LJN: AZ7266, Rechtbank Breda , 981204/05

Datum uitspraak: 30-01-2007
Datum publicatie: 30-01-2007
Rechtsgebied: Straf
Soort procedure: Eerste aanleg - meervoudig
Inhoudsindicatie: Verdachte heeft in talloze computers van derden ingebroken; ten tijde van de ontdekking van deze strafbare feiten, ging het om 50.000 tot 80.000 computers. Uiteindelijk blijkt bij de ontmanteling dat er miljoenen computers zijn besmet. Bij deze inbraken kreeg verdachte met behulp van door hem en of zijn mededader ontwikkeld virus of trojan, de beschikking over persoonlijke gegevens waarmee geld of andere zaken konden worden verworven en in een aantal gevallen ook daadwerkelijk werden verworven. Hoewel verdachte deze strafbare feiten binnenshuis, zittend achter zijn computer, kon plegen, en dus niet feitelijk in woningen of bedrijven behoefde in te breken, is de gemaakte inbreuk op rechten van derden niet minder groot. Het middels het internet verlopende betalingsverkeer, wordt op deze wijze volledig ondermijnd. Het is aan het tijdig ingrijpen van politie en justitie te danken dat het in deze zaak aangetoonde feitelijke misbruik van de verkregen inloggegevens relatief beperkt is gebleven. Verdachte was immers al druk doende om het virus en de trojan verder te exploiteren, zulks met behulp van buitenlandse rekeningnummers en een buitenlandse opdrachtgever. Daarnaast heeft verdachte, gebruikmakend van het botnet, zich schuldig gemaakt aan pogingen om een bedrijf af te persen door te dreigen met een dDOS aanval dan wel door een dDOS aanval uit te voeren. Met dergelijke acties wordt grote inbreuk gemaakt op het nog steeds toenemende economische belang van de informatie- en communicatietechnologie en het grote maatschappelijke belang van het internet en daarmee samenhangende toepassingen. Verdachte heeft zich tenslotte schuldig gemaakt aan overtreding van de Wet Wapens en Munitie.

Uitspraak

RECHTBANK BREDA

Parketnummer(s): 981204/05

1 Partijen. Onderzoek van de zaak.

In de zaak onder voormeld parketnummer van de officier van justitie in het arrondissement Breda[voornaam verdachte]:

[verdachte],
geboren op [datum en plaats]
wonende te [adres]

heeft de meervoudige kamer van deze rechtbank het volgende vonnis gewezen.

De rechtbank heeft de gedingstukken gezien en de zaak onderzocht ter terechtzitting. Zij heeft de vordering van de officier van justitie gehoord en het verweer dat naar voren is gebracht door de verdachte en de raadsman, mr. Van Halderen, advocaat te Haarlem.
2 De tenlastelegging.

De tenlastelegging is gewijzigd overeenkomstig artikel 313 van het Wetboek van Strafvordering. Verdachte staat, met inachtneming hiervan, terecht terzake dat

1.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), of in een deel daarvan, is binnen gedrongen, waarbij hij, verdachte en/of zijn medeverdachte(n) de beveiliging heeft doorbroken, in elk geval de toegang heeft verworven door een technische ingreep, met behulp van valse signalen en/of een valse sleutel en/of door het aannemen van een valse hoedanigheid, namelijk (telkens) door(, gebruikmakend van één of meer kwetsbaarhe(i)d(en) in het besturingssysteem van Windows,) een (al dan niet door verdachte en/of een van zijn mededader(s) gemaakt/ontwikkeld) (versie van een) virus, (onder meer) bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren waarna hij, verdachte en/of zijn mededader(s), door tussenkomst van het geautomatiseerde werk waarin hij/zij is/zijn binnengedrongen de toegang heeft verworven tot één of meer geautomatiseerde werk(en) van één of meer derde(n);
(zaaksdossier B 1, verspreiden Toxbot, artikel 138a lid 1 aanhef en onder b en lid 3 aanhef en onder b Wetboek van strafrecht)

2.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon. op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft verdachte en/of zijn mededader(s) (telkens)
- één of meer (versie(s) van een) virus(en) en/of trojan(s) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Wayphisher) en/of,
- (aan een/zijn botnetwerk) één of meer opdracht(en) gegeven het/de(door verdachte en/of zijn mededader(s) (mede) gemaakte en/of ontwikkelde (versie(s)) virus(sen) en/of de trojan(s) te downloaden en/of op de betreffende en/of één of meer andere computer(s) te installeren (waarna het betreffende virus en/of trojan is geïnstalleerd)
waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest
immers,
- de gebruikers van de aldus 'besmette' computer(s) waren niet meer in staat om betrouwbaar gebruik te maken van een/de online (bancaire) dienst(en) (die doelwit waren van het virus en/of de trojan) (immers werd die gebruiker bij/na het gebruik van (een) internetadres(sen) (van (een) bank(en)) omgeleid naar één of meer andere internetadressen en/of (waarna) de

inloggegevens (ten behoeve van het online/electronisch bankieren) konden en/of werden onderschept)
en/of
- (waarna) verdachte en/of zijn mededader(s) de beschikking kregen over bancaire en/of andere gegeven(s) toebehorende aan één of meer van die gebruiker(s).
(zaaksdossier B4, artikel 161sexies aanhef en onder 2 Wetboek van strafrecht)

3.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, (telkens) opzettelijk één of meer geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten één of meer computer(s) en/of server(s), heeft beschadigd of onbruikbaar gemaakt en/of stoornis in de gang of in de werking van zodanig werk heeft veroorzaakt en/of een ten opzichte van zodanig werk genomen veiligheidsmaatregelen heeft verijdeld,
immers, heeft/hebben verdachte en/of zijn mededader(s) (telkens):
- één of meer (versie(s) van een) virus(sen) gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Toxbot) en/of
- dit/deze virus(sen) op één of meer andere computer(s) geïnstalleerd en/of doen installeren, waarna het/de (aldus besmette) geautomatiseerde werk(en) (vervolgens) (automatisch) herstartte(n) en/of crashte(n), waardoor gemeen gevaar voor goederen en/of voor de verlening van diensten te duchten is geweest,
immers werden (hierdoor) de toetsaanslagen van de gebruiker(s) van de aldus besmette computer(s) (zonder medeweten van die gebruiker(s)) vastgelegd, waardoor verdachte en/of zijn mededader(s) de beschikking kregen over:
- financiële/bancaire gegevens van één of meer bank(en) en/of creditcard maatschappij(en) en/of,
- inlog- en wachtwoordgegevens van één of meer Paypal-account(s) en/of;
- inlog- en wachtwoordgegevens van één of meer Ebay-account(s) en/of;
- één of meer ander(e) gegeven(s)
van (één of meer van) die gebruiker(s).
(zaaksdossier B 1, artikel 161sexies aanhef en onder 2 Wetbock van strafrecht)

4.
hij op één of meer tijdstip(pen) in de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, en/of te Rijswijk, althans in Nederland, tezamen en in vereniging met een ander of anderen, althans alleen, (telkens) opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, heeft veranderd, gewist, onbruikbaar gemaakt en/of ontoegankelijk heeft gemaakt dan wel andere gegevens daaraan heeft toegevoegd,
immers, heeft/hebben verdachte en of zijn mededader(s) (een/zijn/hun botwerk) één of meer opdracht(en) gegeven één of meer computerprogramma('s) van het bedrijf MediaTickets en/of het bedrijf 180Solutions en/of het bedrijf Loudcash en/of het bedrijf Yoursitebar van internet te downloaden en/of te intalleren en aldus één of meer van de betreffende programma('s) aan één of meer geautomatiseerde werk(en) heeft/hebben toegevoegd;
(zaaksdossier B 1, artikel 350a lid 1 Wetboek van strafrecht)

5.
hij op één of meer tijdstip(pen) in de periode van 1 juni 2005 tot en met 4 oktober 2005 te

Loon op Zand en/of te Rijswijk, althans in Nederland, tezamen en in vereniging met een ander of anderen, althans alleen, (telkens) met het oogmerk om zich en/of (een) ander(en) wederrechtelijk te bevoordelen (telkens) 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, het bedrijf MediaTickets en/of het bedrijf 180Solutions en/of het bedrijf Loudcash heeft/hebben bewogen tot de afgifte van één of meer geldbedrag(en), in elk geval van enig goed,
immers heeft/hebben verdachte en/of zijn mededader(s) (telkens) met bovenomschreven oogmerk -zakelijk weergegeven- valselijk en/of listiglijk en/of bedriegelijk en/of in strijd met de toepasselijke (algemene) daaraan gestelde voorwaarden, één of meer programma('s) ontwikkeld door en/of geëxploiteerd door (meer van) genoemd(e) bedrijf/bedrijven verspreid en/of doen verspreiden en/of geïnstalleerd en/of doen installeren op één of meer geautomatiseerde werk(en) (al dan niet behorend tot zijn/hun botnetwerk) waardoor het bedrijf MediaTickets en/of het bedrijf 180Solutions en/of het bedrijf Loudcash (telkens) werden bewogen tot bovengenoemde afgifte;
(zaaksdossier BX, artikel 326 Wetboek van Strafrecht)

