOM

Zeker. Ja, er hangen ook heel veel wetgevingen vast, maar daar is het goed om het over te hebben met iemand van de afdeling zelf.

LIESBETH

Dus waar we eerst enkel te maken hadden met één implant, bleken dat er twee en waar we eerst alleen zicht hadden op Elektron in Nederland weten we dankzij het hacken van de server dat er ook buitenlandse slachtoffers zijn. In Duitsland. Zodra het speelveld zich buiten onze landsgrenzen begeeft, komen er tal van diplomatieke gevoeligheden in het spel. En om die allemaal goed te navigeren, is er de afdeling buitenlandse relaties?

FANNEKE

Ja, hoi Liesbeth.

LIESBETH

Dit is Fanneke en zij werkt bij buitenlandse relaties.

FANNEKE

Ja, dat klopt inderdaad. Ja.

LIESBETH

Vertel. Wat doet de afdeling en wat doe jij?

FANNEKE

Eigenlijk adviseren wij en begeleiden wij alle teams en hun contacten met het buitenland.

LIESBETH

En waarom is hier een hele aparte afdeling voor?

FANNEKE

Omdat we het eigenlijk heel erg belangrijk vinden om met heel veel landen samen te werken omdat we eigenlijk niet weten waar dreigingen vandaan komen. En bovendien, het ene land is sterker in het ene onderwerp dan het andere land.

LIESBETH

En waar is Nederland bijvoorbeeld sterker in?

FANNEKE

Nederland is heel erg sterk op cybergebied.

LIESBETH

Ja?

FANNEKE

Jazeker. Ja, ja.

LIESBETH

Jij gebruikt als ongeveer een van de weinigen die ik deze stage heb gesproken haar eigen naam. Klopt het dan ook dat het bij jou minder supergeheim is dat je hier werkt? Of...

FANNEKE

Het is minder supergeheim, ja. Want je komt natuurlijk heel veel mensen tegen. Je reist ook met bijvoorbeeld onze directeur-generaal Erik Akerboom. Die is toch nog wel eens op tv. En dus, nou ja, je zou herkend kunnen worden. Dus op het moment dat je een operationele functie ambieert, dan is dit misschien niet de beste keus.

LIESBETH

Niet de goede plek om te beginnen, nee. Focus jij je op specifieke landen en een andere collega van jou weer op andere landen? Of...

FANNEKE

Ja, want we hebben echt heel veel relaties in het buitenland. Nou ja, zoals je weet, zijn er in Europa al heel erg veel landen, maar daarbuiten ook. Dus ja, wij hebben het opgedeeld in accounts.

LIESBETH

Welk land doe jij?

FANNEKE

Ik doe Denemarken en andere Scandinavische diensten. Ja, en nog een aantal andere. Als je de taal spreekt, dan is het wel heel handig. Maar in principe, ja, als je er affiniteit mee hebt, dan is dat wel heel fijn.

LIESBETH

Als ik denk aan het soort onderzoeken dat hier wordt uitgevoerd, kan ik me zo voorstellen dat het regelmatig voorkomt dat de gesprekken die ze heeft niet altijd makkelijk zijn.

FANNEKE

Soms moet je ook een nare boodschap brengen.

LIESBETH

En hoe doe je dat?

FANNEKE

Diplomatiek proberen om toch die relatie ook te houden, zorgen dat je op termijn toch verder kan werken samen en vooral ook focussen op de goeie dingen.

LIESBETH

Wanneer je te maken hebt met andere landen, kom je ook automatisch in aanraking met andere culturen, andere wetten, andere normen en waarden. En soms staan die heel ver af van hoe we het hier Nederland gewend zijn. Hoe pakt ze dat aan?

FANNEKE

Daarover ga je met een team in gesprek. Dan wijs je ze op gevoeligheden wat inderdaad wel en niet kan. En dan probeer je op die manier toch de samenwerking vorm te geven. En als blijkt dat het toch te lastig is, dan moet je overwegen om die gegevens niet te delen.

