# Antivirus software versus Malware

*Bachelorscriptie door Anne Westerhof (0815012)*

## Samenvatting

Vroeger waren de enige kwaadaardige programma's virussen en als reactie hierop werd antivirus software uitgebracht. Tegenwoordig zijn er echter veel meer soorten kwaadaardige programma's, ook wel malware genoemd. Niet alle malware werkt op dezelfde manier waardoor huidige antivirus software veel meer diversiteit aan moet kunnen dan vroeger. Hierdoor vroegen wij ons af of huidige antivirus software nog wel geschikt is voor alle huidige malware en of er nog wel voldoende wordt beschermd. We zijn het onderzoek begonnen met een literatuurstudie naar de definitie van malware en de werking van antivirus software. Vervolgens hebben we een enquête uitgevoerd onder computer- en internetgebruikers om hun kennis over malware en antivirus software te onderzoeken. Hierbij hebben we ons vooral gefocused op de kennis wat betreft het gebruik van antivirus software, bijvoorbeeld of de gebruikers begrijpen wat de bij een viruswaarschuwing gesuggereerde alternatieven doen. Vervolgens hebben we een test uitgevoerd onder drie antivirus software paketten, namelijk AVG Free, BitDefender en Norton 360. In dit onderzoek hebben we onderzocht of de verschillende paketten voldoende beschermen tegen huidige malware. Als laatste geven we een blik op de toekomst wat betreft malware en antivirus software.

# Inhoudsopgave

# Introductie

Sinds de opkomst van computers, maar helemaal sinds de opkomst van internet zijn virussen een groot probleem. Om verschillende redenen worden kwaadaardige programma's geschreven, die vervolgens via allerlei manieren worden verspreid. De verzameling van deze kwaadaardige programma's wordt malware genoemd. Niet ieder kwaadaardig programma doet hetzelfde. Sommige programma's zijn gemaakt om resources van de computer te overbelasten, andere zijn gemaakt om gegevens die op de computer staan te achterhalen. Wat het doel ook is, we hebben ze liever niet op de computer. Om computers tegen deze malware te beschermen is er antivirus software ontwikkeld. De bedoeling van antivirus software is dat malware op de computer wordt opgespoord en onschadelijk wordt gemaakt. Ook willen we dat malware wordt gevonden op het moment dat wij op internet aan het surfen zijn, een bestand downloaden, of een e-mail binnenhalen. Dit laatste is al veel moeilijker dan het opsporen van malware die zich al op de computer bevindt. Maar als we malware al kunnen tegenhouden voordat het actief wordt op de computer, zijn we veel beter beschermd tegen de resultaten van de malware en voorkomen we ook de verdere verspreiding van de malware.

Anti-virus software is ontwikkeld om malware tegen te houden, maar zoals we eerder al noemden zijn er veel verschillende soorten kwaadaardige software. Het lijkt dan ook apart dat antivirus software de naam "antivirus" heeft en niet "antimalware". In de tijd dat antivirus software ontstond, waren virussen het enige type malware waar we last van hadden, maar tegenwoordig zijn er dus veel meer verschillende soorten. Om die reden is onderstaand onderzoek uitgevoerd, met als hoofdvraag: " Is huidige anti-virus software nog wel effectief tegen huidige malware?" Omdat het voor dit onderzoek te veel zou zijn om alle mogelijke anti-virus programma's te testen, zijn er 3 uitgekozen. Meer details hierover zijn te vinden in het betreffende hoofdstuk.

Naast de test van de effectiviteit van de anti-virus software is een ander punt belangrijk. Dat is het feit dat anti-virus software alleen effectief is als er goed mee omgegaan wordt door gebruikers. Zo is het belangrijk dat op de computer altijd de nieuwste versie van de anti-virus software staat, dat altijd de nieuwste updates zijn gedownload en voor een schone computer moet er ook regelmatig een virusscan worden uitgevoerd. Om uiteindelijk een conclusie te kunnen geven over hoe effectief anti-virus software op dit moment werkelijk is, zijn gebruikers ondervraagd via een enquête, om te kijken hoeveel computergebruikers hun antivirus software ook werkelijk goed gebruiken.

Tegenwoordig komt malware niet meer alleen op de PC voor. Ook andere apparaten zoals telefoons en tv's met een internet aansluiting kunnen problemen hebben met malware. Dit onderzoek beperkt zich tot malware voor de PC, omdat voor apparaten als tv's en mobiele telefoons de anti-virus software industrie nog niet even ver gevorderd is als voor de PC.

Hieronder gaan we in hoofdstuk één verder met een betere definitie te geven van wat malware is en geven we een overzicht van veel voorkomende soorten malware. Hoofdstuk twee beschrijft de werking van antivirus software. Hoofdstuk drie beschrijft de resultaten van een enquête onder computer gebruikers. In hoofdstuk vier vinden we het onderzoek naar de drie soorten antivirus software en hoe goed ze het op dit moment doen tegen malware. In hoofdstuk vijf sluiten we af met een conclusie en een blik op de toekomst.

# 1 – Definitie malware

Het is belangrijk een goede definitie van malware te geven. Malware is een samentrekking van Malicious Software, wat in het Engels kwaadaardige software betekent. Malware is dus niets anders dan een verzamelnaam voor alle kwaadaardige programma's die tegenwoordig geschreven worden. In algemeen taalgebruik worden alle soorten malware op dit moment vaak virussen genoemd, terwijl een virus eigenlijk maar één soort malware is. Dit hoofdstuk geeft informatie over een selectie van veel voorkomende types malware. Deze informatie is verkregen middels een literatuuronderzoek op basis van boeken in Google Books. Sommige van deze boeken hebben we vervolgens in de bibliotheek opgezocht. Hieronder volgt eerst een kort overzicht van de verschillende soorten malware.

| | | | | |
|---|---|---|---|---|
| **Infecterende malware:** | Virussen | Wormen | | |
| **Verborgen en verhullende malware:** | Trojaanse paarden | Backdoors | Rootkits | |
| **Malware om winst te maken:** | Spyware | Botnets | Keyloggers | Ransomware |
| **Grayware** | | | | |

Bovenstaande tabel geeft een mogelijke indeling van de types malware. Deze is gebaseerd op een indeling van wikipedia en eigen inzichten. Bovenaan staat de infecterende malware. Kenmerkend aan deze types malware is, dat ze een stuk code bevatten om zichzelf te verspreiden. Het belangrijke verschil tussen een virus en een worm is, dat een virus alleen bestanden in zijn omgeving kan besmetten. Met andere woorden, een virus blijft zich verspreiden op één computer, tot een mens een geinfecteerd bestand zelf naar een andere computer stuurt of brengt. Een worm daarentegen, kan zichzelf over het netwerk verspreiden en zo direct andere computers besmetten.

Verborgen en verhullende malware staat in deze categorie, omdat het extra moeite doet zichzelf te verbergen. Virussen en wormen zijn losse bestanden die eenvoudig kunnen worden gevonden, maar bij Trojaanse paarden, Backdoors en Rootkits wordt er extra code meegeleverd om te zorgen dat de malware niet kan worden gevonden.

Malware om winst te maken wordt gekenmerkt door het speciale "kwaadaardige" karakter. Deze types malware willen niet zomaar schade toebrengen aan een computer, maar ze hebben het doel om geld op te leveren voor de maker. Elk type doet dit op zijn eigen manier.

Grayware is genoemd, omdat er dingen zijn die mensen onder malware verstaan, terwijl het eigenlijk geen malware is. Deze soorten hebben we samengevat onder het kopje grayware (het grijze gebied tussen wel en niet malware).

Virussen en wormen zijn de enige types malware die zichzelf kunnen verspreiden binnen een computer of binnen een netwerk. De andere types zijn op zichzelf staande programma's die alleen verspreid kunnen worden als de gebruiker dat zelf doet via e-mail of USB stick óf als ze *onderdeel* zijn van een virus of worm.

## Infecterend

De meest bekende vorm van malware is infecterende malware. Deze vorm van malware worden gekenmerkt door het feit dat ze zichzelf verspreiden. Hierbinnen kunnen we twee soorten malware onderscheiden, namelijk virussen en wormen. Het belangrijkste verschil tussen deze twee is dat virussen verspreid worden door de hulp van mensen en wormen verspreiden zichzelf geheel automatisch. Hieronder beide in detail.

### Virussen

Het eerste onderzoek naar virussen werd gedaan in 1949 door John von Neumann. In zijn werk [2] liet hij zien dat het mogelijk was voor programma's om zichzelf voort te planten. Dit is de essentie van een computer virus. Ondanks dat er nu breed geadverteerd wordt door Apple dat MAC OS X het veiligste besturingssysteem is[3], was het eerste virus toch echt geschreven voor een Apple. Het ging om het Elk Cloner virus [4]. Dit virus was geschreven voor het Apple DOS 3.3 systeem en verspreidde zich door middel van een floppy disk. Bij de 50ste keer dat het werd gebruikt liet het een gedicht zien op het scherm van de computer. Dit voorbeeld laat goed zien hoe een virus in elkaar zit. De code van een virus bestaat vaak uit drie delen.

Het eerste deel van de code zorgt ervoor dat het virus zichzelf kan namaken en andere bestanden kan infecteren, meestal executible (.exe) files zodat het virus wordt uitgevoerd op het moment dat het host programma ( het .exe bestand) wordt uigevoerd.

Het tweede deel van de code wordt ook wel de " trigger" genoemd. Bij het Elk Cloner virus deed het pas echt wat bij de 50ste keer opstarten. In dit geval is " 50 keer opstarten" de trigger. Deze trigger activeert vervolgens het derde stuk code, wat ook wel de "payload" wordt genoemd. Deze payload bevat de (vaak kwaadaardige) acties van het virus. In het geval van Elk Cloner was er nog niet zo heel veel aan de hand, omdat er alleen iets op het scherm werd getoond, maar het kan bijvoorbeeld ook delen van de hard disk verwijderen. [1][8]

Zoals we al zeiden verspreiden virussen zich meestal via executible bestanden. De reden hiervoor is dat een virus alleen zijn werk doet, als het toegestaan wordt om zijn code uit te voeren. Door aan een executible vast te zitten, kan het zijn code uitvoeren op het moment dat een gebruiker deze executible uitvoert. Op het moment dat de code wordt uitgevoerd zoekt een virus naar andere mogelijke hosts en infecteert deze vervolgens. Vroeger werden hierbij vaak bestanden op een floppy disk geïnfecteerd. Op deze manier brachten gebruikers zelf de virussen over naar een andere computer.[5] Tegenwoordig kan dit nog steeds, maar dan meer door het gebruik van USB-sticks. Een tweede vorm waarop virussen zich verspreiden is via e-mail of weblinks. Hierbij kan je denken aan momenten waarop gebruikers zelf bijlages van e-mails openen of links die door vrienden (onbewust) over Instant Messaging programma's worden gestuurd. Zodra iemand op zo'n link klikt, kan via de website het virus automatisch worden gedownload.

Een derde vorm van verspreiding berust op het gebruik van macro's in Office programma's. Deze macro's die je zelf binnen de programma's kan maken zijn eigenlijk "gewoon" stukjes VB script die kunnen worden uitgevoerd. Een virus dat zich voordoet als een macro kan moeilijk te vinden zijn en deze virussen kunnen daarom nogal problemen opleveren, omdat ze zich verspreiden via onschuldige Office-documenten..[5][6]

Door het gebruik van anti-virus software gebruiken de meeste virussen verschillende technieken om zichzelf te verbergen en niet gevonden te worden. Meer hierover bij het hoofdstuk over de werking van anti-virus software.

### Wormen

Wormen werden pas later ingezet dan virussen, mede omdat wormen zich bewust over netwerken en internet verspreiden terwijl virussen alleen binnen de computer verspreiden. Het eerste echte onderzoek begon dan ook pas rond 1970.[7] De eerste echt kwaadaardige worm werd verspreid op 2 november 1988 door Robbert Tappan Morris. Deze Morris worm infecteerde en beschadigde ongeveer 10% van alle computers destijds aangesloten op het internet. Het grote probleem van deze worm was dat het computers meerdere keren kon infecteren en dit gebeurde dan ook zo vaak, dat op een gegeven moment de computer echt niet meer gebruikt kon worden, omdat hij te langzaam was. De schade was enorm (10 – 100 miljoen dollar) en er werd ingezien hoe gevaarlijk een niet beschermd netwerk als het internet kon zijn.[9][10]

Dit voorbeeld laat goed het verschil zien tussen een worm en een virus. Een worm heeft geen mensen nodig om te verspreiden. Wormen gebruiken geen host, maar zijn op zichzelf staande programma's. Om te verspreiden maken ze gebruik van zwakke plekken (niet beschermde plekken) binnen een netwerk. Virussen kunnen zich alleen binnen een computer verspreiden, tenzij ze worden geholpen door mensen via bijvoorbeeld een floppy disk. Wormen kunnen uit zichzelf van computer naar computer gaan en daar steeds een kopie van zichzelf achterlaten.[7][8] Hoewel wormen net als virussen een payload kunnen hebben, zijn er ook wormen die deze niet hebben, zoals het Morris virus. Het kwaadaardige aan wormen zonder payload is dat ze door hun (ongelimiteerde)verspreiding veel bandbreedte gebruiken en hele netwerken kunnen dichtslibben tot op een punt dat netwerken en computers niet meer kunnen worden gebruikt. Wormen die wel een payload hebben, worden vaak gebruikt om andere malware op computers te installeren. Deze andere malware die verderop besproken wordt doet dan het echte werk, terwijl de worm alleen maar wordt gebruikt om deze malware verder te verspreiden. [8]

## Verborgen en verhullende malware

Ook malware moet worden uitgevoerd (door de gebruiker) voordat het iets kan doen. De onderstaande types malware hebben zich gespecialiseerd in verbergen en vermommen, soms om te zorgen dat de gebruiker onwetend zelf de malware uitvoert, soms om te zorgen dat programma's elkaar kunnen uitvoeren zonder dat iemand het merkt.

