

Gezien er nog steeds veel verwarring ontstaat over welke nu de schadelijke software zijn op PC gaan we in deze nieuwsbrief hier wat dieper op in.

1) Virus

Allereerst heb je virussen. Dit zijn de oudste vorm van schadelijke software. Deze zijn ontstaan in de jaren tachtig en werden verspreid via besmette Cdroms, diskettes, BBS-systemen (*de voorloper van het Internet zoals we dat nu kennen*) end... Met de komst van het Internet is dit nu de belangrijkste vorm van virus-verspreiding geworden. Meestal via zogenaamde Peer-to-Peer-netwerken (bv. Kazaa, Limewire etc...). De laatste jaren zijn er veel variaties op virussen gekomen bv. Wormen (Worms) en Trojaanse paarden (Trojans)

De bedoeling van Virussen was allereerst zichzelf te verspreiden door zich te plakken op bestanden, programma's of zich te nestellen op bepaalde plaatsen op je hardeschijf of floppy disk. Zoals bv. De zogenaamde "boot"-sector. (*Dit is de plaats op je harde schijf waarin vitale opstart-informatie zit*). Deze programma's werden dan geactiveert door het geïnfecteerde programma te gebruiken of het systeem op te starten (waarbij men automatisch deze boot-sector gebruikt).

In veel gevallen proberen deze programma's ook bestanden te vernietigen waardoor er ofwel gegevens verloren gaan (bv. Word-bestanden of foto's) of waardoor men de werking van het systeem verstoort (als er bv. Systeembestanden beschadigt zijn).

Nadat deze programma's actief zijn blijven zij meestal in het werkgeheugen paraat om enerzijds mogelijke antivirus-programma's te blokkeren en anderzijds zich klaar te houden om verder bestanden te besmetten.

Virussen kom je voornamelijk op Windows machines tegen. Enerzijds omdat Windows de hoogste verspreidingsgraad heeft. Zo worden er veel meer Windows machines gebruikt dan Apple MacIntosh computers.

Even ter vergelijking:

Op Windows 98 tot en met Windows XP; zijn er meer dan 73000 virussen
Op het ouder Apple besturingssysteem (Mac OS Classic) zijn er tussen de 60 en 80 actieve virussen
Op het huidige Apple OSX systeem zijn er geen.
Op RISC OS (tot 1999 ROS 3.11) zijn er een 89-tal virusfamilies. Sinds RISC OS 3.5/3.7, RISCOS 4 en RISC OS 5 zijn er geen virussen meer bijgekomen.

Ondertussen zijn de meeste virussen uitvoerig gedocumenteerd en kan je via het Internet precies achterhalen wat welk virus doet.

Enkele websites waar je informatie kan vinden over virussen zijn o.a.

<http://www.virusalert.nl/>

http://www.mcafee.com/us/threat_center/default.asp

<http://www.symantec.com/region/nl/avcenter/global/index.html>

Er zijn zelfs computerclubs die zich eveneens bezighouden met deze virus-informatie bijvoorbeeld:

