# Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153

Oerlemans, J.

**Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, m.nt. J.J. Oerlemans**

**Noot**

1. De 'Coinvault-zaak' verdient nadere aandacht. Het betreft de eerste veroordeling voor 'ransomware'[1] in Nederland. Dat is de hoogste tijd, omdat ransomware al jaren[2] één van de meest prevalente vormen is van cybercrime in enge zin.[3] In deze noot ga ik eerst kort in op de feiten van de zaak. Daarna bespreek ik uitgebreider de ten laste gelegde feiten en welke andere delicten van toepassing kunnen zijn. Tot slot werp ik een korte toekomstblik op ransomware.

2. De Rechtbank Rotterdam heeft op 26 juli 2018 twee jongvolwassenen veroordeeld (ECLI:NL:RBROT:2018:6153) tot 240 uur werkstraf en een voorwaardelijke gevangenisstraf van twee jaar voor het besmetten van een groot aantal computers met zelfgemaakte ransomware. De verdachten hebben van november 2014 tot en met september 2015 computers besmet met zelfgemaakte ransomware van de variant 'Coinvault' en 'Bitcryptor'. Deze ransomware is meer specifiek te kwalificeren als '*cryptoware*', waarbij gegevens worden versleuteld.[4] Zonder betaling in virtueel geld (in dit geval Bitcoin) en de ontvangst van de sleutel om gegevens weer toegankelijk te maken, is het zonder back-up in de meeste gevallen onmogelijk de gegevens terug te krijgen.[5]

3. In de uitspraak van de Rechtbank Rotterdam staat weinig informatie over het opsporingsproces, maar uit de mediaberichten over de zaak blijkt dat de verdachten de malware als 'trojan' hebben verspreid. In dit geval was de kwaadaardige software vermomd als commerciële software en 'sleutel-generatoren' die in nieuwsgroepen gratis konden worden download. Nadat duizenden computers waren besmet activeerden de verdachten de cryptoware en eisten ze 250 euro in Bitcoin van hun slachtoffers. De computers stonden als zombiecomputers onder controle van hun command-and-control server. Bij het verbinding maken met de server maakten de verdachten echter geen gebruik van anonimiseringstechnieken (zoals Tor), waardoor het IP-adres terugverwees naar het adres van de abonneehouder (het ouderlijk huis van de verdachten ). Dat leidde tot de arrestatie van de verdachten in een klein dorp nabij Amersfoort.[6]

1. De officier van justitie heeft artikel 138ab Sr, 350a Sr en 317 Sr (afpersing ten laste gelegd). Het ligt het meest voor de hand het delict gegevensaantasting (art. 350a Sr) ten laste te leggen. Het artikel is ervoor gegoten, omdat het (onder andere) strafbaar stelt 'het opzettelijk en wederrechtelijk veranderen, onbruikbaar maken of ontoegankelijk maken van gegevens' met een maximale gevangenisstraf van twee jaren of een geldboete van de vierde categorie. De verdachten hebben gebruik gemaakt van een botnet, waardoor ook sprake is van een gekwalificeerde vorm van computervredebreuk in artikel 138ab lid 3 Sr.[7] Sinds mei

---

[1] Ransomware is software waarmee slachtoffers gedwongen worden losgeld te betalen om weer toegang tot gegevens te krijgen.
[2] Zie bijvoorbeeld Europol, The Internet Organised Crime Threat Assessment, iOCTA, Europol: Den Haag 2016 en 2017.
[3] Dat wil zeggen: de categorie van delicten die gericht zijn tegen de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens op computers en netwerken, zoals computervredebreuk ('hacken'), kwaadaardige software ('malware') en verstikkingsaanvallen ((d)dos-aanvallen).
[4] Zie uitgebreid J.J. Oerlemans e.a., 'Cybercrime en witwassen: bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware', WODC, onderzoek & beleid reeks, nr. 319, Meppel: Boom Criminologie 2016, p. 28-34.
[5] Hoewel de sleutels van CoinVault en van 84 andere typen ransomware beschikbaar worden gesteld op '*nomoreransom.org*'; een internationaal samenwerkingsverband van de politie en IT beveiligingsbedrijven, waarbij zoveel mogelijk sleutels aan slachtoffers beschikbaar worden gesteld.
[6] Zie Tom Kreling, 'Het begon als kick, maar liep volstrekt uit de hand: broers voor de rechter voor afpersen met gijzelingssoftware', *De Volkskrant*, 12 juli 2018. Beschikbaar op: https://www.volkskrant.nl/nieuws-achtergrond/het-begon-als-kick-maar-liep-volstrekt-uit-de-hand-broers-voor-de-rechter-voor-afpersen-met-gijzelingssoftware~b5774034/ (laatst geraadpleegd op 5 augustus 2018). Zie ook Christiaan Beek & John Fokker, 'What Drives a Ransomware Criminal? CoinVault Developers Convicted in Dutch Court', *McAfee*, 13 juli 2018. Beschikbaar op: https://securingtomorrow.mcafee.com/mcafee-labs/what-drives-a-ransomware-criminal-coinvault-developers-convicted-in-dutch-court/ (laatst geraadpleegd op 5 augustus 2018).
[7] Zie ook het 'Toxbot-arrest' HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 een analyse van het arrest in J.J. Oerlemans & B.J. Koops, 'De

