Door **Guus Crone**

Eerste hulp bij malware-infecties

Help! Mijn pc is besmet!

Ook een beschermde pc kan besmet raken met malware. Eén muisklik op een verkeerde link kan resulteren in een supertrage pc, een ongewenste zoekbalk in de browser of pop-ups die u ineens om de oren vliegen. Geen paniek: de meeste malware is er niet op uit uw data te vernietigen. Het is wel zaak deze ongewenste software zo snel mogelijk weer kwijt te raken. We laten u zien hoe u te werk moet gaan. Is uw pc eenmaal schoon, dan is het zaak om dat zo te houden! We doen u een aantal tips aan de hand waarmee u ongenode gasten de toegang tot uw computer ontzegt en voorkomt dat u in de toekomst besmet raakt.

Veel malware kunt u zelf onschadelijk maken met behulp van een virusscanner en enkele spywarescanners. Vaak is dit voldoende om de pc weer helemaal in orde te krijgen. Mocht het niet lukken de pc op deze manier helemaal schoon te krijgen, dan kunt u hulp inroepen op gespecialiseerde forums op het web, waar u door deskundigen van de problemen afgeholpen wordt.

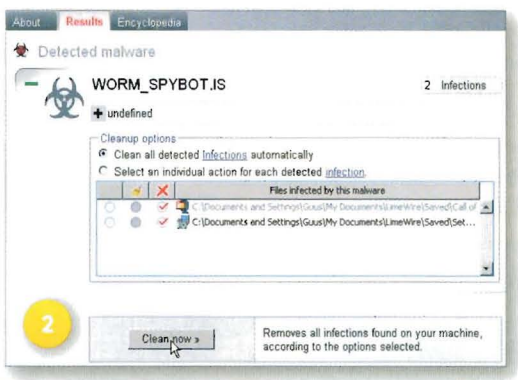
Maar om te beginnen voert u zelf een virusscan uit. U kunt hiervoor de virusscanner gebruiken die u op de pc geïnstalleerd hebt, maar een online virusscanner heeft de voorkeur. Het is immers mogelijk dat de virusscanner op uw pc door de besmetting is aangetast en niet goed meer werkt. Veel online scanners vereisen installatie van een ActiveX-component. U kunt deze scanners meestal alleen via Internet Explorer gebruiken.

HOUSECALL

Housecall, de online scanner van Trend Micro, gebruikt een op Java gebaseerde scanmodule, waardoor deze scanner zowel via IE als Firefox te gebruiken is. Voor een online scan met Housecall gaat u naar http://housecall.trendmicro.com, waar u op de afbeelding met het vergrootglas klikt (afbeelding 1).

▲ *Klik op het vergrootglas om te beginnen met scannen.*

De volgende stappen wijzen zich vanzelf: nadat u akkoord bent gegaan met de voorwaarden, start u Housecall met de gewenste scanmodule. Het scanproces is te volgen in de statusbalk van de browser. Is er malware op de pc aangetroffen, dan klikt u op de knop *Clean now*, waarna Housecall de infectie zal verwijderen (afbeelding 2). Het is mogelijk dat de problemen hiermee al verholpen zijn, maar omdat het niet zeker is of alle malware nu van de pc verdwenen is, voert u nog twee scans uit. Hiervoor gebruikt u Spybot Search & Destroy en Ad-Aware, twee tools die speciaal ontwikkeld zijn voor het verwijderen van spyware.

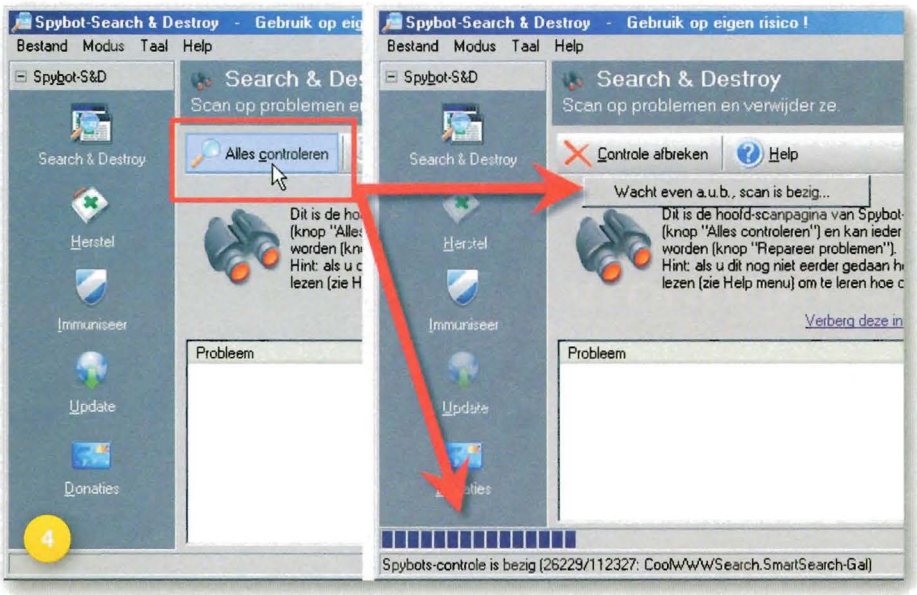


▶ *Zodra er malware op de pc aangetroffen, zorgt een klik op de knop Clean now ervoor dat de infectie wordt verwijderd.*

