ECLI:NL:RBZWB:2020:2699

Instantie	Rechtbank Zeeland-West-Brabant
Datum uitspraak	26-06-2020
Datum publicatie	26-06-2020
Zaaknummer	02/117799-19
Rechtsgebieden	Strafrecht
Bijzondere kenmerken	Eerste aanleg - meervoudig
Inhoudsindicatie	Onderzoek Korcullu, zijnde een vervolg op onderzoek Vari/Willis. Verdachte werkte mee aan het verzenden van spam e-mails uit naam van een bank. Slachtoffers werden door een 'nep'website geleid en waren in de waan dat zij een nieuwe pinpas aanvroegen, maar in werkelijkheid zorgde men er voor dat men de beschikking kreeg over mobiel bankieren van het slachtoffer. Vervolgens werd er een nieuwe pinpas aangevraagd, die werd afgevangen. Hierna werd de rekening van het slachtoffer, met onder andere gebruikmaking van moneymules, leeggehaald. Ook werden er bestellingen gedaan bij diverse webshops. Verdacht krijgt 3 jaar gevangenisstraf waarvan 1 jaar voorwaardelijk met een proeftijd van 3 jaar voor medeplegen van oplichting, medeplegen van computervredebreuk, medeplegen van witwassen, allen meermalen gepleegd, overtreding van artikel 139d en 350d Wetboek van strafrecht en deelname aan een criminele organisatie.
Vindplaatsen	Rechtspraak.nl

Uitspraak

RECHTBANK ZEELAND-WEST-BRABANT

Strafrecht

Zittingsplaats: Breda

parketnummer: 02/117799-19

vonnis van de meervoudige kamer van 26 juni 2020

in de strafzaak tegen

[verdachte]

geboren op [geboortedatum] te Amsterdam

wonende te [adres]

raadsvrouw mr. M.M.C. Glismeijer, advocaat te Amsterdam.

1 Onderzoek van de zaak

De zaak is inhoudelijk behandeld op de zitting van 29 mei 2020, waarbij de officier van justitie, mr. Van Setten, en de verdediging hun standpunten kenbaar hebben gemaakt.

2 De tenlastelegging

De tenlastelegging is gewijzigd overeenkomstig artikel 314a van het Wetboek van Strafvordering (hierna: Sv). Verdachte staat terecht, ter zake dat:

Feit 1. (zaak 1 t/m 3)

hij op een of meer tijdstip(pen) in of omstreeks de periode van 1 oktober 2016 tot en met 14 mei 2019 te Oosterland, gemeente Schouwen-Duiveland en//of Amsterdam en/of Erp en/of Almere, in elk geval op een of meer plaats(en) in Nederland,

meermalen, althans eenmaal, (telkens) tezamen en in vereniging met een of meer anderen, althans alleen,

(telkens) met het oogmerk om zich en/of een ander wederrechtelijk te bevoordelen door het aannemen van een valse naam en/of van een valse hoedanigheid en/of door listige kunstgrepen en/of door een samenweefsel van verdichtsels,

(telkens) een (groot) aantal Rabobank-klanten en/of ING-klant(en) waaronder

- [slachtoffer 1] en/of
- [slachtoffer 2] en/of
- [slachtoffer 3] en/of
- [slachtoffer 4]

heeft/hebben bewogen tot het ter beschikking stellen van gegevens(s), te weten:

- rekening gegevens en/of

- pincode en/of

- verificatiecode en/of

- de (inlog)gegevens (gebruikersnaam en/of wachtwoord) van/voor het (internet)bankieren van/bij de Rabobank en/of ING, door - zakelijk weergegeven - onder meer:

- gebruik te maken van de (valse) na(a)m(en) en/of bedrijfsna(a)m(en) en/of (bedrijfs)logo's van de Rabobank en/of ING en/of

- (vervolgens) een mail te sturen naar voornoemd(e) perso(o)n(en) om een nieuwe bank- en/of betaalpas(sen) aan te vragen en/of

- (vervolgens) in die mail te vragen om een nieuwe bank- en/of betaalpas aan te vragen door op de (hyper)link in de mail te klikken en/of

- (vervolgens) in die/dat (hyper)link/(aanvraag)formulier te vragen om voornoemde gegevens in te vullen en/of

- (vervolgens) tijdens het invullen voornoemde perso(o)n(en) te bellen als zijnde een medewerker van de Rabobank en/of ING om samen met voornoemde perso(o)n(en) de invulvelden door te lopen/in te vullen,

waardoor die (voornoemde) Rabobank- en/of ING- klanten (telkens) werd(en) bewogen tot het ter beschikking stellen van bovenomschreven gegeven(s),

en/of (vervolgens)

de Rabobank en/of ING heeft /hebben bewogen tot de afgifte van enig(e) goed(eren), te weten een of meer bankpas(sen) en/of betaalpas(sen), in elk geval een of meer goed(eren) door -zakelijk weergegeven - onder meer:

- in te loggen met de (eerder) gephiste (inlog)gegevens van voornoemde Rabobank- en/of ING-klant(en) op/in de beveiligde internetbankieren-omgeving van de Rabobank en/of ING en/of

- (vervolgens) in/of die omgeving een nieuwe bankpas aan te vragen,

waardoor die Rabobank en/of ING (telkens) werd bewogen tot bovenomschreven afgifte(n);

Feit 2. (zaak 1 t/m 3)

hij op een of meer tijdstip(pen) in of omstreeks de periode van 1 oktober 2016 tot en met 14 mei 2019 te Oosterland, gemeente Schouwen-Duiveland en/of te Amsterdam en/of Almere en/of Erp in elk geval op een of meer plaats(en) in Nederland,

meermalen, althans eenmaal, (telkens) tezamen en in vereniging met een ander of anderen, althans alleen,

(telkens) opzettelijk en wederrechtelijk in een (gedeelte van) een geautomatiseerd werk, te weten de computer(s) en/of server(s) van de (beveiligde) internetbankieren omgeving van/bij de Rabobank en/of ING, althans in een deel daarvan is/zijn binnengedrongen,

waarbij hij, verdachte, en/of zijn mededader(s) (telkens) de toegang heeft/hebben verworven tot het/de geautomatiseerde werk(en)

- met behulp van(een) valse sleutel(s), te weten de (inlog)gegevens voor het internetbankieren (te weten de gebruikersnaam en/of het wachtwoord) van/bij de Rabobank en/of ING en/of

- door het aannemen van een valse hoedanigheid, te weten zijnde een of meer geautoriseerde Rabobank- en/of ING-klant(en) waaronder

- [slachtoffer 1] en/of
- [slachtoffer 2] en
- [slachtoffer 3] en/of
- [slachtoffer 4] ;

Feit 3. (zaak 1 t/m 5)

hij, op een of meer tijdstip(pen) in of omstreeks de periode van 1 oktober 2014 tot en met 14 mei 2019 te Oosterland, gemeente Schouwen-Duiveland en/of Amsterdam en/of Erp en/of Almere, in elk geval een of meer plaats(en) in Nederland,

(telkens) tezamen en in vereniging met een ander of anderen, althans alleen, een of meer voorwerp(en), te weten:

- een of meer (2) horloge('s), van het merk Rolex (aangekocht bij Schaap en Citroen voor ongeveer € 19.010) en/of
- een of meer goed(eren) van het merk Louis Vuitton, waaronder tas(sen) en/of sjaal en/of zonnebril en/of koffer en/of paspoorthouder(s) (aangekocht bij o.a. Louis Vuitton in de Bijenkorf voor ongeveer € 18.975) en/of
- een of meer contant(e) geldbedrag(en), waaronder een bedrag van ongeveer € 8.095 en/of € 4.300,- en/of
- een personenauto, van het merk Volkswagen Polo voorzien van het kenteken [kenteken] (aangekocht bij Fortis Automotive voor ongeveer € 9.600) en/of
- een (dure) jas, van het merk Sandro (aangekocht bij de Bijenkorf voor ongeveer € 369) en/of
- een of meer Balmain spijkerbroek(en) (aangekocht bij YOOX NET-A-PORTER) en/of
- een of meer cryptocurrency/cryptocurrencies tegoed(en) (aangekocht bij [naam 3] Exchange Services ter waarde van ongeveer € 30.580) en/of
- een of meer andere (luxe) goed(eren), waaronder kleding en/of schoenen en/of telefoon(s) aangekocht bij verschillende (web)winkels (Coolblue en/of BCC en/of Zalando en/of Wehkamp en/of Mediamarkt en/of bol.com en/of Suitsupply en/of Kenzo en/of Farfetch en/of Louboutin en/of Apple en/of Yoox) en/of
- een of meer andere Mastercard- en/of Paysafe- en/of spaar- en/of beleggingstegoed(en) (ter waarde van € 21.823 en/of € 9.125)

(telkens) heeft/hebben verworven, voorhanden heeft/hebben gehad, heeft/hebben overgedragen en/of omgezet, althans van een of meer voorwerp(en), te weten voornoemd(e) goed(eren) en/of geldbedrag(en), (telkens) gebruik heeft/hebben gemaakt, en/of

(telkens) de werkelijke aard, de herkomst, de vindplaats, de vervreemding, de verplaatsing heeft/hebben verborgen en/of verhuld en/of heeft/hebben verborgen en/of verhuld wie de rechthebbende op voornoemd voorwerp was en/of heeft/hebben verborgen en/of verhuld wie op voornoemd(e) voorwerp(en) voorhanden heeft/hebben gehad,

terwijl hij, verdachte en/of zijn mededader(s) (telkens) wist(en) althans redelijkerwijs moest(en) vermoeden dat die voorwerpen geheel of gedeeltelijk - onmiddellijk of middellijk - afkomstig waren uit enig(e) misdrijf/misdrijven, en hij, verdachte, van het plegen van dit/die feit(en) al dan niet een gewoonte heeft gemaakt;

Feit 4. (zaak 7)

hij op een of meer tijdstip(pen) in of omstreeks de periode van 1 oktober 2016 tot en met 14 mei 2019 te Oosterland, gemeente Schouwen-Duiveland en/of te Amsterdam en/of Almere en/of Erp in elk geval op een of meer plaats(en) in Nederland,

meermalen, althans eenmaal, (telkens) tezamen en in vereniging met een ander of anderen, althans

alleen,

(telkens) met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab eerste lid en/of 138b en/of 139c en/of 350a eerste lid en/of 350c Wetboek van Strafrecht wordt gepleegd (telkens) een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van (een) zodanig(e) misdrij(f)(ven), heeft/hebben verworven en/of heeft/hebben ingevoerd en/of heeft/hebben verspreid en/of anderszins ter beschikking heeft/hebben gesteld en/of voorhanden heeft/hebben gehad,

te weten malware Badr, zijnde schadelijke software en/of een computervirus (in de vorm van een programma en/of een bestand waarmee -zakelijk weergegeven- heimelijk een of meer persoonlijke gebruikersfunctie(s) en/of gebruikersgegeven(s) en/of inloggegeven(s) kunnen worden overgenomen)

en/of

een of meer computerwachtwoord(en), toegangscode(s) en/of daarmee vergelijkbaar gegeven(s), waardoor toegang kon worden gekregen tot een (deel van een) geautomatiseerd werk, te weten een (groot) aantal gebruikersgegeven(s) en/of inloggegeven(s), zijnde onder andere gebruikersnamen en (bijbehorend) wachtwoorden en/of creditcardgegevens, van een of meer (1809) geautomatiseerde werken (unieke machine id's) en/of (accounts van) personen

(telkens) heeft/hebben verworven en/of heeft/hebben ingevoerd en/of heeft/hebben verspreid en/of anderszins ter beschikking heeft/hebben gesteld en/of voorhanden heeft/hebben gehad;

Feit 5. (zaak 1 t/m 7)

hij in de periode van 1 oktober 2014 tot en met 14 mei 2019 te Oosterland, gemeente Schouwen-Duiveland en/of Amsterdam en/of Erp en/of Almere, in elk geval op een of meer plaats(en) in Nederland,

heeft deelgenomen aan een organisatie, welke organisatie tot oogmerk had het plegen van misdrijven, namelijk

- oplichting (artikel 326 Wetboek van Strafrecht) en/of
- identiteitsfraude (artikel 231b Wetboek van Strafrecht) en/of
- technische hulpmiddel en/of gegevens voorhanden hebben waardoor toegang kan worden gekregen tot (een) (deel van een) geautomatiseerd werk(en) (artikel 139d en/of 350d Wetboek van Strafrecht) en/of
- computervredebreuk (artikel 138ab Wetboek van Strafrecht) en/of
- aantasting of manipulatie van computergegevens (artikel 350a Wetboek van Strafrecht) en/of
- diefstal door middel van een valse sleutel (artikel 311 Wetboek van Strafrecht) en/of
- witwassen (artikel 420quater/bis/ter Wetboek van Strafrecht).

