Computerrecht 2020/88

Rechtbank Rotterdam 19 maart 2020,
nr. 10/961510-19
(Mrs. I.M.A. Hinfelaar, J.J. Bade en R.J.A.M. Cooijmans)
m.nt. prof. mr. dr. J.J. Oerlemans[1]

(Art. 139d lid 2 sub a jo. art. 138ab Sr)

ECLI:NL:RBROT:2020:2395

In deze zaak ontwikkelde de verdachte een programma (Rubella Macro Builder), waarmee aan Office-documenten zoals Word en Excel een stuk verborgen code wordt toegevoegd. Bij het openen van een geïnfecteerd document wordt de code uitgevoerd. Daarmee maakt de verdachte het bijvoorbeeld mogelijk andere malware te downloaden op de computers van slachtoffers. De verdachte heeft zich schuldig gemaakt aan het vervaardigen, verkopen, verspreiden en voorhanden hebben van malware met het oogmerk computervredebreuk te plegen.

(…)
raadsvrouw mr. F.E. den Hertog, advocaat te Amersfoort.
(…)

3. **Eis officier van justitie**

De officier van justitie mr. W.S. Koorn heeft gevorderd:
- bewezenverklaring van het onder 1 en 2 ten laste gelegde;
- veroordeling van de verdachte tot een gevangenisstraf voor de duur van 18 maanden met aftrek van voorarrest, waarvan 6 maanden voorwaardelijk, met een proeftijd van 2 jaar.

4. **Waardering van het bewijs**

4.1 ***Bewezenverklaring feit 2 zonder nadere motivering***
Het onder 2 ten laste gelegde voorhanden hebben van creditcardgegevens is door de verdachte bekend. Dit feit zal zonder nadere bespreking bewezen worden verklaard.

4.2 ***Bewijswaardering feit 1***

4.2.1 *Standpunt officier van justitie*
Aangevoerd is dat de verdachte drie typen malware heeft vervaardigd, te weten Rubella, Dryad en Cetan. Deze typen malware zijn hoofdzakelijk geschikt voor het voorbereiden van het plaatsen van afluister- en/of hackapparatuur. Dit is strafbaar op grond van artikel 139d lid 2 sub a van het Wetboek van Strafrecht (hierna: WvSr) voor wat betreft het faciliteren van hacken ex artikel 138ab WvSr. Voor wat betreft het kunnen aftappen van toetsaanslagen is dit strafbaar op grond van artikel 350d sub a WvSr. De verdachte heeft deze malware vervolgens verkocht, verspreid, anderszins ter beschikking gesteld en voorhanden gehad. Gelet op het type malware dat de verdachte ontwikkelde en de professionele manier waarop hij zijn handel inrichtte, had hij daarmee ook het oogmerk in de zin van artikel 139d lid 3 WvSr. Het was de persoonlijke bedoeling van de verdachte dat zijn malware zou worden gebruikt voor onder andere hacken.

4.2.2 *Standpunt verdediging*
De verdediging heeft aangevoerd dat Rubella, Dryad en Cetan in feite één programma zijn. Rubella is door de verdachte vervaardigd en daarna door hem op kleine punten gewijzigd en doorontwikkeld, hetgeen heeft geleid tot de andere programma's. De verdachte heeft deze software weliswaar vervaardigd en daarna op de markt gebracht, echter heeft de verdachte hierbij nooit de bedoeling gehad dat er met deze software strafbare feiten zouden worden gepleegd. Dat de verdachte handelde met het oogmerk op computervredebreuk en/of computersabotage kan niet worden vastgesteld. Voorwaardelijk opzet is daarvoor onvoldoende. De verdachte dient daarom te worden vrijgesproken van het onder 1 ten laste gelegde.