6.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 1 september 2005 tot en met 5 september 2005 en/of de periode van 6 september 2005 tot en met 7 september 2005 te Loon op Zand en/of te Rijswijk, althans in Nederland, tezamen en in vereniging met een ander of anderen, althans alleen, (telkens) met het oogmerk om zich en/of (een) ander(en) wederrechtelijk te bevoordelen door geweld en/of bedreiging met geweld en/of met bedreiging dat gegevens die door middel van een geautomatiseerd werk waren opgeslagen, onbruikbaar en/of ontoegankelijk zouden worden gemaakt en/of zouden worden gewist, (het bedrijf) MediaTickets heeft/hebben gedwongen tot de afgifte van één of meer geldbedrag(en) (namelijk ongeveer $ 2.100,- en/of € 2.100,-), in elk geval van enig goed, geheel of ten dele toebehorende aan MediaTickets, in elk geval aan een ander of anderen dan aan verdachte en/of zijn mededader(s)
Immers, heeft/hebben verdachte en of zijn mededader(s) al dan niet via een/zijn/hun botnetwerk)
- gedreigd één of meer handeling(en) te verrichten en/of één of meer opdracht(en) te geven aan één of meer geautomatiseerde werk(en) en/of computer(s) waardoor de (download)server(s) van en/of in gebruik bij MediaTickets offline zou(den) gaan en/of niet meer via het internet bereikbaar zou zijn en/of
- één of meer handeling(en) verricht en/of één of meer opdracht(en) gegeven aan één of meer geautomatiseerde werk(en) en/of computer(s) waardoor de (download)server(s) van en/of in gebruik bij MediaTickets offline is/zijn gegaan en/of niet meer via het internet bereikbaar is/zijn geweest en/of
- één of meerdere d-dos-aanval(len) uitgevoerd gericht tegen (de server(s) en/of de website van en/of in gebruik bij) MediaTickets, teneinde die server(s) en/of website ontoegankelijk/onbereikbaar te maken te maken voor derden;
(zaaksdossier BX, artikel 317 lid 2 Wetboek van strafrecht)

subsidiair, althans, indien het vorenstaande onder 6 niet tot een veroordeling mocht of zou kunnen leiden:

hij op één of meer tijdstip(pen) in of omstreeks de periode van 1 september 2005 tot en met 5 september 2005 en/of de periode van 6 september 2005 tot en met 7 september 2005 te Loon op Zand en/of te Rijswijk, althans in Nederland, ter uitvoering van het door verdachte en/of

zijn mededader voorgenomen misdrijf om, tezamen en in vereniging met een ander of anderen, althans alleen, (telkens) met het oogmerk om zich en/of (een) ander(en) wederrechtelijk te bevoordelen door geweld en/of bedreiging met geweld en/of met bedreiging dat gegevens die door middel van een geautomatiseerd werk waren opgeslagen, onbruikbaar en/of ontoegankelijk zouden worden gemaakt en/of zouden worden gewist, (het bedrijf) MediaTickets te dwingen tot de afgifte van één of meer geldbedrag(en) (namelijk ongeveer $ 2.100,- en/of € 2.100,-), in elk geval van enig goed, geheel of ten dele toebehorende aan MediaTickets, in elk geval aan een ander of anderen dan aan verdachte en/of zijn mededader(s)
Immers, heeft/hebben verdachte en of zijn mededader(s)
- gedreigd één of meer handeling(en) te verrichten en/of één of meer opdracht(en) te geven aan één of meer geautomatiseerde werk(en) en/of computer(s), al dan niet deeluitmakend van een/zijn/hun botnetwerk, waardoor de (download)server(s) van en/of in gebruik bij MediaTickets offline zou(den) gaan en/of niet meer via het internet bereikbaar zou zijn en/of
- één of meer handeling(en) verricht en/of één of meer opdracht(en) gegeven aan één of meer geautomatiseerde werk(en) en/of computer(s), al dan niet deeluitmakend van een/zijn/hun botnetwerk, waardoor de (download)server(s) van en/of in gebruik bij MediaTickets offline is gegaan en/of niet meer via het internet bereikbaar is geweest en/of
- één of meerdere d-dos-aanval(len) uitgevoerd gericht tegen (de server(s) en/of de website van en/of in gebruik bij) MediaTickets, teneinde die server(s) en/of website ontoegankelijk/onbereikbaar te maken te maken voor derden,
terwijl de uitvoering van dat voorgenomen misdrijf niet is voltooid.
(zaaksdossier BX, artikel 317 lid 2 Wetboek van strafrecht)

7.
hij op één of meer tijdstip(pen) in de periode van 28 februari 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met een ander of anderen, althans alleen, (telkens) met het oogmerk om zich en/of (een) ander(en) wederrechtelijk te bevoordelen (telkens) 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, diverse deels onbekend gebleven personen en/of bedrijven, waaronder Marc Hill, althans het bedrijf/de persoon gebruikmakend van het e-mailadres e_gracie78@hotmail.com en/of Uwe [slachtoffer], althans Groove Music en/of Droplet heeft/hebben bewogen tot de afgifte van een Alienware DAW Digital Audio Workstation (op of omstreeks 9 augustus 2005) (handel 1) en/of één of meer (geluids)box(en)/speaker(s) (op of omstreeks 28 februari 2005) (handel 2) en/of één of meer paar Prada schoenen (op of omstreeks 11 september 2005) (handel 3) en/of één of meer PSP('s)/Playstation(s) en/of Ridge Racer (game(s)) (op of omstreeks 29 juli 2005) (handel 4) en/of één of meer PSP('s)/Playstation(s) en/of Ipod(s) (op of omstreeks 20 juli 2005) (handel 5) en/of één of meer videokaart(en) (van
het type/merk Galaxy Geforce) (op of omstreeks 20 juli 2005) (handel 6) en/of één of meer digitale (foto)camera('s) (van het merk Sony), op of omstreeks 12 juli 2005 en/of (tevens) één of meer (andere) PSP's/Playstation(s) en/of één of meer (andere) Ipod(s) en/of één of meer (andere) (foto)camera(`s) en/of één of meer geheugenkaart(en) en/of één of meer laptop(s) en/of één of meer filmcamera(`s) en/of één of meer MP3 speler(s) en/of één of meer DVD-speler(s) en/of één of meer game(s) en/of één of meer navigatiesyste(e)m(en) en/of één of meer onderde(e)l(en) van (een) computersyste(e)m(en) en/of één of meer andere goed(eren), immers heeft/hebben verdachte en/of (één van) zijn mededader(s) (telkens) met bovenomschreven oogmerk -zakelijk weergegeven- via het internet genoemd(e) goederen) besteld en hierbij gebruik gemaakt van
- (een) valse na(a)m(en) en/of (andere) valse persoonsgegevens en/of

- valse/vervalste Ebay-accounts, althans Ebay-accounts waarvan verdachte en/of (één van) zijn mededader(s) wederechtelijk gebruik maakte(n) en/of
- valse/vervalste Paypal-accounts, althans Paypal accounts waarvan verdachte en/of (één van) zijn mededader(s) wederrechtelijk gebruik maakte(n) en/of
- valse creditcardgegevens en/of persoonsgegevens, althans met creditcardgegevens en/of persoonsgegevens waarvan verdachte en/of (één van) zijn mededader(s) wederrechtelijk gebruik maakte(n)
waardoor de bovengenoemde personen en/of bedrijven (telkens) werden bewogen tot bovengenoemde afgifte;
(zaaksdossier BX, artikel 326 Wetboek van Strafrecht)

subsidiair, althans, indien het vorenstaande onder 7 niet tot een veroordeling mocht of zou kunnen leiden:

hij op één of meer tijdstip(pen) in de periode van 28 februari 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met één of meer ander(en), althans alleen, een beroep of gewoonte heeft gemaakt van het kopen van goederen met het oogmerk om zonder volledige betaling zich of (een) ander(en) de beschikking over die goederen te verzekeren,
immers heeft verdachte en/of (één van) zijn mededader(s) (telkens) met dat oogmerk
- één of meer bestelling(en) gedaan en/of geplaatst ter verkrijging van één of meer goed(eren) en/of
- ter (verzekering van de) betaling van dat/die goed(eren) (gestolen en/of op andere (wederrechtelijke) wijze verkregen) bancaire en/of andere betalingsgegegevens opgegeven van (een) ander(en) (niet zijnde verdachte en/of zijn mededader(s))
te weten (in ieder geval) betreffende:
- een Alienware DAW Digital Audio Workstation, op of omstreeks 9 augustus 2005 (handel 1) en/of
- één of meer (geluids)box(en)lspeaker(s), op of omstreeks 28 februari 2005 (handel 2) en/of
- één of meer paar Prada schoenen, op of omstreeks 11 september 2005 (handel 3) en/of
- één of meer PSP('s)/Playstation(s) en/of Ridge Racer (game(s)), op of omstreeks 29 juli 2005 (handel 4) en/of
- één of meer PSP('s)/Playstation(s) en/of Ipod(s), op of omstreeks 20 juli 2005 (handel 5) en/of
- één of meer videokaart(en) (van het type/merk Galaxy Geforce), op of omstreeks 20 juli 2005 (handel 6) en/of
- één of meer digitale (foto)camera(`s) (van het merk Sony), op of omstreeks 12 juli 2005 en/of
(tevens) één of meer (andere) PSP's/Playstation(s) en/of één of meer (andere) Ipod(s) en/of één of meer (andere) (foto)camera('s) en/of één of meer geheugenkaart(en) en/of één of meer laptop(s) en/of één of meer filmcamera(`s) en/of één of meer MP3 speler(s) en/of één of meer DVD-speler(s) en/of één of meer game(s) en/of één of meer navigatiesyste(e)m(en) en/of één of meer onderde(e)l(en) van (een) computersyste(e)m(en) en/of één of meer andere goed(eren);
(zaaksdossier BX, artikel 326a Wetboek van strafrecht)

8.
hij op één of meer tijdstip(pen) in of omstreeks de periode van 5 juli 2005 tot en met 22 juli 2005 te Loon op Zand en/of Rijswijk, althans in Nederland, (telkens) tezamen en in vereniging met één of meer ander(en), althans alleen, opzettelijk wederrechtelijk in een

geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten (een) computer(s) en/of (een) server(s) (toebehorende aan en/of in gebruik bij theworldofgolf), of in een deel daarvan, is binnengedrongen, waarbij hij verdachte, en/of (één van) zijn mededader(s) de beveiliging heeft doorbroken, in elk geval de toegang heeft verworven door een technische ingreep, met behulp van valse signalen en/of een valse sleutel en/of het aannemen van een valse hoedanigheid, waarna hij, verdachte, en/of (een van) zijn mededader(s) vervolgens gegevens, te weten creditcard- en/of (bijbehorende) andere (persoons)gegevens (van klanten van www.theworldofgolf.nl), die waren opgeslagen in dat geautomatiseerde werk waarin hij, verdachte, en/of (een van) zijn mededader(s) zich wederrechtelijk bevond(en), heeft overgenomen en voor zichzelf en/of (een) ander(en) heeft vastgelegd;
(zaaksdossier BX, artikel 138a lid 2 Wetboek van strafrecht)

9.
hij op of omstreeks 4 oktober 2005 te Loon op Zand een wapen (merk Gabilonda) van categorie I onder 7°, te weten een voorwerp dat voor wat betreft zijn vorm, afmeting en kleur een sprekende gelijkenis vertoonde met een pistool van het merk Pietro Beretta, model 98 FS, voorhanden heeft gehad;
(zaaksdossier BX, artikel 13 lid I Wet wapens en munitie).
3 De geldigheid van de dagvaarding.

