

HOSTINGBEDRIJF

Het afvoerputje van het internet zit in een Noord-Hollands dorp



Over dit artikel

Keus voor initialen

Omdat Bap K. en Reinier van E. verdachte zijn in een strafrechtelijk onderzoek, worden hun achternamen met initialen aangeduid. Voor dit artikel heeft NRC met tientallen mensen gesproken die de mannen kennen en/of bij betrokken instanties werken. Het artikel is verder gebaseerd op onderzoeksrapporten, analyses van cybersecuritybedrijven, meldingen van anti-spam-organisaties, rechtbankstukken, Kamer van Koophandel-documenten, mailwisselingen, foto's en openbare informatie uit internetdatabases.

Aan het einde van de dag krijgt Armin een fles Bols mee als dankje. „Maar die moest ik op de terugweg leeggoeien bij de douane. Ik kon nog net één slok nemen.” Zijn meer dan honderd pagina's tellende dossier met bewijsmateriaal laat hij achter.

Een volle negen jaar later zit Armin zich in zijn pied-à-terre in Amsterdam tegenover twee verslaggevers op te vreten. „Hoe is het mogelijk dat dit nog bestaat?” Want op wat naamswijzigingen na is er weinig veranderd aan Ecate. Nog steeds is ontstellend veel hackverkeer, kinderporno en andere schadelijke informatie te herleiden naar het netwerk - laatst nog de rechts-radical website *Vizier op Links*, dat politici en activisten intimideert.

Het enige dat veranderd is, is de lijst met instanties die zich met niet al te veel succes met het bedrijf bemoeiden - de politie, de FIOD, het ministerie van Veiligheid en Justitie, Europol. Die lijst is alleen maar langer geworden, blijkt uit onderzoek van NRC. Vanuit een datacentrum in Noord-Holland verdienen de eigenaren van Ecate nog steeds goed geld aan hun afvoerputje van het internet.

Ondoorzichtig web

Een paar keer per week arriveert er per auto een opvallend duo uit Den Haag op een industrieterrein in Wormer. Het is Bap K., een 75-jarige man met getinte brillenglazen en zijn 34-jarige Haagse zakenpartner Reinier van E. - groot, kaal, afgetraind en in trainingsbroek. Vaak nemen ze twee honden mee naar hun werk. Ze blaffen vanuit de voortuin van het datacentrum naar voorbijgangers.

De zaken beginnen op 13 mei 2002. Bartholomeus Johannes K., dan 56 jaar, richt een bedrijf op, dat hij omdoopt in het 'automatise-

ringservicebureau' Colinks. Bap, zoals hij zichzelf noemt, is Den Haag geboren, heeft een tijd in Zuid-Afrika gewoond, en gaat nu geld verdienen in de snel groeiende hostingbusiness. Het stabiele Nederland is daarvoor een prima plek, met een betrouwbaar stroomnet en grote diepzee-internetkabels die aan land komen. Al gauw trekt Bap de handige Haagse tiener Reinier van E. aan voor de techniek.

Samen beginnen ze een hostingbedrijf: Bap doet de papieren en Reinier sleutelt aan de computers. Tegen betaling kunnen klanten bij hen een server huren om daar hun internetdienst op te draaien. Bap en Reinier regelen de computers, de stroom en de internettoegang - een beetje zoals een huisbaas een kamer verhuurt - en de klanten draaien vanaf die plek hun eigen handeltje op het internet. Wat klanten precies met hun gehuurde server doen, is aan hen. Sommigen knippen de serverruimte op in honderden stukjes en verhuren die weer door aan anderen.

In de jaren daarna spinnen Bap en Reinier een ondoorzichtig web aan bv's dat zich uitstrekt over meerdere landen. Als Reinier nog maar net meerderjarig is, richt hij met Bap de Britse 'limited' Ecate op, op een adres in Kent met honderden andere brievenbusfirma's. Hun andere hostingbedrijven, of variaties daarop, krijgen namen als Novogara, DataZone, Reba Communications, FiberXpress, B&R Holding, IQarus, Increserve en Linkup. Veel van deze bv's doen precies hetzelfde, op hetzelfde adres, onder een andere naam. Sommige bv's bieden zelf weer onderverhuur van servers aan, alsof de mannen klant zijn van zichzelf. Ook poppen er - volgens de autoriteiten aan de mannen toebehorende - bv's op als Quasi Networks en IP Volume, met onbekende bestuurders in de Seychellen. Ecate, een Britse bv, komt jaren na oprichting op naam van de klusjesman van het datacentrum, een man die in een flat in Zaandam woont.

