Rb. Den Haag 7 maart 2019, ECLI:NL:RBDHA:2019:2116

Oerlemans, J.J.

Rb. Den Haag 7 maart 2019, ECLI:NL:RBDHA:2019:2116, *Computerrecht* 2019/93, m.nt. J.J. Oerlemans[1]

Noot

1. In deze uitspraak is een verdachte veroordeelt die gebruik maakte van het beruchte 'Mirai-botnet'. Het Mirai-botnet is het eerste succesvolle botnet die bestond – op zijn hoogtepunt - uit honderdduizenden geïnfecteerde 'internet of things'-apparaten. Drie Amerikanen die het botnet hebben ontwikkeld en daarmee distributed denial-of-service (ddos) aanvallen uitvoerden zijn in 2018 veroordeeld.[2] In deze noot wordt eerst het interessante feitencomplex besproken. Daarna wordt ingegaan op de overweging omtrent de vraag of sprake kan zijn van 'geweld' bij ddos-aanvallen. Ten slotte wordt kort ingegaan op de alternatieve straf van het 'Hack_Right'-traject die de verdachte moet doorlopen.

2. De 20-jarige verdachte beschikte over een Mirai-botnet van ongeveer 10.000 geïnfecteerde apparaten.[3] Zoals in de uitspraak is uitgelegd kon de verdachte via het '*command-and-control center*' van het botnet onder meer een krachtige ddos-aanval uitvoeren. De verdachte heeft naar verluidt een ddos-aanval uitgevoerd op twee goksites en een bitcoinwisselkantoor, ook al is dit detail in de uitspraak - ten onrechte meen ik - geanonimiseerd.[4] Dit soort bedrijven verliezen inkomsten als ze door de grote hoeveelheid verkeer van de dos-aanval hun diensten niet meer kunnen verlenen. De bedrijven kunnen op deze manier worden afgeperst; slechts tegen betaling stopt de aanval. De verdachte eiste het losgeld in Bitcoin. De verdachte maakte ook reclame voor zijn 'ddos-dienst' en verdiende geld door het botnet ter beschikking te stellen aan anderen. Ten slotte heeft de verdachte in het 'Magister'-leerlingensysteem van zijn middelbare school ingebroken en daarmee computervredebreuk gepleegd. Het bewijs tegen de verdachte was onder meer afkomstig uit verstuurde Skypeberichten en forumberichten van de verdachte.

3. De rechtbank is in haar uitspraak een paar keer kort door de bocht en slaat mijns inziens de plank mis in een overweging met betrekking tot het bestanddeel 'geweld' in de delictsomschrijving van het delict afpersing in de zin van artikel 317 Sr. De rechtbank is kort door de bocht als zij stelt dat *"een DDoS-aanval kan worden gekwalificeerd als overtreding van artikel 138ab Sr en artikel 138b Sr*". Van artikel 138b Sr is zonder meer sprake, in dit geval ook in gekwalificeerde vorm in artikel 138b lid 2 Sr, omdat de verdachte gebruik maakte van een botnet. Een ddos-aanval leidt echter niet direct tot overtreding van het delict computervredebreuk in artikel 138ab Sr, omdat het een geautomatiseerd werk ontoegankelijk maakt maar geen sprake is van het binnendringen in een geautomatiseerd werk. Echter, een botnet is een netwerk van geïnfecteerde computers – in dit geval IoT-apparaten – die door een derde worden aangestuurd. Voor het creëren van een botnet moet wel computervredebreuk worden gepleegd, en wel in gekwalificeerde vorm in artikel 138ab lid 3 sub b

---

[1] Jan-Jaap Oerlemans is als onderzoeker verbonden aan eLaw, het centrum voor Recht en Technologie van de Universiteit Leiden.

[2] Security.nl, 'Ontwikkelaars Mirai-botnet ontsnappen aan gevangenisstraf', 19 september 2018. Beschikbaar op: https://www.security.nl/posting/577701/Ontwikkelaars+Mirai-botnet+ontsnappen+aan+gevangenisstraf.

