LJN: BF0770, Gerechtshof 's-Hertogenbosch , 20-000628-07

Datum uitspraak:	12-09-2008
Datum publicatie:	15-09-2008
Rechtsgebied:	Straf
Soort procedure:	Hoger beroep
Inhoudsindicatie:	Computercriminaliteit. Verdachte wordt veroordeeld wegens het plegen van computervredebreuk middels het hacken van computers van derden via een door verdachte beheerd botnetwerk. Vrijspraak van ten laste gelegde opzettelijke vernieling/beschadiging van geautomatiseerde werken, nu niet is gebleken dat daarvan gemeen gevaar voor goederen te duchten is geweest.

Uitspraak

Parketnummer : 20-000628-07
Uitspraak : 12 september 2008
TEGENSPRAAK

Gerechtshof 's-Hertogenbosch
meervoudige kamer voor strafzaken

Arrest

gewezen op het hoger beroep, ingesteld tegen het vonnis van de rechtbank Breda van 30 januari 2007 in de strafzaak met parketnummer 02-981204-05 tegen:

[verdachte],
geboren te [geboorteplaats] op [1986],
wonende te [adres].

1. Hoger beroep

De verdachte en de officier van justitie hebben tegen voormeld vonnis hoger beroep ingesteld.

2. Omvang van het hoger beroep

Het hoger beroep is, blijkens het verhandelde ter terechtzitting in hoger beroep, niet gericht tegen:
- de vrijspraak van het onder 4 en 5 ten laste gelegde,
- het nietig verklaarde gedeelte van het onder 7 primair ten laste gelegde, alsmede
- de vrijspraak van het onder 7 primair ten laste gelegde voor zover het betreft het Alienware DAW Digital Audio Workstation (handel 1).

Al hetgeen hierna wordt overwogen en beslist heeft uitsluitend betrekking op dat gedeelte van het beroepen vonnis dat aan het oordeel van het hof is onderworpen.

3. Onderzoek van de zaak

Dit arrest is gewezen naar aanleiding van het onderzoek op de terechtzitting in hoger beroep, alsmede het onderzoek op de terechtzitting in eerste aanleg.

Het hof heeft kennisgenomen van de vordering van de advocaat-generaal en van hetgeen door en namens de verdachte naar voren is gebracht.

De advocaat-generaal heeft gevorderd dat het hof het beroepen vonnis zal vernietigen en te dien aanzien opnieuw rechtdoende de verdachte zal veroordelen ten aanzien van de feiten onder 1, 2, 3, 6 subsidiair, 7 primair, 8 en 9 tot een gevangenisstraf voor de duur van 24 maanden, waarvan 13 maanden en 5 dagen voorwaardelijk, met aftrek van het voorarrest, alsmede een geldboete van € 9.000,00, subsidiair 4 maanden hechtenis.

4. Vonnis waarvan beroep

Het beroepen vonnis – voorzover aan het oordeel van het hof onderworpen – zal worden vernietigd reeds omdat het hof, anders dan de rechtbank verdachte zal vrijspreken van de feiten 2, 3 en 8.

5. Tenlastelegging

Aan verdachte is - na wijziging van de tenlastelegging ter terechtzitting in eerste aanleg en voor zover thans nog van belang - ten laste gelegd 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 binnengedrongen, waarbij hij, verdachte en/of zijn medeverdachte(n) de beveiliging heeft/hebben doorbroken, in elk geval de toegang heeft/hebben 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 één van zijn mededader(s) gemaakt(e)/ontwikkeld(e)) (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/hebben verworven tot één of meer geautomatiseerde werk(en) van één of meer derde(n);

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/hebben 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 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 kre(e)g(en) over bancaire en/of andere gegeven(s) toebehorende aan één of meer van die gebruiker(s);
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 kre(e)g(en) over:
- financiële/bancaire gegevens van één of meer bank(en) en/of creditcardmaatschappij(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);

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) [slachtoffer] heeft/hebben gedwongen tot afgifte van één of meer geldbedrag(en) (namelijk $ 2.100,- en/of € 2.100,-), in elk geval van enig goed, geheel of ten dele toebehorende aan [slachtoffer], 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 [slachtoffer] 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 [slachtoffer] 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 sever(s) en/of de website van en/of in gebruik bij) [slachtoffer], teneinde die server(s) en/of website ontoegankelijk/onbereikbaar te maken voor derden;

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

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) [slachtoffer] 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 [slachtoffer], in elk geval aan een ander of anderen dan aan verdachte en/of zijn mededader(s),
hij en/of zijn mededader(s) heeft/hebben
- 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 deel uitmakend van een/zijn/hun botnetwerk, waardoor de (download)server(s) van en/of in gebruik bij [slachtoffer] offline zou(den) gaan en/of niet meer via het internet bereikbaar zou(den) 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 deel uitmakend van een/zijn/hun botnetwerk, waardoor de (download)server(s) van en/of in gebruik bij [slachtoffer] 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) [slachtoffer], teneinde die server(s) en/of website ontoegankelijk/onbereikbaar te maken voor derden,
terwijl de uitvoering van dat voorgenomen misdrijf niet is voltooid;

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 [naam] althans het bedrijf/de persoon gebruikmakend van het e-mailadres [naam].com en/of [naam] althans[naam]en/of[naam] heeft/hebben bewogen tot de afgifte van 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, immers heeft/hebben verdachte en/of (één van) zijn mededader(s) (telkens) met bovenomschreven oogmerk – zakelijk weergegeven – via het internet genoemd(e) goed(eren) 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) wederrechtelijk 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;

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/hebben 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 betalingsgegevens 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)/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)
- 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 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);

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 [naam], of in een deel daarvan, is binnengedrongen, waarbij hij, verdachte, en/of (één van zijn mededader(s) de beveiliging heeft/hebben doorbroken, in elk geval de toegang heeft/hebben 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 [naam]), die waren opgeslagen in dat geautomatiseerde werk waarin hij, verdachte, en/of (een van) zijn mededader(s) zich wederrechtelijk bevond(en), heeft/hebben overgenomen en voor zichzelf en/of (een) ander(en) heeft/hebben vastgelegd;
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;

In deze weergave van de tenlastelegging zijn de door de eerste rechter aangebrachte verbeteringen begrepen.

Voorzover in de tenlastelegging taal- en/of schrijffouten voorkomen, zijn deze verbeterd. De verdachte is daardoor niet geschaad in de verdediging.

6. Ontvankelijkheid van het openbaar ministerie

A1.
Van de zijde van verdachte is het verweer gevoerd dat het openbaar ministerie in zijn strafvervolging

niet-ontvankelijk behoort te worden verklaard, omdat er een ernstige schending van beginselen van een goede procesorde heeft plaatsgevonden.