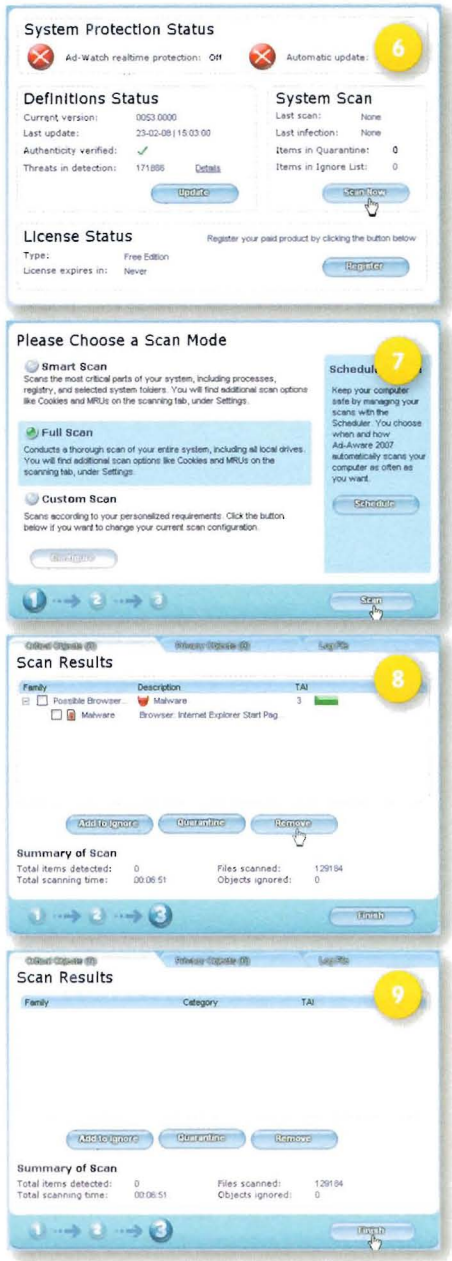
SPYBOT SEARCH & DESTROY

Download eerst Spybot Search & Destroy (http://ct.link.idg.nl/spybot). De installatie zal geen problemen opleveren, maar het is aan te raden om tijdens deze procedure het vinkje bij *Use sytem settings protection (TeaTimer)* weg te halen. Deze functie is niet noodzakelijk voor een goede werking

▼ *Voordat u aan de slag gaat met Spybot dient u het programma eerst te voorzien van de nieuwste updates.*



▲ *Spybot Search & Destroy in actie.*



▶ *Klik op de knop Scan now en vervolgens voor een Full Scan om er zeker van te zijn dat er geen ongewenste restjes op uw pc zijn achtergebleven.*

van het programma en zorgt nogal eens voor verwarring.

Na de installatie wordt er een wizard gestart. Deze kunt u op dit moment het beste overslaan door steeds op *Volgende* te klikken – een back-up maken van het register van een besmette pc is namelijk niet aan te raden en de overige zaken die de wizard regelt, kunnen vanuit het programma zelf uitgevoerd worden. In het laatste venster klikt u op de knop *Start het programma*.

In het hoofdvenster van Spybot klikt u op *Zoek naar updates*, waarna er een venstertje geopend wordt waarin één van de downloadservers al geselecteerd zal staan (afbeelding 3). U klikt hier op *Continue* en in het volgende venster kiest u voor *Download*. Als de updates gedownload zijn, wordt u eraan herinnerd de pc te immuniseren en een scan uit te voeren. Klik achtereenvolgens op *OK* en *Exit* en vervolgens op *Immuniseer*, waarna gemeld zal worden tegen hoeveel kwalijke zaken u al beschermd bent en hoeveel er nog geïmmuniseerd moeten worden. Door op *Immunize* te klikken schakelt u de bescherming tegen deze items in. U bent nu klaar om een scan uit te voeren: klik op *Search & Destroy* en vervolgens op *Alles controleren* om de scan te starten (afbeelding 4). Wanneer er malware wordt aangetroffen verwijdert u deze door op de knop *Repareer problemen* te klikken (afbeelding 5).

