Bijlage bij HOMCOM van 2/12/2024

**Definitie van Spyware**

Zoals de naam al doetvermoeden, wordt spyware doorgaanslosjesgedefinieerdals software die ontworpen is om gegevensteverzamelen van een computer of eenanderapparaat en door testurennaareenderdepartijzondertoestemming of medeweten van de gebruiker.

Hulpmiddel om ditteverwijderen : Superantispyware<https://www.superantispyware.com/free-edition.html>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Definitie vanAdware**

Adware, de afkortingvoor "advertisement-supported software", oftewel "reclame-ondersteunende software", genereertinkomstenvoorontwikkelaars door automatischadvertentiestegenereren op je scherm. Ditgebeurtmeestal in eenwebbrowser.

Hulpmiddel om ditteverwijderen : Adw Cleaner ( is familie van Malwarebytes , zeerkortprogramma )

<https://www.malwarebytes.com/adwcleaner>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Definitie van Malware**

Malware is eenverzamelnaamvoorongewenstekwaadaardige software. Ditwordenookwelcomputervirussengenoemd. Malware wordtgemaakt om informatietestelen van computersystemen, netwerkcomponenten en mobieledragers.

Hulpmiddel om ditteverwijderen : Malwarebytes ( nieuwsteversiezouookvirrussenverwijderen ?? )

<https://www.malwarebytes.com/nl/mwb-download>

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Definitie van Computervirus**

Een **computervirus** of **virus** is een vorm van schadelijke [software](https://nl.wikipedia.org/wiki/Software) ([malware](https://nl.wikipedia.org/wiki/Malware)). Het is een [computerprogramma](https://nl.wikipedia.org/wiki/Computerprogramma) dat zich in een [bestand](https://nl.wikipedia.org/wiki/Computerbestand) kan nestelen, bijvoorbeeld in bestanden van een [besturingssysteem](https://nl.wikipedia.org/wiki/Besturingssysteem). Computervirussen worden als schadelijk beschouwd omdat ze schijfruimte en computertijd in beslag nemen van de besmette computers. In ernstige gevallen kunnen virussen binnen in de computer schade aanrichten, bijvoorbeeld door het wissen en verspreiden van gevoelige gegevens. In zeer ernstige gevallen kan de gebruiker zelfs de totale controle over de computer verliezen.

Hoewel er veel verschillende computervirussen bekend zijn, komt er slechts een fractie daarvan "in het wild" voor. De Wildlist Organization International houdt een maandelijkse lijst bij van de virussen die in het wild zijn aangetroffen. Maandelijks worden er enkele duizenden verschillende virussen in het wild aangetroffen. Veel bestaande virussen zijn niet virulent genoeg om zich zelfstandig te verspreiden.

Het in omloop brengen van een computervirus is een [misdrijf](https://nl.wikipedia.org/wiki/Misdrijf), zowel in het Nederlandse [Wetboek van Strafrecht](https://nl.wikipedia.org/wiki/Wetboek_van_Strafrecht_%28Nederland%29) als in het Belgische [Strafwetboek](https://nl.wikipedia.org/wiki/Strafwetboek).

**Andere soorten malware**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=1) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=1)]

Computervirussen die zich ongemerkt in een computersysteem nestelen en vermenigvuldigen moeten onderscheiden worden van *[Trojanhorses](https://nl.wikipedia.org/wiki/Trojan_horse%22%20%5Co%20%22Trojan%20horse)*. Trojaanse paarden zijn programma's die andere dingen doen dan ze voorgeven, bijvoorbeeld de computer gemakkelijker toegankelijk maken voor andere virussen of spam versturen. [*Wormen*](https://nl.wikipedia.org/wiki/Computerworm) zijn geen virussen maar worden wel vaak zo genoemd. Het zijn zelfstandige programma's die zich direct over het netwerk verspreiden. Als de schade pas aangebracht wordt op een vooraf bepaald tijdstip, zoals bij een tijdbom of op het moment dat de software een bepaalde - vooraf vastgelegde - verandering waarneemt, spreekt men van een *[logic bomb](https://nl.wikipedia.org/wiki/Logic_bomb%22%20%5Co%20%22Logic%20bomb)*.