### Trojaanse paarden

Trojaanse paarden, beter bekend onder de Engelse naam " Trojan Horses" (kortweg: Trojans,) zijn volledig afhankelijk van de gebruiker om hun werk te doen. Ze werken op dezelfde manier als de Grieken, die de Trojanen zelf het paard naar binnen lieten halen. Bij deze malware haalt de gebruiker zelf het vervelende programma naar binnen. Om te verspreiden, kunnen Trojans wel aan virussen vast zitten als de payload. Op die manier kunnen ze worden verspreid, maar ze zullen nog steeds de hulp van een gebruiker nodig hebben om echt te kunnen werken.[11][12] In tegenstelling tot virussen is bij de Trojans niet bekend wanneer de eerste werd losgelaten, mogelijk omdat de eerste ook als virus gezien werd en pas later een aparte naam kreeg. Trojans vermommen zichzelf op twee manieren.
De eerste is de eenvoudigste, maar werkt ook het minst goed. Bij deze vorm van vermommen neemt de

Trojan simpelweg een andere naam aan. Dit is meestal een naam van een programma wat een gebruiker graag uit zou willen voeren zonder verder te kijken of alles wel klopt. Deze kunnen op de computer terecht komen via downloaden of via een e-mail bijlage. Veel mensen zijn inmiddels bekend met het feit dat je voorzichtig moet zijn met .exe bestanden. Om deze reden wordt er soms met de naam van een bestand geknoeid tot deze ongeveer de volgende vorm heeft " ILoveYou.txt .exe". Door de vele spaties kan de echte extensie .exe wegvallen van het scherm waar de gebruiker hem bekijkt en denken dat het een tekst bestand is. Zodra er op wordt geklikt is het te laat en kan de Trojan zijn werk gaan doen.
De tweede mogelijkheid is dat de Trojan zich binnen een ander programma bevindt; het echte programma wordt dan als omhulsel gebruikt. Op het moment dat de gebruiker dit programma opstart doet het programma gewoon zijn werk, maar ondertussen gaat het Trojaanse paard ook zijn werk doen op de achtergrond, vaak zonder dat de gebruiker dit merkt.[11]
Trojans kunnen verschillende functies hebben en heel veel schade aan richten. Net als virussen kunnen ze een desktop veranderen, iets weergeven of bijvoorbeeld je cd-lade open laten gaan. Maar ook andere dingen zijn mogelijk. Zo kan een Trojan ook een backdoor zijn, spyware zijn, adware zijn, of een keylogger zijn. Met andere woorden, een Trojan is uiteindelijk een ander stuk malware, dat vermomd is om niet ontdekt te worden. Dit is een van de redenen dat heel veel malware door anti-virus software gekenmerkt wordt als Trojan [13]. Dat iets een Trojan is, zegt uiteindelijk niets over wat de malware werkelijk doet.

### Backdoors

Backdoors kunnen op verschillende manieren op je computer belanden. Vaak zijn ze vermomd, waarbij het dus Trojans zijn, maar ze kunnen ook rechtstreeks door iemand op het systeem worden gezet, soms zelfs als onderdeel van het besturingssysteem.[14] Ook bij de backdoor zegt de naam veel over het werk van dit stukje malware, het is namelijk een achterdeur. Het doel van de backdoor is om de maker van de backdoor toegang te geven tot de computer waar de backdoor op staat (vanaf bijvoorbeeld zijn eigen computer), zonder de normale beveiligingsstappen te hoeven doorlopen. Hierbij kan je denken aan het invoeren van wachtwoorden of authenticatie op een andere manier die dankzij de backdoor niet hoeft te worden uitgevoerd. Dit kan tot stand komen doordat de backdoor een poort heeft opengezet in het netwerk waardoor een volledige connectie kan worden gemaakt. Een andere eenvoudigere manier waarop een backdoor werkt, is het automatisch veranderen van wachtwoorden, waardoor de maker weet welk wachtwoord er nodig is om in de computer te komen. Als de maker via de backdoor eenmaal binnen is, kan er van alles worden gedaan, zoals het veranderen van gegevens en bestanden, het stelen van informatie of het installeren van andere programma's. [15]
De reden dat de backdoor bij de verhullende malware hoort, is dat de mogelijkheden die gemaakt worden voor de maker om in de computer te komen niet zichtbaar zijn. Een " goede" backdoor werkt dan ook nog steeds, zelfs nadat het originele programma dat de backdoor open zette verwijderd is. Het programma zelf wordt soms makkelijk gedetecteerd door mens of anti-virus software, maar als het programma zijn werk al heeft gedaan, kan het veel moeilijker zijn om uit te vinden wat het programma heeft gedaan en hoe die beveiligproblemen weer kunnen worden opgelost.

### Rootkits

Rootkits zijn een van de meest vervelende types malware. De naam is afgeleid van het Root account op een UNIX computer, die alle mogelijkheden heeft om dingen op de computer te wijzigen. Het doel van een rootkit is niets anders dan het verhullen van acties en bestanden. Een rootkit wordt (door een hacker) geïnstalleerd op een computer nadat hij toegang tot het centrum van het besturingssysteem heeft verkregen. Met andere woorden, een hacker heeft op een andere manier, bijvoorbeeld via een backdoor of door een wachtwoord te kraken, toegang gekregen tot de basis van het besturingssysteem en kan hier allerlei dingen veranderen. Vervolgens installeert hij een rootkit die er voor zorgt dat zijn acties ongezien blijven.

Rootkits kunnen grofweg op twee niveau's hun werk doen. De eerste is op gebruiker niveau en de andere is op kernel niveau. Gebruiker niveau wil zeggen dat de rootkits het werk, of kwaadaardig werk van (onderdelen van) gewone applicaties verhullen. Deze applicaties krijgen van het systeem geheugen toegewezen en alleen met dit geheugen kan de rootkit iets doen. Bij rootkits die werken op kernel niveau is er toegang tot alle geheugen en mogelijkheden van het systeem. Deze type rootkits zijn veel gevaarlijker, juist omdat ze toegang tot alles hebben.

Rootkits zijn erg vervelend voor antivirus software om mee om te gaan. Het probleem is, dat het meestal niet zomaar één bestand is, maar een rootkit bestaan vaak uit verschillende bestanden en processen. Een "goede" rootkit zorgt er voor, dat het zichzelf in stand houdt. Zo kan het mogelijk zijn om een bepaald proces van de rootkit te verwijderen, terwijl direct daarna een ander proces dit eerste, verwijderde, proces weer opnieuw aanmaakt. Dit gebeurt zo snel dat het vaak niet mogelijk is om beide processen goed te verwijderen. Een ander probleem is dat rootkits gemaakt zijn om iets anders te verhullen, maar ook om zichzelf te verhullen. Als antivirus software malware vindt door verdacht gedrag te zoeken, lukt dit bij een rootkit niet, omdat een rootkit juist is gemaakt om verdacht gedrag te verhullen en hierbij zelf normaal te werken. Deze zaken zorgen ervoor dat veel antivirus software rootkits nog niet kan herkennen. De antivirus software die dit wel kunnen zijn nog niet in staat om de rootkit ook werkelijk te verwijderen en op dit moment is de enige oplossing een schone installatie van de harde schijf te maken. [16][17]

## Malware voor winst

De volgende types malware zijn de meest voorkomende, hoofdzakelijk omdat deze types de makers echt wat opleveren. Rootkits helpen hackers om hun toegang tot een systeem te verbergen zodat ze rustig hun gang kunnen gaan en backdoors geven hackers de mogelijkheid om hun werk te doen, maar zelfs bij gebruik van beide methodes kan de hacker nog steeds maar één computer tegelijk aanvallen. Met de volgende types malware kan een maker geld verdienen via honderdduizenden computers tegelijk.

## Spyware

Van alle types malware is de term spyware, naast de term virus, misschien wel het bekendst. Dat wil nog niet zeggen dat de meeste mensen ook weten wat spyware inhoudt. Spyware doet zijn naam eer aan door informatie te stelen van gebruikers. Niet de gegevens die op een computer staan, maar het gebruikersgedrag van de gebruikers, zoals welke websites er worden bezocht en wat er wordt ingetypt (keyloggers, zie verderop), maar ook muisbewegingen en webcam gedrag. Ook kan het andere soorten software installeren, instellingen veranderen, zoals de startpagina van een browser, en bestanden of licentie sleutels stelen. Al met al een hele lijst van vervelende gevolgen. Al deze informatie kan vervolgens worden gebruikt om bijvoorbeeld een adware onderdeel van de spyware in gang te zetten. Adware kan op twee manieren voorkomen, een is bij spyware, de andere is op een manier die bij de grayware zal worden behandeld. Als het bij spyware zit, kunnen er ineens reclame boodschappen in pop-ups tevoorschijn komen, of er worden e-mails met reclame naar de gebruiker verstuurd, nadat het e-mail adres is achterhaald. Naast deze vervelende reclame zorgt spyware er ook nog voor, dat computers onnodig traag worden door alle informatie die wordt verstuurd en kan er zelfs voor zorgen dat een internet verbinding niet meer werkt.[18][19]
Dan blijft de vraag over, hoe kom je nou eigenlijk aan spyware? Een computer kan met spyware worden geïnfecteerd als het bijvoorbeeld onderdeel is van een virus, het kan meekomen met andere programma's die je download, in dit geval valt de spyware ook onder de categorie Trojan. Ook op andere manieren kan spyware zichzelf verhullen en dus als Trojan op de computer terecht komen. Als spyware eenmaal op de computer zit is het mogelijk voor het programma om meer spyware op deze computer te installeren, waardoor dingen snel uit te hand kunnen lopen. [18]

## Keyloggers

Bij keylogging wordt er precies bijgehouden welke toetsen een gebruiker aanslaat en bij keylogging is dit ook het enige wat wordt bekeken. Keylogging kan op verschillende manieren, via software, maar ook via hardware. Hier willen we alleen kijken naar de malware variant en dus naar de software die eventueel verwijderd kan worden met anti-virus software.
Keyloggers zijn vaak een onderdeel van spyware, maar kunnen ook op zichzelf worden gebruikt. Het gevolg van keyloggers is dat in het " beste " geval alleen gezien wordt wat je naar je vrienden schrijft in een messaging programma, maar in het ergste geval worden je wachtwoorden, creditcard nummers en bankgegevens gestolen. Het gevolg zie je dan op je bankrekening.
Keyloggers kun je ook binnenhalen doordat het Trojans zijn en zich voordoen als gewone software en ook kunnen ze verspreid worden als onderdeel van een virus. Naast het gebruiken van anti-virus software kunnen keyloggers op nog een andere manier worden tegengehouden. Hierbij maakt men gebruik van een virtueel toetsenbord. In plaats van wachtwoorden en creditcard nummers in te typen klikt men de bijbehorende letters en cijfers aan op een toetsenbord op het beeldscherm. Op deze manier kunnen keyloggers niet zien wat men doet, hoewel via andere spyware er mogelijk nog steeds problemen kunnen ontstaan. [20][21]

## Botnets

De naam botnet is een afkorting van robot netwerk en kan op twee manieren worden uitgelegd. De eerste beslaat simpelweg een netwerk van bots zoals bijvoorbeeld IRC bots, robots die scripts draaien

op dit messaging platform en kunnen reageren op simpele commando's van andere IRC gebruikers. Mensen die deze bots in een netwerk bijhouden, worden bot herders of bot masters genoemd. Naast deze botnets zijn er ook nog de nieuwere kwaadaardige botnets. Bij deze botnets zijn computers, die geïnfecteerd zijn met zo'n bot, de nodes in het netwerk. Deze bots kunnen vervolgens worden aangestuurd door de bot herder of bot master om allerlei dingen op de geïnfecteerde computers uit te laten voeren. Hierbij kan gedacht worden aan Distributed Denial of Service (DDoS) aanvallen, maar ook aan het versturen van spam of andere kwaadaardige activiteiten. Botnets werken zo goed, omdat de meeste computers tegenwoordig een constante verbinding hebben met internet. Juist doordat de herders of masters daarna zoveel computers tot hun beschikking hebben, kunnen ze heel veel rekencapaciteit gebruiken voor allerlei soorten aanvallen of andere acties, zoals het kraken van wachtwoorden. [21][22]

Een bot kan men op zijn computer krijgen, omdat hij wordt verstuurd als de payload van een virus of worm. Deze wordt verspreid en als het virus of de worm op je computer komt, wordt de bot geïnstalleerd. Deze loggen bij een (IRC) server op het internet, waar de herder of de master er dan weer bij kan om de computer te gebruiken waar de bot op staat. Sommige bot herders willen alleen proberen om zoveel mogelijk bots in hun netwerk te krijgen, andere worden betaald door andere mensen om kwaadaardige dingen uit te voeren, zoals bijvoorbeeld spam versturen.

Als de anti-virus software om botnets te vinden niet helpt, is het handmatig verwijderen de enige mogelijkheid om er vanaf te komen. Het is handig om de internet verbinding te verbreken, omdat de computer dan geen onderdeel meer is van de botnet.