AD-AWARE 2007

Ten slotte voert u een scan uit met Ad-Aware 2007 http://ct.link.idg.nl/adaware). Klik tijdens de installatie op de knop *Use Free* om aan te geven dat u de gratis versie wilt gebruiken. Als u hierna het programma gestart hebt, klikt u allereerst op de knop *Update*. Ad-Aware meldt vervolgens welke updates opgehaald dienen te worden en installeert deze.

U kunt nu de pc scannen: klik op de knop *Scan now* (afbeelding 6) en kies in het volgende venster voor een *Full Scan* (afbeelding 7) en klik tot slot rechtsonder op de knop *Scan*. Na de scan selecteert u de gevonden malware die u wilt verwijderen en ruimt u ze op via de knop *Remove*, waarna u het programma afsluit (afbeelding 8 en 9).

◀ *De aangetroffen problemen.*

HULP

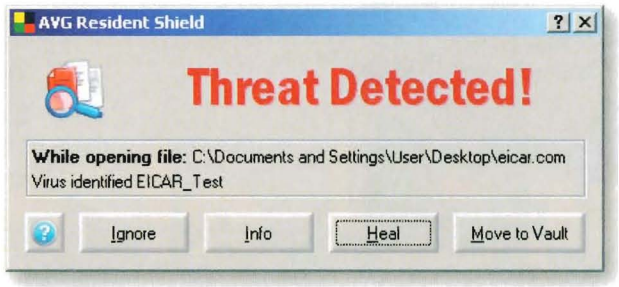
Zoals gezegd, is het mogelijk dat de problemen na de eerste scan al zijn verholpen. Het kan echter ook zo zijn dat de pc na deze drie scans nog steeds niet naar behoren werkt. In dat geval kunt u professionele hulp krijgen op één van de vele websites die gespecialiseerd zijn in het verwijderen van malware. U kunt hiervoor onder andere terecht op ons eigen Computer!Totaal-forum (http://forum.computertotaal.nl) of op gespecialiseerde forums zoals Nucia.nl en Hijackthis.nl. Op deze sites hoeft u zich slechts eenmalig te registreren. De registratie en de hulp zijn gratis.

Aan de hand van een omschrijving van de problemen en een zogeheten HijackThis-log wordt dan bekeken hoe de infectie te verwijderen is. Op ons forum leest u hoe u een HijackThis-log maakt (http://ct.link.idg.nl/hijackthis). Ook wanneer de pc na uw schoonmaakacties geen problemen meer vertoont, kunt u overigens een HijackThis-log op bovengenoemde sites plaatsen en controleren of er nog resten van de infectie zijn achtergebleven.

Voorkom malware-infecties

De vorige pagina's lieten we u zien hoe u malware van uw pc verwijdert. Maar dan is het eigenlijk al te laat... U kunt problemen beter vóór zijn: we leggen uit hoe u uw pc beschermt tegen malware en andere vervelende programma's. We gebruiken zo weinig mogelijk programma's zodat het systeem nauwelijks wordt belast. Daarbij kijken we specifiek naar gratis oplossingen.

Het beveiligen van een pc is niet moeilijk. Twee of drie programma's zijn hiervoor al voldoende. Om te beginnen is dat een firewall, die inkomend internetverkeer blokkeert als dat nodig is. Wanneer u de firewall in uw router gebruikt, is een tweede exemplaar op de pc niet altijd nodig. Daarnaast gebruikt u een antispywareprogramma dat tijdens het surfen bescherming biedt tegen speciale malwarevormen. En ten slotte moet er een virusscanner geïnstalleerd zijn - niet om te scannen, maar vanwege het feit dat zo'n programma voortdurend kijkt of ergens op de pc malware actief wordt en de nodige maatregelen treft als dat het geval is.



▲ *Een goede virusscanner waarschuwt direct tegen bedreigingen.*

VIRUSSCANNER

Voor thuisgebruik is een virusscanner waar u voor moet betalen niet per se noodzakelijk. Scanners als AVG Antivirus Free Edition (http://ct.link.idg.nl/avgantivirus) en Avast! 4 Home Edition (http://ct.link.idg.nl/avasthome) zijn gratis en bieden een prima bescherming. Ze beschikken in ieder geval over de vier eigenschappen waaraan een goede virusscanner moet voldoen.

Allereerst bieden ze *realtime* bescherming. Dat wil zeggen dat ze continu in de gaten houden of er bestanden geopend worden en dit pas toestaan als het sein veilig wordt gegeven. Wordt er malware ontdekt, dan verhindert de scanner dat het bestand geopend wordt en krijgt u een melding met informatie. Daarnaast bevatten ze een e-mailscanner, die eveneens in *realtime* werkt, en een automatische updatefunctie, waardoor de database met virusdefinities zo nodig dagelijks bijgewerkt wordt. En ten slotte hebben ze een *on demand* scanfunctie. Hiermee kunt u een bestand of map via een rechtermuisklik snel scannen.

