Operatie POSITRON aflevering 2 – Pim’s heilige uurtje

PIM

Een actor die binnen komt, probeert natuurlijk wel z'n positie te verstevigen. Dus één stukje malware is misschien niet genoeg. Op de malware server kunnen we wel in ieder geval onderkennen dat er waarschijnlijk twee systemen geïnfecteerd zijn.

LIESBETH

Alsof ik nooit anders heb gedaan, pak ik weer de trein naar Leiden en de bus naar Zoetermeer. In de bus kijk ik om me heen en vraag ik me af wie hier nog meer naar de AIVD onderweg is. Je denkt bij een spion al snel aan het tekenfilm beeld van een man in een lange regenjas en een fedora hoed bijna over de ogen. Maar als me iets opviel van vorig jaar, dan was het wel dat alle mensen die tegenover me zaten, heel normale mensen waren. Alleen met niet zulk normaal werk.

ANOUK

Daarom vind ik dit ook best spannend. Dertien jaar lang vertel ik vriend en vijand niet waar ik werk, en nu zit ik hier gewoon een interview te geven. Dus ik denk dat 't nog veel raarder is als ik het straks terug hoor.

LIESBETH

Mijn naam is Liesbeth Rasker. Dit is aflevering 2 van het nieuwe seizoen van de podcast van de AIVD. Welkom bij De Dienst.

TOM

Goeiemorgen Liesbeth.

LIESBETH

Ja, goedemorgen!

TOM

Welkom terug.

LIESBETH

Zit ik weer.

TOM

Ik ben heel benieuwd wat je ervan vond en wat je allemaal te binnengeschoten is.

LIESBETH

Ja, ik vond het echt, uhm... Overweldigend. Dat is toch echt wel het woord. Ik ben ook erg onder de indruk van deze hele wereld waar ik natuurlijk niet echt bewust van was, en nu toch een klein beetje de deksel van is opgelicht. En ik ben heel benieuwd, ja, wat er gaat gebeuren. Dat is natuurlijk voor mij nog steeds lastig in te schatten.

LIESBETH

Even een kleine herhaling van wat er de vorige aflevering is gebeurd. We zijn gestart met een operatie die ze hier bij de AIVD 'Positron' zijn gaan noemen. De malware, met de codenaam Rookworst, waar de AIVD een onderzoek naar had lopen, dook opeens na een hiaat van een jaar weer op. Bij Elektron BV, om precies te zijn één van de grootste energieleveranciers van Nederland.

Dat kan serieuze gevolgen hebben, maar er is nog veel onduidelijk. Wat is het? Waar komt het vandaan? En vooral, wat is het van plan?

TOM

En nu gaan we de details induiken en proberen om erachter komen wat er gebeurd is. En dat is wel waar jij aan bod komt en waar jij het voortouw in mag gaan nemen.

LIESBETH

Ja, daar was ik al bang voor. Ja... Ja.

TOM

Dus bij deze. Wat ga je doen?

LIESBETH

Ja, wat ga ik doen? Uhm, ik weet 't natuurlijk niet precies, maar ik zou in ieder geval... willen weten... Ja, ik zou willen weten wie het zijn.

TOM

Het is een groep die we een jaar geleden nog actief zagen hacken. En we kennen ze al sinds 2018. We hebben nooit goed kunnen vaststellen welk land er achter zit. Maar het was duidelijk één groep dieecht dat dat typische stukje malware gebruikte en ook doelen aanviel in Nederland die heel erg spionage gericht waren. Alleen toen dus dat gat van twaalf maanden.

LIESBETH

Ja.

TOM

Ja, en dat... Dat roept vragen op bij ons. Van, waarom verdwijn je zo'n lange tijd en kom je opeens terug?

LIESBETH

Maar als je dan nu zie dat dat weer actief is. Het is nog helemaal niet gezegd dat het dus ook daadwerkelijk dezelfde groep is. Het lijkt vooralsnog alleen op elkaar.

TOM

Ja, da's een heel goed punt. En ook belangrijk om te vermelden inderdaad. We herkennen de malware die we gezien hebben. We weten dat die twaalf maanden geleden nog werd gebruik door deze groep Zuurkool. Maar ja, de aanname is inderdaad dat zij het nu weer zijn, maar het zou net zo goed iemand kunnen zijn die de malware gestolen heeft en zelf is gaan gebruiken.

LIESBETH

Ja, of die weet dat die malware zo bestaat, dus is dat ie zich verschuilt achter...

TOM

Absoluut.

LIESBETH

De houding... Of hoe noem je dat, de signatuur...

TOM

De M.O, de modus operandi.

LIESBETH

De M.O. van hun. Oké, er is dus zeker het een en ander bekend, maar eigenlijk ook weer helemaal niet.

TOM

Correct. Uiteindelijk moeten we bijna opnieuw beginnen.

