Annotatie

Oerlemans, J.J.

Computerrecht 2016/175

Rechtbank Rotterdam 20 juli 2016, nr. 1096016713
(Mrs. N. Doorduijn, A.A. Kalk, C.M.A.T. van der Geest)
m.nt. J.J. Oerlemans*

ECLI:NL:RBROT:2016:5814

Verdachte wordt veroordeeld tot een gevangenisstraf van 36 maanden voor het medeplegen van witwassen van gelden verkregen door middel van TorRAT cybercrime in de jaren 2012-2013 en voor het leiden van een criminele organisatie.

[naam 1] [verdachte 1],
geboren te [geboorteplaats] op [geboortedatum] ,
niet ingeschreven in de basisregistratie personen,
wonende te [woonplaats] (Tsjechië) op het adres [adres 1],
raadsman mr. J.J.D. Doleweerd, advocaat te Amersfoort.

(,,,)

4 Waardering van het bewijs

4.1. *Inleiding*

Centraal in deze zaak staat een malware die in 2012 en 2013 door middel van spamruns en het internet werd verspreid en die TorRAT wordt genoemd. Deze malware had tot doel om fraude te plegen bij (rekeninghouders van) ING en de Rabobank. Kort gezegd komt het er op neer dat grote aantallen spammails met veelal aanmaningen of voorstellen voor een betalingsregeling werden verzonden. In die mails zat ogenschijnlijk een link naar een openstaande factuur of ander (pdf)bestand, maar in werkelijkheid betrof het een programma dat de malware op de computer van de gebruiker installeerde. De malware werd door een Command and Control server op het internet aangestuurd. Bij het gebruik van internetbankieren op een besmette computer kon zo het rekeningnummer, de naam van de begunstigde en de omschrijving van de betaling worden aangepast, zonder

4 Zie ook X.E. Kramer en H.L.E. Verhagen (m.m.v. S. van Dongen, A.P.M.J. Vonken), Mr. C. Assers 'Handleiding tot de beoefening van het Nederlands Burgerlijk recht. 10. Internationaal privaatrecht. Deel III. Internationaal vermogensrecht', Deventer: Wolters Kluwer 2015, nr. 1000 & 1001.

* Jan-Jaap Oerlemans is buitenpromovendus bij eLaw, het Centrum voor Recht en Digitale Technologie van de Universiteit Leiden en onderzoeker bij het WODC en de Defensieacademie.

dat dit voor de gebruiker van die computer (direct) zichtbaar was. Op deze wijze konden betalingen door de TorRAT malware worden gewijzigd en omgeleid naar de rekeningen van zogeheten money mules. Het voorgaande blijkt uit de aangiften van ING (bm 1 e.v.)[1] en de Rabobank (bm 3 e.v.) en uit onderzoek van Fox-IT (bm 23 e.v.), de politie (bm 25 e.v. en 33) en Trendmicro (bm 30) en staat op zich ook niet ter discussie.[2]

4.2. ***Relatie tussen TorRAT en de door de banken genoemde overboekingen***

Wat wel in geschil is, is of de overboekingen genoemd in (de bijlagen bij) de aangiften van ING en de Rabobank het gevolg zijn van de TorRAT malware. De officier van justitie stelt dat dit het geval is. Zij heeft ter onderbouwing daarvan bij requisitoir een overzicht overgelegd met diverse dwarsverbanden van verschillende onderzoeksbevindingen. De verdediging heeft betoogd dat de causaliteit zich niet laat vaststellen. Hiertoe is onder meer aangevoerd dat uit de aangiften en rapportages van Fox-IT niet blijkt hoe deze causaliteit is vastgesteld en dat ook uit de getuigenverhoren niet duidelijk is geworden wie de bijlagen bij de aangiften heeft opgesteld en op welke wijze dat is gebeurd. Verder is er in dit verband op gewezen dat getuige/deskundige Sandee heeft aangegeven wat er nodig is om de causaliteit vast te stellen en dat het overzicht van de officier van justitie daaraan niet voldoet. Meer in het algemeen is betoogd dat uit het dossier blijkt dat er in de pleegperiode verschillende virussen waren die gericht waren op banken en dat onvoldoende duidelijk is hoe de banken de in de aangiften genoemde bedragen aan TorRAT hebben toegeschreven.
De rechtbank overweegt hierover het volgende.
De verdediging voert terecht aan dat niet duidelijk is geworden wie de bijlagen bij de aangiften van de banken heeft opgesteld en aan de hand van welke criteria dat is gebeurd. Dit betekent dat niet reeds op basis van die aangiften aangenomen kan worden dat het inderdaad gaat om transacties die zijn veroorzaakt door de TorRAT malware. Daarvoor is aanvullend bewijs nodig. Bij de beoordeling daarvan kiest de rechtbank voor de hierna volgende aanpak.

1. Welke overboekingen zijn relevant voor de bewijsbeoordeling?

In de aangiften van de banken wordt een groot aantal overboekingen naar een substantieel aantal begunstigden genoemd. Niet al die overboekingen en begunstigden zijn relevant voor de vraag of de feiten bewezen kunnen worden. Zo gaat het bij feit 1 alleen om gelden die witgewassen zijn. Dat gebeurde, zoals hierna zal blijken, doordat geld van de rekeningen van money mules – al dan niet na verdere doorboekingen – werd opgenomen in contanten of werd gebruikt om bitcoins te kopen. Overboekingen die de banken hebben tegengehouden of veiliggesteld voordat de bedragen zijn opgenomen of doorgeboekt, zijn op zichzelf dus niet relevant voor de beoordeling of feit 1 bewezen kan worden. Voor feit 2 (criminele organisatie) geldt dit zelfs in sterkere mate. Voor dit feit is op zich niet vereist dat concrete overboekingen worden vastgesteld als gevolg van TorRAT. Feit 2 betreft immers het lidmaatschap van een criminele organisatie met bepaalde oogmerken, en niet individuele fraudegevallen.
Gelet op het voorgaande zal de rechtbank eerst ingaan op de begunstigden zoals die blijken uit de configuratiebestanden en daarna op diverse andere begunstigden waarvan de rechtbank van oordeel is dat die van belang zijn voor de vraag of feit 1 en/of feit 2 ten aanzien van een of meerdere verdachten bewezen kunnen worden. Overboekingen waarvan de officier van justitie bij requisitoir[3] heeft erkend dat deze niet zijn witgewassen en/of waarvan uit de aangiften van de Rabobank blijkt dat deze de bedragen heeft kunnen veiligstellen[4], blijven buiten beschouwing, tenzij deze relevant zijn om bepaalde dwarsverbanden aan te tonen.

2. De rekeninghouders uit de configuratiebestanden

Uit het onderzoek van Fox-IT blijkt dat de TorRAT malware werd aangestuurd door middel van configuratiebestanden. Die bestanden bevatten onder meer de bankrekeningnummers met namen van rekeninghouders waarnaar de malware geld moest overmaken. In § 3.7 van het rapport d.d. 22 maart 2013 van Fox-IT (bm 23) wordt een overzicht gegeven van die rekeningen/begunstigden. De juistheid van dat overzicht staat als zodanig niet ter discussie[5] en de rechtbank heeft ook geen enkele reden om daaraan te twijfelen. Gelet op wat bekend is over de werking van de malware is wettig en overtuigend bewezen dat de in de aangiften genoemde betalingen naar deze bankrekeningen in ieder geval het gevolg zijn van de TorRAT malware. Gelet op de grote schaal waarop overboekingen zijn gedaan naar uitgerekend money mules genoemd in de configuratiebestanden, kan een andere oorzaak van die overboekingen uitgesloten worden.

