Nieuwsbrief 1-2012

W.Bosgra ***Taakaccenthouder digitale criminaliteit***

U leest nu de eerste digitale nieuwsbrief verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer en kennis opdoen voor de opsporing van strafbare feiten gepleegd middels de computer. U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Deze nieuwsbrief zal met enige regelmaat in uw mailbox verschijnen.

Middels deze nieuwsbrief houden wij u op de hoogte van:

- onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- nieuws uit de media
- juridische vragen
- nieuwe technieken
- vele andere wetenswaardigheden

Computercriminaliteit

Onder computercriminaliteit verstaat men die vormen van criminaliteit die betrekking hebben op computersystemen of met computersystemen (inclusief netwerken) worden gepleegd. Computercriminaliteit wordt ook wel cybercriminaliteit of cybercrime genoemd. Cybercrime wordt ook omschreven als het gebruik van cyberspace voor criminele doeleinden. Dit is echter een te beperkte omschrijving.

Voorbeelden

Computervredebreuk: Het zich ongeoorloofd toegang verschaffen tot een computersysteem;

Het kopiëren van vertrouwelijke gegevens;

Ongeoorloofd computerdata verwijderen of aanpassen;

Ongeoorloofd computersystemen uitschakelen of onbruikbaar maken;

Het versturen van virussen;

Fraude met behulp van computers en valsheid in geschrifte met betrekking tot computerdata, bijvoorbeeld door berichten te onderscheppen en te veranderen zoals met een man-in-the-middle-aanval;

Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.

In de toekomst zal het openbaar ministerie zich richten op het beleid van cybercriminaliteit om er voor te zorgen dat er genoeg kennis beschikbaar is om deze vorm van criminaliteit aan te pakken.

Computercriminaliteit kent vele vormen. Vaak worden deze vormen aangeduid met de voorvoeging van het woord ‘cyber’ of met de letter ‘e-’, zoals bijvoorbeeld ‘cyberpesten’ of e-fraude.

Definitie van cybercrime

De term cybercrime komt uit het Amerikaanse recht als algemene aanduiding van misdrijven waarbij computers of netwerken gebruikt worden. Omdat steeds meer misdrijven via of met behulp van een computer gepleegd kunnen worden, begint cybercrime een beetje een modekreet te worden. Om een paar voorbeelden te noemen:

***Cyberpiracy (cyberpiraterij)*: opzettelijke en grootschalige inbreuk op auteursrechten door digitale verspreiding van werken.**

***Cybertrespass* (computervredebreuk): het binnendringen in een systeem of netwerk.**

***Cybervandalisme*: het verstoren of belemmeren van de werking van een systeem of netwerk, of het vernielen van gegevens die daarin opgeslagen of doorgegeven worden.**

***Cyberstalking*: het hinderlijk volgen of lastigvallen van een persoon via e-mail, Websites, SMS-berichten en dergelijke.**

***Cyberterrorisme*: het plegen van terroristische aanslagen op de werking van computers of netwerken.**

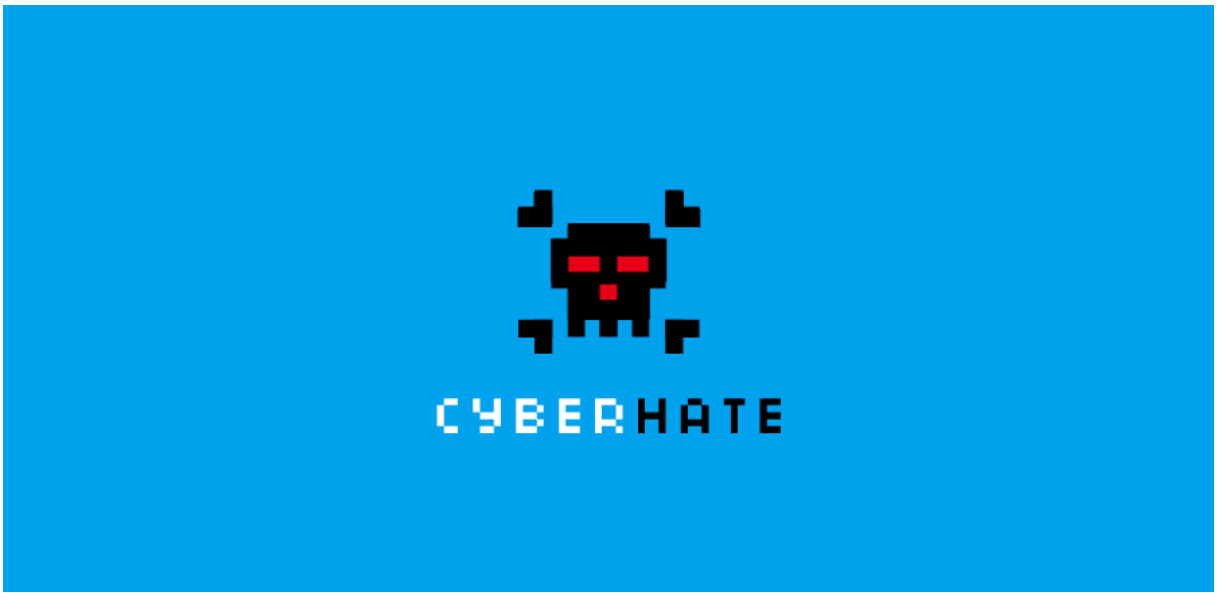
***Cyberdiefstal*: soms wordt hiermee gegevensdiefstal bedoeld, maar ook wel de "diefstal" van objecten in online spellen.**

***Cyberspionage*: het bespioneren van andermans computer of netwerk, of de gegevens die daarop opgeslagen of doorgegeven worden.**

***Cyberfraude*: fraude met behulp van de computer, bijvoorbeeld een bestelling doen bij een Webwinkel met een gestolen creditcard-nummer.**

***Cyberhate*: discriminatie en haatzaaien via Internet**

Bij veel van deze misdrijven is de computer of het netwerk niet meer dan een toevallig hulpmiddel. Iets kopen met een gestolen creditcard is net zo goed strafbaar wanneer het in een winkel gebeurt als wanneer het bij een online aankoop gebeurt.



DE STRAFBARE GEDRAGINGEN

Vernieling

Het opzettelijk vernielen, beschadigen of onbruikbaar maken van een computer- of communicatiesysteem is strafbaar met een jaar cel of boete van 16.750 euro (art. 161sexies lid 1). Iets vergelijkbaars geldt voor het vernielen van opgeslagen of verwerkte gegevens: dit kan zelfs twee jaar cel opleveren (art. 350a lid 1).

Vernieling of onbruikbaar maken van computers of gegevens komt relatief veel voor bij computercriminaliteit. Het kan gebeuren via computervredebreuk, maar dat hoeft niet. De motieven kunnen variëren van vandalisme tot sabotage. Gegevens of computers worden wel vaak vernield door een computerinbreker die zijn sporen wil uitwissen.

