[TITEL]
RECONSTRUCTIE
HOE HET DIGITALE 'BROODSPOOR' NAAR DE JONGE HACKER LEIDDE

[INTRO]
Alarm bij KPN. Een hacker dringt diep door in het netwerk van vaste telefonie en internet. Team High Tech Crime volgde een spoor van digitale vingerafdrukken tot in een jongenskamer.

[KADER]
De KPN-zaak is op dit moment in behandeling bij de rechtbank. Dit verhaal neemt op geen enkele wijze een voorschot op de uitspraak van de rechter. Het verhaal is een belevenis van rechercheurs uit het Team High Tech Crime. 5 maart start een wervingscampagne voor dit team (zie kader).
Omdat de verdachte minderjarig is, vindt de zaak achter gesloten deuren plaats. Peter is niet de echte naam van de verdachte.

[LOPENDE TEKST]
Hij ligt op de grond. Tegen de vloer gedrukt door twee rechercheurs van het Team High Tech Crime, terwijl de hardstyle muziek op zijn kamer op vol volume onverminderd doorklinkt. Het spel is voor de 17-jarige jongen uit. Op de monitor van zijn pc staan diverse schermpjes open. Tijd om de pc af te kunnen sluiten gaven de rechercheurs hem niet.

Het hacken was voor de Barendrechter een hobby, zegt Pim Takkenberg, doorgewinterde rechercheur en teamleider van het Team High Tech Crime (THTC). 'Anderen sparen voetbalplaatjes, hij spaarde zo veel en zo groot mogelijke hacks.' Met de inlog-, bankpas-, examen-, toegangs- en al die andere gegevens die hij tegenkwam, deed de jongen weinig. Daar ging het hem niet om.

Maar dát wisten de rechercheurs van het THTC van de Landelijke Recherche nog niet toen ze twee maanden eerder op de late vrijdagmiddag van 27 januari – de jassen waren aan om het weekeinde te beginnen – een telefoontje kregen: KPN deed aangifte bij THTC van een hack in zijn systemen. Alarmfase rood, een incident met mogelijk nationale gevolgen. Het onderzoek krijgt de willekeurig gekozen naam CARPUE.
'Door zo'n telefoontje stijgt de spanning. Je wílt weten wat er aan de hand is', herinnert rechercheur Hessel Schut zich. Zes jaar geleden verruilde hij zijn baan als systeembeheerder bij de VPRO voor het avontuur, de veelzijdigheid, maar bovenal de maatschappelijke relevantie van het recherchewerk. De jassen gingen uit, er werd eten besteld. 'Gedachten vliegen door je hoofd: hoe erg is het, zal het telefoon- en internetverkeer in Nederland verstoord worden? Wordt het internet platgelegd? Dan kan niemand pinnen, dus ook geen boodschappen betalen?'
De rechercheurs moeten snel zijn. De hacker kan nog actief zijn en niemand weet wie erachter zit en wat hij of zij wil? Een lone wolf die wil chanteren? Een criminele bende die met bankgegevens rekeningen wil plunderen? Of een organisatie die het communicatieverkeer in Nederland wil ontregelen? Teamleider Pim: 'Ik riep alle aanwezigen bij elkaar voor een briefing. We verdelen taken, kijken wat bekend is, wie waarheen gaat, welke hackers we kennen. De volgende dag gaan we bij KPN informatie verzamelen.' Het is diep in de avond als de teamleden naar huis gaan.

De zaak zelf komt aan het rollen negen dagen eerder op woensdag 18 januari 2012, 1.12 uur 's nachts. Een zekere Guus Gielen, '@GielenG', uit Zuid-Korea richt zich op Twitter tot het KPN Webcareteam. 'I saw some abusive activities from one of your servers. I want tot DM you for more details. Please follow me on twitter.'
Het Computer Emergency Response Team van KPN, dat zulke meldingen onderzoekt, bevestigt dat een onbevoegd iemand berichten stuurt vanaf een KPN-server. KPN vraagt het beveiligingsbedrijf Fox-IT de impact ervan te onderzoeken.
De onderzoekers van Fox-IT troffen een hack aan, waarin de naam YUI voorkomt. 'YUI' noemt de hacker zich op internet en zo heet ook een knap Japans zangeresje, ontdekt een rechercheur later tijdens de verhoren van de verdachte. De hacker is dol op Japan, waar hij ooit is geweest. Hij drong sinds 15 januari binnen in honderden servers van KPN. Pim: 'Je weet dan alleen nog niet hóe diep. Kan hij bijvoorbeeld de vaste telefonie van KPN platleggen? Dat is tachtig procent van alle vaste lijnen in Nederland, inclusief alarmnummer 112.'

@GielenG blijkt een student te zijn van de KAIST Universiteit in Zuid-Korea. Met een verzonnen Nederlandse naam hoopte hij de aandacht te trekken van het KPN-webcareteam. Voor de tweet gebruikte de student een vertaalrobot-Nederlands. Hij wil meewerken aan een verhoor, dat als bewijsmateriaal kan dienen.
Plaatsvervangend Teamleider Team High Tech Crime, Gea Wind, vliegt 5 februari naar Zuid-Korea en krijgt alle hulp van haar Koreaanse collega's. 'Een dag na onze aankomst stond student 'Guus' op de stoep. Een droomscenario.' De Koreaanse student vertelt dat hij via de computer in contact met YUI kwam, toen deze de KAIST Universiteit had gehackt. YUI vertelde vol trots over diverse hacks van hem, waaronder de KPN-hack. 'Guus' gelooft hem eerst niet, totdat YUI gestolen data toont van door hem gehackte servers. Via Twitter waarschuwt 'Guus' KPN.