3. Overige relevante begunstigden

De rechtbank stelt ten aanzien van de navolgende begunstigden het volgende vast.
[begunstigde 1], SOL, [begunstigde 2] en [begunstigde 3]
Over deze vier begunstigden wordt het volgende vastgesteld:

– Op de rekeningen van deze vier begunstigden is (onder meer) ingelogd door middel van de IP adressen 95.211.10.3 en/of 95.211.13.35 in de maanden augustus en september 2012. Vanaf die IP adressen is ook ingelogd op de rekeningen van Stichting Aandelenbeheer

1 Voor de leesbaarheid wordt verwezen naar de bewijsmiddelen uit bijlage II bij dit vonnis, steeds aangeduid met 'bm' gevolgd door het nummer.

2 Weliswaar heeft de verdediging verzocht om tegenonderzoek tegen de bevindingen van Fox-IT, maar dat verzoek richt zich op de causaliteit tussen het TorRAT virus enerzijds en de individuele overboekingen die ING, de Rabobank en Fox-IT toeschrijven aan het virus anderzijds en niet zo zeer op het bestaan en de werking van het virus als zodanig.

3 Zie de 'aantekeningen i.v.m. causaal verband TorRAT', overgelegd bij requisitoir.

4 De overboekingen waarbij is aangegeven dat de feitelijke schade nihil is.

5 Zie voetnoot 2.

MBN en [begunstigde 4] (bm 38), twee van de begunstigden genoemd in de configuratiebestanden (bm 23).[6]
– Op de rekeningen van [begunstigde 1], [begunstigde 3] en [begunstigde 2] is tevens ingelogd vanaf het IP adres 95.211.92.234 (bm 38), welk IP adres ook is gebruikt in samenhang met de TorRAT spamrun via aangever 9yards (zie hierover de aangifte van 9yards (bm 9), de aanvullende verklaring van deze aangever met daarin voornoemd IP adres (bm 10) en het overzicht van de spamruns (bm 33)).
– Uit de aangifte van VOF Romijnders (bm 17) blijkt dat van de rekening van deze aangever zowel gelden frauduleus zijn overgeboekt naar S.O.L. B.V. als naar A.R. [begunstigde 5] (een van de begunstigden uit de configuratiebestanden, zie bm 23).

(…)

4. Slotsom ten aanzien van de causaliteit

De rechtbank is van oordeel dat voor de overboekingen naar de begunstigden uit de configuratiebestanden en de overige hiervoor genoemde begunstigden wettig en overtuigend bewezen kan worden dat deze het gevolg zijn van de TorRAT malware. Anders dan de verdediging is de rechtbank van oordeel dat niet per individuele transactie aan de hand van de sessiegegevens van de banken beoordeeld hoeft te worden dat het gaat om een overboeking als gevolg van deze malware. De combinatie van de aangiften en de hiervoor genoemde dwarsverbanden zijn naar het oordeel van de rechtbank toereikend bewijs van de causaliteit tussen de malware en een groot aantal overboekingen en er zijn geen of onvoldoende concrete feiten en omstandigheden aannemelijk geworden die daaraan afdoen (in de zin van de Meer en Vaart-jurisprudentie). Het is niet aannemelijk geworden dat een andere (banking) malware, of een andere dadergroep dan de daders achter TorRAT, (een deel van) deze overboekingen heeft veroorzaakt. De stelling dat dit mogelijk is gebeurd, gaat er zonder adequate onderbouwing aan voorbij dat er op grote schaal betalingen zijn gedaan aan de personen die worden genoemd in de configuratiebestanden en aan andere personen die door middel van diverse dwarsverbanden aan deze malware kunnen worden gelinkt. De suggestie dat de hier bedoelde money mules mogelijk niet alleen voor TorRAT maar ook voor andere gevallen van cyberfraude zijn geronseld, is speculatief, niet onderbouwd en wordt reeds daarom verworpen. Nader onderzoek door een deskundige, zoals door de verdediging van sommige verdachten – naar de rechtbank begrijpt: meer subsidiair en dus voorwaardelijk – is verzocht naar de wijze waarop Fox-IT / de banken zijn gekomen tot de vaststelling van de lijsten bij de aangiften, acht de rechtbank in het licht van het voorgaande niet noodzakelijk.

4.3. ***Witwassen***

Uit de bijlagen bij de aangiften van de banken, verklaringen van diverse money mules en het politieonderzoek (bm 32) blijkt dat bedragen die succesvol werden overgeboekt naar de rekeningen van money mules, voor zover niet door de banken in beslag genomen, veelal contant werden gemaakt door middel van betalingen of werden omgezet in bitcoins, al dan niet nadat zij eerst waren doorgeboekt naar rekeningen van 2de lijns money mules. De opgenomen, doorbetaalde en/of in bitcoins omgezette bedragen zijn op deze wijze witgewassen.[9]

Uit de repliek van de officier van justitie maakt de rechtbank op dat de verdachten niet wordt verweten dat er bitcoins zijn witgewassen, maar dat er geld is witgewassen door dit om te zetten naar bitcoins. De verdachten zullen vrijgesproken worden van het deel van de tenlastelegging waar hen wordt verweten dat zij bitcoins hebben witgewassen.

4.4. ***Het bestaan van een criminele organisatie, de leden daarvan (feit 2) en het medeplegen van het witwassen (feit 1)***

4.4.1. Inleiding

Inherent aan de hiervoor beschreven cyberfraude is het bestaan van een daarop gerichte organisatie. Malware is ontwikkeld, servers zijn gehackt om met behulp van spamruns de malware te verspreiden en money mules zijn geregeld om de beschikking te krijgen over rekeningen om gelden op te laten storten. Deze handelwijze vergt een planmatige aanpak, samenwerking en duidelijke afstemming tussen de daarbij betrokken personen. Zo moesten de gegevens van de money mules worden verwerkt in de configuratiebestanden voordat geld overgemaakt kon worden en moest geregeld worden dat geld zo kort mogelijk na uitbetaling werd opgenomen of overgemaakt. De 'technische kant' en de 'money mule-zijde' moeten dan ook in frequent en nauw verband met elkaar hebben gestaan. Dit heeft plaatsgevonden gedurende geruime tijd en er kan dus zonder meer gesproken worden van een duurzaam en gestructureerd samenwerkingsverband. Kortom, er is sprake van een criminele organisatie.

Die organisatie blijkt ook uit de Tormails tussen Cheng, Chong, Chang, Ching, Jantje, Xel en Eng (zie § B van bijlage II bij dit vonnis). Enkele voorbeelden ter illustratie: in die Tormails worden bankgegevens van money mules en gegevens van betrokken bedrijven gedeeld en een spamrun aangekondigd, een financiele afrekening gemaakt, aanwijzingen gegeven om laptops en telefoons weg te gooien vanwege een lopend onderzoek, wordt overlegd over afspraken bij de kamer van koophandel en er zijn diverse dwarsverbanden tussen het adres [mailadres 4][10] [mailadres 4] en het beheer van de TorRAT malware.

6 Het IP adres 95.211.13.35 is blijkens het rapport van Trend Micro ook gebruikt door 'Jantje' bij het gebruik van scan4you. 'Jantje' gebruikte blijkens dat rapport scan4you om de TorRAT malware te testen op herkenning door antivirussoftware (bm 30).

9 Om misverstanden te voorkomen: de rechtbank ziet de overboeking van de rekening van een slachtoffer naar de money mule als diefstal en nog niet als witwassen. Het is de daarop volgende versluiering van de criminele herkomst door contant maken of omzetting in bitcoins die de rechtbank als witwassen aanmerkt.