LIESBETH

Werken jullie met alle landen samen?

FANNEKE

Nee, maar het zou wel tot de mogelijkheden moeten kunnen behoren, zeg maar. We sluiten niks uit.

LIESBETH

Nee, maar het zou wel tot de mogelijkheden moeten kunnen behoren. Een prachtig diplomatiek antwoord. Dan de case die van een spionagezaak veranderde in een sabotagezaak met nu al slachtoffers in Duitsland en wie weet waar nog meer. Dat zijn ook dingen waarover jullie landen moeten inlichten, lijkt me.

FANNEKE

Ja, het is zo dat BR de teams begeleidt. Dus de specialisten zitten bij de teams, dus daar zit kennis van het onderzoek. Dus wij helpen de teams dan in het contact met het betreffende land.

LIESBETH

Je kunt je voorstellen dat er met het ene land intensiever wordt samengewerkt en meer informatie wordt gedeeld dan met het andere. En daar zitten de volgende overwegingen achter.

FANNEKE

Dan heb je het bijvoorbeeld over: wat is de wettelijke basis voor een dienst om te werken? En hoe wordt daar toezicht op gehouden? Heeft een land, zeg maar, mensenrechtenverdragen getekend en houden ze zich daaraan? Hoe gaan ze om met gegevensbescherming? Hè, dus slaan ze ze op? Vernietigen ze ook gegevens? Dus dat soort zaken, die nemen we mee, zeg maar, in wegingsnotities zoals we dat noemen.

LIESBETH

Wegingsnotities.

FANNEKE

Dus daar doen we onderzoek naar. Op basis daarvan wordt de maat van samenwerking eigenlijk vastgesteld.

LIESBETH

En ik kan me ook voorstellen dat dat iets is wat verandert gedurende het jaar, maar misschien ook wel bij sommige landen in een week.

FANNEKE

Ja, als hun politieke situatie wijzigt, ja, dan gaan we de wegingsnotitie wel aanpassen.

LIESBETH

Ja, precies.

FANNEKE

Dus dat kan wel consequenties hebben. Ja.

LIESBETH

Ik kan me voorstellen dat zeker dat stuk met alle functies binnen de dienst, maar zeker ook met jouw functie, dat er een heel groot belang is bij het vertrouwen, bij het wederzijds vertrouwen van degene met wie jij werkt, die in het andere land zitten met je relaties. En als we het over geheime diensten hebben. Ik bedoel, een groot deel van wat jullie doen, moet ook vooral geheim blijven, ook voor andere landen. Dat zal best een moeilijke balans zijn misschien ook soms.

FANNEKE

Ja, dat is een beetje aftasten. En hoe doe je dat? Je begint eigenlijk heel veilig van: dit is ons probleem. Dat is niet direct jouw probleem, maar hoe kunnen we elkaar vinden? En dan zo langzamerhand moet dat vertrouwen opgebouwd worden. Je gaat heel algemeen vragen stellen aan je partner. Van: goh, heb je hier informatie over? Heb je hier interesse in? En dan probeer je dat uit te bouwen.

LIESBETH

Hoe informeel kan zoiets worden?

FANNEKE

Het kan behoorlijk informeel worden, maar er is wel de nodige afstand. Dus het blijft beperkt tot het hoofdkantoor en een etentje, maar geen privébezoeken. Elke mogelijke schijn van belangenverstrengeling moet je tegengaan.

LIESBETH

Is het weleens gebeurd dat dat vertrouwen is beschaamd?

FANNEKE

Ja, dat gebeurt. Ja, dat gebeurt weleens.

LIESBETH

We pakken onze zaak Operatie Positron er weer eventjes bij. Wat gaat daar nu gebeuren? Mag ik zelf een bericht sturen naar de Duitse dienst? Of doet Fanneke dat?

FANNEKE

Jullie mogen zelf delen met de Duitsers. En dan kunnen we samen toetsen van: nou, wat kan wel gedeeld worden? Wat kan niet gedeeld worden? Maar over het algemeen is de samenwerking met de Duitsers zo goed dat het wel oké is.