Ruzie met brandbijl

Al in de allereerste jaren zijn er klachten over het duo. Als de mannen apparatuur bestellen die vervolgens niet wordt geleverd, staan ze ineens op de stoep om verhaal te halen, schrijft een handelaar in 2004 op een website. „Helaas gaat dat niet op een normaal nivo, en zijn dus klaar met hen.” Een ander moppert dat Bap en Reinier niet luisteren naar klachten over spam-ongewenste, in bulk verstuurde e-mail die meestal is bedoeld om geld af te troggelen - die van hun servers komt. „En zo hebben we nog een hele verzameling andere troep die die lui hosten”, schrijft iemand. „Ik heb het al aantal keer via hun [...] helpdesk geprobeerd, maar dat lijkt net een zwart gat.”

De ruwe stijl van zakendoen blijft. Na een ruzie in 2011 over een onbetaalde stroomrekening vertrekken Bap en Reinier uit een datacentrum in Alphen aan de Rijn, om er zelf een te beginnen. Ze betrekken het oude regionale computercentrum voor zorgverzekeraars in Wormer, twintig minuten boven Amsterdam. De onopvallende loods zit weggestopt aan het einde van een doodlopend straatje op het lokale industrieterrein. De gangen en hallen in het gigantische rekencentrum zijn groot en leeg, slechts een klein deel is in gebruik.

Aan de voorkant ziet het datacentrum eruit als een normaal bedrijf, met een keurig paadje naar een glazen entree, en het fris-blauwe logo van DataOne erboven. Een handjevol mensen wordt aangenomen voor techniek en onderhoud.

Maar achter de gevel gaat het er minder gelijk aan toe, vertellen mensen die er over de vloer kwamen. Achter het fornuis in de enorme industriële keuken staat de spierbundel Reinier vaak een pan vol eieren voor zichzelf te bakken. In een vat naast de puincontainers gaan regelmatig dingen in de fik, zien mensen in de

buurt. De sfeer is meestal amicaal, als de oude Bap weer eens opschept over vliegavonturen en alle vrouwen met wie hij heeft geslapen. Op hun gemak bespreken de twee dreigende rechtszaken. Maar de toon kan ineens omslaan. „Dan is het meteen schelden, 'rot maar op, kanker dit, kanker dat'”, zegt een betrokkene.

Eén keer zit de afgetrainde Reinier een klant achterna met een brandbijl, vertelt die klant. Hij kwam zijn computers weghalen en Reinier vond dat-ie recht had op een flinke som cash. De klant deed geen aangifte omdat hij zelf daarna Reinier weer „flink aantikte” met z'n auto.

Afgeschermd klanten

Het businessmodel van Bap en Reinier wijzigt over de jaren heen niet, zeggen betrokkenen. Dat model is: niks willen weten, niet thuisgeven, tegenwerken.

Dat werkt. De wet schrijft immers voor dat een hostingbedrijf niet kan worden vervolgd voor wat z'n huurders uitspoken. Een hostingbedrijf kan de inhoud van alle bytes op z'n servers ook niet kennen. Maar een hostingbedrijf moet wel in actie komen als het op de hoogte wordt gesteld van illegale informatie. De vraag is hoe snel, en hoe actief dat gebeurt.

In ruil voor geld - dikwijls in anonieme cryptovaluta als bitcoin - worden klanten juist afgeschermd door Bap en Reinier, zeggen betrokkenen. Als bij de hoster een officieel verzoek uit de VS komt om auteursrechtelijk beschermd materiaal weg te halen - een DMCA - dan doen de mannen daar niets mee, zegt één iemand die het zag gebeuren. „DMCA's gaan zo in de prullenbak.” Onderverhuurders adverteren er zelfs mee. „DMCA ignored”, leest een advertentie waarin ruimte in het „state of the art Ecate DataCenter, located in Amsterdam” wordt aangeboden. Ook spammers die maar ongewenste bulkmail blijven sturen, hoeven zich geen zorgen te maken, ziet anti-spam-organisatie Spamhaus. Na een klacht stopt het even, maar „na drie dagen”, zegt data-analist Carel Bitter, gaat het gewoon weer verder vanaf een andere plek in het netwerk. Hij stuurt een lijst met ruim 1.500 meldingen na over de jarenlange spam, malware en andere narigheid afkomstig van het netwerk van de mannen.

