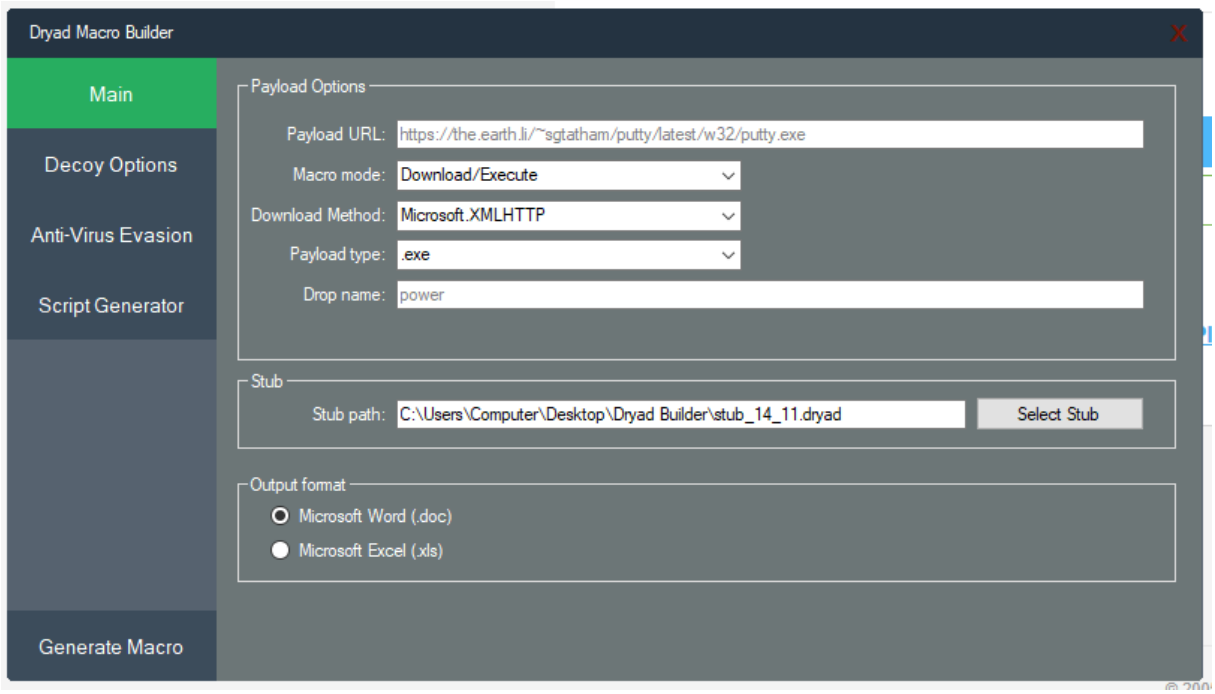
Annotatie bij Macro-malware zaak

Citeertitel: Rb. Rotterdam 19 maart 2020, ECLI:NL:RBROT:2020:2395, Computerrecht 2020/88, m.nt. J.J. Oerlemans

1. De verdachte in deze zaak ontwikkelde het programma 'Rubella Macro Builder'. Het is zogenoemde 'macro-malware', omdat het aan Officedocumenten 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 macro-functionaliteit in Office-documenten een veelgebruikte aanvalstechniek is van cybercriminelen.



Bron: McAfee.

2. De zaak begon niet met een opsporingsonderzoek door de politie, maar met een onderzoek van cybersecuritybedrijf McAfee. De onderzoekers bij McAfee viel een advertentie op het oog van het programma op een hackersforum. Het screenshot van een geprepareerd Word-document had Nederlandse taalinstellingen. Dat is ongebruikelijk in de hackerswereld, waar de voertaal volgens McAfee doorgaans Engels is. Ook was een chataccount (van Jabber) van een ene 'Rubella' te vinden. De onderzoekers namen contact op via Jabber met de aanbieder en toonde 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 bestandnaam van de download te wijzigen, (4) verschillende functionaliteiten om antivirusprogramma's te omzeilen, en (5) de functionaliteit een Word- of Exceldocument te generen.

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 Sr jo 138ab Sr). De verdachte heeft deze malware vervolgens verkocht, verspreid, anderszins ter beschikking gesteld en voorhanden gehad. Het fungeert als 'tool' voor cybercriminelen (zie r.o. 4.2.1). In 2017 berichtte Europol dat misbruik van de macro-functionaliteit in Office-documenten een veel gebruikte aanvalstechniek is van cybercriminelen.[1]
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 zitting dat hij op een bepaald moment de Rubella software is gaan verkopen (r.o. 4.2.3). 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 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 antivirussoftware wordt herkend als zijnde een virus, aldus de rechtbank in zijn uitleg van deze zaak met een hoog technisch karakter (r.o. 4.2.3).
6. De rechtbank leidt het oogmerk onder andere af uit het geanalyseerde berichtenverkeer op 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 artikel 139d lid 2 sub a Sr (r.o. 4.2.3). 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, zie ook Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153, *Computerrecht* 2018/210, m.nt. J.J. Oerlemans en mijn blogbericht over de strafbaarstelling van het vervaardigen en voorhanden hebben van ransomware).
7. De verdachte wordt veroordeeld tot 12 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 3 jaren. Opvallend is dat 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

[1] Zie bijvoorbeeld 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."

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’. De destijds 6,76 Bitcoin (met een waarde van 22.711,97 euro) wordt verbeurd verklaard, omdat deze vermoedelijk met de strafbare feiten zijn verkregen. De strafoplegging valt tegelijkertijd 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 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 aanstond en de politie bewijs direct heeft verzameld. Het zou goed zijn daar mee 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.