LIESBETH

Oké.

FANNEKE

De Duitsers voldoen aan al die criteria die we hebben gesteld, dus die zijn allemaal... Dat is allemaal in orde.

LIESBETH

De criteria die in de wegingsnotities staan dus, zoals zojuist besproken. Tot slot ben ik benieuwd hoe vaak er nou eigenlijk contact is tussen de diensten.

FANNEKE

In het geval van de Duitsers is dat mogelijk een paar keer per dag.

LIESBETH

Een paar keer per dag?

FANNEKE

Ja, ja, we werken op verschillende onderwerpen samen. En met verschillende teams. Dus ja, dus dat is verschillende keren, ja.

LIESBETH

En een van die keren zullen wij nu zijn. Zoals Fanneke al aangaf, moet ik met mijn analist bespreken wat we precies willen overdragen. Dus ik klop weer aan bij Anouk. Anouk!

ANOUK

Hai, daar ben je weer.

LIESBETH

Ja, ik heb met je collega gepraat van de afdeling buitenlandse relaties en zij heeft me aangeraden om met jou te gaan bespreken wat we de Duitsers gaan vertellen over het feit dat ook bedrijven in hun land zijn aangevallen door deze malware.

ANOUK

Ja, klopt. Eigenlijk is dat best een complicerende factor wat er uit die hack is gekomen. Er zijn namelijk meerdere energieleveranciers in Duitsland geraakt. Natuurlijk vinden wij dat aan de ene kant heel vervelend voor de Duitsers. Duitsland is een bondgenoot van ons en wij vinden het heel onwenselijk als een vijandige staat het licht uit zou doen bij een bondgenoot. Maar er is nog wel een reden die direct te maken heeft met het veilig houden van de BV Nederland waarom ik die informatie met ze zou willen delen. En dat is omdat het energienetwerk in Europa best wel met elkaar verbonden is en een aanval in Duitsland, op een energieleverancier in Duitsland, cascade- effecten kan hebben.

LIESBETH

Een cascade-effect is een kettingreactie en dat maakt het dus een dubbele reden om de Duitsers in te lichten. Anouk heeft verder navraag gedaan en het blijkt dat één van de slachtoffers een Duitse vestiging is van Elektron. Dus we gaan vragen of Elektron Nederland contact op kan nemen met hun Duitse collega's. En wij gaan dan de Duitse dienst op de hoogte stellen. Maar je vertelt ze wel gewoon alles.

ANOUK

In het geval van de Duitsers kunnen we redelijk open zijn. Wij zullen niet... zeker als het hier gaat om het veilig houden van hun eigen vitale sector, zullen wij niet terughoudend zijn in het delen van informatie. Wat wel zo is, is dat we natuurlijk altijd onze bron zullen proberen te beschermen.

LIESBETH

Wie is eigenlijk de bron in dit geval?

ANOUK

De hack.

LIESBETH

De hack? Dat zou je... Oké, je zou dus niet zeggen dat het door een hack verkregen is, bedoel je?

ANOUK

Nou ja, in theorie is het natuurlijk ook zo dat als wij heel veel informatie delen, dat zij zelf ook kunnen gaan rechercheren. Want zij willen ook weten wie er achter de aanval zit. En als zij ook bijvoorbeeld deze zelfde server zouden hacken, dan kan dat ons onderzoek wel schaden. Onze operatie die wij daar hebben lopen.

LIESBETH

Omdat jullie allebei tegelijkertijd op dezelfde...

ANOUK

Maar ja, als er twee inbrekers door een huis lopen, is er natuurlijk een grotere kans dat ze betrapt worden. Als de een herrie maakt, is de andere er ook bij, zeg maar. Maar er zit nog een andere kant aan. Die cascade-effecten wat ik zei, binnen Europa, die kunnen natuurlijk ook vanuit andere landen optreden. Dus eigenlijk zouden wij in het kader van bondgenootschap meerdere landen binnen de EU willen waarschuwen hiervoor.

