bitdefender

# ANTIVIRUS 2008

## Gebruiksaanwijzing

# BitDefender Antivirus 2008
## *Gebruiksaanwijzing*

Uitgegeven 2008.03.19



### Wettelijke verklaring


bitdefender

# Inhoudsopgave

**Licentie en garantie** ..... vii

**Voorwoord** ..... xi

1. Conventies die in dit boek worden gebruikt ..... xi
   1.1. Typografische conventies ..... xi
   1.2. Waarschuw. ..... xii
2. De boekstructuur ..... xii
3. Verzoek om commentaar ..... xiii

***Installatie*** ..... 1

**1. Installatie BitDefender Antivirus 2008** ..... 2

1.1. Systeemvereisten ..... 2
1.2. Installatiestappen ..... 3
1.3. Initiële configuratiewizard ..... 5
   1.3.1. Stap 1/6 - BitDefender Antivirus 2008 registreren ..... 6
   1.3.2. Stap 2/6 - Een BitDefender-account maken ..... 7
   1.3.3. Stap 3/6 - Informatie over Real-Time Virusrapportage (RTVR) ..... 9
   1.3.4. Stap 4/6 – De uit te voeren taken selecteren ..... 10
   1.3.5. Stap 5/6 - Wacht tot de taken zijn voltooid ..... 11
   1.3.6. Stap 6/6 – Overzicht weergeven ..... 12
1.4. Upgrade ..... 12
1.5. BitDefender repareren of verwijderen ..... 13

***Basisbeheer*** ..... 15

**2. Aan de slag** ..... 16

2.1. BitDefender Icon in het Systeemvak ..... 17
2.2. Balk scanactiviteit ..... 18
2.3. BitDefender Handmatig scannen ..... 18
2.4. Spelmodus ..... 19
   2.4.1. Gebruik van de Spelmodus ..... 19
   2.4.2. Veranderen van de Spelmodus sneltoets ..... 20

**3. Beveiligingsstatus** ..... 21

3.1. Knop Antivirusstatus ..... 23
3.2. Knop Antiphishing-status ..... 23
3.3. Identiteitscontrole statusknop ..... 24
3.4. Knop Updatestatus ..... 25

**4. Snelle taken** ..... 26

4.1. Beveiliging ..... 26
   4.1.1. Updaten BitDefender ..... 26

4.1.2. Scannen met BitDefender . . . . . 28

**5. Geschiedenis . . . . . 34**

**6. Registratie . . . . . 36**
6.1. Stap 1/3 - BitDefender Antivirus 2008 registreren . . . . . 36
6.2. Stap 2/3 - Een BitDefender-account maken . . . . . 37
6.3. Stap 3/3 - BitDefender Antivirus 2008 registreren . . . . . 39

***Geavanceerd beveiligingsbeheer . . . . . 40***

**7. Instellingsconsole . . . . . 41**
7.1. Algemene instellingen configureren . . . . . 42
7.1.1. Algemene instellingen . . . . . 43
7.1.2. Virusrapportinstellingen . . . . . 44
7.1.3. Instellingen beheren . . . . . 44

**8. Antivirus . . . . . 45**
8.1. Scannen bij toegang . . . . . 45
8.1.1. Het beveiligingsniveau configureren . . . . . 47
8.1.2. Het beveiligingsniveau aanpassen . . . . . 47
8.1.3. Real time-beveiliging uitschakelen . . . . . 51
8.2. Scannen op aanvraag . . . . . 52
8.2.1. Scantaken . . . . . 53
8.2.2. Het snelmenu gebruiken . . . . . 55
8.2.3. Scantaken maken . . . . . 56
8.2.4. Scantaken configureren . . . . . 57
8.2.5. Objecten scannen . . . . . 67
8.2.6. Scanlogboeken weergeven . . . . . 74
8.3. Objecten die zijn uitgesloten van het scannen . . . . . 76
8.3.1. Paden uitsluiten van het scannen . . . . . 78
8.3.2. Extensies uitsluiten van het scannen . . . . . 80
8.4. Quarantainegebied . . . . . 83
8.4.1. Bestanden in quarantaine beheren . . . . . 84
8.4.2. Quarantaine-instellingen configureren . . . . . 84

**9. Privacybeheer . . . . . 86**
9.1. Status Privacybeheer . . . . . 86
9.1.1. Privacybeheer . . . . . 87
9.1.2. Antiphishing-beveiliging . . . . . 88
9.2. Geavanceerde instellingen - Identiteitscontrole . . . . . 89
9.2.1. Privacyregels maken . . . . . 90
9.2.2. Uitzonderingen definiëren . . . . . 93
9.2.3. Regels beheren . . . . . 94
9.3. Geavanceerde instellingen - Registerbeheer . . . . . 95
9.4. Geavanceerde instellingen - Cookiebeheer . . . . . 97
9.4.1. Configuratiewizard . . . . . 99

9.5. Geavanceerde instellingen - Scriptbeheer ..... 101
9.5.1. Configuratiewizard ..... 103
9.6. Systeeminformatie ..... 103
9.7. Antiphishing-werkbalk ..... 105

**10. Update ..... 107**
10.1. Automatische update ..... 107
10.1.1. Een update aanvragen ..... 109
10.1.2. Automatisch update uitschakelen ..... 109
10.2. Update-instellingen ..... 110
10.2.1. De updatelocaties instellen ..... 110
10.2.2. Automatische update configureren ..... 111
10.2.3. Handmatige update configureren ..... 112
10.2.4. Geavanceerde instellingen configureren ..... 112
10.2.5. Proxy's beheren ..... 113