A2.
Daartoe is aangevoerd dat door het openbaar ministerie niet, althans niet tijdig, is voldaan aan het bevel van het hof tot nader onderzoek aan de computers die te linken zijn aan de in het dossier genoemde tien IP-adressen. De late inzending van het aanvullend proces-verbaal op 28 augustus 2008 ‘s avonds aan de raadsman heeft ervoor gezorgd dat er voor hem onvoldoende tijd beschikbaar was om het nog met verdachte te bespreken. Het betreft een schending van de goede procesorde en die is van dien aard dat het openbaar ministerie niet-ontvankelijk verklaard dient te worden, aldus de verdediging.

A3.
Het hof overweegt hieromtrent het volgende.

Op 29 augustus 2008 is tijdens het onderzoek ter terechtzitting in hoger beroep door de raadsman van verdachte verklaard dat hij het betreffende aanvullend proces-verbaal op 28 augustus 2008 aan het einde van de dag heeft ontvangen en dat hij het toen ook heeft bestudeerd, maar dat hij het op dat tijdstip niet meer met zijn client heeft kunnen bespreken. Het hof heeft vervolgens tijdens die terechtzitting het onderzoek voor ruim een half uur onderbroken ten einde de raadsman gelegenheid te geven het betreffende proces-verbaal alsnog met verdachte te bespreken. De raadsman heeft desgevraagd ter terechtzitting verklaard dat dit voldoende was en dat met het onderzoek ter terechtzitting kon worden voortgegaan.
Het hof is van oordeel dat op basis van het vorenstaande niet kan worden geconcludeerd dat sprake is geweest van een schending van beginselen van een goede procesorde of dat doelbewust of met grove veronachtzaming van verdachtes belangen tekort is gedaan aan diens recht op een behoorlijke behandeling van de onderhavige strafzaak.

Het verweer wordt verworpen.

A4.
Nu ook overigens geen feiten of omstandigheden zijn aangevoerd of anderszins aannemelijk zijn geworden die zouden moeten leiden tot niet-ontvankelijkverklaring van het openbaar ministerie, is het openbaar ministerie ontvankelijk in de vervolging.

7. Vrijspraak

B1.
Het hof is van oordeel dat bij gebrek aan voldoende wettige bewijsmiddelen niet kan worden bewezen dat verdachte het onder 2, 3, 6 primair, en 8 ten laste gelegde heeft begaan, zodat hij daarvan wordt vrijgesproken.

Het hof overweegt hiertoe het volgende.

B2.
Ten aanzien van het onder 2 en 3 ten laste gelegde.

Op grond van het onderzoek ter terechtzitting in hoger beroep is het volgende gebleken.
Aan verdachte is onder 2 en 3 telkens ten laste gelegd het misdrijf als bedoeld in artikel 161sexies, aanhef en onder 2°, van het Wetboek van Strafrecht, zoals dit artikel luidde in de ten laste gelegde periode, en waarin is strafbaar gesteld:

“hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel

verijdelt, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is".

Bij de beoordeling van deze ten laste gelegde feiten is de juiste uitleg van de woorden "gemeen gevaar voor goederen of voor de verlening van diensten" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever.

De wetgever heeft artikel 161sexies een plaats gegeven in Titel VII van het Tweede Boek van het Wetboek van Strafrecht, waarin "Misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht" worden omschreven.
Voorts blijkt uit de Memorie van Toelichting dat deze bepaling ziet op gedragingen die gevaar veroorzaken voor personen of goederen, zonder dat deze gedragingen zich richten tegen bepaalde goederen of bepaalde personen (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 19).
Ook in de Memorie van Antwoord geeft de minister aan dat het voorgestelde artikel betrekking heeft op een dienst met "gegevensverwerking of telecommunicatie ten algemene nutte" (Tweede Kamer, vergaderjaar 1989-1990, 21551, nr. 6, pagina 36).
De wetgever heeft kennelijk de strafrechtelijke bescherming van geautomatiseerde werken die gemeen/ ten algemene nutte worden gebruikt, voor ogen gehad.

Het hof is van oordeel dat op grond van de wettige bewijsmiddelen niet is komen vast te staan dat als gevolg van de handelingen van verdachte gemeen gevaar voor goederen of voor de verlening van diensten te duchten is geweest. Het hof kan (slechts) vaststellen dat verdachte via de besmetting met een virus een storing heeft veroorzaakt in de computers van individuele gebruikers (zijnde de computers van de particulieren en/of de bedrijven welke deel uitmaakten van het botnetwerk van verdachte). Deze (rechts)personen waren daardoor (tijdelijk) niet in staat op een veilige wijze gebruik te maken van geautomatiseerde werken van bancaire instellingen of creditcardmaatschappijen.
Niet is komen vast te staan dat ook een storing is veroorzaakt in geautomatiseerde werken van de betreffende bancaire instellingen of creditcardmaatschappijen zelf, waardoor er een gemeen gevaar zou kunnen zijn ontstaan voor de verlening van diensten aan de vele (andere) gebruikers van deze geautomatiseerde werken.

Het hof is op grond van het vorenstaande van oordeel, dat het onder 2 en 3 ten laste gelegde niet kan worden bewezen verklaard.
B3.
Ten aanzien van het onder 6 primair ten laste gelegde.

Het hof is op grond van het onderzoek ter terechtzitting in hoger beroep van oordeel dat het onder 6 primair ten laste gelegde niet wettig bewezen kan worden, nu niet is komen vast te staan dat [slachtoffer] het in de tenlastelegging genoemde bedrag aan verdachte betaald heeft. Derhalve ontbreekt het wettig bewijs voor de "afgifte" van dat bedrag.

B4.
Ten aanzien van het onder 8 ten laste gelegde.

Op grond van het onderzoek ter terechtzitting in hoger beroep of op grond van de inhoud van wettige bewijsmiddelen kan het hof niet vaststellen/bewezen verklaren dat verdachte enige beveiliging heeft doorbroken, althans de toegang tot een gegevensbestand van [naam] heeft verworven door een technische ingreep, met behulp van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid, zodat niet bewezen kan worden dat verdachte wederrechtelijk is binnengedrongen in het geautomatiseerde werk (de/een server) van [naam].