2015 is overigens ook artikel 138b Sr gewijzigd[8], waardoor een strafverzwaring naar een maximale gevangenisstraf van vijf jaar of een geldboete van de vierde categorie van toepassing indien met het plegen van het feit als omschreven in art. 350a Sr 'ernstige schade' wordt veroorzaakt. De memorie van toelichting definieert niet helder wat 'ernstige schade' behelst, maar ik neem aan dat hier ook de besmetting van duizenden computers met ransomware onder valt, zoals in casu het geval was.

2. Bijzondere aandacht verdient ook de tenlastelegging van afpersing (art. 317 Sr) in deze zaak. Het gaat hier om de uitoefening van dwang, om zichzelf wederrechtelijk te bevoordelen met geweld of de bedreiging met geweld, door 'de bedreiging dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist' (zoals staat omschreven in art. 317 lid 2 Sr). Daarvan is in deze zaak sprake, omdat de cryptoware de gegevens ontoegankelijk maakt, tenzij het losgeld wordt betaald in de vorm van Bitcoin (of het systeem op een andere manier met een sleutel kan worden ontsleuteld). De Rechtbank Rotterdam volstaat in haar bespreking van het artikel met: "*de rechtbank is daarbij van oordeel dat het op deze wijze ontoegankelijk maken van bestanden gelijk is te stellen aan het begrip geweld als bedoeld in artikel 317 van het Wetboek van Strafrecht"*.

3. De richtlijn Cybercrime strafvordering[9] noemt de toepasbaarheid van het delict afpersing merkwaardig genoeg in zijn geheel niet. In plaats daarvan worden de artikelen 139d Sr (de plaatsing van malware), art. 326 Sr (oplichting) en art. 284 Sr (dwang) genoemd. De officier van justitie had inderdaad art. 139d lid 2 sub a Sr met verwijzing naar art. 138ab lid 3 Sr ten laste kunnen leggen. Dat zou beter tot uitdrukking doen komen dat de verdachten ook de vervaardiging van de Coinvault-malware wordt verweten. Op het eerste gezicht lijkt bij ransomware de ten laste legging van het delict 'oplichting' (art. 326 Sr) minder voor de hand te liggen. Voor oplichting is immers (onder andere) vereist dat iemand bijvoorbeeld na een 'listige kunstgreep' geld overmaakt. Met andere woorden wordt de betrokkene 'er in geluisd'. Bij ransomware wordt simpelweg de computer van het slachtoffer gegijzeld en losgeld door een anonieme dader wordt geëist; daarbij lijkt van een 'listige kunstgreep' geen sprake. Voor de besmetting van de computer wordt soms wel een 'listige kunstgreep' gebruikt. In deze zaak hebben de verdachten bijvoorbeeld de computers besmet via onschuldig lijkende programma's die via internet ter beschikking zijn gesteld, waarna de slachtoffers na besmetting van cryptoware bewogen worden geld over te maken. Eerder is oplichting wel ten laste gelegd en bewezen verklaard in het geval van '*banking malware*'.[10] Ten slotte kan in de context van ransomware ook nog sprake zijn van het delict dwang (art. 284 Sr), omdat een persoon 'door enige feitelijkheid' (het versleutelen van een computer) een ander wederrechtelijk dwingt iets te doen (losgeld betalen) of te dulden (het versleuteld laten van de computer). Het voordeel van de hoge maximale gevangenisstraf bij art. 317 Sr is dat slachtoffers spreekrecht hebben en ook zware bijzondere opsporingsbevoegdheden mogen worden toegepast, zoals direct afluisteren (art. 126l Sv) en alle vormen van de hackbevoegdheid (art. 126nba Sv).