***BitDefender reddingsschijf ..... 116***

**11. Overzicht ..... 117**
11.1. Systeemvereisten ..... 117
11.2. Bijgeleverde software ..... 118

**12. De BitDefender reddingsschijf gebruiken ..... 121**
12.1. BitDefender reddingsschijf starten ..... 121
12.2. BitDefender reddingsschijf stoppen ..... 122
12.3. Hoe kan ik een antivirusscan uitvoeren? ..... 123
12.4. Hoe kan ik BitDefender updaten over een proxy? ..... 124
12.5. Hoe kan ik mijn gegevens opslaan? ..... 125

***Hulp vragen ..... 127***

**13. Ondersteuning ..... 128**
13.1. BitDefender Knowledge Base ..... 128
13.2. Hulp vragen ..... 129
13.2.1. Ga naar Web-selfservice ..... 129
13.2.2. Een ondersteuningsticket openen ..... 129
13.3. Contactinformatie ..... 130
13.3.1. Webadressen ..... 130
13.3.2. Bijkantoren ..... 130

**Woordenlijst ..... 133**

# Licentie en garantie

INSTALLEER DE SOFTWARE NIET ALS U NIET INSTEMT MET DEZE BEPALINGEN EN VOORWAARDEN. WANNEER U KLIKT OP "IK AANVAARD", "OK", "DOORGAAN" OF "JA", OF WANNEER U DE SOFTWARE OP ENIGE MANIER INSTALLEERT OF GEBRUIKT, DUIDT U AAN DAT U DE VOORWAARDEN VAN DEZE OVEREENKOMST VOLLEDIG BEGRIJPT EN AANVAARDT.

Deze voorwaarden dekken de oplossingen en diensten van BitDefender voor thuisgebruikers waarvoor u een licentie wordt verleend, inclusief verwante documentatie en elke update en upgrade van de toepassingen die u werden geleverd onder de aangekochte licentie of elke andere verwante serviceovereenkomst, zoals gedefinieerd in de documentatie en elke kopie van deze items.

De Licentieovereenkomst is een wettelijke overeenkomst tussen u (een natuurlijk persoon of een rechtspersoon) en BitDefender voor het gebruik van het hierboven geïdentificeerde softwareproduct van BitDefender. Dit omvat de computersoftware en diensten en kan verwante media, afgedrukte materialen, en "online" of elektronische documentatie (hierna aangegeven als "BitDefender") bevatten, die allemaal door de internationale wetten op auteursrecht en internationale verdragen worden beschermd. Door BitDefender te installeren, te kopiëren of te gebruiken, aanvaardt u dat u gebonden bent door de voorwaarden van deze overeenkomst.

Als u de voorwaarden van deze overeenkomst niet aanvaardt, mag u BitDefender niet installeren of gebruiken.

**BitDefender-licentie.** BitDefender is beschermd door de wetten op auteursrecht en internationale verdragen inzake auteursrecht en andere wetten en verdragen inzake intellectuele eigendom. Voor BitDefender wordt een licentie verleend. Het programma wordt dus niet verkocht.

LICENTIEVERLENING. BitDefender verleent u, en u alleen, hierbij de volgende niet-exclusieve, beperkte, niet-overdraagbare licentie met royalty's voor het gebruik van BitDefender.

TOEPASSINGSSOFTWARE U mag BitDefender installeren en gebruiken op zoveel computers als nodig met de beperking die is opgelegd door het totaal aantal gelicentieerde gebruikers. U mag één extra kopie maken voor back-updoeleinden.

DESKTOPGEBRUIKERSLICENTIE Deze licentie is van toepassing op de BitDefender-software die kan worden geïnstalleerd op één computer die geen netwerkdiensten biedt. Elke primaire gebruiker mag deze software installeren op één computer en mag één extra kopie maken op een ander apparaat voor

back-updoeleinden. Het toegelaten aantal primaire gebruikers is het aantal gebruikers van de licentie.

DUUR VAN DE LICENTIE. De hieronder verleende licentie zal beginnen op de aankoopdatum van BitDefender en zal vervallen aan het einde van de periode waarvoor de licentie is aangekocht.

VERVALDATUM. Het product zal zijn functies niet langer uitvoeren zodra de licentie is verlopen.

UPGRADES. Als BitDefender wordt gelabeld als een upgrade, moet u over de geschikte licentie beschikken om een product te gebruiken dat door BITDEFENDER is aangeduid als in aanmerking komend voor de upgrade, om BitDefender te gebruiken. Een versie van BitDefender die als upgrade is gelabeld, vervangt en/of vult het product aan dat werd gebruikt als basis om te bepalen of u in aanmerking kwam voor de upgrade. U mag het resulterende upgradeproduct uitsluitend gebruiken in overeenstemming met de voorwaarden van deze Licentieovereenkomst. Als BitDefender een upgrade is van een component van een pakket softwareprogramma's, dat u als alleenstaand product hebt gelicentieerd, dan kan BitDefender alleen worden gebruikt of overgedragen als onderdeel van dit alleenstaand productpakket en mag hij niet worden gescheiden voor gebruik door meer dan het totale aantal gelicentieerde gebruikers. De voorwaarden en bepalingen van deze licentie vervangen en krijgen de voorrang op alle voorafgaande overeenkomsten die mogelijk bestonden tussen u en BITDEFENDER met betrekking tot het originele product of het resulterende product na een upgrade.