LIESBETH

Ik merk dat ik vooral wil weten met 'wie' we hier te maken hebben. Maar omdat überhaupt ooit te weten te komen, moeten we eerst weten met 'wat' we hier te maken hebben. In de basis is dat een stukje malware. Simpel gezegd software die gebruikt wordt om computersystemen te verstoren. Het woord is een samentrekking van malicious software. De malware kan verschillende doelen hebben. Is het bijvoorbeeld uit op spionage? En wat is er nog meer op te maken uit de informatie die er nu is?

TOM

Ik denk dat het verstandig is als je nu gaat praten met de CND analist, die de alert in SIGINT daadwerkelijk heeft waargenomen. Hij zal veel meer details voor je hebben over wat er precies aan de hand is, waar het allemaal gedetecteerd is en wat het betekent. En daarnaast lijkt 't me een goed idee om ook meteen even te gaan praten met onze inlichtingen analist Anouk, omdat zij jou denk ik veel meer kan vertellen over wat de impact is van zo'n hack en ook wel waarom wij hier achteraan willen gaan. Een beetje over de bredere context van wat het betekent voor de veiligheid van Nederland.

LIESBETH

Mijn eerste gesprek is met Pim. Hij heeft samen met zijn collega's van de afdeling CND de malware ontdekt.

PIM

CND staat voor Computer Network Defence.

LIESBETH

Computer Network Defence, ja.

PIM

En wat wij eigenlijk doen is aanvallen waarnemen van statelijke actoren.

LIESBETH

En hoe doe je dat?

PIM

Eigenlijk hebben we daar verschillende middelen voor. Denk aan SIGENT. Denk aan een central netwerk die netwerk verkeer kan opnemen van partijen die we als Nederland proberen te beschermen. En denk aan log analyse, malware analyse, noem maar op.

LIESBETH

Mochten die termen je niet zeggen. Als je het vertaalt naar de inbraak in de villa waar Tom het eerder over had, komt het er op neer dat er verschillende manieren zijn een inbreker tegen te houden of te betrappen. Door een videocamera op te hangen of bewegingssensoren. Of door er gewoon een hek omheen te bouwen. Pim is een echte vakman met gigantische liefde voor zijn werk, die hier via via terecht is gekomen.

PIM

Ik ben een beetje in mijn netwerk gaan rondvragen. En zo kom ik eigenlijk hier terecht.

LIESBETH

En waar werkte je dan?

PIM

Daar ga ik liever niet op.

LIESBETH

Dat kan je niet vertellen.

PIM

Nee, niet voor de podcast in ieder geval.

LIESBETH

Nee.

PIM

Uhm. Wel een informatica opleiding gedaan. Altijd bezighouden met uhm ja, eigenlijk computers. Veiligheid daarvan, interesse daarin gehad. Altijd in verdiept, altijd gespeeld ermee.

LIESBETH

Wat is er zo leuk aan?

PIM

Ik vind vooral de verdedigende kant leuk. Snappen hoe aanvallen werken en snappen wat je daar tegen kan doen. Proberen dat te kunnen onderkennen. Proberen daar op grote schaal mee te werken. Uhm, om zo een stukje veiligheid toe te voegen in plaats van bijvoorbeeld alleen offensief bezig te zijn, of voor één organisatie proberen dat ze beter geld kan verdienen.

LIESBETH

Net als voor veel van zijn collega's die ik vorig jaar sprak, is het ook voor Pim zaak dat niet iedereen weet dat hij hier werkt. Wat overigens ook de reden is dat we zijn stem hebben vervormd en dat hij niet zijn echte naam gebruikt.

PIM

Vrienden, kennissen. Uhm, daar blijf je gewoon altijd toch op je achterhoede wat je kan vertellen. Dus uhm, ja.

LIESBETH

En heb je dan een soort standaard verhaaltje wat je verteld als dat ter sprake komt?

PIM

Zeker.

LIESBETH

Ja, maar in je vrije tijd is het ook een... Het is ook een hobby van je, dit.

PIM

Ja, en dan ben je er ook mee bezig. En je kan natuurlijk altijd met mensen over techniek praten. Maar soms moet je wel achter houden hoe je het weet.

LIESBETH

En is het dan leuk om van je hobby je werk te maken? Of ben je dan ook een beetje je hobby kwijt?

PIM

Ja, er zijn wel grappige internet plaatjes over... Maar uhm... Ergens ben je een beetje je hobby kwijt, maar aan de andere kant maakt het je werk ook heel leuk. Dus 't is een beetje een balans vinden.

LIESBETH

We hebben het in deze case over Rookworst. Het malware. Om te beginnen, een van de dingen waarin je, wat Tom ook al heeft uitgelegd aan me: jullie hebben dit gedetecteerd doordat jullie die SIGINT stroom beoordelen. En daar hebben jullie allemaal methodes voor om daarin dan afwijkende stukjes data te vinden.