Bij de keus van een virusscanner is het belangrijkste criterium of deze de vier genoemde eigenschappen bezit. Daarentegen zijn cijfers over het percentage virussen dat een bepaalde scanner kan ontdekken praktisch betekenisloos. Laat u hierdoor vooral niet leiden bij uw keus!

FIREWALL

Loopt uw internetverbinding via een router, dan zal deze voorzien zijn van een hardwarematige firewall, die eventuele indringers en ander ongewenst internetverkeer buiten de deur houdt, terwijl hij legitiem verkeer toegang tot de pc geeft. Dat is de taak van een firewall en de exemplaren in routers voeren deze uitstekend uit. Dit soort firewalls controleert alleen het inkomende verkeer, aangezien al het uitgaande verkeer als toegestaan wordt beschouwd. En op een onbesmette pc zal dit ook altijd het geval zijn.

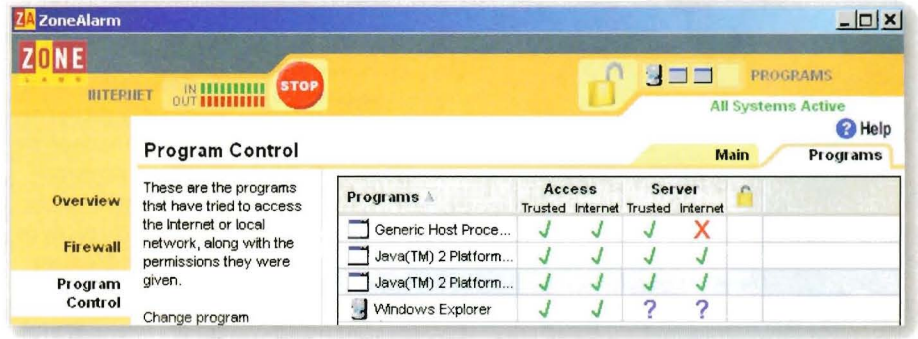
Veel mensen installeren daarnaast een firewall op de pc, die ook het uitgaande verkeer kan controleren. De redenatie hierachter is dan vaak dat op die manier ongewenst uitgaand verkeer ontdekt kan worden. Helaas is die uitgaande controle niet altijd waterdicht, want spyware die 'naar huis wil bellen', zal daar meestal een legitiem proces voor gebruiken dat al toegang tot internet heeft of de firewall op een andere manier proberen te omzeilen. Het overige uitgaande verkeer is legitiem, en in feite hebt u met zo'n tweede firewall wenig meer dan een overzicht van alle processen en programma's die u toegang tot internet hebt gegeven. Aan uw beveiliging voegt dit natuurlijk weinig toe; aan de systeembelasting daarentegen wel. Aangezien het in dit artikel een specifiek doel is de systeembelasting te verlagen, laten we de tweede firewall achterwege, zolang we achter de router zitten.

Het wordt uiteraard anders wanneer u een inbelverbinding of een kabel/adsl-modem zonder firewall gebruikt. In dat geval is een firewall op de pc absoluut noodzakelijk. Goede gratis firewalls zijn onder meer Comodo en ZoneAlarm.

ANTISPYWARE

Afgezien van de manier waarop u surft, downloadt en met uw e-mail omgaat, vormen een virusscanner en firewall uw belangrijkste beveiliging. Indringers worden door de firewall effectief buiten de deur gehouden en de meeste malware krijgt door de virusscanner geen kans om op uw pc actief te worden. Er is echter een categorie malware die nog weleens door deze beveiliging heen breekt. Het gaat dan voornamelijk om spyware, die daarbij vooral gebruik maakt van zwakheden in Internet Explorer. Hierdoor is het bijvoorbeeld mogelijk dat er ActiveX-toepassingen of scripts worden uitgevoerd, die uw pc of uw privacy schade kunnen toebrengen.

Gelukkig bestaan er programma's die dit kunnen voorkomen. Veel van deze applicaties moeten hiervoor echter in het geheugen geladen zijn en belasten de pc dus in meer of mindere mate. Een programma dat dit niet doet is SpywareBlaster. Dit programma brengt alleen bepaalde wijzigingen in het register aan, waardoor deze categorie malware van uw pc wordt geweerd. De belangrijkste methode die SpywareBlaster hiervoor gebruikt is het plaatsen van zogenoemde *killbits* in het register.