De rechtbank is van oordeel dat de dagvaarding met betrekking tot het onder 7. primair tenlastegelegde gedeelte

“en/of (tevens) één of meer (andere) PSP's/Playstation(s) en/of één of meer (andere) Ipod(s) en/of één of meer (andere) (foto)camera(`s) en/of één of meer geheugenkaart(en) en/of één of meer laptop(s) en/of één of meer filmcamera(`s) en/of één of meer MP3 speler(s) en/of één of meer DVD-speler(s) en/of één of meer game(s) en/of één of meer navigatiesyste(e)m(en) en/of één of meer onderde(e)l(en) van (een) computersyste(e)m(en) en/of één of meer andere goed(eren)”

te algemeen en onvoldoende feitelijk omschreven is, mede gelet op de lange tenlastegelegde periode waarin de feiten zouden zijn gepleegd en de onbekendheid van de slachtoffers. Zij zal de dagvaarding voor dat gedeelte nietig verklaren.
De rechtbank is van oordeel dat de dagvaarding voor het overige aan de eisen van artikel 261 van het Wetboek van Strafvordering voldoet en dus geldig is, nu ook overigens niets is gebleken wat daaraan in de weg staat.
4 De bevoegdheid van de rechtbank.

Krachtens de wettelijke bepalingen is de rechtbank bevoegd van het ten laste gelegde kennis te nemen.
5 De ontvankelijkheid van de officier van justitie.

Bij het onderzoek ter terechtzitting zijn geen omstandigheden gebleken die aan de ontvankelijkheid van de officier van justitie in de weg staan. Hij kan dus in zijn vordering worden ontvangen.
6 Schorsing der vervolging.

Bij het onderzoek ter terechtzitting zijn geen gronden voor schorsing der vervolging gebleken.
7 De bewezenverklaring.
7.1 Vrijspraak en de gronden daarvoor.

Door het onderzoek ter terechtzitting is naar het oordeel van de rechtbank niet wettig en overtuigend bewezen hetgeen aan de verdachte onder 4., 5., 6. primair en 8. is ten laste gelegd, zodat hij daarvan zal worden vrijgesproken.

De rechtbank is van oordeel dat, ook al staat vast dat verdachte installaties heeft verzorgd voor MediaTickets en Yoursitebar, het onder 4. tenlastegelegde feit niet wettig en overtuigend bewezen kan worden, aangezien er in het proces-dossier geen bewijs aanwezig is voor het feit dat die installaties zijn geschied doordat verdachte opdracht heeft gegeven aan het botnetwerk om computerprogramma('s) van die bedrijven te downloaden en/of te installeren en die/dat programma('s) aan een of meer geautomatiseerde werk(en) toe te voegen. Ook is er onvoldoende bewijs voor het feit dat die installaties op andere wijze wederrechtelijk zouden hebben plaatsgevonden.
Met betrekking tot de bedrijven 180Solutions en Loudcash is in het procesdossier niets aangetroffen waaruit zou kunnen blijken dat verdachte voor die bedrijven installaties heeft verricht, laat staan dat hij dat op een wederrechtelijke wijze zou hebben gedaan.
Nu niet vaststaat dat er installaties zijn verricht dan wel dat dat op wederrechtelijke wijze zou zijn gebeurd kan, naar het oordeel van de rechtbank, ook niet bewezen worden dat verdachte op die wijze Mediatickets, 180Solutions en Loudcash heeft bewogen tot afgifte van geldbedragen voor die installaties. Dit heeft tot gevolg dat verdachte ook van het onder 5. tenlastegelegde moet worden vrijgesproken.

Voorts is de rechtbank van oordeel dat het onder 6. primair tenlastegelegde niet wettig en overtuigend bewezen kan worden, omdat niet is komen vast te staan dat Mediatickets het in de tenlastelegging genoemde geldbedrag aan verdachte betaald heeft en er aldus geen sprake is van "afgifte" van dat bedrag.

Omdat niet is komen vast te staan dat de handelwijze van verdachte ertoe heeft geleid dat het onder feit 7 genoemde Alienware DAW Digital Audio Workstation werd afgegeven, is dit onderdeel van het onder 7. tenlastegelegde feit niet wettig en overtuigend bewezen

Tenslotte is de rechtbank van oordeel dat, hoewel vaststaat dat verdachte in het bezit was van creditcard- en andere persoonsgegevens van klanten van The World of Golf, niet bewezen kan worden dat verdachte wederrechtelijk in de computer van The World of Golf is binnengedrongen, hetgeen tot gevolg heeft dat ook het onder 8. tenlastegelegde feit niet wettig en overtuigend bewezen kan worden. Immers niet bewezen kan worden dat enige beveiliging is doorbroken of de toegang is verkregen op andere wederrechtelijke wijze.
7.2 Hetgeen bewezen is.

Door het onderzoek ter terechtzitting is evenwel naar het oordeel van de rechtbank wettig en overtuigend bewezen dat de verdachte

1.

op tijdstip(pen) in de periode van 1 juni 2005 tot en met 4 oktober 2005 in Nederland, tezamen en in vereniging met één (telkens) opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten computer(s), is binnen gedrongen, waarbij hij, verdachte en zijn medeverdachte de toegang heeft verworven door een technische ingreep, met behulp van valse signalen, namelijk (telkens) door(, gebruikmakend van één of

meer kwetsbaarhe(i)d(en) in het besturingssysteem van Windows,) een (door verdachte gemaakte/ontwikkelde) (versie van een) virus, (onder meer) bekend onder de naam Toxbot, te verspreiden en/of te installeren waarna hij, verdachte en zijn mededader, door tussenkomst van het geautomatiseerde werk waarin zij zijn binnengedrongen de toegang hebben verworven tot geautomatiseerde werk(en) van derde(n);

2.

op tijdstip(pen) in de periode van 6 juli 2005 tot en met 4 oktober 2005 te Loon. op Zand tezamen en in vereniging met één ander (telkens) opzettelijk stoornis in de gang of in de werking van geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten computer(s) heeft veroorzaakt ,
immers, hebben verdachte en zijn mededader(telkens)
na één trojan te hebben gemaakt (onder meer) bekend onder de naam Wayphisher) (aan een/zijn botnetwerk) opdracht(en) gegeven de(door verdachte en zijn mededadergemaakte trojante downloaden en op de betreffende computer(s) te installeren (waarna de betreffende trojan is geïnstalleerd)
waardoor gemeen gevaar voor de verlening van diensten te duchten is
geweest immers, de gebruikers van de aldus 'besmette' computer(s) waren niet meer in staat om betrouwbaar gebruik te maken van online (bancaire) dienst(en) (die doelwit waren van de trojan) (immers werden die gebruikers bijhet gebruik van internetadres(sen) (van bank(en)) omgeleid naar één ander internetadres en (waarna) de inloggegevens (ten behoeve van het online/electronisch bankieren) konden en/of werden onderschept)
en(waarna) verdachte en/of zijn mededader de beschikking kregen over bancaire en/of andere gegeven(s) toebehorende aan die gebruiker(s).

3.

op tijdstip(pen) in de periode van 6 juli 2005 tot en met 4 oktober 2005 in Nederland, tezamen en in vereniging met één ander (telkens) opzettelijk stoornis in de gang of in de werking van geautomatiseerde werk(en) voor de opslag of verwerking van gegevens, te weten computer(s), heeft veroorzaakt , immers, hebben verdachte en/of zijn mededader (telkens) (versie(s) van een) virus gemaakt en/of ontwikkeld ((onder meer) bekend onder de naam Toxbot) en dit virus op andere computer(s) geïnstalleerd, waarna de (aldus besmette) geautomatiseerde werk(en) (vervolgens) (automatisch) herstartte(n) en/of crashte(n), waardoor gemeen gevaar voor de verlening van diensten te duchten is geweest,
immers werden de toetsaanslagen van de gebruiker(s) van de aldus besmette computer(s) (zonder medeweten van die gebruiker(s)) vastgelegd, waardoor verdachte en zijn mededader de beschikking kregen over:
-inlog- en wachtwoordgegevens van Paypal-account(s) en;
- inlog- en wachtwoordgegevens van Ebay-account(s) van die gebruiker(s).

6. subsidiair

inde periode van 1 september 2005 tot en met 5 september 2005 te Loon op Zand ter uitvoering van het door verdachte voorgenomen misdrijf om met het oogmerk om zich wederrechtelijk te bevoordelen door bedreiging met geweld (het bedrijf) MediaTickets te dwingen tot de afgifte van één geldbedrag(namelijk ongeveer $ 2.100,- toebehorende aan MediaTickets, immers, heeft verdachte gedreigd - opdracht(en) te geven aan computer(s), deeluitmakend van een/zijn botnetwerk, waardoor de server van en in gebruik bij

MediaTickets offline zou gaan en niet meer via het internet bereikbaar zou zijn
terwijl de uitvoering van dat voorgenomen misdrijf niet is voltooid.

en

in de periode van 6 september 2005 tot en met 7 september 2005 te Loon op Zand en/of te Rijswijk, ter uitvoering van het door verdachte en zijn mededader voorgenomen misdrijf om, tezamen en in vereniging met het oogmerk om zich wederrechtelijk te bevoordelen door geweld(het bedrijf) MediaTickets te dwingen tot de afgifte van ééngeldbedrag(namelijk ongeveer $ 2.100,-), toebehorende aan MediaTickets, immers,hebben verdachte en zijn mededader server opdracht(en) gegeven aan computer(s), deeluitmakend van hun botnetwerk, waardoor de server van en- in gebruik
bij MediaTickets offline is gegaan en niet meer via het internet bereikbaar is geweest,
terwijl de uitvoering van dat voorgenomen misdrijf niet is voltooid.