PIM

Als jij naar een website gaat ziet jouw verkeer er op een bepaalde manier uit. Zo praat de malware ook op een bepaalde manier. En dat kan je onderzoeken. Dat kan je fingerprinten. Dus denk bijvoorbeeld aan technische kenmerken hoe die communiceert. En die technische kenmerken kan je op detecteren. Hoe vaak vindt dat plaats? Hoe normaal is dat? Is dat legitiem verkeer of is dat niet legitiem verkeer? Uhm, en daar ga je dan eigenlijk onderzoek naar doen. Wat je dan vaak probeert, dus als je bijvoorbeeld een malware analyse rapport krijgt of samenwerkt met een malware analyst. Hoe communiceert de malware zodat je dat kan intercepteren. En daarmee kan je er allemaal weer informatie naar voren krijgen. Wie praat met wie? Is het een aanval server, is het een slachtoffer. Wat vindt er dan plaats? Wat voor soort communicatie is het? Uiteindelijk wat je probeert, is die data gewoon leesbaar te krijgen. Daar zitten allemaal verschillende lagen tussen. Kijk, ergens komt er data binnen. En dat is op een bepaalde manier zodat dat op internet kan communiceren. Dat moet allemaal geabstraheerd worden naar eigenlijk begrijpbare taal, zodat je het kan opslaan en doorzoeken. Uiteindelijk laad je dat dan bijvoorbeeld in een hele grote databank en die kan je dan bevragen.

LIESBETH

Met 'bevragen' wordt bedoeld dat je gaat uitzoeken wat er in die data wordt getoond, bijvoorbeeld met welke andere IP adressen is vanaf dat adres gecommuniceerd? Hoe vaak per dag gebeurde dat? En is die communicatie te verklaren? Of zitten daar misschien afwijkende elementen in.

PIM

Of veel uitgebreider: ik zoek http verkeer, wat een specifieke user agent heeft, die naar een bepaalde URI gaat. Als je op internet communiceert, heb je even een bepaalde browser.

Die heeft een bepaalde versie, daar zitten bijvoorbeeld bepaalde kenmerken in, dat word bijvoorbeeld ookgebruikt door bijvoorbeeld tracking software om mensen identificeren. Maar daarmee kan je best snel onderscheid maken tussen bijvoorbeeld malware en normaal gebruik verkeer. Als je bijvoorbeeld naar een normaal computernetwerk kijkt die beheerd wordt door een beheerder. Als het een goed beheerd netwerk is, dan heeft iedereen dezelfde browserversie. Daarmee kun je eigenlijk al heel snel kijken: hé, dit zijn alle browsers. Maar daarnaast heb je misschien ook nog andere applicaties. Een updater of een stukje malware heeft misschien een andere user agent. Dat verschil kan je waarnemen. Dat kan je analyseren en dan haal je eigenlijk naar voren: 'Hé, wat gebeurt hier? Wat is dit? Wat vindt hier plaats?'

LIESBETH

Goed, dat is de puzzel die Pim moet gaan oplossen. Zo'n onderzoek begint bij een eerste detectie in SIGINT. En dan?

PIM

In dit geval uhm, is dat voor mij altijd m'n, ja, heilige uurtje zeg maar. Dan pak ik even de rust om goed kijken wat er plaatsvindt. Eigenlijk, de meest voorkomende vragen kan ik al voorspellen. Dus die ga ik even uitzoeken om een goed beeld vormen.

LIESBETH

Wat zijn de meest voorkomende vragen?

PIM

Wie is het victim?

TOM

? Kunnen we al op de server? Uhm, wat weten we er nog meer over? Uhm, allemaal eigenlijk standaard dingetjes die ze standaard gaan vragen. Maar dat is bijvoorbeeld ook: wat voor communicatie is het, wat euh... Hoe vaak vindt 't plaats? Zijn eigenlijk allemaal kleine ja, vragen die standaard terugkomen. En daar heb je gewoon even de rust en tijd nodig om te analyseren.

LIESBETH

Wat gebeurt er als jullie gaan rennen?

PIM

Nou, dan... Eigenlijk gewoon snel contact leggen, snel een team vormen. Welke informatie hebben we? Wat weten we? Wat moet gebeuren? CND heeft eigenlijk vooral data waarop ze acteren, maar een inlichting team heeft veel meer informatie over de actor. Wat is normaal? Hoe werkt ie? Uhm, misschien hebben ze wel contact gehad met een partner, wat nog niet in systemen met terug tevinden is. Dat die actor daarbij actief was. Daarmee probeer je uiteindelijk met z'n allen een situationeel beeld te vormen van wat, welke acties moet er gebeuren?

LIESBETH

En het kan ook zo zijn dat jullie zeggen: 'Oh nou, dit stuk malware doet zus, zus en zo'. En dat dan bijvoorbeeld het andere team zegt: 'Oh, dat maakt niets uit, dat wisten we al. Dat is oké.' Die context kunnen zij dan weer schetsen? Of...?

PIM

Vaak wel. Het ligt er dan heel erg aan in welke fase je zit. Dus zit iemand bijvoorbeeld veel meer in de verkenningsfase en is 'ie een beetje tegen de deur aan het trappen, dan hoef je misschien geen actie te ondernemen. Als jij een actief malware ziet die aan het beaconen is, dan...

