19 april 2018

Naoufal F., bijgenaamd Noffel en kopstuk van de Mocro Maffia, is deze week veroordeeld tot 18 jaar cel voor een mislukte liquidatie. Als bewijsmateriaal gebruikt Justitie data uit een massale hack van speciaal beveiligde telefoons van Ennetcom. Zijn advocate Inez Weski verzette zich hier tegen. Deze uitspraak betekent impliciet dat de rechter dit type bewijsmateriaal toelaatbaar acht. Maar de manier waarop Justitie een sleepnet door zulke data haalt, verdient een veel bredere discussie dan alleen in deze ene rechtszaak.

Arnout Jaspers
Redacteur wiskunde en nieuwsredacteur

Het sleepnet van Justitie

Wat mag wel en wat niet met data uit gehackte telefoons?

Auteur: Arnout Jaspers | 18 april 2018

Arnout Jaspers voor NEMO Kennislink

Justitie gebruikt primitieve en onbetrouwbare methoden om bewijsmateriaal te vergaren uit grote databestanden, zegt data-onderzoeker David Graus. Hij hoopt dat dit niet de manier is waarop de overheid sleepnetten door onze internetdata gaat halen.

Waarschijnlijk gaat menig topcrimineel jarenlang spijt krijgen van zijn blinde vertrouwen in de PGP-telefoons van Ennetcom. In maart 2017 werd bekend dat de Nederlandse justitie anderhalf miljoen e-mails en

tekstberichten heeft ontcijferd die met deze telefoons zijn verstuurd. PGP-encryptie is niet te kraken als het goed gebruikt wordt (zie het kader over PGP onderaan dit artikel), en uiteraard geeft Justitie zelf geen details, maar mogelijk is Ennetcom slordig omgesprongen met het genereren van de geheime sleutels voor de telefoons. (https://www.crimesite.nl/zo-kreeg-politie-pgp-sleutels-handen/)

In de rechtszaak tegen Naoufal F. ('Noffel') speelt bewijsmateriaal uit deze hack een sleutelrol. Noffel wordt er van beschuldigd dat hij een grootschalige drugshandelaar is, en opdracht heeft gegeven tot een liquidatie. Je zou kunnen denken: als hij dat klip en klaar heeft opgetikt in een bericht via zo'n gehackte Ennetcom-telefoon, dan is de zaak rond. Maar zo simpel is het niet.

Laten slapen

Zelfs via die 'onkraakbare' telefoons stuurde men vaak berichten waarin mensen schuilnamen hadden, en gevoelige termen als 'drugs' of 'doodschieten' werden vervangen door woorden als 'fruit' en 'laten slapen'. Althans, dat zegt Justitie, maar de verdediging vindt dat dit eerst nog maar eens bewezen moet worden.

Een ander probleem is dat geen mens die hele database van anderhalf miljoen berichten, afkomstig van ruim dertigduizend afzenders, in z'n geheel kan doorspitten. Dus is er door het Nederlands Forensisch Instituut (NFI) een automatische selectie gemaakt.

Schets van de twee-traps dataselectie in de rechtszaak tegen Naoufval F. De dataselectie was in feite nog een stuk onoverzichtelijker (zie afbeelding hieronder).

David Graus

Het NFI selecteerde eerst met het Google *langdetect*-programma alleen de Nederlandstalige berichten, waardoor ongeveer twee op de drie afvielen. Vervolgens doorzocht het die dataset met Hansken. Dit is een zoekmachine (https://www.forensischinstituut.nl/forensisch-onderzoek/hansken) die door het Nederlands Forensisch Instituut (NFI) speciaal ontwikkeld is om grote hoeveelheden data te doorzoeken op mogelijk bewijsmateriaal.

Zoekmachine Hansken (https://www.forensischinstituut.nl/forensisch-onderzoek/hansken) gebruikt een algoritme dat al sinds de jaren tachtig vrij beschikbaar is: *term frequency- inverse document frequency.* Stel, je beschikt over een groot aantal e-mails, en je wilt zo veel mogelijk te weten komen over het transport van drugs – codewoord 'fruit' – door verdachte Youssef. Als je dan de trefwoorden 'Youssef', 'fruit' en 'vrachtwagen' opgeeft, zoekt het algoritme de e-mails waarin deze woorden het meeste voorkomen, maar wel met een extra afweging: een trefwoord geldt als des te specifieker – en weegt daarom zwaarder – naarmate het in minder e-mails voorkomt. Op deze manier voorkomt het algoritme, dat nietszeggende trefwoorden als 'het' of 'zijn', die in vrijwel elke e-mail zullen voorkomen, het resultaat beïnvloeden. Sinds de jaren tachtig zijn echter veel slimmere algoritmes ontwikkeld om teksten op een bepaald onderwerp te doorzoeken.

