Operatie POSITRON aflevering 4 - Geflipte bits

LIESBETH

Hoe leg je aan je oma uit wat voor werk je doet?

MARK

Niet. Nee, dat is heel lastig.

LIESBETH

We zijn halverwege de zaak en ik ben dus ook halverwege mijn stage. Net als vorig jaar leer ik elke dag nieuwe dingen, maar dit jaar wordt er nog meer een nieuwe wereld voor me geopend. Ik ga er gewoon van uit dat ik iemand kan bellen, dat ik vanaf mijn laptop draadloos iets kan printen en dat een foto die ik met mijn telefoon maak ook ergens in de cloud hangt. De AIVD'ers die ik nu spreek, werken in een laag van de wereld waar ik wel gebruik van maak, maar verder nooit bij stilstond. Bits, bytes, pakketjes, strings, code, data. Een heel groot deel van mijn wereld is er wel uit opgebouwd en nu begin ik er eigenlijk pas oog voor te krijgen, voor de haast grenzeloze mogelijkheden. Maar ook de gevaren.

BAS

Als onze tegenstander alles goed doet, dan staan wij met lege handen. Dat is nou eenmaal de realiteit van dit vak.

LIESBETH

Mijn naam is Liesbeth Rasker. Dit is aflevering 4 van Operatie Positron, de podcast van de AIVD. Welkom bij De Dienst.

LIESBETH

Tom, daar zitten we weer.

TOM

Jazeker, een nieuwe dag, nieuwe kansen. Ja, dit keer een stuk wakkerder dan de vorige.

LIESBETH

Ja, maar het is wel... Je zei dat je het druk ging krijgen, dus dat...

TOM

Absoluut, de tapdata is en masse binnengestroomd. En daar is ook al naar gekeken. Er zijn veel antwoorden en eigenlijk ook nog veel meer vragen in te vinden. Dus ik zou eigenlijk willen voorstellen: we gaan zo snel mogelijk de diepte in, gaan zo snel mogelijk met wat specialisten om tafel zitten om eens te gaan kijken wat ze allemaal gevonden hebben.

LIESBETH

En met wie moet ik dan gaan zitten?

TOM

Ik zou beginnen met een collega van CNI, van Computer Network Investigations, dat is Mark. Hij kan je helemaal meenemen in alles wat er gevonden is in de taps. Hij heeft ook de implant Rookworst bekeken. Dus daar kan hij je ook nog van alles over vertellen als je nog details wil weten. Daarnaast ook handig om meteen even door te lopen naar een collega van Crypto, Bas.

Ik had namelijk al een beetje in de tap gespiekt en ik zag al her en daar wat verkeer voorbijkomen wat er zeer versleuteld uitzag. Dus ik zou meteen met hem even gaan overleggen of er mogelijkheden zijn om te kijken wat daar eigenlijk staat.

LIESBETH

Dus nu gaan we echt de technische details in.

TOM

Zeker weten.

LIESBETH

Ja, want bij een cyberzaak ontkom je natuurlijk niet aan die technische details. Maar alles is op hoofdlijnen ook heel goed te volgen. En het is heel interessant om meer te leren over hoe je apparaten en online diensten eigenlijk werken. Mijn eerste gesprek van de dag is met Mark. Hij zit bij de afdeling CNI.

MARK

CNI staat voor Computer Network Investigation. En investigation is denk ik het sleutelwoord in deze terminologie. En dat gaat om onderzoeken.

LIESBETH

Ja. En hoelang werkt jij al bij de AIVD?

MARK

Ik werk niet bij de AIVD. Ik werk bij de MIVD.

LIESBETH

Mark werkt niet voor de AIVD, wat staat voor Algemene Inlichtingen- en Veiligheidsdienst, maar voor de MIVD. Dat staat voor Militaire Inlichtingen- en Veiligheidsdienst. Ook een geheime dienst dus, maar met andere taken. De MIVD zorgt ervoor dat onze militairen in het buitenland kunnen beschikken over de informatie die ze nodig hebben om hun werk veilig te kunnen doen. Er is tussen AIVD en MIVD wel een aantal gezamenlijke afdelingen, zoals de Joint Sigint Cyber Unit, wat ze hier afkorten met JSCU. Pim werkt daar, uit aflevering 1. En Mark, die ik nu spreek.

MARK

Ik zit op dezelfde werkplek als mijn AIVD-collega's. Ik weet eigenlijk ook niet wie MIVD en wie AIVD is, we lopen allemaal door elkaar.

LIESBETH

In hetzelfde pand dus ook gewoon.