10 Om te voorkomen dat dit document automatisch links aanbrengt naar emailadressen is het @ teken zo veel mogelijk vervangen door "[AT]".

De rechtbank is van oordeel dat er voldoende bewijs is dat achter de bijnamen Cheng, Chong, Chang, Ching, Jantje en Xel de verdachten [verdachte 1], [verdachte 5], [verdachte 4], [verdachte 3], [verdachte 2] en [verdachte 6] schuilgaan en dat zij lid van de criminele organisatie (feit 2) en medepleger van het witwassen (feit 1) zijn.[11,12] Ter toelichting hierop wordt het volgende overwogen.

4.4.2. Verdachte [verdachte 1] (Cheng)

[verdachte 1] is Cheng. Dat kan als volgt worden vastgesteld:[13]

a. In Tormail #034 schrijft Chong aan Ching dat Cheng het nummer [telefoonnummer 1] gebruikt. De historische gegevens van dat nummer zijn vergeleken met het nummer dat op naam staat van [verdachte 1], [telefoonnummer 2]. Daaruit blijkt dat de beide telefoonnummers zich op meerdere tijdstippen rond dezelfde locatie bevonden. Ook is gebleken dat er geen momenten zijn aan te wijzen waarop de mastgegevens zo ver uit elkaar liggen dat het niet mogelijk is dat deze nummers zich in dezelfde omgeving bevonden (bm 105).
b. In Tormail #038 d.d. 14 november 2012 om 09.32 uur schrijft Cheng aan Ching, Chang en Chong dat hij net de trein heeft gereserveerd; vertrek dinsdag 1150 uit Calais terug 1550 lokale tijd. Uit Tormails #041, #047 en #050 blijkt dat het gaat om een bezoek in Engeland van Ching, Cheng, Chang en Chong bij 'Eng' ([naam 18]). Onder [verdachte 1] is een telefoon in beslag genomen (bm 115) en uit de telefonische contacten van die telefoon blijkt dat met die telefoon op 14 november 2012 is gebeld met het nummer 09005040540, het reserveringsnummer van de Eurotunnel (bm 116). Op 15 november 2012 heeft Eurotunnel een reservering bevestigd aan 'de heer P. [verdachte 1] ' (bm 117). Zingstra heeft bevestigd dat hij in Engeland is opgezocht door een delegatie en verklaart dat [verdachte 1] daar deel van uitmaakte (bm 142).
c. [verdachte 1] en [verdachte 5] zijn op 7 december 2012 aangehouden in het onderzoek Rotterdam / Dash (bm 155). Op zaterdag 8 december 2012 verstuurde Chang Tormail #062 aan Ching waarbij hij aangaf dat Chong en Cheng afgelopen vrijdag samen met lid Assen naar een project zijn gegaan; nadien is er niets meer van hen vernomen en zijn zij niet bereikbaar. Op 9 december 2012 reageert Ching daarop met Tormail #085 dat hij (Ching) wil weten wat er aan de hand is, want hij heeft Cheng al een aantal keren op de chat gehad, maar hij reageert nergens op. In de fouillering van de verdachte [verdachte 1] is een telefoon aangetroffen. Daarop is het volgende ontvangen sms-bericht aangetroffen: 'What is happening? Ik zie je op chat en krijg geen reactie? laat me ff wat weten. Gr." (bm 155). Dit bericht is afkomstig van het Thaise nummer van verdachte [verdachte 3] (bm 155 jo 107). Op 10 december 2012 zijn de verdachten [verdachte 1] en [verdachte 5] heengezonden (bm 155) en op 13 december 2012 verstuurde Cheng Tormail #018 aan Ching en Chang, waarbij Cheng aangaf dat alle laptops en telefoons z.s.m. weggegooid moesten worden, omdat er een onderzoek liep.

Door de verdediging van verschillende verdachten is aangevoerd dat uitgesloten is dat [verdachte 1] tijdens zijn detentie toegang had tot de chat, dus dat hij niet degene kan zijn die op de chat gezien is. De rechtbank wijst erop dat uit Tormail #092 blijkt dat chatgesprekken tussen Cheng c.s. niet soepel liepen en dat het voorkwam dat men elkaar wel zag, maar dat er niet werd gereageerd en dat de techniek niet goed functioneerde.

De hier besproken omstandigheden moeten niet alleen in onderlinge samenhang worden gezien, maar ook in de context dat bij [verdachte 1] diverse voorwerpen zijn gevonden die onmiskenbaar zijn gerelateerd aan de TorRAT fraude (de SD-kaart in zijn huis (bm 124 e.v.) en de dongels (bm 123) en meerdere telefoons (bm 113 en 114) in zijn auto). Verder wordt gewezen op de verklaringen van de money mule [begunstigde 8] die [verdachte 1] aanwijst als degene voor wie hij een rekening opende (bm 146). De betrokkenheid van [verdachte 1] bij TorRAT blijkt dus ook (en in ruime mate) uit andere hoofde.

Over de SD-kaart heeft de verdediging van [verdachte 1] aangevoerd dat het gaat om gegevens die op unallocated clusters staat en dat er geen zekerheid is dat het gaat om verwijderde bestanden, wanneer een eventuele verwijdering zou zijn gebeurd en of die SD-kaart is gebruikt op de computer van [verdachte 1]. Geen van deze (en overige) aangevoerde argumenten doen er echter aan af dat op die SD-kaart bijzonder veel relevante TorRAT informatie stond.

Dat [verdachte 1] niet alleen lid van de criminele organisatie was, maar ook een leidinggevende rol had, blijkt uit de Tormails. Die leidinggevende rol wordt nog eens bevestigd, zij het in een iets andere context, door de verklaring van [verdachte 8] dat [verdachte 1] bij het witwassen in het deelonderzoek Rotterdam / Dash de leiding had (bm 147 e.v.).

Ten aanzien van het witwassen wordt nog het volgende overwogen. Dat geen concrete betrokkenheid bij alle opnamen, doorboekingen of money mules kan worden aangetoond, doet er niet aan af dat [verdachte 1] ook daarvoor als medepleger kan worden aangemerkt. Zoals hiervoor al is aangegeven, bestond er een nauw organisatorische verwevenheid tussen de technische kant van de fraude en de money mule zijde. Over en weer maakten deze twee zijden het mogelijk om deze fraude succesvol te plegen en over de gestolen gelden uiteindelijk te kunnen beschikken door middel van witwassen. [verdachte 1] was als geen ander daarvan op de hoogte en hij heeft daaraan een actieve, sturende bijdrage geleverd.

(...)

11 Tormailgebruiker 'Eng' is blijkens Tormail #053 [naam 16] . Dit wordt hierna niet verder uitgewerkt nu Zingstra thans niet terecht staat.

12 Medeverdachte [verdachte 7] wordt in een vonnis van gelijke datum veroordeeld voor medeplegen van een deel van het witwassen (feit 1) en vrijgesproken van lidmaatschap van een criminele organisatie (feit 2). Zijn verklaringen worden deels in dit vonnis voor het bewijs gebruikt, maar voor het overige blijft hij hier buiten beschouwing.

13 Alle hierna genoemde tormails zijn opgenomen in § B van bijlage II bij dit vonnis.

4.6. ***Slotopmerkingen over het bewijs van de feiten 1 en 2***

Mede naar aanleiding van het requisitoir en gevoerde verweren wordt nog het volgende overwogen.