4.2.3 *Beoordeling*
Onder feit 1 is de verdachte ten laste gelegd dat hij drie programma's heeft vervaardigd die hoofdzakelijk geschikt gemaakt en/of ontworpen zijn tot het kortgezegd plegen van '(eenvoudige) computervredebreuk' en (als cumulatief/alternatief) 'computersabotage', en dat hij deze programma's met het oogmerk op deze misdrijven heeft vervaardigd, verkocht, verspreid, anderszins ter beschikking gesteld of voorhanden gehad.
De rechtbank stelt het volgende voorop. Ter zitting heeft de verdachte verklaard dat hij zich in de periode van 15 februari 2018 tot en met 11 maart 2019 bezig hield met het vervaardigen en verkopen van Rubella, Dryad en Cetan. De verdachte heeft verklaard dat hij zich al jaren eerder uit interesse in de beveiliging van geautomatiseerde werken en de werking van malware is gaan verdiepen in dit onderwerp. Toen hij hier veel kennis over had opgedaan heeft hij bij wijze van intellectuele uitdaging Rubella vervaardigd. De verdachte heeft verklaard dat Rubella gezien moet worden als een 'lege huls', die ongedetecteerd door anti-virussoftware toegang kan verkrijgen tot andermans computer. Het is mogelijk dat met gebruik van deze 'lege huls' andere (kwaadwillende) malware op een computer geplaatst wordt. De verdachte heeft ook verklaard dat hij Rubella is gaan verkopen toen hij merkte dat er interesse was voor dergelijke programma's. Dryad en Cetan zijn iets later door hem (door)ontwikkeld en op de markt gebracht. Deze laatste twee programma's dienen hetzelfde doel als Rubella. De verdachte heeft verklaard dat zijn oogmerk,

1 Jan-Jaap Oerlemans is bijzonder hoogleraar Inlichtingen en Recht bij de Universiteit Utrecht en verbonden aan het Montaigne Centrum voor Rechtsstaat en Rechtspleging en het Willem Pompe Instituut voor Strafrechtwetenschappen.

zowel bij het vervaardigen als bij het verkopen van de software, niet gericht was op het faciliteren van computercriminaliteit en dat hij zijn programma's ook niet als zodanig aanbood.

Hoofdzakelijk geschikt

De rechtbank is van oordeel dat Rubella, Dryad en Cetan hoofdzakelijk geschikt gemaakt of ontworpen zijn om computercriminaliteit mogelijk te maken. De rechtbank komt tot deze conclusie op basis van de volgende omstandigheden.

In het proces-verbaal van bevindingen 'onderzoek aan Rubella Macro Builder' relateert de politie dat (een programma als) Rubella Macro Builder een onmisbare functie vervult in het proces van cybercriminaliteit met behulp van malware. Rubella zorgt namelijk voor de eerste stap van 'infectie'; het ongedetecteerd bezorgen van malware op een computersysteem. In het proces-verbaal van bevindingen 'onderzoek aan Cetan' en het proces-verbaal van bevindingen 'onderzoek aan Dryad' is door de politie gerelateerd dat het ook met deze programma's mogelijk is om ongedetecteerd een geautomatiseerd werk binnen te komen. Cetan en Dryad werken op dezelfde manier als Rubella: met behulp van deze programma's lukt het om een macro te genereren in een Worddocument. Zodra dit document wordt geopend, downloadt de macro een bestand van een externe server en voert deze uit. Cetan Macro Builder is een meer geavanceerde, dan wel verbeterde, macro builder ten opzichte van Rubella. Zo is het in Cetan mogelijk om een document door middel van een tekst en een foto een betrouwbaar uiterlijk te geven, zodat een slachtoffer eerder geneigd is om de macrofunctionaliteit in te schakelen. Met Dryad kan een Word-document worden geprepareerd met een macro die vervolgens een programma vanaf een externe locatie downloadt en uitvoert.

De rechtbank is van oordeel dat voor zover de software ook geschikt is voor legale activiteiten (bijvoorbeeld het testen van de eigen beveiliging) dit er niet aan af doet dat de software van de verdachte hoofdzakelijk geschikt gemaakt en ontworpen is om de delicten van eenvoudige computervredebreuk (artikel 138ab eerste lid WvSr), en vervolgens/tevens de delicten van 138b WvSr (belemmering van een geautomatiseerd werk) en/of 139c WvSr (het aftappen of opnemen van gegevens) mogelijk te maken. Uit berichtenverkeer van de telefoon van de verdachte kan worden afgeleid dat de verdachte zelf het verband tussen het maken en verkopen van deze software en de strafbaarstelling op grond van artikel 139d lid 2 WvSr onder a heeft gelegd.