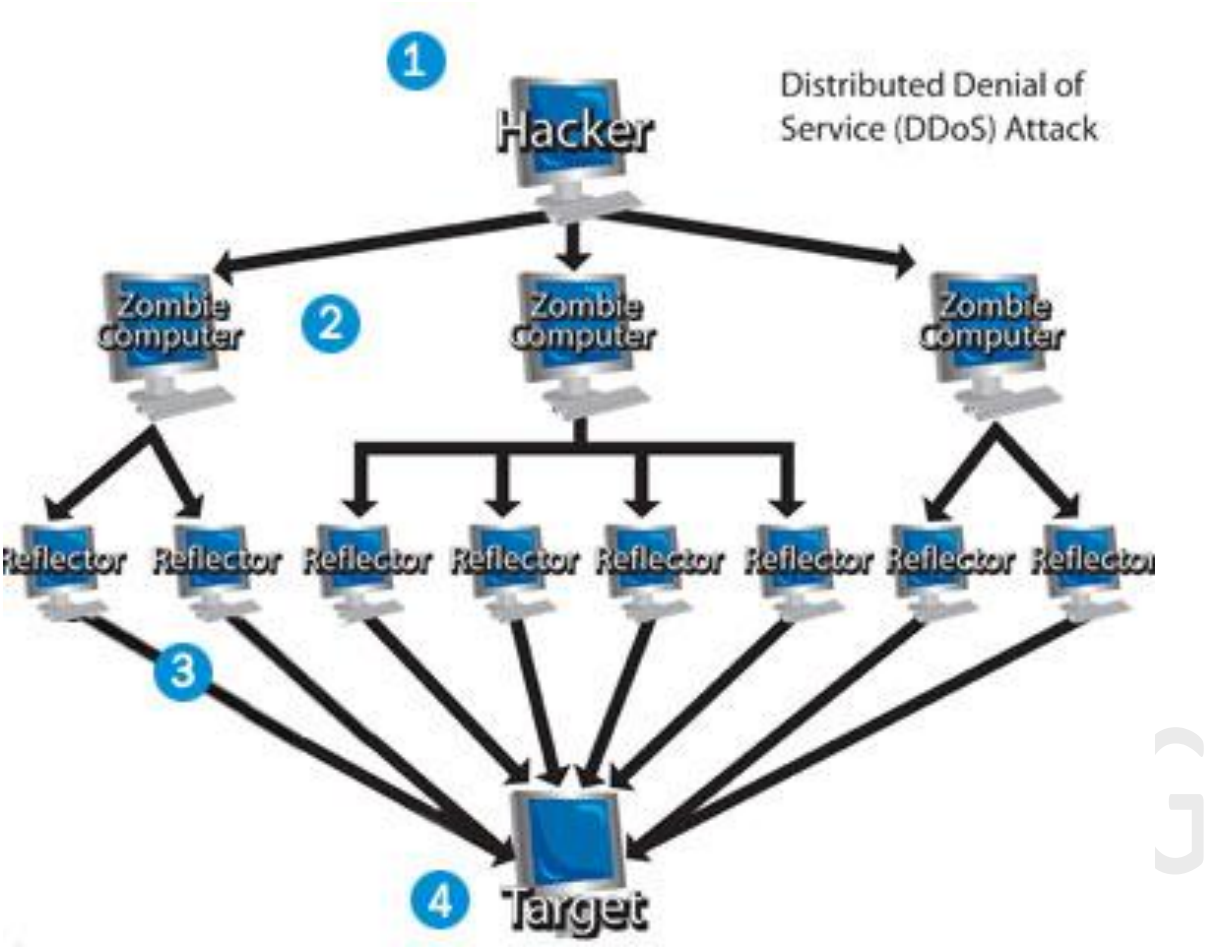
Wat is vernieling

Veroorzaken storing

Onder het vernielen van een computersysteem valt valt niet alleen het fysieke vernielen (bijvoorbeeld uit het raam gooien) daarvan. Ook het veroorzaken van een storing waardoor de werking van de computer (of het netwerk) wordt gehinderd is strafbaar. Zo plaatste een medewerker van de Universiteit van Twente bestanden op een netwerkschijf waardoor deze ontoegankelijk werd. Hij kreeg drie jaar cel (en TBS, vanwege eveneens gepleegde brandstichting).

Vernieling en verstikking

Denial of service - Verkeersopstopping op Internet



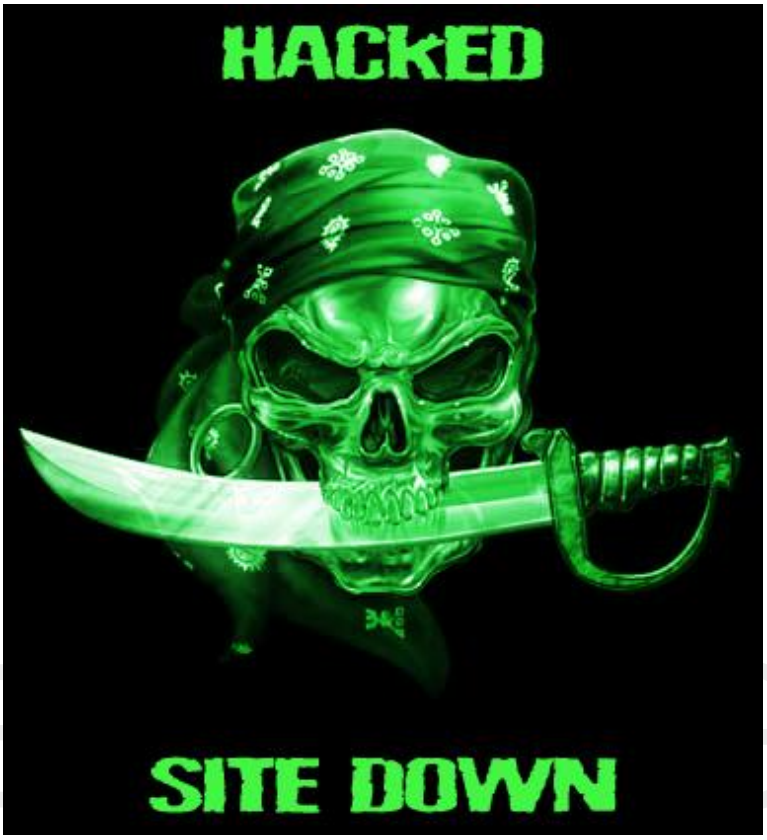
Een storing kan natuurlijk ook met software worden veroorzaakt. Er kan dan ook sprake zijn van een verstikkingsaanval. Zo werd in november 2005 het versturen van tienduizenden berichten als reactie op reclame-spam bestraft met een boete van 10.000 euro. Dit had onder de huidige wet ook als een verstikkingsaanval vervolgd kunnen worden. (Zie verder het aparte hoofdstuk wat volgt in Nieuwsbrief 2)