MARK

In hetzelfde pand. Binnen CNI ben ik een zogenaamde lead onderzoeker. We onderscheiden twee rollen. Een lead onderzoeker is betrokken bij de onderzoeken. En dan hebben we ook domeinspecialisten.

LIESBETH

Mark ziet er best jong uit, maar is hier al een hele tijd werkzaam. Hij is dan ook al tijdens zijn studie informatica gescout door de AIVD en ook hij heeft van zijn hobby zijn beroep gemaakt.

MARK

Ja, ik kreeg wel op een gegeven moment een beetje een vreemd belletje van iemand die zei: we willen verder met je praten of we willen een keer kennismaken. Dus dat was eigenlijk wel heel leuk. Wij zijn echt wel bezig met het ontdekken van dingen en iedereen heeft een natuurlijke nieuwsgierigheid. En daarmee eigenlijk ook een drive om beter te worden in wat je al doet. De ontwikkelingen binnen cybersecurity en dit soort, ja, gerelateerde onderwerpen, staan natuurlijk niet stil, ontwikkelt zich supersnel. En daar moet je een beetje bij blijven. En het liefst vooroplopen in kennis over wat je te onderzoeken hebt.

LIESBETH

Dat is hier de plek voor bij uitstek.

MARK

Zeker. Zeker.

LIESBETH

Misschien dat je net als ik soms niet meer helemaal duidelijk voor ogen hebt wat het verschil is tussen alle mensen die je hebt gehoord, omdat iedereen maar met de data bezig is. Dus even een klein overzicht. Dit zijn de drie belangrijke afdelingen die je in deze podcast hoort. We hebben CND, dat staat voor Computer Network Defense en zij zijn bezig met aanvallen af te weren. En dit doen ze door netwerken geautomatiseerd in de gaten te houden. Dan is er CNE, Computer Network Exploitation. Dit zijn de hackers, daar ga ik later iemand van spreken. En we hebben CNI, Computer Network Investigation. Zij onderzoeken malware en proberen zo de werking van de malware te achterhalen en de makers, dus de daders. Mark is van CNI en dit is in zijn eigen woorden wat zijn werk inhoudt.

MARK

Wij kijken naar de data. Dus er komt een heleboel data binnen. Die moet op de een of andere manier inzichtelijk gemaakt worden. En daar hebben we verschillende tools voor.

LIESBETH

Als je zegt: er komt een hele hoop data binnen. Hoe ziet dat er dan uit?

MARK

Ja, dat zie je niet echt.

LIESBETH

Maar het is een USB-stickie en dat wordt in de computer gedaan en dan is het: Dit is het? Of...

MARK

Laten we het even vergelijken met telefonie. Als jij aan het bellen bent met een vriendinnetje of een vriend of whatever, als je dat opneemt, dan hoor je eigenlijk gewoon twee mensen praten. Als twee computers met elkaar communiceren dan bellen die eigenlijk ook een soort van met elkaar. En die wisselen een heleboel data uit om dat in goede banen te laten lopen. Dus dat is overhead data. Dat zegt waar het pakketje heen moet. Dat wordt opgeknipt in stukjes om het efficiënter te laten verlopen. Daar zit ook echt data in. Dus als jij een website bezoekt, een nu.nl, dat moet over een internetkabeltje of over wifi naar jouw telefoon of naar je laptop toe. Dat zit er in die pakketjes. En als je kijkt naar een stroom data, dan zit dat allemaal opgeknipt in allemaal kleine pakketjes die op je computer weer in elkaar worden gezet. Daar komt...

LIESBETH

Maar hoe ziet het er op jouw scherm uit? Kijk je naar allemaal getallen? Kijk je naar allemaal letters, cijfers? Waar kijk je naar?

MARK

Allemaal sessies.

LIESBETH

Sessies.

MARK

Sessies.

LIESBETH

Hoe zien die sessies er dan uit?

MARK

Over het algemeen zien die dingen eruit als bytes en IP-adressen, waar het vandaan komt, waar het heen gaat, tijdnotatie, wanneer dat dan is gebeurd, welke protocollen het zijn. En vaak is data die we bekijken geëncrypt, versleuteld. Dus dan zien we er eigenlijk ook niet zo heel veel aan. Kunnen we er ook niet eens zo heel veel mee.

LIESBETH

Nee, dan moet dat eerst... Die code moet eerst gekraakt worden, bedoel je.

MARK

Dat kan, maar dat is ook lang niet altijd mogelijk.

LIESBETH

Nee. En dan?

MARK

Is het idee: wat wil jij weten?