LIESBETH

Dat deze malware bestaat.

ANOUK

Dat deze malware bestaat en dat ze moeten zorgen dat al hun energieleveranciers hun detectiemateriaal moeten verrijken met deze technische kenmerken, zodat ze een aanval kunnen voorkomen.

LIESBETH

Maar zoals je inmiddels wel kunt indenken, is het delen van informatie voor een geheime dienst nooit zonder mitsen en maren.

ANOUK

Er zit wel een andere kant aan, want op het moment dat wij al die informatie met alle landen delen en zij zorgen allemaal dat die aanvallen nergens meer binnenkomen, dan alerteert dat ook een aanvaller. En dan zal die naar alle waarschijnlijkheid z'n malware gaan aanpassen.

LIESBETH

Ja, maar als je het niet doet, dan gaat die malware dus door met waar ie mee bezig was.

ANOUK

Ja, maar niet in Nederland.

LIESBETH

Ja, maar wel bij de EU. Die ook weer bondgenoten zijn, kunnen zijn.

ANOUK

Da's een hele lastige afweging. Want als ze hun malware veranderen, dan kunnen wij ze dus ook niet meer onderscheppen als die actor weer aanvallen gaat uitvoeren op die sector in Nederland.

LIESBETH

En we kunnen dat bolletje wol niet verder ontrafelen terug naar de actor, omdat ze er sowieso helemaal mee zullen stoppen.

ANOUK

Aan de ene kant zullen ze de malware gaan veranderen, maar aan de andere kant zullen ze misschien denken: ja, we zijn helemaal aangebrand. Laten we ook gewoon andere infrastructuur, andere aanvalsinfrastructuur gaan gebruiken. Dus die hack die wij hebben op die server, die wordt dan compleet nutteloos.

LIESBETH

Ja, dus dan ben je al het zicht kwijt.

ANOUK

Ja, dus dan hebben we zowel qua weerbaarheid... zijn we minder stevig omdat er andere malware gebruikt kan worden, maar ook in onze operatie, is onze operatie aangebrand.

LIESBETH

De dienst deelt haar inlichtingen dus niet zomaar. Een manier om de bondgenoten toch op de hoogte te stellen zonder de bron, dus de hack, prijs te geven, is door de inlichtingen wit te wassen. Een manier om dat te doen is het NCSC erbij te betrekken. Het Nationaal Cyber Security Centrum. Anouk legt het verder uit.

ANOUK

Omdat wij dus liever niet onze inlichtingen zomaar in het buitenland neer willen leggen, omdat dat kwetsbaar is, omdat we niet willen dat iedereen weet wat onze bron is. Dus we willen die inlichtingen witwassen, zorgen dat onze bron beschermd is. Dat je uit de technische kenmerken die wij delen uiteindelijk... Het feit dat dat van ons vandaan komt, lijkt ook al heel snel, hè, van: hé, dit zijn inlichtingen. We willen eigenlijk niet dat ze dat weten en een manier om dat in dit geval wit te wassen, is door ons NCSC te vragen of zij met hun partners... Dan kunnen zij natuurlijk ook delen van: 'goh, we hebben een aanval gezien in Nederland', alsof de informatie bij hen vandaan komt, alsof zij die van Elektron BV hebben gekregen.

LIESBETH

Zij krijgen informatie van allerlei verschillende partijen.

FANNEKE

Ja, als er incidenten zijn in Nederland of in het buitenland, dan delen de NCSC's van die landen die informatie met elkaar.

LIESBETH

Dus wat zij naar buiten brengen, is in die zin neutraal. Het kan van een geheime dienst komen, het kan ook van een particulier bedrijf komen of het kan van een extern onderzoek komen.

ANOUK

Ja.

LIESBETH

Ah, oké. Wat slim.

ANOUK

Ja.

LIESBETH

Op dit punt in de zaak, hoe groot acht jij eigenlijk de kans dat die actor daadwerkelijk bekend gaat worden?