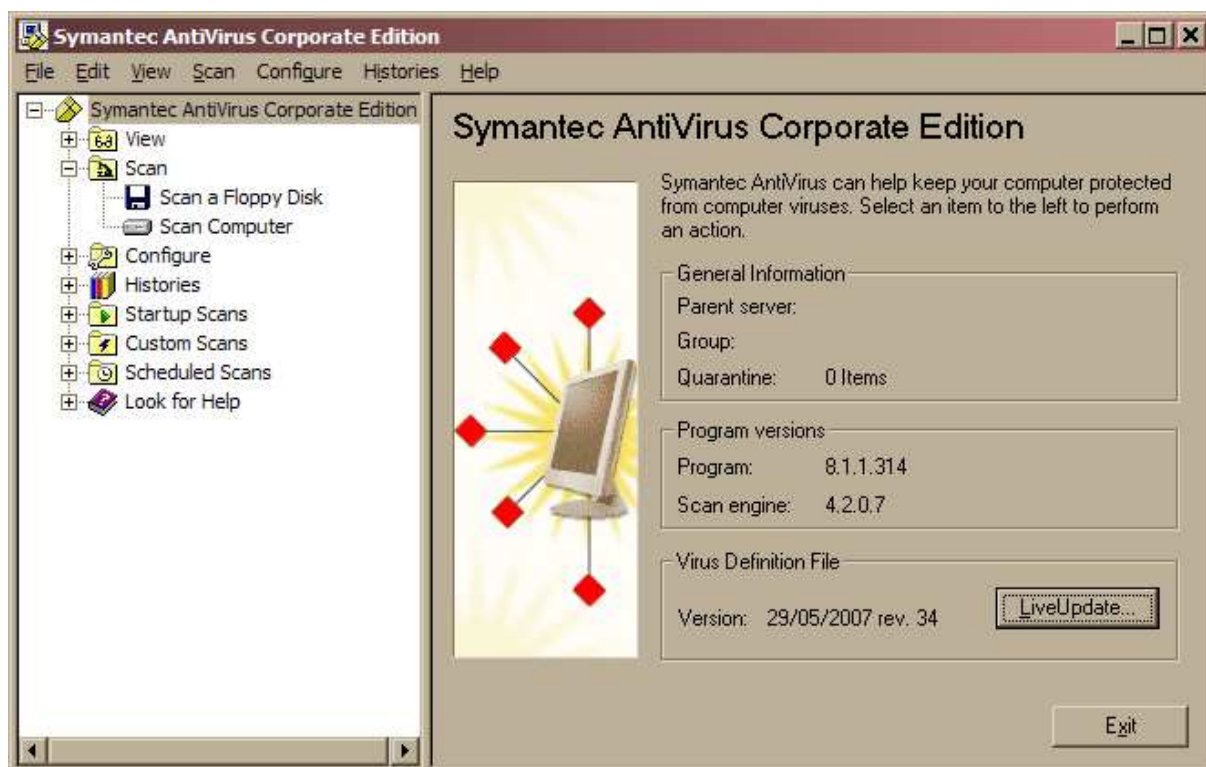
<http://www.ct.be/joomla/>

Op de websites van de 2 bekende anti-virusontwikkelaars vind je zeer veel technische informatie over hoe bepaalde virussen tewerk gaan. Vooral de website van Symantec is wat dat betreft een uitstekende bron van informatie EN nederlandsstalig.

Enkele bekende programma's om je computer tegen virussen te beschermen zijn o.a.

Voor Windows systemen

Symantec (Norton) Antivirus	http://www.symantec.com/nl/be/index.jsp
McAfee Antivirus	http://www.mcafee.com/nl/
Panda Antivirus	http://www.pandasoftware.com/
NOD32	http://www.nod32.nl/
AVG en AVGFree	http://www.grisoft.com
AVAST! Antivirus	http://www.avast.nl/
PC-Cillin	http://www.trendmicro.com



• Afbeelding van Symantec Antivirus voor bedrijven (Corporate Edition).



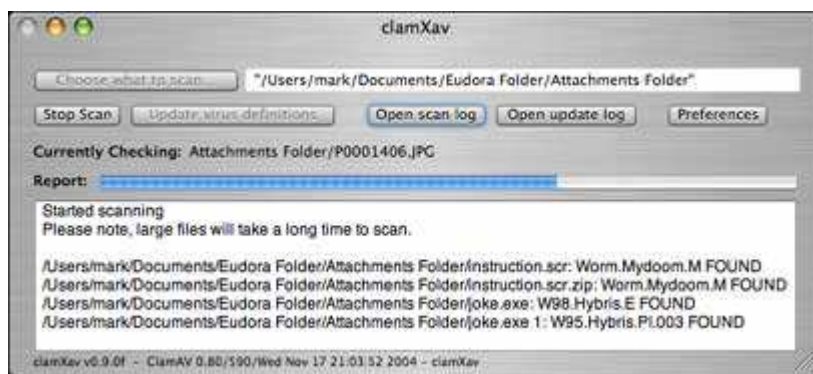
• Afbeelding van AVAST! Antivirus op Windows Vista Ultimate.