LIESBETH

Ja, nou, in het geval van die malware waar we het dus nu over hebben, dan wil ik dus weten wat het precies doet, waar het vandaan komt, waar het heen gaat, wat het al heeft gedaan misschien.

MARK

Ja, lijken me hele goeie vragen.

LIESBETH

Lukt dit altijd? Ik bedoel, is het altijd gezegd dat als zo'n malware bij jullie binnenkomt, dat je die informatie eruit krijgt of blijven de deuren ook weleens dicht?

MARK

De deur blijft ook zeker weleens dicht. Dat klopt.

LIESBETH

En wat dan?

MARK

Dan ga je net zolang door totdat je wel de deur open probeert te krijgen. En soms komt er later in het onderzoek nog wel een puzzelstukje waarmee je uiteindelijk die deur wel open krijgt. Dat is uiteindelijk de bedoeling. Maar soms kom je er ook gewoon echt niet achter en dan moet je het laten rusten. Dan kijken we later nog wel of we daar weer wat mee kunnen, ja of nee.

LIESBETH

Laten we hopen dat we de deuren in onze zaak in ieder geval zo snel mogelijk open krijgen. Om te beginnen met de deuren die we tegenkwamen in de data van de tap. Wat is Mark allemaal tegengekomen?

MARK

Ja, we hebben een aantal dingen. We hebben een tap en dat is op een C2. Jij bent er inmiddels achter, denk ik, wat een C2 is.

LIESBETH

Dat is me uitgelegd.

MARK

Die opdrachtjes kunnen we eigenlijk zien. Of in ieder geval, we zien communicatie tussen de malware en de C2-server. Nu is het zo dat deze over het zogenaamde HTTP-protocol gaan. En in het normale internet is dat open dus te zien wat er dan in die pakketjes zit. Nu is het zo dat deze malware, zoals we ook eerder hebben onderzocht, een eigen encryptielaag hebben. Dus die versleutelt op een eigen manier zijn eigen verkeer. En dat zouden we eventueel kunnen onderzoeken. En dan gaan we in de, wij noemen malware ook wel een binary, dus dat is een... Als jij iets downloadt van het internet en daar staat .exe achter, dan is dat een executable. Dat is zo'n .exe-bestandje en dat voert wat uit. Dan kunnen we kijken: wat doet dat precies? En dan echt op microniveau. Dus stel dat jij vroeger lekker een beetje aan het ontdekken was wat techniek allemaal doet. Dus je trekt een stofzuiger uit elkaar en wat doet dit knopje? En wat doet dat knopje? Nou, zo werkt dat virtueel eigenlijk ook. Om te kijken van: hoe werkt zo'n machinetje eigenlijk? En als we dat helemaal zo in ons jargon 'uit elkaar trekken', dan kun je zien dat er cryptoroutines zijn, dat er stukjes zijn in de code die communicatie opzetten met de C2-software. En dan zouden we eventueel inzicht kunnen krijgen in het verkeer, wat er ook echt naar de C2 gaat.

LIESBETH

Ja, ik neem aan dat de statelijke actor waar dit over gaat, als het een statelijke actor is, dat die dit allemaal zo hebben gebouwd dat dit allemaal niet gaat lukken.

MARK

Ja, dat is wel wat ze meestal proberen.

LIESBETH

Precies. Ben je ook wel eens heel erg onder de indruk van wat je aantreft? Dus dat je denkt: wow, dit is echt waanzinnig gemaakt.

MARK

Zeker. Dat noemen we obfuscatie.

LIESBETH

Obfuscatie.

MARK

Obfuscatie. Dan probeert een andere actor het zo ingewikkeld mogelijk te maken. Er zijn ook tools om dat te doen. In het programmeren gebruik je meestal hele logische namen voor functies in code. Die obfusceren ze dan met hele complexe namen. En dat husselen ze allemaal door elkaar heen, zodat er eigenlijk helemaal niets meer van te volgen is. En je probeert dat dan helemaal terug te reconstrueren. En dat kan heel veel tijd kosten, maar het is enorm bevredigend als het uiteindelijk wel lukt.

LIESBETH

Is dat in dit geval ook zo? Kun je daar al iets over zeggen?

MARK

We kunnen een aantal dingen zeggen. Ik pak het er even bij. Als we kijken naar de opbrengsten van de tap, dan zijn er eigenlijk een aantal conclusies, in het kort, die we hebben. We zien verkeer van slachtoffers. In jargon noemen we dat beaconing. En dat zijn twee slachtoffers. Beide bij hetzelfde bedrijf.