3 De voorvragen

<u>De geldigheid van de dagvaarding.</u>

De raadsvrouw heeft aangevoerd dat de tenlastelegging partieel nietig is, in die zin dat deze onvoldoende feitelijk, onvolledig en daardoor onbegrijpelijk is. In feit 3 wordt gesproken over het

witwassen van "*een of meer andere (luxe) goed(eren), waaronder kleding en/of schoenen en/of telefoon(s) aangekocht bij verschillende (web)winkels (Coolblue en/of BCC en/of Zalando en/of Wehkamp en/of Mediamarkt en/of bol.com en/of Suitsupply en/of Kenzo en/of Farfetch en/of Louboutin en/of Apple en/of Yoox)*"

Ondanks het feit dat er een uitgebreid zaaksdossier 'witwassen' in het dossier zit, is het voor de verdediging niet duidelijk om welke (luxe) goederen het gaat, onder meer nu in de onderliggende zaaksdossiers deze goederen niet worden gespecificeerd

In de woning en auto van verdachte zijn goederen in beslag genomen die afkomstig zijn van een aantal van de genoemde winkels. Ook zijn in de financiële gegevens van verdachte aanwijzingen gevonden voor aankopen bij de genoemde winkels. De rechtbank is dan ook van oordeel dat de tenlastelegging, gelezen in combinatie met dossier, voldoende duidelijk is en verdachte in staat moet worden geacht op basis hiervan zich adequaat te kunnen verdedigen.

De dagvaarding voldoet dus aan de eisen gesteld in artikel 261 Sv en is daarmee geldig. De rechtbank verwerpt derhalve het verweer van de verdediging.

De bevoegdheid van de rechtbank

De rechtbank is bevoegd.

De ontvankelijkheid van het Openbaar Ministerie.

De officier van justitie is ontvankelijk in de vervolging.

De schorsing van de vervolging

Er is geen reden voor schorsing van de vervolging.

4 De beoordeling van het bewijs

4.1 Het standpunt van de officier van justitie

De officier van justitie acht wettig en overtuigend bewezen dat verdachte de feiten heeft gepleegd. Zij baseert zich met name op de Teliogesprekken, de aangiftes, de (informatie uit de) in beslag genomen goederen, de processen-verbaal van bevindingen omtrent de financiële situatie van verdachte en de gegevens die zijn overgedragen vanuit onderzoek VARI.

4.2 Het standpunt van de verdediging

De verdediging is van mening dat de rechtbank niet tot een bewezenverklaring kan komen van feit 1 en wijst daarbij op het feit dat verdachte goederen in bewaring had voor [mededader 1] (hierna: [mededader 1]). Dit betrof mobiele telefoons, laptops, maar later ook koffers en kleding. Op momenten dat zijn eigen telefoon of laptop niet bruikbaar was, logde verdachte wel eens in op de apparaten van [mededader 1] . Op verzoek van [mededader 1] waardeerde verdachte ook beltegoed op, pinde hij een bedrag om een laptop te betalen en haalde en bracht hij de laptops en telefoons wanneer [mededader 1] daar om vroeg. Dat er sprake zou zijn van criminele activiteiten heeft verdachte nooit geweten.

Verdachte ontkent betrokken te zijn geweest bij de oplichting. Hij verklaart dat hij de gegevens

van [aangever] vond in de telefoon van [mededader 1] en deze heeft gekopieerd naar zijn eigen telefoon om [mededader 1] mee te confronteren. De cadeaukaarten van de Bijenkorf heeft hij uit een tas van [mededader 1] gepakt en gebruikt. Deze feiten leveren geen bewijs voor het (mede)plegen van oplichting. Op basis van het dossier kan immers niet worden vastgesteld dat verdachte zelf phishing e-mails heeft verzonden of dat hij personen heeft gebeld en zich heeft voorgedaan als een bankmedewerker. Verdachte heeft ook géén bijdrage van voldoende gewicht geleverd om van medeplegen te kunnen spreken.

Daarbij komt dat er in de zaken van aangevers [slachtoffer 2] , [aangever 2] , [slachtoffer 3] en [slachtoffer 4] telkens door aangevers zelf een nieuwe bankpas werd aangevraagd. Er is daarom geen sprake van het bewegen van de bank tot afgifte van de bankpassen door verdachten. verdachte dient daarom te worden vrijgesproken voor oplichting.

Subsidiair stelt de verdediging dat verdachte partieel dient te worden vrijgesproken ten aanzien van de oplichting van de Rabobank, ING, en 'een groot aantal' klanten, waardoor ook de pleegperiode dient te worden verkort.

Ten aanzien van feit 2 voert de verdediging aan dat geen van de in het dossier genoemde IP-adressen terug zijn te voeren op verdachte. Wel zijn deze (in sommige gevallen) te herleiden tot de BlackBerry KeyOne, Macbook PRO en de Lenovo laptop. Naast het alternatief scenario dat het bezit van verdachte van deze goederen verklaart, maakt het feit dat er contact is geweest met die genoemde goederen nog niet dat bewezen kan worden dat er sprake is geweest van computervredebreuk. Verdachte dient te worden vrijgesproken.

Subsidiair stelt de raadsvrouw dat, conform het aangevoerde ten aanzien van feit 1, partiele vrijspraak dient te volgen. Voor zover de rechtbank al bewezen acht dat verdachte op 23 februari 2019 met het IP-adres behorend bij de server Servitnow verbinding heeft gemaakt met de Rabobank webserver, dient de pleegperiode tot die dag beperkt te worden.

De verdediging refereert zich wat betreft feit drie aan het oordeel van de rechtbank waar het gaat om de schuldheling van twee Rolex horloges, de Louis Vuitton goederen, de Sandro jas en de Balmain broek, maat 28. Voor het overige dient verdachte te worden vrijgesproken.

De Volkswagen Polo is gedeeltelijk door de vader van verdachte betaald, het in de auto aangetroffen geld is van een kennis uit Engeland die op bezoek was gekomen. Het geld in het colbert van verdachte betreft een familiespaarpot van neven en nichten en de contante storting van € 4.300,- was van een afrekening tussen collega's na een uitje Madrid. Deze verklaringen leveren een begin van aannemelijkheid voor een andere herkomst dan de gestelde criminele herkomst. Het OM had hierop verder kunnen rechercheren, maar heeft dat niet of onvoldoende gedaan. Hetzelfde geldt voor de verklaring van verdachte voor de herkomst van de Rolex horloges, de tassen, de Balmain broeken, de opbrengsten van de cryptocurrency en de Paysafe tegoeden van verdachte. Het OM heeft geen getuigen gehoord die de lezing van verdachte zouden kunnen bevestigen. Verdachte dient daarom te worden vrijgesproken voor de opzetheling, nu niet kan worden bewezen dat de voorwerpen en het geld uit misdrijf afkomstig zijn, laat staan dat verdachte dat wist.

Ten aanzien van feit 4 verzoekt de verdediging om vrijspraak, nu verdachte zich niet bewust was van de aanwezigheid van malware op de apparaten die hij voor [mededader 1] in bewaring had. Daarmee kon verdachte ook niet de intentie ('het oogmerk') hebben deze malware te gebruiken.

Nu verdachte in geen van de ten laste gelegde feiten als deelnemer kan worden beschouwd, dient ook vrijspraak te volgen voor feit 5. Uit geen van de bewijsmiddelen blijkt van wetenschap van het plegen van strafbare feiten aan de zijde van verdachte, laat staan dat hij hieraan behulpzaam is geweest.

4.3 **Het oordeel van de rechtbank**

4.3.1 **Aanleiding van het onderzoek en aliassen verdachte**

Op 16 maart 2018 werd er in de cel van [mededader 2] een mobiele telefoon gevonden.

Deze telefoon is in beslag genomen en onderzocht. Uit de gegevens van deze telefoon blijkt dat er mogelijk contact was tussen [mededader 2] en [mededader 1] , beiden op dat moment verdachte in onderzoek VARI. Om die reden zijn de Teliogesprekken van [mededader 1] opgevraagd.[1] In deze gesprekken wordt er met regelmaat gesproken over [voornaam 2] , [voornaam 4] , [alias 2] en [voornaam 3] . Gelet op de inhoud van de gesprekken lijkt het over dezelfde persoon te gaan en zou deze persoon spullen van [mededader 1] hebben en betrokken zijn bij phishing en witwassen.

[mededader 1] sprak voornamelijk met de gebruikers van de nummers [gsm nummer] ([mededader 3] , hierna: [mededader 3] en [gsm.nr] ([mededader 4] hierna: [mededader 4]).[2]

Op 12 november 2017, 15:28 uur, belt [mededader 1] met [mededader 4] , waarbij gezegd wordt dat [alias 2] op vakantie is met [voornaam] , die ook [alias] wordt genoemd.[3] Om 15:34 uur belt [mededader 1] met [mededader 3] , waarbij hij vertelt dat [voornaam 2] in het buitenland is met [alias] .[4] Op 14 november 2017 belt [mededader 4] met [mededader 1] , waarin [mededader 4] zegt dat hij denkt dat [voornaam 3] nog steeds in het buitenland zit. [mededader 1] zegt daarop: "Ja, [alias 2] , [alias 2] ".[5]

Op 1 december 2017 zegt [mededader 1] tegen [mededader 3] dat "ze" in zijn privételefoon gekeken hebben naar foto's van [mededader 3] en [voornaam 2] .[6] In de telefoon van [mededader 1] zijn twee foto's gevonden waarop verdachte [verdachte] zichzelf herkent, en mogelijk ook [mededader 3] .[7]

Op 3 december 2017 zegt [mededader 4] tegen [mededader 1] dat hij [voornaam 4] gisteren zag. [mededader 1] vroeg: [alias 2] ? [alias 2] ?, waarna [mededader 4] verder spreekt over [alias 2] .[8]

Op 7 januari 2018 spreekt [mededader 1] met [mededader 4] over [alias 2] , die op dat moment in Ghana zou zijn.[9]

De telefoon van [mededader 4] werd in beslag genomen en onderzocht. Hieruit bleek dat er een gesprek plaatsvond waarin de naam " [voornaam 3] " voorkwam. Er wordt een bericht gedeeld over een schietpartij in [plaatsnaam] . [mededader 4] geeft aan dat " [voornaam 5] " gebeld moet worden, omdat [voornaam 3] op [plaatsnaam] woont. Ook wordt er gesproken over voorbereidingen om [voornaam 3] te 'klemmen'. Er wordt een screenshot gedeeld van een deurbel met namen erop, naar wat blijkt van de [adres] Later zegt [mededader 4] : "Hij heet [voornaam verdachte] he", waarop hij terugkrijgt: "Achternaam [achternaam verdachte] , toch". Daarna wordt nog de naam gedeeld van [ingeschrevene op adres verdachte] .[10]

Op Facebook is een account onder de naam " [voornaam 3] [achternaam verdachte] " gevonden.[11] Verdachte verklaart dat hij online gebruik maakt van dit alias.[12]

Onderzoek in de GBA wijst uit dat op [adres] , [voornaam 6] [achternaam verdachte] , moeder van verdachte [verdachte] woont. Op het huidige woonadres van [verdachte] staat eveneens [ingeschrevene op adres verdachte] (hierna: [ingeschrevene op adres verdachte]) ingeschreven. [ingeschrevene op adres verdachte] deelt nog een historisch GBA-adres met [verdachte] van augustus 2015 tot januari 2018.[13]

Tussenconclusie:

De rechtbank concludeert dat, gelet op de onderlinge samenhang van deze gesprekken, het verbeteren van de verschillende namen naar [alias 2] , en de overeenkomsten die er zijn op het gebied van de verblijven in het buitenland en het noemen van een reisgenoot, het buiten redelijke twijfel is dat [alias 2] , [voornaam 2] , [voornaam 4] en [voornaam 3] verschillende bijnamen zijn voor dezelfde persoon en dat deze persoon verdachte [verdachte] betreft.