8. Bewezenverklaring

Het hof acht wettig en overtuigend bewezen dat de verdachte het ten laste gelegde heeft begaan, met dien verstande dat:

1.
hij op tijdstippen in de periode van 1 juni 2005 tot en met 4 oktober 2005 te Loon op Zand, althans in Nederland, tezamen en in vereniging met een ander, telkens opzettelijk wederrechtelijk in een geautomatiseerd werk voor de opslag of verwerking van gegevens, te weten computers, is binnengedrongen, waarbij hij, verdachte en zijn medeverdachte de beveiliging hebben doorbroken, in elk geval de toegang hebben verworven door een technische ingreep, met behulp van valse signalen en/of door het aannemen van een valse hoedanigheid, namelijk telkens door, gebruikmakend van één of meer kwetsbaarheden in het besturingssysteem van Windows, een (al dan niet door verdachte gemaakte/ontwikkelde) versie van een virus, onder meer bekend onder de naam Toxbot, te (doen) verspreiden en/of te (doen) installeren waarna hij, verdachte en zijn mededader, door tussenkomst van het geautomatiseerde werk waarin zij zijn binnengedrongen de toegang hebben verworven tot geautomatiseerde werken van derden;

6 subsidiair
in de periode van 1 september 2005 tot en met 5 september 2005 en 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 een ander, met het oogmerk om zich wederrechtelijk te bevoordelen met bedreiging dat gegevens die door middel van een geautomatiseerd werk waren opgeslagen, ontoegankelijk zouden worden gemaakt, het bedrijf [slachtoffer] te dwingen tot de afgifte van een geldbedrag (namelijk ongeveer $ 2.100,-), toebehorende aan [slachtoffer],
hij en/of zijn mededader heeft/hebben
- gedreigd opdrachten te geven aan computers, deel uitmakend van een/zijn botnetwerk, waardoor de server van of in gebruik bij [slachtoffer] offline zou gaan en niet meer via het internet bereikbaar zou zijn, en
- opdrachten gegeven aan computers, deel uitmakend van een/zijn botnetwerk, waardoor de server van of in gebruik bij [slachtoffer] offline is gegaan en niet meer via het internet bereikbaar is geweest, terwijl de uitvoering van dat voorgenomen misdrijf niet is voltooid;
7.
hij op tijdstippen 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/of anderen wederrechtelijk te bevoordelen door het aannemen van een valse naam en een valse hoedanigheid, diverse deels onbekend gebleven personen en/of bedrijven, waaronder [naam] en [naam] heeft bewogen tot de afgifte van
geluidsboxen/speakers op of omstreeks 28 februari 2005 en
één paar Prada schoenen op of omstreeks 11 september 2005 en
PSP's/Playstations en Ridge Racer games op of omstreeks 29 juli 2005 en
PSP's/Playstations en Ipod op of omstreeks 20 juli 2005 en
een videokaart van het type/merk Galaxy Geforce op of omstreeks 20 juli 2005 en
één digitale fotocamera van het merk Sony op of omstreeks 12 juli 2005,
immers hebben verdachte en zijn mededader telkens met bovenomschreven oogmerk – zakelijk weergegeven – via het internet genoemde goederen besteld en hierbij gebruik gemaakt van
- valse namen en/of andere valse persoonsgegevens en
- vervalste Ebay-accounts en/of
- vervalste Paypal-accounts,
waardoor de bovengenoemde personen en/of bedrijven telkens werden bewogen tot bovengenoemde afgifte;

9.
hij 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.

Het hof acht niet bewezen hetgeen verdachte meer of anders is ten laste gelegd dan hierboven is

bewezen verklaard, zodat deze daarvan wordt vrijgesproken.

9. Door het hof gebruikte bewijsmiddelen

Indien tegen dit verkort arrest beroep in cassatie wordt ingesteld, worden de door het hof gebruikte bewijsmiddelen die redengevend zijn voor de bewezenverklaring opgenomen in een aanvulling op het verkort arrest. Deze aanvulling wordt dan aan het verkort arrest gehecht.

10. Bijzondere overwegingen omtrent het bewijs

C1.
De beslissing dat het bewezen verklaarde door de verdachte is begaan berust onder meer op de feiten en omstandigheden als vervat in de hierboven bedoelde bewijsmiddelen, in onderlinge samenhang beschouwd.

C2.
Elk bewijsmiddel wordt - ook in zijn onderdelen - slechts gebruikt tot bewijs van dat bewezen verklaarde feit, of die bewezen verklaarde feiten, waarop het, blijkens zijn inhoud, betrekking heeft.

Het hof overweegt in het bijzonder nog het volgende.

Ten aanzien van het onder 1 bewezen verklaarde

D1.
Zijdens verdachte is door de raadsman ter terechtzitting in hoger beroep bepleit dat verdachte wordt vrijgesproken van het onder 1 ten laste gelegde nu niet bewezen kan worden dat een (minimale) beveiliging is doorbroken dan wel dat een technische ingreep gepleegd is door verdachte en/of zijn medeverdachte, zoals, aldus de verdediging, vereist op grond van artikel 138a van het Wetboek van Strafrecht.

D2.
Het hof overweegt hiertoe het volgende.

Op grond van het verhandelde ter terechtzitting in hoger beroep stelt het hof onder meer het volgende vast.
(bijlage A000:)
a. Op 31 mei 2005 wordt door de Security Manager van het reken- en netwerkdiensten- centrum genaamd [naam] aangifte gedaan terzake computervredebreuk (bijlage 2 van bijlage A000).
b. [getuige 6] bleek een bestand met alle beheerderswachtwoorden van de computersystemen waarover [naam] het beheer heeft, te hebben ontvangen van verdachte (bijlage 3 van bijlage A000).
(bijlage A001:)
c. Verdachte (Het hof: zichzelf ook wel [verdachte] noemend) vertelt in een chatsessie van 25 mei 2005 met [getuige 6](het hof: zichzelf [naam] noemend) dat hij beschikt over een botnet.
d. Uit een chatsessie van 12 april 2005 met [naam] blijkt dat [verdachte] beschikt over de domeinnamen devtech.us, randomized.it, memzero.info, Isass.org, Isass.com, Isass.cc en devnologie.info.
e. Op de website van de antivirusmaatschappij Symantec staat een beschrijving van een bot met de naam W32.toxbot.b. In de beschrijving staat vermeld dat deze bot verbinding maakt met onder meer bovengenoemde domeinen (bijlage 9 van bijlage A001).
f. In een chatsessie van 29 maart 2005 met [naam] verwijst [verdachte] naar betreffende beschrijving van Symantec van W32.toxbot.b en zegt (onder meer): "stomme av's, 'toxbot', had er duidelijk '[naam]' op geplakt." (Het hof: zie in dit verband ook onder k).
g. [verdachte] verklaart in deze chatsessie verder dat hij sinds 2001 beschikt over bots, dat hij in de door hem gemaakte bot de toetsaanslagen op de binnengedrongen computers vastlegt en dat hij in