Toevoegen van gegevens

Onder vernielen van gegevens vallen: het veranderen, wissen of onbruikbaar of ontoegankelijk maken van gegevens. Maar ook het toevoegen van andere gegevens is een vorm van vernieling. Een voorbeeld van dit laatste is het inbreken op iemands Website en daar een pornografische foto aan toevoegen

Defacen van website

Het defacen van een site is een vorm van vandalisme die grofweg het elektronisch equivalent is van graffiti spuiten. De site wordt gehackt en de inhoud van de pagina's wordt aangepast of vervangen, meestal met beledigende of expliciete tekst en foto's. Defacen is een vorm van onbruikbaar maken of vernielen van gegevens en dus strafbaar (art. 350a lid 1)



Gijzelsoftware

Een heel bijzondere versie van vernieling is wat heet ransomware ("gijzelsoftware"). Dergelijke software wist geen gegevens maar versleutelt ze, zodat ze onbruikbaar zijn totdat de juiste sleutel wordt ingevoerd. De verspreider van deze software geeft de sleutel pas af nadat de eigenaar van de gegevens heeft betaald. De gegevens worden dus als het ware in gijzeling genomen tot het losgeld is betaald. Dit valt onder "ontoegankelijk maken van gegevens" en is daarom strafbaar (art. 350a lid 1).

Vernieling en computervredebreuk

Het vernielen van opgeslagen of verwerkte gegevens is ook een misdrijf (art. 350a lid 1). Wanneer dit gebeurt via computervredebreuk (binnendringen in een computersysteem), staat er zelfs vier jaar cel op (art. 350a lid 2).

Aftappen van gegegevens

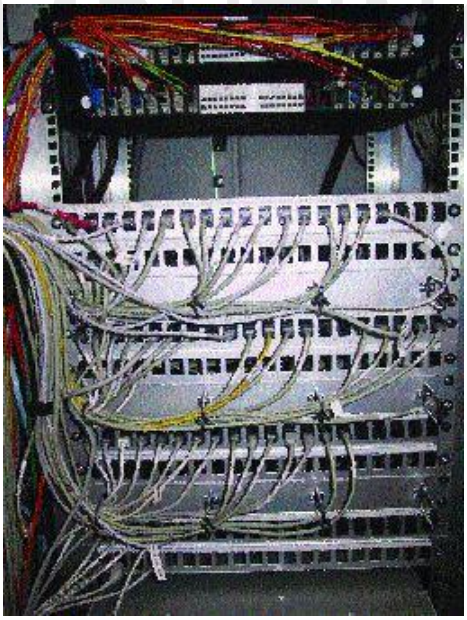
Aftappen van datacommunicatie

Het aftappen (sniffen) of opnemen van gegevens is vaak verrassend eenvoudig. Iedereen kan alle communicatie via draadloze netwerken ontvangen, en in veel gevallen zijn ook gewone, bedrade netwerken aftapbaar voor systemen die op dat netwerk zijn aangesloten.

Aftappen of opnemen

Met "aftappen" en "opnemen" wordt bedoeld het maken van een kopie van opgeslagen of langskomend dataverkeer. Hieronder vallen dus zowel 'live' gegevensstromen als opgeslagen gegevens, bijvoorbeeld in een cache bij een provider. Een kopie van een bestand in iemands cache maken is dus ook "aftappen".

Met technisch hulpmiddel



Aftappen of opnemen van datacommunicatie is strafbaar wanneer dit met een technisch hulpmiddel gebeurt. Dat kan bijvoorbeeld een programma zijn dat op de achtergrond draait en kopieën van alle verzonden e-mails maakt. Op veel netwerken kan elke computer in principe al het dataverkeer op dat netwerk aftappen.

Aftappen zonder technisch hulpmiddel is dus niet verboden. In een Internet-café over de schouder van de buurman meelezen met diens e-mail is niet strafbaar (maar wel onbeleefd). Een programma installeren dat stiekem diens e-mail naar jouw PC kopieert is daarentegen wel strafbaar.

Aftappen en computercriminaliteit

In veel gevallen kunnen gegevens pas worden afgetapt wanneer de "tapper" toegang heeft gekregen tot een computer of netwerk. Iemands mailbox kopiëren vereist toegang tot de

mailserver. Om MSN-gesprekken af te luisteren moet een programma draaien op de PC van het slachtoffer. Dit zijn vormen van computervredebreuk.

Het kopiëren van gegevens na het plegen van computervredebreuk wordt zwaarder bestraft dan "alleen maar" inbreken of "alleen maar" aftappen van gegevens. Op dit misdrijf staat maximaal vier jaar cel, of een boete van 16.750 euro (art. 139c lid 1).

Aftappen: diefstal van gegevens?

Aftappen van gegevens kan strafbaar zijn. Toch komt de term diefstal van gegevens nergens voor in de wet.

Dat aftappen of kopiëren van gegevens niet als "diefstal" wordt aangemerkt, heeft vooral een juridisch-technische reden: gegevens in een computerbestand worden niet gezien als "zaken" die kunnen worden weggenomen. Zonder wegnemen kan er geen sprake van diefstal zijn. Wat meestal gebeurt is dat de inbreker de gegevens kopieert naar zijn eigen systeem, en ze zo zelf kan gebruiken of aan derden kan doorgeven. De oorspronkelijke eigenaar heeft ze dan nog steeds. Het enige dat hij kwijt is, is de exclusieve toegang tot de gegevens.

Computergegevens zijn geen "zaken" in de zin van de wet, en kunnen dus niet worden gestolen. Dat blijkt uit een arrest van de Hoge Raad (december 1996, NJ 1997, 574). Enigzins opmerkelijk is dat wel: giraal geld is namelijk weer wel te stelen (HR 11 mei 1982, NJ 1982, 583), en al in 1921 werd diefstal van electriciteit mogelijk geacht.

In bijzondere gevallen kunnen gegevens weer wel als "steelbaar" gezien worden. In de context van spellen met virtuele werelden werd bijvoorbeeld het stelen van objecten uit Runescape of uit Habbo Hotel strafbaar geacht.

Uitzondering: vrije signalen

Het ontvangen van vrije signalen uit de ether is niet verboden, tenzij je een "bijzondere inspanning" moet leveren om de signalen te kunnen interpreteren.

De bovengenoemde strafbepaling over het aftappen of opnemen van datacommunicatie geldt niet altijd. Er is een uitzondering gemaakt voor het opvangen van door middel van een radio-ontvangapparaat ontvangen gegevens (art. 139c lid 2). Het ontvangen van vrije signalen uit de ether is immers een Europees grondrecht (art. 10 van het Europees Verdrag voor de Rechten van de Mens (PDF)).