4.3.2 **Zaaksdossier 1: [aangever]**

Op 22 december 2017 heeft [mededader 1] een gesprek met [mededader 3] , waarbij er gesproken wordt over het nieuws. [mededader 1] weet te melden dat het gaat over een

zaak waar [verdachte] en [mededader 4] betrokken bij waren. Er zou informatie staan op Telegraaf.nl en op crimesite.nl. Onderzoek wees uit dat er op meerdere nieuwssites vanaf die dag berichten waren geplaatst over een phishingbende. Aangever [aangever] werd genoemd als één van de slachtoffers.[14]

Op 3 januari 2017 werd door aangeefster [aangever 2] aangifte gedaan namens [bedrijfsnaam] . en VOF Landbouwbedrijf [aangever] , beide gevestigd te Oosterland. Zij verklaarde dat haar partner, de directeur van beide genoemde bedrijven (hierna: [aangever]), op 2 december 2016 een e-mailbericht had ontvangen waarvan hij dacht dat het afkomstig was van de Rabobank.[15] In deze e-mail stond vermeld dat nog een oude betaalpas gebruikt werd. Er zou inmiddels een nieuwe, veiligere, betaalpas zijn die nu nog kosteloos zou kunnen worden aangevraagd. In de e-mail stond een link waarop geklikt kon worden om de nieuwe betaalpas aan te vragen.[16]

[aangever] heeft omstreeks 14 december 2016 op de link geklikt. Op het moment dat hij probeerde in te loggen met de Random Reader werd hij gebeld door een vrouwelijke medewerker van de Rabobank. Zij vertelde hem dat zij zag dat hij probeerde in te loggen en bood haar hulp aan. De nieuwe pas werd twee dagen later bezorgd. Op 28 december 2016 kwam er een e-mail van de Rabobank waarin melding werd gemaakt van de aanvraag van een nieuwe betaalpas. Deze pas is nooit aangekomen. Op 2 januari 2017 wilde [aangever] inloggen op de rekeningen, maar dit bleek niet mogelijk met de pas van [bedrijfsnaam] . Met de pas van de VOF lukte dit wel, waarna hij zag dat er grote bedragen van de rekeningen waren gehaald.[17] Uit de details van de transacties blijkt dat er onder andere betalingen aan de Media Markt[18], Wehkamp[19], Zalando[20], Coolblue[21] en BCC zijn gedaan.[22] Daarnaast blijkt dat er een bestelling is geplaatst bij Bol.com voor iPhones en dat er acht betalingen zijn verricht voor een totaal van € 108.513,81 aan [naam 1] B.V. [naam 1] is een Payment Service Provider, die online betalingen verzorgt. In dit geval ging het om betalingen aan de webshops van Kenzo en Farfetch.[23]

4.3.3 **Verhandelen telefoons**

Uit informatie van Belsimpel.nl blijkt dat er op 30 december 2016, op naam van [slachtoffer 1] vier iPhones zijn besteld, welke op 31 december 2016 om 13:38 uur zijn geleverd op [adres 2] .[24]

Eén van deze iPhones werd op 12 januari 2017 in gebruik genomen door een telefoonnummer, geregistreerd op naam van [zwager van verdachte] . Uit de hierop volgende tap werd duidelijk dat het ging om de zwager van verdachte [verdachte] , te weten de partner van [voornaam 7] [verdachte] , zus van verdachte.[25]

Op 14 augustus 2019 werd in de auto van verdachte [verdachte] een iPhone 7 gevonden en in beslag genomen. Op deze iPhone werd een gesprek tussen [verdachte] en [zwager van verdachte] aangetroffen. In dit gesprek zegt [verdachte] op 31 december 2016, om 18:06 uur tegen [zwager van verdachte] dat hij vier iPhones heeft. [zwager van verdachte] vraagt voor hoeveel [verdachte] die weg wil doen.[26]

Tussen 1 februari 2017 en 16 februari 2017 wordt er over en weer gesproken over prijzen voor de "13 inch en 15 inch" en het regelen van een bon voor een telefoon die iemand wil kopen.[27] Op 26 maart 2017 zegt [zwager van verdachte] dat hij een 13 inch voor 1000 heeft weggedaan. Op 28 maart 2017: "nog een".[28]

4.3.4 **Technische gegevens servers**

De door [aangever] ontvangen e-mail is overgedragen aan de politie en werd op 4 januari 2017 onderzocht. Uit de header van de e-mail kan worden afgeleid dat deze verzonden is vanuit een vps server, te weten: " [vps nummer 1] ".[29] Aan de leverancier van deze server, [naam van de BV] B.V., is verzocht om de gegevens van de huurder van deze server te verstrekken. Via de payment service provider van [naam van de BV] ([naam 1]) werd gezien dat er, met één en dezelfde iPhone, betalingen werden verricht voor dit account, maar ook voor tien anderen. Onder deze tien bevonden zich de accounts [3 vps nummers] .[30] Aan

[naam van de BV] is verzocht een kopie van de servers te verstrekken voor nader onderzoek. Op de server van account ' [vps nummer 2] ' stond Windows Server 2012 R2 geïnstalleerd. Daarnaast was het programma 'Sendblaster' geïnstalleerd. Een licentie voor dit programma, noodzakelijk om een e-mail ineens naar tienduizenden e-mailadressen te sturen, werd afgegeven aan [gmail adres] .

In Sendblaster stonden twee adreslijsten: "TEST" en "1".

De lijst "Test" bevatte drie e-mailadressen, waaronder [email adres]

De lijst "1" bevatte 79.812 e-mailadressen van voornamelijk Nederlandse gebruikers.

In de documentmap "downloads" bevond zich een bestand genaamd 5.txt. De inhoud was gelijk aan de lijst "1".

Voor het versturen van e-mails via Sendblaster stond het volgende ingesteld:

Verstuurder: bankzaken@rabobank.nl

Naam van verstuurder: Rabobank

Onderwerp: Onze nieuwe dienstverlening voor 2017 staat klaar voor gebruik

De vanuit Sendblaster verstuurde berichten gingen over het aanvragen van een nieuwe betaalpas en hadden de huisstijl van de Rabobank. De e-mail bevatte een verkorte URL.[31]

In de map "C:\Users\Administrator\Downloads" bevond zich het bestand "2.txt." De inhoud van dit bestand kwam overeen met adreslijst "1" in het programma SendBlaster. Ik zag dat in het programma voor het versturen van email-berichten het volgende stond ingesteld:
Verstuurder: ing@emailing.nl
Naam van verstuurder: ING
Onderwerp: Laatste herinnering: U maakt nog geen gebruik van onze nieuwe betaalpas
In de map "C:\Users\Administrator\Downloads" bevond zich het bestand "GNI VERSTUREN.html".
De inhoud van het bestand kwam overeen met de verstuurde berichten in het programma SendBlaster. De e-mail, verzonden aan [slachtoffer 2] , is identiek aan de inhoud van dit bestand.[32]

Op de accounts [2 vps nummers][33] [2 vps nummers][34] werd een gelijksoortige situatie aangetroffen, maar dan gericht op andere financiële instellingen.

4.3.5 **Overeenkomsten in de verzonden e-mails**

In de loop van het onderzoek VARI ontvingen aangever [aangever] (2 december 2016)[35], verbalisant [naam verbalisant] (12 april 2017)[36], DNP Marketing (1 augustus 2017)[37], en verbalisant [naam verbalisant 2] (2 september 2017)[38] allen een e-mail die schijnbaar afkomstig was van de Rabobank. De e-mailberichten hadden dezelfde opbouw qua uiterlijk en de html opmaak in de broncode was gelijk. In alle e-mails stonden verkorte URL's, die verwezen naar een website die veel gelijkenis vertoonde met die van de Rabobank.[39] Op een van de servers, betrokken bij de phishingwebsite waarnaar gelinkt werd in de e-mail van verbalisant [naam verbalisant] , werd een e-mailbericht gevonden waarin een betaling aan [adres.com] werd geregistreerd. In dat bericht werd als account [naam account] gebruikt. Dit e-mail adres werd eerder gebruikt voor het bestellen van goederen via de rekening van aangever [aangever] .[40]

4.3.6 **Werking van de phishingwebsite**

De door verbalisant [naam verbalisant] ontvangen e-mail is nader onderzocht door verbalisant [naam verbalisant 3] . Hij heeft op de link geklikt, via de domeinnaam het IP-adres en de server achterhaald en deze in beslag genomen. Op deze server vond hij phishing websites, waaronder een gericht op Rabobank rekeninghouders.[41] De werkwijze zoals vervat in de website bestond uit vijf stappen:

1. Verkrijgen van het rekening- en pasnummer;[42]

2. Verkrijgen van gegevens van de benadeelde, waaronder pincode, naam, adres,

woonplaats, e-mailadres en telefoonnummer;[43]

3. Het laten verwerken van een kleurcode door de benadeelde, ter verkrijging van de verificatiecode;[44]

4. Het laten verwerken van een kleurcode door de benadeelde, ter verkrijging van de verificatiecode;[45]

5. Bevestigen van de ingevoerde gegevens en doorzenden naar de werkelijke site van de bank.[46]

Aan de phishingwebsites en het IP adres van de server waren verschillende domeinnamen gekoppeld. Voor ieder van deze domeinen geldt dat er, per genoemde bank, een map was aangemaakt met daarin de gegevens voor het doorsturen van de gephishte gegevens. De hiervoor ingestelde e-mailadressen waren onder andere [email adres .com 2] en [email adres]

De door een benadeelde ingevoerde gegevens werden opgeslagen in een bestand genaamd 1.txt. Opvallend daarbij is dat er, waar er op de website gevraagd wordt om een pasnummer en pincode, er in het tekstbestand wordt gesproken over een 'spa'nr en een 'nip'.[47]

De door stap 1 en stap 2 verkregen gegevens werden door de ontvanger gebruikt om via een smartphone in te loggen op de Rabobank bankieren app. Voor het koppelen van een nieuwe app aan een rekeningnummer is verificatie middels een kleurcode noodzakelijk. Hiervoor zijn de stappen 3 en 4 in de website gebouwd.[48]

De beheerder van de smartphone heeft nu de volledige controle over de (gekoppelde) rekening(en) van de benadeelde, waardoor er een nieuwe betaalpas kan worden aangevraagd.[49]

4.3.7 **Overige zaaksdossiers**

Zaaksdossiers VARI

In het vonnis van [mededader 1] , in overweging 4.3.5, staan de aangiftes en bewijsmiddelen die te relateren zijn aan de aangifte van [aangever] . Het gaat om 16 slachtoffers, die in 9 verschillende zaaksdossiers zijn ondergebracht.[50] Deze overweging is als bijlage bij dit vonnis opgenomen, waarbij wordt vermeld dat alle daarin genoemde bewijsmiddelen deel uitmaken van het huidige procesdossier.[51]

Zaaksdossier 2: [slachtoffer 2]

Op 25 oktober 2016 ontving aangever [slachtoffer 2] een e-mail die afkomstig leek van de ING bank. In deze e-mail werd hem verteld dat zijn pas bijna was verlopen en er een nieuwe moest worden aangevraagd.[52] Hij klikte op de link en vulde zijn gegevens in. Op 27 oktober 2016 werd hij gebeld door de ING bank, met de mededeling dat er binnen een kwartier

€ 3.490,- was afgeschreven. Daarvan was € 1.240 gepind en waren er 15 transacties bij Albert Heijn gedaan.[53] Uit de pingegevens van Albert Heijn bleek dat er op 27 oktober 2016, tussen 15:09 en 15:16 uur met deze pas 7 Mediamarkt- en 8 Bijenkorfkaarten waren gekocht, ieder met een waarde van € 150,-. Met de kaarten van de Bijenkorf waren aankopen gedaan, waarvan er van één van de aankopen camerabeelden voorhanden waren.[54]

De camerabeelden zijn opgevraagd. Op deze beelden is te zien dat een man op 28 oktober 2016, om 14:39 uur, een beige jas met kortharige bontkraag op de toonbank legt, en drie pasjes aan de kassière overhandigd.[55]

Verdachte verklaart dat hij degene is die deze jas heeft gekocht, en dat hij daar cadeaukaarten van de Bijenkorf voor heeft gebruikt.[56]

De e-mail die aan aangever [slachtoffer 2] werd verzonden, is verzonden vanaf IP adres [ip adres 1] Dit IP adres werd gebruikt door [naam van de BV] . ([vps nummer 3] public. [naam van de BV] .com [[ip adres 1]]).[57] Dit IP-adres is teruggevonden in een onder [mededader

1] in onderzoek VARI beslag genomen goed B03.01.005.[58] In datzelfde goed werden alle bank- en persoonsgegevens van aangever [slachtoffer 2] gevonden.[59]

Zaaksdossier 3: Schildersbedrijf [slachtoffer 4]

Op 19 februari 2019 ontving aangever [slachtoffer 3] een e-mail waarin stond dat haar Rabobank pas zou verlopen. Het ging om de zakelijke pas van Schilderwerken [slachtoffer 4] . In de e-mail stond een link waarmee zij haar pas kon vernieuwen. Zij klikte op de link, vroeg een nieuwe pas aan en ondertekende met de Raboreader. Op 23 februari 2019 zag zij dat er een aantal grote bedragen was afgeschreven.[60]

Aangever [slachtoffer 4] , directeur van A. [slachtoffer 4] en afwerkingsbedrijf, meldt dat er op 30 januari 2019 een e-mail werd ontvangen waarin stond dat de bankpas moest worden vervangen. Op 16 februari 2019 werd er € 90.000,- van de rekening van het bedrijf weggehaald.[61]

Uit de aangifte van de Rabobank blijkt dat er voor Schilderwerken [slachtoffer 4] een nieuwe bankpas is aangevraagd, waarna er een reeks aan overboekingen, opnames en storneringen plaatsvinden. In totaal is voor € 18.931,14 frauduleus overgeboekt naar derden.

Van de rekening van [slachtoffer 4] is in totaal € 89.328,10 overgeschreven naar derden. De Rabobank constateert dat er bij de aanvragen van de bankpassen van beide aangevers gebruik werd gemaakt van dezelfde Machine ID.[62]

Onder [verdachte] werd op 14 mei 2019 onder beslagnummer 1106NM57.01.03.004 in beslag genomen een Apple Macbook.[63] Dit goed is onderzocht. Het bleek te gaan om een Apple Macbook Pro A1989 (hierna: de Macbook A1989).[64] Hierop werd het programma "Thunderbird" aangetroffen. Hierin was een aantal e-mail accounts geïnstalleerd, waaronder [email adres]. In dit account stonden 4806 e-mailberichten die vrijwel allemaal afkomstig waren van phishing websites. De gegevens van Schilderwerken [slachtoffer 4] , en [slachtoffer 4] stonden daar in ieder geval tussen. Van hen waren onder andere het rekeningnummer, pincode, emailadres, en ANW-gegevens bekend.[65]

Zaaksdossier 4:

Op 28 april 2019 zag aangever [naam aangever] dat er een betaling van € 2.617,74 met zijn American Express gold card was gedaan bij Mediamarkt. Er waren twee Apple iPhones gekocht. Die aankopen had hij niet zelf gedaan.[66]

Uit contact met American Express blijkt dat door middel van cookie, PC Track en IP informatie 6 accounts die gerelateerd waren aan de fraude met elkaar kon worden verbonden, te weten de accounts van [naam aangever] , [naam aangever] , [naam aangever] , [naam aangever] en [voornaam aangever] [naam aangever] . Vermoed werd, dat er sprake was van een “Account Take Over”. Daarbij werden e-mailadressen, en telefoonnummers gewijzigd om te voorkomen dat de slachtoffers door hadden wat er gebeurde.