David Graus, aan de Universiteit van Amsterdam gepromoveerd in zoekmachinetechnologie en digitaal forensisch onderzoek, werd door Inez Weski, de advocaat van Noffel ingehuurd. Hij sprak met de betrokken forensisch deskundigen en schreef een rapport over zijn bevindingen. Graus: "Een forensische zoekmachine doet *high recall search,* en dat is iets heel anders dan de *high precision search* zoals bijvoorbeeld Google doet." Van Google wil je dat die de meest relevante hits oplevert, en liever niet heel veel. Maar forensisch onderzoekers willen juist zoveel mogelijk bewijsmateriaal uit de data halen.

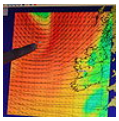
Uitgelicht door de redactie

WISKUNDE

Het platte vlak heeft minstens vijf kleuren nodig

BIOLOGIE

Leven op één pil per dag



BIOLOGIE

Op de eerste rij in Gods theater

Dataset Tandem

Hansken doet dit door simpelweg te zoeken op basis van een lijstje zoektermen die door de gebruiker wordt ingevoerd. In dit geval leverde het NFI namen en bijnamen van verdachten. Dat leverde een dataset op van ongeveer veertigduizend berichten, onder de naam Tandem, waar advocate Weski haar pijlen op richt. Met *high recall search* is het onvermijdelijk dat je ook grote aantallen irrelevante berichten selecteert. Graus verbaast zich over deze primitieve methode. Volgens hem zijn er al sinds de jaren tachtig betere, contextgerichte methoden ontwikkeld om data op bepaalde onderwerpen te doorzoeken.

Diagram van de dataselectie door het NFI en het Team High Tech Crime op de Ennetcom-dataset. Het gebied met de rode stippen staat voor het bewijsmateriaal in de zaak tegen Noffel H.

Arnout Jaspers voor Nemokennislink

In feite zijn er drie 'zoekslagen' op de Ennetcom-data gedaan: nadat het OM de oogst van de eerste lijst zoektermen had bekeken, gaf de rechter-commissaris nog twee keer toestemming aan het NFI om, in opdracht van het OM, de zoektermen uit te breiden. De Tandem dataset is dus twee keer uitgebreid.

Daarnaast deed het Team High Tech Crime (THTC), een onderdeel van de landelijke politie, een andere selectie op de data, waarmee het beoogde specifiek de 'criminele conversaties' uit de Tandem-dataset te vissen. Dat deed het THTC door in alle berichten te zoeken naar een of meer woorden uit een 'topiclijst' van 116 termen. Aangezien ook via de Ennetcom-telefoons niemand het expliciet heeft over 'drugstransport', 'huurmoordenaar' of andere evident criminele zaken, bevat die lijst ook heel alledaagse woorden als 'hard', 'boot', 'fruit', 'meloen', 'vis' en 'vrachtwagen'. Hoe het THTC aan die lijst komt is onduidelijk; mogelijk is die handmatig samengesteld op basis van ervaringen van rechercheurs in eerdere onderzoeken.

Criminele conversaties

Om te bewijzen dat hun selectie specifiek de criminele conversaties uit Tandem vist, vermeldt het THTC in de processtukken dat gebruikers met nul hits op deze 116 zoektermen gemiddeld maar 5,6 gesprekken voeren, gebruikers met één hit gemiddeld 9,7 gesprekken, en gebruikers met twee of meer hits gemiddeld 183 gesprekken. Dat zou dan leiden tot de conclusie: "Hoe meer berichten van een adres in de data beschikbaar zijn, hoe duidelijker de mogelijk criminele relevantie van de inhoud van het berichtenverkeer naar voren komt." Een ongeldige redenatie, vindt Graus, aangezien de kans dat zulke algemene zoektermen in de berichten van een gebruiker voorkomen sowieso toeneemt naarmate die gebruiker meer berichten verstuurt. Graus: "Als een student van mij dit zou inleveren, zou dit echt niet door de beugel kunnen."

Graus vraagt zich ook af hoe het zit met ontlastende informatie. Stel, iemand stuurt een bericht waarin hij zegt dat hij X 'gaat laten slapen'. Dit bericht zal in Tandem terecht komen, maar als uit het antwoord duidelijk wordt dat dit een grapje over X betreft, komt dit dan ook in de dataset?

Een meer juridisch bezwaar is dat niet meer goed na te gaan valt hoe de selectie van Tandem precies tot stand gekomen is. Hansken is namelijk nog steeds in ontwikkeling door het NFI, en gedurende het zich over

maanden uitstrekkende onderzoek kwam zo ongeveer iedere drie weken een nieuwe versie uit. Maar in die opeenvolgende veranderingen kregen Graus en de verdediging geen inzage. Graus: “In wezen is Hansken een apparaat dat bewijsmateriaal genereert uit ruwe data, maar het apparaat verandert steeds.”