LIESBETH

Waar we al bang voor waren, is dus inderdaad het geval. We hebben te maken met twee slachtoffers, wat ook betekent dat we met een serieuze aanvaller te maken hebben die zich niet zomaar gewonnen gaat geven.

MARK

Het werkt vaak zo dat: een aanvaller zit in het netwerk van een slachtoffer, in dit geval Elektron BV, en plaatst daar meerdere implants, dus eigenlijk meerdere stukjes malware op diverse computers.

LIESBETH

Om de kansen te spreiden dat ze erin blijven.

MARK

Exact. Oké, stel dat ze ontdekt worden op plek A, dan zitten ze nog op plek B.

LIESBETH

En we dachten dat het er eentje was. Maar dat is dus...

MARK

Dat zijn er twee. We hebben twee afzonderlijke machines gezien en dat noem je in het jargon persistence. Zo goed mogelijk blijven zitten waar je al zit.

LIESBETH

En moet ik me nou voorstellen dat de een op de computer van de receptionist zit en de ander op een andere computer? Of hoe ziet het eruit?

MARK

Dat kan. Wij zien op dit moment niet goed waar ze precies zitten. Wat wij zien is een weerspiegeling van hoe een computer zich op het internet gedraagt. Dus we zien een user agent. En dat is dan eigenlijk de identiteit van een computer. En we zien twee verschillende user agents. Dat zegt ons in ieder geval dat het twee verschillende computers zijn.

LIESBETH

Maar waar en van wie die precies staan of zijn...

MARK

Dat zouden we bij Elektron BV moeten checken. Ja, dat kunnen we...

LIESBETH

Is dat relevant?

MARK

Zeker. Zeker. Dat kan. Als het de computer van de receptionist is, dan is er misschien niet zo'n probleem. Maar als het de centrale fileserver is waar al hun bedrijfsgeheimen of wat ze ook maar willen beschermen staan, dan is dat een stuk problematischer. Daarnaast zien we ook een andereserver connectie maken met de C2 en het vermoeden is natuurlijk dat dat een ander deel is van de actorinfrastructuur om de informatie uit het netwerk van het slachtoffer een stapje verder richting de actor te brengen.

LIESBETH

Dus dan gaan we er nog een stap verder af eigenlijk.

MARK

Ja, ja, je moet je eigenlijk voorstellen dat jij vanuit Nederland naar iemand in Zwitserland belt, vanuit Zwitserland weer naar Amerika, van Amerika weer door. En jij ziet eigenlijk alleen naar wie jij in Zwitserland hebt gebeld. En de boodschap die gaat helemaal over alle schijven door naar de...

LIESBETH

Een ouderwetse telefoonketting voor als je vroeger moest doorbellen dat het eerste uur uitviel.

MARK

Ja, je weet niet waar het uiteindelijk vandaan komt. Maar je weet wel de laatste die je al gebeld heeft.

LIESBETH

En dan ga je stapje voor stapje voor stapje proberen steeds dichter bij de bron te komen?

MARK

Ja, maar lang niet al die servers staan alleen in Nederland of hebben we toegang toe. Dus dat maakt het heel complex.

LIESBETH

Ik vind nog steeds moeilijk om het...

MARK

Te visualiseren?

LIESBETH

Ja.

MARK

Dat snap ik. Ja, dat blijft ook zo.

LIESBETH

Dat blijft zo. Want hoe leg je aan je oma uit wat voor werk je doet?

MARK

Niet? Nee, dat is heel lastig. Ja.

LIESBETH

Dan zeg je: ik doe iets met computers.

MARK

Ja, daar komt het wel op neer. Ja, ja.

LIESBETH

En dan zegt ze... vraagt ze dan jou steeds als zij iets met haar computer heeft of jij het even voor haar wil oplossen?

MARK

Ze heeft een iPad, daar kan ze alles mee. Dat is helemaal top.

LIESBETH

Geweldig!

MARK

Het is wel goed te doen om het visueel te maken, maar dat zul je er altijd bij nodig hebben om het goed te begrijpen. Dus ik maak ook een plaatje in mijn rapport van wat er aan de hand is, omdat het anders gewoon niet zo goed te begrijpen is. Als ik zeg: twee slachtoffers en C2 en er wordt nog ietsgepollt van een andere server... Ja, dat gaat natuurlijk het ene oor in en dat andere oor uit als je daar niet zo'n beeld bij hebt, maar als je daar een schema van ziet, dan is dat al veel beter.

LIESBETH

Is dat een ingewikkeld schema of zou je dat in theorie nou ook hier op papier...