Wordt "een bijzondere inspanning" geleverd, of een niet toegestane ontvanginrichting gebruikt, dan is er echter toch sprake van strafbaar afluisteren. Een bijzondere inspanning kan bijvoorbeeld zijn het afluisteren van de encryptie-sleutel of het zich voordoen als de werkelijke ontvanger (denk aan het spoofen of vervalsen van een MAC-adres).

Opnemen van gesprekken

Naast algemene regels over het aftappen van datacommunicatie kent de wet ook speciale regels over het aftappen, afluisteren of opnemen van gesprekken tussen mensen. Met een "gesprek" bedoelt de wet expliciet niet datacommunicatie; daarvoor is immers bovengenoemd artikel 139c al toegevoegd.

Het afluisteren en opnemen van gesprekken van anderen kan op vele manieren. Bekende voorbeelden zijn richtmicrofoons, verborgen dictafoons, keyloggers of het opvangen van elektromagnetische signalen van computerschermen uit de buurt. Om te bepalen of afluisteren of opnemen strafbaar is, richt de wet zich echter vooral op het karakter van het gesprek.

Opnemen van gesprekken in besloten omgeving

Iemand die geen deelnemer is aan een gesprek in een woning, besloten lokaal of erf, mag dit niet opnemen. Hierop staat zes maanden cel of een boete van 16.750 euro (art. 139a lid 1).

Het opnemen van gegevens die worden verwerkt of overgedragen per computer valt hier niet onder, tenzij er gebruik wordt gemaakt van een hulpmiddel zoals een keylogger of software op de computer in de woning in kwestie (art. 139a lid 2). Het inbreken op een mailserver om zo iemands e-mailconversaties te lezen, valt dus niet onder "opnemen van gesprekken". Het is wel computervredebreuk en aftappen van datacommunicatie.

Heimelijk opnemen van gesprekken

Gesprekken die buiten een woning worden gevoerd, mogen ook niet heimelijk worden opgenomen door een derde (art. 139b lid 1). Wie bijvoorbeeld stiekem in de bus een gesprek van twee andere passagiers opneemt, pleegt dus een strafbaar feit. Maar als het in alle openbaarheid gebeurt, is opnemen van gesprekken geen probleem. Een bedrijf mag dus gesprekken tussen klanten en medewerkers opnemen, wanneer dit bij het begin van het gesprek wordt vermeld.

Ook hier geldt dat het opnemen van gegevens die worden verwerkt of overgedragen per computer hier niet onder valt (art. 139b lid 2). Het gaat wederom om zaken als afluisteren van een gesprek met een parabolische richtmicrofoon of het stiekem installeren van een opname-apparaat bij de deelnemers.

Opnemen van eigen gesprekken

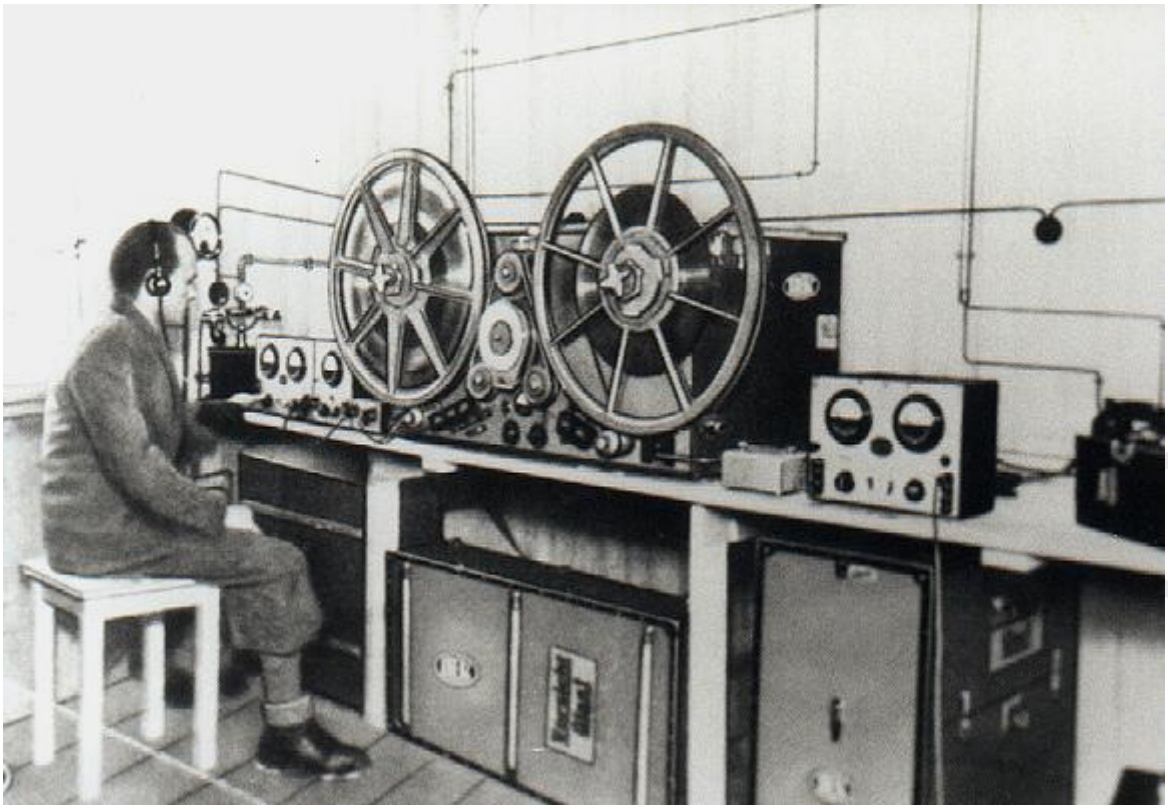
De deelnemers aan een gesprek mogen dus wel zelf hun gesprekken opnemen (ook wanneer ze dat niet met de andere partij besproken hebben). Ze mogen ook een ander dit laten opnemen. Dan is die ander uiteraard niet strafbaar.

Een telefoongesprek opnemen dat je zelf voert, mag je dus opnemen - ook wanneer je dat niet meldt aan de tegenpartij. Alleen het heimelijk opnemen van zo'n gesprek zonder deelnemer te zijn is dus strafbaar (tenzij je toestemming hebt van één van de deelnemers).

Zo'n opname mag niet zomaar gepubliceerd worden. De andere partij zal waarschijnlijk niet verwacht hebben dat het gesprek opgenomen werd. Er moet een goede reden zijn om diens privacy-belang opzij te zetten. Een voorbeeld is gebruik van de opname als bewijs van bedreiging.