1. Medeplegen van feit 1

Voor medeplegen is volgens vaste rechtspraak vereist dat er sprake is van een voldoende nauwe en bewuste samenwerking met een ander of anderen, waarbij het accent ligt op de samenwerking en minder op de vraag wie welke feitelijke handelingen heeft verricht. Wel moet de eigen bijdrage van een verdachte van voldoende gewicht zijn. Voor de verdachten [verdachte 1], [verdachte 5], [verdachte 4], [verdachte 3], [verdachte 2] en [verdachte 6] bestaat die samenwerking daaruit dat zij ieder taken verrichten waardoor de TorRAT fraude mogelijk werd. Enerzijds is de techniek nodig. Anderzijds is het de beschikbaarheid van voldoende en tijdig inzetbare money mules die het mogelijk maakt om gelden daadwerkelijk te ontvreemden: eerst door het op te nemen in de configuratiebestanden en vervolgens als betalingsadres voor het ontvreemde geld. Het witwassen is in deze zaak vervolgens een onlosmakelijk onderdeel van de fraude; immers, als het geld te lang bij de money mules staat, dan kunnen de banken transacties blokkeren en gelden terughalen, zoals in deze zaak veelvuldig is gebeurd. Die samenwerking moet naar zijn aard nauw geweest zijn. Anders dan de verdediging van bijvoorbeeld [verdachte 3] heeft bepleit, is de rechtbank van oordeel dat het niet zo is dat per transactie gekeken moet worden naar de (bewijsbare) bijdrage van ieder der verdachten. Voor ieder van deze verdachten geldt dat zij een rol van voldoende gewicht hebben gespeeld binnen de TorRAT fraude en dat rechtvaardigt strafrechtelijke verantwoordelijkheid voor het geheel.

2. Pleegperiode

Door de verdediging van verschillende verdachten is aangevoerd dat zij in ieder geval na december 2012 geen betrokkenheid meer hadden met TorRAT. Aan de verdediging van die verdachten kan worden toegegeven dat uit de bewijsmiddelen blijkt dat de TorRAT fraude met name plaatsvond in de tweede helft van 2012. In 2013 is enige tijd rust geweest, met name tussen februari en juni 2013. Daarna zijn er weer TorRAT fraudes of pogingen daartoe geweest in de periode tot oktober 2013. Voor zover door de verdediging is aangevoerd dat er geen betrokkenheid meer was in 2013, had het op hun weg gelegen om dat nader te onderbouwen. Hetzelfde geldt voor het verweer van diverse verdachten dat zij voor bepaalde data (in ieder geval) geen betrokkenheid bij TorRAT hadden. Als pleegperiode houdt de rechtbank daarom aan de periode van 4 mei 2012 (de datum van de oudste Tormail) tot en met 21 oktober 2013. Laatstgenoemde datum is de dag van aanhouding van [verdachte 1], [verdachte 5], [verdachte 4] en [verdachte 2], zie p. 8 van het Armor relaasproces-verbaal. Na die datum zijn geen nieuwe TorRAT gevallen gebleken (bm 8 en 24).

3. Pleegplaats

Door de verdediging van [verdachte 3] is aangevoerd dat een bedrag van € 7.013,68 is witgewassen via Jeanesshop in België en er op gewezen dat België niet als pleegplaats op de telastlegging staat. Dit verweer slaagt en in zoverre vindt in de zaken van alle verdachten een partiële vrijspraak ter zake van het witwassen plaats (voornoemd bedrag is onderdeel van het totaalbedrag genoemd in feit 1).

4. Bewezen verklaarde bedrag (feit 1)

Gelet op hetgeen hiervoor is overwogen over de verschillende overboekingen en begunstigden en nu enkele money mules niet nader zijn besproken in dit vonnis, zal de rechtbank in de bewezenverklaring volstaan met het bewezen verklaren van het witwassen van geldbedragen en niet van een concreet bedrag.

5. Getuigenverklaringen

De verdediging van een aantal verdachten heeft aangevoerd dat de verklaringen van diverse money mules, van [verdachte 6] en van [naam 11] onvoldoende betrouwbaar zijn en/of dat het ondervragingsrecht ten aanzien van deze getuigen niet naar behoren kon worden gerealiseerd, bijvoorbeeld doordat zij zich op een verschoningsrecht beriepen of bijzonder emotioneel werden. Dit verweer slaagt niet. De voor het bewijs gebruikte getuigenverklaringen vinden voldoende steun in andere bewijsmiddelen en de hierna volgende veroordeling berust niet in doorslaggevende mate op deze verklaringen.
De verdediging van [verdachte 3] heeft bij gelegenheid van het pleidooi een voorwaardelijk verzoek gedaan tot het horen van [begunstigde 10] als getuige. Aan de beoordeling van dit verzoek wordt niet toegekomen nu niet is voldaan aan de voorwaarde waaronder dit verzoek is gedaan (zie p. 10 bovenaan van de pleitnota).

6. Oogmerk organisatie

De verdediging van een aantal verdachten heeft terecht aangevoerd dat het oogmerk van de criminele organisatie in feit 2 van de tenlastelegging te ruim is omschreven. Voor die delen van het tenlastegelegde oogmerk waar geen bewijs voor is, vindt een partiele vrijspraak plaats.

4.7. ***Bewezenverklaring***

In bijlage II heeft de rechtbank de inhoud van wettige bewijsmiddelen opgenomen, houdende voor de bewezenverklaring redengevende feiten en omstandigheden. Op grond daarvan, en op grond van de redengevende inhoud van het voorgaande, is wettig en overtuigend bewezen dat de verdachte het onder 1 en 2 ten laste gelegde heeft begaan op die wijze dat:

1. hij, in de periode van 4 mei 2012 tot en met 21 oktober 2013
in Nederland en/in Groot-Brittannië,
tezamen en in vereniging met anderen
van het plegen van witwassen een gewoonte heeft gemaakt, door van voorwerpen, te weten geldbedragen de herkomst en de verplaatsing te verhullen,

immers hebben verdachte en zijn mededaders voornoemde geldbedragen verkregen door
- het (laten) versturen van grote hoeveelheden e-mailberichten (zogenaamde 'spamruns') waardoor computers van derden zijn geïnfecteerd met Torrat malware en vervolgens
- de mogelijkheid verkregen het online betalingsverkeer tussen de klant en de bank te manipuleren en vervolgens die gelden onder valse omschrijvingen naar andere bankrekeningen overgeschreven en/of laten overschrijven dan waartoe opdracht was gegeven en vervolgens
- die geldbedragen (meermalen) doorgeboekt naar (buitenlandse en/of zakelijke) bankrekeningen die (indirect) door hem en/of zijn mededaders werden beheerd en/of gecontroleerd en/of gebruikt en/of (vervolgens)
- die geldbedragen van die bankrekeningen opgenomen in contanten (ter doorbreking van de papertrail) en/of- de digitale banktegoeden en/of contante bedragen omgezet naar 'bitcoins',en/of-een door middel van oplichting/phishing van Katholieke Belangenvereniging voor Ouderen (KBO) te Ooij verkregen geldbedrag (ongeveer 8.155,00 zegge acht duizend en honderd en vijfenvijftig euro) doorgeboekt/overgeboekt naar (een) bankrekening(en) die (indirect) door hem en/of zijn mededaders werd(en) beheerd en/of gecontroleerd en/of gebruikt en/of (vervolgens) met dat geldbedrag gouden munten gekocht en/of beheerd

welke geldbedragen- middellijk of onmiddellijk – van misdrijf afkomstig zijn,
terwijl hij en zijn mededaders wisten dat/die voorwerpen- onmiddellijk of middellijk -afkomstig waren uit enig misdrijf;
2. hij in de periode van 4 mei 2012 tot en met 21 oktober 2013,
in Nederland en/in Groot-Brittannië,
heeft deelgenomen aan een organisatie, welke organisatie tot oogmerk had het plegen van misdrijven, namelijk het
- opzettelijk en wederrechtelijk toegang verschaffen tot een geautomatiseerd werk (strafbaar gesteld in artikel 138ab Wetboek van Strafrecht);
- opzettelijk en wederrechtelijk toegang belemmeren tot een geautomatiseerd werk of daaraan gegevens aan te bieden of toe te zenden (strafbaar gesteld in artikel 138b Wetboek van Strafrecht)
- diefstal door twee of meer verenigde personen en door middel van een valse sleutel (strafbaar gesteld in 311 lid 1 onder 4 en 5 Wetboek van Strafrecht)
- witwassen als bedoeld in artikel 420ter Wetboek van Strafrecht,

van welke organisatie verdachte mede- oprichter en- leider was.