Het EOKM, het expertisebureau online kindermisbruik, stuit ook op een muur bij de twee. Als het meldpunt van het EOKM dubieus materiaal op het netwerk van de twee aantreft, stuurt het een melding naar het bedrijf van de mannen. Dat moet het dan offline halen - dat is afgesproken met de branche. Maar regelmatig moet het meldpunt eerst maar eens bij de klant van het Haagse duo aantonen dat het kind op het plaatje écht minderjarig is. Als de meldingen van het meldpunt al aankomen, want soms belanden ze in de spamfolder of blijkt het e-mailadres van het meldpunt ineens geblokkeerd, merken ze bij het EOKM. Het webformulier dat het duo heeft laten maken waarop akelige plaatjes kunnen worden aangemeld, is om onduidelijke redenen zo ingericht dat het maar vijf meldingen per uur aankan - onwerkbaar volgens het meldpunt.

Joviale toon

Treuzelen en trainieren is hun tactiek, zegt ook advocaat Jos Klaus die in 2013 tegen Ecate procedeerde voor een consortium van horlogemakers. Die zagen allerlei nepversies van hun dure horloges verkocht worden op sites die bij de hoster waren ondergebracht. De communicatie verliep zeer stroef. Op de eerste brief reageerde Bap pas na een week, vertelt Klaus. Toen Bap de ip-adressen van die sites had gekregen waar hij om had gevraagd, zei hij vervolgens dat hij de brief enkel in Word-formaat wilde ontvangen, niet in pdf, zegt Klaus. „Dat was omdat hij wilde 'knippen en plakken'.” Daarna gebeurde

Vanuit een datacentrum in Wormer runt een Haags duo een hostingbedrijf. Ze staan al jaren op de radar bij de autoriteiten wegens cybercriminaliteit, malware en kinderporno op hun netwerk. Dat hindert het duo niet.

Tekst **Carola Houtekamer** en **Rik Wassens** Illustraties **Roland Blokhuisen**



» Vervolg van pagina 25

er niets meer. Er zat voor Klaus niks anders op dan een zaak te beginnen en Ecatel moest van de rechter de websites offline halen.

Directeur Tim Kuik van auteursrechtenorganisatie Brein kreeg van de mannen te horen dat hij moet ophouden met het sturen van juridische geformuleerde klachtenbrieven, vertelt hij. „Ze wilden dat ik op joviale toon in een gesprek zou vertellen wat er mis was, en dan zouden ze wel eens kwijb.” Ze verstopten zich daarbij achter hun web van bv’s. In 2017 moest Kuik de mannen dagvaarden om ze iets te laten zeggen over één van hun buitenlandse bv’s. Ze ontkenden betrokkenheid en wezen naar hun klusjesman die was vooruitgeschoven als directeur. In de rechtszaal stond die nerveus z’n verhaal te doen.

Al die jaren blijven de klachten komen. Zeus, een groot botnet waarmee bankgegevens worden gestolen en gijzelsoftware op computers wordt gezet, blijkt mede op servers in hun beheer te draaien. Voetbalwedstrijden uit de Britse eredivisie, de Premier League, worden zonder toestemming van de organisatie via hun netwerk gestreamd. Klanten die bij bonafide internetbedrijven de deur worden gewezen, stappen over naar Ecatel. Een oud-werknemer van concurrent LeaseWeb: „Die zagen we dan weer opdruken bij Ecatel.”

Het Team High Tech Crime van de politie weet dat het niet klopt bij Ecatel. In de periode rond Jart Armins bezoek aan Driebergen in 2012 komen ze opvallend vaak in het oude rekencentrum in Wormer. Met regelmaat zijn buitenlandse opsporingsdiensten op zoek naar een klant van de twee. De Nederlandse politie komt dan op hun verzoek een server bij de mannen kopiëren.