AUTEURSRECHT. Alle rechten, aanspraken op en belangen in BitDefender en alle auteursrechten in en voor BitDefender (met inbegrip van, maar niet beperkt tot elke afbeelding, foto, logo, animatie, video, audio, muziek, tekst en "applet" die in BitDefender zijn geïntegreerd), de begeleidende gedrukte materialen en elke kopie van BitDefender zijn eigendom van BITDEFENDER. BitDefender is beschermd door wetten op auteursrecht en internationale verdragsvoorwaarden. U moet BitDefender daarom behandelen als elk ander materiaal dat auteursrechtelijk is beschermd. U mag geen kopieën maken van het gedrukte materiaal, dat bij BitDefender wordt geleverd. U moet alle auteursrechtelijke bepalingen produceren en overnemen in hun oorspronkelijke vorm voor alle gemaakte kopieën, ongeacht de media of de vorm waarin BitDefender bestaat. U mag een licentie van BitDefender niet verhuren, verkopen, leasen of delen. U mag geen reverse engineering toepassen, niet opnieuw compileren, demonteren, afgeleide werken maken, vertalen, of enige poging ondernemen om de broncode van BitDefender te onthullen.

BEPERKTE GARANTIE. BITDEFENDER garandeert dat de media waarop BitDefender wordt verdeeld, vrij is van defecten gedurende een periode van dertig dagen vanaf

de datum waarop BitDefender aan u werd geleverd. Uw enig verhaal bij een inbreuk op deze garantie, is dat BITDEFENDER, volgens eigen voorkeur, de defecte media vervangt na ontvangst van de beschadigde media, of het bedrag, dat u voor BitDefender hebt betaald, terugbetaalt. BITDEFENDER biedt geen garantie dat BitDefender ongestoord of vrij van fouten zal werken, of dat de fouten zullen worden gecorrigeerd. BITDEFENDER garandeert niet dat BitDefender zal voldoen aan uw behoeften.

TENZIJ UITDRUKKELIJK UITEENGEZET IN DEZE OVEREENKOMST, WIJST BITDEFENDER ALLE ANDERE GARANTIES, UITDRUKKELIJK OF IMPLICIET, AF MET BETREKKING TOT DE PRODUCTEN, VERBETERINGEN, ONDERHOUD OF ONDERSTEUNING DIE HIERMEE VERWANT IS OF ALLE ANDERE MATERIALEN (TASTBAAR OF NIET-TASTBAAR) DIE DOOR BITDEFENDER ZIJN GELEVERD. BITDEFENDER WIJST HIERBIJ UITDRUKKELIJK ALLE IMPLICIETE GARANTIES EN BEPALINGEN AF, MET INBEGRIP VAN, MAAR NIET BEPERKT TOT IMPLICIETE GARANTIES VAN VERKOOPBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL, AANSPRAKEN, NIET-INTERFERENTIE, NAUWKEURIGHEID VAN GEGEVENS, NAUWKEURIGHEID VAN INFORMATIEVE INHOUD, SYSTEEMINTEGRATIE EN NIET-INBREUK VAN RECHTEN VAN DERDEN DOOR HET FILTEREN, UITSCHAKELEN OF VERWIJDEREN VAN DERGELIJKE SOFTWARE VAN DERDEN, SPYWARE, ADWARE, COOKIES, E-MAILS, DOCUMENTEN, ADVERTENTIES OF GELIJKSOORTIGE ZAKEN, ONGEACHT OF ZE VOORTVLOEIEN UIT STATUTEN, WETTEN, HANDELSWIJZEN, DOUANE EN PRAKTIJKEN, OF HANDELSGEBRUIK.

AFWIJZING VAN SCHADE. Iedereen die BitDefender gebruikt, test of evalueert draagt het volledige risico met betrekking tot de kwaliteit en prestatie van BitDefender. BITDEFENDER zal in geen geval aansprakelijk zijn voor elke willekeurige schade, met inbegrip van en zonder beperking op directe of indirecte schade, voortvloeiend uit het gebruik, de prestatie of de levering van BitDefender, zelfs indien BITDEFENDER op de hoogte werd gesteld van het bestaan of de mogelijkheid van dergelijke schade. SOMMIGE LANDEN STAAN DE BEPERKING OF UITSLUITING VAN AANSPRAKELIJKHEID VOOR INCIDENTELE OF GEVOLGSCHADE NIET TOE. DE BOVENSTAANDE BEPERKING OF UITSLUITING ZAL BIJGEVOLG MOGELIJK NIET VAN TOEPASSING ZIJN OP U. IN GEEN GEVAL ZAL DE AANSPRAKELIJKHEID VAN BITDEFENDER DE AANKOOPPRIJS, DIE U VOOR BITDEFENDER HEBT BETAALD, OVERSCHRIJDEN. De afwijzingen en beperkingen, zoals hierboven beschreven, zullen steeds worden toegepast ongeacht of u BitDefender gebruikt, evalueert of test.

**BELANGRIJKE MEDEDELING AAN GEBRUIKERS.** DEZE SOFTWARE IS NIET FOUT-TOLERANT EN IS NIET ONTWIKKELD OF BEDOELD VOOR GEBRUIK IN

EEN GEVAARLIJKE OMGEVING DIE EEN STORINGSVEILIGE PRESTATIE OF WERKING VEREIST. DEZE SOFTWARE IS NIET VOOR GEBRUIK BIJ DE BEDIENING VAN VLIEGTUIGNAVIGATIE, NUCLEAIRE FACILITEITEN OF COMMUNICATIESYSTEMEN, WAPENSYSTEMEN, DIRECTE OF INDIRECTE LIFE-SUPPORTSYSTEMEN, LUCHTVERKEERSLEIDING, OF ELKE TOEPASSING OF INSTALLATIE WAAR DEFECTEN DE DOOD, ERNSTIGE LICHAMELIJKE LETSELS OF MATERIËLE SCHADE KUNNEN VEROORZAKEN.