2003 heeft ontdekt hoeveel geld je ermee kunt verdienen.
h. Op basis van bovenstaande informatie werd een opsporingsonderzoek opgestart naar vermeende computervredebreuk.
(Proces-verbaal B1:)
i. Op grond van het onderzoek bleek verdachte samen met [medeverdachte]een botnetwerk te beheren. In het internetverkeer was zichtbaar dat verdachte een virus dat hij beheerde en mogelijk muteerde regelmatig verstuurde naar [medeverdachte] Zichtbaar was dat beiden commando's gaven aan het botnetwerk dat zij beheerden om nieuwe versies van het virus te verspreiden.
j. Tevens was zichtbaar dat de servers van het botnetwerk informatie gaven over de omvang van het botnetwerk. Zo was op 11 juli 2005 zichtbaar dat het botnetwerk uit meer dan 30.000 systemen bestond en op 8 augustus 2005 uit 50.095 systemen (bijlage 3 van proces-verbaal B1).
(Proces-verbaal B1.1:)
k. In een chat van 18 juli 2005 zegt verdachte dat hij eindelijk respect heeft en verwijst hij naar een website waarbij iemand refereert aan een virus met de naam [naam]32.[verdachte] en zegt hij dat de anderen het 'codbot' noemen en Symantec 'toxbot' (bijlage 1 van proces-verbaal B1.1).
l. In een testopstelling werd deze bot getest en werden de functionaliteiten beschreven. In een aanvullend proces-verbaal van 17 juli 2008 van verbalisanten [verbalisant 1] en [verbalisant 2] wordt een nadere omschrijving gegeven van de computers die zijn gebruikt in deze testopstelling (Het hof: zie hierna).
(Aanvullend proces-verbaal 17 juli 2008:)
m. In de testopstelling werden computers gebruikt die waren voorzien van het besturingssysteem Windows XP. Gebruikers van Windows XP kunnen er voor kiezen om dit systeem automatisch te laten voorzien van updates. Periodiek worden deze updates cumulatief aangeboden, zodat gebruikers ook in één keer alle updates kunnen installeren. Deze cumulatieve updates worden ook wel servicepacks genoemd. Ten tijde van het onderhavige onderzoek waren er reeds twee servicepacks, te weten Service Pack 1 (september 2002) en Service Pack 2 (augustus 2004). Het infecteren door de Toxbot blijkt te geschieden door het doorbreken van een beveiliging in Windows (XP) systemen die niet zijn voorzien van servicepack 2. Deze vorm van infectie is nagebootst in de testopstelling.
n. Door middel van deze infectiemethode kan het Toxbot virus een systeem binnendringen en zich daar nestelen als een programma. Om zich op deze manier als programma in een systeem als Windows te nestelen zijn 'administrator' of 'SYSTEM' rechten vereist op de betreffende computer.
o. Een standaard Windows XP installatie is beveiligd tegen het inloggen van buitenaf om daar vervolgens door middel van het gebruik van SYSTEM en/of administrator rechten programma's op te installeren.
(rapportage [verbalisant 1] 26 augustus 2008:)
p. Het Windows XP systeem is voorzien van talloze beveiligingen om onbevoegden van het systeem te weren. Het ontwikkelen van de updates en periodieke servicepacks is een reactie op de manieren die ontwikkeld zijn door hackers om deze beveiligingen te doorbreken of te omzeilen.
q. Uitgaande van het gegeven dat Windows XP standaard is voorzien van beveiliging is er voor gekozen om in de testopstelling gebruik te maken van XP systemen die niet zijn voorzien van updates of servicepacks. Temeer ook, omdat virussen als Toxbot zich juist richten op deze PC's.
r. In 2003 werden manieren ontdekt om via ingangen van hidden shares een beveiliging te doorbreken. Door middel van het opzettelijk geven van verkeerde signalen aan delen van het Windows besturingssysteem van PC's kan een systeem dusdanig in de war raken dat delen tijdelijk onbruikbaar raken of zelfs crashen. Dit is ook waargenomen bij de werking van het Toxbotvirus.
s. Om te voorkomen dat een (Toxbot)virus direct wordt gedetecteerd door een virusscanner wordt door hackers een techniek genaamd packing gebruikt. Deze techniek zorgt ervoor dat het virus wordt 'ingepakt' in een gecomprimeerd en versleuteld bestand, waardoor het ondetecteerbaar blijft voor virusscanners.
(Proces-verbaal B1.2:)
t. Op 2 augustus 2005 wordt via afgetapte internetdata bij verdachte waargenomen dat op 28 juli 2005 een update commando werd gegeven door [verdachte] aan het botnetwerk. Dit commando hield in dat de geïnfecteerde computers in het botnetwerk de opdracht krijgen om ergens op het internet een nieuwe bot, genaamd tox.exe te downloaden en starten.
u. Het bestand tox.exe is door verbalisant [verbalisant 1] uitgevoerd op een computer met het Windows besturingssysteem. Het programma tox.exe bleek een nieuw uitvoerbaar programma met de

naam mapi32.exe aan te maken. Het bestand bleek te zijn versleuteld en gecomprimeerd (ofwel gepackt) zoals in de rapportage van 26 augustus 2008 is omschreven, om herkenning door virusscanners te voorkomen.
v. Na het scannen van dit bestand met een antivirusprogramma werd de bot geïdentificeerd als de W32.Toxbot.

D3.
Bij de beoordeling van dit ten laste gelegde feit is de juiste uitleg van de woorden "wederrechtelijk binnendringen" van belang. Het hof heeft daartoe gezocht naar de bedoeling van de wetgever.

Van wederrechtelijk binnendringen in de zin van artikel 138a van het Wetboek van Strafrecht is sprake indien men zich de toegang verschaft tegen de onmiskenbare wil van de rechthebbende, welke zowel uit woorden als uit daden kan blijken.
Zoals uit de wetsgeschiedenis blijkt kan daarbij worden gedacht aan het plaatsen van een tekst op het beeldscherm dat toegang voor onbevoegden verboden is. Maar omdat deze woorden een per ongeluk tot stand gekomen toegang niet uitsluiten, bevat voornoemd artikel 138a onder meer ook het aanvullende vereiste dat sprake moet zijn van enige beveiliging, ofwel een kenbare drempel zodat onbevoegden zich niet simpelweg de toegang kunnen verschaffen. (Tweede Kamer, vergaderjaar 1991-1992, 21 551, nr. 11, pagina 18). Artikel 138a verlangt niet meer dan een minimale, doch wel daadwerkelijke beveiliging. Met andere woorden; indien het slachtoffer van computervredebreuk kan aantonen dat er sprake is van enige reële beveiliging dan is dat voldoende. (Tweede Kamer, vergaderjaar 1989-1990, 21 551, nr. 3, pagina 16).