Uit de betalingsgegevens bleek dat er (onder andere):

- een bestelling was betaald bij Mediamarkt met de pas van [naam aangever] ,
- een bestelling was betaald bij Apple met de pas van [voornaam aangever]
- een bestelling was betaald bij Suitsupply.com met de pas van [voornaam aangever] ,
- een bestelling was betaald bij Yoox Net-a-Porter met de pas van [voornaam aangever] .[67]

De laatstgenoemde order van 25 maart 2019 is uitgeleverd op 26 maart 2019 op [adres 3] Het betrof een Balmain jeans, waaronder één met referentie [nr 1] , maat 28, € 990,-, met next day delivery. Bij de bestellingen is gebruik gemaakt van het IP adres [ip adres + kenmerk] Het betreft de server [vps naam] .gz.[68] De registratiegegevens van deze server (naam, adres, email en tel. nr.) werden teruggevonden op de Macbook A1989, vanuit een phishing actie bij Rabobank. Op 14 januari 2019 werden deze gegevens ontvangen op [email

adres] .[69]

Uit onderzoek aan de Macbook A1989 werd vastgesteld dat er vanuit deze laptop meerdere malen contact was gemaakt met IP adres [ip adres + kenmerk] , zijnde een server van Flexwebhosting. Vanuit deze server werd er, middels een Remote Desktop Protocol (RDP) vrijwel dagelijks contact gemaakt met het IP adres [ip adres + kenmerk][70] Op deze server werden in de data afbeeldingen gevonden van de ID kaart van [voornaam aangever] [naam aangever] en het paspoort van [naam aangever] . Daarnaast werden er twee afbeeldingen gevonden van American Express creditcards, op naam van [naam aangever] en [naam aangever] .[71]

Op 14 mei 2019 werd verdachte [verdachte] aangehouden in zijn auto. De losse goederen uit de auto zijn in dozen naar het politiebureau gebracht. Daar zijn ze gefotografeerd. Onder deze goederen bevond zich een factuur, gericht aan [naam aangever] , [adres 4] , met betrekking tot een Balmain Jeans, maat 28, voor € 990,-. Daarnaast werden er kosten berekend voor next day delivery.[72]

4.3.8 **In beslag genomen (luxe) goederen**

[adres]

Op 14 augustus 2019 werd in de woning aan [plaatsnaam] 57 te Amsterdam onder andere in beslag genomen:

- een jas, merk Sandro, beige-kleurig met lichte kraag en donkere knopen,
- een Rolex Oyster Perpetual, type Yacht-master,
- goederen van Louis Vuitton, te weten: zonnebril, sjaal, paspoort hoes (met paspoort [verdachte]), rugzak, sporttas, handtas, rugzak,
- zes spijkerbroeken van Balmain,
- een bedrag van € 6.740,-, in de binnenzakken van een colbert.[73]

Ten aanzien van de Rolex(en)

In de onder [mededader 1] in beslag genomen telefoon B03.01.002 in onderzoek VARI werd een foto aangetroffen waarop [mededader 1] en [verdachte] samen staan, vergezeld door een verkoper van Schaap en Citroen. Beiden hebben een doos met een Rolex horloge in de hand. Aan Schaap en Citroen is verzocht om de gegevens van deze aankoop, en eventuele eerdere aankopen te verstrekken. Hieruit bleek dat [initialen 1] [verdachte] , [plaatsnaam] 57 te Amsterdam op 23 februari 2015 een Rolex Oyster Perpetual, serienummer 3M43X116 voor € 9.990,00 en op 30 januari 2016 een Rolex Oyster Perpetual, serienummer [nr 2] , voor € 9.020,00 had gekocht. De facturen waren contant betaald.[74]

Ten aanzien van de Louis Vuitton goederen

In de onder [mededader 1] in beslag genomen telefoon B03.01.002 in onderzoek VARI werd een foto aangetroffen waarop [mededader 1] en [verdachte] samen staan, vergezeld door een vrouw en drie tassen op de voorgrond. Ook is er een tweede foto waarop een factuur te zien is van Louis Vuitton, locatie Bijenkorf Dam 1, Amsterdam, op naam van [voornaam 3] . Uit de opgevraagde gegevens van de Bijenkorf blijkt dat dit account is aangemaakt op 26 november 2013 en er sindsdien € 18.975,- is aangekocht onder dit klantprofiel. De factuur op de foto werd ook door de Bijenkorf toegestuurd. Hierop is te zien dat de factuur contant werd betaald met 132 briefjes van € 50,-. Uit de facturen blijkt dat er in ieder geval een rugtas, rolkoffer, koffer, clutch en twee paspoorthoezen zijn gekocht.[75]

Volkswagen Polo, [kenteken]

Op 14 augustus 2019 werd in de auto van [verdachte] , een Volkswagen Polo met kenteken [kenteken] onder andere in beslag genomen:

- een Apple iPhone 7,
- een Paysafe prepaid mastercard,

- een Louis Vuitton rugzak,

- een bedrag van € 1.355,-, in een bakje onder de stoel.[76]

Ten aanzien van de Paysafe prepaid mastercard

In de in beslag genomen Apple iPhone 7 werden de accountgegevens van twee Paysafecard accounts aangetroffen. Het ging om:
- [mededader 5] , [gsm nr 1] , [plaatsnaam] 57 Amsterdam,
- [voornaam verdachte] A. [verdachte] , [gsm nr 1] , [voornaam 3] . [emailadres 1] , [plaatsnaam] 57 Amsterdam.
Voor deze accounts zijn er 108 unieke vouchers ingewisseld voor 25-100 euro ieder. Vier daarvan, gekocht tussen 1 oktober 2014 en 31 november 2014, voor het account " [mededader 5] ", alle andere voor het account van [verdachte] .
In de periode van 22 maart 2015 tot en met 14 augustus 2017 is er voor € 9.125,- aan vouchers gekocht. De totale waarde van de aankopen en opwaarderingen bedraagt

€ 8.600,05. In de bankgegevens van [verdachte] is geen aankoop van een voucher terug te vinden.[77] [verdachte] verklaart dat deze accounts van hem zijn.[78]

[adres 5]
In de woning aan [adres 5] , het verblijfadres van de vriendin van [verdachte] :
- de doos van de Rolex Oyster Perpetual, type Yacht-master,
- een tweede doos voor een Rolex,
- een tas, handtas (met bon) en paspoorthouder van Louis Vuitton.[79]

4.3.9 **Onderzoek financiën en aangekochte goederen**

Onderzoek naar bankgegevens

Uit onderzoek naar de inkomsten en uitgaven van verdachte in de periode van 1 april 2016 tot en met 15 december 2018 zijn onderzocht. Hieruit blijkt dat verdachte een totaal van

€ 1.500,- heeft gestort op online beleggingsplatform DEGIRO, € 1.500,- naar [naam 3] Cryptocurrency exchange (hierna: [naam 3]) heeft overgemaakt en € 20.366,- op zijn spaarrekeningen heeft gestort.[80]

Uit informatie van [naam 3] blijkt dat het account van [verdachte] in de periode van 18 juli 2017 tot en met 2 februari 2018 gevoed werd met een totaal (geschat) bedrag van € 34.955,64.

In de periode van 13 februari 2019 tot en met 3 april 2019 werd gezien dat verdachte op 7 maart 2019 een contant bedrag van € 4.300,- stortte op zijn bankrekening.[81]

Onderzoek naar overige goederen

Op 9 januari 2016 werd er een bestelling voor schoenen geplaatst bij Louboutin op naam van [mededader 1] . Het afleveradres betrof [adres] .[82]

Uit onderzoek aan de in beslag genomen Macbook A1989 blijkt dat er in de internethistorie melding wordt gemaakt van de aankoop van een giftcard voor Suit Supply op naam van [voornaam aangever] .[83]

Aankoop Volkswagen Polo

Op 30 oktober 2015 werd er door Fortis Automotive aan verdachte [verdachte] een Volkswagen Polo Bluemotion geleverd, met kenteken [kenteken] , voor een bedrag van € 9.600,-. Daarbij staat genoteerd dat het bedrag in 2 termijnen is betaald, eenmaal € 4.750,- en eenmaal

€ 4.850,-.[84]

Uit de analyse van de bankrekening van verdachte in de periode van 1 januari 2015 tot en met 31 maart 2016 blijkt niet van een girale overboeking naar de verkoper van de auto.[85]

4.3.10 **Overig (digitaal) onderzoek**

Macbook Pro A1398

Op 14 augustus 2019 is onder verdachte een Macbook Pro A1398 (hierna: Macbook 1398) in beslag genomen. De Username was "j.n.", Displayname " [voornaam verdachte] n" en het AccountID [voornaam verdachte] . [verdachte] @hotmail.com. In dit Macbook is (onder andere) een foto gevonden met daarop [mededader 1] , [verdachte] , [mededader 4] , [mededader 3] en een onbekend gebleven persoon. Alle vijf de mannen laten de rode onderkant van hun schoen zien.[86]

Lenovo laptop

Op 14 augustus 2019 werd in de woning van [verdachte] een Lenovo laptop aangetroffen. Ook werd er een factuur aangetroffen voor de aanschaf van deze laptop. Het betrof een contante betaling, met een girale bijbetaling van € 177,87. De bankrekening waar deze bijbetaling mee is gedaan behoort toe aan verdachte [verdachte] .[87]

Macbook Pro A1989

Uit onderzoek aan de Macbook 1989 bleek dat er data aanwezig was, verkregen door malware. Het ging om "Arkei Stealer" en Baldr. Beide programma's betreffen "info stealers", die van geïnfecteerde computers gebruikersnamen, wachtwoorden, creditcardnummers en andere gevoelige informatie proberen te achterhalen.

Er waren 1809 unieke Machine ID's te zien, afkomstig van "Arkei Stealer". Van vrijwel ieder apparaat was een schermafdruk gemaakt en waren gebruikersnamen, wachtwoorden en andere identificerende gegevens te zien. De beheerstool om deze gegevens te beheren was ook aanwezig op de laptop. In de gegevens van de [naam server] -server werd gezien dat het beheerspaneel van Baldr via die server werd benaderd.

De Baldr malware, en het beheerspaneel, werden aangetroffen in de veiliggestelde gegevens van deze laptop.[88]

Daarnaast werd er, onder andere, geconstateerd dat:

- het e-mail account [email adres] gekoppeld was aan het e-mail programma "Thunderbird",

- dat er in het account [email adres] 6109 berichten zaten, waaronder phishinggegevens gericht op onder andere American Express, Rabobank, SNS Bank en ABN AMRO. 161 berichten waren afkomstig van IP adres van de [naam server] server.[89]

- het e-mailaccount [emailadres 2] in gesteld was als standaard e-mailadres in het programma "tutanota-desktop",

- de gebruikersnaam van deze laptop " [naam 2] " is,

- [voornaam verdachte] . [verdachte] @hotmail.com en " [nr 3] " recent gebruikt waren,

- er op 1 februari 2019 via Google gezocht werd naar "gstar fraud junior".

- de login voor de [naam server] (zie 4.3.7) " [naam 2] ", en het password " [pasword] !" was.[90]

iPhone 7

Uit onderzoek aan de iPhone 7 van [verdachte] is gebleken dat:

- er een Instagramaccount bestaat met gebruikersnaam " [naam 2] .A", welk is gekoppeld aan e-mailadres [voornaam verdachte] . [verdachte] @icloud.com.

- er notities in de telefoon stonden met (onder andere) als inhoud:

- [emailadres 3] – Rabobank2019!

- [emailadres 2]

- 1-11-2016: "[code]"

- 16-12-2016, " [track en tracecode] ”

- twee track and trace codes die overeenkomen met de bezorging van iPhones, besteld bij Coolblue en betaald vanaf de rekening van [aangever] .[91]

BlackBerry KeyOne (BBB100-2)

Op 13 en 26 januari 2019 maakt [verdachte] beltegoed over van zijn bankrekening naar Lebara, voor telefoonnummer [gsm nr 2] . Bij deze overboeking worden respectievelijk [emailadres 2] en [voornaam verdachte] . [verdachte] @hotmail.com opgegeven als e-mailadressen.[92]

Vastgesteld werd dat dit telefoonnummer gebruikt werd in de Apple iPhone 7, de Apple iPhone X en de BlackBerry KeyOne (hierna: de BlackBerry), alle drie in beslag genomen onder [verdachte] . Ook waardeerde [verdachte] tweemaal het beltegoed op van nummer [gsm nr 3] , welk nummer eveneens in de BlackBerry had gezeten.[93]

Onderzoek wees uit dat deze twee nummers gebruikt zijn in de BlackBerry in de periode van 21 augustus 2018 tot en met 20 februari 2019. Van 16 december 2018 tot 13 januari 2019 is de BlackBerry niet gebruikt met deze nummers.[94] [verdachte] verbleef van 15 december 2018 tot 13 januari 2019 in Ghana.[95]

Er is een beperkt aantal gesprekken (4 uitgaand, 14 ingaand), maar een groot aantal datasessies (2.500).