Afluisterapparatuur

Naast het afluisteren of aftappen zelf stelt de wet ook het plaatsen en aanbieden van afluisterapparatuur strafbaar (art. 139d). Hieronder vallen ook computerprogramma's waarmee kan worden afgeluisterd, afgetapt of opgenomen. Dat wil niet zeggen dat elk programma waarmee netwerkverkeer kan worden opgenomen nu verboden is. Het apparaat of de software moet hoofdzakelijk geschikt of ontworpen zijn om heimelijk op te nemen.



Een Trojaans paard dat op de achtergrond draait en alle communicatie stiekem naar een server stuurt, is dus verboden. Een programma dat alleen het langskomend netwerkverkeer laat zien maar niet speciaal geschikt of bedoeld is voor heimelijk netwerkverkeer afluisteren, is niet verboden.

Plaatsen van afluisterapparatuur

Het plaatsen van afluister-, aftap- of opnameapparatuur met het doel om gesprekken, telecommunicatie, gegevensoverdracht of gegevensverwerking af te luisteren of op te nemen is een misdrijf (art. 139d lid 1). Hierop staat een jaar cel of een boete van 16.750 euro. Ook wanneer er nog niets afgeluisterd of getapt is.

Aanbieden van afluisterapparatuur

Wie een afluisterapparaat vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, loopt eveneens het risico op een celstraf van één jaar of een boete van 16.750 euro (art. 139d lid 2).

Heling van afgeluisterde gegevens

Naar analogie van heling, het doorgeven of doorverkopen van gestolen goederen, is ook het doorgeven of verkopen van illegaal afgeluisterde gegevens strafbaar gesteld (art. 139e). Het hebben van een voorwerp waarop wederrechtelijk verkregen gegevens zijn opgeslagen, dus bijvoorbeeld een bestand op een harde schijf, kan zes maanden cel opleveren. Ook op het doorgeven van zo'n voorwerp (of alleen de gegevens zelf) staat deze straf.

Volgens onderzoek van het NIPO uit 2002 heeft met name de financiële en zakelijke dienstverlening relatief veel last van computercriminaliteit. Bijna een kwart van de criminaliteit gaat om inbraak in of misbruik van gegevensbestanden.

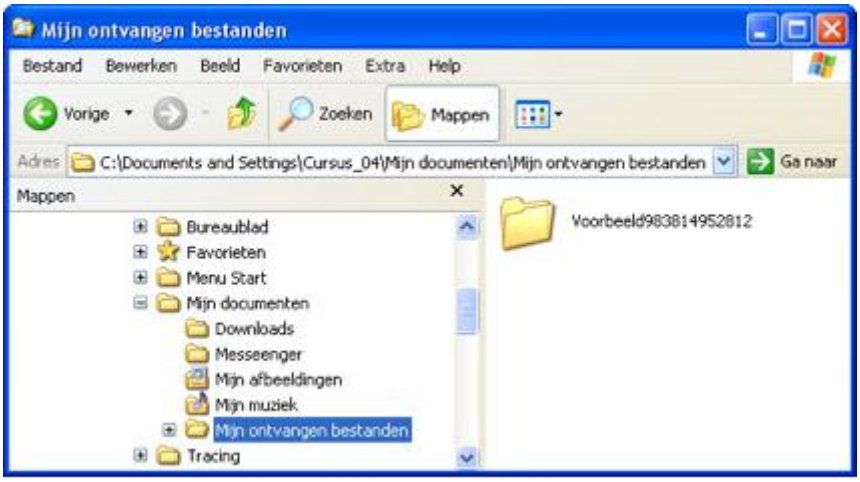
MSN Chat via Windows

In de nieuwere versies van MSN/Live Messenger kunnen alle chatgesprekken worden bijgehouden in logbestanden. Gevoerde gesprekken zijn dan te bekijken zonder in te loggen.

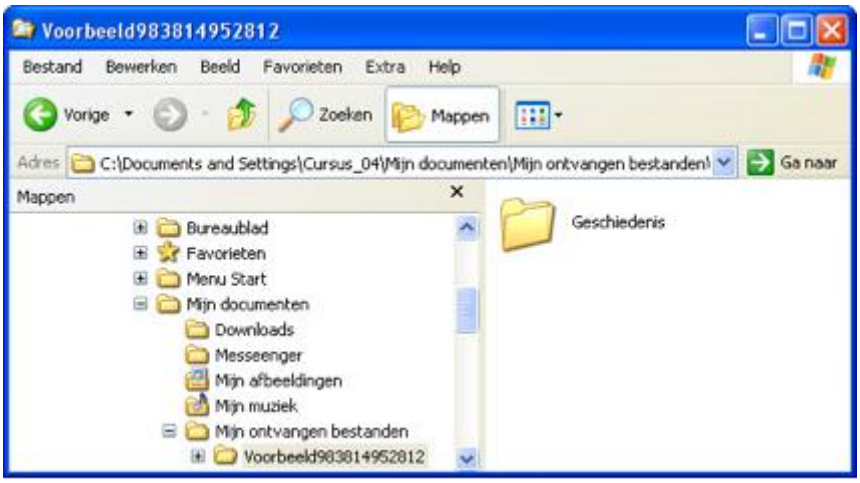
Om uw chatgesprekken zichtbaar te maken kunt u het volgende doen:

Windows
Start Windows Verkenner.
Ga naar de map C:\Documents and Settings. U ziet hier submappen voor alle gebruikersaccounts.

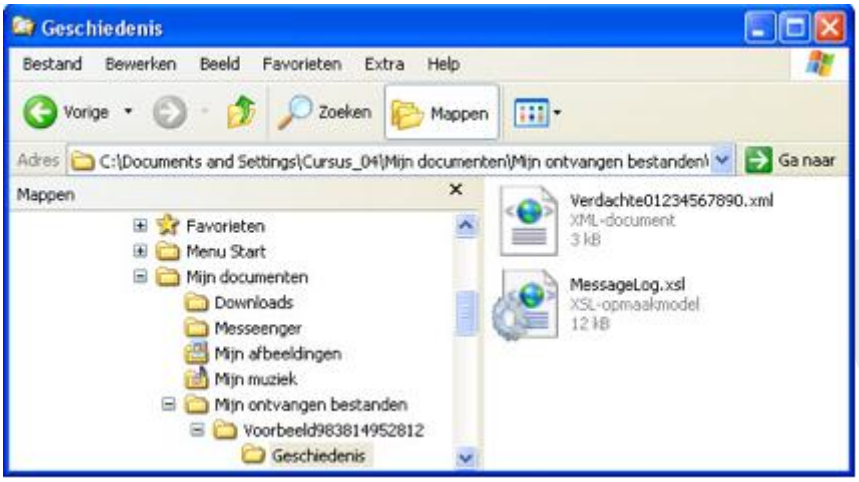
Open de map van de gewenste account en ga daarin naar Mijn documenten, Mijn ontvangen bestanden. U ziet vervolgens een map met de naam van de gebruiker van het MSN programma (het gebruikte e-mailaccount) en een getal. Open deze map.