### Ransomware

Bij deze vorm van malware is het erg duidelijk waarom het in de categorie van winstgevende malware valt. Ransomware komt van het Engelse word ransom, wat losgeld betekent. De manier waarop dit type malware tewerk gaat lijkt dan ook heel erg op de manier waarbij losgeld gevraagd wordt, nadat iemand is gekidnapped. Alleen in dit geval gaat het niet om personen, maar om bestanden. Ransomware wordt door de gebruiker zelf binnengehaald, waarbij ransomware mogelijk een Trojan kan zijn om te zorgen dat het sneller door de gebruiker wordt binnengehaald. Als de ransomware eenmaal op de computer staat, zoekt het bestanden op die mogelijk waardevol zijn voor de gebruiker, zoals Office bestanden en foto's. Door de ransomware worden deze bestanden versleuteld en onleesbaar gemaakt. Er wordt een berichtje achtergelaten, vaak in dezelfde map, waarin gegevens staan over betaling. Als de gebruiker dit geld betaald, worden de bestanden weer vrijgegeven.
Deze methode wordt niet veel gebruikt, omdat er enkele nadelen aanzitten. Zo is de versleuteling die wordt gebruikt niet altijd even goed, waardoor de gebruiker soms zelf met een andere programmaatje de versleuteling kan opheffen zonder iets te betalen. Een ander nadeel is, dat er een traceerbare geldstroom plaatsvindt, waardoor het voor de autoriteiten makkelijker te vinden is. Daarbij is de ransomware zelf redelijk makkelijk te vinden voor antivirus software, omdat het zelf geen verhullende onderdelen bij zich heeft. Het nadeel is, dat wanneer het pas gevonden wordt nadat het zijn werk heeft gedaan, het verwijderen van de ransomware zelf niet zoveel zin meer heeft, omdat de bestanden dan al versleuteld zijn. Toch is ransomware niet iets dat heel gevaarlijk is, met name doordat het zo weinig voorkomt en door de nadelen die er aan kleven. [37]

## Grayware

Tijdens ons onderzoek zijn wij de term grayware tegen gekomen. Hieronder zou software vallen die niet helemaal gewone software is, maar ook geen virus. Als voorbeeld worden spyware en adware genoemd. [23] Zelf vinden wij de term grayware een goede term voor software dat op een virus lijkt, maar het niet is. Toch willen wij adware en spyware daar niet onder classificeren. Juist door de mogelijkheid van spyware om echt belangrijke informatie te achterhalen is het echte malware (kwaadaardige software). De adware is vaak een gevolg van de spyware en hoewel misschien minder schadelijk is het nog steeds iets waar je duidelijk niet om hebt gevraagd. Maar wat is dan wel grayware? Wij willen grayware definiëren als software die ongewenst, maar wel vrijwillig op de computer is geïnstalleerd. Hierbij kan je denken aan toolbars of andere (ongewenste) programma's die met een gewenst programma mee worden geïnstalleerd. Maar dan wel op zo'n manier dat als je het installatieproces goed bekijkt er een mogelijkheid is om deze niet te installeren. Hetzelfde geldt voor advertenties bij programma's waarvan de gebruiker van te voren weet dat deze bij het programma zullen zitten, omdat het nou eenmaal freeware is. Dit kunnen bijvoorbeeld advertenties zijn bij muziek programma's zoals het vroegere kazaa en limewire. Soms zijn deze advertenties verplicht om het programma te laten draaien. Toch is het geen malware, omdat je er voor kan kiezen het niet op je computer te hebben. Sommige anti-virus software verwijdert ook dit soort advertenties, met als gevolg dat programma's voor gebruikers niet meer werken. Hierin kan een probleem zitten. Bij dit onderzoek wordt alleen maar gekeken naar malware en niet naar wat wij hier als grayware geclassificeerd hebben.

## Conclusie

Bovengenoemde types malware komen dus steeds meer voor, maar dit geldt op het moment alleen voor Windows gebruikers. Hoewel er zoveel verschillende soorten zijn, worden ze bijna allemaal gericht op het Windows platform. Ten eerste omdat de beveiliging minder goed is dan bijvoorbeeld Mac of Linux en ten tweede omdat Windows een veel gebruikt besturingssysteem is. Daardoor kan er een grotere groep mensen in één keer worden benaderd wat een groter effect oplevert. Toch is een uitbreiding naar malware op Mac of Linux niet ondenkbaar. Een ander, misschien groter probleem, is dat internet niet langer iets is alleen voor computers en aangezien het internet de belangrijkste bron is voor het verspreiden van malware, kunnen we binnenkort misschien ook malware voor telefoons en tv's verwachten. De eerste antivirus software voor telefoons is er dan ook al, maar deze programma's zijn nog zeer nieuw. Toch kan het belangrijk zijn om de ontwikkelingen in de gaten te houden, want misschien moeten we op een bepaald moment wel antivirus software op onze tv's of spelcomputers gaan installeren.

# 2 – Werking anti-virus software

Anti-virus software werkt tegenwoordig op verschillende manieren. Het bekijken van websites van verschillende fabrikanten geeft het idee dat het ene product nog beter werkt dan het andere product, door alle nieuwe technieken die worden gebruikt. Grofweg kan de werking van anti-virus software in twee taken worden verdeeld. De eerste is het detecteren van malware, de tweede is het onschadelijk maken van deze malware. Dit hoofdstuk beschrijft hoe anti-virus software op dit moment deze taken uitvoert en in het kort wat er op dit moment nog fout gaat.

## Detectie

Voordat anti-virus software iets tegen malware kan doen, moet het de malware eerst vinden. We onderscheiden twee soorten bescherming: Reactieve bescherming wordt toegepast nadat het bestand al op de computer staat.
De beste bescherming van de computer vindt plaats op het moment dat malware gevonden wordt, vóór het de kans krijgt actief te worden op de computer waar het naar toe is verzonden. Dit wordt ook wel pro-actieve bescherming genoemd. Hieronder worden beide vormen besproken. [25]

### Reactief

Reactieve bescherming vindt plaats bij virusscans, maar ook bij virussen die proberen de computer te infecteren. Wat het detecteren reactief maakt, is dat het alleen werkt op virussen die al bekend zijn. De eerste manier waarop dit gebeurt is met behulp van een “handtekening”, in het Engels signature genoemd. Deze handtekening bestaat uit een enkele regel bits uit de malware, die wordt opgeslagen in een database. Bij de controle van een bestand wordt dit bestand vergeleken met alle handtekeningen in de database. Als een van de handtekeningen overeenkomt, wordt het bestand aangemerkt als malware en krijgt de gebruiker een waarschuwing om actie te ondernemen. Deze methode wordt toegepast zowel bij virusscans, als op het moment dat een bestand wordt gedownload vanaf internet of via een e-mail. Het nadeel hiervan is, dat de malware al bekend moet zijn voordat het gevonden kan worden. Zodra er een nieuw virus kwam en bekend werd bij een aantal experts, werd het virus geanalyseerd en werd de digitale handtekening opgesteld. Vroeger werkte dit redelijk goed, omdat virussen nog niet zo snel verspreidden. De experts hadden vaak de handtekening al geanalyseerd voordat het virus ver verspreid kon worden en gebruikers die hun anti-virus programma regelmatig updaten hadden dus nergens last van. Met de komst van wormen en andere manieren om virussen verder te verspreiden kan deze mogelijkheid achterhaald zijn, omdat er te snel nieuwe malware bij komt.
Een andere soortgelijke methode werd rond dezelfde tijd (en nu nog steeds) gebruikt. Het is een variatie op de vorige methode die ook nieuwe virussen moest kunnen identificeren. Dit wordt gedaan aan de hand van de handtekeningen, alleen wordt er nu niet gekeken naar overeenkomende handtekeningen, maar via handige heuristieken wordt gezocht naar stukken van de handtekening die overeenkomen. Als er maar genoeg bits overeenkomen met die van al bekende malware, wordt er een waarschuwing gegeven dat een bepaald bestand mogelijk malware kan zijn. Het nadeel is, dat niet alle bestanden die volgens deze heuristiek als malware worden aangeduid, dit ook echt zijn. Een gebruiker met weinig verstand van computers zou zonder na te denken een goed of belangrijk bestand kunnen

verwijderen en er vervolgens achter komen dat een programma, of zelfs het hele besturingssysteem niet meer werkt. [25][26][27] Met deze methodes kunnen virussen, wormen, en spyware worden gevonden. Hierbij horen dus ook de trojaanse paarden die alleen maar verhulde andere malware is, maar ook keyloggers en de programma's die backdoors veroorzaken. Men moet er rekening mee houden, dat de gevolgen van zo'n backdoor (bijvoorbeeld het open zetten van een poort) door het verwijderen van het bestand meestal niet ongedaan wordt gemaakt. Bots en rootkits kunnen op die manier niet altijd worden gevonden. Meestal worden er voor deze twee daarom andere methodes gebruikt.
Uit de definitie van een rootkit volgt, dat rootkits zich bezig houden met het verhullen van processen, geheugen en andere componenten van de computer. Daarom is er een methode, om naar het gedrag van een rootkit te kijken.
Er worden twee verschillende aanvragen gedaan naar dezelfde informatie, bijvoorbeeld : "Wat staat er op dit moment in het geheugen. Beide aanvragen worden op een andere manier uitgevoerd. Zo kan de ene lokaal worden uitgevoerd en de andere vanaf een andere computer. Allebei zouden ze dezelfde informatie op moeten leveren, maar als de antwoorden op de aanvragen niet gelijk zijn zou dit kunnen betekenen dat er een rootkit actief is. Deze methode is niet exact en kan soms niet exact aangeven of een rootkit actief is of niet. Er kunnen ook valse positieven optreden, waardoor iets wordt aangemerkt als een rootkit terwijl het dat helemaal niet is. Een ander probleem is dat veel tools rootkits wel kunnen ontdekken, maar niet kunnen verwijderen door de manier waarop ze zich binnen het besturingssysteem genesteld hebben.[28][29]
Ook bots/botnets kunnen niet altijd goed worden geidentificeerd aan de hand van hun handtekening, door de manier waarop ze in elkaar zitten. Maar voor bots zijn er ook nog andere manieren om ze te ontdekken, nadat ze zich al op de computer hebben gevestigd. Een manier hiervoor is om te kijken naar netwerk en/of computer activiteit. Doordat bots contact hebben met meestal IRC servers zullen zij voor netwerk activiteit zorgen. Als deze netwerk activiteit niet door iets anders verklaard kan worden, bijvoorbeeld doordat er verder geen programma's actief zijn kan dit wijzen op een bot. Ook processor activiteit terwijl er verder niets uitgevoerd wordt kan wijzen op een bot die bezig is, maar er kunnen ook andere (ongewenste) activiteiten bezig zijn. Deze methodes zijn dan ook niet geweldig om bots te vinden, maar in combinatie met handtekening herkenning is de detectie van bots toch redelijk. [30][31]

### Proactief

Met proactieve bescherming bedoelen wij, dat tot nu toe onbekende virussen kunnen worden gevonden. In de huidige tijd waarin via internet redelijk makkelijk nieuwe malware kan worden verspreid, kan zo'n bescherming zeer gewenst zijn. De manier waarop dat op dit moment het meest wordt gedaan is gedragsherkenning. Bij deze methode observeert het programma gedrag van andere bestanden, programma's en processen op de computer en vergelijkt dit met het beveiligingsbeleid van de computer. Zo hebben bepaalde programma's toestemming om nieuwe processen te creeeren en andere zullen dat niet hebben. Door te kijken wat er gebeurt kan een programma dat illegaal nieuwe programma's maakt, gestopt of zelfs verwijderd worden. Hoewel deze methode goed werkt bij nog onbekende malware zitten er ook nadelen aan. Zo moet malware eerst op de computer actief zijn voor ongewenst gedrag gespot kan worden. Een manier om dit probleem op te lossen is om die bestanden die gecontroleerd moeten worden, eerst uit te voeren in een virtuele omgeving. Op die manier kan

malware niet echt schade toebrengen aan een computer, maar kan er wel worden geobserveerd wat het gedrag van dat bestand is. Een ander nadeel van deze methode is dat er een redelijke kans op valse positieven zijn. Sommige bestanden zullen nou eenmaal processen maken of mailtjes versturen, omdat ze daarvoor gemaakt zijn. Een anti-virus programma kan als reactie hierop een waarschuwing geven en de gebruiker vragen actie te ondernemen. Een gebruiker die weinig verstand heeft van computers en virussen zou zonder na te denken een goed werkend programma kunnen verwijderen.[27][32]

Zoals al eerder gezien onder het kopje reactief, is gedragsherkenning ook een goede manier om bots te herkennen. Alleen wordt er bij botherkenning vooral gekregen naar dat wat veroorzaakt wordt (internet en CPU acitiviteit) en niet naar de oorzaak zelf (de bot). Ook bij rootkits kan gedragsherkenning lastig zijn, juist doordat een rootkit het gedrag van iets kan maskeren. Om toch via gedragsherkenning de rootkit zelf te vinden kan het handig zijn om naar verborgen bestanden en processen te zoeken. Juist als er veel van deze gevonden worden, of wanneer er verborgen processen gevonden worden die niet verborgen hadden moeten zijn kan dit wijzen op een rootkit. Ook bij deze methode geldt echter, dat er veel valse positieven gevonden kunnen worden en zelfs als het een rootkit is, is met deze methode nog niet aan te tonen waar die zit of hoe deze onschadelijk gemaakt zou kunnen worden. [17]

### Onschadelijk maken

Nadat de software malware heeft ontdekt, moet er ook nog wat mee worden gedaan. Tenslotte is het malware die we niet op onze computer willen hebben. De meeste anti-virus software geeft verschillende opties als malware is gevonden op het moment dat het bestand binnenkomt of later tijdens een volledige scan van de computer. Deze bestaan uit de optie “clean” , schoonmaken, de optie “delete”, verwijderen, “quarantine”, in quarantaine plaatsen of soms “ignore”, negeren. Niet alle opties zijn even geschikt en daarom is het niet verstandig om altijd dezelfde actie uit te voeren. Wat houdt elke actie in en voor welke soorten malware is hij geschikt?

De laatste optie is misschien de meest voor de hand liggende. Wanneer er wordt gekozen voor negeren, wordt er niets met het geinfecteerde bestand gedaan. Tenzij de gebruiker zeker weet dat het een false positive is, of dat hij het risico wilt nemen om het bestand te gebruiken is dit geen verstandige optie, omdat het malware de kans geeft te verspreiden en zijn werk te doen. Dit geldt voor elke soort malware die werd gevonden.