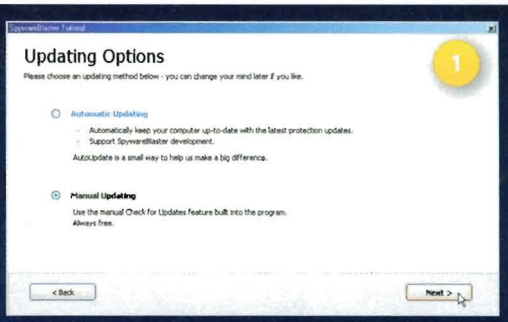
▲ *Bij een inbelverbinding is een goede firewall als ZoneAlarm onontbeerlijk.*

INSTALLATIE EN GEBRUIK VAN SPYWAREBLASTER

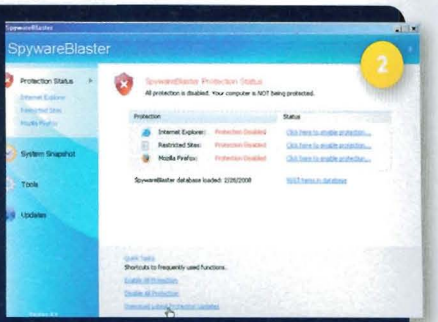
U downloadt SpywareBlaster via Javacool Software (www.javacoolsoftware.com). De installatie zal geen problemen opleveren. Wanneer u het programma hierna voor het eerst start, verschijnt er een korte tutorial. Tijdens het doorlopen daarvan krijgt u de keus tussen automatisch en handmatig updaten. Voor de eerste optie hebt u de betaalde versie nodig, maar omdat er slechts eens in de twee à drie weken een update uitkomt, kunt u het beste voor handmatig updaten kiezen (afbeelding 1).

Na de tutorial belandt u in het hoofdvenster van SpywareBlaster. Hier klikt u eerst op *Download Latest Protection Updates*, waarna het updatevenster opent (afbeelding 2). Daarin klikt u op de knop *Check for Updates* en vervolgens zal een eventuele update direct gedownload worden (afbeelding 3). Als de updates gedownload zijn, klikt u linksboven in het venster op *Protection Status* (afbeelding 4), waarna u de bescherming activeert door op *Enable All Protection* te klikken. Alle in rood aangegeven teksten en iconen zullen vervolgens groen worden als teken dat de bescherming ingeschakeld is (afbeelding 5). Onder *Protection Status* kunt u nu zien welke bescherming SpywareBlaster voor Internet Explorer heeft ingeschakeld en welke sites in de internetzone met beperkte toegang zijn geplaatst.

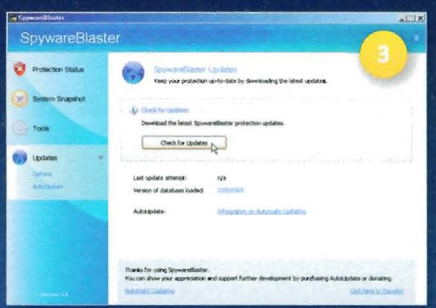
SpywareBlaster biedt ook enige bescherming voor Firefox. Deze beperkt zich echter tot het weren van tracking cookies, een mogelijkheid die Firefox zelf niet heeft. Omdat deze browser geen gebruik maakt van ActiveX is bescherming tegen toepassingen van deze categorie niet nodig. Wilt u voorkomen dat Firefox kwaadaardige scripts uitvoert, dan kunt u de add-on NoScript (http://ct.link.idg.nl/noscript) installeren.



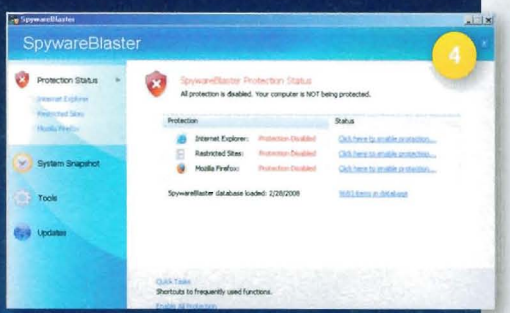
▲ *Controleer om de paar weken op updates voor SpywareBlaster.*



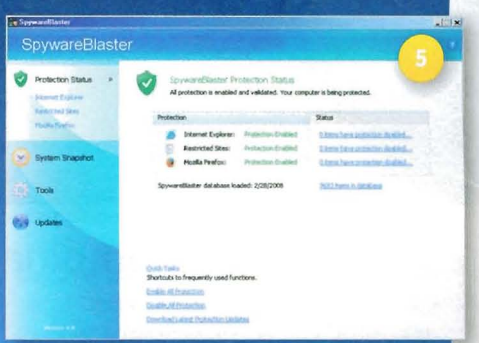
▲ *Het updatevenster..*



▲ *Updates worden direct gedownload..*



▲ *Na een update activeert u de bescherming met één muisklik.*



▶ *De bescherming is ingeschakeld.*

Deze voorkomen dat kwaadaardige ActiveX-elementen gedownload, geïnstalleerd of uitgevoerd worden. Daarnaast plaatst het programma enkele duizenden sites, waarvan bekend is dat ze malware op uw pc kunnen installeren, in de internetzone met beperkte toegang. Voor deze zone geldt de hoogste beveiliging, waardoor het installeren van ActiveX-elementen en het uitvoeren van scripts door deze sites onmogelijk wordt. Zie het kader voor installatie en gebruik.