MARK

Ik kan het heel makkelijk tekenen.

LIESBETH

Doe eens?

MARK

Ik zal even een willekeurig papiertje pakken. Een pen.

LIESBETH

Ik heb hier ook een opschrijfboekje voor je.

MARK

Ja, is goed.

LIESBETH

Steeds ben ik op zoek naar een visuele weergave van het abstracte werk dat ze hier doen. En dat krijg ik nu eindelijk. Dus pak pen en papier of teken in je hoofd mee. We beginnen aan de bovenkant van het A4.

MARK

Ik teken even een groot vak, dat is het slachtoffernetwerk. Daarin zitten een heleboel kleine vakjes en die representeren dan de computers. Dit is Elektron. Laten we Elektron maar schrijven. En wat ik uit de tap haal, dus uit het netwerkverkeer, is dat hier twee vakjes zitten, dus twee computers. En daar teken ik een pijltje buiten het grote vak.

LIESBETH

De twee vakjes zitten dus in het vak van Elektron en ze staan voor de twee geïnfecteerde computers.

MARK

En die maken alle twee een verbinding met de C2 en die C2 die teken ik even buiten het grote vak.

LIESBETH

De C2-server is, zoals we in de vorige aflevering bespraken, een van de waarschijnlijk vele tussenstops tussen slachtoffer en actor in. Dit is de server die zich vermomt als onschuldige website van een pannenkoekenrestaurant en die ontvangt de data van de twee computers. En die server zijn we aan het tappen.

MARK

Dus we hebben zicht op al het verkeer wat erin en wat eruit gaat. En we kunnen niet alles lezen omdat dat deels ook versleuteld is. Maar we weten in ieder geval wel dat het er is. Die C2 wordt dan weer bevraagd door een andere computer, ook buiten alle andere netwerken, we weten eigenlijk niet zo veel daarvan. Maar we weten wel dat die connectie maakt met de C2. Dus dat is eigenlijk heel simpel wat er aan de hand is. En de andere server die connectie maakt met de C2, dus de andere actorinfrastructuur, die gaat over https. En daar moeten we eens even beter naar kijken of daar misschien een foutje in geslopen is. Maar over het algemeen kun je zeggen: https, daar kunnen we gewoon niet in kijken.

LIESBETH

Daar kunnen we niet doorheen.

MARK

Nee, daar kunnen we even niet... Daar kunnen we gewoon niet in kijken.

LIESBETH

Is dit knap werk van degene die dit heeft gemaakt?

MARK

Jawel, ik vind vooral een eigen implementatie van encryptie, ja, als dat goed wordt gedaan, dan is dat heel knap. Maar meestal is het ook wel zo dat mensen die het wiel opnieuw uitvinden daar foutjes inmaken, omdat ze niet de expert zijn op cryptografie. Maar soms gebeurt dat echt op een dusdanige manier dat we daar totaal niet doorheen komen. En soms maken mensen foutjes.

LIESBETH

Vind je net toch ergens een muizengaatje waar je wel doorheen kunt.

MARK

Ja. Dus daar zouden we beter naar moeten kunnen kijken.

LIESBETH

Kun je op dit niveau ook al zien hoe groot en ook dus hoe serieus de eventuele dader is?

MARK

Het is zeker serieus.

LIESBETH

Dit zijn geen hobbyisten meer.

MARK

Dit zijn geen hobbyisten.

LIESBETH

Omdat een deel van de data door encryptie, dus door versleuteling, niet direct zichtbaar is voor Mark en zijn team, ga ik praten met iemand die dat wellicht kan oplossen. Ik loop naar Bas. Hij is van de afdeling encryptie en hij zat al in het vak toen het vak er nog heel anders uitzag.

BAS

Ja, klopt al een hele tijd.

LIESBETH

Al een hele tijd. Wat is een hele tijd? Hoe werk je hier al?

BAS

Sinds 2002 werk ik.

LIESBETH

Bas is ook MIVD'er en heeft in de afgelopen twintig jaar dat hij hier werkt op het gebied van cyber een hoop, zo niet alles, zien veranderen. Ik vraag wat er op zijn afdeling op dit moment gebeurt.

BAS

Wij proberen vercijferde data te ontcijferen, leesbaar te maken of er op andere manieren zoveel mogelijk bruikbare informatie uit te halen.

LIESBETH

Ben je dan heel goed in puzzels?

BAS

Minder goed dan sommige andere mensen.

LIESBETH

Dat is denk ik bescheidenheid.