Hetgeen meer of anders is ten laste gelegd is niet bewezen. De verdachte moet daarvan worden vrijgesproken.

5. Strafbaarheid feiten

De verdediging heeft ontslag van alle rechtsvervolging bepleit ten aanzien van het onder 1 tenlastegelegde. Hiertoe is het volgende aangevoerd:
De eerste twee ten laste gelegde witwasvarianten zijn niet te kwalificeren als het strafbare feit witwassen. Deze varianten worden telkens door de toevoeging van de frase "en/of" gescheiden en bij elk van de varianten ontbreekt het bestanddeel dat de verdachte "wist dan wel redelijkerwijs had moeten vermoeden dat de voorwerpen afkomstig zijn van enig misdrijf".
Voorts is het daderschap van de verdachte gebaseerd op de gestelde betrokkenheid van de verdachte bij TorRAT en de omstandigheid dat de witgewassen voorwerpen afkomstig zouden zijn uit TorRAT hetgeen betekent dat er derhalve sprake is van witwassen van voorwerpen die zijn verkregen door het zelf begaan van een strafbaar feit. In een dergelijk geval is de kwalificatie van het witwassen – voor zover dat ziet op het voorhanden hebben en het verwerven van die voorwerpen – niet mogelijk.
De rechtbank verwerpt beide verweren en overweegt daartoe als volgt.
Het is niet ongebruikelijk om verschillende vormen van witwassen op de onderhavige manier cumulatief ten laste te leggen. Het is naar het oordeel van de rechtbank evident dat de frase "terwijl hij en/of zijn mededader(s) wist(en), althans redelijkerwijs moest(en) vermoeden dat dat/die voorwerp(en) – onmiddellijk of middellijk – (deels) afkomstig was/waren uit enig misdrijf" betrekking heeft op alle daaraan voorafgaande witwasvarianten.
Uit de bewezenverklaring volgt dat de verdachte handelingen heeft verricht die een op het verhullen van de criminele herkomst van de door eigen misdrijf verkregen geldbedragen gericht karakter heeft. Het bewezenverklaarde kan derhalve worden gekwalificeerd als (gewoonte)witwassen.
De bewezen feiten leveren op:
1. medeplegen van het een gewoonte maken van witwassen;
2. het deelnemen aan een organisatie die tot oogmerk heeft het plegen van misdrijven, van welke organisatie hij (mede)oprichter en leider was.

Er zijn geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van de feiten uitsluiten.
De feiten zijn dus strafbaar.

6. Strafbaarheid verdachte

Er is geen omstandigheid aannemelijk geworden die de strafbaarheid van de verdachte uitsluit.
De verdachte is dus strafbaar.

7. Motivering straf

7.1. *Algemene overweging*

De straf die aan de verdachte wordt opgelegd, is gegrond op de ernst van de feiten, de omstandigheden waaronder de feiten zijn begaan en de persoon en de persoonlijke omstan-

digheden van de verdachte. Daarbij wordt in het bijzonder het volgende in aanmerking genomen.

7.2. ***Feiten waarop de straf is gebaseerd***

De verdachte heeft zich samen met anderen schuldig gemaakt aan grootschalige en langdurige criminele activiteiten, die opvallen door professionaliteit, geraffineerdheid en het intensieve samenwerkingsverband.

Voornoemde criminele activiteiten bestonden hieruit dat de verdachte samen met zijn mededaders rekeninghouders van Rabobank en ING-bank (ING) heeft benadeeld.

Via zogenaamde "spamruns" werden duizenden mails verstuurd naar met name midden- en kleinbedrijven in de zakelijke sector. Deze mails betroffen veelal aanmaningen of voorstellen voor een betalingsregeling. In de mails zat een link naar, ogenschijnlijk, een openstaande factuur of ander (pdf)bestand, maar in werkelijkheid betrof het een programma dat ongemerkt kwaadaardige software, in casu zogenaamde "TorRAT malware", op de computer van de gebruikers achterliet waardoor het internetbankieren op afstand door een Command en Control server kon worden gemanipuleerd. Bij het gebruik van internetbankieren op een besmette computer kon zo het rekeningnummer, de naam van de begunstigde en de omschrijving van de betaling worden aangepast, zonder dat dit voor de gebruiker van die computer (direct) zichtbaar was. Op deze wijze konden betalingen door de TorRAT malware worden gewijzigd en omgeleid naar de rekeningen van zogeheten money mules, zijnde personen die hun rekening, bankpas en pincode, al dan niet bewust en al dan niet vrijwillig, ter beschikking hadden gesteld. De geldbedragen werden vervolgens zo snel mogelijk aan het zicht van de banken en politie en justitie onttrokken door deze – al dan niet met tussenkomst van een tweedelijns-money mule waar het geld naar werd doorgeboekt – zo snel mogelijk contant te maken middels een contante geldopname of werden omgezet in bitcoins. De opgenomen, doorbetaalde en/of in bitcoins omgezette bedragen werden op deze wijze witgewassen.

De verdachte was één van de oprichters van en had een leidinggevende rol binnen voornoemd samenwerkingsverband, dat door de duurzaamheid en gestructureerde vorm daarvan als criminele organisatie wordt gekwalificeerd. Hij onderhield als enige contact met de TorRAT malwarebeheerder zijnde medeverdachte [verdachte 2] en hij gaf opdrachten aan- en werd terug gerapporteerd door de andere medeverdachten.

7.3. ***Persoonlijke omstandigheden van de verdachte***

7.3.1. Strafblad

De rechtbank heeft acht geslagen op een uittreksel uit de justitiële documentatie van
6 juni 2016, waaruit blijkt dat de verdachte eerder is veroordeeld, zij het al geruime tijd geleden.

7.4. ***Conclusies van de rechtbank***

Gelet op hetgeen de rechtbank hierboven heeft overwogen, komt zij tot de volgende conclusies.

De verdachte en zijn medeverdachten hebben het systeem van internetbankieren op grove wijze aangevallen en het vertrouwen dat een ieder moet kunnen hebben in de integriteit van het elektronische betalingsverkeer geschaad.

Niet alleen een groot aantal rekeninghouders, maar ook de bankinstellingen zijn door het handelen van de verdachte en zijn medeverdachten gedupeerd geraakt.

Daarnaast wordt door het witwassen van "crimineel verkregen geld" het plegen van criminele activiteiten in stand gehouden en indirect ook bevorderd, want zonder personen als de verdachte die criminele gelden een (schijnbaar) legale herkomst verschaffen, is het genereren van illegale winsten een stuk minder lucratief. Witwassen vormt tevens een ernstige bedreiging van de legale economie en tast de integriteit van het financiële en economische verkeer aan.