TOT SLOT

Een goede firewall, een goede virusscanner en SpywareBlaster voorzien uw pc van een uitstekende en in veel gevallen afdoende beveiliging, waardoor het systeem niet overmatig belast wordt. Bedenk dat dit niet de enige en evenmin de belangrijkste factoren in uw beveiliging zijn. Zo is het van groot belang dat uw besturingssysteem en alle overige programma's van de laatste beveiligingsupdates zijn voorzien.

Windows en Office houdt u moeiteloos up-to-date door via het Configuratiescherm de Automatische Updates in te schakelen. Om te controleren of uw overige programma's updates nodig hebben, kunt u de pc regelmatig online laten scannen door de Secunia Software Inspector (u vindt deze op http://secunia.com/software_inspector).

En over scannen gesproken: een maandelijkse online malwarescan via het al eerder genoemde Kaspersky (www.kaspersky.com/virusscanner) of Trend Micro's Housecall (http://housecall.trendmicro.com) is aan te raden.

Als uw pc normaal functioneert zal dit hooguit enkele *low level threats* opleveren, waar u zich geen zorgen over hoeft te maken. Andere scans uitvoeren of vaker scannen is overbodig, zolang de pc geen vreemd gedrag vertoont.

De grootste kans op een malware-infectie loopt u echter nog altijd door onverstandig surf-, en downloadgedrag en door de wijze waarop u met uw e-mail en e-mailbijlagen omgaat. En dat komt nu aan de orde...

▲ *Houd de programma's op uw pc actueel met Secunia.*

Veilig surfen, downloaden en e-mailen

De meeste malwarebesmettingen worden niet veroorzaakt door een gebrek in de beveiligingssoftware, maar door ondoordacht gedrag van de gebruiker tijdens het surfen, downloaden en e-mailen. Een verstandig internetgebruik is daarom de belangrijkste factor bij het virus- en spywarevrij houden van uw pc. Door eenvoudigweg een beetje uit te kijken bij uw activiteiten op het *world wide web* vermindert u de kans op een malware-infectie drastisch.

Om te beginnen hebt u een veilige browser nodig. De twee meest gebruikte browsers (Internet Explorer en Firefox) zijn redelijk goed beveiligd, vooropgesteld dat ze van de laatste updates zijn voorzien. Toch kunnen deze browsers nog wel enige extra bescherming gebruiken. Het beste programma hiervoor is SpywareBlaster (zie pagina 22). De veiligste browser is op dit moment Opera, dat geen aanvullende bescherming nodig heeft.

▲ *Opera laat in het adresveld zien of een site betrouwbaar is.*

DUBIEUZE SITES

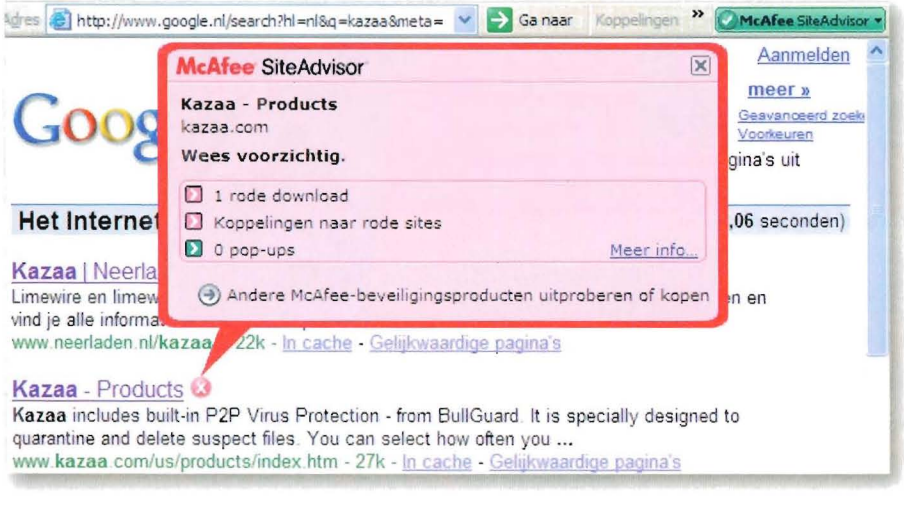
Behalve via lekken in browsers installeren onbetrouwbare sites malware vaak via scripts of kwetsbaarheden in browserplug-ins. Om dit te voorkomen kunt u uiteraard het uitvoeren van scripts onmogelijk maken en allerhande browserplug-ins uitschakelen, maar op deze manier mist u natuurlijk wel de vele leuke mogelijkheden die u hiermee op betrouwbare sites hebt. Het alternatief is dus ervoor te zorgen dat u niet op malafide sites terechtkomt.

