20 maart 2014

Vanaf vandaag log ik nooit meer onbeschermd in op een openbaar wifi-netwerk. Met een hacker onderzocht ik de openbare wifi van een paar koffiezaken en het bleek kinderlijk eenvoudig om van willekeurige mensen berichten, wachtwoorden, geslacht, seksuele voorkeur, afkomst, hobby's, koopgedrag en zelfs bankgegevens te achterhalen.

Dit geef je allemaal prijs als je inlogt op een openbaar wifi-netwerk

Correspondent Technologie & Surveillance

Maurits Martijn

Illustratie: Esther Aarts (voor De Correspondent)

In de rugzak van Wouter Slotboom (34) zit een klein zwart apparaatje, iets groter dan een sigarettenpakje, met een antenne eraan. Ik ontmoet Wouter op een willekeurig terras in de binnenstad van Amsterdam. Het is zonnig, bijna alle tafels zijn bezet. Sommige mensen praten met elkaar, anderen werken op hun laptop of spelen met hun smartphone.

Wouter pakt zijn laptop uit zijn rugzak, legt het zwarte apparaatje op tafel en verbergt het onder een menukaart. We bestellen koffie bij de serveerster en vragen het wachtwoord van het wifi-netwerk. Intussen zet Wouter het apparaatje en zijn laptop aan. Hij start wat programma's op en zijn scherm vult zich met regels groene tekst. Langzaam wordt duidelijk dat het apparaatje van Wouter contact legt met de laptops, smartphones en tablets van de terrasbezoekers.

Op zijn scherm verschijnen woorden als 'iPhone van Joris' en 'MacBook van Simone.' De antenne van het apparaatje vangt de signalen op die de laptops, smartphones en tablets afgeven.

> *Martin is op vliegveld*
> *Heathrow geweest, slaapt waarschijnlijk in het White Tulip Hostel en heeft coffeeshop*
> *The Bulldog bezocht*

Er verschijnt meer tekst op het scherm. We kunnen van alle apparaten die contact hebben gemaakt met het zwarte apparaatje, zien op welke wifi-netwerken zij al eerder zijn aangesloten. Soms zijn dat onherleidbare namen met veel cijfers en letters, maar vaker dragen de wifi-netwerken de naam van de locatie waar ze bij horen.

We zien dat dezelfde Joris een McDonalds heeft bezocht, waarschijnlijk in Spanje op vakantie is geweest (veel Spaanstalige netwerknamen) en weleens heeft gekart (hij heeft ingelogd bij een bekend kartcentrum in het westen van het land). Een andere terrasbezoeker, Martin, is ingelogd geweest op het netwerk van vliegveld Heathrow en de Amerikaanse vliegtuigmaatschappij Southwest. In Amsterdam slaapt hij waarschijnlijk in het White Tulip Hostel. Hij heeft ook coffeeshop The Bulldog bezocht.

Sessie 1: iedereen laten inloggen op ons nepnetwerk

De serveerster brengt onze koffie en geeft ons het wachtwoord van het wifi-netwerk van het café. Nadat Slotboom is ingelogd, is hij in staat om het hele terras van internet te voorzien en al het internetverkeer door het kleine apparaatje te laten stromen.

De meeste smartphones, laptops en tablets zoeken automatisch naar een wifi-netwerk. Het liefste vinden ze een wifi-netwerk waar zij al eerder op aangesloten zijn geweest. Als je weleens in de trein bent ingelogd op het T-Mobile-netwerk, dan vraagt jouw apparaat zich constant af: is er een T-Mobile-netwerk in de buurt?

> *Mijn telefoon logt vanzelf in op een van deze netwerken, die dus in werkelijkheid allemaal bij het zwarte apparaatje horen*

Het apparaatje van Slotboom is in staat om die zoekpogingen te registreren en zich voor te doen als de bekende, vertrouwde wifi-netwerken van de terrasbezoekers. Ik zie bijvoorbeeld dat in de lijst van beschikbare netwerken op mijn iPhone opeens de naam van mijn thuisnetwerk verschijnt, dat van mijn werk en van een hele trits openbare plekken die ik heb bezocht (cafés, hotellobby's, treinen). Mijn telefoon logt vanzelf in op een van deze netwerken, die dus in werkelijkheid allemaal bij het zwarte apparaatje horen.