LIESBETH

Wat is beaconen?

LIESBETH

'Beaconing' is weer zo'n belangrijke term die vaker terug gaat komen. Dit is de communicatie van de malware met zijn afzender. Want inderdaad, een actor, die stuurt die malware op pad zeg maar, in zo'n systeem, om binnen te komen. Maar die geeft ook die malware een soort rugzak met een taak. Namelijk: of haal informatie binnen, of schakel het systeem uit. Even heel globaal gedacht. Dus die malware, die daar dan in zit. die gaat steeds terug communiceren naar waar die vandaan komt met: Nou, dit lukt, of dit is er aan de hand, of dit zie ik, of dit heb ik nu gedaan.

PIM

Klopt.

LIESBETH

En die communicatie die zien jullie.

PIM

In dit geval hebben we die communicatie gezien.

LIESBETH

Precies. Ja, en dan is het zaak om dat uit te schakelen of in de gaten te houden. Of in ieder geval...

PIM

Weten dat het plaatsvindt en reageren. Want ja, vanuit SIGINT weet je dat het plaatsvindt. Maar, dan wil je eigenlijk wel weten wat is er gebeurd. En krijg je eigenlijk de start van een inlichten onderzoek.

LIESBETH

Wat zit er in je rugzak en wie heeft hem op pad gestuurd.

PIM

Ja.

LIESBETH

Dat die Rookworst nu herkend wordt, is omdat 12 maanden geleden al een onderzoek liep en er al een hele hoop voorwerk is gedaan in dit geval. Maar stel, dat was niet zo geweest. Hoe was deze malware dan gevonden? Als die... Als er nog niet duidelijk was dat dit überhaupt bestond?

PIM

Ja, daar zijn heel veel verschillende manieren voor. Dat kan bijvoorbeeld zijn dat we informatie krijgen en op basis van die informatie gaan acteren. Dus of dan...

LIESBETH

Wat voor informatie?

PIM

Denk aan een partner die een berichtje stuurt dat ze een nieuwe malware hebben onderkend. Dat wij ook gaan kijken: hebben wij hier last van? Dat kan informatie zijn omdat we eigenlijk vanuit eigen onderzoek een nieuw onderzoek starten. Maar het kan ook gewoon zo simpel zijn dat een bedrijf een security dienstverlening heeft afgenomen en zelf iets heeft gevonden.

LIESBETH

Er zijn dus meerdere manieren om te ontdekken dat er iets aan de hand is, net zoals dat er meerdere manieren zijn om die malware ergens binnen te krijgen en de aanval uitgevoerd kan worden. Pim legt uit hoe een aanvaller zijn malware in het systeem krijgt.

PIM

Je gaat proberen om op basis van het target te kunnen communiceren. Dus als jij een ministerie wil raken, euh, of bij een ministerie wil binnenkomen, dan helpt het om de taal te spreken. Dan helpt het om te communiceren hoe ze normaal communiceren, om juist zo gericht mogelijk binnen te komen, omdat de kans op klikken veel groter wordt.

LIESBETH

Ja, dus je bedoelt dat bij de groep Zuurkool waarschijnlijk mensen zitten die Nederlands spreken.

PIM

Die bijvoorbeeld Nederlands spreken, of die snappen van: hé, dit is het jargon van dat vakgebied. Dat helpt om te klikken.

LIESBETH

Dit wordt 'phishing' genoemd en daar heb je ongetwijfeld van gehoord. Een aanvaller stuurt jou een mail waarbij het lijkt alsof die van je bank komt, de Belastingdienst of een social media platform dat je gebruikt. En door op die link te klikken haal je ook een stukje malware of ransomware naar binnen. Het zal je verbazen hoe vaak en op welke schaal dit gebeurt. De Belastingdienst alleen al bijvoorbeeld registreerde in 2020 dik 150 duizend meldingen van phishing berichten vanuit hun naam.

LIESBETH

Proberen ze het hier ook wel eens te hacken, het gebouw hier, of het netwerk hier?

PIM

Dat is zeer waarschijnlijk.

LIESBETH

Ja, en dat zien jullie dan ook gebeuren? En dan hoor je ze rammelen aan de poorten en dan denk je: nou dat gaat je mooi niet lukken.

PIM

Je weet nooit of het nooit lukt, maar dat is dan inderdaad onderzoekswaardig, van: wat heeft niet plaatsgevonden en wat gebeurt hier?

LIESBETH

Terug naar de zaak. Pim heeft de malware Rookworst gedetecteerd, een eerste analyse uitgevoerd en komt tot de volgende conclusies:

PIM

Nou, wat ik tot nu toe gezien heb in de data is dat we een victim hebben, Electron, die beacont met een malware server. En het lijken, op de data die we kunnen zien, dat er waarschijnlijk één á twee victims zijn. Dan weet je dat er iets serieus aan de hand is waar je wel op moet acteren.