D4.
Het hof leidt uit de vorenstaande onder D1. ad m. tot en met q. opgenomen feiten en omstandigheden af dat iedere versie van Windows XP, zodra een particulier die aankoopt, is uitgerust met (een standaard) beveiliging. Naar het oordeel van het hof is hierbij sprake van enige reële beveiliging zoals hiervoor onder D3. is beschreven. Met betrekking tot deze beveiliging acht het hof tevens de rapportage van verbalisant [verbalisant 1] van 26 augustus 2008 van belang, waar deze het volgende inhoudt:

"Als het gaat om een belangrijke beveiliging van XP in een netwerkomgeving als internet, is het volgende punt in dit verband het belangrijkste voorbeeld: Windows XP is een Windows variant uit de zogenaamde 'NT' familie, ontstaat uit Windows NT3.5 opgevolgd door Windows NT4.0, Windows 2000, Windows XP en Windows Vista. In de versies tot en met Windows 2000 was het in sommige gevallen mogelijk om deze via het netwerk te benaderen en er met gebruikmaking van Administratorrechten bestanden naar toe te sturen en zelfs uit te voeren. De genoemde methode maakte gebruik van de standaard door Windows aangemaakte verborgen shares als C$ en ADMIN$. Microsoft heeft deze optie van administrator toegang bij de introductie van XP bewust geblokkeerd en actief deze manier van niet-geautoriseerd gebruik beveiligd door deze toegang van buitenaf gebruik te laten maken van de geminimaliseerde rechten van het standaard aanwezige 'Guest' account. Een dergelijk Guest account heeft onvoldoende systeemrechten om die dingen te doen die door middel van het Toxbot virus wel worden gedaan. (……) Het blokkeren van de verborgen shares nam voor anderen de laatste mogelijkheid weg om via het netwerk administrator rechten te verkrijgen zonder actief een beveiliging te doorbreken. In 2003 werden manieren ontdekt om via de oude ingangen van de hidden shares toch toegang te verkrijgen.".

Voorts blijkt uit hetgeen onder D1. ad r. tot en met u. is opgenomen dat verdachte het virus zodanig versleutelde en comprimeerde (het zogenoemde packing), dat het betreffende systeem het virus niet als een fout herkende. Het virus verspreidde zichzelf vervolgens als een 'worm' middels de besmette computer naar andere computers.
Deze werkwijze houdt naar het oordeel van het hof niets anders in dan dat verdachte niet alleen gaten in systeembeveiliging opzocht ten einde als administrator/system en aldus onder een valse hoedanigheid in de zin van artikel 138a van het Wetboek van Strafrecht, binnen te dringen, maar zich daarbij tevens bediende van een technische ingreep met behulp van valse signalen, te weten door in

dit geval verhuld en onherkenbaar, middels het 'verpakte' virus binnen te dringen.
Gelet op de gehanteerde werkwijze, als hiervoor weergegeven is het hof van oordeel dat er sprake is van het doorbreken van de systeembeveiliging en van het verwerven van toegang middels een technische ingreep (tegen de onmiskenbare wil van de rechthebbende) als bedoeld in artikel 138a van het Wetboek van Strafrecht.

D5.
Gelet op het vorenstaande onder D4 overwogene waren ook de versies van vóór Windows XP (onder meer Windows NT 3.5, Windows NT 4.0 en Windows 2000) voorzien van een minimale (standaard) beveiliging. Het vorenstaande heeft derhalve ook te gelden voor zover is binnengedrongen in Windows systemen anders dan Windows XP.

Het hof verwerpt in zoverre het verweer.

Ten aanzien van het onder 6, subsidiair bewezen verklaarde

E1.
Zijdens verdachte is door de raadsman ter terechtzitting in hoger beroep bepleit dat verdachte dient te worden vrijgesproken van het onder 6, subsidiair ten laste gelegde, nu het oogmerk van wederrechtelijke bevoordeling ontbreekt en er (ook) geen sprake is van enig geweld of dreiging met geweld.

E2.
Het hof overweegt hieromtrent het volgende.

Op grond van het verhandelde ter terechtzitting stelt het hof (onder meer) de volgende feiten en omstandigheden vast.
(Proces-verbaal B2:)
a. Uit het onderzoek is gebleken dat verdachte en [medeverdachte] zich bezig hielden met het downloaden van advertentiesoftware.
b. Verdachte en zijn medeverdachte gaven opdrachten aan de computers van hun botnetwerk om software van het bedrijf [slachtoffer] te downloaden en incasseerden de commissie van [slachtoffer], terwijl de individuele gebruikers van de (botnet)computers geen opdracht hadden gegeven tot het downloaden van de betreffende software en terwijl [slachtoffer] in haar algemene voorwaarden uitdrukkelijk had opgenomen dat downloaden alleen plaats diende te vinden met toestemming van de gebruiker (proces-verbaal B1.5, bijlage 14).
(Proces-verbaal B2.1:)
c. In juli 2005 vindt er via de email een berichtenwisseling plaats tussen verdachte (alias [emailadres]) en het bedrijf [slachtoffer] middels het emailadres van [emailadres]. (bijlage 1 van proces-verbaal B2.1). [naam]' ziet dat verdachte veel installaties verricht en is bereid meer te betalen per installatie bij het toenemen van het aantal installaties.
d. Uit een berichtenwisseling op 1 september 2005 blijkt dat [slachtoffer] niet bereid is te betalen, omdat gebleken is dat van de computers die verdachte aanmeldde het programma van [slachtoffer] zeer snel weer werd verwijderd. Verdachte reageert op dezelfde dag hierop dat hij hoopt dat hij nog de 2100 krijgt omdat hij veel tijd en werk heeft gestoken in het promoten van de software van [slachtoffer] en dat, wanneer media [slachtoffer] toch niet zo betrouwbaar is, hij hoopt dat de server uit blijft omdat media [slachtoffer] dat verdient (bijlage 1, pagina 25 van proces-verbaal B2.1).
e. Tijdens een berichtenwisseling op 3 september 2005 schrijft verdachte aan [slachtoffer] dat hij denkt dat de vriendelijke manier niet werkt en dat hij niet weet hoeveel verlies [slachtoffer] zou hebben wanneer de downloadserver offline gaat. Verdachte zegt vervolgens dat hij zou helpen wanneer [slachtoffer] eerlijk is en betaalt wat ze hem schuldig zijn.
f. Uit chats tussen verdachte en [medeverdachte] op 5 en 7 september 2005 blijkt dat verdachte en [medeverdachte]bezig zijn de website van [slachtoffer] down te laten gaan. Zichtbaar is dat [medeverdachte] ddos-opdrachten geeft.
g. Uit informatie van Microsoft blijkt dat deze ddos-commando's op het botnetwerk zijn vastgelegd en verbalisant [verbalisant 3] ondervindt op 5 september 2005 ook feitelijk dat de website van

[slachtoffer] onbereikbaar is.

E3.
Het hof leidt uit het vorenstaande af dat verdachte in de periode van 1 september 2005 tot 7 september 2005 met [medeverdachte] heeft gepoogd [slachtoffer] af te persen zoals onder 6 subsidiair bewezen is verklaard.

Het hof verwerpt het onderdeel van het verweer inhoudende dat het oogmerk van wederrechtelijke bevoordeling ontbreekt, nu dit oogmerk naar het oordeel van het hof onmiskenbaar blijkt uit het feit dat verdachte, die buiten medeweten van de gebruikers om en in strijd met de algemene voorwaarden van [slachtoffer] software heeft gedownload (zie hiervoor onder E2 ad b.), van [slachtoffer] voor deze verleende dienst geld (ongeveer $ 2100,=) wilde hebben, en toen [slachtoffer] weigerde te betalen dreigementen heeft geuit die bij uitvoering ervan aanzienlijke schade zouden kunnen veroorzaken voor [slachtoffer].