7. primair

op tijdstip(pen) in de periode van 28 februari 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met anderen, met het oogmerk om zich en/ofander(en) wederrechtelijk te bevoordelen oor het aannemen van een valse naam envan een valse hoedanigheid ,
diverse deels onbekend gebleven personen en/of bedrijven, waaronder Uwe [slachtoffer] en Droplet heeft bewogen tot de afgifte van
(geluids)box(en)/speaker(s) (op of omstreeks 28 februari 2005) en één paar Prada schoenen (op of omstreeks 11 september 2005) en PSP('s)/Playstation(s) en Ridge Racer (game(s)) (op of omstreeks 29 juli 2005) en/ PSP('s)/Playstation(s) en Ipod(s) (op of omstreeks 20 juli 2005) en één videokaart (van het type/merk Galaxy Geforce) (op of omstreeks 20 juli 2005) en één digitale (foto)camera (van het merk Sony), op of omstreeks 12 juli 2005, immers hebben verdachte en (één van) zijn mededader(s) (telkens) met bovenomschreven oogmerk
-zakelijk weergegeven- via het internet genoemd(e) goederen) besteld en hierbij gebruik gemaakt van
- valse nam(en) en (andere) valse persoonsgegevens en vervalste Ebay-accounts en vervalste Paypal-accounts, waardoor de bovengenoemde personen en/of bedrijven werden bewogen tot bovengenoemde afgifte.

9.

op 4 oktober 2005 te Loon op Zand een wapen (merk Gabilonda) van categorie I onder 7°, te weten een voorwerp dat voor wat betreft zijn vorm, afmeting en kleur een sprekende gelijkenis vertoonde met een pistool van het merk Pietro Beretta, model 98 FS, voorhanden heeft gehad.

De rechtbank overweegt hierbij dat, waar in de bewezenverklaring tekstuele wijzigingen zijn aangebracht, dit is gebeurd in verband met de spelling dan wel de zinsopbouw.
De rechtbank is van oordeel dat verdachte hierdoor niet in zijn verdediging is geschaad.

Hetgeen onder 1. tot en met 3., 6. subsidiair, 7. primair en 9. meer of anders is ten laste gelegd

dan hierboven bewezen is verklaard, is naar het oordeel van de rechtbank niet bewezen. Verdachte zal hiervan worden vrijgesproken.

8 Het bewijs.

De overtuiging van de rechtbank, dat de verdachte het bewezen verklaarde heeft begaan, is gegrond op de feiten en de omstandigheden die zijn vervat in de volgende bewijsmiddelen. De bewijsmiddelen worden slechts gebezigd met betrekking tot het feit, waarop zij in het bijzonder betrekking hebben.

8.1 De bewijsmiddelen.

8.2 De bijzondere overwegingen omtrent het bewijs.

Het horen van getuigen.

Door de verdediging is diverse malen aangevoerd dat de directie van MediaTickets en de personen die de goederen ontvingen in de studentenhuizen als getuigen gehoord hadden kunnen worden, maar dat dat niet is gebeurd.

Hoewel de raadsman in zijn pleidooi niet expliciet gevraagd heeft om deze personen alsnog als getuigen te horen, vat de rechtbank dit toch als een zodanig verzoek op. Bij de beoordeling van dat verzoek zal de rechtbank uitgaan van het noodzakelijk-heids-criterium.

De rechtbank verwijst naar hetgeen ten aanzien van deze verzoeken door haar in het kader van de eerdere behandelingen reeds is beslist. Hetgeen daaraan ten grondslag ligt, heeft naar het oordeel van de rechtbank nog steeds gelding en wordt door de rechtbank gehandhaafd. Overigens zijn de verklaringen van elk van deze getuigen, gelet op het aanwezige bewijs, in redelijkheid niet nodig voor enige door de rechtbank te nemen beslissing. Daarnaast is de rechtbank van oordeel dat de verdediging bij het horen van vier verbalisanten door de rechter-commissaris ruimschoots de gelegenheid heeft gehad om over het totale onderzoek uitgebreid vragen te stellen en er derhalve aan de wensen van de verdediging recht is gedaan.

Stukken in de Engelse taal.

De verdediging heeft tijdens het onderzoek ter terechtzitting aangegeven niets te begrijpen van enkele onderdelen van het dossier die mogelijk als bewijsmiddel zouden kunnen dienen. De reden daarvoor was dat de betreffende passages (chats en e-mails) in de Engelse taal zijn opgenomen en niet (door een beëdigd vertaler) zijn vertaald. De rechtbank begrijpt hieruit dat de betreffende passages van het bewijs dienen te worden uitgesloten.

De rechtbank overweegt hieromtrent het volgende:

De rechtbank stelt voorop dat er geen verplichting bestaat om processtukken te laten vertalen. Het gaat in deze zaak om, in de Engelse taal gevoerde en uitgewerkte chats en emailverkeer, waaraan verdachten hebben deelgenomen. Vaststaat daarmede dat ook verdachten de Engelse taal voldoende machtig zijn om de inhoud van deze stukken te begrijpen. De verdediging heeft bovendien nooit om een vertaling verzocht, zulks noch vóór noch tijdens de inhoudelijke behandeling van de zaak, alwaar enkele van deze stukken zijn voorgehouden. Nu de raadsman van verdachte desgevraagd bovendien heeft aangegeven dat hij de Engelse taal beheerst, doch niet in de hoedanigheid waarin hij thans optreedt, dient dit nauwelijks als serieus te betitelen verweer te worden verworpen.

De inhoud van het dossier.

Door de verdediging zijn als eerste de volgende verweren ten aanzien van het door het Openbaar Ministerie gepresenteerde bewijs gevoerd:

1 Er bevindt zich in het dossier geen aangifte.
2 Er is verzuimd kopieën over te leggen van harde schijven van de pc's behorende bij de IP adressen die bij het onderzoek zijn gevonden.
3 Alles is gebaseerd op technisch onderzoek.
4 In het ongewisse is of er enig direct verband bestaat tussen de geïnfecteerde pc's en verdachten.

Met hetgeen is vermeld onder 1 en 2 miskent de verdedi-ging, dat deze zaken niet vereist zijn voor de vraag of tot een bewezenverklaring kan worden gekomen. Immers het gepleegd zijn van een strafbaar feit en de aard daarvan, wat in het algemeen de inhoud van een aangifte vormt, alsmede de vraag of pc's zijn besmet, kan ook uit andere bewijs-middelen naar voren komen, bijvoorbeeld uit hetgeen door verbali-santen zelf als feiten en omstandigheden is waargenomen of ondervonden, waarbij de eigen kennis en deskundigheid van de verbalisanten, mede een rol speelt. Dat bewijs kan ook zijn gebaseerd op gevolg-trek-kingen die logischerwijs uit het wel aanwezige bewijsmateriaal moeten worden getrokken.

De deskundigheid van verbalisanten is door de verdediging niet bestreden. De rechtbank heeft zelf ook geen aanleiding om daaraan te twijfelen, zodat de rechtbank van de deskundigheid van de verbalisanten op het gebied waarop het onderhavige onderzoek zich richt, uitgaat.

Wanneer, zoals in deze zaak aan de orde is, een virus wordt geschreven dat, zoals het toxbot, bestemd is om zichzelf als een virus te verspreiden, dan kan op grond van de bevinding van de verbalisanten dat er vanuit een server opdracht wordt gegeven aan pc's om dat virus te downloaden, het gegeven dat daarna blijkt dat er pc's contact zoeken met de server en het feit dat er handelingen blijken te zijn verricht die in het virus staan omschreven, de conclusie geen andere zijn dan dat er pc's zijn besmet. Enig onderzoek van die pc's en/of een aangifte van de eigenaar van die pc's is dan geen vereiste om tot een bewezenverklaring te kunnen komen.

De stelling dat er alleen technisch onderzoek is, behoeft geen bespreking, nu uit het dossier duidelijk anders blijkt.

Hetgeen is aangevoerd onder 4, vormt voor de rechtbank aanleiding om alvorens in te gaan op het bewijs voor de diverse bewezen verklaarde feiten, afzonderlijk in te gaan op hetgeen uit het dossier omtrent de identiteit van de daders naar voren komt.

De verdachten.
Vooropgesteld moet worden dat het door verdachten gestelde gebruik van de onderzochte computers door anderen, volstrekt niet is onderbouwd. Een dergelijke onderbouwing had van verdachten mogen worden verlangd gelet op de vele zich in het dossier bevindende bewijsmiddelen die wezen op gebruik door hen.
Voor de verdachte [verdachte 1] geldt daarnaast nog dat op de vraag of er naast [verdachte 1] nog iemand anders is geweest die zowel gebruik heeft gemaakt van de PC die [verdachte 1] bij Orit gebruikte als de pc op [verdachte 1]'s huisadres, verdachte geen antwoord heeft gegeven. Behalve [verdachte 1] zou alleen een dergelijk persoon hebben kunnen bewerkstelligen dat gegevens die betrekking hebben op feit 7, de afgifte van geluidsboxen, in beide pc's te vinden zijn.

Uit de bewijsmiddelen blijkt het volgende:
Het onderzoek tegen verdachte en zijn mededader is aangevangen nadat in een aangifte door Sara, het reken- en netwerk-diensten-centrum van Universitair Nederland, was gemeld dat

wachtwoorden en gebruikersnamen waren ontvreemd. Dit feit was Sara ter kennis gebracht door de heer [naam], werkzaam als systeembeheerder bij [naam bedrijf], bij welk bedrijf verdachte [verdachte 1] als stagiair werkzaam was. Hij had de informatie over de ontvreemdde bestanden van verdachte [verdachte 1] zelf ontvangen tijdens een chat met [verdachte 1].(dossier A bijlage A001 pag 4).
Een chat waarin [verdachte 1] de nickname detox gebruikte.
[naam] geeft informatie over de IP adressen waarmee [verdachte 1] op internet zat. Een aantal daarvan waren in gebruik bij [naam bedrijf] en één betrof een aansluiting die op naam stond van [verdachte 1].