LIESBETH

1 á 2 victims? We hadden er 1, we hadden Electron. Maar je bedoelt misschien is er nog wel meer? Wat...

PIM

Nou, een actor, als die binnenkomt, probeert natuurlijk wel z'n positie te verstevigen. Dus één stukje malware is misschien niet genoeg. Op de malware server kunnen we wel in ieder geval onderkennen dat er waarschijnlijk twee systemen geïnfecteerd zijn.

LIESBETH

De malware server is dus de server van de aanvaller waar de malware mee 'beacont', waar ie mee communiceert. Want die hacker, die moet wel in contact kunnen staan met zijn malware. Maar dat kan ie natuurlijk niet rechtstreeks doen. Dus tussen de computer van die hacker en die van het slachtoffer zit een hele keten aan servers, aan tussenstops, om zo ongezien mogelijk te werk te kunnen gaan. Zo'n externe server wordt de C2 server genoemd, wat staat voor 'Command & Control'.

PIM

Vaak is er gewoon een... ja een kennis-expert op dit dossier. Dat is eigenlijk de eerste persoon naar wie je toegaat. Die kan ons het meeste vertellen. Ook over serieusheid, is het logisch. Die bepaalt eigenlijk wat we gaan doen. En dan wordt het voor mij iets meer achteroverleunen. Dan is het eigenlijk bijvoorbeeld wachten op informatie. Maar ook al ja, voortborduren. Dan kan ik me eigenlijk een beetje terugtrekken en richten op de analyse. Wat zien we nog meer op die C2 server gebeuren? En welke... Kunnen we andere victims zien? Welke informatiebronnen heb ik nog meer waar ik meerinformatie uit kan halen? We hebben bijvoorbeeld ook een sensor netwerk waar we data uit kunnen halen. Vinden we daar dit... vindt dit daar ook op plaats? Waarschijnlijk niet, want anders hadden we het al geweten. Maar we willen toch nog even kijken van; dit IP adres van de server, wat heeft die nog meer gedaan de afgelopen tijd?

LIESBETH

En jij zit dus de hele tijd te puzzelen met al deze codes met al deze verschillende opties? Met al deze potentiële routes naar het antwoord.

PIM

Ja. Eigenlijk proberen zoveel mogelijk informatie voor het inlichtingenteam te verzamelen vanuit databronnen die we hebben. Zodat er goeie acties ondernomen kunnen worden.

LIESBETH

Waar ik bij het terrorisme onderzoek prima een voorstelling kon maken van wat de AIVD'ers nou daadwerkelijk doen, is dat nu lastiger. Iemand achtervolgen of afluisteren spreekt nou eenmaal een stuk meer tot de verbeelding dan informatie halen uit C2 servers.

PIM

Uhm, waar het eigenlijk op neerkomt is gewoon een taaltje waarin je bepaalde logica kan toepassen. Uiteindelijk is het heel veel logica, maar het begint bijvoorbeeld met...

LIESBETH

Ja, er ligt hier voor mij een A4 en daar staat boven Suricata. En als ik dan een zin zou voorlezen staat er: alert tcp any any streepje pijltje any any flow komma punt server dubbele punt get Mozilla... Nou, echt, voor mij... Dit ziet er een beetje uit als ik mijn voorhoofd op het toetsenbord leg. Dan zou je dit krijgen. Maar jij... Dit is waar jij in zit de hele dag.

PIM

Ja, bijvoorbeeld als je ook kijkt wat eigenlijk dit aangeeft. Dus dat je op op een bepaalde manier verkeer probeert te raadplegen. Uhm, je hebt bijvoorbeeld Mozilla 5.0. Dat is zo'n user agent. Dat is eigenlijk wat je browser bijvoorbeeld standaard mee stuurt. Of de malware. Om daarop te selecteren krijg je eigenlijk een combinatie van dingen. Dus wat hier heel erg plaatsvind is bijvoorbeeld een user agent, hier zit een stukje van de cookie in. Er zijn bijvoorbeeld onderdelen van de HTTP headers die eigenlijk de malware inzichtelijk maken voor ons. Dat je uit die hele grote bak data, hoe kan je nou die malware halen? Nou, als die altijd zo praat kan je dit zo zien. Hier ga je misschien nog bijvangstmee krijgen, 'false positives': iets wat hier op lijkt, maar geen malware is. En er zit een stukje triage en duiding op. Maar uiteindelijk gaat 't gewoon... Ja, je hebt iets van een filter mechanisme nodig om steeds verder in die trechter de juiste informatie te krijgen. En daar is Suricata bijvoorbeeld een van deze dingen van.

LIESBETH

Dit is de manier waarop jullie... hoe die data eruit ziet en waar jij dan in zit te wroeten.

PIM

Dit is eigenlijk een manier om uit die grote bak data naar voor te halen van: hé, waar moet ik even naar kijken? Wat is belangrijk?

LIESBETH

Ja ja, oké.