Met deze BlackBerry werd op 2 maart 2019, tussen 16:42 en 16:47 uur gebruikmakend van telefoonnummer. [nr 4] , de website www.rabobank.nl.betaalsysteem.info bezocht. Deze site wordt gehost door Reg.RU en is aangemaakt op 1 maart 2019. Van 16:45 uur tot 16:47 uur werden ook de officiële websites van de Rabobank benaderd.[96]

Uit onderzoek aan de data betreffende de telefoontap op nummer ... [nr 4] bleek dat er met behulp van een Remote Desktop Protocol verbinding werd gemaakt met het [ip adres 2] (zie 4.3.7). Er waren in ieder geval twee apparaten gekoppeld aan de BlackBerry die gebruik maakten van de dataverbinding, te weten een Apple Macbook en een Lenovo laptop.[97]

In de periode van 19 februari 2019 tot en met 18 maart 2019 is er een data- en voice tap geplaatst op nummer .. [nr 4] . in de hele periode werd dit nummer alleen gebruikt in de BlackBerry.

Op 3 maart 2019 is er een datasessie van ongeveer een uur, waarbij het nummer aanstraalt op een zendmast op Schiphol. Er vond een datasessie plaats van ruim een uur. Omdat het nummer vanaf 10:17 uur met telkens ongeveer een minuut er tussen aanstraalde in Amsterdam, Purmerend, Nigtevecht en Maarssen, wordt vermoed dat het toestel zich op dat moment in een vliegtuig bevond. Op dezelfde dag, tot 10:07 uur, straalde het nummer van [verdachte] (.. [nr 5]) ook aan op de masten rondom Schiphol. Uit een tapgesprek van 7 maart 2019 blijkt dat [verdachte] naar Spanje is geweest voor een Champions League wedstrijd.[98]

Op 9 april 2019 nam verdachte contact op met de klantenservice van Lyca Mobile, waarbij hij wilde weten welke instellingen hij moest gebruiken om dataverkeer mogelijk te maken met een BlackBerry.[99]

Over het meenemen van de telefoon verklaart verdachte zelf dat het klopt dat hij deze telefoon regelmatig bij zich droeg, ook in het buitenland.[100]

Server Flexwebhosting 46.17.3.35 ([naam server])

De server is onderzocht. Op deze server werd, onder andere gevonden:

- tekstbestanden met e-mailadressen, gerubriceerd op onderwerpen als “verzekering”, “gemeente Rijswijk”, “Amsterdam”,

- meer dan 3 miljoen opgeslagen e-mailadressen,

- het programma “Email Extractor”, geregistreerd op [emailadres 4] ,

- het programma Sendblaster, geregistreerd op [gmail adres] ,

- 13 tekstbestanden met daarin phishing e-mails gericht op verschillende banken.[101]

Beltegoed.nl

Uit onderzoek aan de bankrekening van verdachte is gebleken dat hij in de periode van 6 april 2016 tot 9 oktober 2018 16 maal beltegoed heeft gekocht. Op twee directe opwaarderingen van Ghanese nummers na, werd er telkens een opwaardeercode naar een e-mailadres gestuurd. De bijbehorende e-mailadressen waren: [voornaam verdachte] . [verdachte] @gmail.com, [emailadres 2] , [emailadres 7] en [emailadres 6] .[102]

Het e-mailadres [emailadres 8] komt 2050 keer terug, verdeeld over diverse in beslag genomen GSM toestellen in onderzoek VARI. Het e-mailadres werd onder andere gebruikt voor het bestellen van phishing websites en goederen.

In het in onderzoek VARI in beslag genomen goed met nummer B01.02.001 werden koppelingen naar deze e-mailadressen gevonden, waaronder:

- een e-mail van [gmail adres] naar [emailadres 8] met daarin een IBAN en BIC/SWIFT nummer.
- een notitie " http:// [emailadres 9] "
- een inlog in het account [emailadres 7] .[103]

4.3.11 **Betrokkenheid [verdachte] en alternatief scenario**

De rechtbank stelt vast dat verdachte een alternatief scenario schetst en daarmee stelt dat hij met de strafbare feiten niets van doen heeft gehad. Verdachte verklaart immers dat hij gedurende langere periode meerdere goederen in bewaring had voor [mededader 1] . Dat ging niet alleen om elektronica, bijvoorbeeld de Macbook Pro A1989, Lenovo, of BlackBerry, maar ook om andere luxe goederen, zoals Balmain broeken, Louis Vuitton tassen, of cadeaukaarten. Op momenten dat [mededader 1] tegen verdachte zei dat hij iets nodig had, zorgde verdachte er voor dat dit bij [mededader 1] terecht kwam. Hetzelfde gold voor de opwaarderingen van de telefoonnummers. Op het moment dat [mededader 1] aan verdachte vroeg om beltegoed te regelen, dan deed verdachte dat. Hoewel verdachte hier eerst geen vraagtekens bij zette, heeft hij op enig moment wel ingelogd op de elektronica die hij voor [mededader 1] moest bewaren. Van een aantal opmerkelijke zaken maakte verdachte aantekeningen in zijn eigen telefoon, zodat hij daar vragen over kon stellen aan [mededader 1] . [mededader 1] wist hem echter gerust te stellen, waardoor verdachte doorging met het bewaren van spullen.

Tussenconclusie rechtbank omtrent het alternatief scenario

Gelet op de hierboven opgesomde bewijsmiddelen valt het de rechtbank (onder andere) op dat verdachte in het bezit is van de BlackBerry en daar ook het beltegoed voor betaalt. De telefoonnummers die gebruikt worden in deze BlackBerry, worden ook gebruikt in de iPhone 7 en de iPhone X die verdachte verklaart te gebruiken. De BlackBerry neemt verdachte overal mee naar toe en voor het opwaarderen van beltegoed gebruikt hij e-mailadressen die gelinkt worden aan phishing, en zelfs terug te voeren zijn naar meerdere zaaksdossiers in onderzoek VARI.

Met de BlackBerry wordt, middels een RDP, de [naam server] server bediend. De inlognaam voor deze server is gelijk aan de Instagram accountnaam van verdachte. Op deze server zijn een veelvoud aan phishing en malware gerelateerde zaken gevonden. De BlackBerry is met regelmaat aan twee andere apparaten gekoppeld, die beide ook bij verdachte zijn aangetroffen.

De Macbook Pro A1989 heeft ook dezelfde inlognaam als de Instagram accountnaam van verdachte. Op deze Macbook zijn, naast een veelvoud aan zaken die gelieerd kunnen worden aan phishing en malware, ook persoonlijke zaken van verdachte teruggevonden.

In de iPhone 7 van verdachte zijn aantekeningen gevonden waarin inlog gegevens voor e-mailaccounts staan en persoonlijke gegevens van slachtoffer [aangever] , twee dagen nadat hij op de link in zijn e-mail had geklikt. Opvallend detail is de spelfout in de bedrijfsnaam. Ook is er een gesprek met zijn zwager over de verkoop van vier iPhones, nadat er vier iPhones zijn gekocht met geld van [aangever] , die vier uur daarvoor afgeleverd waren op een nabij adres.

Waar er voor verdachte telkens dwarsverbanden zijn te vinden tussen de telefoons, servers en Macbooks en zijn persoonlijke informatie geldt dat niet voor [mededader 1] . Van enig gebruik van voornoemde elektronica door [mededader 1] is in het hele dossier niet gebleken. Deze verklaring van verdachte wordt daarom op geen enkel vlak ondersteund. De rechtbank is daarom ook van oordeel dat deze verklaring volstrekt onaannemelijk is. Zij gaat er dan ook van uit dat verdachte de (hoofd)gebruiker was van de in zijn woning aangetroffen goederen. De rechtbank ziet zich gesterkt in deze opvatting door de grote hoeveelheid luxe goederen die verdachte in zijn bezit heeft. Verdachte draagt Rolex horloges van bijna € 10.000,-, heeft meerdere Louis Vuitton tassen, en draagt dure merkschoenen en –kleding. Deze goederen passen niet bij de levensstijl die verwacht kan worden bij personen met het legale inkomen zoals verdachte dat kent. Bovendien komt uit het onderzoek naar voren dat het merendeel van deze goederen contant zijn betaald.

Tussenconclusie rechtbank omtrent de betrokkenheid verdachte

De rechtbank is van oordeel dat verdachte een minder zichtbare, maar niet minder belangrijke rol vervulde bij een (in wisselende samenstelling opererende) groep van personen die zich bezig hield met phishing-fraude. Hij had toegang tot de digitale middelen die noodzakelijk waren voor het plegen van de feiten en beheerde (mede) de bijbehorende servers, zorgde voor de doorverkoop van de met gestolen geld gekochte goederen, en maakte de buitgemaakte cadeaukaarten te gelde. De rechtbank stelt dan ook vast dat verdachte actief was bij alle facetten van het plegen van deze feiten.

4.3.12 **Overwegingen ten aanzien van feiten 1 en 2**

Uit de hierboven genoemde bewijsmiddelen blijkt dat in de ten laste gelegde periode op meerdere tijdstippen e-mails zijn verzonden naar klanten van de Rabobank en de ING bank, waarbij deze klanten werden aangespoord een nieuwe bankpas aan te vragen. Deze e-mailberichten leken van die banken afkomstig, doordat de naam en huisstijl van die banken werden gebruikt. Daarbij zorgde het programma "Sendblaster" ervoor dat het ook leek alsof de e-mail werd verzonden vanaf een e-mailadres van die banken. De hyperlink die vermeld werd in deze e-mail leidde hen naar een website waarop rekeningnummer, pasnummer, pincode, telefoonnummer en e-mailadres ingevoerd moesten worden. Die gegevens werden door de website automatisch doorgezonden naar [mededader 1] . Met deze gegevens kon [mededader 1] beginnen met het registreren van een nieuwe mobiele telefoon voor de bankier app. Indien dit niet direct mogelijk was, deelde hij de gegevens met [mededader 6] zodat zij de betreffende klant kon bellen. Terwijl [mededader 6] aan de lijn was met de klant, onderhielden [mededader 6] en [mededader 1] contact met elkaar om de timing goed te houden. [mededader 1] moest op de achtergrond ervoor zorgen dat de juiste codes op de website verschenen, zodat hij de registratie kon voltooien. Na het scannen van de codes had [mededader 1] de volledige controle over de rekening van het slachtoffer, alsmede over de daaraan gekoppelde rekeningnummers. Vanaf dat moment kon en werd er, zonder dat daarvoor een code hoefde te worden gescand, een nieuwe betaalpas aangevraagd. Deze betaalpas was nodig om het geld van de rekening van het slachtoffer door te boeken naar een andere rekening.

Voor de banken leek het, door deze handelwijze, alsof de rechtmatige eigenaar van de rekening een verzoek deed om een nieuwe bankpas te mogen ontvangen, waardoor tot uitgifte werd overgegaan. Het verweer van de verdediging dat aangevers zelf een nieuwe pas hebben aangevraagd en daarom geen sprake kan zijn van oplichting, zal daarom ook worden verworpen.

Gelet op al hetgeen hier naar voren is gebracht en het feit dat de rechtbank het alternatief scenario niet geloofwaardig acht, is de rechtbank van oordeel dat wettig en overtuigend bewezen is dat verdachte zich, in bewuste en nauwe samenwerking met een ander, schuldig heeft gemaakt aan de onder 1 en 2 ten laste gelegde feiten.

Aan de door de verdediging bepleite beperking van de pleegperiode gaat de rechtbank voorbij. Zoals in het voorgaande is overwogen bestond de handelwijze als geheel uit vele losse 'stappen'. Een beperking van de pleegperiode tot de dag waarop een specifieke e-mail is verstuurd gaat aan die vaststelling voorbij.

4.3.13 **Overwegingen ten aanzien van feit 3**

De rechtbank stelt allereerst vast dat sprake is van opbrengsten uit eigen misdrijf.

De Hoge Raad heeft in het arrest van 21 april 2015[104] overwogen dat in het geval het witwassen de opbrengsten van eigen misdrijf betreft, van de witwasser – om tot de kwalificatie 'witwassen' te kunnen komen – in beginsel een handeling wordt gevergd die op verhullen/verbergen is gericht en dat dan uit de motivering door de rechter moet kunnen worden afgeleid dat de verdachte het voorwerp niet slechts heeft verworven of voorhanden heeft gehad, maar dat zijn gedragingen ook (kennelijk) gericht zijn geweest op het daadwerkelijk verbergen of verhullen van de criminele herkomst van het voorwerp.

De rechtbank is van oordeel dat het doorboeken van geld van de rekening van de slachtoffers naar andere (voor verdachte bereikbare) rekeningen, het kopen en uitgeven van (anonieme) cadeaukaarten, en het aanschaffen van goederen met het geld van slachtoffers en deze vervolgens voor contanten doorverkopen verhullingshandelingen betreffen.