De tweede, redelijk extreme optie is verwijderen. Zodra er voor verwijderen wordt gekozen, wordt het hele bestand van de computer verwijderd, waarbij het ook niet langs de prullenbak gaat. Opnieuw geldt, zolang een gebruiker zeker weet wat het bestand is en dat het niet nodig is, kan men zonder problemen voor deze optie kiezen. Maar in het geval dat het een false positive is, wordt een niet geinfecteerd bestand weggehaald, of in het geval dat het een essentieel bestand was voor bepaalde software, kan het zijn dat deze software niet meer functioneert. Soms betekent dit dat het besturingssysteem zelfs niet meer opstart. Ook deze optie kan altijd en op elke soort malware worden uitgevoerd, tenzij de malware zelf iets heeft ingebouwd waardoor het niet verwijderd kan worden. In dat geval is het soms nodig om het handmatig te verwijderen.

De derde optie is quarantaine. Bij deze optie wordt ook het hele bestand weggehaald, maar niet van de computer verwijderd. In plaats daarvan wordt het op een afgezonderde plek neergezet waar het geen schade kan doen en ook geen verbinding heeft met het netwerk. Hier blijft het staan totdat de gebruiker er verder iets mee doet. Dit is een goede manier wanneer niet zeker is of iets een false positive is en of een bestand echt nodig is. Als men na een paar weken nog eens de lijst bekijkt met de bestanden die in

quarantaine staan, kan besloten worden alsnog bestanden te verwijderen en andere bestanden misschien terug te halen. Deze methode werkt prima bij de meeste malware. Soms kan een bestand echter niet worden verplaatst, bijvoorbeeld door ingebouwde beveiling in de malware.

De eerste optie is schoonmaken. Hoewel dit de meest gewenste is, kan hij niet altijd worden uitgevoerd en ook niet elke anti-virus software biedt deze mogelijkheid. Bij clean wordt er geprobeerd om alleen de slechte code uit een bestand te verwijderen. Bij virussen die altijd een ander bestand moeten infecteren om te verspreiden gaat dit vaak goed, maar bij wormen, die op zichzelfstaande programma's zijn, maar ook bij bots, keyloggers en andere malware die niets anders infecteren, is schoonmaken meestal geen optie. Dit is waarschijnlijk ook de reden dat de meeste moderne anti-virus software dit niet meer als optie laten zien.

Het is vaak mogelijk om binnen antivirus software aan te geven dat altijd dezelfde actie moet worden uitegevoerd bij een gevonden virus. Het blijkt echter dat dit niet verstandig is, omdat het verwijderen van een bestand altijd tot problemen kan lijden en zeker vervelend is bij een false positive. Eigenlijk zou een gebruiker elke gevonden infectie apart moeten bekijken, liefst de naam van de malware opzoeken op internet en aan de hand daarvan een keus maken. Wat gebruikers werkelijk doen, komt in het volgende hoofdstuk aan bod. [33][34]

### Nieuwe methodes

Er wordt altijd gezocht naar andere methodes om computers te beveiligen en één van deze methodes willen we hier nog noemen. Het gaat om een bedrijf met de naam tripwire die zich specialiseert in data beveiliging. Hun methode berust niet op traditionele antivirus software, maar ze maken gebruiken van real time data controle. Hoewel het hele pakket van van tripwire allerlei methodes gebruikt om data te beveiligen, is voor ons de meest interessante die waarbij de data continu vergeleken wordt. Er wordt niet precies verteld hoe de methode werkt, maar wel dat elke verandering die op de computer wordt aangebracht, bijgehouden wordt. Elk nieuw bestand dat binnenkoment, maar ook elke verandering in de configuratie, zoals toegang die wel of niet verleend wordt of processen die starten, wordt gecontroleerd. Als het enigzins gevaarlijk of verdacht lijkt, wordt er een melding uitgedaan naar een gebruiker die kan bepalen of de verandering plaats had mogen vinden. Op deze manier wordt er niet alleen beschermd tegen aanvallen van buitenaf, maar ook aanvallen die mogelijk vanuit het bedrijf zelf komen. Wij spreken over bedrijf, omdat op dit moment deze methodes nog niet goed werken voor particulier gebruik. Om het goed te laten werken is er iemand nodig die redelijk veel verstand heeft van computers. De gemiddelde computergebruiker heeft niet de benodigde kennis over processen en toegangsrechten om dit systeem succesvol te gebruiken. Toch kan het misschien een mogelijkheid zijn voor de toekomst als hier nog verder onderzoek naar gedaan wordt. [36]

# 3 – Wordt anti-virus software goed gebruikt?

De eerste twee hoofdstukken waren bedoeld om kennis te verkrijgen over wat malware is en hoe antivirus software er tegen optreedt. Met deze kennis is het makkelijker om te bedenken dat voor alle antivirus software altijd de updates gedownload moeten worden en wat je moet doen bij een viruswaarschuwing of aan het einde van een computerscan. Wij vermoeden dat de gemiddelde computergebruiker niet goed op de hoogte is van deze informatie. Omdat deze scriptie de vraag beantwoordt in hoeverre antivirus software goed werkt bij correct gebruik van deze software, vinden we het ook belangrijk om uit te vinden hoeveel mensen hun antivirus software ook werkelijk goed gebruiken en wat zij weten over malware en hun antivirus software. Om dit te kunnen onderzoeken hebben we een enquête gemaakt. Deze enquête is te vinden in de bijlagen van deze scriptie en de resultaten zijn hieronder gepresenteerd en geanalyseerd.

## Methode

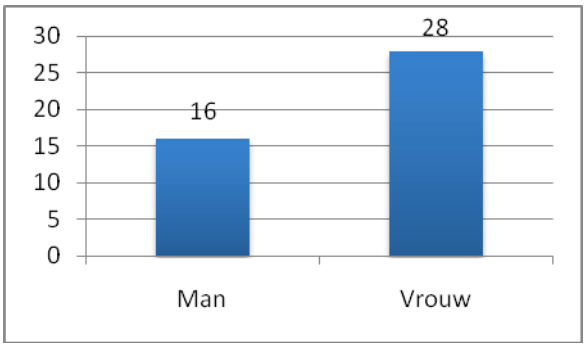
Om een goede enquete te krijgen is de enquete in twee stappen gemaakt. De eerste versie is verspreid onder mensen bij ons in de buurt, simpelweg om te kijken of de vragen goed werden begrepen en goed beantwoord werden en of er informatie miste of niet. Aan de hand hiervan is de enquête aangepast tot de huidige versie die vervolgens is verspreid.

Om te zorgen dat de uitslag slaat op de gemiddelde computergebruiker is de enquête verspreid onder mensen van alle leeftijden, zowel mannen als vrouwen. Wij verwachten dat sommige van hen meer kennis over het onderwerp zullen hebben dan anderen, daardoor kunnen wij bij voldoende respons een gemiddelde zien. De enquête is verspreid via internet, omdat mensen die antivirus software gebruiken ook het internet zullen gebruiken. Ook is de enquête verspreid onder klanten van een bedrijf dat mensen helpt bij computerproblemen. Dit lijkt misschien een slechte keus, omdat er zo een bepaalde groep mensen wordt aangesproken, maar de problemen die deze mensen hebben zijn altijd heel divers, waarbij uit ervaring blijkt dat sommige echt meer kennis hebben over hun computer dan anderen. Daarbij verwachten wij in combinatie met de respons van de mensen op internet een realistisch beeld van de kennis over antivirus software van de gemiddelde computergebruiker te krijgen.

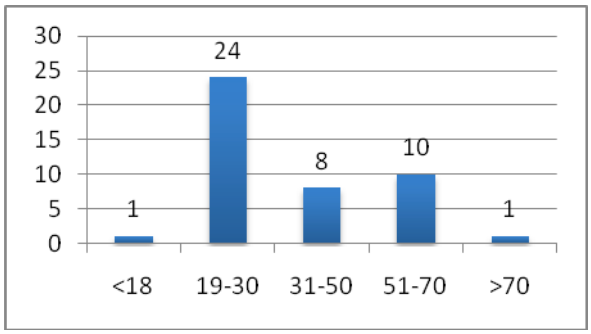
Belangrijk is nog de definitie van goed gebruik. Wij willen onderzoeken of computergebruikers hun antivirus software goed gebruiken. Wat we hiermee bedoelen is dat de gebruikers zorgen dat deze altijd de laatste versie van hun antivirus software hebben. Dat ze zorgen dat ze altijd de laatste updates van het antivirus software op de computer hebben staan en dat ze genoeg kennis hebben om te weten wat een viruswaarschuwing inhoudt, wat de verschillende opties doen en welke het beste gebruikt kan worden in bepaalde situaties. Alleen in dat geval kan er effectief opgetreden worden tegen malware.

## Resultaten

De eerste twee vragen zijn alleen vragen om te kijken of de enquete verspreid is geweest onder voldoende verschillende mensen. Hiervoor hebben wij gekeken naar geslacht en leeftijd. Onderstaande grafieken geven de verdeling weer. In totaal hebben 44 mensen de enquete ingevuld.



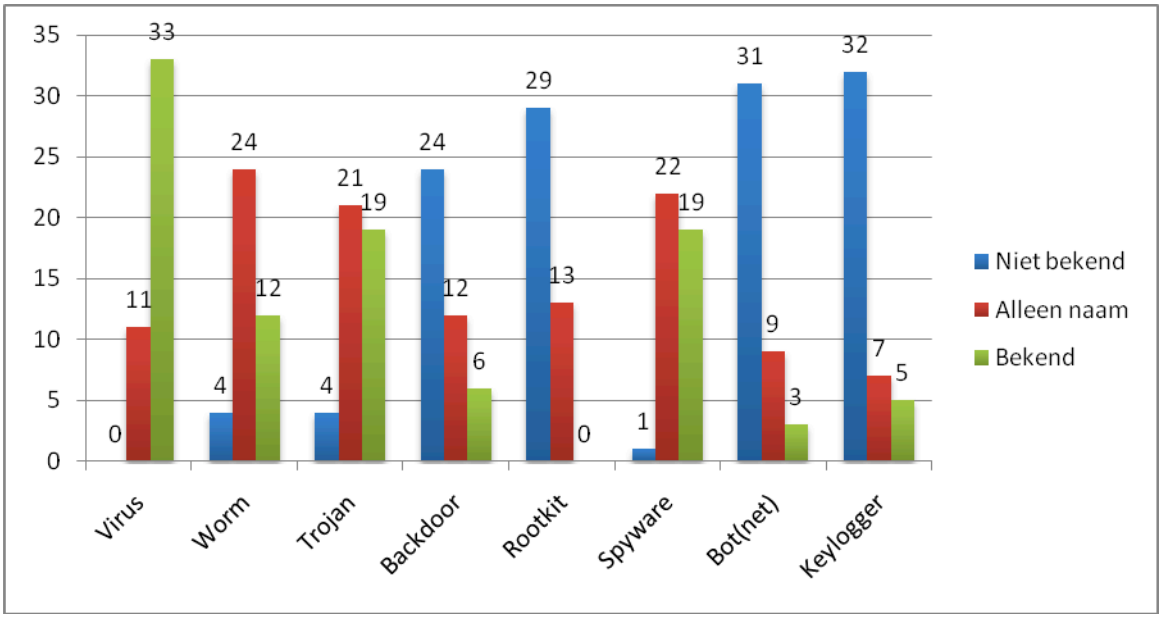

Figuur 1.




Figuur 2.

Zoals te zien is, hebben meer vrouwen de enquete ingevuld dan mannen. Dit kwam doordat in een gezin zowel de man als de vrouw de computer gebruiken en de vrouwen meer zin hadden om mee te werken aan het onderzoek dan mannen. Bij de leeftijd is er een piek bij 19-30 jaar. We vermoeden dat dit komt, omdat door deze leeftijdscategorie de computer het meest wordt gebruikt. Natuurlijk wordt onder de 18 jaar de computer ook veel gebruikt, maar we vermoeden dat dit meer is voor het spelen van spellen, dan voor het invullen van enquetes of het bezighouden met problemen zoals malware. Hoe dan ook is de spreiding groot genoeg om de enquete representatief te maken voor de gemiddelde gebruiker.

Bij de volgende vraag hebben we bekeken hoe bekend de verschillende types malware zijn. In eerste instantie hebben we mensen laten aangeven of ze de naam van een bepaald type malware kennen en zo ja, of ze weten wat het doet. Als er aangegeven werd dat ze precies wisten wat het was, wilden we dat bevestigd hebben door een korte omschrijving. In onderstaande grafiek, figuur 3, is de verdeling te zien.

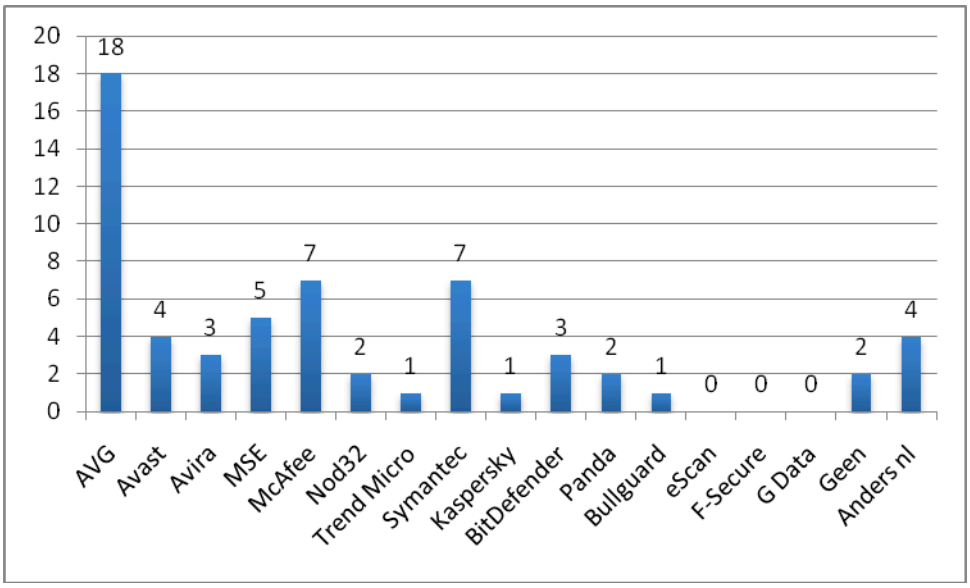



Figuur 3. (Welke soorten malware kent u?)