ALGEMEEN. Deze overeenkomst zal worden beheerd door de Roemeense wetten en de internationale voorschriften en verdragen inzake auteursrecht. De exclusieve jurisdictie en rechtsgebied om elk geschil te beslechten dat voortvloeit uit deze licentievoorwaarden, ligt bij de rechtbanken van Roemenië.

Prijzen, kosten en vergoedingen voor het gebruik van BitDefender zijn onderhevig aan wijzigingen zonder dat u hiervan vooraf op de hoogte wordt gebracht.

In geval van ongeldigheid van een willekeurige voorwaarde van deze overeenkomst, zal de ongeldigheid geen invloed hebben op het resterende gedeelte van deze overeenkomst.

BitDefender en de logo's van BitDefender zijn handelsmerken van BITDEFENDER. Alle overige handelsmerken die in het product of in verwante materialen worden gebruikt, zijn eigendom van hun respectieve eigenaars.

De licentie wordt onmiddellijk beëindigd zonder kennisgeving als u een van deze voorwaarden en bepalingen overtreedt. U zult geen aanspraak kunnen maken op een terugbetaling van BITDEFENDER of enige andere wederverkopers van BitDefender na het beëindigen omwille van deze reden. De voorwaarden en bepalingen met betrekking tot de vertrouwelijkheid en beperkingen op het gebruik zullen van kracht blijven, zelfs na het beëindigen van de licentie.

BITDEFENDER kan deze voorwaarden op elk ogenblik herzien en de herziene voorwaarden zullen automatisch van toepassing zijn op de overeenkomende versies van de software die wordt verdeeld met de herziene voorwaarden. Als een van deze voorwaarden ongeldig is of niet kan worden afgedwongen, zal dit de geldigheid van de rest van de voorwaarden niet beïnvloeden die geldig en afdwingbaar blijven.

In geval van tegenstrijdigheid of inconsistentie tussen de vertalingen van deze voorwaarden in andere talen, zal de Engelse versie die door BITDEFENDER is uitgegeven, de voorrang krijgen.

Neem contact op met BITDEFENDER op het adres 5, Fabrica de Glucoza str., 72322-Sector 2, Boekarest, Roemenië of op het telefoonnr.: 40-21-2330780 of Fax: 40-21-2330763, e-mailadres: office@bitdefender.com.

# Voorwoord

Deze handleiding is bedoeld voor alle gebruikers die voor **BitDefender Antivirus 2008** hebben gekozen als een beveiligingsoplossing voor hun computers. De informatie die in dit boek wordt geleverd is niet alleen geschikt voor geavanceerde computergebruikers, maar is ook gemakkelijk te begrijpen door iedereen die met Windows kan werken.

Dit boek biedt u een beschrijving van **BitDefender Antivirus 2008**, het bedrijf en het team dat het programma heeft samengesteld. Het zal u ook begeleiden doorheen de installatieprocedure en u leren hoe u het programma kunt configureren. U zult leren hoe u **BitDefender Antivirus 2008** kunt gebruiken, updaten, testen en aanpassen. Deze handleiding biedt u alle informatie die u nodig hebt om optimaal gebruik te maken van BitDefender.

Wij wensen u veel aangenaam en nuttig leesplezier.

# 1. Conventies die in dit boek worden gebruikt

## 1.1. Typografische conventies

In dit boek worden verschillende tekststijlen gebruikt, zodat de tekst leesbaarder is. De weergave en betekenis worden in de onderstaande tabel weergegeven.

| Weergave | Beschrijving |
|---|---|
| `sample syntax` | Syntaxisvoorbeelden zijn gedrukt in `enkelspatietekens`. |
| http://www.bitdefender.com | De URL-koppeling wijst naar een externe locatie op http- of ftp-servers. |
| support@bitdefender.com | E-mailadressen worden in de tekst ingevoegd voor contactgegevens. |
| “Voorwoord” (p. xi) | Dit is een interne koppeling naar een locatie in het document. |
| `filename` | Bestandsnamen en mappen worden afgedrukt met een `enkelspatielettertype`. |

| Weergave | Beschrijving |
|---|---|
| **option** | Alle productopties worden afgedrukt met **harde** tekens. |
| `sample code listing` | De codeweergave wordt gedrukt met `enkelspatietekens`. |

## 1.2. Waarschuw.

De waarschuwingen zijn opmerkingen in de tekst die grafisch zijn gemarkeerd en uw aandacht wordt getrokken naar extra informatie met betrekking tot de huidige paragraaf.

***Opmerking***
De opmerking is slechts een kort commentaar. Hoewel u opmerkingen kunt weglaten, kunnen ze toch waardevolle informatie bieden zoals over een specifieke functie of een koppeling naar een verwant onderwerp.

***Belangrijk***
Dit vereist uw aandacht en het wordt niet aanbevolen dit te negeren. Doorgaans betreft het niet-kritische, maar belangrijke informatie.

***Waarschuwing***
Dit is kritische informatie die u aandachtig moet lezen. Er zullen geen ernstige problemen optreden als u de aanwijzingen volgt. U moet de informatie lezen en begrijpen omdat hier iets wordt beschreven dat hoge risico's inhoudt.

# 2. De boekstructuur

Het boek bestaat uit verschillende delen die de belangrijkste onderwerpen bevatten. Bovendien vindt u ook een woordenlijst die enkele technische termen toelicht.

**Installatie.** Stapsgewijze instructies voor het installeren van BitDefender op een werkstation. Dit is een uitgebreide les over het installeren van **BitDefender Antivirus 2008**. Er wordt gestart met de vereisten voor een geslaagde installatie. Daarna wordt u verder begeleid doorheen het volledige installatieproces. Tot slot wordt de verwijderingsprocedure beschreven voor het geval u BitDefender moet verwijderen.