---

Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *NJB* 2011, vol. 86, nr. 18, p. 1181-1185.

[8] Naar aanleiding van de implementatie van Richtlijn 2013/40/EU over aanvallen op informatiesystemen, Wet van 22 april 2015, *Stb*. 2015, 165.

[9] *Stcrt.* 2018, nr. 3271.

[10] Zie Rb. Rotterdam 2 oktober 2015, ECLI:NL:RBROT:2015:7044 en Rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814, m.nt. J.J. Oerlemans, *Computerrecht* 2016/175 met bevestiging in hoger beroep: Hof Den Haag 5 september 2017, ECLI:NL:GHDHA:2017:2519.

4. Met de opkomst van het Internet of Things raken steeds meer apparaten die autonome beslissingen kunnen nemen met het internet verbonden.[11] Dat brengt bijvoorbeeld met zich mee dat mensen opgesloten kunnen raken in hun hotelkamer, omdat de kamerdeur met het elektronische slot niet meer functioneert na een ransomwarebesmetting.[12] Het ontoegankelijk maken van een slimme auto met ransomware tegen losgeld voor een flink bedrag lijkt mij ook goed denkbaar. In deze gevallen ziet het vereiste 'geweld' bij afpersing mogelijk meer op het goed zelf in plaats van de opgeslagen gegevens op de computer. Toch lijkt het dat het geweld of de bedreiging van geweld zich daarbij meer richt op het *gebruik* van het goed, dan op het goed zelf; het omhulsul van het goed blijft ten slotte intact. Het is overigens ook denkbaar dat met ransomware het geweld of de bedreiging van geweld zich richt tegen een persoon. Als medische apparaten aan het lichaam (zoals een insulinepomp) of in het lichaam (zoals een pacemaker) verbonden zijn met een netwerk en op afstand ontoegankelijk wordt gemaakt, kan namelijk sprake van (de dreiging van) geweld jegens een persoon bij het gebruik van ransomware.

5. Los van deze theoretische bespiegeling over de strafbaarstelling van ransomware is van belang te realiseren dat de besmetting van ransomware op IoT-apparaten geen '*science fiction*' is. Ransomware is een groeiend probleem. De 'WannyCry'-aanval heeft in mei 2017 ziekenhuizen in het Verenigd Koninkrijk, het spoorwegsysteem tussen Duitsland en de Russische Federatie, telecommunicatiebedrijven in Spanje en Portugal en Petrochemische bedrijven in China en Brazilië en autofabrikanten in Japan platgelegd.[13] De Nederlandse samenleving zal zich moeten voorbereiden op deze vormen van cybercrime en maatregelen moeten treffen (niet alleen op het gebied van strafrecht). Daarnaast is nu al een tendens zichtbaar dat cybercriminelen de aanvallen gerichter worden uitgevoerd, zoals het besmetten van medische apparaten[14] in ziekenhuizen, waarbij een veel groter bedrag wordt geëist: in de tienduizenden euro's in plaats van die doorgaans 500 euro voor besmette PC's.[15] De strafrechtpraktijk lijkt hier nog onvoldoende op voorbereid.

[11] Zie Van Berkel e.a., '(Verkeerd) verbonden in een slimme samenleving. Het Internet of Things: kansen, bedreigingen en maatregelen.', WODC, Cahiers 2017-08, Den Haag: WODC 2017.
[12] Zie redactie, 'Sleutelpasjes eeuwenoud Oostenrijks hotel gehackt', *Algemeen Dagblad*, 30 januari 2017. Beschikbaar op: https://www.ad.nl/digitaal/sleutelpasjes-eeuwenoud-oostenrijks-hotel-gehackt~a54de529 (laatst geraadpleegd op 5 augustus 2018). Hier ligt het overigens voor de hand niet de deur zelf, maar de software op de een centrale computers die de hotelkamerdeuren bestuurt besmet is geraakt. De hoteleigenaar nam hierna overigens geen enkel risico meer en stapte over op fysieke sleutels.
[13] Europol 2017, p. 26.
[14] Zie ENISA, 'Threat Landscape Report 2017', p. 56.
[15] Zie ook Europol 2017, p. 19.