BAS

We hebben een heleboel hele goeie mensen hier.

LIESBETH

Ja, precies. Maar als ik een bak met letters uitstrooi, dan kun je heel snel daar verbanden in zien of abstracte dingen concreet maken? Moet ik het me zo voorstellen?

BAS

Voor een deel wel, ja.

LIESBETH

Kun je me in hele simpele bewoordingen uitleggen wat een cryptoalgoritme eigenlijk is?

BAS

Ja, dat is een lastige vraag. Ja, uiteindelijk is het een algoritme dat data vercijfert of op de een of andere manier onleesbaar maakt. Dus data, uiteindelijk op het laagste niveau is dat een hele stroom nullen en enen achter elkaar. En wat crypto uiteindelijk doet op zo'n stuk data is dat het gewoon sommige van die nullen in een één verandert en omgekeerd, maar dan op zo'n manier dat een buitenstaander niet meer kan zien wat er oorspronkelijk was. En je kunt aan die bits natuurlijk ook niet zien welke bits er uiteindelijk zijn omgeklapt. Dus daarmee komt de hele data... Ja, die ziet eruit alsof het random is. Dat is het doel van crypto. Dus uiteindelijk het nut... Zo'n cryptoalgoritme bepaalt dan welke bits je om gaat klappen en welke bits je met rust laat.

LIESBETH

We hebben het nu over deze malware waarvan we de crypto willen breken eigenlijk, waardoor het hele idee van crypto ook een soort onderdeel van de tegenstander wordt. Maar tegelijkertijd, het beveiligt ons ook.

BAS

Ja, ja, zeker.

LIESBETH

Als je op WhatsApp ook een nieuw bericht opent, staat er ook boven: deze gesprekken zijn encrypted. Maak jij gebruik van WhatsApp?

BAS

Ja.

LIESBETH

Wel?

BAS

Ja.

LIESBETH

Da's veilig genoeg dus.

BAS

Ik zou er geen staatsgeheimen over versturen. Nee, maar om gewoon de de familie te appen. Daar is het veilig genoeg.

LIESBETH

Ja, niet alles wat je vervolgens hebt ontcijferd is ook daadwerkelijk van belang. Dus je moet ook nog eens een heel hoop werk uitvoeren voordat... En dat is dan misschien niet eens bruikbaar.

BAS

Ja, nee, wij hebben in het verleden ook wel eens een afdelingshoofd gehad die ons vroeg of we niet de belangrijkste berichten als eerste konden ontcijferen. Dus toen hebben we inderdaad geantwoord of hij kon aangeven welke vercijferde berichten het belangrijkste waren.

LIESBETH

En wat zei hij toen?

BAS

Ja, toen stond ie met zijn mond vol tanden.

LIESBETH

Toen begreep hij het.

BAS

De eerste vraag is altijd van: wat weten we daarvan? Is het puur onbekende data of weten we al wat voor algoritmes er gebruikt zijn? Weten we wat voor programmatuur er gebruikt is en al dat soort dingen? Als je de programmatuur in handen hebt waarmee het is vercijferd, dan kun je die uit elkaar gaan trekken en onderzoeken en kijken wat daar in zit. Op het moment dat je een kopie van die programmatuur, van die malware in handen hebt, dan kun je die gaan onderzoeken en dan kom je er vrij snel achter welke cryptoalgoritmes er gebruikt worden.

LIESBETH

Dus in deze zaak, deze malware wordt bij jou neergelegd. Waar begin jij dan?

BAS

Nou, we beginnen inderdaad met kijken van: de programmatuur, die gaan we onderzoeken: wat voor algoritme zit erin? Maar ook: waar halen ze de sleutels vandaan? Hoe genereren ze die? Waar slaan ze die op? Zitten daar nog fouten in? Gebruiken ze slechte randomgeneratie bijvoorbeeld? Dat je sleutels krijgt die op elkaar lijken? Of dat er meerdere berichten met dezelfde sleutels worden vercijferd? Al dat soort dingen, dat zijn allemaal foutjes die ze kunnen maken. En dat zijn haakjes waar wij dan aan kunnen gaan peuteren.

LIESBETH

Is het leuk werk?

BAS

Ik vind het ontzettend leuk werk.

LIESBETH

Ja? Wat maakt het zo leuk voor jou?