De verdachte heeft zich bij zijn handelen enkel laten leiden door financieel gewin en heeft daarbij tevens misbruik gemaakt van personen die door financiële en/of andersoortige problemen als kwetsbaar zijn aan te merken.

Voor feiten als de onderhavige kan, gezien de ernst, de duur en het grote aantal gedupeerden, niet met een andersoortige straf dan een gevangenisstraf worden volstaan.

Bij de bepaling van de duur daarvan is gelet op straffen die in andere, min of meer vergelijkbare zaken, zijn opgelegd en de leidinggevende rol van de verdachte. Anders dan door de verdediging is bepleit, is geen aansluiting gezocht bij de LOVS orientatiepunten voor oplichting. Die orientatiepunten zijn in dit geval niet passend gelet op de grootschalige wijze van fraude en het grote aantal slachtoffers.

Op grond van het vorenstaande acht de rechtbank, alles afwegende, een onvoorwaardelijke gevangenisstraf van na te noemen duur passend en geboden.

8. **In beslag genomen voorwerpen**

De lijst van inbeslaggenomen voorwerpen is als bijlage III aan dit vonnis gehecht.

De rechtbank zal overeenkomstig de vordering van de officier van justitie de onder de nummers 4 t/m 64 en 66 op de lijst van inbeslaggenomen voorwerpen genoemde voorwerpen verbeurd verklaren.

De bewezen feiten zijn met behulp van deze voorwerpen begaan danwel deze goederen kunnen bijgedragen hebben aan het begaan van die feiten. Voor toepassing van artikel 33c, eerste lid Sr wordt geen aanleiding gezien.

Ten aanzien van de onder nummer 65 genoemde sleutelbos zal een last worden gegeven tot teruggave aan de rechthebbende zijnde de verdachte.

De verdediging heeft subsidiair verzocht te bepalen dat privéfoto's, voor zover aanwezig op de gegevensdragers, worden veiliggesteld en geretourneerd. Nu de officier van justitie heeft toegezegd zich hiervoor te zullen inspannen, kan dit punt verder onbesproken blijven.

9. ***Vorderingen benadeelde partijen/ schadevergoedingsmaatregel***

Coöperatieve Rabobank U.A. (Rabobank) en ING hebben zich als benadeelde partijen in het geding gevoegd en schriftelij-

ke vorderingen tot schadevergoeding ingediend. De banken stellen schade te hebben geleden wegens het vergoeden van de als gevolg van bancaire malware ontstane schades aan hun benadeelde rekeninghouders. Het gaat om een bedrag van respectievelijk € 166.227,25 (Rabobank) en € 105.491,42 (ING).
De officier van justitie heeft geconcludeerd tot toewijzing van beide vorderingen.
Door de verdediging is bepleit dat beide benadeelde partijen niet ontvankelijk in hun vorderingen dienen te worden verklaard. Hiertoe is – onder verwijzing naar jurisprudentie van de Hoge Raad dienaangaande – aangevoerd dat Rabobank en ING geen rechtstreekse schade hebben geleden als gevolg van het onder 1 bewezen verklaarde feit. Het onder 1 bewezen verklaarde feit is jegens de desbetreffende rekeninghouders gepleegd en Rabobank en ING zijn derhalve niet getroffen in enig belang dat door de met dat feit overtreden strafbepaling wordt beschermd.
De rechtbank verwerpt het verweer en overweegt daartoe het volgende.
Vooropgesteld moet worden dat een benadeelde partij een vordering tot schadevergoeding kan indienen als er sprake is van schade die rechtstreeks aan haar is toegebracht door het bewezenverklaarde feit (art. 361 en 51f, eerste lid, Sv). Uit de jurisprudentie van de Hoge Raad blijkt dat deze eis niet te strikt moet worden uitgelegd (vergelijk ECLI:NL:HR:2016:1522 en de conclusie bij dat arrest). Er moet worden gekeken naar de concrete omstandigheden van het geval, waarbij de vraag of het slachtoffer is geraakt in het belang dat de geschonden norm beschermt, niet doorslaggevend is (vergelijk voornoemd arrest). Niet uitgesloten is dat de schade weliswaar niet het rechtstreekse gevolg is van de bewezen verklaarde gedraging als zodanig, maar dat – gelet op de uit de bewijsvoering blijkende gedragingen van de verdachte – de door de benadeelde partij geleden schade in zodanig nauw verband staat met het bewezen verklaarde feit, dat die schade redelijkerwijs moet worden aangemerkt als rechtstreeks aan de benadeelde partij door dat feit te zijn toegebracht, zoals bedoeld in voornoemde wetsartikelen.
Kijkend naar de concrete omstandigheden van het geval is naar het oordeel van de rechtbank sprake van een zodanig nauw verband. De verdachte is veroordeeld voor lidmaatschap van een criminele organisatie die met behulp van een computervirus geld ontvreemdde van rekeningen van de klanten van de ING en de Rabobank. Die gelden werden vervolgens weggesluisd en zo buiten het bereik van de banken gehouden. Voor zover de banken hun klanten hebben gecompenseerd voor de schade (zie hierna) is dat in het maatschappelijke verkeer een voorzienbare reactie en het rechtstreekse gevolg van een fraude die zich richt op klanten van een bank.

De vordering van de Rabobank

Rabobank zal in haar vordering niet-ontvankelijk worden verklaard nu de onderbouwing van de vordering zich beperkt tot een verwijzing in het voegingsformulier naar de aangifte en er geen bewijsstukken in het geding zijn gebracht waaruit blijkt dat de Rabobank haar klanten heeft gecompenseerd. De rechtbank is van oordeel dat een nader onderzoek naar de gegrondheid van de vordering en de omvang daarvan een onevenredige belasting van het strafproces zou vormen. De vordering kan derhalve slechts bij de burgerlijke rechter worden aangebracht.
De rechtbank ziet geen aanleiding voor een proceskostenveroordeling in de verhouding tussen de verdachte en de Rabobank.

De vordering van de ING

De rechtbank is van oordeel dat aan de benadeelde partij door het onder 1 bewezen verklaarde feit rechtstreeks schade is toegebracht en dat de vordering genoegzaam is onderbouwd.
De vordering zal worden toegewezen. De verdachte moet de benadeelde partij een schadevergoeding betalen van € 105.491,42.
Nu de verdachte het strafbare feit ter zake waarvan schadevergoeding zal worden toegekend samen met mededaders heeft gepleegd, zijn zij daarvoor ieder hoofdelijk aansprakelijk. Indien en voor zover de mededaders de benadeelde partij betalen is de verdachte in zoverre jegens de benadeelde partij van deze betalingsverplichting bevrijd.
Nu de vordering van de benadeelde partij zal worden toegewezen, zal de verdachte worden veroordeeld in de kosten door de benadeelde partij gemaakt, tot op heden begroot op nihil en in de kosten ten behoeve van de tenuitvoerlegging nog te maken.
Tevens wordt oplegging van de hierna te noemen maatregel als bedoeld in artikel 36f van het Wetboek van Strafrecht passend en geboden geacht.

10. Toepasselijke wettelijke voorschriften

Gelet is op de artikelen 33, 33a, 36f, 47, 57, 140 en 420ter van het Wetboek van Strafrecht.

11. Bijlagen

De in dit vonnis genoemde bijlagen maken deel uit van dit vonnis.