Dat dit programma in hoofdzaak geschikt of ontworpen is om het wissen/onbruikbaar maken dan wel vernielen van een geautomatiseerd werk te plegen (artikel 350a en/of 350c WvSr) acht de rechtbank gelet op de dossierinformatie onvoldoende vaststaan. De verdachte wordt dan ook – partieel – vrijgesproken van overtreding van artikel 350d WvSr.

Oogmerk in artikel 139d lid 2 sub a WvSr

De rechtbank is van oordeel dat met 'oogmerk' in artikel 139d lid 2 WvSr wordt bedoeld 'met de (persoonlijke) bedoeling'. Artikel 139d lid 2 WvSr is aan de Nederlandse strafwetgeving toegevoegd en op 1 september 2006 in werking getreden, om aan de verplichtingen die voortvloeien uit het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (hierna: Cybercrimeverdrag) te voldoen. Artikel 6 van het Cybercrimeverdrag verplicht de verdragspartijen om in hun nationale wetgeving als strafbaar aan te merken:

a. *het opzettelijk en wederrechtelijk vervaardigen, verkopen, verkrijgen voor gebruik invoeren, verspreiden of anderszins beschikbaar stellen van:*
   i. *een technisch hulpmiddel, waaronder begrepen een computerprogramma, dat hoofdzakelijk is ontworpen of geschikt gemaakt voor het plegen van een van de strafbare feiten, bedoeld in de artikel 2 tot en met 5 (van hetzelfde verdrag).*

In artikel 6 lid 2 van het Cybercrimeverdrag is bepaald dat dit artikel niet als zodanig mag worden uitgelegd dat sprake is van strafrechtelijke aansprakelijkheid wanneer de in het eerste lid van dit artikel bedoelde vervaardiging, verkoop, verkrijging voor gebruik, invoer, verspreiding of andere vorm van beschikbaarstelling of het bedoelde bezit niet bedoeld is voor het plegen van een overeenkomstig de artikelen 2 tot en met 5 van dit Verdrag strafbaar gesteld feit, zoals ten behoeve van het geautoriseerd testen of het beschermen van een computersysteem.

In de Nederlandse wetgeving is blijkens de tweede nota van wijziging (*Kamerstukken II* 2005/06, 26671, 7) uiting gegeven aan het voorgaande door het begrip 'oogmerk' op te nemen in artikel 139d lid 2 (en 3) WvSr. Indien iemand een technisch hulpmiddel voorhanden heeft dat hoofdzakelijk ontworpen is tot het plegen van computervredebreuk, maar hij dit middel alleen gebruikt om de beveiliging van z'n eigen computer te testen, heeft hij niet het oogmerk om het misdrijf computervredebreuk te plegen. Hij valt dan niet in de termen van de strafbepaling.

De persoonlijke bedoeling van de verdachte

De rechtbank is van oordeel dat de verdachte bij zowel het vervaardigen van de software, als het verkopen en voorhanden hebben de bedoeling had dat hiermee tenminste computervredebreuk en daarmee samenhangende computercriminaliteit wordt gepleegd. De rechtbank leidt dit af uit de volgende omstandigheden.

De technische mogelijkheden van de door de verdachte vervaardigde malware zijn volledig gericht op het omzeilen van anti-virussoftware. De verdachte heeft de producten zelf gemaakt en had dan ook als geen ander de wetenschap van alle functionaliteiten en mogelijkheden, waaronder met name ook de illegale mogelijkheden, die zijn software de gebruikers ervan daardoor biedt. De verdachte heeft ter terechtzitting verklaard dat hij zich 'niet zo bezighield met waar zijn klanten zijn software voor gebruikten', maar de rechtbank acht dat niet aannemelijk.