Ook Voor Linux bestaan er Antivirusprogramma's.

ClamAV <http://www.clamav.net/about/>
Panda Antivirus for Linux <http://www.pandasoftware.com/download/linux/linux.asp>

Voor Apple Mac OS X heb je o.a

Sophos Antivirus <http://www.sophos.com/products/es/endpoint/sav-mac.html>
Symantec Antivirus for Mac http://www.symantec.com/home_homeoffice/products/category.jsp?pcid=ma
ClamXAV <http://www.clamxav.com/>
McAfee Virusscan http://www.mcafee.com/us/enterprise/products/anti_virus/file_servers_desktops/virex.html



•Afbeelding van ClamXAV op Mac OS X.

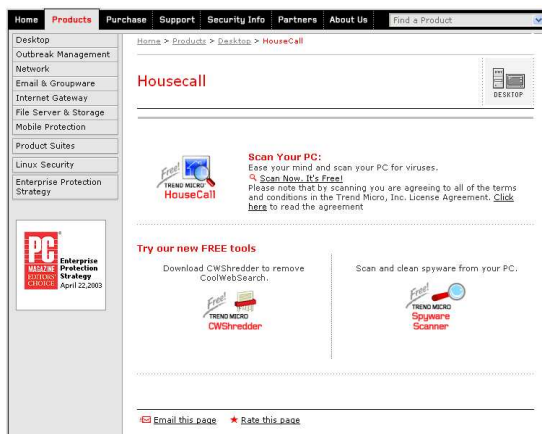
Risc OS alle versies

Vprotect van Pineapple Software wordt standaard meegeleverd met elke RISC OS machine.
Vzap (Vigay Software) <http://www.vigay.com/software/vzap.html>

Online Antivirus scanning (via het Internet)

Je kan zelfs je Windows PC scannen op virussen via het Internet. De bekende fabrikanten van anti-virussoftware hebben eveneens een zogenaamde "Online-virusscanner". Je kan deze gebruiken als je er een probleem is met je antivirusprogramma op je PC. Of als extra controle wanneer je vermoedt dat er toch iets binnengeslopen is.

Housecall van trend Micro <http://housecall.trendmicro.com/>
Security Check van Symantec <http://security.symantec.com/>



•Afbeelding van Housecall Online-virusscanner.

2) Adware

Deze software heeft tot doel om reclame op Uw scherm te laten zien. Oorspronkelijk werd Adware gezien als middel om ontwikkelkosten van software te recupereren. Waardoor je als gebruiker bepaalde software zeer goedkoop of zelfs gratis kon verkrijgen. Veel populaire gratis software bezit zelfs vandaag de dag nog steeds een of andere vorm van reclame. Ik denk bijvoorbeeld aan MSN Messenger (tegenwoordig Live Messenger geheten) waarin onderaan een kleine reclame-banner zit. In principe is Adware dan ook onschadelijk. In veel gevallen zal betreffende software zelfs niet werken wanneer deze Adware wordt uitgeschakeld.

De problemen zijn ontstaan doordat ook vele websites van Adware gebruik maken. Wanneer je dan zonder het te beseffen een aantal Adware hebt draaien dan ga je al snel problemen ondervinden met je normale surfen. Bovendien gebruiken Adware een stuk van het maandelijks beschikbaar Data-volume dat je mag gebruiken met je Internetverbinding. Vooral goedkopere Internetverbindingen hebben strikte beperkingen mbt. het maandelijks te verbruiken Data-volume. Dus vooral gebruikers van deze "Light"-internetverbindingen hebben er alle baat bij om Adware te beperken.



•Live Messenger, merk onderaan de reclamebalk op.

3) Spyware

Deze zijn in feite een variant op Adware. Doch kunnen in tegenstelling tot Adware wel schadelijk zijn. Het gaat hier om een groep van software die eventueel in combinatie met reclame allerlei informatie van de computergebruiker tracht te verzamelen en door te sturen naar de makers van de Spyware. Om deze dan later te verkopen en/of zelf te (mis)gebruiken. Er bestaan zelfs programma's die volledig internet verkeer omleiden (*proxy*) via een spy-proxy waardoor AL je internetverkeer kan worden gevolgd.