Slotboom kan ook zelf een gefingeerde naam geven aan het netwerk, waardoor de gebruikers denken dat ze zijn aangesloten op het netwerk van het café. Als een café bijvoorbeeld een wifi-netwerk heeft met willekeurige letters en cijfers ('FRITZBOX XYZ123') dan kan Slotboom het netwerk de naam van het café geven ('Starbucks'). Daar loggen mensen veel sneller op in, vertelt hij.

We zien dat steeds meer terrasbezoekers inloggen op *ons* netwerk. De sirenenzang van het kleine zwarte apparaatje is onweerstaanbaar. Al twintig smartphones en laptops zijn van ons.

Slotboom kan nu, als hij wil, iedereen die op ons is aangesloten totaal ruïneren. Hun wachtwoorden achterhalen. Hun identiteit stelen. Hun bankrekening plunderen. Later vandaag zal hij laten zien hoe hij dat zou aanpakken: ik geef hem toestemming mij te hacken en te demonstreren wat hij allemaal kan. Maar hij zou het met iedereen met een smartphone die zoekt naar een netwerk of met een laptop die inlogt op een wifi-netwerk kunnen doen. Zelfs, in bijna alle gevallen, als die netwerken beveiligd zijn. Dan duurt het alleen iets langer.

Alles valt te kraken

Dat openbare wifi-netwerken onveilig zijn, is geen nieuw verhaal.(*Lees bijvoorbeeld hier hoe Alexander Klöpping inlogde op de Facebook-accounts van bezoekers van de Coffee Company.)* Maar het is wel een verhaal dat niet vaak genoeg verteld kan worden. Er zijn in Nederland nu 8,5 miljoen smartphonebezitters en 7 miljoen tableteigenaars. Naar schatting hebben bijna tien miljoen Nederlanders een laptop. Grote kans dat nagenoeg iedere Nederlander met één van die draagbare apparaten weleens is ingelogd op een openbaar wifi-netwerk. In het café, in de trein, in een hotel.

Er zijn maatregelen (*Drie maatregelen die je kunt treffen.)* te treffen om je internetverkeer beter te

beschermen als je een wifi-netwerk opgaat. Bovendien zijn sommige wifi-netwerken beter beveiligd dan andere. Sommige mail- of sociale mediadiensten maken gebruik van veiligere versleutelingstechnologieën dan hun concurrenten.

Maar loop een dag met Wouter Slotboom door de stad en je komt er achter dat ongeveer alles en iedereen via een wifi-netwerk te kraken valt. Vorig jaar, zo blijkt uit de Veiligheidsmonitor (*De veiligheidsmonitor 2013 van het CBS)* van het Centraal Bureau voor de Statistiek, waren meer dan 850.000 Nederlanders slachtoffer van *hacking*, variërend van inbraak op een computer of smartphone tot het inloggen op iemands e-mail- of facebookaccount. Bijna 60.000 Nederlanders waren slachtoffer van succesvolle zogenoemde *phishing*- of *pharming*-aanvallen, waarbij betalingsgegevens via gehackte computers of websites van gebruikers worden ontfutseld.

> Vorig jaar waren meer dan 850.000 Nederlanders slachtoffer van hacking, variërend van inbraak op pc of smartphone tot het inloggen op iemand e-mail of Facebook-account

Rapport na rapport toont aan dat digitale identiteitsfraude een steeds vaker voorkomend probleem is. Nu hebben hackers en cybercriminelen veel verschillende trucs tot hun beschikking.

Maar open wifi-netwerken maken het ze wel heel erg makkelijk. Het Nationaal Cyber Security Centrum, een afdeling van het ministerie van Veiligheid en Justitie, adviseert niet voor niets: 'Het is af te raden in openbare plaatsen van een publiek wifi-netwerk gebruik te maken. Als u dat toch doet, vermijd dan werk of financiële activiteiten.'

Ik heb Wouter Slotboom verzocht om vandaag deze demonstratie te geven. Hij is een 'ethisch hacker,' een *good guy*, een techneut die wil laten zien wat de gevaren kunnen zijn van internet en technologie. Hij adviseert individuen en bedrijven hoe zij zichzelf beter kunnen beschermen. Dat doet hij meestal door, zoals vandaag, gewoon te laten zien hoe simpel het is om schade toe te brengen.

Want kinderspel is het. Het apparaatje is goedkoop, de software die nodig is om het verkeer af te lezen werkt heel simpel en is gewoon te downloaden. 'De enige benodigdheden zijn 70 euro, een gemiddeld IQ en een beetje geduld,' zegt hij. Om de liefhebbers van kinderspelletjes niet al te veel tegemoet te komen, zal ik in dit verhaal zo min mogelijk ingaan op de technische aspecten, zoals de apparatuur, de software en de te downloaden apps.