Dat kunt u ten eerste doen door bepaalde categorieën sites te vermijden. Pornosites, goksites en sites waar illegale software, cracks en serials worden aangeboden zijn beruchte malwareverspreiders, die u beter nooit kunt bezoeken. Natuurlijk zijn er ook onbetrouwbare sites die niet tot een van deze groepen behoren. Wanneer u zo'n site via Google wilt bezoeken, zult u de waarschuwing krijgen dat uw computer en persoonlijke gegevens mogelijk gevaar lopen als u dit doet. De zoekmachine gebruikt hiervoor een database die permanent bijgewerkt wordt en gegevens over duizenden sites met minder goede bedoelingen bevat.

SITEADVISOR

Een ander handig hulpmiddel om te zien of u met een gerust hart naar een bepaalde site kunt gaan is de McAfee SiteAdvisor (www.siteadvisor.com). Via een kleurenindicator in de browser krijgt u te zien of de bezochte site te vertrouwen is. Kleurt de indicator rood, dan is dat niet het geval. Dat wil natuurlijk nog helemaal niet zeggen dat u dan ook meteen een besmetting hebt opgelopen, maar het is wel aan te raden de betreffende site verder links te laten liggen. Daarnaast toont de SiteAdvisor onveilige sites in de zoekresultaten van Google.

▼ *SiteAdvisor geeft een waarschuwing bij malafide websites.*



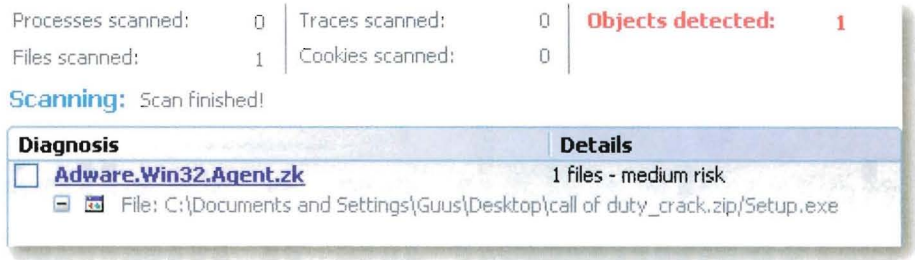
VEILIG DOWNLOADEN

Wilt u een minder bekend programma gebruiken, maar weet u niet zeker of dit veilig is, zoekt u dan via Google op de term **spyware**, in combinatie met naam van de betreffende applicatie. U komt er dan snel achter of deze malware bevat of niet. Als extra voorzorg kunt u dergelijke programma's na het downloaden even scannen via de *on demand* scanfunctie van uw virusscanner.

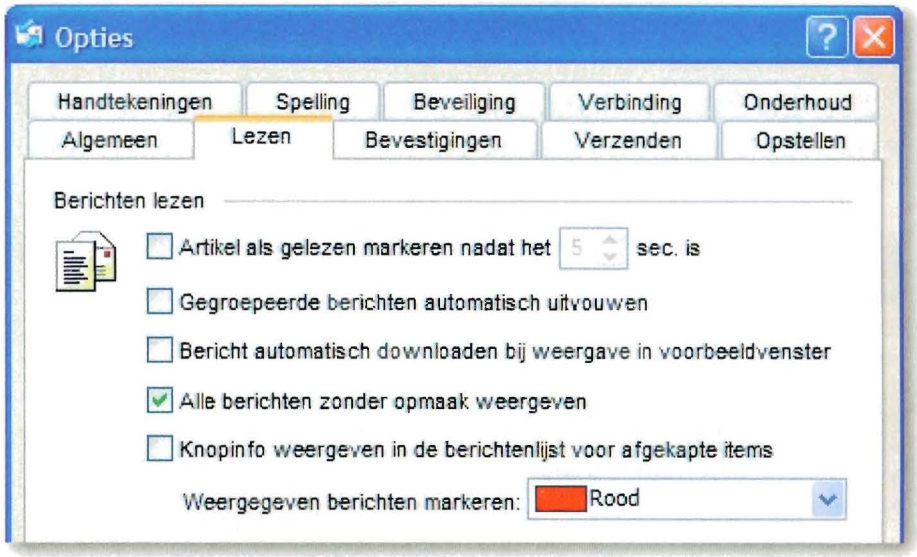
Muziek en films worden voornamelijk via p2p-programma's, nieuwsgroepen en BitTorrent gedownload. De laatste twee methoden zijn redelijk veilig, maar met p2p-programma's als LimeWire en BearShare moet u op uw hoede zijn. De netwerken waar deze programma's gebruik van maken zijn enorm vervuild met malware. Eigenlijk is alleen het downloaden van muziek via deze programma's veilig, al moet u ook daarbij voorzichtig

zijn. Het downloaden van (illegale) programma's, cracks en serials langs deze weg is vragen om moeilijkheden.