Dat de verdachte zijn producten aan de man bracht op hackersfora acht de rechtbank daarbij een relevant gegeven, evenals de wijze waarop hij zijn producten aanprees. Zo is te lezen in een digitale advertentie van Rubella dat het mogelijk is om aan deze malware een powershell payload toe te voegen. Met 'payload' wordt malware bedoeld die een kwaadwillende wil uitvoeren bij zijn slachtoffer.[2] In de advertentietekst wordt verder benadrukt dat het mogelijk is om met deze malware anti-virusdetectie te omzeilen. Tevens wordt benadrukt in de advertentietekst dat de malware al vier weken FUD zou zijn. Wanneer een bestand FUD is, wordt bedoeld dat het niet door anti-virus software wordt herkend als zijnde een virus.[3]
De rechtbank leidt het oogmerk in het bijzonder ook af uit de volgende door de verdachte gevoerde gesprekken. Op 30 augustus 2018 is vanuit het toestel van de verdachte een screenshot gestuurd naar een nummer dat is opgeslagen onder de naam [naam]. Het screenshot bevat een afbeelding van een e-mail afkomstig van Google waarin wordt aangegeven dat de FBI informatie met betrekking tot een Google-account heeft gevorderd. Dit screenshot werd direct gevolgd door berichten van de verdachte die er op neerkwamen dat de verdachte enorm geschrokken was van deze e-mail. Zo stuurde de verdachte: *"Ik stop nu per direct"*. De verdachte verdiepte zich vervolgens in de strafbaarheid van computervredebreuk en stuurde tevens: *"het maken, vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van dergelijke software is een strafbaar feit (art. 139d lid 2 onder a). Hierop staat een jaar cel (of een boete van 16.750 euro)."* Zijn gesprekspartner zegt daarop: *"Dan betaal je je boete en je zit goed"*. De verdachte zegt dan: *"Ik denk niet dat ik met dat geld die boete kan betalen"*. Zijn gesprekspartner zegt dan: *"En dan mag je nog 2 jaar zitten"* en *"Want illegaal geld"*. De verdachte stuurde vervolgens*: "Dat is kk lang"* en *"Een jaar in de cel"*.
Een dag later is de verdachte er kennelijk achter gekomen dat de aanleiding voor de FBI om zijn accountgegevens op te vragen betrekking heeft op iets uit het verleden en niet ziet op waar hij op dat moment mee bezig is. De verdachte voert dan een gesprek met de gebruiker van het telefoonnummer [telefoonnummer] en zegt deze persoon die e-mail van Google te negeren: *"Ja negeer die mail"* en *"Is oude case"*, en iets verderop in het gesprek: *"Er staat 2017 in de case nummer"*. Daarna werd er vanuit de telefoon van de verdachte het volgende bericht verstuurd: *"Maar ik zit nog diep er in"*. Op de vraag verstuurd vanaf de telefoon met het nummer [telefoonnummer]: *"Hoe bedoel je"* werd volgend antwoord gestuurd: *"Dat ik nog malware doe"* en *"Ik code het nu"*. Enige tijd later in het gesprek wordt vanuit het toestel van de verdachte verstuurd: *"Ik dacht zeg, maar dat dat mailtje over mijn shit van nu ging"* en *"Ik dacht ze hebben me gevonden"*.
De rechtbank leidt uit voorgaande gesprekken af dat de verdachte wel degelijk wist dat het product dat hij verkocht door anderen gebruikt werd voor kwalijke en niet legale activiteiten. Het stadium van 'klieren' op internet, zoals de verdachte zelf verklaard heeft begonnen te zijn, was de verdachte toen al lang voorbij en dat wist hij ook. Desondanks ging de verdachte direct nadat hij van de schrik was bekomen door met het vervaardigen en verkopen van zijn malware op hackersfora.
De verdachte wist als geen ander dat zijn producten in feite alleen betekenis hadden voor illegale toepassingen – allemaal te begrijpen onder de noemer van computercriminaliteit als hiervoor bedoeld – en dat de kopers van zijn produkten geen ander doel (kunnen) hebben gehad dan gebruikmaking daarvan voor dergelijke illegale toepassingen. In die volle wetenschap heeft de verdachte, tegen betaling van aanzienlijke bedragen, een groot aantal verkooptransacties uitgevoerd. Deze hebben gedurende lange tijd plaatsgevonden, zoals ten laste gelegd in de periode van 15 februari 2018 tot en met 11 maart 2019. Het handelen van de verdachte moet daarom worden aangemerkt als met de bedoeling dat hiermee computercriminaliteit zou worden gepleegd. Aan deze gevolgtrekking doet niet af dat het verdachte uiteindelijk te doen zal zijn geweest om zijn financieel voordeel. De conclusie is dat sprake is van het in artikel 139d lid 2 sub a WvSr vereiste oogmerk.