De stelling van de raadsman dat geen sprake is van het plegen van geweld dan wel dreigen met geweld door verdachte behoeft geen bespreking nu het hof deze bestanddelen van de tenlastelegging niet bewezen acht.

Ten aanzien van het onder 7, primair bewezen verklaarde

F1.
Zijdens verdachte is door de raadsman ter terechtzitting in hoger beroep bepleit dat verdachte dient te worden vrijgesproken van het onder 7, primair ten laste gelegde, nu een bewezenverklaring van dit feit strandt bij gebrek aan overtuigend bewijs.

Het hof overweegt hieromtrent het volgende.

F2.
Op grond van het verhandelde ter terechtzitting in hoger beroep stelt het hof de volgende feiten en omstandigheden vast.
(Proces-verbaal B3:)
a. Verdachte heeft in een/zijn botnetwerk een of meer virussen uitgezet die functionaliteiten bevatten om inloggegevens van banken en van Ebay-accounts te onderscheppen. Het virus “trojan Wayphisher” heeft verdachte samen met een ander, bekend onder de naam ‘[naam] ontwikkeld.
(bijlage 02:)
b. Vanaf het getapte IP-adres van verdachte is te zien dat gekeken wordt in Ebay accountgegevens van slachtoffers van bovengenoemde virussen. Verdachte logt onder de naam ‘fatal_inc’ in op de betreffende accounts en verandert na het inloggen de adresgegevens van het account. Vervolgens komen er berichten binnen met daarop de gegevens van dergelijke slachtoffers.
c. Het gevolg is dat verdachte beschikt over het Ebay-account van derden en daarmee goederen bestelt via de website Ebay, gebruik makend van de opgebouwde betrouwbaarheid van de oorspronkelijke gebruiker van het account.
d. Zo bleek dat verdachte van één van de oorspronkelijke houders van een Ebay-account een bericht ontvangt waarin deze houder verdachte verzoekt om het account aan hem terug te geven.
e. De betalingen van de goederen vinden vervolgens plaats via op dezelfde wijze door verdachte gehackte Paypal-accounts met gebruikmaking van gestolen creditcardgegevens.
(processen-verbaal)
f. Vorenstaande werkwijze wordt bevestigd door de verklaringen van de getuigen [getuige 1], [getuige 2], [getuige 3], [getuige 4], [getuige 5] en [getuige 7]ten overstaan van de politie (dossier C) alsmede ter terechtzitting in hoger beroep d.d. 22 augustus 2008.
Handel 2 (geluidsboxen):
g. In een opgenomen en afgeluisterd gesprek van 13 augustus 2005 belt de heer [naam]naar de huislijn van de familie [verdachte] alwaar hij de vader van verdachte aan de telefoon krijgt. [naam] belt namens zijn vriend [naam] en het gesprek gaat over de levering door[naam]van twee boxen die via Ebay gekocht zijn en waarvan de betaling van € 640,00 niet is doorgekomen. Er volgen nog enkele

gesprekken en op 9 september 2005 wordt weer contact opgenomen met verdachte over de geleverde boxen van [naam] op het adres van verdachte.
h. De bestelling van de genoemde geluidsboxen is op naam van [naam] gedaan en op het adres van verdachte afgeleverd. Op de afleverbon van de Duitse post is met de naam [verdachte] ondertekend.
i. Uit onderzoek van de harddisk van de door verdachte gebruikte computer blijkt dat de betreffende speakers besteld zijn. De prijs bedraagt € 640,00 en de betaling is middels Paypal geschied. Het bedrijf waar gekocht is betreft [naam].
j. Uit het onderzoek blijkt verder dat er emailverkeer is tussen genoemde [naam] en het emailadres[emailadres]. Dit emailadres blijkt door verdachte (zelf) gebruikt te worden.
Handel 3 (Prada-schoenen):
k. In een opgenomen en afgeluisterd gesprek van 12 september 2005 wordt verdachte gebeld door getuige [getuige 3]. Verdachte vertelt [getuige 3] dat de schoenen morgen binnenkomen. In een ander gesprek later op die dag vertelt verdachte dat hij heeft gezien dat de schoenen vanuit Italië zijn verzonden.
l. Op 13 september 2005 belt verdachte naar de pakketten bezorgdienst DHL over een zending uit Italië met het [nummer].
m. Uit een IP-tap van het IP-adres in gebruik bij verdachte is te zien dat verdachte een mailbericht ontvangen heeft waarin de zending van de schoenen bevestigd wordt. Er wordt in het bericht over een zending met hetzelfde nummer als hiervoor onder l. genoemd gesproken. Als ontvanger staat [naam]met vermelding van het woonadres van verdachte.
n. Het emailadres dat verdachte gebruikt blijkt te zijn verkregen middels een gehackt Ebay-account op een wijze als hiervoor onder b. omschreven.
o. Uit een afleverlijst van DHL blijkt dat het bovengenoemde pakket met de schoenen op 14 september 2005 door DHL is afgeleverd en ontvangen door [naam].
Handel 4 (PSP's en games):
p. Op 29 juli 2005 verstuurt getuige [getuige 2] een SMS aan de telefoon van verdachte welke inhoudt dat twee PSP's en twee games binnen zijn.
q. Door [getuige 2] wordt vervolgens op diezelfde dag een SMS naar[getuige 8]gestuurd met het bericht dat twee PSP's en twee games (Ridge Racer) binnen zijn en of hij wil laten weten of hij ze koopt.
r. Vervolgens neemt [getuige 2] weer contact op met verdachte en vertelt hem dat de PSP's en games zijn verkocht.
s. Uit een lijst van TPG-post blijkt op 29 juli 2005 twee maal een pakket te zijn afgeleverd op het adres van verdachte.
t. Op 17 juli 2005 zijn deze spellen betaald door [naam] met vermelding van het woonadres van [getuige 2].
Handel 5 (PSP's/Playstations en I-pod):
u. Uit opgenomen en afgeluisterde telefoongesprekken tussen verdachte en [getuige 2] op 20 juli 2005 en 21 juli 2005 blijkt dat [getuige 2] verdachte belt over het binnen zijn van twee PSP's en een Ipod. [getuige 2] zegt dat er de naam [naam] op staat en verdachte zegt daarop dat hij die naam,[naam] overal gebruikt.
v. Verdachte zegt verder dat hij heeft gezien dat[getuige 2]heeft ondertekend met zijn eigen naam en dat dat niet slim is, omdat het onder een andere naam is verzonden. Verdachte zegt dat [getuige 2] het beste met de naam kan ondertekenen waaronder het verzonden wordt en dat hij die naam voortaan aan [getuige 2] zal doorgeven. Tot nu toe is alles verzonden onder de naam [naam], zegt verdachte.
w. Uit een bezorglijst van TPG-post blijkt dat op 19 juli 2005 en op 20 juli 2005 een pakket is afgeleverd aan het adres van [getuige 2].
x. Op 20 juli 2005 zegt [getuige 2] dat twee PSP's binnen zijn op naam van [naam]. Deze bestelling blijkt vervolgens uit een overzicht van Paypalbetalingen. Ook de bestelling van de Ipod blijkt uit dit overzicht. In de lijst met Paypalbetalingen is te zien dat de naam [naam] gebruikt is om goederen te ontvangen op zowel het adres van [getuige 2] als op het adres van verdachte.
Handel 6 (Videokaart Galaxy geforce):
y. Uit het hiervoor onder x. genoemd overzicht van Paypal blijkt dat op 20 juli 2005 is betaald voor een videokaart Galaxy Geforce met als ontvanger[naam] met vermelding van het adres van verdachte.
z. De betreffende videokaart is 10 dagen na de bestelling in het bezit van verdachte.

