

Courbois Software

Virussen

Een **computervirus** (in het dagelijks taalgebruik wordt meestal kortweg over virus gesproken) is een vorm van schadelijke software (malware). Het is een computerprogramma dat zich in een bestand kan nestelen, bijvoorbeeld in bestanden van een besturingssysteem. Computervirussen worden als schadelijk beschouwd, want ze nemen schijfruimte en computertijd in beslag van de besmette computers; in ernstige gevallen kunnen ze in de computer schade aanrichten (zoals het wissen en verspreiden van (gevoelige) gegevens).

Computervirussen, die zich ongemerkt in een computersysteem nestelen en vermenigvuldigen, moeten onderscheiden worden van Trojan horses. Trojaanse paarden zijn programma's die andere dingen doen dan ze voorgeven, bijvoorbeeld de computer gemakkelijker toegankelijk maken voor andere virussen, of spam versturen terwijl je een spelletje speelt. Wormen 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.

Geschiedenis

In 1984 beschreef de Amerikaan Fred Cohen in zijn thesis Computer Viruses – Theory and Experiments een functioneel computervirus voor het Unix-besturingssysteem. In 1987 publiceerde de Duitser Ralph Burger in het boek Computer Viruses, a high tech disease de complete broncode van een werkend virus voor MS-DOS. Bijna alle computervirussen uit de periode 1987 tot circa 1991 zijn gebaseerd op de publicaties van Cohen en Burger. De Nederlander Jan Terpstra pionierde in deze periode via zijn BBS als een van de eersten met het opsporen en onschadelijk maken van computervirussen. Hij wordt gezien als een van de grondleggers van de antivirusindustrie.

Oorspronkelijk (vanaf circa 1988) verspreiden virussen zich vooral via software op diskettes en (illegale) cd-roms. Sinds e-mail een grote vlucht genomen heeft, verspreiden virussen zich vooral via e-mailprogramma's en dragen zij bij aan de hoeveelheid 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 Outlook, Microsoft Outlook Express, Google Mail en Windows Live Mail. Macrovirussen verspreiden zich voornamelijk via Office-bestanden.

Alternatieve besturingssystemen

Virussen komen vrijwel alleen op het besturingssysteem Microsoft Windows voor. Andere besturingssystemen, bijvoorbeeld GNU/Linux en Mac OS X worden vrijwel in het geheel niet blootgesteld aan computervirussen. Over de redenen kan men discussiëren en speculeren, maar de volgende redenen worden vaak aangegeven:

Windows is een zeer populair besturingssysteem, waardoor virusmakers zich veel eerder hierop zullen richten.

Veel Windows-programma's, waaronder veel Microsoftprogramma's, pogen zo gebruiksvriendelijk en idiotproof te zijn, dat de veiligheid hiervoor het veld heeft moeten ruimen.

Andere besturingssystemen, zoals GNU/Linux en Mac OS, zijn door hun openbaarheid veel minder vatbaar of vrijwel onvatbaar voor virussen.

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's aan te schaffen voor Mac OS X.

Bestrijding

Er is een complete industrie die softwarepakketten ontwikkelt, met name voor Microsoft Windows, om virussen te bestrijden. De bekendste softwarepakketten voor virusbestrijding zijn:

- NOD32
- Clamav/Clamwin (Open source)
- Symantec/Norton Antivirus
- McAfee
- Kaspersky
- Avast
- AVG
- Avira
- Microsoft Security Essentials

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 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 ook geen kwaad kan uitrichten.

Sommige viruswaarschuwingen worden per e-mail doorgestuurd. Bijna altijd betreft dit een hoax.

Wijzen van verspreiding

De gebruikelijke wijzen waarop een virus in een computer kan doordringen zijn:

- diskette
- geheugenkaarten
- besmette cd-rom
- modem (niet via internet, bijvoorbeeld BBS)
- e-mail
- bestanddeling (bijvoorbeeld Kazaa, LimeWire, en andere P2P-downloadsystemen)
- misbruik van bugs in het besturingssysteem zoals Microsoft Windows, of bugs in het e-mailprogramma zoals Microsoft Outlook en Microsoft Outlook Express
- door het ghosten van een besmette harddisk

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 met wie u in het verleden al contact heeft gehad omdat de e-mailadressen in het adresboek vaak gebruikt worden voor de verzending.

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. De bijlage is een virus.

Ook populair zijn e-mails met virussen die de indruk wekken afkomstig te zijn van een mailserver of internetprovider. 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. Maar er zijn ook nog steeds veel 'domme' virussen die zich beperken tot gewoon een "Hi" of "see attached file".

Het virus zelf

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 te verbergen. Hierdoor is het schijnbaar een onschuldig tekstbestand. Ongelukkig genoeg is deze optie standaard ingeschakeld op de meeste versies van Microsoft Outlook, 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, Microsoft Powerpoint, Microsoft Excel of Microsoft Access.

De recentere virussen maken gebruik van de spoofeigenschap: het sturen onder een e-mailadres van iemand anders.