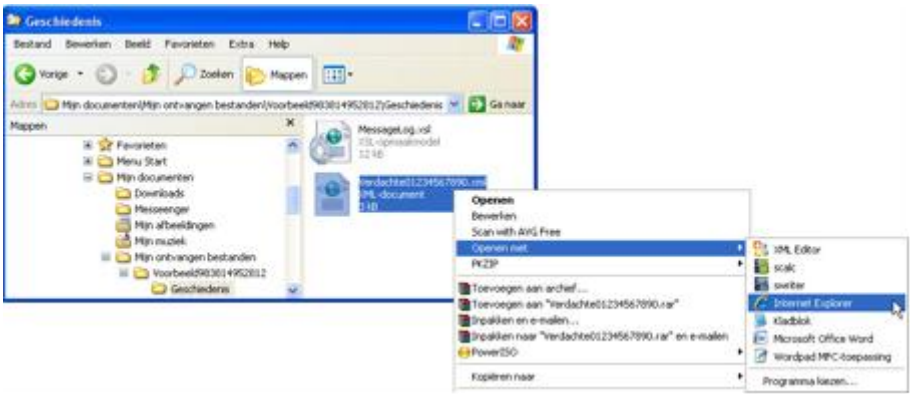
U ziet nu de submap Geschiedenis. Open deze map.



Klik met de rechtermuisknop op het logbestand waarin het e-mailadres / naam van de persoon die de belediging heeft geuit (het bestand wordt blauw).



Kies in het snelmenu “Openen met” en klik op het programma Internet Explorer. Wanneer het programma Internet Explorer niet getoond wordt in de lijst dan kunt u op 'Openen met' klikken en vervolgens het programma Internet Explorer aanklikken.



Alle bewaarde gesprekken met de persoon die de belediging heeft geuit worden nu getoond. Maak een afdruk van de gesprekken. U kunt eventueel ook het bewuste bestand op een cd-rom branden en toevoegen bij uw aangifte.

Bedenkt u wel dat de namen die u ziet misschien geen echte namen zijn, maar enkel de namen zoals die in Messenger zijn opgegeven. Hebt u in de bij Stap 3 en 4 vermelde mappen geen logbestanden gevonden dan staat de optie om de chatgesprekken te loggen uitgeschakeld. U kunt deze inschakelen door binnen het programma MSN/Live Messenger onder Extra – Opties – Berichten de regel “Gesprek automatisch in een bestand opslaan” aan te vinken en op “Toepassen” en “OK” te klikken.

E-mail headers zichtbaar maken

U kunt contact hebben gehad via e-mail. Een e-mailbericht kan gegevens bevatten die mogelijk de afzender kan traceren. Dit worden e-mailheaders genoemd. Deze gegevens zijn vergelijkbaar met het briefhoofd van een papieren brief. Hoe u deze headers zichtbaar kunt maken vindt u hieronder. Zoek uw e-mailprogramma op en voer de stappen uit die beschreven staan.

Gmail

- Log in op uw Gmail account
- Open het bewuste bericht
- Klik op de blauwe pijlpunt rechts naast de knop “Beantwoorden”
- Klik in het geopende menu op “Origineel weergeven”
- Selecteer alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Gmail (eenvoudige HTML weergave)

- Log in op uw Gmail account
- Open het bewuste bericht
- Klik op “Origineel weergeven”
- Selecteer in het geopende menu alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Hotmail / Windows Live

- Log in op uw Windows Live Hotmail account
- Klik met de rechtermuisknop op het bewuste bericht en kies “Berichtbron weergeven"
- Selecteer alle getoonde tekst (Ctrl + a) en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Mail (Apple)

- Start het programma Mail
- Selecteer het bewuste bericht.
- Selecteer binnen de tap “Weergave” de subtap “Bericht”
- Selecteer binnen subtap “Bericht” “Lange kopteksten”
- Of druk na het selecteren van het bericht op de toetsen cmd + u
- Selecteer (cmd + a) alle getoonde tekst in het tekstvenster en kopieer (cmd + c) dit.
- Plak (cmd + v) gekopieerde gegevens in het programma Teksteditor, Pages of Word.
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen.

Outlook

- Start het programma Outlook
- Selecteer het bewuste bericht.
- Klik met de rechtermuisknop op het bewuste bericht en kies “Opties"
- Ga met de cursor (pijltje) in de kolom staan achter “Internetheaders” en selecteer alle getoonde tekst (Ctrl + a) binnen deze kolom en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Outlook Express

- Start het programma Outlook Express
- Selecteer het bewuste bericht.
- Klik met de rechtermuisknop op het bewuste bericht en kies “Eigenschappen"
- Klik bovenin het geopende scherm op de tab “Details”
- Klik onderin in de tab “Details” op de knop “Bron van het bericht…”
- Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Thunderbird (Apple)

- Start het programma Thunderbird
- Selecteer het bewuste bericht.
- Selecteer binnen de tab “Beeld” de regel “Berichtbron”
- Of druk na het selecteren van het bericht op de toetsen cmd + u
- Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (cmd + a) in het tekstvenster en kopieer (cmd + c) dit.
- Plak (cmd + v) gekopieerde gegevens in het programma Teksteditor, Pages of Word.
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen.

Thunderbird (Windows)

- Start het programma Thunderbird
- Selecteer het bewuste bericht.
- Selecteer binnen de tab “Beeld” de regel “Berichtbron”
- Of druk na het selecteren van het bericht op de toetsen Ctrl + u
- Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Windows Live Mail (als programma geinstalleerd)

- Start het programma Windows Live Mail
- Selecteer het bewuste bericht.
- Klik met de rechtermuisknop op het bewuste bericht en kies “Eigenschappen"
- Klik bovenin het geopende scherm op de tab “Details”
- Klik onderin in de tab “Details” op de knop “Bron van het bericht…”
- Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Yahoo (Nieuwe lay-out)

- Log in op uw Yahoo account
- Selecteer het bewuste bericht
- Klik met de rechtermuisknop op het bewuste bericht en kies “View Full Headers"
- Ga met de cursor (pijltje) in het nieuw geopende venster staan en selecteer alle getoonde tekst (Ctrl + a) binnen dit venster en kopieer (Ctrl + c) dit
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Yahoo (Classic lay-out)

- Log in op uw Yahoo account
- Open het bewuste bericht
- Klik rechtsonder op de pagina, achter de meerkeuzelijst “Select `message Encoding” op “Full Headers"
- De regel met het onderwerp en afzender wordt nu vergroot en de headers van het bewuste bericht wordt zichtbaar in een lichtgekleurd kolom
- Selecteer alle tekst in deze kolom vanaf de eerste tot en met de laatste regel. Doe dit met je muis en houd daarbij de linkermuisknop ingedrukt zodat de tekst blauw gearceerd wordt.
- Wanneer de tekst blauw gearceerd is kopieer (Ctrl + c) deze
- Plak (Ctrl + v) gekopieerde gegevens in het programma Kladblok, Wordpad of Word
- Sla het bestand op of print dit bestand en neem dit mee wanneer u aangifte gaat doen

Belangrijk in de header is het X-originating IP

Hiermee is de provider en gebruiker te achterhalen.