Oogmerk artikel 193d lid 3 WvSr

De rechtbank zal niet ingaan op het betoog van de officier van justitie om overtreding van artikel 139d lid 3 WvSr bewezen te verklaren, nu die strafbare gedraging niet ten laste is gelegd.

4.2.4 *Conclusie*

Het eerste onderdeel onder 1 ten laste gelegde is wettig en overtuigend bewezen. De rechtbank spreekt de verdachte partieel vrij voor het tweede onderdeel van het onder 1 ten laste gelegde.

4.3 ***Bewezenverklaring***

(…)

De verdachte heeft de bewezen verklaarde feiten op die wijze begaan dat:

Feit 1:

hij in de periode van 15 februari 2018 tot en met 11 maart 2019 te Utrecht,
meermalen, een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt en/of ontworpen is tot het plegen van een misdrijf als bedoeld in artikel 138ab eerste lid, 138b en/of 139c Wetboek van strafrecht,
heeft vervaardigd, verkocht of voorhanden heeft gehad,
met het oogmerk dat daarmee een van die misdrijven werd gepleegd,

2 Bron vermeld in het proces-verbaal van verdenking (LERDA18011-13) (vul geboortedatum in):
https://nl.wikipedia.org/wiki/Payload, bezocht op 21-11-2018.

3 Bron vermeld in het proces-verbaal van verdenking (LERDA18011-13) (vul geboortedatum in):
https://en.wikipedia.org/wiki/Fully_undetectable, bezocht op 21-11-2018.

immers heeft verdachte malware (Rubella Macro Builder, Dryad en Cetan) vervaardigd en op hackfora verkocht, welke malware hoofdzakelijk was ontworpen om voornoemde misdrijven te plegen door het mogelijk te maken om op met deze malware geïnfecteerde computers:
– .xls en/of.doc bestanden te genereren die macros bevatten
– bestanden te downloaden en/of uit te voeren
– opdrachten uit te voeren.
– toetsaanslagen te loggen

Feit 2:
hij in de periode van 20 mei 2017 tot en met 11 maart 2019 te Utrecht,
creditcardgegevens (42) voorhanden heeft gehad,
waarvan verdachte wist dat die bestemd waren tot het plegen van het in artikel 231b Wetboek van Strafrecht omschreven misdrijf.
Hetgeen meer of anders is ten laste gelegd is niet bewezen. De verdachte moet daarvan worden vrijgesproken.

5. Strafbaarheid feiten

De bewezen feiten leveren op:
Ten aanzien van feit 1:
met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b en/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, vervaardigen, verkopen en voorhanden hebben, meermalen gepleegd;
Ten aanzien van feit 2:
gegevens voorhanden hebben waarvan hij weet dat zij bestemd zijn tot het plegen van een in artikel 231b van het Wetboek van Strafrecht omschreven misdrijf.
Er zijn geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van de feiten uitsluiten. De feiten zijn dus strafbaar.

6. Strafbaarheid verdachte

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

7. Motivering straf

(…)

7.3 *Persoonlijke omstandigheden van de verdachte*

7.3.1 *Strafblad*
De rechtbank heeft acht geslagen op een uittreksel uit de justitiële documentatie van 14 maart 2019, waaruit blijkt dat de verdachte niet eerder is veroordeeld voor strafbare feiten.