**Basisbeheer.** Beschrijving van het basisbeheer en onderhoud van BitDefender.

**Geavanceerd beveiligingsbeheer.** Een gedetailleerde voorstelling van de beveiligingsmogelijkheden die door BitDefender worden geboden. De hoofdstukken

bieden een gedetailleerde verklaring van alle opties van de console met de geavanceerde instellingen. U wordt geleerd hoe u alle BitDefender-modules te configureren en gebruiken om uw computer op een efficiënte manier te beveiligen tegen elk type malwarebedreiging (virussen, spyware, rootkits, enz.).

**BitDefender reddingsschijf.** Beschrijving van de BitDefender reddingsschijf. Dit zal u helpen de functies die door deze opstartbare cd worden geboden, te begrijpen en te gebruiken.

**Hulp vragen.** Informatie over waar u om hulp kunt vragen indien er zich onverwachte problemen voordoen.

**Woordenlijst.** De woordenlijst biedt een verklaring voor enkele technische en ongebruikelijke termen die u in de pagina's van het document zult vinden.

# 3. Verzoek om commentaar

We willen u uitnodigen ons te helpen dit boek te verbeteren. Wij hebben alle informatie zo goed mogelijk getest en gecontroleerd. Laat ons weten of u enige tekortkomingen hebt ontdekt in dit boek of als u ideeën hebt om dit te verbeteren, zodat wij u de best mogelijke documentatie kunnen bieden.

U kunt contact met ons opnemen door een e-mail te sturen naar documentation@bitdefender.com.

***Belangrijk***
Wij verzoeken u al uw e-mails met betrekking tot de documentatie in het Engels te schrijven, zodat we uw opmerkingen op een efficiënte manier kunnen verwerken.

# Installatie

# 1. Installatie BitDefender Antivirus 2008

Het hoofdstuk **BitDefender Antivirus 2008 installeren** van deze handleiding bevat de volgende onderwerpen:

- Systeemvereisten
- Installatiestappen
- Initiële configuratiewizard
- Upgrade
- BitDefender repareren of verwijderen

## 1.1. Systeemvereisten

Voor een correcte werking van het product, moet u vóór de installatie ervoor zorgen dat een van de volgende besturingssystemen op uw computer is geïnstalleerd en aan de overeenkomende systeemvereisten wordt voldaan:

- Besturingsplatform: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (of hoger)

### Windows 2000

- 800 MHz processor of hoger
- Minimum 256 MB RAM-geheugen (512 MB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

### Windows XP

- 800 MHz processor of hoger
- Minimum 256 MB RAM-geheugen (1 GB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

### Windows Vista

- 800 MHz processor of hoger
- Minimum 512 MB RAM-geheugen (1 GB aanbevolen)
- Minimum 60 MB beschikbare harde schijfruimte

**BitDefender Antivirus 2008** kan voor een evaluatie worden gedownload van de BitDefender website: http://www.bitdefender.com.

## 1.2. Installatiestappen

Zoek het installatiebestand en dubbelklik op dit bestand. Hierdoor wordt de installatiewizard gestart, die u zal helpen tijdens het installatieproces.

Voordat u de installatiewizard uitvoert, zal BitDefender controleren op nieuwere versies van het installatiepakket. Als er een nieuwere versie beschikbaar is, zult u worden gevraagd deze versie te downloaden. Klik op **Ja** om de nieuwere versie te downloaden of klik op **Nee** om door te gaan met de installatie van de versie die beschikbaar is in het installatiebestand.


**Installatiestappen**

Volg deze stappen om BitDefender Antivirus 2008 te installeren:

1. Klik op **Volgende** om door te gaan of klik op **Annuleren** als u de installatie wilt afbreken.

2. Klik op **Volgende**.

   BitDefender Antivirus 2008 waarschuwt u als er andere antivirusproducten op uw computer zijn geïnstalleerd. Klik op **Verwijderen** om het overeenkomende product te verwijderen. Klik op **Volgende** als u wilt doorgaan zonder de gedetecteerde producten te verwijderen.

   ***Waarschuwing***
   Het is sterk aanbevolen de andere gedetecteerde antivirusproducten te verwijderen voordat u BitDefender installeert. Het uitvoeren van twee of meer antivirusproducten tegelijk op een computer, maakt het systeem doorgaans onbruikbaar.

3. Lees de Licentieovereenkomst, selecteer **Ik aanvaard de voorwaarden van de Licentieovereenkomst** en klik op **Volgende**. Als u niet instemt met deze voorwaarden, klik dan op **Annuleren**. Het installatieproces wordt afgebroken en u verlaat de installatie.
4. BitDefender Antivirus 2008 wordt standaard geïnstalleerd onder `C:\Program Files\BitDefender\BitDefender 2008`. Als u het installatiepad wilt wijzigen, klikt u op **Bladeren** en selecteert u de map waarin u BitDefender Antivirus 2008 wilt installeren.

   Klik op **Volgende**.
5. Selecteer de opties met betrekking tot het installatieproces. Sommige opties zullen standaard zijn geïnstalleerd.
   - **Leesmij-bestand openen** - hiermee opent u het leesmij-bestand aan het einde van de installatie.
   - **Een snelkoppeling op het bureaublad plaatsen** - hiermee plaatst u een snelkoppeling naar BitDefender Antivirus 2008 op het bureaublad aan het einde van de installatie.
   - **Cd uitwerpen nadat installatie is voltooid** - om de cd uit te werpen aan het einde van de installatie. Deze optie verschijnt wanneer u het product vanaf de cd installeert.
   - **Windows Defender uitschakelen** - hiermee wordt Windows Defender uitgeschakeld. Deze optie verschijnt alleen in Windows Vista.