Bap en Reinier doen meestal niet moeilijk over de komst van de politie, wie maakt hén wat? Eén keer is de politie er op verzoek van de VS, vertelt een betrokkene. Of ze een kopje koffie willen? Een rondleiding? Bij een diesel-agregaat vertelt Reinier grijnzend aan de politie dat-ie ‘m zelf heeft ingeregeld en de elektriciën een paar honderd piek heeft toegestopt om er een zegeltje op te plakken.

Kat-en-muisspelletje

Er zijn ook keren dat zo’n bezoek minder soepel gaat. Dan moet de politie dreigen met het inrammen van de voordeur als er niet snel open wordt gedaan. Maar het blijft een kat-en-muisspelletje zonder gevolgen. Voor een seriële strafrechtelijk onderzoek waarbij kwade opzet van Bap en Reinier wordt aangetoond, bestaat bij het Openbaar Ministerie volgens betrokkenen geen animo.

Intussen beginnen steeds meer instanties zich aan Ecatel te ergeren. De naam valt regelmatig in een werkgroep die de ‘notice and takedown’-gedragscode voor de hostingsector beheert. Die vrijwillige gedragscode is in 2008 op verzoek van de overheid opgesteld door de internetbranche en schrijft voor dat hostingbedrijven bij een melding van kinderporno of ander verboden materiaal, de informatie meteen offline halen.

De gedragscode werkt wel, zegt werkgroepvoorzitter Maarten Simon van domeinregistratieclub SIDN, maar de hoeveelheid kinderporno in Nederland bleef schrikbarend hoog. „Eén naam die jarenlang telkens naar voren kwam was Ecatel. Ze hadden de gedragscode nooit onderschreven en handelden er ook niet naar. Dat deed afbreuk aan de gedragscode.” Waarom wordt daar niks aan gedaan, vroeg Simon

aan de politie, het OM en het ministerie van Justitie die erbij zaten. „Het is lastig, zeiden ze. ‘Als we een bevel geven om iets te verwijderen, halen ze de informatie net op tijd weg.’” Alex de Joodse, nu compliance officer bij het internetknooppunt AMS-IX, zat bij die gesprekken. „Iedereen zei: we moeten wat tegen ze doen. Maar het had geen prioriteit. Het was blijkbaar geen spannend project.”

In 2015 stapt het Team High Tech Crime af op hoogleraar cybersecurity Michel van Eeten van de TU Delft. „De korpsleiding is er helemaal klaar mee om op internationale politie-conferenties aangesproken te worden op de rotzooi die in Nederland staat, zeiden ze. ‘Iedereen weet van Ecatel’, zeiden ze ook. Maar het was gebaseerd op anekdotes. Roddel, achterklap en slechte statistieken. De vraag was of wij hard konden maken welke Nederlandse hosters de meeste rotzooi verspreiden.”

Van Eeten hielp de politie met een ranglijst waarin hij de hoeveelheid schadelijke activiteit vanaf het netwerk – kinderporno, cyberaanval-len, spam en phishing – afzette tegen de omvang van het bedrijf, vertelt hij via Teams. Bij de top-tien zat inderdaad Ecatel. „Maar eigenlijk heb je daar niks aan. Je moet meten hoe bereidwillig een bedrijf is om slechtheid weg te halen. En zelfs daar heb je niks aan. Want een bewust kwaadwillende hoster zal juist z’n best doen om ergoed uit te zien en luisteren naar meldingen, terwijl hij aan de achterkant z’n klant bedient door bijvoorbeeld snel een site te verplaatsen.” Je moet eigenlijk aantonen dat een bedrijf moed-willig meewerkt aan criminaliteit, zegt Van Eeten. „Maar dat is heel moeilijk te bewijzen. Op die frustratie loopt de politie al jaren stuk.”