7.3.2 *Rapportages*
Reclassering Nederland heeft een rapport over de verdachte opgemaakt, gedateerd 18 februari 2020. Dit rapport houdt het volgende in.
De reclassering schat de kans op recidive op korte termijn in als laag, echter is het onduidelijk hoe deze kans op langere termijn zal zijn als de interesse in
informatietechnologie toeneemt en de verdachte in contact komt met nieuwe vrienden met dezelfde interesse en (mogelijk andere) vaardigheden. Om de kans op recidive te verkleinen en de vaardigheden van de verdachte een positieve draai te geven, wil de reclassering hem, in het kader van een verplicht reclasseringscontact, aanmelden bij het programma Hack_Right, voor jonge hackers. In het toezicht kan verder worden gecontroleerd of betrokkene zich daadwerkelijk niet meer bezighoudt met criminele zaken.
De rechtbank heeft acht geslagen op dit rapport.

7.4 *Conclusies van de rechtbank*
Gelet op hetgeen de rechtbank hierboven heeft overwogen, komt zij tot de volgende conclusies.
Gezien de ernst van de feiten zou in beginsel niet anders kunnen worden gereageerd dan met het opleggen van een onvoorwaardelijke gevangenisstraf. De rechtbank zal echter afzien van het opleggen van een onvoorwaardelijke gevangenisstraf die langer is dan het voorarrest van 12 dagen in maart 2019, gezien de persoon van de verdachte. In plaats daarvan wordt de maximale taakstraf opgelegd van 240 uren en een voorwaardelijke gevangenisstraf van 180 dagen met een proeftijd van 3 jaren.
De verdachte was nog heel jong ten tijde van de bewezen verklaarde feiten (te weten 19 en net 20 jaar) en was voorafgaand aan deze zaak niet eerder veroordeeld voor strafbare feiten. De verdachte studeert Informatiekunde en heeft zijn leven verder op orde. De rechtbank heeft, mede op basis van de zitting, de indruk verkregen dat de verdachte inmiddels van de ernst van de feiten en alle mogelijke consequenties daarvan, ook in strafrechtelijke zin, doordrongen is. Dit geeft voor de rechtbank in dit specifieke geval de doorslag om als strafmodaliteit niet te kiezen voor een onvoorwaardelijke gevangenisstraf die langer is dan de voorlopige hechtenis destijds heeft geduurd.
Het voorwaardelijke strafdeel dient er tevens toe de verdachte ervan te weerhouden in de toekomst opnieuw strafbare feiten te plegen. Vanwege de voorwaardelijke gevangenisstraf gedurende een proeftijd van drie jaren en vanwege het leereffect dat van deze strafzaak zal uitgaan voor de verdachte, vindt de rechtbank het niet nodig of wenselijk daarbij ook nog bijzondere voorwaarden op te leggen, ook niet voor het volgen van het programma Hack_Right.
Alles afwegend acht de rechtbank de voorgenoemde straffen, tesamen met de hieronder besproken verbeurdverklaringen, passend en geboden.
Dit is een andere en minder zware bestraffing dan door de officier van justitie is geëist. Deels komt dit door voor-

noemde overwegingen over de persoon van de verdachte, deels doordat de rechtbank minder bewezen acht dan dan de officier van justitie.
(…)

9. **Toepasselijke wettelijke voorschriften**

(…)