   Klik op **Installeren** om de installatie van het product te starten.

   ***Belangrijk***
   Tijdens het installatieproces verschijnt een wizard. De wizard helpt u bij het registreren van **BitDefender Antivirus 2008**, het maken van een BitDefender-account en het instellen van BitDefender voor het uitvoeren van belangrijke beveiligingstaken. Voltooi het door de wizard begeleide proces om naar de volgende stap te gaan.

6. Klik op **Voltooien**. U wordt gevraagd uw systeem opnieuw te starten zodat het installatieprogramma de installatie kan voltooien. Wij adviseren dit zo snel mogelijk te doen.

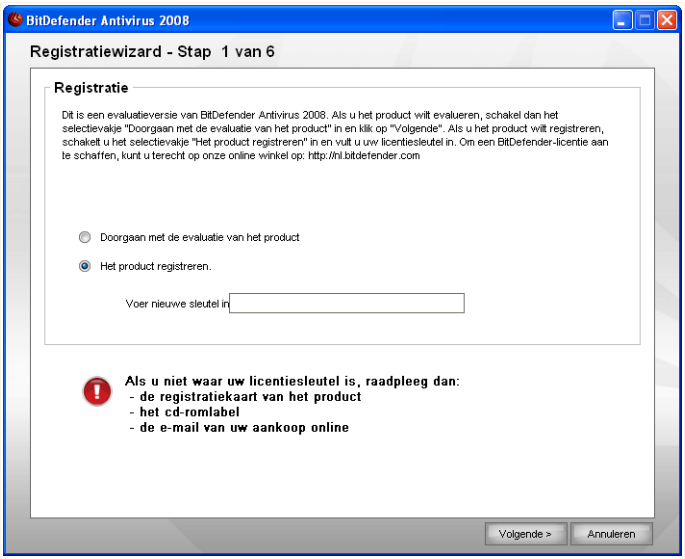
   Als u de standaardinstellingen voor het installatiepad hebt geaccepteerd, ziet u in `Program Files` een nieuwe map, genaamd `BitDefender`, met daarin de submap `BitDefender 2008`.

## 1.3. Initiële configuratiewizard

Tijdens het installatieproces verschijnt een wizard. De wizard helpt u bij het registreren van **BitDefender Antivirus 2008**, het maken van een BitDefender-account en het instellen van BitDefender voor het uitvoeren van belangrijke beveiligingstaken.

U bent niet verplicht deze wizard te voltooien. Wij raden u echter aan dit toch te doen om tijd te besparen en zeker te zijn dat uw systeem veilig is, zelfs voordat BitDefender Antivirus 2008 is geïnstalleerd.

## 1.3.1. Stap 1/6 - BitDefender Antivirus 2008 registreren



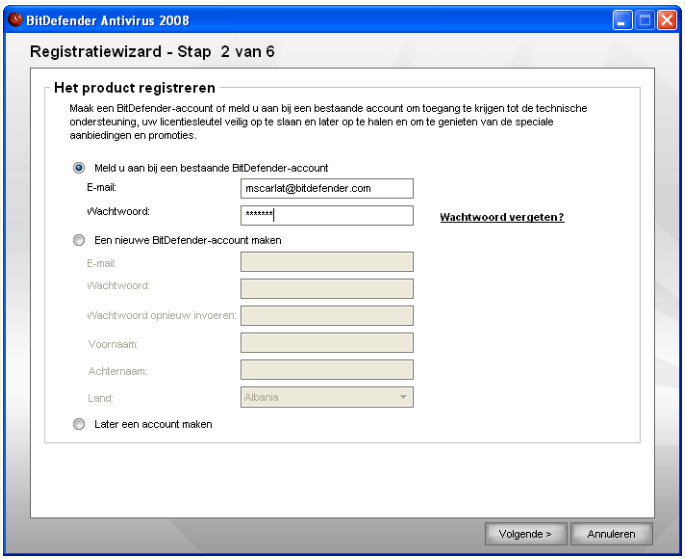

**Registratie**

Selecteer **Het product registreren** om **BitDefender Antivirus 2008** te registreren. Geef de licentiesleutel op in het veld **Voer nieuwe sleutel in**.

Selecteer **Doorgaan met de evaluatie van het product** om het product verder te testen.

Klik op **Volgende**.

## 1.3.2. Stap 2/6 - Een BitDefender-account maken




**Account maken**

### Ik heb geen BitDefender-account

Om van de gratis technische ondersteuning en andere gratis diensten van BitDefender te kunnen genieten, moet u een account maken.

***Opmerking***
Als u later een account wilt maken, selecteert u de overeenkomende optie.

Voor het maken van een BitDefender-account, selecteert u **Een nieuwe BitDefender-account maken** en geef de vereiste informatie op. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mail** - voer uw e-mailadres in.
- **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in.

*Opmerking*
Het wachtwoord moet minstens vier tekens bevatten.

- **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.
- **Voornaam** - voer uw voornaam in.
- **Achternaam** - voer uw achternaam in.
- **Land** - selecteer het land waar u woont.

*Opmerking*
Gebruik het door u ingevoerde e-mailadres en wachtwoord om in te loggen op uw account op http://myaccount.bitdefender.com.

Om een account te kunnen maken, moet u eerst uw e-mailadres activeren. Controleer uw e-mailadres en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Klik op **Volgende** om door te gaan.

## Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. In dit geval, klikt u alleen maar op **Volgende**.