12. Beslissing

De rechtbank:
verklaart bewezen, dat de verdachte de onder 1 en 2 ten laste gelegde feiten, zoals hiervoor omschreven, heeft begaan;
verklaart niet bewezen hetgeen aan de verdachte meer of anders ten laste is gelegd dan hiervoor bewezen is verklaard en spreekt de verdachte daarvan vrij;
stelt vast dat het bewezen verklaarde oplevert de hiervoor vermelde strafbare feiten;
verklaart de verdachte strafbaar;
veroordeelt de verdachte tot een gevangenisstraf voor de duur van 36 (zesendertig) maanden;
beveelt dat de tijd die door de veroordeelde voor de tenuitvoerlegging van deze uitspraak in verzekering en in voorlopige hechtenis is doorgebracht, bij de uitvoering van de

opgelegde gevangenisstraf in mindering wordt gebracht, voor zover deze tijd niet reeds op een andere vrijheidsstraf in mindering is gebracht;
beslist ten aanzien van de voorwerpen, geplaatst op de lijst van inbeslaggenomen en nog niet teruggegeven voorwerpen, als volgt:
- verklaart verbeurd als bijkomende straf voor de feiten 1 en 2 de voorwerpen onder de nummers 4 t/m 64 en 66 op de als bijlage III gevoegde lijst van inbeslaggenomen goederen;
- gelast de teruggave aan de verdachte van het onder nummer 65 inbeslaggenomen goed;

verklaart de benadeelde partij Rabobank niet-ontvankelijk in de vordering;
veroordeelt de verdachte hoofdelijk met diens mededaders, des dat de een betalende de ander zal zijn bevrijd, om tegen behoorlijk bewijs van kwijting aan de benadeelde partij ING, te betalen een bedrag van € 105.491,42 (zegge: honderdvijfduizendvierhonderdeenennegentig euro en tweeënveertig eurocent), geheel bestaande uit materiële schade, met dien verstande dat indien en voor zover zijn mededaders betalen de verdachte in zoverre van deze verplichting is bevrijd;
veroordeelt de verdachte in de proceskosten door de benadeelde partij ING gemaakt, tot op heden aan de zijde van de benadeelde partij begroot op nihil, en in de kosten ten behoeve van de tenuitvoerlegging nog te maken;
legt aan de verdachte de maatregel tot schadevergoeding op, inhoudende de verplichting aan de staat ten behoeve van de benadeelde partij ING te betalen € 105.491,42 (zegge: honderdvijfduizendvierhonderdeenennegentig euro en tweeënveertig eurocent);
beveelt dat bij gebreke van volledige betaling en volledig verhaal van het bedrag van
€ 105.491,42 vervangende hechtenis zal worden toegepast voor de duur van 365 dagen; toepassing van de vervangende hechtenis heft de betalingsverplichting niet op;
verstaat dat betaling aan de benadeelde partij ING, waaronder begrepen betaling door zijn mededaders, tevens geldt als betaling aan de staat ten behoeve van de benadeelde partij en omgekeerd.

Noot

1. De onderhavige uitspraak betreft één van de weinige veroordelingen voor banking malware in combinatie met witwassen.[1] De zaak geeft een exclusief kijkje in de *high tech crime* wereld van banking malware en het witwassen van de crimineel verkregen gelden. Op juridisch gebied is de bewijsconstructie van de rechtbank interessant en moet de vraag worden gesteld op welke wijze witgewassen bitcoins in beslag kunnen worden genomen.

2. De verdachten hebben met kwaadaardige software, genaamd "TorRAT", computers besmet teneinde de internetbankiersessie van hun slachtoffers te manipuleren. De computers van slachtoffers werden besmet via e-mails met ogenschijnlijk een aanmaning of voorstel voor een betalingsregeling.[2] Na het openen van de bijlage werd de malware op de computers van de slachtoffers geïnstalleerd en maakte de software via het anonimiseringprogramma Tor verbinding met de zogenaamde Command-and-Control server van de verdachten. Via een Command-and-Control server hebben de verdachten een overzicht van de besmette computers en kunnen instructies aan de besmette computers (ook wel 'zombie computers' genoemd) worden verstuurd. De verdachten verkrijgen daarmee controle over enkele functionaliteiten van de computers. Software dat functionaliteiten van computers op afstand kan overnemen wordt ook wel een Remote Access Tool (of RAT) genoemd. Samen met het feit dat de malware verbinding maakt met Tor, kan de naam van de malware – TorRAT – worden verklaard.

3. In dit geval heeft de malware als doel om de internetbankiersessies van de slachtoffers te manipuleren. In de uitspraak wordt beschreven dat de malware in werking treedt op het moment dat een slachtoffer zijn of haar bankwebsite opzoekt om online te bankieren. Met de malware kan tijdens het internetbankieren (buiten het zicht van de gebruiker) het rekeningnummer, de naam van de begunstigde en de omschrijving van de betaling worden aangepast en vervolgens geld naar een ander rekeningnummer worden overgemaakt.[3] Op deze wijze zijn betalingen met de TorRAT malware gewijzigd en omgeleid naar money mules. Money mules worden door de rechtbank omschreven als personen die hun rekening, bankpas en pincode, al dan niet bewust en al dan niet vrijwillig, ter beschikking hebben gesteld. Vervolgens is het geld in de meeste gevallen zo snel mogelijk contant opgenomen of omgezet in de virtuele valuta Bitcoin. Bitcoins kunnen worden aangekocht via Bitcoin exchanges.[4] Deze handelingen leverden volgens de rechtbank de volgende delicten op: computervredebreuk (art. 138ab Sr), het verzenden van spam (art. 138b Sr), het aftappen of opnemen van gegevens met malware (art. 138c Sr), het installeren van malware (art. 139d Sr), het in bezit hebben van de malware (art. 139e Sr), diefstal met een valse sleutel (art. 311 lid 1 onder 4 en 5 Sr) en oplichting (art. 326 Sr).

4. De rechtbank acht tevens het delict gewoontewitwassen (art. 420bis Sr) bewezen. De vereiste verhullingshandeling bestond daarbij uit het overboeken van het geld naar de rekeningen van money mules in combinatie met het contant opnemen van het geld of omzetten van het geld in bitcoins.[5] De overboeking van de rekening van een slachtoffer naar de money mule ziet de rechtbank als diefstal en nog niet als witwassen. Het is de daarop volgende versluiering van de criminele herkomst door het contant maken

1 Zie ook Rb. Rotterdam 2 oktober 2015, ECLI:NL:RBROT:2015:7041 (*Computerrecht* 2015/223) en Rb. Zeeland 29 juni 2016, ECLI:NL:RBZWB:2016:3877 die in de Strafrecht rubriek van dit nummer wordt genoemd.

2 Zie r.o. 4.1.

3 Zie r.o. 4.1 en 7.1. Zie voor een meer technische omschrijving van de werking van banking malware ook Rb. Zeeland-West-Brabant 29 juni 2016, ECLI:NL:RBZWB:2016:3877, r.o. 4.3.3 en Rb. Rotterdam 2 oktober 2015, ECLI:NL:RBROT:2015:7038, r.o. 5.1.1.

4 Zie bijvoorbeeld T. Spaas en M. Van Roey, 'Quo vadis Bitcoin?', *Computerrecht* 2015/84 voor meer informatie over de werking van Bitcoin.