Dat de nickname detox door [verdachte 1] en de nickname oo door [verdachte 2] werd gebruikt, blijkt verder uit het volgende:
Blijkens het proces-verbaal zijn in het chatverkeer tussen detox en oo, bij het uitwisselen van bestanden, de IP adressen zichtbaar, welke IP adressen zijn terug te voeren op verdachten. [verdachte 2] verklaart dat hij wel eens heeft gechat met iemand die de nickname detox gebruikt en van wie hij denkt dat de echte naam [voornaam verdachte] is. In een van die chats worden tussen detox en oo telefoonnummers uitgewisseld die ofwel op naam staan van een van de verdachten ([verdachte 2]) ofwel blijkens telefoontaps in gebruik zijn bij een van de verdachten ([verdachte 1]). Uit een chat (dd 12 juli) tussen detox en oo blijkt dat er gereageerd wordt op een sms die vanuit het telefoonnummer van [verdachte 2] is verstuurd naar het telefoonnummer in gebruik bij [verdachte 1]. [getuige] verklaart dat [verdachte 1] de naam detox als nickname gebruikt en dat hij van [verdachte 1] heeft gehoord over een jongen die op een kamp woonde. [verdachte 2] woont volgens zijn verklaring op een kamp. [verdachte 1] verklaart zelf ook dat hij de naam detox een keer heeft gebruikt en dat hij de chatpartner van [voornamen verdachte] is, terwijl hij tevens verklaart dat het zo kan zijn dat hij in die chat de naam detox gebruikt. En tenslotte worden op de computer van [verdachte 1] bestanden aangetroffen waarin de naam detox staat vermeld.

Vorenstaande in onderlinge samenhang beschouwd, leidt de rechtbank tot het oordeel dat [verdachte 1] aan het internetverkeer heeft deelgenomen onder de naam “detox” en [verdachte 2] onder de naam “oo”.
Feiten 1 en 3:
De vervaardiging van het toxbotvirus door [verdachte 1] blijkt uit hetgeen [verdachte 1] met [naam] bespreekt in de chat van 29 maart, waarin [verdachte 1] aangeeft dat hij op het door Symantec ontdekt virus detox had geplakt, terwijl hij in een chat op 19 juli zegt dat hij respect heeft, verwijzend naar hetgeen Symantec over het W32.detox virus had geschreven. Door [verdachte 1] worden blijkens de bevindingen van verbalisanten op grond van het internetverkeer en/of de chats bestanden gedownload (detox.exe op 11 juli en 9 augustus en tox.exe op 2 augustus) die bij onderzoek door verbalisanten een versie blijken te zijn van het toxbot virus. Tenslotte verklaart [getuige] dat hij een bot kent dat detox heet en dat [verdachte 1] hem had verteld dat hij dat geschreven had. [getuige] geeft een beschrijving van een functionaliteit van dat virus dat overeenstemt met functionaliteiten die ook voorkomen in de door verbalisanten onderzochte versies van het toxbot virus, zoals de aanwezigheid van keyloggers.

De werking en inhoud van het virus blijkt uit het onderzoek dat de verbalisanten hebben gedaan bij een aantal door hen aangetroffen versies van het virus (tox.exe op 28 juli, detox.exe op 9 augustus, de bestanden config.h en dETOX, welk laatste bestand onderdeel vormde van het bestand xCore.rar, al welke bestanden werden aangetroffen op de vaste schijf van [verdachte 1]) alsmede uit het onderzoek van Symantec naar het aangetroffen virus. Uit

dit onderzoek en uit de bevindingen van verbalisanten op basis van het internetverkeer en de verklaring van [verdachte 2] over het updaten van de besmette computers (bots), blijkt ook dat er in de loop der tijd diverse versies zijn ontwikkeld.

De werking van het virus is dat het toxbot virus misbruik maakt van een kwetsbaarheid (vulnerability) in het systeem van windows door middel van exploits. Het probeert zich te installeren als een service onder windows, zodra de computer wordt gestart, waarbij het zichzelf een onopvallende naam geeft. Vervolgens probeert het een verbinding op te zetten met een IRC server. Aan de hand van de commando's die het binnen krijgt via de IRC server, voert het bepaalde taken uit, zoals het scannen van andere computers op open poortjes en het vervolgens eventueel infecteren/aanvallen van die computers. Als zo'n scan succesvol is, probeert detox zichzelf naar het kwetsbare systeem toe te kopiëren. Het virus bevat tevens de mogelijkheid dat toetsaan-slagen worden vastgelegd wanneer de gebruiker van de geïnfecteerde computer zich op sites bevindt waarbij in het internet adres een van de in het virus vermelde woorden "bank", "login", "ebay" en "paypal" voorkomt.
Qua inhoud vermelden de onderzochte versies allen internet-adressen waarmee verbinding moest worden gezocht. Een aantal van die adressen komt in alle versies voor, zoals bijvoorbeeld het adres oxff.memzero.info. Verder worden in alle versies kanalen (van IRC servers) vermeld waarmee verbinding moet worden gemaakt, van welke kanalen er in ieder geval een aantal onder beheer stonden van verdachten. Daarnaast komen er de hiervoor genoemde woorden "bank" en dergelijke in voor.
De werking van het virus en enkele van de daarin voorkomende exploits en opdrachten, zijn onderzocht en blijken te functioneren dan wel is in het internetverkeer de werking gebleken.

Bij dit alles werd gebruik gemaakt van IRC servers, waarvan er blijkens het proces-verbaal diverse door verdachten ofwel geheel onder hun beheer waren gebracht dan wel waarop zij de beschikking hadden over alleen aan hen ter beschikking staande kanalen.

Op grond van vorenstaande oordeelt de rechtbank dat verdachten in deze zaak de beschikking hadden over een (door [verdachte 1] ontworpen) werkend virus dat de mogelijkheid bezit om de toegang te verwerven in computers en van daaruit weer andere computers binnen te dringen en de toegang te verwerven en dat verdachten de mogelijkheid hadden om dat virus via servers te verspreiden.

Dat met behulp van dit virus ook daadwerkelijk computers zijn besmet, blijkt uit de chats waarin over een botnet wordt gesproken, de verklaring van [verdachte 2] dat hij [verdachte 1] helpt bij het updaten van oude robots naar een undetected versie, de commando's die door verdachten worden gegeven om bestanden te downloaden en de bevindingen van verbalisanten dat er een groot aantal gebruikers met de server verbinding hebben en dat er nieuwe bots verbinding maken. Dat laatste zou niet gebeuren wanneer, zoals verdachten tijdens een eerdere behandeling hebben betoogd, er alleen sprake was een fictief aantal, in het IRC programma tevoren opgenomen aantal gebruikers van de server.

Bij de beoordeling van de bewezenverklaring van feit 1 heeft de rechtbank stil gestaan bij de vraag of in dit geval gesproken kan worden van het doorbreken van een beveiliging. Ofschoon verdedigd zou kunnen worden dat een besturingssysteem wordt gemaakt om daarvan alleen via de normale weg gebruik te maken en dat wanneer dat gebruik op een andere dan de door de makers beoogde wijze gebeurt, van doorbreken sprake is, moet dit onderdeel van art. 138a Sr toch zo worden uitgelegd dat daarvan alleen sprake is wanneer een zich op de computer bevindende beveiliging, bijvoorbeeld in de vorm van een wachtwoord of een firewall wordt

gebroken. Weliswaar kent het virus ook die mogelijkheid, maar niet is komen vast te staan dat daarvan gebruik is gemaakt. Hetgeen het virus blijkens hetgeen hiervoor is omschreven doet, levert een technische ingreep op met behulp van valse signalen.

Uit het proces-verbaal blijkt dat het botnet al bestond voor de ten laste gelegde periode. Dat betekent mitsdien dat er op 1 juni 2005, de eerste dag van die periode, reeds computers waren besmet, maar ook, zo moet worden aangenomen dat die computers weer andere computers hadden besmet. Daarmee stond de rechtbank voor de beantwoording van de vraag welke computer moet worden beschouwd als computer die is binnengedrongen door een technische ingreep en welke computer als computer waartoe men vervolgens de toegang heeft verworven.

In dit geval is geen sprake van een hacker die binnendringt in één geautomatiseerd werk teneinde van daaruit tot een aan dat werk verbonden of met dat werk in verbinding staand geautomatiseerd werk de toegang te verkrijgen.
In dit geval is sprake van computers/servers waarover [verdachte 1] en zijn medeverdachte al dan niet gedeeltelijk het beheer hadden en van waaruit computers werden besmet die vervolgens weer ander computers besmetten. Nu er sprake is van een door [verdachte 1] vervaardigd virus dat het in zich had dat het zich geheel zelfstandig verspreidde, terwijl verdachten via de servers ook het beheer over de besmette computers hielden en aan die computers opdrachten konden geven, kan elke geïnfecteerde computer niet alleen worden beschouwd als een
geautomatiseerd werk waarin door een technische ingreep wordt binnengedrongen, maar ook als een computer waartoe vanuit een reeds eerder geïnfec-teerde computer de toegang is verkregen. Dat zou aan het bewijs van de strafverzwarende omstandigheid in de weg staan indien na 1 juni 2005 geen nieuwe computers waren besmet. Dat is echter blijkens het proces-verbaal niet het geval. De besmetting is tot aan de ontmanteling doorgegaan. Op elk moment in de ten laste gelegde periode kan mitsdien een moment worden gevonden waarop sprake is van binnengedrongen geautomatiseerde werken van waaruit weer de toegang wordt verschaft tot andere geautomatiseerde werken.

Het bewijs dat gegevens werden vastgelegd als bedoeld in de laatste alinea van feit 3, blijkt uit de hiervoor beschreven in het virus ingebouwde mogelijkheid om middels keyloggers gegevens te vergaren, de op de server(s) en de vaste schijf van [verdachte 1] aangetroffen bestanden zoals “paypal.txt”, met daarin inlognamen en wachtwoorden van gebruikers en het ophalen van dergelijke bestanden door [verdachte 1].
Feit 2:
Antivirusbedrijven detecteren medio juli 2005 het bestaan van een trojan, de Wayphisher Trojan. Deze trojan leidt gebruikers van besmette computers op het moment dat zij gebruik willen maken van online bancaire diensten, om naar de site “banks.wayser.net” alwaar hen een fake website wordt voorgeschoteld en de door hen vervolgens ingetypte inloggegevens naar voorgeprogrammeerde emailadressen worden verzonden.