**Geschiedenis**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=2) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=2)]

Het computervirus ontstond al in de beginjaren van [ARPANET](https://nl.wikipedia.org/wiki/ARPANET). [Ray Tomlinson](https://nl.wikipedia.org/wiki/Ray_Tomlinson), de bedenker van [e-mail](https://nl.wikipedia.org/wiki/E-mail), schreef met zijn collega Bob Thomas twee programaatjes: Creeper en Reaper. Het eerste verspreidde razendsnel de tekst "I'mthecreeper, catch me ifyoucan" over het netwerk, het tweede ruimde het weer op.[[1]](https://nl.wikipedia.org/wiki/Computervirus#cite_note-1) In 1984 beschreef de Amerikaan [Fred Cohen](https://nl.wikipedia.org/w/index.php?title=Fred_Cohen&action=edit&redlink=1) in zijn [thesis](https://nl.wikipedia.org/wiki/These) *Computer Viruses – TheoryandExperiments* een functioneel computervirus voor het [Unix](https://nl.wikipedia.org/wiki/Unix)-[besturingssysteem](https://nl.wikipedia.org/wiki/Besturingssysteem). In 1987 publiceerde de Duitser [Ralph Burger](https://nl.wikipedia.org/w/index.php?title=Ralph_Burger&action=edit&redlink=1) in het boek *"Computer Viruses, a high techdisease"* de complete [broncode](https://nl.wikipedia.org/wiki/Broncode) van een werkend virus voor [MS-DOS](https://nl.wikipedia.org/wiki/DOS_%28besturingssysteem%29). Bijna alle computervirussen uit de periode 1987 tot circa 1991 zijn gebaseerd op de publicaties van Cohen en Burger.

Oorspronkelijk (vanaf circa 1988) verspreidden virussen zich vooral via software op [diskettes](https://nl.wikipedia.org/wiki/Diskette) en (illegale) [cd-roms](https://nl.wikipedia.org/wiki/Cd-rom). Sinds [e-mail](https://nl.wikipedia.org/wiki/E-mail) een grote vlucht genomen heeft verspreiden virussen zich vooral via e-mailprogramma's en dragen zij bij aan de hoeveelheid [junkmail](https://nl.wikipedia.org/wiki/Junkmail) die de doorsnee internetgebruiker ontvangt. Ze maken daarbij vaak gebruik van het adresboek dat de gebruiker in zijn e-mailprogramma heeft gemaakt. De meest gebruikte en daardoor gevoeligste e-mailprogramma's zijn [Microsoft Office Outlook](https://nl.wikipedia.org/wiki/Microsoft_Office_Outlook), [Outlook Express](https://nl.wikipedia.org/wiki/Outlook_Express), [Windows Mail](https://nl.wikipedia.org/wiki/Windows_Mail), [Google Mail](https://nl.wikipedia.org/wiki/Google_Mail) en [Windows Live Mail](https://nl.wikipedia.org/wiki/Windows_Live_Mail). Macrovirussen verspreiden zich voornamelijk via [Office](https://nl.wikipedia.org/wiki/Microsoft_Office)-bestanden.

Uit een verslag van [IBM](https://nl.wikipedia.org/wiki/IBM) bleek dat het aantal bekende computervirussen in 2004 met 25 procent toegenomen was tot 112438. Ongeveer 6 procent van de gescande e-mails in 2004 bevatten een virus. Het aantal geïnfecteerde e-mails ligt daarmee dubbel zo hoog als in 2003 (3 procent). In 2002 was dat slechts een half procent.