Figuur 3 laat zowel opvallende als verwachte resultaten zien. De vier soorten malware: Virus, Worm, Trojan en Spyware zijn het meest bekend. Er zijn meer mensen die deze vier van naam kennen of

helemaal kennen dan mensen die er nog nooit van hebben gehoord. Zoals verwacht zijn er maar weinig mensen die van een backdoor, rootkit, bot of keylogger gehoord hebben. Toch laten de getallen hier een fout beeld zien. Zoals gezegd moesten de ondervraagden ook invullen wat ze dachten dat een bepaald type malware was als ze aangaven te weten wat het was. Hier zijn opvallende uitspraken gedaan. Sommige uitspraken bij “Wat is een virus?” zijn heel erg algemeen, zoals : “Iets wat je computer beschadigd” en “Iets dat je computer aantast”. Dit soort uitspraken geven voor ons aan dat men weet dat het slecht voor de computer is, maar daar houdt het ook op. Vervelender zijn uitspraken van mensen die denken te weten wat een virus is, maar het eigenlijk helemaal niet weten. Mensen zeggen bijvoorbeeld: “Een programma dat zichzelf doorstuurt.” Of “Een programma dat bestanden van je computer verwijderd en zich “automatisch” verspreid.” Ook zijn veel mensen het erover eens dat een virus een programma is wat er puur voor zorgt dat andere programma’s niet meer werken. Deze reacties zijn voor ons teleurstellend, omdat we in ieder geval nog had gehoopt dat mensen wisten wat een virus was, ook al kenden ze misschien de andere soorten malware niet. Maar behalve dat het schade aan de computer brengt was er  maar één iemand die wist dat een virus alleen door mensen zelf verspreid kan worden.
Het was nog erger bij de uitleg die gegeven werd bij de worm en Trojan. Beide werden vaak benoemd als “Een virus dat…”. Hieruit blijkt, dat veel mensen denken dat de andere soorten malware vormen zijn van een virus, terwijl ze eigenlijk iets totaal anders zijn. Er kwam zelfs een reactie dat een worm een synoniem zou zijn voor virus. Toch moeten we concluderen dat de Trojan bekender is dan een worm. Dit blijkt niet alleen uit de aantallen, maar ook uit het feit dat er reacties kwamen dat een Trojan met andere bestanden meekwam of “eruit ziet als een gewoon word bestand.” Natuurlijk zit er veel meer achter, maar toch lijken mensen een idee te hebben van wat een Trojan is. Bij de overige vormen van malware geven mensen eerlijk aan niet te weten wat het is, of het zelfs nog nooit te hebben gehoord. De enkeling die hier aangeeft precies te weten wat het is, geeft ook de goede omschrijving, waardoor wij vermoeden dat van de 44 mensen die deze enquete hebben ingevuld, ongeveer 3 mensen echt verstand hebben van de verschillende soorten malware. De rest denkt voornamelijk te weten wat het is, maar heeft eigenlijk geen idee. Vooral bij spyware blijken veel mensen te denken dat cookies onder spyware vallen en dat ze cookies zien als een inbreuk op hun privacy.

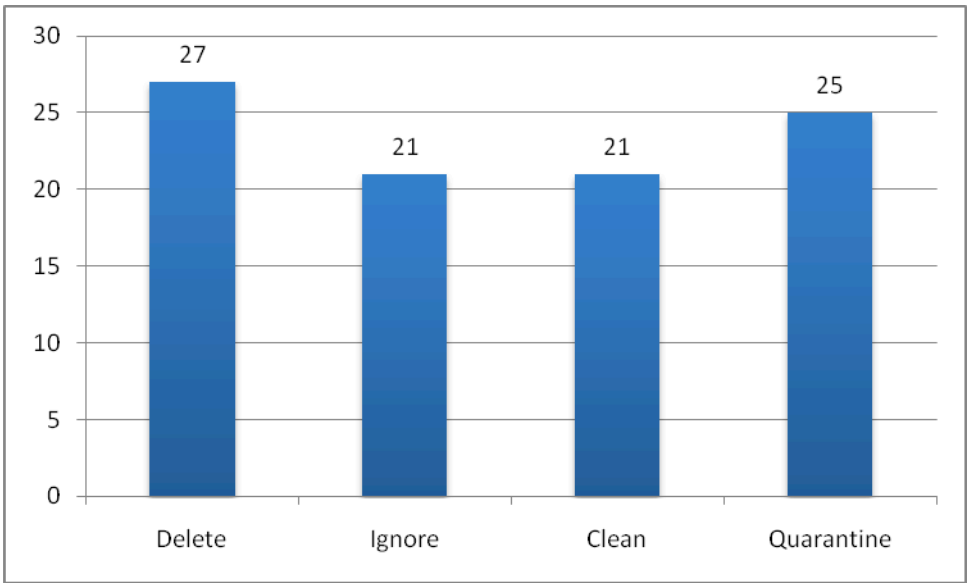
Naast weten wat mensen van malware weten, wilden we ook weten wat zij over antivirus software wisten. Onze eerste vraag hierbij was welke software paketten door deze mensen zelf werden gebruikt. We hebben namelijk bij ons onderzoek een aanname gemaakt dat AVG de meestgebruikte gratis antivirus software is en dit wilden we bevestigd zien. Onderstaand figuur 4 geeft de verdeling weer.



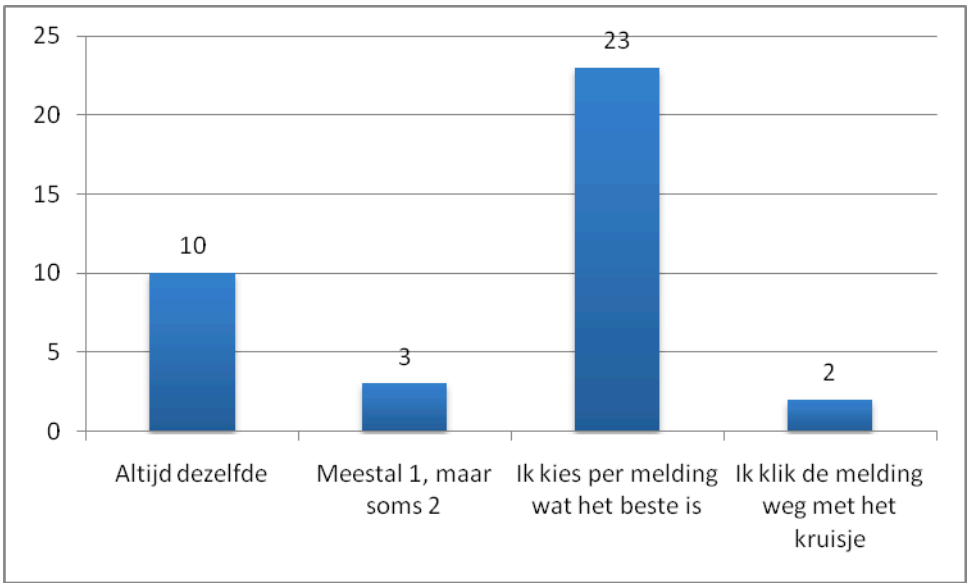
Figuur 4 (Welke antivirus software paketten gebruikt u?)

Het totaal aantal bij deze vraag komt uit op 60, wat betekent dat sommige mensen de vraag niet helemaal goed hebben gelezen en alle antivirussoftware hebben aangeklikt die ze gebruiken in plaats van alleen die ze het meest gebruiken. Toch laat figuur 4 zien dat AVG inderdaad de meest gebruikte antivirus software is. Ook McAfee wordt veel gebruikt, vermoedelijk omdat die ooit genoteerd stond als de beste antivirus software, en zoals verwacht staat Symantec van Norton op een gedeelde tweede plek. Hier zijn geen onverwachte uitkomsten bij, behalve dat bij anders “CCleaner” genoemd werd, wat helemaal geen antivirus software is.

De volgende vragen gaan over wat mensen doen bij een viruswaarschuwing of aan het einde van een virusscan. Om te weten op welke opties mensen klikken, hebben we eerst gevraagd welke opties er worden weergegeven, daarna welke optie ze meestal kiezen en als laatste hebben we gevraagd of ze kunnen vertellen wat ze denken dat elke optie betekent. De volgende figuren 5 en 6 laten de eerste twee antwoorden in grafiek zien.



Figuur 5 (Welke opties heeft jou antivirus software?)

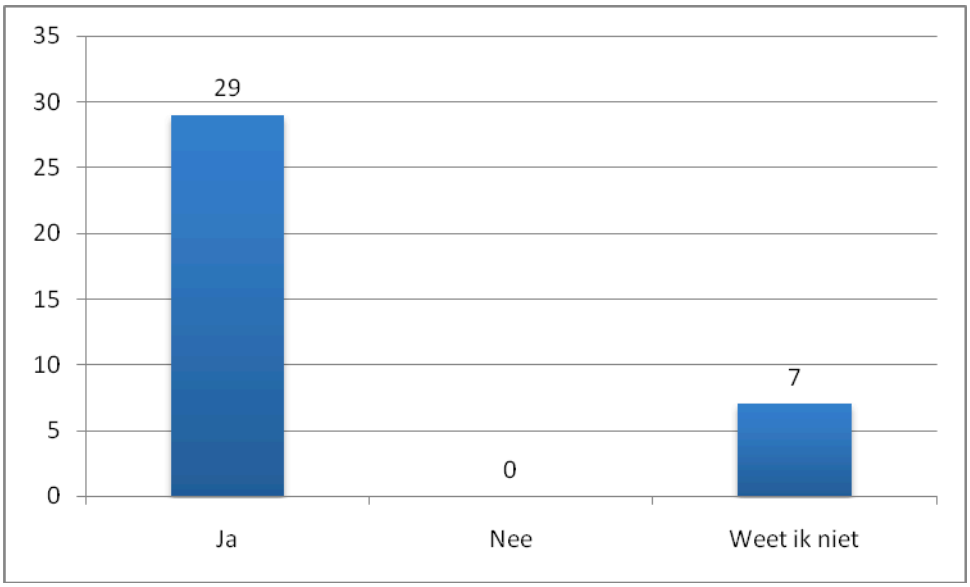


Figuur 6 (Welke optie kies je bij een viruswaarschuwing?)

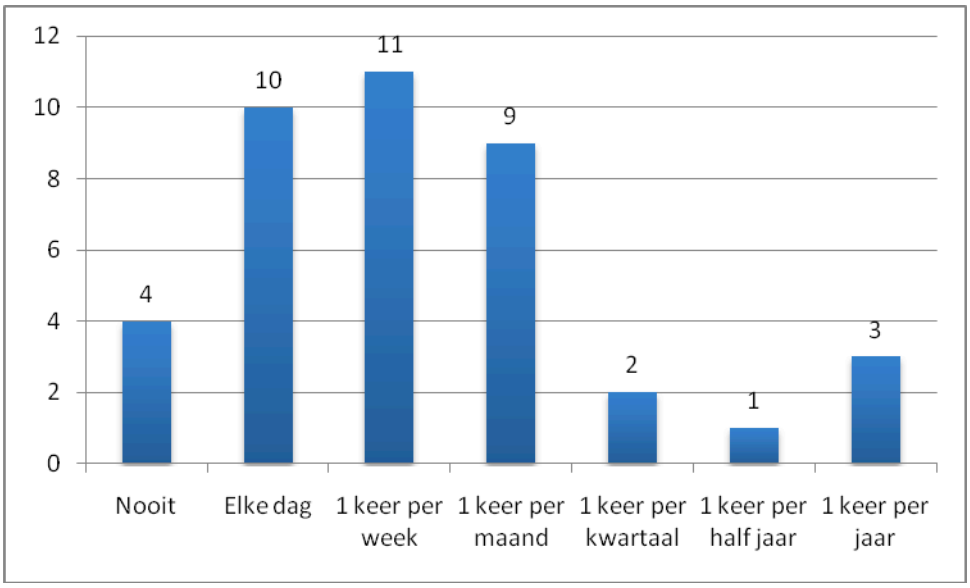
In figuur 5 is te zien dat de meeste antivirus software paketten ongeveer dezelfde opties laten zien. Oorspronkelijk was er ook de optie “anders” maar bij geen van de ondervraagden werd er nog een andere optie weergegeven. Opvallend is, dat de meeste mensen, ondanks dat ze van de meeste typen malware geen idee hebben wat het is, toch aangeven per melding de beste optie te kiezen. Daar waar altijd dezelfde wordt gekozen gaat het in ongeveer 60% van de gevallen om de “delete” optie en in de andere 40% van de gevallen om quarantaine. Om te kijken of mensen echt per melding de beste optie konden kiezen, hebben we gevraagd of ze weten wat elke optie doet. De antwoorden op deze vraag hebben ons verrast. De meeste mensen wisten wel dat bij verwijderen het hele bestand wordt verwijderd en dat bij de optie negeren er helemaal niets gebeurd. De meest interessante waren dan ook de opties schoonmaken en quarantaine. Bij de optie schoonmaken bleken maar weinig mensen te weten wat deze doet. Er kwamen reacties zoals “Hierbij wordt het verwijderd” Soms met een

toevoeging zoals “Het wordt zo verwijderd, maar dan dieper dan bij verwijderen”. Ook waren er reacties zoals “De geschiedenislijst van je virusscanner wordt leeggehaald” en “blijft op zijn plaats zonder werkzaam te zijn”. Zes van de ondervraagden gaven aan te weten dat het bij schoonmaken gaat om enkel het verwijderen van de virus code uit de rest van het bestand. Bij quarantaine leken meer mensen te weten wat er gebeurt. De reactie dat “het bestand in een apart mapje wordt gezet, om later nog eens naar terug te keren” kwam bij 70% van de ondervraagden terug. Andere reacties bestonden uit “Er gebeurt niets bij quarantine” of “Ik heb geen idee”. Helaas zijn er dus ook nog mensen die dit soort meldingen gewoon wegklikken zonder er verder iets mee te doen. Er zat zelfs een reactie bij van iemand die bang was om ook maar een van functies aan te klikken voor het geval dit de computer zou beschadigen.