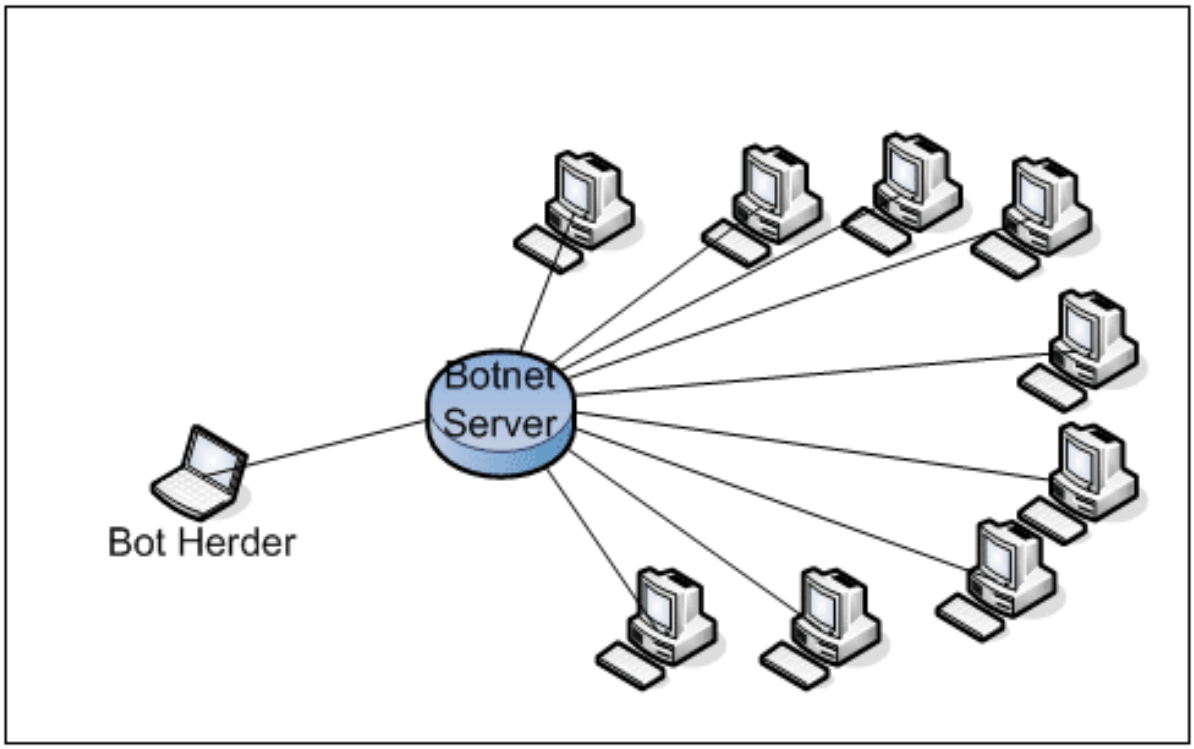
(zie volgende afbeelding)

Return-Path: <bogdan@fx.ro>
Received: from srv01.advenzia.com (root@localhost)
by emailaddressmanager.com (8.11.6/8.11.6) with ESMTP id i2OApwQ14083
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:58 GMT
X-ClientAddr: 193.231.208.29
Received: **from** corporate.fx.ro (corporate.fx.ro [193.231.208.29])
by srv01.advenzia.com (8.11.6/8.11.6) with ESMTP id i2OApvs14078
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 10:51:57 GMT
Received: from mail.fx.ro (mail3.fx.ro [193.231.208.3])
by corporate.fx.ro (8.12.11/8.12.7) with ESMTP id i2OAtxBr025924
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:59 +0200
Received: from localhost.localdomain (corporate2.fx.ro [193.231.208.28])
by mail.fx.ro (8.12.11/8.12.3) with ESMTP id i2OAtoQe006624
for <support@emailaddressmanager.com>; Wed, 24 Mar 2004 12:55:50 +0200
Date: Wed, 24 Mar 2004 12:55:50 +0200
Message-Id: <200403241055.i2OAtoQe006624@mail.fx.ro>
Content-Disposition: inline
Content-Transfer-Encoding: binary
MIME-Version: 1.0
To: support@emailaddressmanager.com
Subject: How to read email headers
From: bogdan@fx.ro
Reply-To: bogdan@fx.ro
Content-Type: text/plain; charset=us-ascii
X-Originating-Ip: [80.97.5.101]
X-Mailer: FX Webmail webmail.fx.ro
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
Status:

Botnet

Een botnet is een netwerk van een groot aantal computers die besmet zijn door een zogenaamde bot: een programma dat zelfstandig geautomatiseerd werk kan uitvoeren. Deze geïnfecteerde computers (zombies) staan bij mensen thuis of bij bedrijven, in bibliotheken, eigenlijk overal. De meeste gebruikers weten niet dat hun computer onderdeel is van een botnet. Ook uw computer kan op dit moment deel uitmaken van een botnet.

Vanuit één centraal punt kan een kwaadwillend persoon al deze computers opdrachten geven. De computers kunnen dan gebruikt worden voor het versturen van bijvoorbeeld spam of phishing e-mails, het manipuleren van online verkiezingen, het manipuleren van zoekresultaten in zoekmachines, voor het verzorgen van een enorme hoeveelheid verkeer naar een website zodat deze bezwijkt (een DDos-aanval). Wanneer u bijvoorbeeld een e-mailbericht wilt versturen of een website wilt bezoeken, zult u merken dat dit allemaal trager verloopt. Zodra een bot op uw computer is geïnstalleerd, zal deze vaak proberen uw anti-virusprogramma of uw firewall uit te schakelen.



De bot kan ook uw creditcard- of bankgegevens onderscheppen of een achterdeur openen op uw computer, zodat er ongemerkt toegang is tot uw persoonlijke informatie. Een bot-programma kan uw computer besmetten via een virus of via een beveiligingslek in uw browser of besturingssyteem. Wanneer een bot uw computer heeft besmet, kan uw computer gebruikt worden om de bot verder te verspreiden (bijvoorbeeld via e-mail).