PIM

Uiteindelijk is het, denk ik, gewoon een beetje professioneel puzzelen. Je hebt informatie, je hebt gesprekken. Je probeert met elkaar hypotheses op te stellen, en die ga je proberen te beantwoorden. Welke databronnen heb je daarvoor nodig en welke actoren zijn er actief?

LIESBETH

En zijn er wel eens zaken geweest waarbij je echt nog s avonds in bed lag te malen en dat je dacht: Hoe kan het nou? Hoe kan het nou, ik snap het niet?

PIM

Of weekenden dat je dan zelf gaat prutsen, om het proberen te reproduceren en te snappen... Natuurlijk blijft dat ja. Het zijn problemen die blijven knagen. Je probeert een oplossing te vinden. Dat heeft... Dat hebben heel veel mensen hier, en dat maakt af en toe ook leuk.

LIESBETH

Ja, precies.

PIM

Of eigenlijk altijd wel.

LIESBETH

Ja, je moet het... Je moet echt een de puzzel willen. De de code wil kraken. Letterlijk.

LIESBETH

Hoe vaak Pim ook zegt dat hij 'gewoon een taaltje gebruikt' om de datastromen te analyseren: ik vind er weinig gewoons aan. Maar de grote lijn is me duidelijk. En terwijl Pim verder gaat met zijn heel gewone werkzaamheden, moet er ook contact opgenomen worden met Elektron BV. Hoe dat moet, en wat we hen gaan vertellen, bespreek ik met Anouk.

ANOUK

Ik begrijp voldoende van cyber om het op een dusdanige manier uit te leggen dat de mensen die er iets mee moeten het ook kunnen volgen.

LIESBETH

Anouk heeft, in tegenstelling tot Pim en Tom, dan ook geen technische achtergrond. Ze werkt nu zo'n 13 jaar bij de dienst, iets wat ze van kinds af aan al wilde. En ze begon als algemeen bewerker.

ANOUK

Nou ja, ik heb eigenlijk altijd al bij de dienst willen werken. Ja, bij de geheime dienst. Dat leek me als kind al fantastisch. Maar ik heb hier toch niet gesolliciteerd toen ik afgestudeerd was.

LIESBETH

Want wat heb je gestudeerd?

ANOUK

Communicatiewetenschappen. Want ik dacht dat als je een link zou hebben met De Dienst, dat je dan al niet meer hier kon werken. Dus ik was heel erg bang dat als ik naar de website zou surfen om te kijken hoe De Dienst in elkaar zit en of er vacatures zijn... Ik dacht: Nee, dat kan nooit zo werken, want dan heb je natuurlijk de link gelegd, dat is toch...

LIESBETH

En je dacht dat die link al te veel was.

ANOUK

Ik had toen al eigenlijk een cyber... Toch het gevoel, dus. Maar uiteindelijk vertelde iemand dat ik me gewoon kon... Daar kon kijken en heb ik gesolliciteerd.

LIESBETH

En was het alles wat je ervan had gehoopt?

ANOUK

En nog veel meer. Ja, het is fantastisch.

LIESBETH

Hoe ga je daar in je privéleven mee om? Wie vertel je wel wat je waar je werkt, wie niet?

ANOUK

Ja, ik ben daar heel erg beperkt in, dus daarom vind ik dit ook best spannend. 13 jaar lang vertel ik vriend en vijand niet waar ik werk, en nu zit ik hier gewoon een interview te geven. Dus...

LIESBETH

Ja, inderdaad. Hoe is dat ?

ANOUK

Heel raar? Ja, ik denk dat nog veel raarder is als ik het straks terug hoor.

ANOUK

Familie weet het. En euh. Een paar naaste vrienden. Maar eh... Nee, er zijn ook vrienden die ik dagelijks spreek en die weten het niet. Ik vind vooral moeilijk als er over de dienst gesproken wordt op feestjes. En je kunt nooit iets zeggen. En dat uhm.

LIESBETH

En je kan dan niet hier... Je kan het niet heel uitgebreid gaan verdedigen.

ANOUK

Nee.

ANOUK

Het team waar ik in zit, daar krijgen we eigenlijk alle incidenten binnen. Uhm, omdat je vaak bij een incident nog niet meteen weet wie de actor is die erachter zit. Als je dat ooit te weten komt. En dan komt dat in eerste instantie bij ons team terecht. En de bewerkers in mijn team die gaan dan kijken of ze op een of andere manier een haakje hebben. Dat ze weten welke actor daarachter zit. En dat kun je soms al zien aan euh, een combinatie van het type aanval en de uh, het slachtoffer. Dat je gewoon weet: nou, die slachtoffers, en ze hebben op die manier de aanval uitgevoerd. Of ze hebben die malware gebruikt. Nou dat is typisch die ene hackersgroep, dat doen ze altijd. Dus dan heb je een vermoeden... of die hebben ze eerder gebruikt. Nou, dan geven wij het aan bewerkers die eerder onderzoek naar die groep hebben gedaan.