ANOUK

Ik acht dat wel... Ik acht het aannemelijk dat we een beeld gaan hebben welke partij het is.

LIESBETH

Ja?

ANOUK

Ja.

LIESBETH

Op basis waarvan denk je dat?

ANOUK

Nou, ik hoop eigenlijk dat we nog wel de kans hebben om iets verder onderzoek te doen. Dus dat het niet zo snel de operatie aangebrand is dat we niet meer verder kunnen. En ja, zoals er natuurlijk al eerder gezegd is: hackers laten handtekeningen achter. Infrastructuur zegt iets. Weet je, welke infrastructuur gebruikt is. Slachtoffers, welke slachtoffers gekozen worden. En daar kun je vaak ook wel uithalen wat de achterliggende intentie is. Welke landen zouden er überhaupt baat bij hebben om de infrastructuur in Nederland of andere Europese landen aan te vallen? Ja, wie wil er een dusdanige maatschappelijke ontwrichting in ons land of omliggende landen bewerkstelligen?

LIESBETH

Ja, oké, dan zou er een indruk kunnen komen. En dan?

ANOUK

En dan niet zo veel.

LIESBETH

Nee?

ANOUK

Nee, het is niet zo dat wij rechtszaken aanspannen tegen de personen die daadwerkelijk achter de knoppen zitten.

LIESBETH

Nee, dat snap ik. Maar het resultaat is dus inderdaad dat je dan die beveiliging op die plekken nog beter omhoog gooit, eventueel diplomatieke consequenties.

ANOUK

Ja, daar moet je aan denken.

LIESBETH

Ja.

LIESBETH

Diplomatieke consequenties dus. Dat zou een eindpunt kunnen worden van deze zaak, die weliswaar voor nu ten einde loopt, maar dat zeer zeker nog niet is. Voor mijn laatste gesprek neem ik weer plaats tegenover Tom.

TOM

De Duitsers zijn gebeld. We hebben de technische details nog even na getelext, dus ik hoop dat ze aan de slag kunnen om gewoon bij hen hetzelfde doen als wij ook gedaan hebben en de boel weg te halen. Want daar kunnen we onszelf wel een klein schouderklopje geven, want we hebben wel gewoon, de acute dreiging is in Nederland weggehaald.

LIESBETH

Ja, die dubbele malware bij Elektron, die is eruit.

TOM

Die is weg. En we hebben ook verder geen verdere sporen aangetroffen van nog meer backdoors.

LIESBETH

Maar dat weet je in principe nog niet.

TOM

Nee, dat is natuurlijk nooit honderd procent zeker. We hebben niks meer gezien. Ik weet dat de commerciële partij ook nog niks gezien heeft.

LIESBETH

De commerciële partij die zij hadden ingehuurd om die eerste weg te halen.

TOM

Dus ik hoop dat het inderdaad zo blijft en dat we niks meer gaan vinden.

LIESBETH

Maar ik begreep al van Anouk: Daarmee is dit nog niet afgerond, het onderzoek an sich, want de bol wol is er nog niet.

TOM

Nee, zeker niet. De bol wol is absoluut nog niet volledig ontrafeld. Het was natuurlijk zo dat we deze groep al 12 maanden niet gevolgd hadden. En nu hebben we dus dit incident gehad. Dus dat onderzoek gaat nu, ja, ik wil niet zeggen beginnen, maar we gaan wel echt heel erg veel verder nu. Kijk, ik kan het een beetje... maar wat we nu gedaan hebben en waar we nu staan... Je zou het een beetje kunnen visualiseren als je je een stamboom inbeeldt waarbij we eigenlijk dus helemaal onderaan, dus bij de nieuwste generatie zijn we als het ware begonnen.