De sfeer verandert als in 2017 Ferdinand

Grapperhaus (CDA) aantreedt als minister van Justitie. Grapperhaus, weet iedereen al gauw, vindt de hoge plek van Nederland op de wereldwijde ranglijst als hostingland van kinderporno verbijsterend. Hij wil er echt wat aan doen. Tegen de *New York Times*, dat in een onderzoek naar drie beruchte kinderpornowebsites bij de mannen in Wormer uitkwam, zegt hij: „Ik realiseerde me de mate van de wreedheid niet, en hoe ver het gaat.” Op de sites stonden tussen de grote hoeveelheden foto’s van lachende kinderen in sexy poses ook expliciete en gewelddadige beelden met baby’s en peuters.

In maart 2018 gaat onder leiding van het ministerie van Justitie en Veiligheid een flinke groep mensen aan tafel. De landelijk officier kinderporno is er, de werkgroep voor de hosting-gedragscode, vertegenwoordigers uit de internetsector, afgevaardigden van Economische zaken, het EOKM, het team kindermisbruik van de politie uit Zoetermeer, hoogleraar Van Eeten van de TU Delft.

Detectiesysteem

Grapperhaus zet een paar zaken in gang. Er komt een technisch detectiesysteem voor kinderpornografisch materiaal – een *hashchecker* – waar hostingbedrijven zich op kunnen aansluiten. Plaatjes, verkregen uit strafzaken in binnen- en buitenland, die bij hun klanten staan en die in dat systeem voorkomen, kunnen dan automatisch verwijderd worden. Ambtenaren gaan nadenken over de oprichting van een ‘content-autoriteit’ die boetes op kan leggen aan weigerachtige hosters. Ook wordt de gedragscode een stuk minder vrijwillig. Aan een melding van het kinderpornomeldpunt moet zonder discussie binnen 24 uur gehoor worden gegeven en aan Van Eeten wordt gevraagd om te monitoren of bedrijven zich daaraan houden. Werken bedrijven niet mee, dan zal Grapperhaus – daartoe aangespoord door de Tweede Kamer – de ranglijst van Van Eeten vrijgeven: *naming and shaming*.

Dat levert eind 2020 een eerste publiek rapport op waar het hostingbedrijf IP Volume afwisselend op nummer 2 of 3 staat als beste vindplaats voor kinderporno in Nederland. Ondanks de inschrijving in de Seychellen gaan alle instanties ervan uit dat IP Volume vanuit Nederland opereert en tot de wolk aan internetbedrijfjes rond het Haagse duo behoort.

Maar op de vraag hoe snel IP Volume reageert op meldingen van het kinderpornomeldpunt, kan Van Eeten geen antwoord geven. In een brief van oktober 2020 aan de Kamer legt Grapperhaus zelf uit dat IP Volume „niet meewerkt



en zelfs (technische) belemmeringen opwerpt” tegen het meldpunt. Daarom doet de politie de meldingen, om deze een „dwingend karakter” te geven. Maar het helpt allemaal niet echt, constateert Grapperhaus ook – IP Volume blijft laks.

Vanaf zijn ‘rondetafel’ geeft de minister zijn ambtenaren de opdracht om uit te zoeken wat er dan strafrechtelijk kan worden gedaan tegen kwaadwillende hostingbedrijven. Dat blijkt heel moeilijk. Niet alleen moet worden aangetoond dat een bedrijf de klant bewust faciliteert, ook het bijzonder internationale karakter van het internet werkt tegen. Het is telkens de vraag wie verantwoordelijk is voor de illegale content, of dat er sprake is van onderhuur of doorsluizen naar een ander land. Wat als het land waar een klant staat geregistreerd niet mee wil werken aan een strafrechtelijk onderzoek? Wat als de klant onvindbaar is? Het internet is overal, en tegelijkertijd nergens.

Diefstal van ip-adressen

Eind 2019 komt er nóg een instantie op de lijst van autoriteiten die zich bemoeien met de Haagse mannen. Dat is Europol, het Europese politieagentschap. Die wordt erbij gehaald door de 67-jarige internetactivist en -onderzoeker Ron Guilmette, die zich aan de andere kant van de wereld in de VS zit te ergeren. Guilmette is een internetveteraan, hij werkte in de jaren tachtig aan internet toen het nog ARPAnet heette. Met spijt zag hij in de jaren erna aan hoe het mooie wetenschappelijke project, gebaseerd op vrijwillige afspraken tussen welwillende partijen, volliep met rotzooi en spam. Vooral aan spam kreeg hij een grote hekel. „Het is een rare fascinatie”, vertelt hij via Skype. „Ik wilde gewoon e-mail behouden voor de mensheid. Spammers verpesten dat.”