Noot

1. De verdachte in deze zaak ontwikkelde het programma 'Rubella Marco Builder'. Het is zogenoemde 'macromalware', omdat het aan Office-documenten zoals Word en Excel een stuk verborgen code toevoegt die iets uitvoert. De verdachte had het programma zo geprogrammeerd dat het heimelijk verbinding legde met een externe server waardoor cybercriminelen hun eigen malware konden plaatsen op de computers van de slachtoffers. De zaak is interessant, omdat het een van de weinige veroordelingen is voor de vervaardiging van malware door een Nederlander en het misbruik maken van de macrofunctionaliteit in Office-documenten een veelgebruikte aanvalstechniek is van cybercriminelen.
2. De zaak begon niet met een opsporingsonderzoek door de politie, maar met een onderzoek van cybersecuritybedrijf McAfee.[4] De onderzoekers bij McAfee viel een advertentie op het oog van het programma op een hackersforum. Het screenshot van een geprepareerd Worddocument had Nederlandse taalinstellingen. Dat is ongebruikelijk in de hackerswereld, waar de voertaal volgens McAfee doorgaans Engels is. Ook was een chataccount (van Jabber) van ene 'Rubella' te vinden. De onderzoekers namen contact op via Jabber met de aanbieder en toonden interesse in de software. Nader onderzoek van de malware – 'Dryad' genaamd – toonde verschillende functionaliteiten aan, zoals (1) de mogelijkheid een uitvoeringsbestand te downloaden van een aangegeven URL, (2) de mogelijkheid (o.a.) een .exe-bestand op een computer te starten, (3) de bestandsnaam van de download te wijzigen, (4) verschillende functionaliteiten om antivirusprogramma's te omzeilen, en (5) de functionaliteit een Word- of Excel-document te genereren.
3. De verdachte wordt het vervaardigen van malware, te weten 'Rubella', 'Dryad' en 'Cetan' ten laste gelegd. Deze typen malware zijn hoofdzakelijk geschikt voor het voorbereiden van het plaatsen van afluister- en/of hackapparatuur (strafbaar gesteld in art. 139d lid 2 sub a jo. art. 138ab Sr). De verdachte heeft deze malware vervolgens verkocht, verspreid, anderszins ter beschikking gesteld en voorhanden gehad. Het fungeert als 'tool' voor cybercriminelen.[5] In 2017 berichtte Europol dat misbruik van de macrofunctionaliteit in Office-documenten een veelgebruikte aanvalstechniek is van cybercriminelen.[6]
4. De verdediging voert aan dat de verdachte geen oogmerk had dat met de software computervredebreuk wordt gepleegd. Het benodigde oogmerk voor de strafbaarstelling zou dus ontbreken, waardoor de verdachte moet worden vrijgesproken. De rechtbank gaat daar niet in mee. Er is veel bewijs voorhanden dat tot bewezenverklaring van het benodigde oogmerk leidt. De verdachte zegt in zijn verklaring bijvoorbeeld dat de software is ontwikkeld om antivirusprogramma's te omzeilen en toegang te krijgen tot andermans computer. Ook verklaart hij ter zetting dat hij op een bepaald moment de Rubella software is gaan verkopen.[7] Dat is mijns inziens in feite een bekentenis.
5. De rechtbank overweegt dat verdachte de producten op hackersfora verkocht en daarop zijn producten aanprees. Zo is te lezen in een digitale advertentie van Rubella dat het mogelijk is om aan deze malware een 'powershell payload' toe te voegen. Met 'payload' wordt malware bedoeld die een kwaadwillende kan uitvoeren bij zijn slachtoffer. In de advertentietekst wordt verder benadrukt dat het mogelijk is om met deze malware antivirusdetectie te omzeilen. Tevens wordt benadrukt in de advertentietekst dat de malware al vier weken FUD zou zijn. Wanneer een bestand FUD is, wordt bedoeld dat het niet door antivirussoftware wordt herkend als zijnde een virus, aldus de rechtbank in zijn uitleg van deze zaak met een hoog technisch karakter.[8]
6. De rechtbank leidt het oogmerk onder andere af uit het geanalyseerde berichtenverkeer op de telefoon van de verdachte. Hieruit blijkt dat de verdachte zelf het verband al heeft gelegd tussen het maken en verkopen van deze software en de strafbaarstelling op grond van art. 139d lid 2 sub a Sr.[9] De verdachte wordt ook veroordeeld voor het voorhanden hebben van creditcardgegevens van 42 personen, terwijl hij wist dat het mogelijk was om met deze gegevens creditcardfraude te plegen. De rechtbank acht het ontoegankelijk maken van gegevens met de programma's *niet* bewezen, omdat uit de beschikbare dossierinformatie onvoldoende is gebleken dat de door de verdachte vervaardigde en verkochte malware hoofdzakelijk geschikt of ontworpen was om gegevens te wissen of onbruikbaar te maken, dan wel vernieling van een geautomatiseerd werk te plegen (zoals bij ransomware).[10]