Dat was Elektron, de hack daar. En als je dan naar boven zou kijken, dan zie je eigenlijk maar één link en dat is gewoon naar jou, naar jouw ouder of naar je ouders. En dat was wat wij gezien hadden, want wij zagen die link met die C2-server van pannenkoekenpalazzo.nl. En als je dan weer één generatie verdergaat, dat deden wij ook, we hebben toen die tweede laag aan C2-servers ontdekt. En dan wat we nu zouden willen, is zeg maar nog een generatie omhoog, zodat je als je dan naar achter kijkt, dan zie je al die nieuwe generaties onder je als een soort van boom verschijnen. Want op de heenweg zagen we steeds maar één pad. We zien steeds het pad voorwaarts, stapje voor stapje dichter bij de hackers. Maar als je achterom kijkt, eigenlijk hebben we superveel gezien, we zagen de hack bij Elektron. Er zijn wat stappen genomen en nu zien we dat de hacks wereldwijd zitten. We hebben de Duitsers kunnen helpen, dus we hebben nu al veel meer inzicht in wat er eigenlijk gaande is in deze hele campagne. En dat proces gaan we gewoon voortzetten, want ik merk aan jou en aan mezelf dat ik heel geïrriteerd worden van het feit dat ik nog steeds niet weet wie dit gedaan heeft.

LIESBETH

recies, dus los van het technisch onderzoek. Want we moeten gewoon verder op die stamboom en dus ook op die server keten.

TOM

Zeker.

LIESBETH

Wat zijn andere manier om erachter te komen wie dit is? Ga je bijvoorbeeld vergelijken met andere zaken? Hoe zou jij dit aanpakken als bewerker?

TOM

Ja, absoluut. Dus ik ga op zoek naar parallellen met dingen die ik eerder gezien heb. Dus we hebben nu direct de targeting met een vrij, nou ja, overtuigend sabotageoogmerk nu op een energie-industrie. Het allereerste wat we gaan doen, is gewoon gaan kijken: Waar hebben we dit eerder gezien? Weet je, welke groepen zijn geïnteresseerd in dit soort hacks? Nou, dan kun je al een heleboel afstrepen. En dan ga je her en der dus inderdaad bewijzen zoeken om die lijst steeds kleiner te maken. En we hadden het er al eerder over gehad. We kunnen kijken naar die management interface van: die is in het Engels geschreven, zeer waarschijnlijk niet de moedertong van de hackers. Dus we gaan eens kijken. Kunnen we daar foutjes, grammaticale fouten in zien die kenmerkend zijn voor voor bepaalde groepen? En het hele technische pad gaat ook verder. Want we zitten nu op die server, CNE-matig, dus gehackt. En zover wij weten, zijn we nog niet ontdekt. En we weten ook: er waren nog actieve slachtoffers aanwezig. Dus de actor gebruikt dat ding nog. Dus we gaan dat gewoon rustig in de gaten houden. En tot nu toe hebben we ze altijd zien inloggen via SSH over Tor, dat is een anonimiseringsnetwerk. Maar misschien maken ze een foutje en vergeten ze Tor aan te zetten en loggen ze een keer per ongeluk direct in. En dan hebben we zeg maar de volgende generatie in de stamboom en de volgende stap in onze kluwen wol die we uit elkaar aan het trekken zijn. Dus uiteindelijk wil ik gewoon op het systeem van de hacker zitten en gewoon precies zien wat ze aan het doen zijn.

LIESBETH

Je zegt inderdaad: ik ga kijken naar vergelijkbare zaken. Ook in jullie jaarverslag staan een aantal landen die jullie in de gaten houden of waar jullie zeker op dit onderwerp extra alert op zijn. Is er iets te zeggen over dat specifieke landen met specifieke dingen bezig zijn? Als in: staat het ene land bekend om dit en het andere land bekend om dat?

TOM

Ja kijk, er zijn grove trends te zien. Ik bedoel, dat China bekendstaat om economische spionage, is geen geheim. En dat is ook op het cyberveld zo. Maar stel, zo'n groep als Rusland, een gigantisch groot land. Ja, het is heel moeilijk om te zeggen dat Rusland één doel heeft.