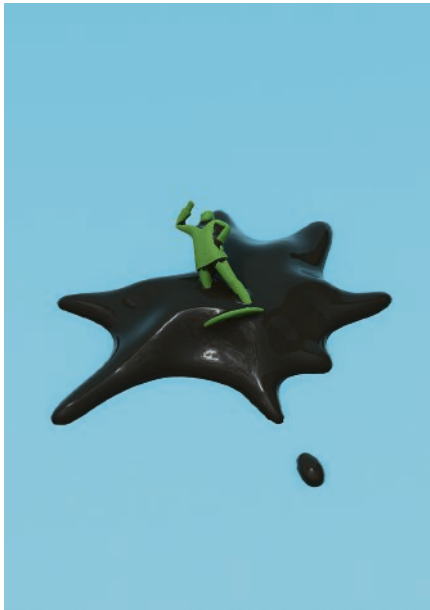
In zijn nachtelijke jachten op spammers stuitte Guilmette op iets vreemds: de diefstal van een enorme serie ip-adressen, met een straatwaarde van in de miljoenen dollars. De ip-adressen behoorden toe aan Afrikaanse bedrijven en organisaties, maar leken te worden beheerd door een klein bedrijfje in Wormer. Hij schreef er in grote woorden en op opgewonden toon over op mailinglijsten van netwerkoperators, maar reacties bleven uit.

Samen met een Zuid-Afrikaanse journalist vogelt Guilmette uit hoe de vermeende diefstal moest zijn gegaan. In een technisch vakblad beschrijven ze hoe een Israëlische zakenman bij de Afrikaanse internetautoriteit zou hebben gerommeld met de eigendomsinformatie van de ip-adressen. Ze beschrijven hoe de adressen bij een Limburgse zakenman zouden zijn beland en daarna beheerd worden door het netwerk van Bap en Reinier.

Het is geen toeval dat de dubieus verkregen Afrikaanse adressen belanden bij de twee, zegt Guilmette via Skype. „Iedereen, elke website, elk apparaat dat op internet zit, heeft een ip-adres nodig, anders komen de data niet aan”, doceert hij. „Maar zoals iedereen weet raken de ip-adressen op. En daarom zijn ze veel geld waard.” Kwaadwillenden hebben extra veel ip-adressen nodig, zegt hij ook. „Hun adressen worden vaak na een tijdje geblokkeerd door anderen, en dan moeten ze weer nieuwe adressen hebben voor hun spam en hun aanvallen.”

De artikelen leiden tot weinig vervolg, behalve dat de Afrikaanse internet-autoriteit begin dit jaar publiekelijk erkent dat er iets gek is met deze adressen en dat het sowieso 2,4 miljoen ip-adressen kwijt is.

Guilmette, gefrustreerd, neemt zelf in september 2019 contact op met Europol over het bedrijf van de twee Haagse mannen. Europol wil in gesprek met hem, samen met het Nederlandse Team High Tech Crime en de FIOD. Er volgt



een Skypegesprek met een groep agenten en ambtenaren, waarin Guilmette zijn vondsten uiteenzet. „Ze wilden van alles weten, en ze zouden laten weten wat ermee ging gebeuren. Maar daarna heb ik niets meer van hen gehoord.”

Op de ochtend van 22 september 2020 staan er twintig auto’s en busjes voor de deur van het datacentrum in Wormer, het parkeerterrein staat helemaal vol. De fiscale opsporingsdienst FIOD is groot uitgerukt. Bap en Reinier moeten mee, net als de klusjesman, maar die wordt na een verhoor meteen vrijgelaten. Bij het datacentrum wordt hij daarna niet meer gezien.

Op de website van het OM komt over de inval te staan dat de fiscus een „bulletproof hoster” is binnengevallen met zeven ondernemingen, waaronder minstens één op de Seychellen. Het OM denkt dat er voor tonnen te weinig belasting is betaald. „Veel klanten betalen met bitcoins en die inkomsten zouden via verhuulende constructies weggesluisd worden.” De FIOD neemt de administratie mee, 70.000 euro cash, tonnen aan bitcoins, vijf auto’s en twee tasers. Was dit de beste aanpak?