De rechtbank acht wettig en overtuigend bewezen dat verdachte tezamen met een derde deze trojan heeft gemaakt en in zijn botnetwerk heeft uitgezet. Verdachte heeft immers enige tijd voordat de trojan ontdekt werd, namelijk op 6, 8 en 9 juli 2005, bestanden verzonden aan een derde die zich Sox noemde. De inhoud van deze bestanden was op een aantal punten gelijk aan de inhoud van de bestanden die met de Wayphisher trojan worden aangeduid. Zo zat er in de bestanden dezelfde registratiecode, zijnde een unieke combinatie van 32 letters en cijfers en hadden zij dezelfde functionaliteit namelijk het omleiden van bezoekers van adressen van

financiële instellingen naar een andere site, zijnde “banks.wayser.net”.
De door verdachte verzonden bestanden waren bovendien kort voor verzending gecompileerd, hetgeen erop duidt dat het verdachte is geweest die de bestanden heeft gemaakt.
Voorts blijkt uit nader technisch onderzoek dat op de computer van verdachte de vermoedelijke bronbestanden van de trojan stonden, en dat de site “banks.wayser.net” was geregistreerd door de gebruiker van een emailadres waarop verdachte, blijkens het opgenomen tapverkeer, kon inloggen.

Naast dit technische onderzoek steunt de bewezenverklaring voorts op hetgeen verdachte in afgetapt internet- en telefoonverkeer meldt. Zo legt verdachte in een chatgesprek met [verdachte 2] op 12 juli 2005 de werking van de trojan uit en vertelt hij in een telefoongespr[getuige]met [getuige] op 27 juli 2005 dat er veel geld wordt uitgeloofd om er achter te komen wie verantwoordelijk is voor het Wayphisher virus en adviseert hij [getuige], als deze iets wil bijverdienen, dat hij hem op het adres van zijn ouders kan vinden.

Het verweer van de raadsman dat de trojan nooit enige werking in de praktijk heeft gehad, wordt verworpen.
Verbalisanten hebben geconstateerd dat verdachte op 11 juli 2005 het bestand “main.exe” (zijnde de trojan Wayphisher) naar een server heeft verzonden en dat hij de door het toxbotvirus besmette computers opdracht heeft gegeven dit bestand van de server te downloaden en te installeren.
De raadsman stelt dat uit de getapte gegevens blijkt dat daarbij niet het juiste commando is gegeven. In de door verbalisant [naam] gemaakte Analyse van de Detox broncode wordt immers, aldus de raadsman, aangegeven dat de op 11 juli 2005 gegeven commando’s niet voldoen aan het WebDownload commando zodat alleen de download en niet installatie van de trojan kan hebben plaatsgevonden.
De rechtbank acht dit verweer onvoldoende onderbouwd, gelet op het feit dat verbalisant [naam] heeft vastgesteld dat [verdachte 1] met de op 11 juli 2005 gegeven commando’s niet alleen de bots opdracht gaf tot downloaden doch ook tot het installeren van de trojan. Het verweer gaat er voorts, niet onderbouwd vanuit, dat de definities van de te geven commando’s van het toxbotvirus met versie xLegion/0x031, zijnde de versie die in oktober 2005 op de computer van verdachte is aangetroffen en die nader is onderzocht, gelijk zijn aan de definities van de commando’s die moesten worden gegeven op 11 juli 2005.

Dat de trojan Wayphisher daadwerkelijk computers heeft besmet, blijkt bovendien niet alleen uit voormeld technisch onderzoek doch vloeit tevens voort uit de navolgende feiten en omstandigheden:
a. antivirusbedrijven ontdekken kort na 11 juli 2005 het bestaan van de trojan;
b. computergebruikers rapporteren op internetfora problemen over de werking van hun systeem. Uit de door hen overgelegde lijsten (gegenereerd door het programma “Hijackthis”) bleek dat de unieke registratiecode van Wayphisher in hun computer te staan;
c. De FBI meldt dat de server van de universiteit van Arlington is besmet en de besmetting bevatte de unieke registratiecode en de omleiding naar de site “banks.wayser.net”;
d. Verdachte geeft in een chatgesprek met Sox, gevoerd op de dag nadat de trojan in het botnetwerk is uitgezet, aan dat hij “een hoop postbankgegevens” heeft geoogst;
e. Vastgesteld is dat een programma in deze pagina’s inloggegevens verzendt naar emailadressen en dat in de inbox van deze emailadressen zich inloggegevens bevinden; verdachte heeft ook op deze adressen ingelogd;

Het verweer van de verdediging bestaande uit de enkele stelling dat uit de testopstelling van

een door de verdediging aangezochte deskundige blijkt dat de bots niet in staat waren om enig downloadcommando uit te voeren, is, in het licht van vorenstaande en gelet op de deskundigheid van de verbalisanten, onvoldoende onderbouwd. Dit verweer wordt derhalve verworpen.

De raadsman betwist dat er enig te duchten gemeen gevaar voor verlening van diensten is geweest, nu niet vaststaat dat de in het dossier aangetroffen (inlog)gegevens en/of creditcardgegevens op echtheid zijn gecontroleerd en ook niet is komen vast te staan dat deze gegevens met behulp van de trojan zijn verkregen.
De rechtbank verwerpt dit verweer nu is vastgesteld wat de functionaliteit van de trojan was, dat de trojan in het botnetwerk is uitgezet en dat inloggegevens zijn onderschept. Het kan dan niet anders zijn dan dat de onderschepte gegevens echt waren. Dat de gegevens echt waren, blijkt voorts uit de bewezenverklaring van hetgeen aan verdachte onder feit 7 wordt verweten, namelijk het met behulp van deze gegevens oplichten van derden.
Het feit dat de trojan tot gevolg heeft dat bezoekers van online bancaire diensten daarvan geen betrouwbaar gebruik meer kunnen maken, maakt dat er sprake is van te duchten gemeen gevaar voor deze diensten.

De rechtbank acht derhalve wettig en overtuigend bewezen dat verdachte dit feit tezamen en in vereniging met een derde met nickname Sox heeft gepleegd. Zulks blijkt uit het feit dat verdachte voorafgaande aan het uitzetten van de trojan in het netwerk, de bestanden met de trojan aan Sox heeft verzonden en uit het tapverkeer tussen beiden van 12 juli 2005 waarin fake internetpagina's van financiële instellingen worden uitgewisseld en later aan de trojan worden toegevoegd.

Feit 6. Subsidiair:
De verdediging heeft ter terechtzitting verzocht om verdachte vrij te spreken van de onder 6 subsidiair ten laste gelegde pogingen tot afpersing in de aldaar genoemde periodes. De rechtbank acht echter de pogingen tot afpersing op 3 en 7 september 2005 wel bewezen.

De rechtbank overweegt daartoe het volgende:
Uit het dossier blijkt dat verdachte [verdachte 1] installaties van de software van het bedrijf Mediatickets verzorgt en daarvoor (per installatie) recht heeft op betaling . Dit volgt onder andere uit de zich in het dossier bevindende e-mails tussen [verdachte 1] (derlord@g-mail.com) en een persoon met het e-mail adres Pepperjack@mediatickets.net.

[verdachte 1] heeft zich tweemaal schuldig gemaakt aan een poging tot afpersing van Mediatickets, de eerste maal in de periode van 1 tot en met 5 september 2005 en de tweede maal, tezamen en in vereniging met [verdachte 2], in de periode 6 tot en met 7 september 2005.

Bedreiging met een Ddos aanval op 3 september
In het getapte e-mail verkeer van [verdachte 1] is op 3 september 2005 zichtbaar dat Mediatickets zich bij [verdachte 1] had beklaagd over het snelle verwijderen van hun software, hetgeen voor haar aanleiding vormde om [verdachte 1] niet te betalen. [verdachte 1] heeft daarop gedreigd de server van Mediatickets offline te laten gaan, hetgeen betekent dat de internetsite van Mediatickets niet meer bereikbaar is. Dit zou dan worden hersteld zodra betaling (van $ 2100,--) alsnog zou plaatsvinden.
Uit het getapte internetverkeer betreffende een chat tussen [verdachte 1] en [verdachte 2] blijkt dat laatstgenoemde op 2 september 2005 bij [verdachte 1] informeert of hij al een mail

gestuurd heeft voor zijn geld. Voorts valt uit dit chatgesprek af te leiden dat het gesprek betrekking heeft op een (mogelijke) Ddos aanval die zou stoppen als er maar betaald werd.

Hoewel er op basis van bovenstaande en andere, zich in het dossier bevindende informatie mogelijk al sprake zou kunnen zijn geweest van een of meer uitgevoerde Ddos aanvallen rond de periode van 3 september 2005, acht de rechtbank dat, bij gebreke van meer concrete informatie waaruit kan blijken dat die aanval(len) werkelijk hebben plaatsgevonden, niet wettig en overtuigend bewezen. Wel acht de rechtbank op basis van de hiervoor weergegeven feiten en omstandigheden, in onderlinge samenhang bezien, wettig en overtuigend bewezen dat [verdachte 1] op 3 september Mediatickets met een Ddos aanval heeft bedreigd.

Ddos aanval 7 september
In een chat op 7 september omstreeks 23.00 uur praten [verdachte 1] en [verdachte 2] weer over Mediatickets. Omdat Mediatickets nog steeds niet heeft betaald, besluiten [verdachte 1] en [verdachte 2] een Ddos aanval uit te voeren. Op diens verzoek geeft [verdachte 1] het adres van de downloadserver van Mediatickets aan [verdachte 2] die vervolgens enkele commando's in de chat plakt. Uit deze commando's blijkt dat er een Ddos aanval op Mediatickets.net en MT-download.com gaat worden uitgevoerd.

In het dossier bevindt zich tevens informatie afkomstig van Microsoft waaruit blijkt dat "oo" (al eerder geïdentificeerd als [verdachte 2]) Ddos commando's geeft aan het botnetwerk. Volgens het op ambtseed opgemaakte proces verbaal van verbalisant [naam] vergaarde Microsoft informatie over botnets met het zgn. BMAT programma (Botnet Monitoring Analysis Tool). Microsoft analyseert hiermee malware en botnets. Zo kunnen bijvoorbeeld commando's die een botnetwerk-beheerder geeft aan het botnet worden gevolgd en vastgelegd. Uit deze informatie bleek dat aan een botnet dat gebruik maakte van de server 0x80.online-secured.com (al eerder geïdentificeerd als een van de servers van het botnet van [verdachte 1] en [verdachte 2]) commando's werden gegeven door 'oo'. Het gaat hierbij inhoudelijk om dezelfde commando's die door [verdachte 2] in de hiervoor genoemde chat werden geplakt.