Programma's als LimeWire en BearShare bevatten overigens filters, waarmee u voorkomt dat bepaalde bestandstypen of sleutelwoorden in de zoekresultaten opduiken. U kunt op deze manier zelfs zodanig filteren dat uitsluitend muziekbestanden getoond worden. Al is het downloaden van muziek via deze programma's redelijk veilig, u moet wel alert blijven. Een bestand van 117 kB dat volgens de titel de Vijfde Symfonie van Beethoven is, is dat zeker niet. In het gunstigste geval gaat het om een flauwe soundbite, maar het bestand kan ook iets schadelijkers verbergen.



▲ *Cracks bevatten vaak nare verrassingen.*



▼ *Laat ontvangen berichten als platte tekst weergeven.*

VEILIG E-MAILEN

Veel mensen gebruiken Outlook, Outlook Express, Thunderbird of een soortgelijk mailprogramma. Daarnaast wordt vaak een *web based* e-maildienst als Hotmail of Gmail gebruikt. Het is aan te raden beide te gebruiken, en daarbij een scheiding te maken tussen de doeleinden waarvoor u elk van deze accounts aanwendt.
Zo kunt u een webmail-account gebruiken voor minder belangrijke zaken als registratie op een website of forum, terwijl u de e-mailaccount die u van uw provider krijgt voor zakelijk en privé-gebruik reserveert. Deze laatste beheert u dan via een van de genoemde programma's. Evenals uw browser moet uw e-mailprogramma van de laatste beveiligingsupdates voorzien zijn. Als u ervoor zorgt dat het adres van deze account uitsluitend bekend blijft bij vertrouwde contactpersonen, dan zult u weinig of geen ongewenste of riskante post via deze account ontvangen.

Loopt de hoeveelheid ongewenste post in uw Hotmail-account de spuigaten uit, dan gebruikt u deze eenvoudigweg niet meer en maakt u een nieuwe aan.

WEES OP UW HOEDE

Wanneer u mail ontvangt zijn er een paar zaken die u in de gaten moet houden. Dat is ten eerste de afzender en ten tweede de eventuele bijlage die een bericht vergezelt. Post van bekenden kunt u doorgaans gewoon openen. Met bijlagen moet u iets voorzichtiger zijn, ook als ze van familie, vrienden of kennissen afkomstig zijn; u zult niet de eerste zijn die een leuk spelletje toegestuurd krijgt, waarvan de afzender niet weet dat het een virus bevat. Sla dergelijke bestanden eerst op en scan ze op malware voordat u ze opent. Post van onbekenden, met of zonder bijlagen, kunt u het best direct naar de prullenbak verwijzen.
Zorg er verder voor dat ontvangen berichten niet als html, maar als platte tekst worden weergegeven. In Outlook Express doet u dat door naar *Extra* / *Opties* te gaan en op het tabblad *Lezen* de optie *Alle berichten zonder opmaak weergeven* aan te vinken. Dit voorkomt dat eventueel kwaadaardige html-code wordt uitgevoerd. In uw web-based mailaccount zal een ontvangen bericht altijd in platte tekst getoond worden.

Verder moet u nooit ingaan op verzoeken via e-mail om wachtwoorden te verstrekken. Criminelen proberen u deze gegevens soms afhandig te maken via nagemaakte e-mails die bijvoorbeeld van uw bank of internetprovider afkomstig lijken te zijn. Deze zullen echter nooit op die manier dergelijke informatie van u vragen. Krijgt u zo'n verzoek, meld dit dan bij de betreffende bank of bij uw internetprovider.

TOT SLOT

Wanneer u bovenstaande voorzorgsmaatregelen in acht neemt en daarbij de benodigde beveiligingssoftware gebruikt, hoeft u zich weinig zorgen te maken over malware-infecties. Met een maandelijkse online scan op malware controleert u dat de in dit artikel besproken tips en programma's voldoende bescherming bieden: onze scans vinden steevast niets of hooguit een enkele *low level threat*.

▼ *Aan de omvang is te zien dat het geselecteerde bestand niet hetgeen is dat gezocht wordt.*