Want je kunt ook in open bronnen voorbeelden vinden van Russische hackersgroepen die eigenlijk alle drie de hoofdtakken doen. We zien beïnvloeding, we zien spionage en we zien een stukje sabotage. Dus weet je, voor zoiets is het heel moeilijk om te zeggen... Korte antwoord: nee.

LIESBETH

Nee.

TOM

Dat is te algemeen, daar kunnen we het nog niet mee vaststellen.

LIESBETH

Nee. En bovendien als je op een gegeven moment in die server zit van die hacker of je hebt die hacker te pakken, dan weet je nog steeds niet wie die hacker heeft ingeschakeld om dit te doen.

TOM

Nee, dus dan krijg je nog meer... Ja, het is een oneindige boom dit. Je gaat je dan weer afvragen: ja, waar komen dan deze opdrachten vandaan? Weet je, hoe speelt dit beleidswijs in het land waar het dan uiteindelijk om blijkt te gaan?

LIESBETH

Ja, misschien reikt dit te ver, hoor, voor deze zaak en voor deze stage ook. Maar aan het eind van deze stamboom, aan het eind van deze serverketen zit even nu voor het gemak een kamer vol met hackers die deze malware hebben gemaakt en hebben uitgezet. Maar die groep hackers, die bedenkt dat niet zelf. Die hebben ook weer een opdracht gekregen van iemand. Dat kan een ander bedrijf zijn, een statelijke actor. Whatever.

TOM

Waarschijnlijk.

LIESBETH

Dit is een soort hele andere laag van de wereld, zeg maar. Maar dit soort mensen die... Dat is toch nooit helemaal te herleiden dan wie hun die opdracht geeft?

TOM

Nee, nee. Daar komen we uiteindelijk denk ik niet achter. We gaan wel hopelijk, in ieder geval als het aan mij ligt, proberen te achterhalen welk land in ieder geval verantwoordelijk is en misschien ietsspecifieker welke groep. Maar wie de aansturing gegeven heeft en de opdrachten daartoe en de motiveringen erachter... Daar heb ik een hard hoofd in of we daar achter komen.

LIESBETH

Maar ergens is dus die kamer met hackers. Uiteindelijk zijn dat ook gewoon mensen die 's ochtends naar hun werk gaan en 's avonds meestal weer naar huis. Die daar in opdracht van weer iemand anders de malware hebben gecodeerd die wij er nu na diepgravend onderzoek uit hebben gehaald. Zou zo'n hacker nou stilstaan bij de mogelijke gevolgen van zijn of haar werk, van de enorme onrust die dergelijke malware in landen veroorzaakt? Van ziekenhuizen die geen stroom meer hebben? Dat beeld blijft me intrigeren, ook al is het nog zo frustrerend dat we niet te maken hebben met één duidelijke dader die uiteindelijk aangeklaagd zou kunnen worden. Maar voor nu is het belangrijkste gelukt. De hack bij Elektron is opgelost. De treinen blijven rijden, we kunnen nog steeds geld pinnen, 112 blijft bereikbaar, supermarkten blijven bevoorraad en ga zo maar door.

TOM

Ik ben ook wel heel benieuwd eigenlijk, Liesbeth, wat jij nou precies vond van deze toch wel rollercoastertour in het cyberwereldje.

LIESBETH

Nou, dat was het zeker. Inderdaad, ja. Nou, ik moet zeggen dat ik vooraf wel grote zorgen had. Want ik dacht: god, hoe ga ik me nou staande houden in de cyberwereld? De vraag is of dat überhaupt op die manier gelukt is, inderdaad. Maar wat ik geinig vond en wat ik vooraf echt niet had verwacht, is dat het eigenlijk toch op heel vlakken hetzelfde was als vorig jaar. In de zin dat zo'n onderzoek begint met iets wat opvalt.

TOM

Zeker. Ja, absoluut.

LIESBETH

Een nieuwsgierige student of iets in die datastroom, wat dat dan verder is en dat het zich op die manier steeds verder ontvouwt en dat je ook dezelfde vraagstukken af en toe hebt. In hoeverre ga je je positie kenbaar maken? In hoeverre hou je jezelf nog even gedeisd?