4 Zie voor onderstaande beschrijving: J. Fokker & T. Roccia, 'McAfee ATR Aids Police in Arrest of the Rubella and Dryad Office Macro Builder Suspect', *McAfee Blog*, 16 juli 2019.
5 Zie r.o. 4.2.1.
6 Europol, *Internet organised threat assessment report 2017*, p. 57: *"A common approach is to attach a malicious attachment to an email, often a Microsoft Office document containing malicious macro code – a tactic that Dridex is notorious for resurrecting. Alternatively the message may include a link to a malicious URL which will then attempt to infect the target computer when they visit the site."*.
7 R.o. 4.2.3.
8 Zie r.o. 4.2.3.
9 R.o. 4.2.3.
10 Zie ook Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, m.nt. J.J. Oerlemans over de strafbaarstelling van het vervaardigen en voorhanden hebben van ransomware.

7. De verdachte wordt veroordeeld tot twaalf dagen gevangenisstraf (de tijd dat hij in voorarrest heeft gezeten) en een taakstraf van 240 uur, met daarbij een voorwaardelijke gevangenisstraf van 180 dagen met een proeftijd van drie jaren. Opvallend is dat de reclassering adviseerde de verdachte aan te melden bij het programma 'Hack_Right' om een positieve draai te geven aan de vaardigheden van de verdachte. Binnen het programma lopen jonge hackers bijvoorbeeld stage bij een cybersecuritybedrijf. De rechtbank vindt het niet nodig dat de verdachte het programma Hack_Right volgt, vanwege 'de voorwaardelijke gevangenisstraf gedurende een proeftijd van drie jaren en vanwege het leereffect dat van deze strafzaak zal uitgaan voor de verdachte'.[11] De strafoplegging valt lager uit dan de officier van justitie heeft geëist. Dat is volgens de rechtbank te verklaren vanwege de overwegingen van de persoon van de verdachte en deels omdat minder wordt bewezen dan de officier van justitie ten laste had gelegd.

8. Juridisch gezien is er weinig op te merken aan de uitspraak. De rechtbank voert de juiste overwegingen in deze technische zaak en het oordeel van de rechtbank is begrijpelijk. De straf kan als laag worden gezien, omdat de software het mogelijk maakt voor cybercriminelen om op grote schaal computervredebreuk te plegen. De veroorzaakte schade door de software is mogelijk aanzienlijk. Echter, op het delict staat slechts maximaal twee jaar gevangenisstraf en de rechtbank legt een flinke voorwaardelijke gevangenisstraf met proeftijd op. Met deze straf kan de verdachte verder gaan met zijn studie en verder werken aan zijn toekomst. Het was wel interessant geweest meer te lezen over de bewijsgaring van de politie onder leiding van het Openbaar Ministerie. Vermoedelijk is een netwerkzoeking ex art. 125j Sv toegepast toen de politie in de collegezaal de verdachte arresteerde en de laptop van de verdachte doorzocht. In de media is te lezen dat de laptop nog aan stond en de politie het bewijs direct heeft verzameld.[12] Het zou goed zijn daar meer over te lezen, omdat er nauwelijks jurisprudentie is over de bevoegdheid van de netwerkzoeking. De advocaat heeft hier echter geen verweer op gevoerd, waardoor de rechtbank er ook geen overwegingen aan hoeft te wijden. Met name de technische details van de zaak en het geringe aantal veroordelingen voor het vervaardigen van software die als 'tool' door cybercriminelen wordt gebruikt, maakt de zaak lezenswaardig.

Prof. mr. dr. J.J. Oerlemans

11 Ook worden 6,76 Bitcoin verbeurdverklaard, omdat deze vermoedelijk met de strafbare feiten zijn verkregen.

12 Zie o.a. R. Wassens, 'Celstraf voor 21-jarige malware-ontwikkelaar', *NRC.nl*, 19 maart 2020 en Redactie, 'Utrechtse student krijgt 192 dagen cel voor verkoop malware', *Security.nl*, 20 maart 2020.