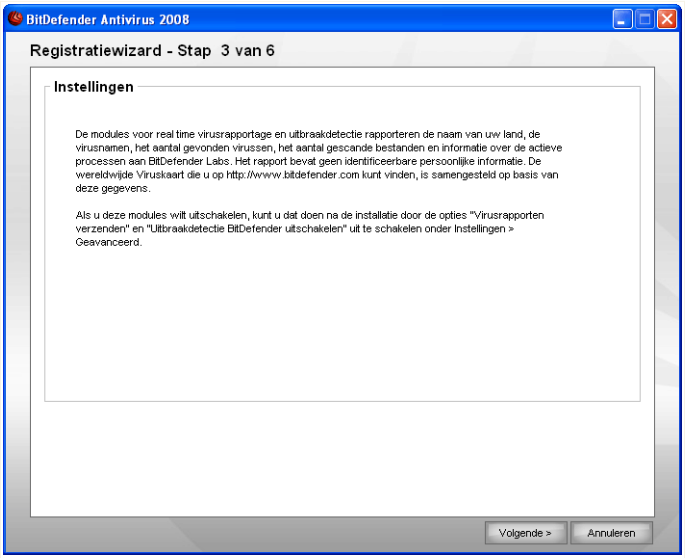
Als u al een actieve account hebt, maar BitDefender deze niet detecteert, selecteer dan **Inloggen op een bestaande BitDefender Account** en vul het e-mailadres en het wachtwoord van uw account in.

*Opmerking*
Als u een verkeerd wachtwoord hebt ingevuld, kunt u het opnieuw invullen nadat u hebt geklikt op **Next**. Klik op **Ok** om het wachtwoord opnieuw in te vullen of op **Annuleren** om het programma te verlaten.

Als u uw wachtwoord hebt gegeven, klikt u op **Wachtwoord vergeten?** en volgt u de instructies.

Klik op **Volgende** om door te gaan.

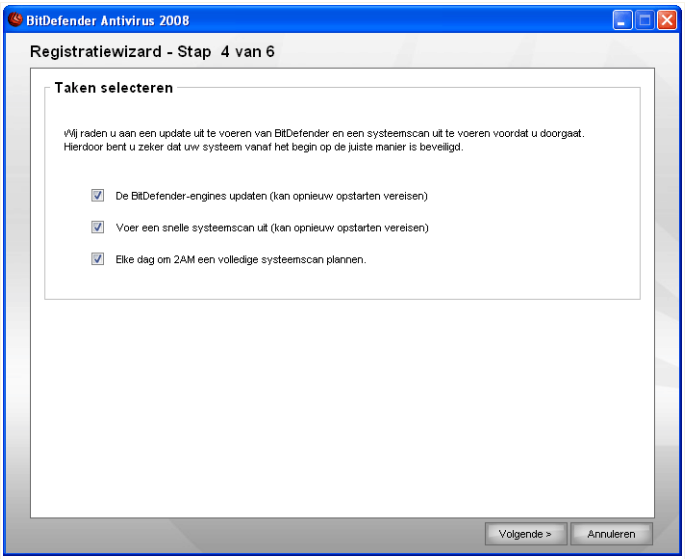
## 1.3.3. Stap 3/6 - Informatie over Real-Time Virusrapportage (RTVR)




**RTVR-informatie**

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

## 1.3.4. Stap 4/6 – De uit te voeren taken selecteren




**Taakselectie**

Stel BitDefender Antivirus 2008 in om belangrijke taken voor de beveiliging van uw systeem uit te voeren.

De volgende opties zijn beschikbaar:

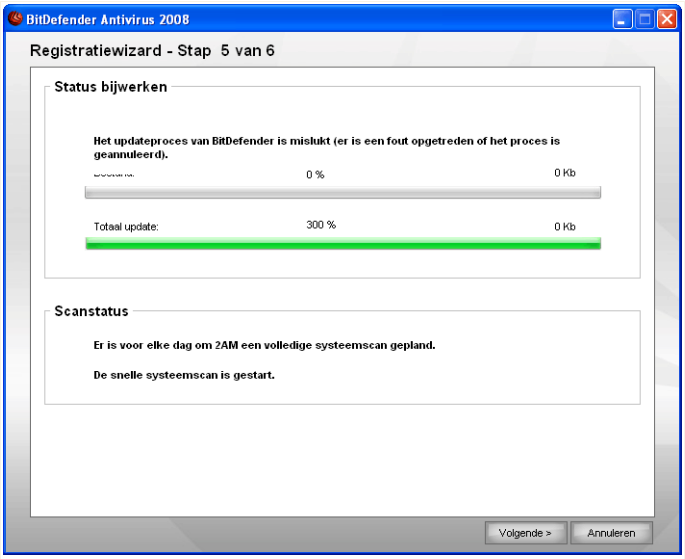
- **De BitDefender-engines updaten (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een update van de BitDefender-engines uitgevoerd om uw computer te beschermen tegen de meest recente bedreigingen.
- **Voer een snelle systeemscan uit (kan opnieuw opstarten vereisen)** - bij de volgende stap wordt een snelle systeemscan uitgevoerd zodat BitDefender kan controleren of uw bestanden in de mappen `Windows` en `Program Files` niet zijn geïnfecteerd.
- **Elke dag om 2 uur een volledige systeemscan uitvoeren** - voert elke dag om 2 uur een volledige systeemscan uit.

***Belangrijk***
Wij raden u aan deze opties in te schakelen voordat u naar de volgende stap gaat, zodat de beveiliging van uw systeem gegarandeerd is.

Als u alleen de laatste optie of geen enkele optie selecteert, wordt de volgende stap overgeslagen.