Illustratie: Esther Aarts

Sessie 2: naam, wachtwoord en seksuele voorkeur scannen

Bewapend met Slotbooms rugzak verplaatsen we ons te voet naar een koffiezaak die niet alleen bekend staat om de prachtige bloemetjes op het melkschuim van de caffè latte, maar ook om de vele zzp'ers die er overdag op hun laptop zitten te werken. Deze vestiging is vandaag afgeladen met

mensen die geconcentreerd naar hun beeldscherm kijken.

Slotboom start zijn apparatuur op. Er gebeurt exact hetzelfde als net: binnen een paar minuten zijn er een stuk of twintig apparaten verbonden met ons apparaat. We zien weer de Mac-adressen en hun inloggeschiedenis en sommige namen van apparaten. Op mijn verzoek gaan we nu een stap verder.

Slotboom start een ander programma (ook eenvoudig te downloaden) en is nu in staat om veel meer informatie over de aanwezige smartphones en laptops te achterhalen. Zo zien we de specificaties van de telefoontypen (bijvoorbeeld: Samsung Galaxy S4), de taalinstellingen van verschillende apparaten of de versie van het besturingssysteem (bijvoorbeeld iOS 7.0.5).

> *We zien dat een van de aanwezigen de app van homodatingsite Grindr op zijn smartphone heeft staan*

Dat laatste is enorm waardevolle informatie voor een kwaadwillende hacker: als een apparaat een verouderd besturingssysteem heeft dan zijn er online altijd wel 'bugs,' gaten in het beveiligingssysteem te vinden. Als je die informatie hebt dan weet je hoe je het besturingssysteem binnen kunt treden en het apparaat over kunt nemen. Een steekproef in de koffiezaak wijst uit dat geen van de aanwezige apparaten het meest recente besturingssysteem heeft gedownload en dat van al deze verouderde systemen online een bug is te vinden.

We kunnen nu meer van het daadwerkelijke internetverkeer van de aanwezigen zien. We zien dat iemand met een MacBook Nu.nl bekijkt. Op Slotbooms scherm verschijnen namen van apparaten die bezig zijn om via WeTransfer documenten te versturen of contact maken met Dropbox of actief zijn of Tumblr. We zien dat iemand net is ingelogd op FourSquare. De naam van deze persoon verschijnt ook. We googelen hem en zien dat hij een paar meter van ons vandaan zit.

Ook van degenen die *niet* aan het werk of aan het surfen zijn komt informatie binnen. Veel mailprogramma's en apps maken constant contact met hun servers. Dat is nodig om, bijvoorbeeld, nieuwe e-mail op te halen. Wij kunnen van sommige apparaten en programma's zien welke informatie er naar welke server wordt gestuurd.

En nu wordt het echt intiem. We zien dat een van de aanwezigen de app van homodatingsite Grindr op zijn smartphone heeft staan. We zien de naam van zijn smartphone en het type (bijvoorbeeld iPhone 5s).

We doen het niet, maar aan de hand van andere informatie die zijn smartphone afgeeft zou het een koud kunstje zijn te achterhalen om welke bezoeker van de koffiezaak het gaat. Ongeveer tegelijkertijd zien we dat iemands telefoon contact probeert te maken met een Russische mailserver en daarbij het wachtwoord meestuurt. Ook dat is door ons uit te lezen.

Sessie 3: studie, hobby's en relatieproblemen inzien

Veel apps, programma's, sites en software maken gebruiken van versleutelingstechnologieën die er in principe voor zorgen dat de informatie die verstuurd en ontvangen wordt, niet door onbevoegden te lezen is. Maar als de gebruiker eenmaal inlogt op 'ons' wifi-netwerk, dan kan die beveiliging vaak met een ontsleutelprogramma relatief simpel worden omzeild.

Tot ons beider verbazing zien we informatie die een app over een aanwezige bezoeker verstuurt naar een bedrijf dat online advertenties verkoopt. We zien onder andere: de locatiegegevens, type-informatie over de telefoon en informatie over het wifi-netwerk.

Ook zien we de naam (voor- en achternaam) van een vrouw die gebruikmaakt van '*social bookmarking*'-site Delicious, een sociaal netwerk waar gebruikers interessante sites (*bookmarks*) met elkaar delen. In principe zijn de pagina's van Delicious-gebruikers openbaar. Toch voelen we ons voyeurs als we zien hoeveel we aan de hand van deze informatie over deze vrouw te weten kunnen komen.