**Invloed van het besturingssysteem**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=3) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=3)]

Virussen komen het meest op het besturingssysteem [Microsoft Windows](https://nl.wikipedia.org/wiki/Microsoft_Windows) voor. Andere besturingssystemen zoals [GNU/Linux](https://nl.wikipedia.org/wiki/Linux) en [Mac OS X](https://nl.wikipedia.org/wiki/Mac_OS_X), worden minder vaak blootgesteld aan computervirussen. Sinds eind [jaren 2000](https://nl.wikipedia.org/wiki/2000-2009) komt hier langzaam verandering in door de stijgende populariteit van andere besturingssystemen. Deze zijn vaak niet aangepast om bescherming te bieden tegen virussen. Over de redenen dat Windows een geliefd doelwit is voor virusschrijvers kan men speculeren, maar de volgende redenen worden vaak aangegeven:

* Windows is een populair besturingssysteem, waardoor virusmakers zich sneller hierop zullen richten; ze hebben immers een grotere doelgroep.
* Veel Windows-programma's pogen zo [gebruiksvriendelijk](https://nl.wikipedia.org/wiki/Gebruiksvriendelijk) en [idiotproof](https://nl.wikipedia.org/wiki/Idiotproof%22%20%5Co%20%22Idiotproof) te zijn, dat de [veiligheid](https://nl.wikipedia.org/wiki/Computerbeveiliging) hiervoor het veld heeft moeten ruimen.
* Windows was van oorsprong gericht op *personal* computers, terwijl andere besturingssystemen zoals Linux en Mac OS X, vanaf de grond af zijn opgebouwd met het oog op meerdere gebruikers en netwerkgebruik. Werking en veiligheid van Linux en OS X zijn hierdoor veel beter bestand tegen de gevaren van internet.

Dit betekent echter niet dat deze besturingssystemen niet beschermd zouden moeten worden. Ze kunnen immers "drager" zijn van virussen en wormen voor Windows-systemen. Als besmette bestanden op bijvoorbeeld een Linux-systeem staan, kan het voorkomen dat de Windows-machines virusvrij gemaakt zijn, maar dat er daarna weer een nieuwe besmetting gebeurt via die bestanden. Tegenwoordig wordt ook aangeraden [antivirusprogramma](https://nl.wikipedia.org/wiki/Antivirussoftware)'s aan te schaffen voor Mac OS X.

Tegenwoordig komen virussen meer en meer voor GNU/Linux en Mac OS X (bijvoorbeeld [MacShield](https://nl.wikipedia.org/wiki/MacShield%22%20%5Co%20%22MacShield)). GNU/Linux was in 2011 een populair doelwit op dedicated servers. Omdat dedicated servers de laatste jaren betaalbaarder zijn geworden voor particulieren en GNU/Linux een gratis besturingssysteem is, komt dit meer en meer voor.

**Levensloop**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=4) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=4)]

Computervirussen hebben een zekere levensloop, gaande van het creëren tot het uitroeien van het virus. Het creëren gaat om de tijd die de programmeur nodig heeft om een virus te ontwikkelen. Vervolgens komt het virus tot stand en wordt het gekopieerd naar een strategische plaats zodat het zo vlug mogelijk verspreid kan worden. Daarna volgt de reproductie. Een virus vermenigvuldigt zich een aantal keren vooraleer het actief wordt. Voor bepaalde virussen vindt vervolgens een activeringsprocedure plaats. Het ogenblik waarop iemand de aanwezigheid van een virus vaststelt, wordt de ontdekking genoemd. Zodra de ontdekking is gebeurd, zullen software-ontwikkelaars trachten de aanwezigheid van het virus vast te stellen. Na deze assimilatie volgt de uiteindelijke uitroeiing.

**Bestrijding**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=5) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=5)]

Er is een complete industrie die softwarepakketten ontwikkelt om virussen te bestrijden, zowel voor Windows als voor [Mac OS X](https://nl.wikipedia.org/wiki/Mac_OS_X). Naast de softwarepakketten die op pc's of servers van bedrijven draaien is er nog een technologie om virussen te bestrijden, de zogenaamde *managed e-mail solutions*. Hierbij wordt de mail al op de [server](https://nl.wikipedia.org/wiki/Server) van de e-mailaanbieder gecontroleerd op virussen en spam. Het voordeel hiervan is dat een geïnfecteerde mail niet in het eigen systeem van de gebruiker komt en daar dus geen kwaad kan uitrichten.