ANOUK

Als we het heel erg kort door de bocht neerzetten, zijn criminele hackers groepen vooral uit op financieel gewin. Dus die zullen allerlei acties doen om te zorgen dat ze gewoon geld binnen kunnen halen. En dan zie je dus dat ransomware aanvallen, en die WhatsApp fraude, dat zijn echt typische voorbeelden van, ja, geld binnenhalende criminelen die daar cyber als middel voor gebruiken.

ANOUK

Statelijke actoren. Die zijn veel meer geïnteresseerd in informatie, dus spionage of sabotage of heimelijke beïnvloeding. Dus eigenlijk is dat al een eerste verschil. Overigens, nou zeg ik dit zo simpel van 'is een beetje kort door de bocht', maar dat is het ook best wel. Want er zijn echt wel al voorbeelden waarbij de criminele groeperingen voor een overheid werken. En dan bepaalde hacks uitvoeren en alle buit die ze binnenhalen, alle informatie die ze jatten... Een deel daarvan gaat naar hun overheid toe. Maar het deel dat ze over hebben, dat verkopen ze gewoon op de zwarte markt.

LIESBETH

Met Pim heb ik het gehad over het onderzoeken van de datastroom, maar De Dienst heeft in dit soort gevallen ook de samenwerking met het slachtoffer nodig.

ANOUK

Weet die partij überhaupt dat ze aangevallen zijn?

LIESBETH

Ja precies.

ANOUK

En nou ja, dan is het wel de vraag of het in ons belang is om die partij daarover te informeren.

LIESBETH

Ja, want deze deze malware is gevonden doordat jullie die datastromen in de gaten houden. Maar wanneer weer gaat er een belletje naar Elektron BV, en wie doet dat? Of hoe gaat dat?

ANOUK

Nou ja, dat is dus wel... Dit is dan wel het moment. En kijk, Elektron bv is een energieleverancier, dus dat is de vitale sector. En op het moment dat de vitale sector in het geding is. Nou, dan hebben we het natuurlijk ook over maatschappelijke ontwrichting als daar een sabotage actie op zou plaatsvinden. Ja en, nou ja, als de nationale veiligheid in het geding is, dan komen wij in actie. We willen zo snel mogelijk naar een Elektron toe om ze aan de ene kant te informeren, en de andere kant ook handvatten te geven hoe ze het kunnen mitigeren. En mitigeren betekent dat ze het kunnen oplossen. De... Dus dat ze de actor uit hun netwerk kunnen krijgen.

LIESBETH

Ja. En ze, ze zullen... Zij zullen niet blij zijn met zo'n belletje.

ANOUK

Nee, nee, nee, nee, dat gaan ze niet blij mee zijn, nee. En we hebben daar Incident Response voor. Dat is een team dat daar naartoe gaat en... Nou het eerste wat we doen is kijken of er ook contacten hebben? Het is natuurlijk nogal wat om als Dienst zomaar even out of the blue te bellen naar een bedrijf en te zeggen 'goh, we hebben nieuws voor u'. En vaak zijn er met de bedrijven in vitale sector al contacten.

ANOUK

Samenwerking is cruciaal. Want cyberaanvallen kennen dus geen grenzen. Maar er zitten ook al andere kanten aan. Als wij alle kennis die wij hebben, alle technische kenmerken zouden delen... Laten we zeggen met alle Europese landen. Da's best risicovol. Want de kans dat dan uitlekt naar het de actor land, dus de aanvallende partij, dat iedereen inmiddels op de hoogte is van bepaalde malware die zij gebruiken... Nou ja, wat doet die aanvaller dan? Ja, z'n malware aanpassen zodat die niet meer gevonden wordt.

LIESBETH

En dan zijn jullie het zicht kwijt.

ANOUK

Ja, dus er is altijd een afweging tussen je operationele belang en het zicht dat je wil houden. En het, uhm, weerbaarheidsbelang voor je bondgenoten. En voor jezelf.

LIESBETH

Ja, en inderdaad het zich dat je wil houden. Want deze Rookworst... Je zou misschien zeggen: die moet je er zo snel mogelijk uithalen. Maar als ik het zo hoor, dan is het misschien nog wel fijner om hem erin te houden. En dat je kan zien wat het doet.

ANOUK

Ja, dat is een euh... Dat is een lastige.

LIESBETH

Zijn dat de beslissingen waar jullie ook mee bezig zijn?

ANOUK

Zeker. Kijk, het is natuurlijk in het belang van een Elektron BV en van de commerciële partij die zij in zullen huren, om uiteindelijk deze malware weer uit hun systeem te halen. Of eigenlijk moet ik zeggen: de actor uit het systeem te werken. Want waarschijnlijk zal er meer dan één malware type binnen zitten, inmiddels hè. Ze proberen 'persistent threat' te krijgen, zo noemen we dat.

LIESBETH

Meerdere paarden tegelijk.