Eerst googelen we haar naam, waardoor we direct op basis van haar foto kunnen bepalen wie het is en waar ze in de koffiezaak zit. We komen erachter dat ze uit een ander Europees land komt en pas sinds kort in Nederland woont. Het is maar goed dat Slotboom en ik met elkaar fluisteren: via Delicious ontdekken we dat ze een paar maanden geleden een site van een taalcursus Nederlands heeft gebookmarked én een site met informatie over de Nederlandse inburgeringscursus.

> We zijn nog geen twintig minuten binnen en we weten hoe ze heet, waar ze vandaan komt, waar ze gestudeerd heeft, dat ze geïnteresseerd is in yoga en dat ze tips zoekt hoe je een relatie redt

We zijn nog geen twintig minuten binnen en we weten al hoe de vrouw heet die op vier meter afstand van ons zit, waar ze vandaan komt, waar ze gestudeerd heeft, dat ze geïnteresseerd is in yoga, een aanbieding voor een anti-snurkmatras heeft gebookmarked, recent in Thailand en Laos is geweest en opvallende interesse toont voor sites die tips geven hoe je een relatie kunt redden.

Slotboom laat nog wat hackertrucjes zien. Zo kan hij een app op zijn telefoon de opdracht geven dat iedereen die een bepaald woord op een site tegenkomt (bijvoorbeeld 'Opstelten') een ander woord te lezen krijgt (bijvoorbeeld 'Dutroux'). We testen het en het werkt. Of dat iedereen die een foto op een site laadt, een foto die door Slotboom is uitgekozen te zien krijgt. Grappig als je kattenkwaad uit wilt halen, maar het maakt het ook mogelijk om op iemands smartphone, bijvoorbeeld, afbeeldingen van kinderporno te laden, waarvan het bezit strafbaar is.

Illustratie: Esther Aarts

Wachtwoord onderschept

We bezoeken nog één café. Mijn plan was om ook met een trein te gaan reizen en naar het gemeentehuis te gaan, maar onze beperkte steekproef heeft het probleem met wifi-netwerken nu wel duidelijk gemaakt. Mijn laatste verzoek aan Slotboom is om te demonstreren wat hij zou doen als hij mij echt schade toe wil brengen. Hij vraagt mij naar Live.com (het mailprogramma van Microsoft) te surfen en daar een willekeurige gebruikersnaam en wachtwoord in te toetsen. Enkele seconden nadat ik dat gedaan heb, verschijnen die gegevens op zijn scherm. 'Nu heb ik de inloggevens van je mail. Het eerste dat ik dan zou doen is het wachtwoord van je mail veranderen en bij andere diensten die je gebruikt aangeven dat ik het wachtwoord ben vergeten. De meeste mensen gebruiken hetzelfde e-mailaccount voor alle diensten. En die nieuwe wachtwoorden

komen dan dus binnen in jouw mailbox, zodat ik die ook tot mijn beschikking heb.'

We doen hetzelfde met Facebook: Slotboom is in staat om vrij makkelijk de door mij ingevoerde inlog- en wachtwoordgegevens te onderscheppen .

> *In twintig minuten slaagt hij erin mijn inloggegevens en wachtwoorden van Live.com, SNS-bank, Facebook en DigiD te bemachtigen*

Een andere truc is dat Slotboom mijn internetverkeer omleidt. Hij geeft zijn programma de opdracht dat ik, als ik surf naar bijvoorbeeld SNS.nl of DigiD.nl, uitkom op een site van hem. Een gekloonde site, die voor de bezoeker identiek lijkt aan de vertrouwde site, maar die volledig onder controle is van Slotboom. *DNS-spoofing,* in jargon. De gegevens die ik op de site achterlaat worden op de server van Slotboom opgeslagen. In twintig minuten slaagt hij erin mijn inloggegevens en wachtwoorden van Live.com, SNS-bank, Facebook en DigiD te bemachtigen.

De boodschap is nu wel overgekomen. Ik ga nooit meer onbeschermd een openbaar wifi-netwerk op.

Alle namen in dit stuk zijn gefingeerd, behalve die van Wouter Slotboom. We hebben de onderschepte data met de grootst mogelijke zorgvuldigheid behandeld en direct na het bezoek aan het laatste café gewist.