5 Zie r.o. 4.3.

of omzetting in bitcoins dat de gedraging tot witwassen maakt. De rechtbank komt ook tot het oordeel dat sprake is van een criminele organisatie (art. 140 Sr).[6] Daarbij wordt opgemerkt dat voor het plegen van de 'cyberfraude' een daarop gerichte organisatie noodzakelijk is. Een groep van personen heeft in dit geval de malware ontwikkeld, servers zijn gehackt om de e-mails voor de malware verspreiding te distribueren, en money mules zijn geronseld om beschikking te krijgen over rekeningen om geld op te storten. De rechtbank komt tot de conclusie dat daarvoor een planmatige aanpak, samenwerking en duidelijke afstemming tussen de betrokkenen noodzakelijk is geweest. Ter onderbouwing van deze samenwerking worden enkele passages afkomstig uit e-mails aangehaald. De verdachten maakten gebruik van de (niet meer beschikbare) dienst TorMail, die kan worden beschreven als een gratis webmail dienst die alleen via Tor bereikbaar is. Uit de uitspraak wordt niet helder hoe toegang tot deze e-mails is verkregen.

De verdachte was één van de oprichters van de criminele organisatie en had een leidinggevende rol binnen het criminele samenwerkingsverband. Hij is veroordeeld tot een gevangenisstraf van 3 jaar. Tevens moet de verdachte een stevige schadevergoeding betalen van € 105.491,42 aan de ING. De vordering van de Rabobank werd onvoldoende gemotiveerd geacht. De medeverdachten zijn veroordeeld voor gevangenisstraffen variërend van 9 tot 36 maanden, afhankelijk van hun rol binnen de criminele organisatie en strafblad.

5. Met betrekking tot de bewijsvoering is het interessant dat de officier van justitie stevig leunt op bijlagen van frauduleuze transacties die zijn aangeleverd door een IT beveiligingsbedrijf en de betrokken banken zelf. De verdediging voerde echter aan dat daaruit niet direct blijkt dat de TorRAT malware deze frauduleuze transacties veroorzaakt. Teneinde de causaliteit vast te stellen bespreekt de rechtbank 15 frauduleuze transacties uitvoerig. Daaruit blijkt volgens de rechtbank dat de configuratiebestanden afkomstig zijn van TorRAT en de frauduleuze transacties met behulp van de malware zijn uitgevoerd.

Overigens zij opgemerkt dat de rechtbank in de uitspraken onder andere IP adressen *in zijn geheel opneemt*. Daar kan kritiek op worden geleverd, omdat de IP adressen (nog steeds) zijn terug te voeren tot bepaalde dienstverleners en de Autoriteit Persoonsgegevens IP adressen als een persoonsgegeven beschouwt.

6. Ten slotte is het opvallend dat in het persbericht van het Openbaar Ministerie over de zaak in 2013 nog wordt opgemerkt dat beslag is gelegd op 56 bitcoins, die destijds zijn omgezet in meer dan € 7700.[7] De uitspraak refereert niet naar deze beslaglegging. Evenwel sta ik hier kort bij stil aangezien die inbeslagneming van bitcoins een aantal juridische vragen oproept.

Ten eerste de vraag of bitcoins als *goed* gekwalificeerd kunnen worden en daarmee vatbaar zijn voor inbeslagname. Hoewel een goed ook onstoffelijk kan zijn en giraal geld kan betreffen, worden gegevens binnen het strafrecht in principe niet gekwalificeerd als goed.[8] Uit verschillende arresten kan echter worden afgeleid dat als de gegevens, kort gezegd, uniek zijn en in het economisch verkeer van waarde is, zij toch als goed kunnen worden beschouwd.[9] Het Openbaar Ministerie neemt ook de positie in dat bitcoins als goed kunnen worden beschouwd en vatbaar zijn voor inbeslagname.[10]

De tweede vraag is op welke wijze de bitcoins in beslag kunnen worden genomen. Er is geen formele openbare werkwijze van het Openbaar Ministerie beschikbaar. Een UNDOC rapport over witwassen met virtuele betalingsmiddelen beschrijft dat het gebruikelijk is dat, indien de bitcoins zich in een Bitcoin portemonnee[11] op een computer of gegevensdrager bevinden, eerst het voorwerp zelf in beslag wordt genomen.[12] Vervolgens kunnen de bitcoins worden overgemaakt naar een Bitcoin adres dat is aangemaakt door de opsporingsambtenaren. Als laatste stap kunnen de 'inbeslaggenomen' bitcoins via Bitcoin exchanges worden omgezet in euro's en op een rekening van het Openbaar Ministerie worden gestort. Uit een interview in het magazine van het Openbaar Ministerie blijkt dat deze wijze van inbeslagname overeenkomt met de wijze waarop bitcoins in Nederland in beslag worden genomen.[13] Slechts één uitspraak is beschikbaar waarin expliciet wordt genoemd dat de gegevensdrager, een USB-stick met daarop 147 bitcoins, verbeurd is verklaard door de rechtbank omdat de bitcoins op strafbare wijze zijn verkregen en de USB-stick aan de verdachte toebehoort.[14] Onduidelijk blijft in ieder geval op welke wijze bitcoins in beslag worden genomen die alleen via een portemonnee in een online account bereikbaar zijn. Wordt daarvoor misschien van een vorm van een netwerkzoeking gebruikgemaakt? Het laatste woord zal dus nog niet gezegd zijn over de inbeslagname van bitcoins en andere digitale betalingsmiddelen.

J.J. Oerlemans

6 Zie r.o. 4.4.

7 Zie Landelijk Parket, 'Hackers plunderen bankrekeningen', 24 oktober 2013. Beschikbaar op: https://www.om.nl/vaste-onderdelen/zoeken/@32220/hackers-plunderen/ (Laatst geraadpleegd op 11 augustus 2016).

8 Zie HR 23 mei 1921, *NJ* 1921, p. 564 e.v., m.nt. Taverne; HR 11 mei 1982, *NJ* 1982/583, m.nt. A.C. 't Hart en *Kamerstukken II* 1989/90, 21551, 3, p. 3 en HR 3 december 1996, *NJ* 1997/574.

9 Zie HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251, *NJ* 2012/536, m.nt. N. Keijzer (Runescape); HR 31 december 2012, ECLI:NL:HR:2012:BQ6575 (diefstal van belminuten); Hof 's-Gravenhage 3 december 2015, ECLI:NL:GHDHA:2015:3355, *Tijdschrift voor Internetrecht* 2014, nr. 3, p. 83-86, m.nt. J.S. Nan & B.W. Schermer (diefstal van eindexamens op de Ibn Ghaldoun school).

10 Zie het interview met landelijk officier van justitie cybercrime Martijn Egberts door Thea van der Geest, 'Misbruik van bitcoins', *Opportuun*, jrg. 21, nr. 6, 2015, p. 9. Beschikbaar op: om.nl.

11 Een Bitcoin wallet is software waarmee verbinding wordt gemaakt met het Bitcoin-netwerk en waar bitcoins van de gebruiker in worden beheerd.

12 Zie United Nations Office on Drugs and Crime (UNODC), *Basic manual of the detection and investigation of the laundering of crime proceeds using virtual currencies*, 2014, p. 101-107 en p. 155. Beschikbaar op: https://www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf.

13 Zie het interview met landelijk officier van justitie cybercrime Martijn Egberts door Thea van der Geest, 'Misbruik van bitcoins', *Opportuun*, jrg. 21, nr. 6, 2015, p. 9-10. Beschikbaar op: om.nl. Overigens koos de FBI in de Silk Road zaak voor de verkoop van bitcoins door middel van veiling. Zie bijvoorbeeld 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 januari 2014. Beschikbaar op: www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php (laatst geraadpleegd op 11 augustus 2016).

14 Zie Hof Arnhem-Leeuwarden 7 juli 2016, ECLI:NL:GHARL:2016:5563.