**Wijzen van verspreiding**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=6) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=6)]

Voorbeelden van manieren waarop een virus in een computer kan doordringen zijn:

* [Websites](https://nl.wikipedia.org/wiki/Website)
* [USB-sticks](https://nl.wikipedia.org/wiki/USB-stick)
* [diskette](https://nl.wikipedia.org/wiki/Diskette)
* [geheugenkaarten](https://nl.wikipedia.org/wiki/Geheugenkaart)
* [cd-rom](https://nl.wikipedia.org/wiki/Cd-rom), [dvd](https://nl.wikipedia.org/wiki/Dvd) ...
* [modem](https://nl.wikipedia.org/wiki/Modem) (niet via internet, bijvoorbeeld [BBS](https://nl.wikipedia.org/wiki/Bulletin_board_system))
* [e-mail](https://nl.wikipedia.org/wiki/E-mail)
* bestanddeling (bijvoorbeeld [Kazaa](https://nl.wikipedia.org/wiki/Kazaa%22%20%5Co%20%22Kazaa), [LimeWire](https://nl.wikipedia.org/wiki/LimeWire%22%20%5Co%20%22LimeWire) en andere [p2p](https://nl.wikipedia.org/wiki/Peer-to-peer)-systemen)
* misbruik van [bugs](https://nl.wikipedia.org/wiki/Bug_%28technologie%29) ([vulnerabilities](https://nl.wikipedia.org/wiki/Vulnerabilities%22%20%5Co%20%22Vulnerabilities)) in software
* door het aankoppelen van een besmette harddisk
* Infectie door in [BIOS](https://nl.wikipedia.org/wiki/Basic_Input/Output_System) genestelde code. Alleen het wissen of het verwijderen van de [harde schijf](https://nl.wikipedia.org/wiki/Harde_schijf) heeft dan geen zin.
* Infectie door in de batterijchip van een [laptop](https://nl.wikipedia.org/wiki/Laptop) genestelde code. Dit is een nieuw onderzoeksgebied en komt nog heel zelden voor.
* Infectie via de draadloosnetwerkkaart. Hiervoor zijn [hardwarespecifieke](https://nl.wikipedia.org/wiki/Hardware) instructies nodig. Via een bufferoverflow zou hiermee toegang verschaft kunnen worden tot de computer zelf.
* Open netwerkpoorten en het niet gebruiken van een [wachtwoord](https://nl.wikipedia.org/wiki/Wachtwoord), een makkelijk te kraken of een makkelijk te achterhalen wachtwoord (bijvoorbeeld omdat hetzelfde wachtwoord overal gebruikt wordt door iemand). Hierdoor kan er externe code verstuurd worden naar deze computer.
* [Windows Update](https://nl.wikipedia.org/wiki/Windows_Update) (en mogelijk ook andere authentieke updatemethoden). Deze verspreidingsmethode is voor het eerst gesignaleerd in [Flame](https://nl.wikipedia.org/wiki/Flame_%28malware%29). Het was mogelijk gemaakt door een [Man-In-The-Middle](https://nl.wikipedia.org/wiki/Man-in-the-middle-aanval%22%20%5Co%20%22Man-in-the-middle-aanval) en het gebruik van valse certificaten, die gegeneerd konden worden door zwakheden in het [md5](https://nl.wikipedia.org/wiki/Md5)-algoritme.

**Verspreiding per e-mail**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=7) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=7)]

De e-mails die een virus bevatten proberen meestal de indruk te wekken dat ze een belangrijke boodschap bevatten en afkomstig zijn van een bekende afzender die men kan vertrouwen. Vaak is de schijnbare afzender iemand waar de persoon in kwestie in het verleden al contact mee heeft gehad. Dit komt doordat de e-mailadressen in het [adresboek](https://nl.wikipedia.org/wiki/Adresboek) vaak gebruikt worden voor de verzending van zulke berichten. Valse virusberichten worden [hoaxes](https://nl.wikipedia.org/wiki/Hoax%22%20%5Co%20%22Hoax) genoemd.