Meestal gaat het om systeem informatie. Welke computer heeft de desbetreffende gebruiker, welk besturingssysteem, welke hardware zit er in de PC? Maar er kan ook ingetypte informatie worden doorgestuurd. Onschuldige dingen zoals een zoekterm in een of andere search-engine (*zoekrobot*) maar ook wachtwoorden en login-informatie van je PC-banking. Met spyware moet je uiterst voorzichtig zijn want je weet nooit wat met welk programma wordt doorgestuurd.

Veel spyware vind je dus terug in programma's waar je informatie mee kan zoeken. Nep-Google Toolbars of nep-Ebay plugins zijn het beste voorbeeld. Ook zogenaamde cookies zijn een stuk spyware. (*Een cookie is een klein tekstbestandje met een code*). Bv. als je een taal van een website kiest dan wordt deze keuze in een cookie opgeslagen. Wanneer je later terug naar die website gaat zal je webbrowser automatisch de juiste taal gebruiken. In dit geval is de cookie een onschuldig onderdeel van het surfen.

In principe is het zo dat Adware en Spyware geen beschadigingen toebrengen aan je besturingssysteem in tegenstelling tot virussen die echt proberen bestanden kapot te maken. Wat niet wil zeggen dat ze niet voor problemen zorgen. In sommige gevallen kunnen de wederkerend pop-ups zodanig vervelend worden dat normaal internetverkeer zeer sterk wordt beïnvloed. Bovendien is het opvallend dat vooral Windows PC's het slachtoffer zijn van Spyware. Doordat veel Spyware via zogenaamde ActiveX-uitbreidingen binnensluipen kan in sommige gevallen een webbrowser die geen ActiveX ondersteunt, bv. Mozilla Firefox of Opera, al een oplossing zijn. (*ActiveX-applicaties zijn kleine programma's waarmee je je Internet Explorer kan uitbreiden. Bv. de Google-toolbar is zo'n ActiveX-uitbreiding.*)



•Spyware a la carte. Allerelei voorbeelden van zowel ActiveX- als "gewone" spyware.

Hoe verwijder je Adware en Spyware

Op Windows systemen zijn er de twee bekende programma's

Adaware <http://www.lavasoft.com/>
Spybot - Search & Destroy <http://www.safer-networking.org/>

Dit zijn 2 programma's die je computers scannen op adware en spyware. De laatste heeft zelfs een aantal instellingen die ook op actieve wijze spyware tegen houden. Zo word het veranderen van je startpagina in Internet Explorer tegen gehouden. Sommige spyware gebruiken een speciale startpagina om zichzelf te activeren. Je kan trouwens nog heel wat meer doen met Spybot. Vandaar dat het gebruik van dit programma toch wel enige voorkennis vereist.

Enige programma's die actief je PC beschermen tegen spyware zijn

SpywareBlaster <http://www.javacoolsoftware.com>
SpywareGuard <http://www.javacoolsoftware.com>

SpywareGuard is een gelijkaardige functie als wat Spybot gebruikt om je startpagina te beschermen. SpywareBlaster injecteert een lijst met schadelijk websites in Internet Explorer en Firefox zodat je weerhouden wordt om naar die (slechte) websites te gaan of om bepaalde software te installeren.



*Ad-Aware 2007 de vervanger van Ad-Aware Personal SE welke binnenkort beschikbaar komt.

De hier aangehaalde producten zijn een kleine greep uit de beschikbare hulpmiddelen voor PC en/of Mac.

Uiteraard kan U steeds op ons rekenen wanneer U het slachtoffer bent van computervirussen, adware en spyware en assistentie nodig hebt bij het verwijderen van deze "malware". Zo ook voor andere computertechnische problemen. Hieronder het bekende telefoonnummer:

0495 22 19 74