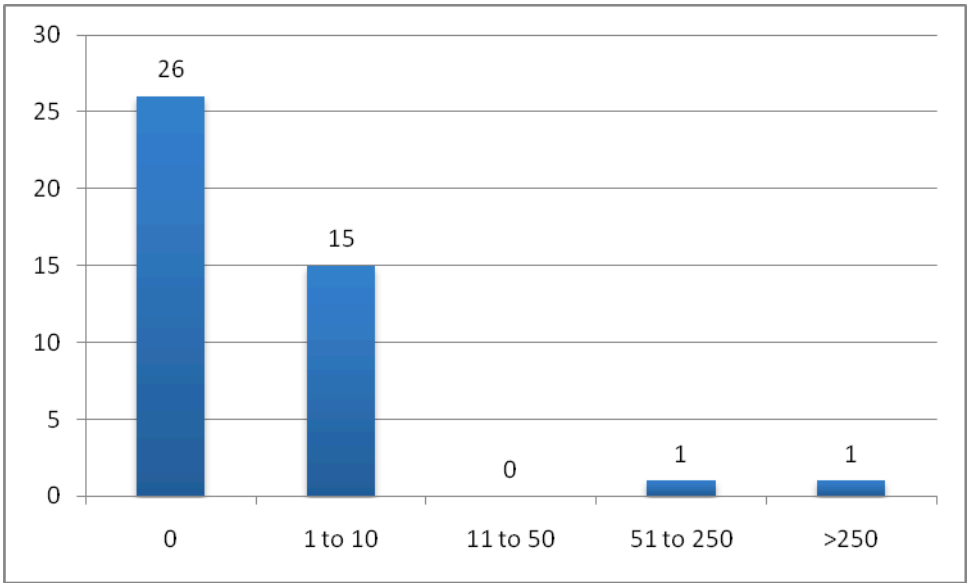
Een laatste belangrijk punt om te weten hoe mensen met hun antivirus software omgaan is hun gedrag wat betreft updates en virusscans. De onderstaande figuren geven het gedrag van mensen betreffende deze punten weer.



Figuur 7 (Is uw antivirus software up to date?)




Figuur 8 (Hoe vaak voert u een computer scan uit?)




Figuur 9 (Hoeveel infecties werden er bij uw laatste scan gevonden?)

De gegevens laten zien dat de meeste mensen hun zaken behoorlijk goed op orde hebben. De software is up to date, er wordt minimaal een keer per maand of vaker gescand en er worden maar weinig infecties gevonden op de computer. Dit laatste zegt vooral iets over de software zelf. Het is belangrijk om te onthouden dat het aantal infecties wat bij een gebruiker gevonden kan worden ook afhangt van het surf gedrag van de gebruiker. Zo zal iemand die veel download en surft vaker iets binnenhalen dan iemand die bijna nooit op de computer zit. Het zou dan ook interessant zijn geweest om te vragen hoe vaak iemand gebruik maakt van zijn computer en hoe vaak iemand achter internet zit, maar we wilden de focus leggen op de kennis die iemand heeft over malware. Toch zijn er interessante verbanden te zien. De twee mensen waarbij wel veel malware werden gevonden zijn dezelfde mensen die maar een keer per jaar een scan uitvoeren. Het lijkt er dus op dat er wel degelijk redelijk wat malware in een jaar

wordt binnen gehaald, maar door vaak te scannen lijkt het mee te vallen, omdat er vaak niets of maar een beetje wordt gevonden op dat moment. Naar deze verschijnselen zouden nog andere interessante onderzoeken gedaan kunnen worden. Bijvoorbeeld een jaar lang van verschillende mensen bijhouden wat bij elke scan gevonden wordt. Hiervoor hadden we echter geen tijd. Ook hebben we gevraagd of mensen weten waar updates bij hun antivirus software voor dienen. Ongeveer de helft van alle mensen kon ons vertellen dat updates waren om te zorgen dat nieuwe malware herkend kon worden. De andere helft kwam niet verder dan "zorgen dat het programma up to date blijft". De laatste groep bevatte ook de mensen die aangaven niet te weten of hun antivirus software geupdate was of niet.

## Informeel

Tijdens dit onderzoek hebben we met veel mensen over dit onderzoek gesproken. Niet in alle gevallen hadden we de mogelijkheid om de enquête voor te leggen, maar toch wilden we graag eens informeel vragen wat zij wisten over hun antivirus software en malware in het algemeen. Een veelvoorkomend problem wat we helaas niet met onze enquête hebben kunnen aantonen, is het wisselen van versie van antivirus software. Hoewel bekend was dat updates nodig waren voor de software en dat deze vaak automatisch worden uitgevoerd, was soms niet bekend dat een versie verouderd was. Bij veel mensen waar we kwamen was er AVG geinstalleerd, maar dit was meestal versie 8.0 of 9.0 terwijl de nieuwste versie AVG 10.0 is. De oudere versies ontvangen geen database updates meer, waardoor ze niet zo goed werken als de nieuwste versie. De mensen waren erg verrast toen we vertelden dat hun antivirus software niet goed was, omdat men ervan overtuigd waren dat als er maar antivirus software op de computer staat, het genoeg is om beschermd te zijn.  Ook kregen we vaak te horen: "Maar hij doet die updates toch automatisch?" Normaal klopt dit, maar niet als er een hele nieuwe versie uitkomt die zeker niet altijd automatisch gedownload wordt. De mensen aan wie we de enquête alsnog voorlegde en die erover gingen nadenken bleken er toch meer over te weten dan ze dachten. Bij een eerste vraag over de verschillende opties, bijvoorbeeld wat quarantaine betekende wisten de meeste mensen het niet, totdat ze even de tijd namen om na te denken wat quarantaine zou kunnen betekenen. Dit heeft bij ons de vraag opgeroepen of de antwoorden die gegeven zijn in de enquete gelijk is aan de kennis die mensen hebben op het moment dat ze een virusmelding binnen krijgen, of dat die kennis alleen bovenkwam omdat mensen gingen nadenken over de vragen. Helaas hebben we hier geen verder onderzoek naar kunnen doen en moeten we aannemen dat de antwoorden in de enquete kloppen met de werkelijkheid. Ook hebben we informeel rondgevraagd of er wel eens problemen optraden na het verwijderen van gevonden bestanden. We hebben verschillende verhalen gehoord waarbij programma's niet meer werkten, of soms zelfs de computer niet meer opstartte. Dit soort problemen kunnen ook voorkomen bij het verplaatsen naar quarantaine, alleen is het bestand dan makkelijker terug te halen. Altijd verwijderen kiezen is dus slim tegen malware, maar wil nog niet zeggen dat het ook de beste optie voor de computer is. Opnieuw is dit echter iets waar nader onderzoek naar gedaan zou kunnen worden, maar waar we hier geen tijd voor hadden.

## Conclusie

Het doel van de enquete was om uit te vinden was computergebruikers wisten over malware en of zij hun antivirus software correct gebruiken. Hun kennis blijkt verdeeld. Van alle ondervraagden was er maar één die een kloppende beschrijving gaf van de verschillende soorten malware en de rest komt niet verder dan te weten dat een virus schade toebrengt en gaat er verder vanuit dat elk type wat werd genoemd allemaal een virus is. Sommigen wisten iets meer dan anderen, maar over het algemeen kan gesteld worden dat de gemiddelde computergebruiker de verschillende types malware kan onderscheiden.

De vraag blijft wel of deze kennis noodzakelijk is voor goede antimalware bescherming. Gezien de resultaten worden er op de meeste computers maar weinig infecties gevonden, hoewel dit dan wel bij een wekelijke of maandelijkse scan is. Ook weet de meerderheid wel waar updates voor zijn en voert deze dan ook uit. Zelfs de kennis over wat de verschillende opties doen bij antivirus software is redelijk goed aanwezig, maar toch lost dit enkele vragen nog niet helemaal op. Hoe is het bijvoorbeeld mogelijk om per infectie de beste oplossing te kiezen als niet eens bekend is wat voor malware het is? Of als je aan het bestand niet kan zien of iets wel of geen malware is? Op dit punt kan de gebruiker naar ons idee nog meer doen om malware infecties tegen te gaan. De infectie teller bij de verschillende antivirus scans moeten uiteindelijk allemaal naar nul en hoe meer mensen hier aan meewerken, hoe makkelijker het gaat.

# 4 – Werkt anti-virus software bij goed gebruik?

Inmiddels hebben we vastgesteld welke verschillende soorten malware er zijn en hoe antivirus software werkt. Ook hebben we gezien wat een gemiddelde computergebruiker weet over malware en antivirus software. Om echter goed te kunnen zeggen of huidige antivirus software goed genoeg werkt tegen alle malware van deze tijd is het misschien wel het meest belangrijk om te kijken naar hoe goed antivirus software werkt als deze goed wordt gebruikt. Als hoofdonderzoek van deze scriptie is er dan ook onderzoek gedaan naar de werking van antivirus software, wanneer deze goed wordt gebruikt. Dat wil zeggen, wanneer men weet welke acties uitgevoerd moeten worden om malware op te ruimen en dat altijd alle updates geinstalleerd zijn, zowel als de laatste versie van de antivirus software.

## Methode

Om te onderzoeken of antivirus software goed werkt tegen huidige malware is het onderzoek in twee delen gesplitst. In het eerste deel is er gezocht op internet naar websites die malware bevatten en op de computer probeert te zetten om een vaste route over het net vast te stellen waarbij malware wordt binnengehaald. Bij het tweede deel van het onderzoek wordt gebruik gemaakt van drie verschillende antivirus software paketten die vervolgens op twee verschillende manieren op deze route worden getest. In onderstaande paragrafen zal elk deelonderzoek in detail worden uitgelegd.

Beide delen van het onderzoek worden uitgevoerd op een virtuele pc binnen een macbook pro. Op deze manier kan de malware zonder gevaar voor de host computer binnen worden gehaald en kan de pc gemakkelijk voor elk onderzoek weer worden schoongemaakt, door een snapshot die gemaakt is van de virtuele machine voordat er enige virussen worden binnengehaald.

### Malware verzamelen

Het is erg lastig om aan malware te komen voor een onderzoek als deze. Aangezien het illegaal is om malware te verspreiden is er nergens een plek op het internet waar "testsets" gedownload kunnen worden. Ook makers van antivirus software zijn niet bereid om malware te geven voor een onderzoek als deze. Hoewel dit begrijpelijk is maakte dit het lastig om het onderzoek goed uit te kunnen voeren. Als alternatief is de oplossing gevonden om handmatig websites af te gaan die op malware blacklists staan. Ook zijn dit soort websites te vinden, door met geactiveerde antivirus software websites te bezoeken (zoals crack and serial websites), waarbij het antivirus programma een waarschuwing geeft. Hiervoor is Avast gebruikt en niet één van de te onderzoeken antivirus programma's.

### Antivirus software testen

Er zijn geen programma's bekend die kunnen kijken of alle malware van een computer is verwijderd. Als dit het geval was zou de perfecte antivirus software namelijk al bestaan. Het is daarom onmogelijk om objectief te bepalen wanneer een computer helemaal schoon is. Het onderzoek is vooral een vergelijkend onderzoek, maar één waar wel conclusies uit getrokken kunnen worden.

De geteste pakketen zijn van drie verschillende makers. De eerste is Norton 360 van Symantec. De reden voor het testen van dit antivirus pakket is dat het vaak voorgeinstalleerd wordt op nieuwe laptops en

computers. Hierdoor maken veel gebruikers, vooral gebruikers met weinig verstand van verschillende antivirus software paketten gebruik van dit pakket.
Het tweede programma dat wordt getest is AVG Free Edition. Dit is de enige gratis antivirus software die bij dit onderzoek wordt getest. Omdat zowel Avast Free als AVG Free veel gebruikt zijn, maar er niet genoeg tijd is om ze allebei te testen is de keuze gevallen op AVG Free Edition. Het derde en laatste pakket is BitDefender. Volgens een recente antivirus test[35] zou dit het beste programma moeten zijn om malware tegen te gaan. Als dit inderdaad het geval is zou dit ook uit onze test moeten blijken. Van alle drie de paketten is een gratis versie te downloaden, waardoor ze zeer geschikt zijn om te testen.

Aangezien gebruikers antivirus software hoofdzakelijk op twee manieren gebruiken, worden er twee testen uitgevoerd. De eerste test onderzoekt de functie van antivirus software om actief malware tegen te gaan tijdens het surfen op het net. Voor deze test zal de gevonden malware route gelopen worden, met één van de drie paketten geactiveerd. Er wordt elke keer gestart met een schone computer. Met het programma Wireshark wordt de netwerkactiviteit gecontroleerd om te kijken welke netwerkactiviteit er is op de schone computer om straks te kunnen controleren of alle malware is gevonden. Tenslotte zijn er veel types malware die voor verhoogde netwerkactiviteit zorgen. Elke keer dat de route wordt gelopen zal er bij worden gehouden hoeveel malware waarschuwingen er door het betreffende pakket worden weergegeven en hoeveel malware er wordt tegen gehouden. Aan het eind van de route wordt de computer nog een keer gecontroleerd met Wireshark om te kijken of er toch iets op de computer is terechtgekomen dat voor verhoogde netwerk acitiviteit zorgt.
Om de paketten nog iets directer te kunnen vergelijken is de route ook een keer “gelopen” met alle drie de paketten tegelijkertijd actief.

De tweede test controleert de mogelijkheden van het antivirus pakket om infecties te vinden, nadat ze op de computer zijn terechtgekomen. Hiervoor zal opnieuw als extra controle het programma Wireshark worden gebruikt. Aan het begin van de test zal Wireshark worden gedraaid om een nulpunt vast te stellen en te zien wat voor netwerkactiviteit plaatsvindt voordat de malware is binnengehaald door de route te volgen. Vervolgens wordt de malware route afgelegd. Hierna voeren de paketten elk een computerscan uit, waarbij wordt genoteerd hoeveel bedreigingen zijn gevonden door het betreffende pakket. Deze bedreigingen worden hierbij nog niet onschadelijk gemaakt, om steeds de andere paketten ook een kans te geven de bedreigingen te vinden. Nadat van elke scan is genoteerd hoeveel bedreigingen zijn gevonden, zullen de gevonden bedreigingen worden verwijderd. Hierna wordt de computer nog een keer gecontroleerd met Wireshark, waarbij als alles goed is verwijderd, dezelfde netwerkactiviteit plaatsvindt als op het nulpunt.