Ook een bekende truc is het misbruiken van de naam van een firma zoals de virusmail *MS Update Announcement*. Deze e-mail lijkt bedrieglijk echt en er wordt in gesuggereerd dat door uitvoer van het bijgevoegde programma de computer wordt beveiligd tegen de nieuwste virussen. De afzender is echter niet Microsoft en de bijlage is een virus.

Verder zijn e-mails met virussen die de indruk wekken afkomstig te zijn van een mailserver of [internetprovider](https://nl.wikipedia.org/wiki/Internetprovider) ook populair. Dat zijn berichten zoals "Mail Delivery failure" of "Internet Provider Abuse" of iets gelijkwaardigs. Sommige virussen zijn in staat om de e-mails af te stemmen op het e-mailadres van de geadresseerde, zo kan iemand met bijvoorbeeld een @yahoo.com-adres een e-mail krijgen die schijnbaar van de helpdesk van Yahoo afkomstig is maar in werkelijkheid van iemand anders.

Door het inlassen van een valse melding dat het bericht virusvrij is trachten sommige virussen de kans op infectie te verhogen. Toch zijn er ook nog steeds veel 'domme' virussen die zich beperken tot gewoon een "Hi" of "seeattached file".

Bij verspreiding via e-mail is het virus meestal bijgesloten in bijlage. De bestandsnaam kan vast zijn maar ook op basis van het e-mailadres van de ontvanger of volstrekt willekeurig. Meestal is er een poging gedaan om te verbergen dat het een uitvoerbaar bestand is. Een constructie zoals *data.txt.pif* is gebruikelijk (deze truc werkt echter alleen op computers met het Microsoft Windows-systeem). Men maakt hier handig gebruik van de optie die sommige e-mailclients hebben om de [bestandsextensie](https://nl.wikipedia.org/wiki/Bestandsextensie) te verbergen. Hierdoor is het schijnbaar een onschuldig tekstbestand. Ongelukkig genoeg is deze optie standaard ingeschakeld op de meeste versies van [Microsoft Outlook](https://nl.wikipedia.org/wiki/Microsoft_Outlook), [Outlook Express](https://nl.wikipedia.org/wiki/Outlook_Express).

De bestandsextensie van het virus kan verschillen. Macrovirussen kunnen aanwezig zijn in documenten die een macrotaal ondersteunen die programma's kan opstarten zoals het geval is bij [Microsoft Word](https://nl.wikipedia.org/wiki/Microsoft_Word), [Microsoft Powerpoint](https://nl.wikipedia.org/wiki/Microsoft_Powerpoint), [Microsoft Excel](https://nl.wikipedia.org/wiki/Microsoft_Excel) of [Microsoft Access](https://nl.wikipedia.org/wiki/Microsoft_Access).

De recentere virussen maken gebruik van de [spoofeigenschap](https://nl.wikipedia.org/wiki/Spoofing%22%20%5Co%20%22Spoofing): het sturen onder een e-mailadres van iemand anders.

**Soorten virussen**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=8) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=8)]

Vroeger waren er allerlei typen virussen die op hun eigen manier schade aanrichtten.

Zo waren er bestandsvirussen die viruscode aan programma's toevoegden die de extensie EXE of COM hebben. Als er zo'n programma wordt gestart, wordt het virus geactiveerd. Dan kan het virus zich naar andere bestanden kopiëren.

Bootsectorvirussen voegden gegevens toe aan het opstarten van een besturingssysteem.

Macrovirussen werden verspreid in bestanden met een macro erin, zoals Word-documenten.

Zoals reeds gezegd zijn [computerwormen](https://nl.wikipedia.org/wiki/Computerworm) en [Trojaanse paarden](https://nl.wikipedia.org/wiki/Trojaans_paard_%28computers%29) geen virussen, maar wel andere vormen van [malware](https://nl.wikipedia.org/wiki/Malware).