Boeven vangen

Dat Noffels advocate Weski er alle belang bij heeft om het bewijsmateriaal uit de Ennetcom-hack te ondergraven, zal duidelijk zijn. Maar al kan de selectie van de dataset en de transparantie van de methodes ongetwijfeld beter – zijn dit nu echt bezwaren waar de hardwerkende Telegraaflezer van wakker ligt? Die zal allicht denken: ‘hoe meer boeven je vangt, hoe beter.’

Maar wat zijn ‘boeven’? Graus wijst er op, dat van de 5500 gehackte accounts in de Tandem-dataset, er maar twee of 2 of 3 van belang zijn voor de rechtszaak tegen Naoufal F. Ennetcom is een Canadees bedrijf, en de rechter in Canada stelde als voorwaarde voor het ‘uitleveren’ van de gehackte data, dat de Nederlandse justitie er niet een sleepnet doorheen ging halen om bewijsmateriaal over alle mogelijke wetsovertredingen door alle gebruikers te verzamelen. Dus deze rechtszaak mag geen voorwendsel zijn, om ook bijvoorbeeld zwartspaarders tegen de lamp te laten lopen. Maar wie garandeert dat de Fiod niet over een tijdje ook een kijkje neemt in de Tandem-dataset?

Het automatisch doorzoeken van enorme hoeveelheden data is ook aan de orde bij de extra bevoegdheden die de AIVD krijgt onder de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Als *high recall search* op basis van heel algemene zoektermen de norm wordt bij het doorploegen van terabytes aan internetdata, zal dat enorme aantallen valse sporen en onterechte verdenkingen opleveren. Graus: “Je mag hopen dat ze bij de AIVD wat beters hebben.”

- *Het NFI verklaart via een woordvoerder dat ze over deze zaak niets kunnen zeggen tegen de media. Het THTC reageert niet op een verzoek om commentaar.*

Pretty Good Privacy (PGP)

PGP is op zich een mooi systeem, door Phil Zimmerman al in 1991 bedacht. Het principe is dat wanneer jij als zender een stuk tekst of een ander bestand wilt sturen naar een ontvanger, je dit versleutelt met een veilig symmetrisch systeem; bijvoorbeeld AES (Advanced Encryption Standard). Voor zowel het versleutelen als ontsleutelen van dit bestand gebruik je een random sleutel, die alleen voor het versturen van dit bestand aangemaakt is en die alleen jij en de ontvanger mogen weten. In de praktijk genereert je computer deze sleutel, die doorgaans 128 of 256 bits lang is, overeenkomend met een paar dozijn toetsenbord-tekens.

Uiteraard schiet je er niets mee op als je nu deze eenmalige sleutel in een e-mail aan de ontvanger stuurt: dat is net zo onveilig als hem het hele bestand onversleuteld e-mailen. Immers, de veronderstelling is dat de NSA of andere afluisteraars alles meelezen wat jij verstuurt. Maar nu komt de slimme truuk van PGP: de eenmalige sleutel verstuur je met een ander, asymmetrisch systeem (in de praktijk vrijwel altijd RSA). Zo'n systeem heeft twee sleutels: een publieke sleutel, om bestanden te versleutelen, en een geheime sleutel, om die bestanden weer te ontsleutelen. De ontvanger hoeft zijn publieke sleutel niet geheim te houden, integendeel, hij kan die op zijn facebook-pagina zetten. Iedereen kan daarmee bestanden versleutelen, die alleen met de geheime sleutel weer leesbaar te maken zijn, en die houdt de ontvanger natuurlijk wel geheim.

Dus jij versleutelt de eenmalige sleutel met de publieke sleutel van de ontvanger, en stuurt hem dit kleine bestandje samen met het AES-versleutelde bestand toe. Overigens is er allerlei software te downloaden – ook gratis – die dit allemaal achter de schermen voor je regelt, het enige wat je zelf hoeft te doen is een geheim wachtwoord kiezen.

Waarom zou je trouwens niet meteen het hele bestand versleutelen met de publieke sleutel van de ontvanger, en dat versturen? Het probleem is, dat asymmetrische systemen zeer rekenintensief zijn; het kost nogal wat tijd om een flink bestand daarmee te versleutelen. Symmetrische systemen als AES zijn veel sneller. Door beide te combineren, omzeilt PGP het geheime-sleutelprobleem terwijl het toch snel is.

Dit artikel publiceerde NEMO Kennislink op 18 april 2018