## Route

Het bleek lastiger dan verwacht om deze blacklists te vinden. Hoewel er vaak namen van websites worden genoemd staan er geen adressen bij, of het zijn adressen van websites die allang niet meer bestaan. Na enige tijd is het gelukt om een virus database te vinden.[38] Deze database wordt elk uur aangepast en hierin staan de namen van virussen met websites waar dat virus op dat moment te vinden is. In eerste instantie hebben wij vijftig adressen verzameld om de tests mee uit te voeren. Het nadeel was, dat veel van deze websites de problemen binnen een paar dagen oplossen. Hierdoor kwam het dat wij twee onderzoeken hadden uitgevoerd, op een andere dag verder wilde, maar dit met andere malware hebben moeten doen. Om het onderzoek zo goed mogelijk te houden heben wij op één dag vroeg in de ochtend opnieuw vijftig adressen met malware verzameld en op diezelfde dag alle onderzoeken uitgevoerd, inclusief de twee die wij al hadden gedaan. De websites die wij hebben gebruikt staan bij de bijlagen vermeld.

## Resultaten

### Software actief

De eerste van de drie paketten die aanstond terwijl de vijftig websites werden geopend, was BitDefender, aangezien deze het beste zou moeten zijn. Op het nulpunt hebben we Wireshark laten lopen en er was erg weinig netwerkactiviteit te zien. Er was alleen HTTP en TCP verkeer van 199.7.71.72 naar 172.16.108.128 en andersom. Daarna zijn we alle websites afgegaan, met alleen BitDefender actief. Geen enkele website werd hierbij getoond, want iedere keer stond er een melding van BitDefender dat deze website was geblokkeerd vanwege malware. Zelfs als het ging om een website waar een bestand met malware erin gedownload zou worden, werd dit geblokkeerd nog voor we de kans kregen om het bestand ook werkelijk te downloaden. Dit geldt ook voor websites waar de download niet eens automatisch gestart zou zijn, omdat we eerst zouden moeten inloggen, maar toch werd deze website geblokkeerd. Dit gaf het idee dat BitDefender niet alleen een lijst van malware bij houdt, maar ook een lijst van blacklisted websites. In ieder geval laat het ons zien dat BitDefender een zeer goede proactieve werking heeft, omdat alles ruim op tijd wordt onderschept. Aan het eind van de route hebben we Wireshark nog een keer gedraaid en de netwerkactiviteit was, zoals verwacht, nog steeds exact hetzelfde als op het nulpunt.

De extreem goede resultaten van BitDefender waren wel opvallend en wekte de indruk dat BitDefender misschien in contact stond met de gebruikte database voor het onderzoek.  Om dit uit te sluiten hebben we nog een kort onderzoek op Google uitgevoerd. Dit heeft geen enkele bewijs opgeleverd dat BitDefender samenwerkt met deze database. Daarbij claimt de database onafhankelijk te zijn. Deze resultaten waren voor ons genoeg om aan te nemen dat BitDefender niet rechtstreeks deze database gebruikt en wel de resultaten van het onderzoek te gebruiken.

Het tweede pakket dat we hebben getest is Norton 360, omdat we het vermoeden hadden dat, omdat het een allround betaald antivirus pakket was, Norton na BitDefender de meeste websites zou moeten blokkeren. Gebleken is dat Norton veel minder websites tegen hield dan BitDefender. Slechts vijftien van de vijftig websites zorgde ervoor dat Norton een website blokkeerde. In 80% van de gevallen werd

een bestand echter geblokkeerd nadat het al gedownload was. We konden dus gewoon de geinfecteerde bestanden downloaden en daarna scande Norton het bestand om vervolgens een waarschuwing te geven. Dit werkt alleen goed voor malware die al wat beter bekend is en dit is waarschijnlijk ook de reden dat Norton er maar vijftien blokkeerde. De malware gebruikt voor dit onderzoek, waren vaak pas een uur eerder ontdekt op websites, wat ons doet denken dat sommige mogelijk echt nieuwe malware kan zijn. De reactieve werking van Norton is dus redelijk goed, maar proactief stelt Norton weinig  voor, omdat iets eerst op de computer moet staan voor het gecontroleerd wordt.

Het derde en laatste pakket dat is getest, is AVG Free Edition. Ook AVG blokkeerde precies vijftien van de vijftig websites en bestanden, maar dit waren niet dezelfde als die door Norton werden geblokkeerd. In sommige gevallen wel, maar beide hadden unieke malware die door de ene wel en door de andere niet werden geblokkeerd. Ook AVG werkt voornamelijk door een bestand te scannen en te blokkeren nadat het op de computer terecht is gekomen. Wel waren er enkele websites die door AVG direct werden geblokkeerd, maar door Norton niet gebeurde. Bij zowel de test met Norton als de test met AVG is zowel voor als na de test Wireshark gebruikt, om te kijken welke netwerkactiviteit er was. In alle drie de gevallen was de netwerkactiviteit voor het onderzoek gelijk, alleen bij Norton en AVG was er naderhand nog één soort activiteit bijgekomen. Het gaat om verkeer van 172.16.108.128 naar 188.165.234.33 en andersom. Gek genoeg is er voor het adres 188.165.234.33 op internet geen informatie beschikbaar via IP whois. We hebben het vermoeden dat dit verkeer dus wel degelijk door malware is veroorzaakt, met name omdat na het terugzetten van de computer in de oorspronkelijke staat, dit verkeer weer weg was. Er was dus geen abnormaal hoog netwerkverkeer, maar toch wel verkeer naar een schijnbaar onbekend adres. Helaas bestond ook dit voornamelijk uit HTTP en TCP verkeer waarvan de herkomst niet konden achterhalen.

Als laatste onderzoek zijn wij nog een keer alle websites afgelopen met de drie pakketten tegelijkertijd actief. Het meest opvallende is, dat Norton geen kans kreeg om iets te doen. Norton is duidelijk veel langzamer dan beide andere pakketten. AVG kreeg af en toe nog de kans om iets te blokkeren, weliswaar nadat BitDefender het ook al had geblokkeerd, maar AVG lijkt vooral te kijken naar wat er in cookies en temporary bestanden binnenkomt om hierdoor websites met malware te blokkeren. Doordat echter geen van de websites of bestanden werkelijk naar de computer werden gedownload vond Norton helemaal niets. Opvallend is dat de verschillende paketten elkaar als infectie aanduiden. Zo weigeren BitDefender en Norton goed met elkaar samen te werken. Beide hebben met AVG geen problemen. Toch zorgt dit ervoor dat het erop lijkt dat antivirus software zo is gemaakt, dat je maar één pakket tegelijk kan gebruiken.

| | AVG | BitDefender | Norton |
|---|---|---|---|
| 1 | 1 | 1 | 1 |
| 2 | | 1 | |
| 3 | | 1 | |
| 4 | | 1 | |
| 5 | | 1 | |
| 6 | 1 | 1 | |
| 7 | 1 | 1 | |
| 8 | | 1 | 1 |
| 9 | | 1 | |
| 10 | | 1 | |
| 11 | 1 | 1 | 1 |
| 12 | 1 | 1 | 1 |
| 13 | | 1 | 1 |
| 14 | | 1 | |
| 15 | | 1 | |
| 16 | 1 | 1 | 1 |
| 17 | | 1 | |
| 18 | 1 | 1 | 1 |
| 19 | 1 | 1 | |
| 20 | | 1 | 1 |
| 21 | | 1 | 1 |
| 22 | | 1 | |
| 23 | | 1 | |
| 24 | | 1 | |
| 25 | | 1 | |
| 26 | | 1 | |
| 27 | | 1 | |
| 28 | | 1 | |
| 29 | | 1 | 1 |
| 30 | | 1 | |
| 31 | 1 | 1 | 1 |
| 32 | 1 | 1 | 1 |
| 33 | | 1 | |
| 34 | | 1 | 1 |
| 35 | | 1 | |
| 36 | | 1 | |
| 37 | | 1 | |
| 38 | | 1 | |
| 39 | | 1 | |
| 40 | | 1 | |
| 41 | 1 | 1 | |
| 42 | 1 | 1 | 1 |
| 43 | | 1 | |
| 44 | | 1 | |
| 45 | 1 | 1 | 1 |
| 46 | | 1 | |
| 47 | | 1 | |
| 48 | 1 | 1 | |
| 49 | | 1 | |
| 50 | 1 | 1 | |

1 Betekent dat er een blokkering of waarschuwing van de software kwam.

## Computerscans

Na deze tests zijn we alle websites nog een keer afgegaan zonder antivirus pakket actief. Naderhand heeft elk pakket een computerscan uitgevoerd waarbij elk van de pakketten de volgende aantallen infecties vonden:

| | AVG | BitDefender | Norton |
|---|---|---|---|
| Aantal: | 23 | 35 | 10 |

Er is geen exacte informatie bekend over hoeveel infecties dit van het totaal zijn, voornamelijk omdat niet elk van de vijftig websites iets op de computer zal hebben gezet. Er is duidelijk te zien dat BitDefender veruit het beste scoort, gevolgd door AVG, terwijl Norton maar een magere tien infecties vindt. Hierna heeft Wireshark nog een keer gedraaid, waarbij er geen extra netwerkverkeer meer werd gevonden, dus wij vertrouwen er op dat BitDefender heeft verwijderd wat nodig was om dit te voorkomen.

## Conclusie

Uit het onderzoek blijkt dat BitDefender zijn werk beter doet dan Norton, of AVG. Het is veel interessanter om te zien waarom BitDefender zoveel meer tegenhoudt. Het lijkt erop dat BitDefender een grotere, meer up-to-date database heeft dan elk van de andere pakketten. Ook werkt BitDefender duidelijk proactief, elke bedreiging wordt tegengehouden nog voordat deze op de computer wordt gezet, terwijl Norton pas bestanden controleert nadat ze op de computer staan. AVG lijkt hier een beetje tussenin te zitten, door sommige bestanden pas te controleren nadat ze op de computer staan, en andere al op de website. Er is een grote kans dat BitDefender iets teveel tegenhoudt. Via sommige websites zou er niets op de computer terecht zijn gekomen, omdat wij niet waren ingelogd, maar toch werd dit al door BitDefender gesignaleerd. Hoewel dit te streng lijkt kan het geen kwaad, omdat er wel degelijk malware zat en het geen false positive was. Een andere mogelijkheid is om twee verschillende pakketten tegelijkertijd te gebruiken. Zo is te zien dat AVG en Norton samen meer tegenhouden dan elk van de pakketten apart. Helaas zijn de meeste antivirus pakketten zo geprogrammeerd, dat ze niet met elkaar samen kunnen werken, omdat ze of elkaar als malware zien of weigeren te werken zolang er een ander pakket op de computer staat, tenzij deze check handmatig wordt uitgezet.
Ook bij het scannen van de computer achteraf wordt er door BitDefender veel meer gevonden dan Norton en AVG. Het is hierbij erg jammer dat je voor Norton zelfs nog geld moet betalen, terwijl de gratis AVG meer infecties vindt en verwijderd dan Norton. Alle gevonden infecties zijn gecontroleerd en het waren ook werkelijk de bestanden die via de websites waren binnengehaald, dus er waren in dit geval geen false positives bij die zorgen dat BitDefender alleen maar beter lijkt. Hij was ook werkelijk beter.

Uiteindelijk wilden we weten of antivirus software goed werkt bij correct gebruik. We kunnen dus zeggen dat BitDefender zijn werk goed doet. Als alle updates gedaan zijn, beschermt BitDefender zonder meer de computer en zorgt ervoor dat alles goed blijft werken. Ook had BitDefender een mooie optie om bij elke gevonden infectie een voorstel te doen over het feit of het verwijderd moest worden of in quarantaine moest worden gezet.
Over de andere twee pakketten zijn we veel minder te spreken. Naar ons idee doet AVG prima wat het moet doen, hoewel er hier en daar nog verbeteringen kunnen worden aangebracht, het is tenslotte een gratis antivirus pakket. Norton 360 is het meest complete pakket wat Symantec aanbiedt en ten opzichte van de andere paketten scoort hij erg slecht. Tijdens het surfen zijn de presentaties gelijk aan die van AVG, maar bij iets wat al op de computer staat vindt hij erg weinig van de infecties en daarnaast werkt hij twee keer zo langzaam als AVG en bijna drie keer zo langzaam als BitDefender. Onze conclusie is dat BitDefender in onze test het best scoorde en wij zouden dan ook BitDefender aanraden voor iedereen die betaalde antivirus software wil gebruiken. Voor iedereen die geen geld wil uitgeven is AVG een prima optie.

# 5 – Conclusie – Een blik op de toekomst

Uit de enquête is gebleken dat er nog steeds malware op computers wordt aangetroffen bij computerscans, waaruit blijkt dat de bescherming van antivirus software tegen huidige malware nog niet optimaal is. Ook tijdens de testen met geactiveerde antivirus software, blijkt dat niet alle antivirus software alle malware tegenhoudt die op de computer probeert te komen. Hoe kunnen we computers nog beter beschermen tegen malware?