Verdachte was intensief betrokken bij het plegen van strafbare feiten en plukte daar, direct, de vruchten van. Hij werkte samen met (onder andere) [mededader 1] en deed dat al gedurende langere tijd. Gelet op de bovengenoemde bewijsmiddelen en de betrokkenheid van verdachte bij het plegen van de strafbare feiten, stelt de rechtbank vast dat verdachte van witwassen een gewoonte maakte.

Dit maakt dat de rechtbank bewezen acht dat verdachte zich schuldig heeft gemaakt aan het in bewuste en nauwe samenwerking met anderen plegen van witwassen ten aanzien van de twee Rolex horloges, de Louis Vuitton goederen, de contanten in het colbert en in de auto van verdachte, de € 4.300,- die door verdachte contant werd gestort, de Volkswagen Polo, de jas van Sandro, de Balmain broeken, de luxe goederen bij de diverse (web)winkels en de tegoeden op de Paysafe kaart.

Ook ten aanzien van de spaar- en beleggingstegoeden overweegt de rechtbank dat er sprake is van witwassen. In de bevraagde periode is het girale vermogen van verdachte met ruim

€ 21.000,- toegenomen. Deze toename is, naar het oordeel van de rechtbank, toe te schrijven aan het feit dat verdachte door zijn criminele activiteiten geld opzij heeft kunnen zetten.

Ten aanzien van de cryptocurrency tegoeden overweegt de rechtbank dat verdachte een verklaring heeft gegeven voor het verwerven hiervan, te weten dat hij al jaren handelt in digitale valuta en daar winsten mee heeft behaald. Het is een feit van algemene bekendheid dat met de handel in digitale valuta, met name voor diegenen die "vroeg" zijn ingestapt, grote winsten behaald konden worden. Het is daarom niet zonder meer onaannemelijk dat verdachte een van deze personen zou kunnen betreffen. Verdachte heeft verklaard bij verschillende sites geregistreerd te hebben gestaan, maar uiteindelijk alle tegoeden bij [naam 3] bijeen te hebben gebracht. Uit de stukken blijkt, naar het oordeel van de rechtbank, niet dat dit juist, maar ook niet dat dit onjuist is. Nu aldus niet met voldoende zekerheid valt vast te stellen dat deze tegoeden afkomstig zijn van opbrengsten uit (eigen) misdrijf, zal de rechtbank verdachte voor dit onderdeel partieel vrijspreken.

4.3.14 **Overwegingen ten aanzien van feit 4**

Gelet op de hierboven genoemde bewijsmiddelen en de constatering dat het alternatief scenario van verdachte als onaannemelijk wordt gezien, stelt de rechtbank vast dat verdachte op de hoogte was van de inhoud van de gegevens op de Macbook A1989, maar ook op de [naam server] server en daar ook actief gebruik van maakte. Op dit apparaat en op deze server is malware gevonden waarmee persoonsgegevens kunnen worden buitgemaakt (Baldr malware), maar ook de resultaten van een soortgelijk programma (Arkei Stealer malware). Dat verdachte het oogmerk had om met deze gegevens strafbare feiten te plegen, blijkt uit bewijsoverwegingen die de rechtbank voor de hiervoor behandelde feiten heeft opgenomen. Gelet op de aard van de aangetroffen malware en gegevens gaat het in ieder geval om het oogmerk tot het plegen van feiten als omschreven in artikelen 138ab, 138b en 139c Wetboek van Strafrecht.

Gelet op de werkwijze ten aanzien van de American Express creditcards, kan ook bewezen worden verklaard dat verdachte het oogmerk had tot het plegen van feiten als omschreven in artikelen 350a en 350c Wetboek van Strafrecht. De accounts van de creditcardhouders die werden benaderd werden gewijzigd, om te voorkomen dat men voortijdig ontdekt zou worden.

De rechtbank is daarom ook van oordeel dat wettig en overtuigend kan worden bewezen dat verdachte dit feit heeft gepleegd.

4.3.15 **Overwegingen ten aanzien van feit 5**

Voor het vaststellen van het bestaan van een criminele organisatie in de zin van artikel 140 Wetboek van Strafrecht blijken uit de geldende jurisprudentie de navolgende criteria.

Er moet sprake zijn van een samenwerkingsverband, van twee of meer personen met een zekere duurzaamheid en structuur en een bepaalde organisatiegraad, dat tot (feitelijk en gewenst) doel heeft het plegen van misdrijven. De deelnemers aan zo'n organisatie dienen niet ieder voor zich, maar in het verband van deze organisatie te participeren en dus te behoren tot de organisatie. Daarbij is het niet noodzakelijk dat zij bekend waren met alle andere personen die deel uitmaakten van de organisatie dan wel met alle andere personen in de organisatie samenwerken. De samenstelling van het samenwerkingsverband hoeft niet steeds dezelfde te zijn geweest.

Om iemand te kunnen aanmerken als deelnemer dient hij of zij tenminste een aandeel te hebben in, dan wel ondersteuning te verlenen aan, gedragingen die strekken tot of rechtstreeks verband houden met de verwezenlijking van het oogmerk van die organisatie.

De bijdrage dient een zekere duur en intensiteit te hebben alvorens gesteld kan worden dat sprake is van deelname. In dat verband is specifieke deelneming aan misdrijven waarop het oogmerk van de organisatie is gericht niet nodig, maar wel de wetenschap van het plegen van misdrijven in zijn algemeenheid. Daarbij is voorwaardelijk opzet niet voldoende. Wetenschap van één of verscheidene concrete misdrijven is niet vereist. Evenmin enige vorm van opzet op de door de organisatie beoogde concrete misdrijven.

Uit de hierboven genoemde bewijsmiddelen blijkt dat een grote mate van samenwerking bestond tussen meerdere personen, waarbij verdachte een grote rol heeft gespeeld. Verdachte is in het geheel betrokken geweest van het begin – het verkrijgen van persoonlijke informatie middels malware – tot het einde – de verkoop van de met gestolen geld gekochte goederen. Gelet op het tijdsbestek waarin dit alles diende te gebeuren, moet er een grote mate van organisatie zijn geweest om een en ander voor elkaar te krijgen. Voordat een slachtoffer door had dat geldbedragen werden afgeschreven, moest het geld immers al zijn opgenomen van de rekeningen en moesten van dat geld bestelde goederen zijn opgehaald van de afleveradressen. Het feit dat, ondanks het uitgebreide onderzoek in de zaak VARI, verdachte destijds buiten schot is weten te blijven, toont naar het oordeel van de rechtbank aan dat er een grote mate van coördinatie plaats heeft moeten vinden.

De rechtbank is dan ook van oordeel dat wettig en overtuigend bewezen kan worden verklaard dat er een criminele organisatie bestond die tot oogmerk had oplichting,

computervredebreuk, witwassen en het voorhanden hebben van malware met het oogmerk tot verkrijging van gegevens waarmee toegang kan worden verkregen tot geautomatiseerde werken en aantasting of manipulatie van computergegevens.

Uit het voorgaande volgt dat verdachte als deelnemers van deze organisatie kan worden aangemerkt.

4.4 **De bewezenverklaring**

De rechtbank acht wettig en overtuigend bewezen dat verdachte

Feit 1. (zaak 1 t/m 3)

in de periode van 1 oktober 2016 tot en met 14 mei 2019 in Nederland, meermalen, telkens tezamen en in vereniging met een of meer anderen, telkens met het oogmerk om zich en/of een ander wederrechtelijk te bevoordelen door het aannemen van een valse naam en van een valse hoedanigheid en door listige kunstgrepen en door een samenweefsel van verdichtsels,

telkens een groot aantal Rabobank-klanten en/of ING-klanten waaronder

• [slachtoffer 1] en

• [slachtoffer 2] en

• [slachtoffer 3] en

• [slachtoffer 4]

hebben bewogen tot het ter beschikking stellen van gegevens, te weten:

- rekening gegevens en

- pincode en

- verificatiecode en

- de (inlog)gegevens (gebruikersnaam en/of wachtwoord) van/voor het (internet)bankieren van/bij de Rabobank en/of ING, door - zakelijk weergegeven - onder meer:

- gebruik te maken van de namen en/of bedrijfsnamen en/of bedrijfslogo's van de Rabobank en ING en

- vervolgens een mail te sturen naar voornoemde personen om een nieuwe bank- en/of betaalpas aan te vragen en

- vervolgens in die mail te vragen om een nieuwe bank- en/of betaalpas aan te vragen door op de (hyper)link in de mail te klikken en

- vervolgens in dat aanvraagformulier te vragen om voornoemde gegevens in te vullen en

- vervolgens tijdens het invullen voornoemde personen te bellen als zijnde een medewerker van de Rabobank om samen met voornoemde personen de invulvelden door te lopen/in te vullen,

waardoor die voornoemde Rabobank- en ING- klanten telkens werden bewogen tot het ter beschikking stellen van bovenomschreven gegevens,

en vervolgens

de Rabobank en ING heeft bewogen tot de afgifte van enig goed, te weten een of meer bankpassen en/of betaalpassen, door -zakelijk weergegeven - onder meer:

- in te loggen met de inloggegevens van voornoemde Rabobank- en ING-klanten in de beveiligde internetbankieren-omgeving van de Rabobank en ING en

- vervolgens in die omgeving een nieuwe bankpas aan te vragen,

waardoor die Rabobank en ING telkens werd bewogen tot bovenomschreven afgiften;

Feit 2. (zaak 1 t/m 3)

in de periode van 1 oktober 2016 tot en met 14 mei 2019 in Nederland, meermalen, telkens tezamen en in vereniging met een ander of anderen, telkens opzettelijk en wederrechtelijk in een

geautomatiseerd werk, te weten de computers en/of servers van de (beveiligde) internetbankieren omgeving van de Rabobank en ING, is binnengedrongen, waarbij hij, verdachte, en zijn mededaders telkens de toegang hebben verworven tot de geautomatiseerde werken

- met behulp van valse sleutels, te weten de inloggegevens voor het internetbankieren (te weten de gebruikersnaam en het wachtwoord) van de Rabobank en ING en

- door het aannemen van een valse hoedanigheid, te weten zijnde een of meer geautoriseerde Rabobank- en ING-klanten waaronder

• [slachtoffer 1] en

• [slachtoffer 2] en

• [slachtoffer 3] en

• [slachtoffer 4] ;

Feit 3. (zaak 1 t/m 5)

in de periode van 1 oktober 2014 tot en met 14 mei 2019 in Nederland, tezamen en in vereniging met een ander of anderen, voorwerpen, te weten:

- 2 horloges, van het merk Rolex (aangekocht bij Schaap en Citroen voor ongeveer

€ 19.010,-) en

- goederen van het merk Louis Vuitton, waaronder tassen en een sjaal en een zonnebril en een koffer en paspoorthouders (aangekocht bij o.a. Louis Vuitton in de Bijenkorf voor ongeveer € 18.975,-) en

- contante geldbedragen, waaronder een bedrag van ongeveer € 8.095 en € 4.300,- en

- een personenauto, van het merk Volkswagen Polo voorzien van het kenteken [kenteken] (aangekocht bij Fortis Automotive voor ongeveer € 9.600) en

- een jas, van het merk Sandro (aangekocht bij de Bijenkorf voor ongeveer € 369) en

- Balmain spijkerbroeken (aangekocht bij YOOX NET-A-PORTER) en

- andere luxe goederen, waaronder kleding en schoenen en telefoons aangekocht bij verschillende (web)winkels (Coolblue en BCC en Zalando en Wehkamp en Mediamarkt en bol.com en Suit Supply en Kenzo en Farfetch en Louboutin en Apple en Yoox) en

- Mastercard- en Paysafe- en spaar- en beleggingstegoeden (ter waarde van € 21.823,- en

€ 9.125,-) heeft verworven, voorhanden heeft gehad, heeft overgedragen en omgezet, en

(telkens) de herkomst, heeft verborgen en verhuld, terwijl hij, verdachte en zijn mededaders telkens wisten dat die voorwerpen - onmiddellijk of middellijk - afkomstig waren uit enige misdrijven, en hij, verdachte, van het plegen van dit feit een gewoonte heeft gemaakt;

Feit 4. (zaak 7)

in de periode van 1 oktober 2016 tot en met 14 mei 2019 in Nederland, meermalen, telkens met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab eerste lid en 138b en 139c en 350a eerste lid en 350c Wetboek van Strafrecht wordt gepleegd een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van zodanige misdrijven, voorhanden heeft gehad, te weten malware Baldr, zijnde schadelijke software (in de vorm van een programma waarmee -zakelijk weergegeven- heimelijk persoonlijke gebruikersfuncties en gebruikersgegevens en inloggegevens kunnen worden overgenomen)

en computerwachtwoorden, toegangscodes en daarmee vergelijkbare gegevens, waardoor toegang kon worden gekregen tot een (deel van een) geautomatiseerd werk, te weten

een groot aantal gebruikersgegevens en inloggegevens, zijnde onder andere gebruikersnamen en (bijbehorende) wachtwoorden en creditcardgegevens, van een of meer (1809) geautomatiseerde werken (unieke machine ID's) en accounts van personen telkens voorhanden heeft gehad;

Feit 5. (zaak 1 t/m 7)

in de periode van 1 oktober 2014 tot en met 14 mei 2019 in Nederland, heeft deelgenomen aan een organisatie, welke organisatie tot oogmerk had het plegen van misdrijven, namelijk

- oplichting (artikel 326 Wetboek van Strafrecht) en

- identiteitsfraude (artikel 231b Wetboek van Strafrecht) en

- technische hulpmiddel en gegevens voorhanden hebben waardoor toegang kan worden gekregen tot (een) (deel van een) geautomatiseerde werken (artikel 139d en/of 350d Wetboek van Strafrecht) en

- computervredebreuk (artikel 138ab Wetboek van Strafrecht) en

- aantasting of manipulatie van computergegevens (artikel 350a Wetboek van Strafrecht) en

- diefstal door middel van een valse sleutel (artikel 311 Wetboek van Strafrecht) en

- witwassen (artikel 420quater/bis/ter Wetboek van Strafrecht).