**Mailvirussen**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=9) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=9)]

Dit zijn de 'ouderwetse' virussen die zichzelf als bijlage verspreiden via e-mail. Tijdens een besmetting kan er automatisch een mailserver geïnstalleerd worden, zodat er geen gebruik hoeft te worden gemaakt van een e-mailprogramma op de geïnfecteerde computer. Ook de mailserver van de internetprovider waar de besmette computer mee is verbonden, hoeft niet te worden gebruikt. Internetproviders controleren streng op dit soort virussen dus de kans is groot dat de berichten er direct zouden worden uitgefilterd als ze via de provider verstuurd zouden worden.

Door een goede virusscanner te installeren en die altijd up-to-date te houden kan men zich wapenen tegen deze virussen. De meeste internetproviders filteren de geïnfecteerde mail er al uit. Bij sommige providers moet er daarvoor extra betaald worden.

**Mobiele virussen**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=10) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=10)]

Ook voor mobiele telefoons bestaan er tegenwoordig virussen. Een echte doorbraak blijft echter uit, ondanks het feit dat [mobiele telefoons](https://nl.wikipedia.org/wiki/Mobiele_telefoon) en [smartphones](https://nl.wikipedia.org/wiki/Smartphone) aan het uitgroeien zijn tot volwaardige computers.

Uit een studie van een groep netwerkdeskundigen onder leiding van hoogleraar [Albert-LászlóBarabási](https://nl.wikipedia.org/w/index.php?title=Albert-L%C3%A1szl%C3%B3_Barab%C3%A1si&action=edit&redlink=1" \o "Albert-László Barabási (de pagina bestaat niet)) (Northeastern University, Boston, Verenigde Staten) blijkt dat we hiervoor vooral moeten kijken naar de besturingssystemen van de mobiele telefoons. Er zijn namelijk heel veel verschillende besturingssystemen, zoals dat ook het geval is bij pc's. Virussen kunnen enkel worden overgedragen tussen twee apparaten met hetzelfde besturingssysteem.[[2]](https://nl.wikipedia.org/wiki/Computervirus#cite_note-fcalb-2)

De onderzoekers rekenden uit dat minstens 10 procent van alle mobiele telefoons hetzelfde [besturingssysteem](https://nl.wikipedia.org/wiki/Besturingssysteem) moet hebben alvorens een epidemie mogelijk is. Om tot dat resultaat te komen bekeken ze gedurende een maand de telefoongegevens van zes miljoen mobiele abonnees. Met die gegevens stelden ze een simulatie op met mobiele telefoongebruikers waarin ze ongeremd virussen konden loslaten.

Na een heleboel virusuitbraken kwamen ze dus tot de conclusie dat of een [epidemie](https://nl.wikipedia.org/wiki/Epidemie) uitbreekt afhankelijk is van de populariteit van een welbepaalde telefoon. Een populaire telefoon zal immers meer kans hebben om een andere telefoon tegen te komen met hetzelfde besturingssysteem waarop het virus kan worden overgedragen.

**De overdracht**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=11) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=11)]

De overdracht van mobiele virussen kan op drie manieren: via bluetooth, via mms of via het internet.

Hoe een besmetting gebeurt via [internet](https://nl.wikipedia.org/wiki/Internet) ligt voor de hand. De gebruiker van de telefoon downloadt het virus rechtstreeks van het internet en besmet zo zijn telefoon.

Besmetting via de [bluetooth](https://nl.wikipedia.org/wiki/Bluetooth)-methode duurt langer en is makkelijker te detecteren. De reeds besmette telefoon zoekt contact met andere telefoons binnen zijn bereik en eens hij een vatbaar slachtoffer heeft gevonden kopieert het virus zichzelf naar de andere telefoon.[[2]](https://nl.wikipedia.org/wiki/Computervirus#cite_note-fcalb-2)

De laatste methode is veruit de efficiëntste[[2]](https://nl.wikipedia.org/wiki/Computervirus#cite_note-fcalb-2). Een telefoon stuurt automatisch een [mms](https://nl.wikipedia.org/wiki/Multimedia_Messaging_Service) naar iedereen uit zijn netwerk met in de bijlage geen foto of filmpje, maar wel een virus. Als de ontvanger de mms dan opent en instemt om het 'filmpje' te bekijken, heeft het virus vrij spel en kan het zich verder verspreiden.