aa. Uit een overzicht van TPG-post blijkt dat er op 30 juli 2005 een pakket is afgeleverd aan het adres van verdachte.
Handel 7 (Sony camera):
bb. In een opgenomen en afgeluisterd gesprek tussen verdachte en [getuige 2] op 16 juli 2005 zegt verdachte dat hij een Sony Cybershot heeft staan.
cc. Verdachte heeft vervolgens een gesprek met [getuige 4] en vraagt of hij nog interesse heeft in een Sony camera voor een bedrag van € 180,=. [getuige 4] zegt dat zijn broertje hem wel wil hebben.
dd. Op het paypalbetalingsoverzicht is te zien dat deze camera is betaald door [naam] met vermelding van het woonadres van verdachte. Te zien is dat er een bedrag van € 339,90 voor is betaald.

F3.
In tegenstelling tot de raadsman acht het hof op grond van vorenstaande en de overige (in de aanvulling) gebezigde bewijsmiddelen wettig en overtuigend bewezen dat verdachte tezamen en in vereniging met één of meer anderen gebruik heeft gemaakt van onderschepte inloggegevens om daarmee onder een valse naam, 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 bankgegevens van derden (vervalste Paypal-accounts), zoals onder 7, primair, bewezen is verklaard. Daarbij is niet van belang of de goederen ook werkelijk betaald zijn.

Het verweer wordt verworpen.

11. Strafbaarheid van het bewezen verklaarde

G1.
Het bewezen verklaarde onder 1 is voorzien en strafbaar gesteld bij artikel 138a, eerste lid juncto artikel 47, eerste lid, aanhef en onder 1° juncto artikel 57 van het Wetboek van Strafrecht, zoals deze artikelen luidden ten tijde van het bewezen verklaarde.

G2.
De raadsman heeft namens verdachte ter terechtzitting in hoger beroep bepleit dat de opzettelijke en wederrechtelijke toegang tot een informatiesysteem alleen dan strafbaar is, indien het feit wordt gepleegd door een inbreuk op de beveiligingsmaatregelen. Indien het feit middels een technische ingreep wordt gepleegd is het, aldus de verdediging, niet strafbaar. Het vorenstaande zou voortvloeien uit het bepaalde in het (Europese) Kaderbesluit 2005/222 JBZ d.d. 25 februari 2005.

G3.
Het hof overweegt hieromtrent het volgende.

Het genoemde kaderbesluit bepaalt onder meer het volgende:

Artikel 2
1. Iedere lidstaat treft de nodige maatregelen om opzettelijke, onrechtmatige toegang tot een informatiesysteem of enig onderdeel daarvan strafbaar te stellen, althans voor gevallen die niet onbeduidend zijn.
2. Iedere lidstaat kan (onderstreping hof) beslissen dat de in lid 1 bedoelde gedragingen alleen strafbaar worden gesteld indien het feit wordt gepleegd door een inbreuk op de beveiligingsmaatregelen.
(…..)
Artikel 12

1. De lidstaten treffen de nodige maatregelen om uiterlijk op 16 maart 2007 aan de bepalingen van dit kaderbesluit te voldoen.
(……)

G4.

Het hof leidt uit het vorenstaande enkel af dat de lidstaten kunnen beslissen dat het plegen van computervredebreuk alleen strafbaar is, wanneer het feit wordt gepleegd door een inbreuk op de beveiliging. Dwingend en rechtstreeks werkend is dit voorschrift derhalve niet.
Ten overvloede overweegt het hof dat uit artikel 12 blijkt dat, al zou het bepaalde in artikel 2 wel dwingend en rechtstreeks werkend zijn geweest, dit voorschrift niet eerder dan op 16 maart 2007 ook feitelijk in de Nederlandse wetgeving behoefde te worden opgenomen.

Naar het oordeel van het hof faalt derhalve de stelling dat verdachte ten tijde van het plegen van het onder 1 bewezen verklaarde feit (in de periode 1 juni 2005 tot en met 4 oktober 2005) alleen strafbaar zou zijn indien sprake was van een technische ingreep.

Het hof verwerpt het verweer.

G5.
Het bewezen verklaarde onder 6 subsidiair is voorzien en strafbaar gesteld bij artikel 317, tweede lid, juncto artikel 312, tweede lid, aanhef en onder 2° en de artikelen 45 en 47 van het Wetboek van Strafrecht, zoals deze artikelen luidden ten tijde van het bewezen verklaarde.

G6.
Het bewezen verklaarde onder 7 primair is voorzien en strafbaar gesteld bij artikel 326, juncto artikel 57 van het Wetboek van Strafrecht, zoals deze artikelen luidden ten tijde van het bewezen verklaarde.

G7.
Het bewezen verklaarde onder 9 is voorzien bij artikel 13, eerste lid van de Wet wapens en munitie en strafbaar gesteld bij artikel 55, eerste lid van deze wet, zoals deze artikelen luidden ten tijde van het bewezen verklaarde..

Er zijn ook overigens geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van de feiten uitsluiten.

Het bewezenverklaarde wordt gekwalificeerd zoals hierna in de beslissing wordt vermeld.
12. Strafbaarheid van de verdachte

Er zijn geen feiten of omstandigheden aannemelijk geworden die de strafbaarheid van verdachte uitsluiten.

De verdachte is daarom strafbaar voor het hiervoor bewezen verklaarde.

13. Op te leggen straf

H1.
Bij de bepaling van de op te leggen straf is gelet op de aard en de ernst van hetgeen bewezen is verklaard, op de omstandigheden waaronder het bewezen verklaarde is begaan en op de persoon van de verdachte, zoals een en ander bij het onderzoek ter terechtzitting naar voren is gekomen.

Het hof overweegt in het bijzonder het volgende.