Voor zover in de tenlastelegging kennelijke taal- en/of schrijffouten voorkomen, zijn die fouten in de bewezenverklaring verbeterd. Verdachte is daardoor niet in zijn verdediging geschaad.

De rechtbank acht niet bewezen hetgeen meer of anders is ten laste gelegd. Verdachte zal daarvan worden vrijgesproken.

5 De strafbaarheid

Er zijn geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van de feiten uitsluiten. Dit levert de in de beslissing genoemde strafbare feiten op.

Verdachte is strafbaar, omdat niet is gebleken van een omstandigheid die zijn strafbaarheid uitsluit.

6 De strafoplegging

6.1 De vordering van de officier van justitie

De officier van justitie vordert aan verdachte op te leggen een gevangenisstraf voor de duur van 48 maanden met aftrek, waarvan 12 maanden voorwaardelijk.

6.2 Het standpunt van de verdediging

De verdediging verzoekt de rechtbank, op het moment dat er een bewezenverklaring zou volgen, te volstaan met een straf gelijk aan het voorarrest. Verdachte zat ruim zes maanden vast, waarvan een maand in beperkingen. Dit is hem zeer zwaar gevallen. Nadat hij vrij is gekomen heeft hij een baan gevonden en werkt hij aan zijn toekomst. De reclassering heeft positief over hem bericht en zijn werkgever is ook positief over hem. Hij heeft een relatie en trouwplannen. Verdachte heeft er hard aan gewerkt zijn leven op de rit te krijgen. Het doorkruisen van deze ontwikkelingen is niet in zijn belang. Indien er een zwaardere straf zou moeten volgen dan de al uitgezeten straf, verzoekt de verdediging om een forse voorwaardelijke straf op te leggen.

6.3 Het oordeel van de rechtbank

De rechtbank is van oordeel dat verdachte zich schuldig heeft gemaakt aan het (medeplegen) van oplichting, computervredebreuk, witwassen en het voorhanden hebben van malware met het oogmerk van verkrijging van gegevens waarmee toegang kan worden verkregen tot geautomatiseerde werken en aantasting of manipulatie van computergegevens, alsmede aan deelname aan een criminele organisatie. De organisatie verstuurde in groten getale misleidende e-mails uit naam van een bank of andere financiële instelling, met daarin een link naar een ‘phishing website’. Op deze website werd slachtoffers verzocht hun gegevens achter te laten, waarmee

verdachte en zijn mededaders toegang verkregen tot de online bankieren omgeving van de slachtoffers. Nadat een nieuwe pinpas was aangevraagd en afgevangen, kon de rekening van het slachtoffer middels overboekingen naar 'money mules', pintransacties en betalingen aan diverse webshops worden leeggehaald. Dat dit een nauwgezette planning en coördinatie vraagt, is uit het dossier wel gebleken. Verschillende personen moesten op de juiste tijdstippen over de juiste (persoonlijke) gegevens van een slachtoffer beschikken. De acties moesten elkaar op de juiste manier en binnen een kort tijdsbestek opvolgen om de kans op ontdekking te minimaliseren. Gelet op de pleegperiodes van deze feiten, heeft dit jaren door kunnen gaan.

Verdachte heeft in dit geheel een zeer grote rol gespeeld. Dit blijkt vooral uit de in beslag genomen gegevensdragers, waarin zowel aanwijzingen zijn gevonden voor bemoeienis met het verzamelen van persoonsgegevens, als het doorverkopen van met het gestolen geld gekochte goederen.

De mate van organisatie en coördinatie, vereist om dit soort feiten te kunnen plegen, overschrijdt naar het oordeel van de rechtbank de 'gewone' fraude zaken. De potentiele schade en maatschappelijke impact van 'phishing' is enorm. Daarbij komt dat het een relatief 'veilige' vorm van criminaliteit is, waarbij verdachten zich vaak kunnen verschuilen achter een web van digitale versluieringen en daardoor heel moeilijk te traceren zijn. Het voorkomen van dit soort feiten vergt voortdurend een grote oplettendheid van banken, andere instellingen en al hun klanten. De bestrijding van phishingfraude is complex en vergt een grote inspanning van het Openbaar Ministerie. Dit blijkt temeer uit het feit dat het verdachte is gelukt om in het onderzoek VARI, ondanks dat dit een zeer omvangrijk onderzoek betrof, buiten schot te blijven. Ook nu realiseert de rechtbank zich dat verdachte het achterste van zijn tong niet heeft laten zien. De BlackBerry, van waaruit de server met malware werd aangestuurd, is immers op slot gebleven. Het vermoeden is dan ook dat ook hier de werkelijke schade (vele malen) groter is dan dat naar voren is gekomen in het dossier.

Gelet op al hetgeen hier genoemd is, is de rechtbank van oordeel dat alleen een forse gevangenisstraf op zijn plaats kan zijn. Zoals reeds toegelicht heeft verdachte een grote en cruciale rol gehad in een zeer professioneel opererende criminele organisatie die verantwoordelijk is geweest voor het oplichten van een groot aantal personen. De aard en ernst van de feiten, de lange pleegperiode, de omvang van de schade en intensiteit van het samenwerkingsverband maken dat de rechtbank komt tot een gevangenisstraf van 36 maanden, waarvan 12 voorwaardelijk met een proeftijd van drie jaar, met aftrek van de tijd die verdachte in voorarrest heeft doorgebracht.

7 De benadeelde partij

7.1 Vordering benadeelde partij Rabobank

De Rabobank heeft een vordering ingediend ter hoogte van € 70.793,47. Ter onderbouwing van deze vordering heeft zij aangevoerd dat klanten van de Rabobank door het handelen van verdachte zijn gedupeerd, en dat de Rabobank hen, uit coulance, heeft gecompenseerd.

Bij de beoordeling van de vordering van de vordering van een benadeelde partij dient het volgende als uitgangspunt.

Maatstaf onrechtmatigheid

Op de vordering van de benadeelde partij is het materiële burgerlijk recht van toepassing (HR 28 mei 2019, ECLI:NL:HR:2019:793). Op grond van het bepaalde in artikel 6:162 BW is degene die een toerekenbare onrechtmatige daad pleegt jegens een ander verplicht de schade die de ander dientengevolge lijdt te vergoeden. Op grond van art. 6:166 BW zijn alle leden van de groep hoofdelijk aansprakelijk voor de schade die één van de leden van de groep heeft veroorzaakt. Voor het aannemen van groepsaansprakelijkheid is vereist dat de kans op het aldus (met de

groep) toebrengen van schade verdachte had behoren te weerhouden van zijn gedragingen in groepsverband (HR 2 oktober 2015, ECLI:NL:HR:2015:2914).

Maatstaf schadebegroting

Voor vergoeding aan de benadeelde partij komt overeenkomstig de regels van het materiële burgerlijk recht slechts in aanmerking de schade die de benadeelde partij heeft geleden als gevolg van de onrechtmatige gedragingen van de verdachte, voor zover deze schade op de voet van art. 6:98 BW aan de verdachte kan worden toegerekend (HR 28 mei 2019, ECLI:NL:HR:2019:793). Daartoe dient te worden beoordeeld in hoeverre de door de benadeelde partij gevorderde schade redelijkerwijze kan worden toegerekend aan het schadeveroorzakende (onrechtmatige) handelen van verdachte.

Stelplicht

Op de benadeelde partij rust in beginsel de last de feiten en omstandigheden te stellen - en in geval van betwisting daarvan bewijs bij te brengen - die tot toewijzing van haar vordering kunnen leiden. Worden voornoemde feiten en omstandigheden betwist dan zal de rechter aan de hand van de onderbouwing van de stellingen over en weer moeten beoordelen of de feiten en omstandigheden die tot toewijzing van de vordering kunnen leiden in voldoende mate zijn komen vast te staan (HR 28 mei 2019, ECLI:NL:HR:2019:793).

Ontvankelijkheid in het strafproces

De civiele vordering van de benadeelde partij is toewijsbaar in het strafproces voor zover de schade een 'rechtstreeks gevolg' geacht kan worden te zijn van het bewezenverklaarde feit. De concrete omstandigheden van het geval zijn bepalend voor de beantwoording van de vraag of voldoende verband bestaat tussen het bewezenverklaarde handelen van de verdachte en de door de benadeelde geleden schade om te kunnen aannemen dat de benadeelde door dit handelen rechtstreeks schade heeft geleden (HR 5 juli 2016, ECLI:NL:HR:2016:1522). Rechtsopvolgers onder bijzondere titel van de benadeelde partij kunnen niet in hun vordering worden ontvangen in het strafproces (HR 5 oktober 1965, ECLI:NL:HR:1965:AB3848, NJ 1966/292)."

De rechtbank overweegt dat in het bewezenverklaarde feit en hetgeen daartoe door de rechtbank is overwogen besloten ligt het oordeel dat verdachte jegens de Rabobank onrechtmatig heeft gehandeld en uit dien hoofde schadeplichtig is.

De schade die de Rabobank vordert betreft evenwel schade die haar rekeninghouders hebben geleden en die de Rabobank – naar zij heeft gesteld – onverplicht heeft vergoed aan deze rekeninghouders. De Rabobank acht zich – zo begrijpt de rechtbank haar vordering – gesubrogeerd in de rechten van de door haar gecompenseerde klanten. Voor deze schade geldt dat de Rabobank niet rechtstreeks schade heeft geleden door een strafbaar feit. Zij vordert deze schade immers als rechtsopvolgster van haar rekeninghouders.

Dit maakt dat de rechtbank de Rabobank niet-ontvankelijk in haar vordering zal verklaren. De Rabobank kan haar vordering aanbrengen bij de burgerlijke rechter.

7.2 **Vordering benadeelde partij ING**

De ING heeft een vordering ingediend ter hoogte van € 3.619,-.

De rechtbank overweegt, met inachtneming van dezelfde uitgangspunten zoals verwoord onder 7.1, dat in het bewezenverklaarde feit en hetgeen daartoe door de rechtbank is overwogen besloten ligt het oordeel dat verdachte jegens de ING onrechtmatig heeft gehandeld en uit dien hoofde schadeplichtig is.

Een deel van de door de ING gevorderde schade, € 120,-, betreft de onderzoekskosten die de ING in deze zaak heeft gemaakt. Deze schade ziet de rechtbank als schade die is toe te rekenen aan het onrechtmatige handelen van verdachte en ook als een rechtstreeks gevolg van het strafbare

feit kan worden aangemerkt.

Ter onderbouwing van het overige deel van deze vordering, € 3.490,-, heeft zij aangevoerd dat een klant van de ING door het handelen van verdachte is gedupeerd, en dat de ING deze klant voor dit bedrag schadeloos heeft gesteld. ING acht zich – zo begrijpt de rechtbank de vordering – gesubrogeerd in de rechten van de door haar onverplicht gecompenseerde klant. Voor deze schade geldt dat ING niet rechtstreeks schade heeft geleden door een strafbaar feit. Zij vordert deze schade immers als rechtsopvolgster van een rekeninghouder.

Dit maakt dat de rechtbank de ING niet-ontvankelijk in haar vordering zal verklaren. De ING kan haar vordering aanbrengen bij de burgerlijke rechter.

8 Het beslag

8.1 De onttrekking aan het verkeer

Het hierna in de beslissing genoemde in beslag genomen voorwerp is vatbaar voor onttrekking aan het verkeer.

Gebleken is dat het feit is begaan met behulp van dit voorwerp.

8.2 De verbeurdverklaring

De hierna in de beslissing genoemde in beslag genomen voorwerpen zijn vatbaar voor verbeurdverklaring.

Gebleken is dat deze voorwerpen aan verdachte toebehoren en deze geheel of grotendeels door middel van strafbare feiten zijn verkregen, dan wel dat de feiten zijn begaan of voorbereid met behulp van deze voorwerpen.

9 De wettelijke voorschriften

De beslissing berust op de artikelen 14a, 14b, 14c, 33, 33a, 36b, 36c, 58, 138ab, 139d, 140, 326 en 420 van het Wetboek van Strafrecht zoals deze artikelen luidden ten tijde van het bewezen verklaarde.