Alle routes waren doodgelopen en niemand bij de instanties wist meer wat te doen, zeggen meerdere betrokkenen. Dus toen is de FIOD er maar op afgestuurd. Los van elkaar verwijzen mensen naar de Amerikaanse gangster Al Capone. „Die kon ook nergens op worden betrapt, alleen maar op belastingontduiking.”

Of het afvoerputje nu is opgeschoond, moet nog blijken. Een tijd was het doodstil rond het oude rekencentrum, vertellen mensen, maar sinds kort rijden de auto’s weer af en aan.

Bap en Reinier willen niets kwijt over de inval. „Hoe komt u erbij dat het bericht van het OM op de website ziet op mij of op aan mij gelieerde bedrijven?”, schrijft Bap aan NRC.

Niet open voor gesprek

De mannen staan niet open voor een gesprek met de verslaggevers. Wel stuurt Bap drie keer schriftelijk art van vragen, waarin hij ontkent dat er vanaf zijn netwerk malware is verspreid, een botnet is aangestuurd, of nephorloges zijn verkocht. Maar wat hij het meest wil benadrukken is dat hij of zijn bedrijven géén rol spelen bij het verspreiden van kinderporno. „Wanneer iemand een melding maakt van iets wat bij wet verboden is, dan wordt daar direct actie op ondernomen”, schrijft hij.

Het is juist het kinderpornomeldpunt dat niet meewerkt, stelt Bap. Die sturen vaak foutieve meldingen met verwijzingen naar plaatjes die niet bij hen staan en weigert de *tool* te ge-

bruiken die hij heeft laten ontwikkelen om plaatjes te melden. Die tool kan nu wel meer dan vijf meldingen per uur aan, schrijft hij.

Bap vindt het onrecht dat minister Grapperhaus de naam van IP Volume noemt als bedrijf dat slecht reageert op kinderpornomeldingen, dat ligt aan die foutieve meldingen. „IP Volume heeft om een rectificatie bij de minister gevraagd.” Bovendien is hij niet de directeur van IP Volume, schrijft hij. Die zit op de Seychellen. Dat zijn zakenpartner Reinier wel de mail afhandelt voor IP Volume „betekent nog niet gelijk dat deze persoon bestuurder is”. Iemand moet toch een keer de stekker eruit trekken bij dit duo, moppert Ron Guilmette op Skype. „Twee mannen die zoveel rottigheid op het wereldwijde internet veroorzaken. Ik begrijp het gewoon niet. Het is echt een gebrek aan interesse van de internetgemeenschap en van de autoriteiten. En dat in het keurige Nederland.”

De internetgemeenschap doet vooral snog weinig. Op het internet, in feite een netwerk van kleinere netwerken, is niet iedereen met elkaar verbonden. Buren moeten data doorgeven. Als de bedrijven die IP Volume toegang geven tot de rest van het internet allemaal besluiten dat niet meer te doen, kan het bedrijf niet meer het internet op. *De-peering* heet dat, en heel sporadisch gebeurt dat.

Maar dat is zeer omstreken, zegt Guilmette. Dat gaat in tegen de vrijwillige, decentrale opzet van het internet. Nee, zeggen ze dus ook bij het grootste doorgeefluik, de Amsterdam Internet Exchange. Een woordvoerder: „Wij zijn alleen maar een snelweg, we gaan niet over de inhoud. We kunnen toch niet heel paternalistisch gaan kijken wat zo’n partij host?”

‘Druk werkt’

De mannen luisteren de laatste tijd iets beter, zegt directeur Arda Gerkens van het EOKM. Dit jaar ontving het meldpunt 24 meldingen van kinderporno. „Beduidend minder. Druk werkt.” Maar die druk moet dan wel blijven. Gerkens: „Alle hostingproviders krijgen met dit probleem te maken, sommigen meer dan andere. Er zitten erbij die het vuur uit de sloffen lopen om het zo snel mogelijk op te schonen. Bij sommigen kan het beter, maar die verwijderen wel zonder discussie binnen 24 uur het materiaal. En je hebt er één waar altijd gedonder is, en dat is IP Volume.”