H2.
Verdachte heeft zijn informaticakennis gebruikt voor omvangrijke en wereldwijde criminele internetactiviteiten. Met dergelijke activiteiten wordt een grote inbreuk gemaakt op het nog steeds toenemende economische belang van de informatie- en communicatietechnologie en op het grote maatschappelijke belang van het internet en daarmee samenhangende toepassingen.
Voorts heeft verdachte zich schuldig gemaakt aan een poging tot afpersing en aan het samen met anderen oplichten van op internet als verkopende partij optredende (rechts)personen.
Verdachte heeft door zijn optreden daarmee tevens schade toegebracht aan het vertrouwen in het

handelsverkeer middels internet.

Het vorenstaande brengt mee dat naar het oordeel van het hof niet kan worden volstaan met een andere of lichtere sanctie dan een straf welke onvoorwaardelijke vrijheidsbeneming voor de hierna te vermelden duur met zich brengt.
Daarbij is rekening gehouden met de ernst van het bewezen verklaarde in de verhouding tot andere strafbare feiten, zoals onder meer tot uitdrukking komt in het hierop gestelde wettelijk strafmaximum.

Bij de straftoemeting heeft het hof tevens rekening gehouden met de omstandigheden dat de verdachte terzake strafbare feiten nog niet eerder is veroordeeld.

H3.
De raadsman van verdachte heeft – geheel subsidiair – aangevoerd dat de omstandigheden als hiervoor onder A1 en A2 genoemd, dienen te leiden tot strafvermindering. Het hof overweegt dienaangaande dat dit verweer op dezelfde gronden als hiervoor overwogen onder A3 wordt verworpen.

H4.
Met oplegging van een lange voorwaardelijke straf wordt enerzijds de ernst van het bewezen verklaarde tot uitdrukking gebracht en wordt anderzijds de strafoplegging dienstbaar gemaakt aan het voorkomen van nieuwe strafbare feiten.

13. Beslag

I1.
Het na te melden inbeslaggenomen en nog niet teruggegeven voorwerp, met betrekking tot hetwelk het onder 9 ten laste gelegde en bewezen verklaarde is begaan, dient te worden onttrokken aan het verkeer, aangezien het ongecontroleerde bezit daarvan in strijd is met de wet.

I2.
De andere na te melden inbeslaggenomen en nog niet teruggegeven voorwerpen, volgens opgave van verdachte aan hem toebehorend, zijn vatbaar voor verbeurdverklaring, nu het voorwerpen zijn met behulp waarvan het bewezen verklaarde onder 1, 6 en 7 is begaan of voorbereid.
Het hof heeft hierbij rekening gehouden met de draagkracht van verdachte.

I3.
Van hetgeen verder in beslag genomen en nog niet teruggegeven is, zal de teruggave aan de verdachte worden gelast.

14. Toepasselijke wettelijke voorschriften

De beslissing is gegrond op de artikelen 14a, 14b, 14c, 24, 33, 33a, 36b, 36c, 45, 47, 57, 138a 312, 317 en 326 van het Wetboek van Strafrecht en de artikelen 13 en 55 van de Wet wapens en munitie, zoals deze luidden ten tijde van het bewezen verklaarde.

BESLISSING

Het hof:

Vernietigt het vonnis waarvan beroep, voorzover aan het oordeel van het hof onderworpen, en doet in zoverre opnieuw recht.

Verklaart niet bewezen, dat verdachte het onder 2, 3, 6, primair, en onder 8 ten laste gelegde heeft

begaan en spreekt verdachte daarvan vrij.

Verklaart, zoals hiervoor overwogen, wettig en overtuigend bewezen, dat verdachte het onder 1, 6, subsidiair, 7, primair, en onder 9 ten laste gelegde heeft begaan.

Verklaart niet bewezen hetgeen verdachte meer of anders is ten laste gelegd dan hierboven is bewezen verklaard en spreekt verdachte daarvan vrij.

Verklaart dat het bewezen verklaarde oplevert:

1
Medeplegen van computervredebreuk meermalen gepleegd.

6 subsidiair
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.

Verklaart verdachte deswege strafbaar.

Veroordeelt verdachte tot een gevangenisstraf voor de duur van 730 (zevenhonderddertig) dagen.

Bepaalt, dat een gedeelte van de gevangenisstraf, groot 405 (vierhonderdvijf) dagen, niet zal worden tenuitvoergelegd, tenzij de rechter later anders mocht gelasten, op grond dat verdachte zich vóór het einde van een proeftijd van 2 (twee) jaren aan een strafbaar feit heeft schuldig gemaakt.

Bepaalt, dat de tijd, door verdachte vóór de tenuitvoerlegging van deze uitspraak in verzekering en voorlopige hechtenis doorgebracht, bij de tenuitvoerlegging van de opgelegde gevangenisstraf geheel in mindering zal worden gebracht.

Beveelt de onttrekking aan het verkeer van het inbeslaggenomen voorwerp, ten aanzien waarvan nog geen last tot teruggave is gegeven, te weten:
- een wapen, Gabilonda Y CIA SA-3-1-4-2 en twee doosjes gele balletjes.

Verklaart verbeurd de inbeslaggenomen voorwerpen, ten aanzien waarvan nog geen last tot teruggave is gegeven, te weten:
- 2 stuks computertoebehoren, 2 stuks SD kaarten in verpakking, SA-3-1-1-2, 2
- 1 harddisk, merk digitel WD 800, SA-3-1-1-1
- Muziekcomputer, I-river, SA-3-1-2-2
- Computertoebehoren, Pentium 4 processor, SA-3-1-1-3
- 1 plastic DS Doos met twee memorycards, SA-3-1-3-4
- 1 computer, merkloos, SA-3-1-3-7
- 1 computer, Target, SA-3-1-4-1
- 1 computer, Sony Laptop Vaio, pcg SA-3-1-1-3-8
- computertoebehoren, scan disk, memory card 1 gb
- computertoebehoren, adapter blue tooth in doos, SA-3-1-1-4
- Armband, kleur zilver, merk Bulgari, met vijf cirkelvormige schakels + cirkelvormige sluiting
- 1 muziekcomputer, merk Apple, I-pod, SA-3-1-5-1

Gelast de teruggave aan verdachte van de inbeslaggenomen voorwerpen, ten aanzien waarvan nog geen last tot teruggave is gegeven, te weten:
- Fototoestel, merk Casio, SA-3-1-3-1

- Mobiele telefoon plus lader, merk Nokia (pincode mogelijk 6996)
- Mobiele telefoon plus lader, merk Samsung, (pincode mogelijk 6996) SA-3-1-3-3
- judo medaille
- papier met notities, SA-3-1-2-5
- 3 kledingstukken, zijnde twee shirts plus 1 vest, SA-3-1-1-7 .

Aldus gewezen door
mr. H. Harmsen, voorzitter,
mr. N.J.L.M. Tuijn en mr. A. de Lange,
in tegenwoordigheid van mr. C.A. Blokx-van Roosmalen, griffier,
en op 12 september 2008 ter openbare terechtzitting uitgesproken.