In het (vervolg) van de chat van 7 september vindt nog de volgende conversatie plaats:
Omstreeks 23:15 uur zegt [verdachte 1] "weer down" en antwoordt [verdachte 2] "hmmm ja vaag is wel een dikke lijn"
Omstreeks 23:18 uur zegt [verdachte 2] "hmm hij lag wel" "maar niet down volgens mij"; [verdachte 1]: "hiero issie down"

In het dossier zijn geen gegevens aangetroffen waaruit blijkt dat er door Mediatickets betaald is.

Op basis van de hiervoor weergegeven feiten en omstandigheden, in onderlinge samenhang bezien, acht de rechtbank wettig en overtuigend bewezen dat verdachte [verdachte 1] tezamen en in vereniging met medeverdachte [verdachte 2] op 7 september 2005 een Ddos aanval hebben uitgevoerd op Mediatickets en daardoor dit bedrijf hebben trachten af te persen. In de tenlastelegging is deze strafbare gedraging tweemaal omschreven, eenmaal met behulp van een omschrijving van de wijze waarop een Ddos aanval wordt uitgevoerd en eenmaal middels dede vermelding dat er één of meerdere Ddos aanvallen zijn gedaan. Nu de rechtbank de, in de tenlastelegging als eerste genoemde wijze bewezen acht en er geen bewijs is dat er meerdere Ddos aanvallen hebben plaatsgevonden, zal de rechtbank de andere omschrijving

niet bewezen achten.

Met betrekking tot feit 6 primair en subsidiair heeft de raadsman van [verdachte 1] aangevoerd dat bij zijn cliënt het oogmerk van wederrechtelijke bevoordeling ontbrak nu [verdachte 1] recht meende te hebben op het geld. Dit oogmerk kan volgens de raadsman ook niet worden afgeleid uit het feit dat [verdachte 1] moet hebben beseft dat hij door zijn handelwijze de grenzen van de maatschappelijke betamelijkheid verre zou overschrijden; er zou slechts sprake zijn van een puberale actie van cliënt. De rechtbank verwerpt dit verweer. Een Ddos aanval heeft tot gevolg dat (de website van) een internetbedrijf gedurende langere of kortere tijd niet meer benaderd kan worden en mogelijk ook dat het bedrijf zelf in zijn communicatiemogelijkheden wordt beperkt. Het is van openbare orde dat bedrijven hierdoor grote schade kunnen lijden. Door het dreigen met, laat staan het uitvoeren van zo'n aanval, worden naar de mening van de rechtbank de grenzen van het maatschappelijk betamelijke wel degelijk in grove mate overschreden, terwijl verdachte dit ook heeft beseft. Dit besef blijkt onder andere uit de hierboven genoemde e-mail van [verdachte 1] aan Mediatickets waarin hij aangeeft dat het bedrijf door het down gaan van de download server schade zal lijden.

Feit 7 primair:
Gelet op de hiervoor omschreven partiële nietigverklaring van de dagvaarding en de vrijspraakoverweging wordt in het navolgende ingegaan op de verwijten omschreven onder handel 2 tot en met 7.

De rechtbank heeft reeds vastgesteld dat verdachte de Wayphisher trojan (mede) heeft gemaakt en in het toxbotnetwerk heeft uitgezet. Zowel in het toxbotvirus als in de trojan zaten functionaliteiten om inloggegevens van banken en van Ebay accounts te onderscheppen. Voorts is vastgesteld dat verdachte herhaaldelijk inlogde op (voorgeprogrammeerde) emailadressen alwaar in de inbox berichten stonden met daarin de onderschepte inloggegevens. Op de computer van verdachte zijn 324 Paypal accounts met bijbehorende wachtwoorden aangetroffen. Tot slot bevat het dossier verklaringen van [getuige], [getuige], [getuige] en [getuige] waarin (ieder op bepaalde onderdelen) wordt aangegeven dat verdachte onder een andere naam spullen kocht met gestolen creditcards en deze op zijn eigen of een ander adres liet afleveren.

De rechtbank acht wettig en overtuigend bewezen dat verdachte feitelijk gebruik heeft gemaakt van de onderschepte inloggegevens om daarmee onder een valse naam en met behulp van een Ebay account van een derde goederen te kopen en ten behoeve van de betaling van deze goederen gebruik te maken van vervalste bankfaciliteiten van derden.
Niet van belang is of de verkopende derden al dan niet betaald zijn. Immers, voldoende aannemelijk is dat zij niet tot afgifte van hun goederen zouden zijn overgegaan indien zij hadden geweten dat verdachte gebruik maakte van valse of vervalste gegevens.

Verdachte heeft de onderhavige strafbare feiten tezamen en in vereniging met één of meerdere anderen gepleegd. Zo heeft hij de trojan, zijnde het programma waarmee de inloggegevens van derden werden verkregen, tezamen met "Sox" ontwikkeld en heeft hij met derden afspraken heeft gemaakt omtrent de verdere uitvoering van het plan om derden met behulp van de aldus verkregen inloggegevens op te lichten.
Op grond van het het hieronder weergegeven bewijs ten aanzien van de zaken "handel 2 tot en met "handel 7", acht de rechtbank wettig en overtuigend bewezen dat een derde, de verkoper van de hierna te noemen goederen, op de wijze zoals hiervoor beschreven, is bewogen tot afgifte daarvan.

Boxen/speakers (handel 2)
Verdachte heeft op of omstreeks 28 februari 2005 speakers gekocht van een Duitser, genaamd [slachtoffer], handelend onder de naam Groove Music. Verdachte deed zich in het emailverkeer met [slachtoffer] voor als [slach[slachtoffer].
Opvallend is dat "[slachtoffer]" (lees verdachte) ten tijde van de aankoop aangeeft enkel met behulp van zijn Paypalaccount te willen betalen, ook als dat betekende dat hem dan extra kosten in rekening werden gebracht. Voorts is vastgesteld dat verdachte toegang had tot het emailadres van [slachtoffer] en dat emailverkeer onder de naam [slachtoffer] ook is aangetroffen op een computer bij Orit die verdachte gebruikte.
[slachtoffer] heeft de verkochte speakers afgeleverd op het huisadres van verdachte. Dit wordt niet alleen door [slachtoffer] aangegeven; ook "[slachtoffer]" erkent in het emailverkeer de aflevering, terwijl de ontvangstbevestiging door verdachte is ondertekend.
De Prada schoenen (handel 3)
Verdachte heeft op of omstreeks 11 september 2005 Prada schoenen gekocht van een bedrijf uit Turijn, genaamd Droplet en zulks op naam van en met behulp van de Ebay account van [slachtoffer]. Uit de tapgegevens blijkt dat hij voormeld Ebay account heeft gewijzigd waarna hij op het gewijzigde emailadres een dag later een bericht van het Italiaanse bedrijf ontvangt inhoudende dat de schoenen zullen worden verzonden aan [opgegeven naam door verdachte], wonend op het adres van verdachte. Verdachte heeft de schoenen kort daarna ontvangen, zo blijkt uit het afgetapte telefoongesprek tussen hem en DHL alsmede uit de aflevergegevens waarop hetzelfde nummer is te zien als op de verzendbevestiging van het Italiaanse bedrijf.

2 PSP's en Ridge Racer (handel 4)
Verdachte heeft op of omstreeks 17 juli 2005 twee PSP's en games van een derde gekocht onder de naam [slachtoffer]. Deze naam, zo heeft verdachte telefonisch aan [getuige] gemeld, gebruikte hij overal voor. Hij maakte gebruik van het emailadres ediko26@yahoo.com.
De goederen zijn afgeleverd op het adres van [getuige], hetgeen bleek uit het SMS bericht van [getuige] aan verdachte van 29 juli 2005, inhoudende dat de twee PSP's en de twee games binnen zijn.

2 PSP's (handel 5)
Verdachte heeft voorts op dezelfde wijze als hiervoor omschreven (onder de naam [slachtoffer]) op of omstreeks 16 juli 2005 twee PSP's gekocht van iemand in het overzicht aangeduid als [verzonnen naam door verdachte]. Deze artikelen zijn, op verzoek van verdachte, afgeleverd op het adres van [getuige]. Dit leidt de rechtbank af uit de het gegeven dat de PTT op dit adres, korte tijd later, namelijk op 19 en 20 juli 2005, twee pakjes afgeleverd.

De videokaart (handel 6)
Verdachte heeft op of omstreeks 20 juli 2005 een videokaart Galaxy Geforce, gekocht van een derde. De videokaart is afgeleverd aan ene [verzonnen naam door verdachte], wonende op het adres van verdachte. Verdachte heeft in een afgetapte telefoongesprek, gevoerd op 30 juli 2005, aangegeven dat er een videokaart is geleverd. Dit wordt ook bevestigd door het feit dat de PTT een pakketje op die datum aan het adres van verdachte heeft geleverd.
Gelet op het tijdsverloop tussen de koop en aflevering, is aannemelijk dat het hier om dezelfde videokaart gaat.

De Sony camera Cybershot (handel 7)
Verdachte heeft op of omstreeks 12 juli 2005 een camera gekocht van een derde. Deze camera

diende te worden geleverd op het adres van [verzonnen naam door verdachte], wonende op het adres van [getuige]. Verdachte heeft, zo blijkt uit een afgetapt telefoongesprek van 16 juli 2005, deze Sony camera aangeboden aan [slachtoffer] en uiteindelijk verkocht aan diens broer.
9 De strafbaarheid van het bewezene.

Het ten laste van verdachte bewezen verklaarde levert de volgende misdrijven op:

1. Medeplegen van computervredebreuk, gepleegd door tussenkomst van een openbaar telecommunicatiewerk, terwijl hij vervolgens door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde, meermalen gepleegd.

2. Medeplegen van opzettelijk stoornis veroorzaken in enig geautomatiseerd werk voor opslag of verwerking van gegevens, terwijl daarvan gemeen gevaar voor de verlening van diensten te duchten is, meermalen gepleegd.

3. Medeplegen van opzettelijk stoornis veroorzaken in enig geautomatiseerd werk voor opslag of verwerking van gegevens, terwijl daarvan gemeen gevaar voor de verlening van diensten te duchten is, meermalen gepleegd.

6. subsidiair 1:
Poging tot afpersing
en
poging tot afpersing, terwijl het feit wordt gepleegd door twee of meer verenigde personen.

7. primair:
Medeplegen van oplichting, meermalen gepleegd.