Ondertussen zoeken de THTC-collega's van Gea naar sporen. Maar dat sporenonderzoek kent beperkingen. Anders dan bij het onderzoek op een plaats delict, bevinden digitale sporen zich in een computersysteem, dat je niet met een lint af kunt zetten; het moet doordraaien. 'Net als de Rotterdamse haven. Die kun je niet even voor iedereen afsluiten, de economische schade is te groot', legt Hessel uit.
Om de hacker te vinden 'loopt' het THTC het spoor van digitale broodkruimels af - programma's, namen, hacksporen. De hacker blijkt de stepstone-methode te gebruiken. Deze methode, waarbij systeemlekken worden opgespoord, gebruiken meer hackers. Zoals een inbreker die door de wijk loopt, op zoek naar openstaande ramen en deuren of dingen als trappen die hem helpen binnen te komen. Bij KPN is het een oud beveiligingsprogramma, dat een lek kent. Door een mislukte automatische update viel de KPN-beveiliging terug op zijn oude systeem.
De digitale broodkruimels leiden naar Japan, Rusland. Hessel: 'Hij probeerde zich af te schermen door via een computer in een ander land in te loggen. Maar zoals een inbreker met een bivakmuts zich laat verraden door een zichtbare moedervlek, zo verraden specifieke woorden een hacker.'

Het onderzoekt duurt twee maanden. Dit lijkt aan de lange kant als je weet dat je een digitaal spoor in één dag kunt natrekken. Hessel: 'Nationale wetgeving in elk land verbiedt dat je voor onderzoek zomaar in computers in dat land snuffelt: je moet ernaar toe om een kopie te maken van die computer. Dat elk land andere wetgeving heeft, maakt dit extra complex.'
Van computer naar computer, van land naar land volgen rechercheurs YUI tot in elf landen waar hij systemen heeft gehackt. Ze komen steeds dichterbij. Uiteindelijk in Barendrecht, bij een pc op een huisadres, van de 17-jarige, die daarmee door het THTC als verdachte wordt gekenmerkt.

Met taps volgt het team in Driebergen de internetactiviteiten van de verdachte. Tot in een chat de naam YUI op het scherm verschijnt. Pim: 'Dezelfde naam die we bij de hacks zagen. De cirkel was rond.'
Om een goed moment voor de aanhouding te vinden brengen de rechercheurs via taps en fysieke observaties het volledige leven van Peter in kaart. Dat moment is cruciaal, de computer móet aan staan en aan blijven om te voorkomen dat de datasporen ontoegankelijk worden achter een wachtwoord. Daar helpt een 'jiggler' bij, een apparaat dat muisbewegingen nabootst en de pc niet uit laat vallen.

Dinsdagochtend 20 maart begint wolkeloos en fris. Hessel en zijn acht collega's posten in hun wagens. Ze wachten op het juiste moment voor een inval: wanneer Peter weer online gaat. Dat is eind van de ochtend. Actie! Vijf rechercheurs omsingelen het huis, vier gaan naar binnen, de trap op, op zoek naar Peter. Uit zijn kamer klinkt harde housemuziek. Met een klap knalt de kamerdeur open en grijpen twee rechercheurs Peter, die op de vloer van de kamer belandt. Ze voeren hem af. Na de aanhouding komt de rechter-commissaris voor het veiligstellen van sporen. Nu die er is, kunnen bewijsstukken mee: twee laptops, diverse bestandsdragers én de nog draaiende pc. Dan pas kan hij het volume van de muziek uit die pc zachter zetten. De housemuziek verstomt.

Epiloog
Peter legt snel een volledige bekentenis af in de verhoren. Vijf weken van verhoren leggen zijn activiteiten bloot. Andere gedupeerde organisaties en landen worden ingelicht. Naar verwachting wordt de zaak vóór de zomer door de rechter behandeld.

[KADER]
Vacatures
Het zestigkoppige Team High Tech Crime van de KLPD zoekt nieuwe krachten, dertig in totaal. Tijdens de Second Edition van de Cybercrime Challenge kunnen jongeren hun technische skills tonen. Dat kan op de Tek Tok-bijeenkomst, die dinsdag 5 maart van 20.00 tot 22.00 uur is in het Paard van Troje in Den Haag. Die staat volledig in het teken van de wervingscampagne voor dertig vacatures bij het Team High Tech Crime. Het interactieve programma wordt ook op internet uitgezonden.
www.tektok.nl

[KADER]
High Tech Crime
Met de digitalisering van de maatschappij gaan steeds meer criminelen online. Zo zijn er criminele organisaties die wereldwijd computers hacken en zo een netwerk bouwen waarmee ze systemen kunnen platleggen, zoals het BredoLab uit 2009. Het gaat om complexe vormen van cybercrime die vitale ICT-infrastructuur beschadigt of lamlegt en het vertrouwen van de burgers in het internet schaadt.

Om het groeiende aantal zaken het hoofd te bieden, groeit het in 2007 opgerichte Team High Tech Crime mee. De hightech-crimewereld verandert voortdurend: criminelen onderzoeken nieuwe technologische ontwikkelingen en kraken die, om die te misbruiken. Dit vraagt van het THTC om hoogwaardige expertise, creativiteit en de wil telkens grenzen te verleggen.

Ongeveer de helft van het aantal teamleden heeft een politieachtergrond, de andere helft komt van buiten de politie. Zij doen onderzoek, tappen, observaties, doorzoekingen, aanhoudingen, verhoren, dossiers opmaken, invallen enz.

Aantal medewerkers
2007 (start) 33
2012 60
2013 90
2014 119