Uit een rapport van 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.

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, zowel in het Nederlandse Wetboek van Strafrecht als in het Belgische Strafwetboek.

Soorten virussen

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.

Tegenwoordig wordt onderscheid gemaakt tussen drie hoofdtypen:

Worm

Dit is technisch gezien eigenlijk geen virus want het heeft geen ander programma nodig om te opereren. Wormen opereren zelfstandig, ze hoeven niet mee te liften met een e-mail of een programma. Een worm maakt gebruik van gaten in de beveiliging om zich zelfstandig van computer naar computer te verspreiden. Sommige wormen installeren malware en stelen op die manier persoonlijke gegevens of maken het geïnfecteerde systeem lid van een illegaal botnet waarmee spam kan worden verstuurd of DDoS-aanvallen op andere computers kunnen worden uitgevoerd.

Door de computer altijd up-to-date te houden, kan men zich wapenen tegen wormvirussen. Als er een nieuwe update is, moet die zo snel mogelijk geïnstalleerd worden.

Trojan

Trojans (Trojaanse paarden) maken geen gebruik van een zwakke plek op een computer, maar van een zwakke plek in de computergebruiker. Trojans doen zich voor als een leuk programmaatje, een screensaver, een leuk filmpje enz. Computergebruikers trappen erin en downloaden het bestand en besmetten zo hun eigen computer. Vooral in peer-to-peer-netwerken zijn veel trojans actief. Ze hebben dan bijvoorbeeld de bestandsnaam Christina_Aguilera_bloot_in_bad.exe. Mensen die Christina Aguilera leuk vinden, downloaden het bestand en klikken erop. Het lijkt dan net of er niets gebeurt, maar in feite wordt de computer op dat moment onzichtbaar besmet en verandert het systeem in een zombie (een computer die op afstand bestuurbaar is door de mensen die de trojan hebben gemaakt).

Tegen trojans kan men zich alleen wapenen door goed op te letten en niet alles meteen te geloven. Daarom dienen gratis programma's en andere software alleen uit betrouwbare bron gedownload te worden en er moet niet op 'OK' geklikt worden zonder te lezen wat er eigenlijk staat.

Mailvirussen

Dit zijn de 'ouderwetse' virussen die zichzelf als bijlage verspreiden via e-mail. Tijdens een besmetting kan er een mailserver automatisch geïnstalleerd worden, zodat er geen gebruik hoeft te maken 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.

Mailvirussen vervalsen het afzenderadres, vaak door adressen te gebruiken uit het adressenboek op de computer. Daardoor kan het gebeuren dat je een e-mail krijgt van het adres van je vriend Piet, terwijl het bericht eigenlijk verstuurd is vanaf de computer van Kees. Het virus doet dat zodat je Piet gaat lastigvallen in plaats van Kees, zodat de chaos nog wat groter wordt. Veel mailvirussen hebben als doel, troep te maken. Door mailservers te verstoppen, mailprogramma's te verstoppen, en e-mail onbruikbaar te maken.

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

Ook voor mobiele telefoons bestaan er tegenwoordig virussen. Een echte doorbraak blijft echter uit, ondanks het feit dat gsm's en smartphones aan het uitgroeien zijn tot volwaardige computers.

Uit een studie van een groep netwerkdeskundigen onder leiding van Hoogleraar Albert-László Barabási (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.

De onderzoekers rekenden uit dat minstens 10% van alle mobiele telefoons hetzelfde besturingssysteem moet hebben alvorens een epidemie mogelijk is. Om tot dat resultaat te komen bekeken ze gedurende een maand de telefoongegevens van maar liefst 6 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 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

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

Hoe een besmetting gebeurt via internet ligt voor de hand. De gebruiker van de telefoon downloadt het virus rechtstreeks van het internet en besmet zo zijn telefoon. Deze methode is de minst efficiënte van de drie omdat de overdracht niet gebeurt van telefoon naar telefoon en kan zo ook aangezien worden als een buitenbeentje.

De bluetooth-methode is heel wat efficiënter. 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. De bluetooth-methode is een goede manier om een virus snel te verspreiden over korte afstand, maar heeft als nadeel dat verspreiding over grotere afstand niet mogelijk is.

De laatste methode is veruit de efficiëntste. Een telefoon stuurt automatisch een mms 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 virussen

Bootsectorvirus.

Dit virus voegt gegevens toe aan het opstarten van een besturingssysteem. Op die manier kan het schijven en bestanden aantasten.

Macrovirus.

Dit virus wordt verspreid door bestanden met een macro erin. Voorbeelden zijn Word-documenten. De meeste andere virussen worden alleen door EXE-bestanden verspreid.

Tijdbomvirus.

Dit virus wordt pas actief op een bepaalde datum, vooral op 1 april of vrijdag de dertiende. De werking van zulke virussen verschilt, maar ze kunnen wel gegevens verwijderen.

Kaasschaafvirus.

Dit virus verwijdert steeds delen van een programma, totdat het programma niet meer gebruikt kan worden.