9. Handelen in strijd met artikel 13, eerste lid, van de Wet wapens en munitie.

10 De strafbaarheid van verdachte.

Verdachte is strafbaar voor hetgeen te zijnen laste bewezen is verklaard, nu niet is gebleken van enige omstandigheid die zijn strafbaarheid zou opheffen.

11 De straffen en maatregelen.

11.1 De algemene overwegingen omtrent de straf.

Op grond van de aard van het bewezene alsmede op grond van de omstandigheden waaronder dit is gepleegd en de persoon van de verdachte, zoals een en ander uit het onderzoek ter terechtzitting is gebleken, is de rechtbank van oordeel dat aan verdachte de straf behoort te worden opgelegd, die zij hierna zal bepalen.
11.2 De bijzondere overwegingen omtrent de straf.

Tijdens het onderzoek ter terechtzitting heeft de officier van justitie gevorderd aan de verdachte voor het onder 1. tot en met 5., 6. subsidiair, 7. primair, 8. en 9.tenlastegelegde, met dien verstande dat feit 8. alleen is gepleegd en niet tezamen en in vereniging) op te leggen een gevangenisstraf van 36 maanden met aftrek van voorarrest, waarvan 6 maanden

voorwaardelijk met een proeftijd van 2 jaar.

Verdachte heeft in talloze computers van derden ingebroken; ten tijde van de ontdekking van deze strafbare feiten, ging het om 50.000 tot 80.000 computers. Uiteindelijk blijkt bij de ontmanteling dat er miljoenen computers zijn besmet. Bij deze inbraken kreeg verdachte met behulp van door hem en of zijn mededader ontwikkeld virus of trojan, de beschikking over persoonlijke gegevens waarmee geld of andere zaken konden worden verworven en in een aantal gevallen ook daadwerkelijk werden verworven. Hoewel verdachte deze strafbare feiten binnenshuis, zittend achter zijn computer, kon plegen, en dus niet feitelijk in woningen of bedrijven behoefde in te breken, is de gemaakte inbreuk op rechten van derden niet minder groot. Het middels het internet verlopende betalingsverkeer, wordt op deze wijze volledig ondermijnd.

Het is aan het tijdig ingrijpen van politie en justitie te danken dat het in deze zaak aangetoonde feitelijke misbruik van de verkregen inloggegevens relatief beperkt is gebleven. Verdachte was immers al druk doende om het virus en de trojan verder te exploiteren, zulks met behulp van buitenlandse rekeningnummers en een buitenlandse opdrachtgever. Het is dan ook duidelijk dat deze zaak beslist geen spannend jongensboek is of een puberale actie van [verdachte 1], zoals de verdediging badinerend heeft gesteld. [verdachte 1] moet worden beschouwd als een intelligente jongeman die bewust misbruik maakt van zijn kennis op computergebied en die zich ook terdege er van bewust moet zijn geweest, gelet op hetgeen bewezen is, dat hij zich met criminaliteit op grote schaal bezig hield.
Daarnaast heeft verdachte, gebruikmakend van het botnet, zich schuldig gemaakt aan pogingen om Mediatickets af te persen door te dreigen met een dDOS aanval dan wel door een dDOS aanval uit te voeren. Met dergelijke acties wordt grote inbreuk gemaakt op het nog steeds toenemende economische belang van de informatie- en communicatietechnologie en het grote maatschappelijke belang van het internet en daarmee samenhangende toepassingen.

Verdachte heeft zich tenslotte schuldig gemaakt aan overtreding van de Wet Wapens en Munitie, hetgeen slechts marginaal in de strafmaat wordt meegenomen.
De rechtbank is van oordeel dat dit ernstige feiten zijn waarvoor in principe een gevangenisstraf van aanzienlijke duur moet worden opgelegd.

Verdachte is niet eerder met justitie in aanraking geweest.

Uit het rapport van de reclassering zijn geen bijzonderheden naar voren gekomen betreffende de persoon van verdachte en voorts blijkt daaruit dat interventie vanuit de reclassering niet nodig is.
De rechtbank acht de tijd die verdachte in voorarrest heeft doorgebracht onvoldoende om daarmee de ernst van de bewezen verklaarde feiten tot uitdrukking te brengen, zelfs indien daarbij wordt betrokken het gedeelte dat voorwaardelijk zal worden opgelegd. De rechtbank heeft er echter ook oog voor dat verdachte, na geruime tijd in voorarrest te hebben doorgebracht, inmiddels zijn leven weer heeft opgepakt en in februari aanstaande zijn opleiding zal hervatten. De rechtbank zal daarom een gevangenisstraf opleggen die, na aftrek van de tijd voor de vervroegde invrijheidstelling, ertoe leidt dat verdachte niet weer van zijn vrijheid zal worden beroofd, tenzij zich een geval als bedoeld in artikel 15a van het Wetboek van Strafrecht voordoet, hetgeen verdachte echter zelf in de hand heeft.
Nu verdachte deze kans geboden wordt en het, gelet op het bepaalde in art 9 lid 4 van het Wetboek van Strafrecht, in dit geval niet mogelijk is om hem naast gevangenisstraf een taakstraf op te leggen bestaande in een werkstraf, resteert de rechtbank onder deze

omstandigheden geen andere mogelijkheid dan hem tevens een geldboete op te leggen om de ernst van de feiten extra te benadrukken. Uit het proces-verbaal komt naar voren dat verdachte over voldoende middelen de beschikking moet hebben om deze boete te kunnen voldoen.
Bij het bepalen van het voorwaardelijk deel van de gevangenisstraf, speelt een belangrijke rol dat de rechtbank er bepaald niet gerust op is dat verdachte het verwerpelijke van zijn handelen inziet. Dat is voor de rechtbank reden om aan hem een lange voorwaardelijke straf op te leggen met de maximale proeftijd, opdat hij zo lang mogelijk ervan doordrongen blijft dat een nieuwe misstap op computergebied ernstige gevolgen voor hem kan hebben.

12 De overwegingen omtrent het beslag.

12.1 De overwegingen omtrent de verbeurdverklaring.

De in beslag genomen voorwerpen, op de aan dit vonnis gehechte beslaglijst genoemd onder de nummers 1. tot en met 4., 8. tot en met 10., 13., 15. tot en met 17., 19 en 20., zijn vatbaar voor verbeurdverklaring.

Gebleken is dat dit voorwerpen zijn met betrekking tot dan wel met behulp waarvan de bewezen verklaarde feiten 1. tot en met 3., 6. subsidiair en 7. primair zijn begaan dan wel die door middel van die strafbare feiten zijn verkregen.

12.2 De overwegingen omtrent de onttrekking aan het verkeer.

De in beslag genomen voorwerp, op de aan dit vonnis gehechte beslaglijst genoemd onder nummer11., zijnde het wapen en de balletjes, zijn vatbaar voor onttrekking aan het verkeer.

Gebleken is dat het onder 9. bewezen verklaarde feit is begaan met betrekking tot die voorwerpen.

Voorts zijn die voorwerpen van zodanige aard dat het ongecontroleerde bezit daarvan in strijd is met de wet en het algemeen belang.

12.3 De overwegingen omtrent de teruggave van in beslag genomen goederen.

De rechtbank zal de teruggave gelasten van de in beslag genomen voorwerpen, op de aan dit vonnis gehechte beslaglijst genoemd onder de nummers 5. tot en met 7., 11., zijnde de judomedaille, 14. en 18., aan verdachte, aangezien die voorwerpen niet vatbaar zijn voor verbeurdverklaring of onttrekking aan het verkeer en deze onder verdachte in beslag zijn genomen..
13 De toepasselijke wetsartikelen.

De beslissing berust op de artikelen 10 (oud), 14a (oud), 14b (oud), 14c, 23 (oud), 24, 24c, 27, 33, 33a, 36b, 36c, 45 (oud), 47, 57, 91, 138a (oud),161sexies (oud), 317 en 326 (oud) van het Wetboek van Strafrecht en de artikelen 13, 55 (oud), 56 en 60 van de Wet Wapens en Munitie.
14 De beslissing.

RECHTDOENDE beslist de rechtbank als volgt.

Zij verklaart de dagvaarding nietig voor zover deze betrekking heeft op het hierboven onder 3 genoemde gedeelte dat onder 7. primair is ten laste gelegd en zij verklaart de dagvaarding voor het overige deel geldig.

Zij verklaart niet bewezen hetgeen de verdachte onder 4., 5.,6. primair en 8. is ten laste gelegd en spreekt hem daarvan vrij.

Zij verklaart het ten laste gelegde bewezen, zodanig als hierboven onder 7.2 is omschreven.

Zij verklaart niet bewezen hetgeen verdachte onder 1. tot en met 3., 6. subsidiair, 7. primair en 9. meer of anders is ten laste gelegd en spreekt hem daarvan vrij.

Zij verstaat dat het aldus bewezen verklaarde oplevert de onder 9. vermelde strafbare feiten.

Zij verklaart de verdachte deswege strafbaar.

Zij veroordeelt verdachte tot een gevangenisstraf voor de duur van 24 MAANDEN.

Zij beveelt dat van deze gevangenisstraf een gedeelte groot 8 MAANDEN niet zal worden ten uitvoer gelegd, tenzij de rechter later anders mocht gelasten op grond dat de verdachte zich voor het einde van een proeftijd, die hierbij wordt bepaald op drie jaar, aan een strafbaar feit heeft schuldig gemaakt.

Zij bepaalt dat de tijd door de verdachte voor de tenuitvoerlegging van deze uitspraak in verzekering en in voorlopige hechtenis doorgebracht in mindering zal worden gebracht bij de uitvoering van het onvoorwaardelijke gedeelte van de opgelegde gevangenisstraf.

Zij veroordeelt verdachte tot betaling van een geldboete ten bedrage van € 9000,= (zegge: NEGENDUIZENDEURO), bij gebreke van betaling en verhaal te vervangen door hechtenis voor de duur van vier maanden.

Zij verklaart verbeurd de onder 12.1 genoemde voorwerpen.

Zij verklaart aan het verkeer onttrokken de onder 12.2 genoemde voorwerpen.

Zij gelast de teruggave aan verdachte van de onder 12.3 genoemde voorwerpen.

Dit vonnis is gewezen door mr. Kooijman, voorzitter, mr. Schoenmakers en mr. Wiemans, rechters, in tegenwoordigheid van de griffier Moonen-Scheepens en is uitgesproken ter openbare terechtzitting op 30 januari 2007.