**Andere**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=12) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=12)]

* [*Bootsectorvirus*](https://nl.wikipedia.org/wiki/Bootsectorvirus). Dit virus voegt gegevens toe aan het opstartgedeelte van een computer die het besturingssysteem moet starten (de [bootsector](https://nl.wikipedia.org/wiki/Bootsector)).
* [*Macrovirus*](https://nl.wikipedia.org/wiki/Macrovirus). Dit virus wordt verspreid door bestanden met een macro erin. Voorbeelden zijn Word-documenten.
* [*Tijdbomvirus*](https://nl.wikipedia.org/w/index.php?title=Tijdbomvirus&action=edit&redlink=1). Dit virus wordt pas actief op een bepaalde datum of tijd (1 april en vrijdag de dertiende zijn daarbij populair). Hierbij kan elk soort virus worden geactiveerd.
* [*Logic bomb*](https://nl.wikipedia.org/wiki/Logic_bomb). Dit virus activeert als er een bepaalde, voorgeprogrammeerde, verandering optreedt in de computer. Hierbij kan elk soort virus worden geactiveerd.
* [*Bestandsvirus*](https://nl.wikipedia.org/w/index.php?title=Bestandsvirus&action=edit&redlink=1). Als een programma gestart wordt, wordt het virus geactiveerd en als het geactiveerd is kan het zich naar andere programma's kopiëren.

**Zie ook**

]

* [Lijst van malware](https://nl.wikipedia.org/wiki/Lijst_van_malware)
* [Phishing](https://nl.wikipedia.org/wiki/Phishing)
* [Spam (post)](https://nl.wikipedia.org/wiki/Spam_%28post%29)
* [Social engineering (informatica)](https://nl.wikipedia.org/wiki/Social_engineering_%28informatica%29)
* [Trojaans paard (computers)](https://nl.wikipedia.org/wiki/Trojaans_paard_%28computers%29)
* [Computerworm](https://nl.wikipedia.org/wiki/Computerworm)

**Referenties**

[[bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&veaction=edit&section=14) | [brontekst bewerken](https://nl.wikipedia.org/w/index.php?title=Computervirus&action=edit&section=14)]

**Op andere**[**Wikimedia**](https://nl.wikipedia.org/wiki/Wikimedia_Foundation)**-projecten**

* 

[***Media***](https://commons.wikimedia.org/wiki/Category%3AComputer_viruses#mw-subcategories)

 op Commons

* 

[***Definitie***](https://nl.wiktionary.org/wiki/computervirus) op WikiWoordenboek

* 

[***Boeken***](https://nl.wikibooks.org/wiki/Veilig_op_het_internet/Virussen)

 op Wikibooks

* Backer, J. 2009. Mobiele epidemie, Quest, oktober 2009, p. 108-110
* Ministerie van economische zaken. April 2000. Gids voor internetgebruikers, p. 47-48
* Wokke, A. 24 april 2009. Mobiele virussen gaan zicht verspreiden via mms (<https://tweakers.net/nieuws/59787/mobiele-virussen-gaan-zich-verspreiden-via-mms.html>), (geraadpleegd op 30 november 2009)
* Wang, P. , González, M. , Hidalgo, C. , Barabási, A. 2009. From human mobilitypatternto mobile virus'sspreading ([https://web.archive.org/web/20110626220820/http://puwang.barabasilab.com/Talks/Venice\_PPT.pdf](https://web.archive.org/web/20110626220820/http%3A/puwang.barabasilab.com/Talks/Venice_PPT.pdf)), (geraadpleegd op 30 november 2009)
* Pruyn, R. 28 september 2007. Mobiele virussen lopen twintig jaar achter, (itprofessional.be), (geraadpleegd op 30 november 2009)
* Metheringham, N. 13 december 2010. EximExploit In The Wild Advisory (<http://packetstormsecurity.org/files/96667/Exim-Exploit-In-The-Wild-Advisory.html>), (geraadpleegd op 12 juni 2011)