U kunt door middel van een poortscan controleren of vreemden toegang hebben tot uw computer. U kunt gratis een poortscan doen op: ***www.ipscanner.nl***, ***www.ojvweb.nl***

Besmet? Klik hier voor de Kaspersky verwijder tool:

http://www.kaspersky.com/virusscanner

HACKING

Bij hacking denken we direct aan inbraak in een computer of computernetwerk. Ook het blokkeren van websites is een activiteit van hackers. De gevolgen van hacking kunnen ernstig zijn: misbruik van persoonlijke gegevens (bankrekeninginformatie, creditcardnummers), het wissen van gegevens op de harde schijf en het gebruik van uw computer voor ongewenste handelingen (opslaan van illegaal materiaal).

Iemand die hackt uit crimineel, ideologisch of vernielzuchtig oogpunt, noemen we ook wel een cracker. Soms huren bedrijven hackers in om de beveiliging van hun systemen te testen zodat veiligheidslekken kunnen worden gedicht. Een andere groep hackers zijn de script kiddies. Zij vinden het leuk om websites te verminken, zonder echte reden.

Hacking is strafbaar. De delictsomschrijving voor hacking luidt: het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval

sprake wanneer de toegang tot het werk wordt verworven:

a. door het doorbreken van een beveiliging,

b. door een technische ingreep,

c. met behulp van valse signalen of een valse sleutel, of

d. door het aannemen van een valse hoedanigheid.

Computervredebreuk of hacken is dus het binnendringen ("inbreken") in een computersysteem of netwerk. Dit kan uiteraard op vele manieren, en de wet geeft daar geen algemene definitie voor. Bij de behandeling in de Tweede Kamer gaf de minister aan dat dit van geval tot geval uit de rechtspraak zal moeten blijken.

Vaak wordt de term "hacken" gebruikt om activiteiten zoals computervredebreuk of computerinbraak aan te duiden. Dit is eigenlijk niet juist: een hacker is iemand die zeer goed en creatief met computers om kan gaan, en meestal niet er op uit is om schade aan te richten. Toch worden activiteiten van hackers (in deze positieve betekenis van het woord) gezien als computervredebreuk als ze, om welke reden dan ook, wederrechtelijk in systemen binnendringen.

Artikel 138ab lid 1 noemt het doorbreken van een beveiliging, gebruik maken van een technische ingreep, valse signalen of een valse sleutel en het aannemen van een valse hoedanigheid als voorbeelden van computervredebreuk. Deze categorieën zijn niet bedoeld als volledige taxonomie, er kan best overlap tussen zitten. Een paar voorbeelden uit elke categorie:

Doorbreken van een beveiliging: het laten crashen van het inlog-programma, zodat iedereen zonder verdere controle naar binnen mag

Een technische ingreep: het systeem zo ver krijgen dat het een instructie uitvoert waardoor de toegang wordt verleend tot bepaalde gegevens (het digitale equivalent van het kortsluiten van een elektronisch slot zodat de deur opengaat)

Valse signalen of een valse sleutel:: een geraden of afgekeken wachtwoord van een ander gebruiken, of je computer andermans IP-adres laten aannemen (IP spoofing)

Het aannemen van een valse hoedanigheid: je computer de naam geven van de printserver en zo toegang tot de map met printjobs krijgen, of de helpdesk bellen, zeggen dat het je eerste dag bij systeembeheer is en vragen wat het wachtwoord ook alweer was. Ook phishing, een e-mail of website laten lijken op die van een bank om zo pincodes en dergelijke te pakken te krijgen, kan hieronder vallen.

Wie dus één van deze handelingen verricht, pleegt in ieder geval computervredebreuk. Het is mogelijk dat er andere vormen van binnendringen zijn (of komen) die niet hier onder vallen. De rechter zal dan moeten bepalen of dit dan een strafbare vorm van binnendringen is.

SPYWARE

Spyware (ook wel adware genoemd) zijn computerprogramma's die meestal zonder expliciete toestemming van de gebruiker op de computer worden geïnstalleerd. Vervolgens verzamelt het programma informatie over het gebruik van de computer, met name het surfgedrag. De verzamelde informatie wordt vaak via het internet verzonden naar informatiemakelaars die aan de hand hiervan een profiel van de computergebruiker kunnen opstellen om aan hem reclame op maat te kunnen verzenden. Ook wordt de informatie vaak gebruikt om de gebruiker tijdens het surfen ongevraagde webpagina's te tonen, de zogenaamde pop-ups.

Hoe komt spyware op de computer terecht?

Spyware wordt soms in combinatie met (gratis) software verzonden. Het gaat dan bijvoorbeeld om software die u via websites kunt downloaden. Vooral bij websites met illegale software loopt u verhoogd risico op spyware. Als u software installeert, is het daarom belangrijk dat u altijd de gebruikersovereenkomst doorleest.

Daarnaast zijn er ook websites die bij uw bezoek proberen om spyware te installeren op uw computer. Als dit gebeurt, verschijnen er bijvoorbeeld allerlei vreemde schermen in beeld die vragen of u op ‘ja’ of ‘akkoord’ wilt klikken.

Ook bijlagen van e-mails (van veelal onbekende afzenders) kunnen spyware bevatten.

Is uw computer geïnfecteerd met spyware?

Een spyware-infectie herkent u aan de volgende signalen:

1. Uw computer is merkbaar trager en loopt vaker vast.

2. Op het bureaublad bevinden zich nieuwe iconen die u niet zelf geplaatst heeft.

3. Uw startpagina van het internet is gewijzigd naar een vreemde pagina die u niet ingesteld heeft.

4. Als u een foute URL intoetst komt u telkens op dezelfde, vaak commerciële, website terecht.

5. Er komen constant pop-ups in beeld waar u niet om gevraagd heeft.

6. Bij het zoeken op internet via een zoekmachine ziet u in plaats van de gewenste zoekresultaten reclame.

7. Er bevindt zich een nieuwe werkbalk in uw browser waar u niet om gevraagd hebt, en die zich moeilijk laat verwijderen.

Spyware verwijderen

U kunt spyware verwijderen met gratis software. Tegenwoordig is alleen anti virus software en een firewall op uw computer niet voldoende. Verschillende internationale bedrijven hebben daarom speciale software ontwikkelt dat gespecialiseerd is op het gebied van adware en spyware verwijderen en het voorkomen van de installatie hiervan.

In deze software kunt u onderscheid maken tussen programma's die spyware verwijderen in het algemeen, programma's die een specifieke infectie van spyware verwijderen en software die je beschermt tegen deze vorm van malware. U kunt deze software hier downloaden:

http://www.spywaretips.nl/download_antispyware.php

In de volgende nieuwsbrief o.a.:

- **uitleg over Cloud Computing**
- **wat is een keylogger**
- **Vissen ? Ohhh……Phishing**