ANOUK

Ja, als je eenmaal binnen bent dan zorg je dat je zo diep mogelijk op zoveel mogelijk manieren je tentakels uitslaat, zodat je echt goed binnen kunt blijven. Nou ja, zo een commerciële partij en Elektron BV, die willen zo snel mogelijk die aanval eruit hebben. En wij waarschijnlijk ook op hetmoment dat de nationale veiligheid in het geding is, dan... Maar als we dat nog niet weten, of niet zeker weten of ja... Dan willen we ook wel graag weten wie zit hierachter en wat hebben ze daar allemaal zitten? En wat is de infrastructuur die ze gebruiken? Dus een soort van terug rechercheren: waar komt die aanval vandaan?

LIESBETH

Waar het telefoontje van de professor vorig jaar haar topje van de ijsberg is, is dat nu de eerste detectie van de malware. En eigenlijk zijn we al iets verder, want het feit dat er malware werd gevonden zegt wel dat er iets aan de hand is. Al is nog niet duidelijk wat. Dit is hoe Anouk ernaar kijkt:

ANOUK

Het kan net zo goed met een sisser aflopen als heel serieus zijn. Dit soort incidenten komen regelmatig voor en het is echt niet altijd prijs. Dus ik kan dat hier ook echt niet inschatten van tevoren. Omdat het een energieleverancier is, zal ik wel intern in ieder geval natuurlijk onze leidinggevende, maar ook zijn leidinggevenden daarvan op de hoogte stellen. Zo van: nou, weet dat we dit uitlopen. Weet dat er een mogelijk sabotage oogmerk zou kunnen zijn. Nog tien slagen om de arm houden, maar weet dat we dit nu uitlopen en dat we onderweg zijn naar Elektron BV.

LIESBETH

Precies, en dit zijn dingen die jullie wel goed in de gaten houden.

ANOUK

Zeker, ja.

TOM

Oké, Liesbeth, eerste indrukken.

LIESBETH

Ja, euh, hoop geleerd, maar het is me ook wel duidelijker geworden. Ik begrijp steeds meer wat jullie doen. Ik begrijp ook dat er sommige dingen zijn die ik gewoon niet ga begrijpen en dat dat okay is. Ik zit het natuurlijk ook, ja dat is onvermijdelijk, het een beetje te vergelijken met vorig jaar. En dan denk ik wel van: okay, maar... Wat gaan we doen? Wat gaat er gebeuren?

TOM

We moeten naar Elektron.

TOM

Ja, daar is het gebeurd. Daar zit de informatie die we willen hebben. Ehm, dus we gaan gewoon het Incident Response Team bij mekaar halen en die gaan euh daarheen. En die gaan proberen om samen met Elektron kunnen vast te stellen wat er gebeurd is. En daarbij is heel belangrijk dat ze de goeie informatie te pakken krijgen die voor ons onderzoek het allerbelangrijkste is. We hebben het over, gewoon: wat is op die systemen gebeurd? Dat staat in de zogenaamde logging. We willen een stukje van het netwerk verkeer hebben. Kunnen we kijken wat er... of die malware nog steeds aan het beaconnen is.

LIESBETH

Ja, het communiceren met zijn afzender.

TOM

Absoluut. En we willen gewoon een kopie van malware hebben, zodat we die helemaal uit mekaar kunnen gaan trekken en kan kijken: wat is 'ie aan te doen?

LIESBETH

En gaat Elektron zomaar de deur voor ons openzetten?

TOM

Dat weten we niet, dat is altijd de vraag.

LIESBETH

Oké, dus we moeten het team bij elkaar gaan halen.

TOM

Team bij elkaar, busje in. En dan vooral met de schurende banden die kant op.

LIESBETH

Mijn tweede dag zit erop en onderweg naar huis dansen alle gesprekken door mijn hoofd. Hoe groot mijn afstand tot cyber ook is, eigenlijk is er heel veel te snappen van de grote lijnen zonder de details helemaal te doorvoelen. En hoe meer ik de reikwijdte doorzie, hoe meer deze wereld me weet te trekken.

LIESBETH

De volgende aflevering gaan we kijken naar wat het bezoekje aan Elektron heeft opgeleverd en wat er in de malware te vinden is. Voor degenen die met ons mee puzzelen: Tom heeft de volgende details voor je.

TOM

Met een beetje geluk wil euh, Elektron ons van informatie voorzien. En natuurlijk, zodra die informatie binnen is en deze podcast gepubliceerd is, kun je het allemaal terugvinden op OperatiePositron.nl. En dit keer een dossier met een kopie van de malware, pcap-je van het interne netwerk verkeer en natuurlijk heel veel logging. Allemaal klaar om in elkaar gehaald te worden en geïnspecteerd te worden. Veel plezier en succes.

LIESBETH

Dit was de tweede aflevering van De Dienst, een podcast van de AIVD. Gepresenteerd door mij, Liesbeth Rasker, en geproduceerd door Het Podcast Kantoor in samenwerking met WerkMerk. Abonneer je nu, zodat je niets van dit nieuwe onderzoek hoeft te missen. En laat ons vooral weten wat je van deze serie vindt in een recensie in je favoriete podcast app.