Om deze vraag te kunnen beantwoorden is het handig om eerst nog eens het literatuuronderzoek te bekijken. In het eerste deel van dit onderzoek hebben we onderscheid gemaakt tussen de verschillende soorten malware. Al deze soorten moeten tegengehouden worden door antivirus software, waardoor het onderscheid in eerste instantie niet zo zinvol lijkt, maar toch is het onderscheid tussen deze verschillende soorten malware nodig.
Ten eerste om te kijken welke verschillende technieken malware gebruikt om zich te verbergen, zodat antivirus software zich op al deze vormen kan richten en zich verbeteren om alle vormen tegen te gaan. Zo kan de huidige antivirus software nog niet omgaan met rootkits. Ze worden vaak niet gevonden en zelfs al worden ze wel gevonden dan kunnen ze nog niet automatisch worden verwijderd. Maar ook voor andere vormen van malware moet de beveiliging nog worden verbeterd. Zo kunnen de meeste antivirus software paketten wel malware vinden die backdoors open zet, maar als dit pas gevonden wordt nadat het op de computer staat, kan de backdoor al zijn open gezet. De antivirus software kan dan nog wel de malware verwijderen, maar niet meer de schade inperken die al is gedaan. Voor deze soorten malware, maar ook andere die gelijk actief worden en zichzelf gaan verspreiden zoals wormen, is proactieve bescherming van antivirus software erg belangrijk. Uit dit onderzoek is gebleken dat bij twee van de drie geteste antivirus software paketten de proactieve bescherming nog minder dan de helft van alle malware wordt tegen gehouden. Norton 360 bleek zelfs helemaal geen proactieve bescherming te hebben, want alles werd pas gecontroleerd nadat het op de computer stond.

Het onderscheid tussen de verschillende soorten malware is voor gebruikers ook zinvol om te weten. Zo blijkt dat veel mensen denken dat een virus en een worm hetzelfde is, maar hoewel ze vaak dezelfde soorten schade aanbrengen, is er een zeer belangrijk verschil. Zo verspreid een virus binnen de computer waar het op staat en kan pas naar een andere computer worden gebracht als de gebruiker dat zelf doet. Een worm kan zich automatisch over een netwerk verspreiden, zonder dat daar een gebruiker voor nodig is. Wanneer er een melding komt van antivirus software over een bestand waar een virus in zit en over een ander bestand met een worm, zelfs al doen het virus en de worm in principe hetzelfde, is het bestand met de worm nog altijd gevaarlijker dan het virus. Dit zou de beslissing van een een gebruiker kunnen beïnvloeden om het virus in quarantaine te zetten en de worm gelijk te verwijderen. Hier ligt dus een mogelijkheid om bescherming te verbeteren, zowel voor de gebruiker als voor de software fabrikant. Als gebruikers leren over de verschillende soorten malware, zoals wat het is, wat het doet en hoe het verspreidt, terwijl de antivirus software bij elke melding niet alleen de naam van de malware geeft, maar ook een makkelijker te begrijpen term voor de gebruiker zoals “bot” of “worm”, kan de gebruiker beter beslissen wat er moet gebeuren met het bestand, maar ook of het misschien

nodig is om gebruikers in het netwerk te waarschuwen of om de eigen harde schijf nog eens extra te controleren. Stel dat de antivirus software bijvoorbeeld aangeeft wanneer een soort malware een backdoor open zet, door simpelweg “backdoor” te laten zien. Dan weet de gebruiker dat de malware zelf is verwijderd, maar ook dat het mogelijk is dat er een poort open staat die niet open moet staan. Een ervaren gebruiker kan hier zelf iets aan doen, maar zelfs een niet ervaren gebruiker weet zo dat hij zijn computer zou moeten laten nakijken. Op dit moment lijkt de enige aanduiding die gegeven wordt in dit opzicht vaak dat van “Trojan” te zijn, maar waarom doen ze dit niet bij alle verschillende types. Op deze manier kunnen gebruikers en antivirus software samen aan betere bescherming werken.

Daarnaast is het commerciele karakter van antivirus software een probleem. Zo blijkt dat het zinvol kan zijn om twee verschillende antivirus software pakketten op de computer te hebben, maar zolang deze elkaar als malware zien en waarschuwingen geven of zelfs niet werken zolang er een tweede pakket op staat kan hier geen gebruik van worden gemaakt. Dit lijkt puur om geld te gaan, want de gratis versie van AVG heeft geen problemen met andere pakketten en de andere pakketten ook niet met AVG. Toch zou deze “beveiliging” om maximaal één pakket tegelijk op de computer te hebben beter niet aanwezig kunnen zijn. Niet alleen omdat het voor een betere bescherming tegen malware zorgt, maar ook omdat het hebben van twee pakketten hooguit zou betekenen dat een gebruiker twee licenties betaalt. Geen van beide pakketten verliest hier geld op. Pas als een gebruiker besluit te wisselen omdat het tweede pakket beter blijkt is het nadelig voor de eerste fabrikant. Maar als het niet meer toegestaan zou zijn om andere pakketten uit te sluiten zou dit voor een gezonde concurentie kunnen zorgen, waar betere bescherming uit voortkomt. Dit is echter speculatie en kan niet met zekerheid worden gezegd.

De bovenstaande resultaten gelden alleen wanneer, zoals bij het onderzoek, de antivirus software goed wordt gebruikt. Toch blijkt uit de enquête dat nog niet iedereen de software goed gebruikt. Er zijn zelfs mensen die niet weten of hun software up-to-date is of niet. Bij deze mensen is de kans dus aanwezig dat ze niet de laatste versie van hun antivirus software hebben, zoals ook informeel gezien is, wat de beveiliging slechter maakt. Een reden hiervoor zou kunnen zijn dat veel van de antivirus software niet erg intuitief is. Het is mogelijk om aan te geven dat updates automatisch moeten worden gedaan en als dat niet zo is wordt er een duidelijke melding gegeven dat de software niet up-to-date is, maar als er een hele nieuwe versie is, zoals bij AVG, wordt daar soms geen melding over gegeven. Ook opties om antivirus software in te stellen is vaak redelijk moeilijk te vinden en soms is het zelfs moeilijk om te weten wat alle opties betekenen en wat ze doen. Dit gedeelte van antivirus software is bij dit onderzoek buiten beschouwing gelaten, maar het is niet moeilijk voor te stellen dat onderzoek naar wat een goede interface is en hoe antivirus software eruit zou moeten zien, zou kunnen bijdragen aan een betere beveiliging.

Een andere plek waar antivirus software mogelijk van belang wordt is op andere apparaten dan computers die in verbinding staan met internet. Hierbij kan men denken aan smartphones en nieuwere televisies. De mogelijkheid bestaat dat ook voor deze systemen in de toekomst malware zal worden gemaakt, waardoor antivirus software voor deze apparaten van belang wordt. Op het moment is AVG bijvoorbeeld al wel beschikbaar voor telefoons, maar een echte malware dreiging is er nog niet. Toch is het zeker niet uit te sluiten dat deze er in de toekomst wel komt.

## 6 – Literatuur


[1] ^ Jussi Parikka (2007) "Digital Contagions. A Media Archaeology of Computer Viruses", Peter Lang: New York. Digital Formations-series. ISBN 978-0-8204-8837-0, p. 18-19

[2] ^ von Neumann, John (1966). "Theory of Self-Reproducing Automata". *Essays on Cellular Automata* (University of Illinois Press): 66–87. Retrieved June 10., 2010.

[3] http://www.apple.com/why-mac/better-os/#viruses

[4] Anick Jesdanun (1 September 2007). "School prank starts 25 years of security woes" CNBC

[5] Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002 Abstract at http://vx.netlux.org/lib/aas10.html

[6] Vesselin Bontchev. "Macro Virus Identification Problems"*FRISK Software International*.

[7] Computer security: art and science Door Matt Bishop, p 623-624

[8] New Perspectives on Computer Concepts 2010, Brief Door June Jamrich Parsons,Dan Oja, p163

[9] http://morrisworm.larrymcelhiney.com/morris_appeal.txt

[10] http://query.nytimes.com/gst/fullpage.html?res=9C0CE1D71038F936A35756C0A966958260&scp=2&sq=robert+tappan+morris&st=nyt

[11] Malware: fighting malicious code Door Ed Skoudis,Lenny Zeltser, p251-270, 187-188

[12] Jamie Crapanzano (2003): "Deconstructing SubSeven, the Trojan Horse of Choice", SANS Institute, Retrieved on 2009-06-11

[13] http://news.bitdefender.com/NW1094-en--BitDefender-Malware-and-Spam-Survey-finds-E-Threats-Adapting-to-Online-Behavioral-Trends.html

[14] Thwarted Linux backdoor hints at smarter hacks; Kevin Poulsen; SecurityFocus, 6 November 2003.

[15]http://www.windowsecurity.com/articles/Hidden_Backdoors_Trojan_Horses_and_Rootkit_Tools_in_a_Windows_Environment.html

[16] Windows Rootkit Overview. Symantec. 2006-03-26. Retrieved 2010-08-17.

[17] Rootkits: subverting the Windows kernel, Greg Hoglund,James Butler, 2006, 4-20

[18] Blocking spam and spyware for dummies Door Peter H. Gregory,Michael A. Simon,Mike Simon, p 11-12,15

[19] Spyware and Adware Door John Aycock, p1-3,9

[20] Cormac Herley and Dinei Florencio (2006-02-06). "How To Login From an Internet Cafe Without Worrying About Keyloggers", p1

[21] Computer Security: Protecting Digital Resources Door Robert C. Newman, p58

[22] CompTIA security+ review guide Door James Michael Stewart, p 9

[23] Proceedings of the International Conference of Information Warfare and security, maart 2006, p23

[24] http://www.webopedia.com/index.php/TERM/G/greyware.html

[25] Fuzzing for software security testing and quality assurance Door Ari Takanen,Jared DeMott,Charles Miller, 11,12

[26] Biologically inspired approaches to advanced information ...: Volume 1, Auke Jan Ijspeert, Masayuki

Murata, Naoki Wakamiya, 2004, 153-164
[27] Behavior Blocking: The Next Step in Anti-Virus Protection, Carey Nachenberg, March 19, 2002

[28] Windows Forensic Analysis DVD Toolkit Door Harlan Carvey, 392,393
[29] Rootkits for dummies Door Larry Stevenson,Nancy Altholz, 244-246

[30] Botnet detection: countering the largest security threat geredigeerd door Wenke Lee,Cliff Wang,David Dagon,1-3
[31] Combating spyware in the enterprise Door Brian Baskin,Tony Piltzecke, 116-119
[32] Detecting unknown massive mailing viruses using proactive methods, Ruiqi Hu and Aloysius K. Mok, 82 83, 2004
[33] http://antivirus.about.com/b/2007/03/11/clean-quarantine-or-delete.htm
[34] Troubleshooting and Maintaining Your PC All-in-One Desk Reference For Dummies, Dan Gookin, 457
[35] http://www.av-test.org/certifications?order=protection_desc&lang=en
[36] http://www.tripwire.com/information-security/data-protection/
[37] Crimeware: understanding new attacks and defenses, Markus Jakobsson,Zulfikar Ramzan, 374-376
[38] Virus database, http://support.clean-mx.de/clean-mx/viruses.php

# 7 – Bijlagen

## Lijst met virussen

Ons advies is om deze websites NIET zomaar te bezoeken, tenzij je op een mac zit of een computer gebruikt waar geen belangrijke informatie op staat of in verbinding staat met een belangrijk netwerk.

http://174.45.249.187/Baby/Telegrama.exe
http://fearkiddo.fileave.com/ToPCloner.exe
http://mac-defence.com/download.php
http://softnyx.net/CustomerFile/hack(5).rar
http://www.miranda.gov.ve/modules/mod_ans/images/allnet.jpg
http://www.sfmati.ru/ps-x.jpg
http://www.skyway3.com/e107_themes/107_images/ipays.jpg
http://www.splavar.com/hytera/catalog/images/inject.txt
http://own3ed.tv/1itemdbow
http://www.volishovo.ru/e107_plugins/jscripts/allnet.jpg

http://bertswarehouse.com/allnet.jpg
http://vk.758036-x1cea13d.ru/attach/566754_108189996/881148818/DSC000095.scr
http://botku.webs.com/mampuz.jpg
http://botku.webs.com/vito.jpg

http://www.winlivefiles.com.br/arquivos/msn/win/slides/2011/slide_homem_mulher_cebola_apresetacao.ppt.exe
http://brutinhozika.t35.com/hostpobrutin.txt
http://idocreative.ru///logs/allnet.jpg
http://kytickabila.com/admin/getfile.php
http://eshop.spin3d.com.tw/images/infobox/ipays.jpg
http://miliardov.com/pusk3.exe

http://92d.cz.cc/d.php?f=18%26e=0
http://adrieath.cx.cc/manuale.pdf
http://kingkinglove.tk/
http://eurosystems.it/conf_commerciale/images/open.jpg
http://gaberunzz.t35.com/unixBSD/aa/xcz.txt
http://indra.ucoz.org/loadind.txt
http://kirtou.homeip.net/osCommerce/catalog/images/microsoft/indo.jpg
http://klubasvega.lt/e107_themes/byroe.jpg

http://s659.chomikuj.pl/file.aspx?id=249149488&vid=249149488&tk=1478202&t=63440

4500978439145&d=60&k=1348532&name=keygen.exe
http://kolbasy.net/images/cafe.jpg
http://promocoesvisa.eu.pn/visabrasil.com.br/cmdd.txt
http://quatangvp.com/images/page/myid.jpg
http://178.18.243.222/d.php?f=75&e=4
http://tal.ohhappy.net/counter/documents/logon.txt
http://videmos.org/login.gif
http://jabashop.co.kr/member/id1.txt
http://www.balkmetafoor.be/templates/ID-RFI.txt
http://www.envoidefichier.com/e-BigSend/
http://hegs.fileave.com/

http://comercioexport.com.br/envi1.txt
http://www.compreevenda.info/calimage/baner.txt
http://diretor7.t35.com/1/fx29sh.txt
http://www.coolergas.com/.mods/cmd.txt
http://www.le-galetas.com/temp/
http://diretor7.t35.com/1/rs.txt
http://www.energeticherbals.co.za/images/default/sprd.txt
http://www.energeticherbals.co.za/images/default/ID.txt
http://diretor7.t35.com/1/fx29id2.txt
http://coolergas.com/.mods/cmd.txt
http://com.rb.ma/editor/plug/kill.jpg