TOM

Ja. En het feit misschien dat het uiteindelijk een semi open einde heeft.

LIESBETH

a, ja, precies ja. En nu denk ik nog meer dan vorig jaar. Maar ook zeker toen ik met de hacker, toen David tegenover me zat. Toen dacht ik: ja, datzelfde gevoel had ik een beetje vorig jaar. Hè, van echt dat speuren. Echt dat heimelijke, dat zit hier eigenlijk ook gewoon in. Of niet eigenlijk, maar dat zit hier dus ook in. Dus het lijkt super ver ervan af te staan en dat is het ook. Maar toch ligt het ook dichter bij elkaar dan dat ik aan het begin van deze stage had voorzien. En het is absoluut niets voor mij. Ik heb sowieso niet dat technische niveau, dat zal ik ook nooit meer halen. Maar ik heb ook niet de hacker mindset waar jij het over hebt.

TOM

En die is wel essentieel om te hebben.

LIESBETH

Maar gelukkig voor mij en voor jou heeft Tom die mindset wel. Net als alle anderen die ik hier heb gesproken. En zij blijven deze zaak ook in de gaten houden, want ooit gaat de actor een foutje maken. Computerwerk is immers mensenwerk, zoals we hebben geleerd. En zo worden de sporen bij elkaar verzameld, net zo lang totdat we bovenaan de keten uitkomen. En wie een beetje heeft opgelet de afgelopen afleveringen, weet eigenlijk wel bij welke statelijke actor dat dan waarschijnlijk gaat zijn. En je weet dan dus ook dat die actor nu weliswaar is tegengehouden, maar dat het daar niet bij zal blijven. De dreiging blijft bestaan, voortdurend, ook al kunnen we hem niet zien.

TOM

Ja, ja, die is letterlijk onzichtbaar.

LIESBETH

Ja, en dat maakt het zo dat je denkt: ja, nou ja, het zal toch allemaal wel, het werkt toch allemaal, het licht komt uit... Niks aan de hand. Maar de kwetsbaarheid in die zin ervan is veel minder makkelijk te doorgronden. Als je dat naast een CT-zaak legt, is dat veel duidelijker.

TOM

Absoluut.

LIESBETH

Maar ja, ik vond het fascinerend. Ik heb een hoop geleerd. Ja.

LIESBETH

et zit erop. Mijn tweede stage is voor nu afgerond. Ik loop voor de laatste keer naar de beveiliger van het pand om mijn telefoon uit het kluisje te halen en ik kijk nu toch anders naar dat ding. Naïef als het mag zijn, maar ik heb lang gedacht dat ik niet zoveel te maken had met de cyberwereld. Of beter gezegd, ik stond er gewoon niet zo bij stil. Wat ik in ieder geval meeneem, is dat ik veel secuurder omga met mijn eigen digitale veiligheid. Vanaf nu zal ik elke update die mijn laptop aanbiedt braaf uitvoeren in plaats van hem een week lang weg te klikken. Ik ga een password manager instellen en ik laat mijn laptop nooit meer onbeheerd achter. Dat ik nu ook weet wat SIGINT, beaconnen, een APT en SCADA betekent, is een mooie bijkomstigheid. En voor het grote werk reken ik op David, Pim, Tom, Ellen en alle anderen. Mocht je de hele serie met ons hebben mee gepuzzeld, dan staat er nog een laatste easter egg voor je klaar op operatiepositron.nl. Tenminste, als je hem kunt vinden. Dit was de zesde en laatste aflevering van het tweede seizoen van De Dienst, een podcast van de AIVD, gepresenteerd door mij, Liesbeth Rasker, en geproduceerd door Het Podcast Kantoor in samenwerking met Werk Merk. Wil je meer weten over wat de AIVD doet of zou je het leuk vinden om er te werken? Ga dan naar werkenbijdeaivd.nl.