[3] In de uitspraak worden helaas geen details gegeven over hoe de verdachte beschikking had over het Mirai-botnet. Mogelijk betrof het een kopie van het botnet, waarvan de broncode door de ontwikkelaars in 2016 online werd gezet.

[4] Zie Security.nl, 'Hagenaar veroordeeld voor ddos-aanvallen met Mirai-botnet', 7 maart 2019. Beschikbaar op: https://www.security.nl/posting/600511/Hagenaar+veroordeeld+voor+ddos-aanvallen+met+Mirai-botnet.

Sr.[5] Daarnaast is het mij niet helemaal duidelijk waarom sprake is van artikel 161sexies Sr, omdat in dat geval is vereist dat de ddos-aanval een 'gemeen gevaar voor goederen of voor de verlening van diensten te duchten is'. De websites zijn geen 'diensten van algemene nutte', zoals overheidswebsites. Volgens de rechtbank is er een 'gemeen gevaar voor goederen of de verlening van diensten', omdat de aanval er toe leidde dat vijf andere websites onbereikbaar waren. Het is denkbaar dat deze vijf websites op dezelfde webserver stonden als één van de websites die is aangevallen.

4. De rechtbank overweegt verder dat sprake is van het delict afpersing als bedoeld in artikel 317 van het Wetboek van Strafrecht (Sr). Daarbij stelt de rechtbank dat *zonder meer* sprake is van 'geweld', omdat 'websites en servers onbruikbaar worden gemaakt' en 'maatregelen genomen moeten worden om de aanval af te slaan en de website en server te herstellen'. Mijns inziens had de officier van justitie simpelweg art. 317 lid 2 Sr ten laste moeten leggen, waarbij geen sprake hoeft te zijn van geweld. Bij art. 317 lid 2 Sr bestaat de dwang bij afpersing uit 'de bedreiging dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist'. Het gelijk stellen van het begrip 'geweld' met het onbereikbaar maken van een webserver, zoals de rechtbank Den Haag in deze zaak, is juist niet vanzelfsprekend en onnodig. De officier van justitie had op de zitting de tenlastelegging nog kunnen wijzigen.

5. De verdachte is veroordeeld tot 377 jeugddetentie, waarvan 360 dagen voorwaardelijk en een taakstraf van 120 uur, waarvan 60 uur voorwaardelijk. Belangrijker is dat de verdachte de alternatieve straf van het 'Hack_Right'-initiatief krijgt opgelegd. Jaarlijks worden in Nederland rond de 70 jongeren (tussen 12 en 23 jaar) aangehouden voor cybercrime.[6] In 2018 hebben elf jongeren aan de pilot van Hack_Right meegedaan. Hack_Right is een traject dat kortgezegd jongeren laat inzien dat ze het verkeerde pad bewandelen en er ook legale alternatieven zijn die hun meer kan bieden. Alleen jongeren die bekennen, geen zeer ernstige vormen van cybercriminaliteit hebben gepleegd en bereid zijn zich op een positieve manier te ontwikkelen, komen ervoor in aanmerking. Bovendien moet het om een eerste cyberdelict gaan. Later in het traject reikt worden de jongeren daadwerkelijk alternatieven aangeboden om zich ten goede in te zetten, bijvoorbeeld als ethisch hacker bij een 'cyberwerkplaats' bij een bedrijf.[7]

---

[5] Zie ook HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 (*Toxbot*-arrest).

[6] Zie Ina Reitzema, 'Halt ziet toekomst in speciale werkstraf voor jonge hackers', *Dagblad van het Noorden*, 17 januari 2019. Beschikbaar op: https://www.dvhn.nl/groningen/Halt-ziet-toekomst-in-speciale-werkstraf-voor-jonge-hackers-24071533.html.

[7] Zie Politie.nl, 'Hack_Right: jonge hackers weer op het rechte pad', 18 december 2018. Beschikbaar op: https://www.politie.nl/nieuws/2018/december/18/hack-right-jonge-hackers-weer-op-het-rechte-pad.html.