Naar Spanhaus luisteren ze ook een beetje, zegt Carel Bitter. „Want als ze geblokkeerd worden, komen hun data niet meer aan.” Maar eigenlijk zou de politie de tent moeten opdoeken, vindt Bitter. „Het lijkt alsof er bij het OM niet genoeg wil is voor een goed onderzoek naar deze hele slechte hoster.” De cyberaanval-len treffen meestal geen Nederlandse doelen, de slachtoffers van kinderporno zijn doorgaans geen Nederlandse kinderen. „We hebben er blijkbaar niet genoeg last van.”

Bitter vraagt zich ook af waarom een hoster zo weinig hoeft te weten van de klandizie. „Banken moeten toch ook weten met wie ze zaken doen?” Een e-mailadres als contactgegevens zou niet genoeg moeten zijn.

Internetactivist Jart Armin blijft ook gefrustreerd achter. „Weetje, ik heb echt successen gehad. We zaten het *Russian Business Network* op de hielen. We hebben het beruchte hostingbedrijf McColo neergehaald. Dat Ecatel nog bestaat zie ik als één van mijn grootste mislukkingen.”

„Jullie zelfbeeld klopt niet”, zegt hij over Nederland. „Ik ben jaren geleden op een cybersecurity-congres jullie minister van Justitie tegen het lijf gelopen” – hij herkent vagelijk een foto van Ivo Opstelten. „Die vertelde ik over Ecatel. ‘Dat klopt niet’, had de minister gezegd. ‘Het Nederlandse internet is heel schoon. Dat checken we elke dag’. Zo denken jullie blijkbaar.”

Reacties

Bap K. ontkent dat er vanaf het netwerk van hem en Reinier van E. malware is verstuurd, botnets zijn aangestuurd of dubieuze horloge- of medicijnverkoop is geweest. De nominatie door Host Exploit was „onderdeel van een heksenjacht.” Hij wijst erop dat veel bona fide beveiligingsbedrijven gebruikmaken van hun diensten, en dat hun scanverkeer gedetecteerd kan worden als aanvalsverkeer. Tegen kinderporno treden hij en Van E. op.

K. ontkent verder dat Ecatel, of andere bedrijven onder zijn beheer, de verhuizing van slechte klanten faciliteert. Afgesloten klanten komen soms wel via een onderverhuurder weer online. „Dit probleem zie je bij elke provider. Het is helaas niet anders.” Ecatel bestaat sinds 2017 niet meer, en K. ging al in 2009 uit het bestuur van het bedrijf, benadrukt hij. Bedrijven die in 2021 nog adverteren met Ecatel, verspreiden „bewust foute informatie”.

K. gaat niet in op vragen waarom IP Volume internetverkeer doorstuurt naar de vermeende gestolen ip-adressen van de Afrikaanse internet-autoriteit. K. zegt niet de eigenaar van de ip-adressen te zijn en deze niet te gebruiken. „Deze ip-adressen behoren tot een partij uit Israël.”

Het Openbaar Ministerie en de Landelijke Eenheid van de politie laten weten niet te kunnen ingaan op concrete personen of bedrijven. Wel stelt het OM dit. „De kern van het probleem van *bad hosting* is dat de bestaande Europese en Nederlandse regulering van hosters beperkt lijkt en hoofdzakelijk is ingegeven vanuit (bedrijfs)economische overwegingen, privacybelangen en vrijheid van meningsuiting. De hostingbedrijven worden enkel gezien als doorgeefluik.”

Dat bemoeilijkt ook strafrechtelijk onderzoek, waarvoor een verdening van opzet door de hoster nodig is. Dat is heel moeilijk aan te tonen, schrijft het OM. De communicatie tussen klant en hoster kan niet zomaar gevorderd worden, omdat een hoster niet verantwoordelijk is voor die klant. De politie sluit zich daarbij aan.

De website van Vizioer op Links stond zestien dagen bij een klant van het datacentrum in Wormer. De klant verwijderde de site eind december van zijn netwerk vanwege veel klachten.

De klusjesman die in het datacentrum werkte en in 2015 directeur van Ecatel werd, heeft niet gereageerd op vragen van NRC.