BAS

Het is een... Ja, zoals je net al zei: het is een puzzel. Het is een intellectuele uitdaging. Het is gewoon ontzettend gaaf als het je lukt, als jij slimmer bent dan de ander. Als het natuurlijk voor een goed doel is, de veiligheid van Nederland, voor de bedrijven. Dat maakt het alleen maar nog leuker. Het hangt heel erg af van wat je weet van tevoren en hoeveel je weet over de gebruikte vercijfering. Op het moment dat je zeg maar weet dat er RC4 is gebruikt, nou ja, dat is een redelijk sterk algoritme. Dan weten we al dat we niet op zoek hoeven te gaan naar een zwakheid daarin en dat we op zoek moeten gaan naar een zwakheid in de manier waarop die gebruikt is. Dus dan gaan we heel erg zoeken van: worden er sleutels hergebruikt? Worden er zwakke sleutels gebruikt, slechte random? Al dat soort dingen. Als onze tegenstander alles goed doet, dan staan wij met lege handen. Dat is nou eenmaal de realiteit van dit vak. Vaak heb je dan nog wel situaties waarin we kunnen zeggen: misschien kunnen we in samenwerking met onze hackers nog wat extra informatie naar binnen halen. Dat we daarmee nog wel een stap verder kunnen komen.

LIESBETH

In onze zaak is de hoop dat we de versleuteling eraf weten te halen, zodat we te weten komen met wie de C2-server nog meer communiceert. Het zou namelijk zomaar kunnen dat er nog een Elektron is of heel veel Elektrons. Die C2, de website Pannenkoekenpalazzo.nl, is op dit moment de grote sleutel in de zaak die hopelijk zo snel mogelijk in het slot gaat vallen.

BAS

Ja, ik sta te popelen om met die data aan de slag te gaan. Zeker als ik zie dat ze op één verbinding RC4 hebben gebruikt. Dat lijkt erop te duiden dat ze zelf iets hebben geïmplementeerd.

LIESBETH

Kun je eigenlijk kort uitleggen wat dat is, RC4?

BAS

RC4 is een vercijfermethode. Een algoritme. Ergens in de jaren negentig bedacht, toen heel veel gebruikt. Tegenwoordig enigszins in diskrediet.

LIESBETH

Maar het duikt hier toch weer op.

BAS

Ja, ja, hij wordt nog vaak gebruikt wel. Hij is heel simpel te implementeren.

LIESBETH

Maar moeilijk te kraken.

BAS

Moeilijk te kraken als ie goed geïmplementeerd is en goed gebruikt. Zelf geïmplementeerde crypto is altijd leuk voor ons, want daar is de kans groot dat er wat mis mee is.

LIESBETH

Dat er wat te halen valt.

BAS

Ja, van tevoren kun je op basis van een paar steekwoorden dat moeilijk inschatten. Je moet er echt in duiken en eraan gaan peuteren en dan kijken of je ver genoeg kunt komen.

LIESBETH

Als dat allemaal al gelukt is, hè, stel, wat doe je dan? Aan wie geef je het dan door? Waar gaat het dan heen?

BAS

Dat verschilt een beetje van zaak tot zaak. Als het onze cyberjongens zijn, gaat het vaak direct terug naar hen. Zij hebben natuurlijk vaak ook zelf de technische kennis en knowhow om met die sleutels dan weer zelf aan de slag te gaan en de boel zelf te ontcijferen en verder met die data te gaan. Als het meer naar analisten of mensen gaat die meer op de inhoud zijn, dan moeten wijzelf ook de boel ontcijferen en een beetje in een leesbaar formaat zien aan te leveren.

LIESBETH

In normale mensentaal.

BAS

Ja, ja, ja, en we kijken of we het gewoon netjes aan kunnen leveren aan het grote cluster dat we hebben in een formaat dat door alle tools kan worden gelezen.

LIESBETH

Ja, zodat ik er ook wat van begrijp.

BAS

Ja, zodat onze analisten het inderdaad direct kunnen lezen en zodat alle metadata netjes beschikbaar is en geanalyseerd kan worden.

LIESBETH

Ja ja, oké.

LIESBETH

Ik ga terug naar Tom om uit al deze technische details te stappen en even uit te zoomen.

TOM

Oké, Liesbeth. Vertel het maar, welke nieuwe dingen over de casus heb je allemaal al gehoord?

LIESBETH

Ja, o, het was wel weer een dag met veel informatie. Wat in ieder geval een grote ontdekking is, als ik het goed begrijp, is dat er niet één probleem is, maar twee. We hebben niet één geïnfecteerde computer, maar twee? Zeg ik het dan goed?