10 De beslissing

De rechtbank:

Voorvragen

- verklaart de dagvaarding geldig;

Vrijspraak

- **spreekt verdachte partieel vrij** van hetgeen onder feit 3 ten laste is gelegd ten aanzien van de cryptocurrency;

Bewezenverklaring

- verklaart het ten laste gelegde bewezen, zodanig als hierboven onder 4.4 is omschreven;

- spreekt verdachte vrij van wat meer of anders is ten laste gelegd;

Strafbaarheid

- verklaart dat het bewezen verklaarde de volgende strafbare feiten oplevert:

feit 1: medeplegen van oplichting, meermalen gepleegd

feit 2: medeplegen van computervredebreuk, meermalen gepleegd

feit 3: medeplegen van witwassen, meermalen gepleegd

feit 4: met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c van het Wetboek van Strafrecht wordt gepleegd, een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, voorhanden hebben

en

met het oogmerk dat daarmee een misdrijf als bedoeld in art. 350a, eerste lid, of 350c Sr wordt gepleegd, voorhanden hebben van een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf en het voorhanden hebben van een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan;

feit 5: deelname aan een criminele organisatie

- verklaart verdachte strafbaar;

Strafoplegging

- veroordeelt verdachte tot **een gevangenisstraf van 36 maanden, waarvan 12 maanden voorwaardelijk met een proeftijd van drie jaar**;

- bepaalt dat het voorwaardelijke deel van de straf niet ten uitvoer wordt gelegd, tenzij de rechter tenuitvoerlegging gelast, omdat verdachte voor het einde van de proeftijd de hierna vermelde voorwaarden niet heeft nageleefd;

- stelt als **algemene voorwaarde** dat verdachte zich voor het einde van de proeftijd niet schuldig maakt aan een strafbaar feit;

- bepaalt dat de tijd die verdachte voor de tenuitvoerlegging van dit vonnis in voorarrest heeft doorgebracht in mindering wordt gebracht bij de tenuitvoerlegging van de opgelegde gevangenisstraf;

Voorlopige hechtenis

- heft de schorsing van de voorlopige hechtenis op;

Beslag

- verklaart verbeurd de inbeslaggenomen voorwerpen, te weten:
- 1 STK Kaart, G_532564, Mastercard
- 1 STK Kaart, G_532551, Cadeaukaart Visa
- 1 STK Kaart, _532539, Cadeaucard Bijenkorf
- 1 STK Telefoonautomaat _31212;

- verklaart onttrokken aan het verkeer de onder verdachte in beslag genomen BlackBerry KeyOne;

Benadeelde partijen

- verklaart de benadeelde partij Rabobank niet-ontvankelijk in hun vordering en bepaalt dat die vordering bij de burgerlijke rechter kan worden aangebracht.

Benadeelde partijen

- veroordeelt verdachte tot betaling aan de benadeelde partij ING van € 120,-, ter zake van materiële schade;

- verklaart de benadeelde partij in het overige gedeelte van de vordering niet-ontvankelijk en bepaalt dat de vordering voor dat gedeelte bij de burgerlijke rechter kan worden aangebracht;

- veroordeelt verdachte tevens in de kosten van de benadeelde partij tot nu toe gemaakt en ten behoeve van de tenuitvoerlegging nog te maken, tot op heden begroot op nihil.

Dit vonnis is gewezen door mr. Goossens, voorzitter, mr. Felix en mr. Schild, rechters, in tegenwoordigheid van Van Rensch, griffier, en is uitgesproken ter openbare zitting op 26 juni 2020.

---

[1] Indien wordt verwezen naar een paginanummer van het eindproces-verbaal met dossiernummer ZBRDD18003 (onderzoek "Korcullu") van de dienst regionale recherche Cyber team Zeeland-West-Brabant, opgemaakt in de wettelijke vorm door daartoe bevoegde opsporingsambtenaren en doorgenummerd van 1 tot en met G0000 0162 Proces-verbaal van bevindingen aangaande Teliogesprekken tussen [initialen 2] [mededader 1] , [naam 6] en [naam 7] over een persoon door hen aangeduid als [voornaam 2] / [alias 2] / [voornaam 4] / [voornaam 3] , pag. A0000 0202

[2] Proces-verbaal identificatie aliassen [voornaam 2] , [voornaam 4] , [alias 2] en [voornaam 3] , pag. A0000 0138

[3] Geschrift, zijnde een tapgesprek, pag. A0000 0221

[4] Geschrift, zijnde een tapgesprek, pag. A0000 0222

[5] Geschrift, zijnde een tapgesprek, pag. A0000 0153

[6] Geschrift, zijnde een tapgesprek, pag. A0000 0205

[7] Proces-verbaal van verhoor verdachte, pag. B0000 0226

[8] Geschrift, zijnde een tapgesprek, pag. A0000 0206

[9] Geschrift, zijnde een tapgesprek, pag. A0000 0274

[10] Geschrift, zijnde een uittreksel van een WhatsApp gesprek, pag. A0000 0168

[11] Geschrift, zijnde een kopie van de Facebook homepage van [voornaam 3] [achternaam verdachte] , pag. A0000 0170

[12] Proces-verbaal van verhoor verdachte, pag. B0000 0165

[13] Proces-verbaal van bevindingen, pag. A0000 0145

[14] Proces-verbaal van bevindingen aangaande Teliogesprekken tussen [initialen 2] [mededader 1] en [naam 6] en [naam 7] over een persoon door hen aangeduid als [voornaam 2] / [alias 2] / [voornaam 4] / [voornaam 3] , pag. A0000 0212

[15] Indien wordt verwezen naar een paginanummer van het eindproces-verbaal met dossiernummer ZBRAA17009 (onderzoek "Vari") van de regionale eenheid politie Zeeland-West-Brabant, opgemaakt in de wettelijke vorm door daartoe bevoegde opsporingsambtenaren en doorgenummerd van 1 tot en met 4657, wordt er achter het paginanummer "VARI" vermeld. Proces-verbaal van aangifte [aangever 2] , pag. 584 VARI

[16] Geschrift, zijnde een uitdraai van de ontvangen e-mail, als bijlage bij de aangifte, pag. 591 VARI

17 Proces-verbaal van aangifte [aangever 2] , pag. 585 VARI
18 Geschrift, zijnde een uitdraai van de details van een transactie, pag. 604 VARI
19 Geschrift, zijnde een uitdraai van de details van een transactie, pag. 609 VARI
20 Geschrift, zijnde een uitdraai van de details van een transactie, pag. 610 VARI
21 Geschrift, zijnde een uitdraai van de details van een transactie, pag. 614 VARI
22 Geschrift, zijnde een uitdraai van de details van een transactie, pag. 618 VARI
23 Proces-verbaal van bevindingen, pag. C0001 0015
24 Proces-verbaal van bevindingen, pag. G0000 0012
25 Proces-verbaal van bevindingen, pag. G0000 0019
26 Geschrift, zijnde een uitdraai van chatgesprek, pag. G0000 0108
27 Geschrift, zijnde een uitdraai van chatgesprek, pag. G0000 0109
28 Geschrift, zijnde een uitdraai van chatgesprek, pag. G0000 0111
29 Geschrift, zijnde een uitdraai van de header van de e-mail, pag. 639 VARI
30 Proces-verbaal van bevindingen, pag. 642 e.v. VARI
31 Proces-verbaal van bevindingen, pag. 95 e.v. VARI
32 Proces-verbaal van bevindingen [naam van de BV] – vps 53537, pag. C0002 0186
33 Proces-verbaal van bevindingen, pag. 103 e.v. VARI
34 Proces-verbaal van bevindingen, pag. 115 e.v. VARI
35 Geschrift, zijnde een e-mailbericht verzonden aan [aangever] , pag. 636 VARI
36 Proces-verbaal van bevindingen, pag. 153 e.v. VARI
37 Geschrift, zijnde een e-mailbericht verzonden aan DNP Marketing, pag. 104 (dossier "Willis")
38 Proces-verbaal van bevindingen, pag. 215 e.v. VARI
39 Proces-verbaal van bevindingen beschrijving modus operandi, pag. 233 VARI
40 Proces-verbaal van bevindingen onderzoek phishingkit server [nr 6] , Pag. 164 VARI
41 Proces-verbaal van bevindingen onderzoek phishingkit server [nr 6] , Pag. 160 VARI
42 Proces-verbaal van bevindingen modus operandi, pag. 240 VARI
43 Proces-verbaal van bevindingen modus operandi, pag. 241 VARI
44 Proces-verbaal van bevindingen modus operandi, pag. 243-244 VARI
45 Proces-verbaal van bevindingen modus operandi, pag. 246-247 VARI
46 Proces-verbaal van bevindingen onderzoek phishingkit server [nr 6] , Pag. 161 VARI
47 Proces-verbaal van bevindingen onderzoek phishingkit server [nr 6] , pag. 168 VARI
48 Proces-verbaal van bevindingen modus operandi, pag. 242 e.v. VARI
49 Proces-verbaal van bevindingen modus operandi, pag. 248 VARI
50 Geschrift, zijnde een vonnis ten aanzien van verdachte [mededader 1] in de zaak VARI, pag. A0000 0328
51 Zie bijlage "overweging 4.3.5", aan het vonnis gehecht
52 Geschrift, zijnde de door [slachtoffer 2] ontvangen e-mail, pag. C0002 0057
53 Proces-verbaal van aangifte [slachtoffer 2] , pag. C0002 0042
54 Proces-verbaal van bevindingen, pag. C0002 0044
55 Proces-verbaal van bevindingen, pag. C0002 0046
56 Proces-verbaal van verhoor verdachte, pag. B0000 0166
57 Proces-verbaal van onderzoek IP adres, pag. C0002 0160
58 Proces-verbaal van aantreffen server gegevens in goed VARI uit onderzoek, pag. C0002 0181

[59] Proces-verbaal van aantreffen gegevens [slachtoffer 2] in goed VARI uit onderzoek, pag. C0002 0200

[60] Proces-verbaal van aangifte [slachtoffer 3] , pag. C0003 0013

[61] Proces-verbaal van aangifte [slachtoffer 4] , pag. C0003 0040

[62] Proces-verbaal van aangifte fraude / phishing Rabobank, pag. C 0003 0021

[63] KVI, pag. D0000 0191

[64] Proces-verbaal veiligstellen Apple Macbook Pro A1989, pag. D 0000 0147

[65] Proces-verbaal van bevindingen, pag. C0003 0060

[66] Proces-verbaal van aangifte [naam aangever] , pag. C0004 0042

[67] Proces-verbaal van bevindingen, pag. C0004 0057

[68] Proces-verbaal van bevindingen, pag. C0004 0066-67

[69] Proces-verbaal veiligstellen Apple Macbook Pro A1989, pag. D 0000 0147

[70] Proces-verbaal van bevindingen, pag. C0004 0006

[71] Proces-verbaal van bevindingen, pag. C0004 0020

[72] Proces-verbaal van bevindingen, pag. C0004 0081

[73] Lijst van in beslag genomen goederen, pag. D0000 0071 e.v.

[74] Proces-verbaal van bevindingen, pag. A 0000 0044

[75] Proces-verbaal van bevindingen, pag. C0001 0099

[76] Proces-verbaal van bevindingen, pag. D0000 0117

[77] Proces-verbaal verstrekking gevorderde gegevens, pag. C0005 0190

[78] Proces-verbaal van verhoor verdachte, pag. B0000 0165

[79] Proces-verbaal van bevindingen, pag. C0005 0004

[80] Proces-verbaal van bevindingen gevorderde bankgegevens, pag. C0005 0040

[81] Proces-verbaal van bevindingen gevorderde bankgegevens, pag. C0005 0111

[82] Geschrift, zijnde een factuur van Louboutin, pag. C0000 0067

[83] Proces-verbaal van bevindingen, pag. A0000 1110

[84] Geschrift, zijnde een koopcontract / factuur, pag. C0005 0186

[85] Proces-verbaal van bevindingen gevorderde bankgegevens, pag. C0005 0166

[86] Proces-verbaal van bevindingen, pag. A0000 0039

[87] Proces-verbaal van bevindingen aankoop Lenovo laptop Mediamarkt, pag. A0000 1030

[88] Proces-verbaal van bevindingen, pag. C0007 0085

[89] Proces-verbaal van bevindingen onderzoek Macbook Pro A1989, pag. A0000 1101

[90] Proces-verbaal gebruik accountnaam [naam 2] door [verdachte] , pag. A0000 1042

[91] Proces-verbaal van bevindingen, pag. C0001 0060

[92] Proces-verbaal van bevindingen, pag. A0000 0538

[93] Proces-verbaal van bevindingen, pag. A0000 0051

[94] Proces-verbaal van bevindingen, pag. A0000 0571

[95] Proces-verbaal van bevindingen, pag. A0000 0452

[96] Proces-verbaal van bevindingen, pag. A0000 0571

[97] Proces-verbaal van bevindingen, pag. A0000 0598

[98] Proces-verbaal van bevindingen, pag. A0000 0988

[99] Geschrift, zijnde een uitdraai van een tapgesprek, pag. C0004 0129

[100] Verklaring van verdachte, afgelegd ter terechtzitting van 29 mei 2020

101 Proces-verbaal van bevindingen, pag. A0000 0831

102 Proces-verbaal van bevindingen bestellingen Beltegoed.nl, pag. C0001 0108

103 Proces-verbaal van bevindingen gebruik emailadressen [verdachte] , pag. C0001 0112

104 Vindplaats: ECLI:NL:HR:2015:1090