TOM

Zeker. Nee, dat heb ik... dat is ook meteen mij even ingefluisterd en ik ben meteen gerend naar Ellen van het NBV. En zij heeft meteen de telefoon gepakt en Elektron gebeld om ze hierover te informeren. Toen kregen we het antwoord terug: ze vonden het heel goed, heel fijn dat we het even gemeld hadden. Ze gaan er nu ook meteen naar kijken. Maar we hebben ook meteen gehoord dat zij besloten hadden om de acteur uit het netwerk te verwijderen.

LIESBETH

Ja, dat lijkt me logisch.

TOM

Ja, moet ik zeggen, is het ook. Ik snap het heel goed. Zeker als groot energiebedrijf wil je niet dat er zomaar iemand in je systemen bladert. Voor ons is het een beetje jammer. Het feit dat zij een implant verwijderd hebben, geeft wel aan een actor heel duidelijk weer van: oké, we weten dat je hier bent. We hebben je gevonden. Dus onze enige positie is een stukje labiel geworden nu. Dus het is wel zo...

LIESBETH

Zijn ze er allebei uit?

TOM

Nee, ze hebben dit gedaan voordat we ze op de hoogte hadden gesteld van de tweede implant.

LIESBETH

Dus die zit er nog in.

TOM

Die zit er nog in. De eerste is verwijderd. Ik ga er wel van uit dat ze die tweede nu ook vrij snel eruit gaan gooien. Maar het is aan ons nu wel zaak om zoveel mogelijk inlichtingen die we kunnen pakken, te grijpen om ze veilig te stellen. Ik ga er nu van uit dat de hackers hun zaakjes zo snel mogelijk gaan opruimen.

LIESBETH

Ja, ze gaan dus die malware terugtrekken.

TOM

Ze gaan de malware terugtrekken. En veel belangrijker, ik zou er wel op durven wedden dat ze Pannenkoekenpalazzo gaan opheffen.

LIESBETH

Ja, en dan kom je helemaal nooit meer te weten wat hier...

TOM

Dan weten we het echt niet meer. Nee.

LIESBETH

Maar die ene is er uit, die andere zit er nog in. Dat is de laatste kans die er is om verder te komen in deze zaak eigenlijk. Wat zijn dan nu de opties om dat te bewerkstelligen?

TOM

Ik denk dat we zo snel mogelijk achter het Pannenkoekenpalazzo aan moeten en er een kopie van gaan maken.

LIESBETH

Zodat alles wat daar nu op is, dat dat in ieder geval bewaard blijft.

TOM

Absoluut, ja, dat we die snapshot in ieder geval hebben.

LIESBETH

Ja. Is dat genoeg?

TOM

Ik heb geen idee, het is alles wat we nu hebben en dus ik wil eigenlijk daar zo snel mogelijk een aanvraag voor schrijven. Waarschijnlijk onder spoed. We gaan Joey even bellen. Binnen halen en dan zo snel mogelijk richting Mark en zijn team. Die gaat op de eerste plaats proberen te begrijpen wat er allemaal op de server staat. Of we daar iets aan hebben. Dan kunnen we kijken of er misschien sleutels liggen die we kunnen gebruiken om het verkeer te ontcijferen.

LIESBETH

Het rennen van CND'er Pim uit aflevering 2 en het spoedje van jurist Joey zijn nu allemaal aan de orde. Iedereen is alert, want het hele onderzoek staat op losse schroeven en valt definitief om als de actor inderdaad de C2-server offline haalt, omdat hij door het verwijderen van die ene implant doorheeft dat hij gezien is. Wie de aanvaller is en wanneer hij dan weer toeslaat, zijn dingen waar de AIVD dan helemaal geen zicht meer op heeft. Er gaat nu een kopie van de server gemaakt worden, zodat alles wat er nu is in ieder geval niet verloren gaat en we dat verder kunnen onderzoeken. De challenge voor wie met ons mee rechercheert gaat ook door. Hier is Tom met de volgende opdracht.

TOM

Nou, de image is aangevraagd. De data is onderweg, klaar om helemaal uit elkaar gehaald te worden door het team van Mark van CNI. En als je nou zelf zin hebt om mee te helpen, dan is deze informatie altijd weer beschikbaar op operatiepositron.nl en dit keer heel veel goodies. We hadden al eerder gezien dat de volgende hub aan het pullen was op Pannenkoekenpalazzo via https. Maar wij zagen geen Diffie-Hellman en dat biedt mogelijkheden.

LIESBETH

Dit was de vierde aflevering van De Dienst en podcast van de AIVD. Gepresenteerd door mij, Liesbeth Rasker, en geproduceerd door Het Podcast Kantoor in samenwerking met Werk Merk. 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 podcastapp.