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

## 1.3.5. Stap 5/6 - Wacht tot de taken zijn voltooid

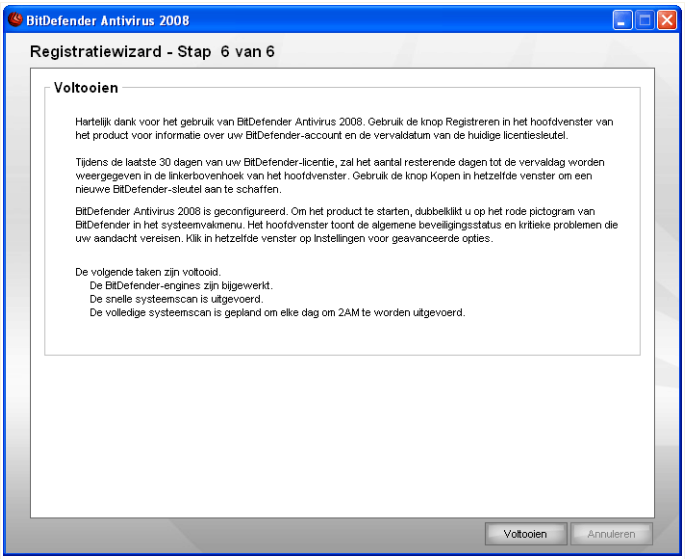



**Taakstatus**

Wacht tot de taak of taken zijn voltooid. U kunt de status bekijken van de taak of taken die in de vorige stap zijn geselecteerd.

Klik op **Volgende** om door te gaan of op **Annuleren** om de wizard af te sluiten.

### 1.3.6. Stap 6/6 – Overzicht weergeven




**Voltooien**

Dit is de laatste stap van de configuratiewizard.

Klik op **Installeren** om de installatie van het product te starten.

## 1.4. Upgrade

De upgradeprocedure kan op een van de volgende manieren worden uitgevoerd:

- **Installeren zonder de vorige versie te verwijderen - voor v8 of hoger, zonder Internet Security**

  Dubbelklik op het installatiebestand en volg de wizard die is beschreven in het gedeelte "*Installatiestappen*" (p. 3).

  ***Belangrijk***
  Tijdens het installatieproces zal een foutbericht verschijnen dat wordt veroorzaakt door de `Filespy-service`. Klik op **OK** om door te gaan met de installatie.

- **Verwijder uw vorige versie en installeer de nieuwe - voor alle BitDefender-versies**

  U moet eerst uw vorige versie verwijderen, vervolgens uw computer opnieuw opstarten en daarna de nieuwe versie installeren zoals beschreven in het hoofdstuk "*Installatiestappen*" (p. 3).

  ***Belangrijk***
  Als u een upgrade uitvoert vanaf BitDefender v8 of hoger, raden wij u aan de BitDefender-instellingen, de Vriendenlijst en de Spammerslijst op te slaan. Nadat de upgrade is voltooid, kunt u deze items laden.

## 1.5. BitDefender repareren of verwijderen

Als u **BitDefender Antivirus 2008** wilt repareren of verwijderen, volg dan dit pad vanaf het startmenu van Windows: **Start** → **Programma's** → **BitDefender 2008** → **Repareren of verwijderen**.

U wordt gevraagd uw keuze te bevestigen door te klikken op **Volgende**. Een nieuw venster wordt geopend, waarin u het volgende kunt selecteren:

- **Repareren** - om alle programmacomponenten die bij de vorige installatie werden geïnstalleerd, opnieuw te installeren.

  Als u ervoor kiest BitDefender te repareren, verschijnt een nieuw venster. Klik op **Repareren** om het reparatieproces te starten.

  Start de computer opnieuw op nadat u dit wordt gevraagd en klik daarna op **Installeren** om BitDefender Antivirus 2008 opnieuw te installeren.

  Nadat het installatieproces is voltooid, verschijnt een nieuw venster. Klik op **Voltooien**.
- **Verwijderen** - om alle geïnstalleerde componenten te verwijderen.

  ***Opmerking***
  Wij raden u aan de optie **Verwijderen** te selecteren voor een zuivere nieuwe installatie.

  Als u ervoor kiest BitDefender te verwijderen, verschijnt een nieuw venster.

  ***Belangrijk***
  Wanneer u BitDefender verwijdert, bent u niet langer beveiligd tegen malwarebedreigingen, zoals virussen en spyware. Als u wilt dat Windows Defender wordt ingeschakeld nadat u BitDefender hebt verwijderd, schakelt u het

overeenkomende selectievakje in. Deze optie is alleen beschikbaar op Windows Vista.

Klik op **Verwijderen** om het verwijderen van BitDefender Antivirus 2008 van uw computer te starten.

Tijdens het verwijderen wordt u gevraagd ons uw feedback te geven. Klik op **OK** om deel te nemen aan een online onderzoek van niet meer dan vijf korte vragen. Als u niet wilt deelnemen aan het onderzoek, klikt u op **Annuleren**.

Nadat het verwijderen is voltooid, verschijnt een nieuw venster. Klik op **Voltooien**.

***Opmerking***

Nadat het verwijderen is voltooid, raden wij u aan de map `BitDefender` te verwijderen uit de map `Program Files`.

## *Er is een fout opgetreden tijdens het verwijderen van BitDefender*

Als er een fout is opgetreden tijdens het verwijderen van BitDefender, wordt het verwijderen afgebroken en verschijnt een nieuw venster. Klik op **Hulpprogramma Verwijderen uitvoeren** om zeker te zijn dat BitDefender volledig is verwijderd. Met het hulpprogramma voor het verwijderen worden alle bestanden en registersleutels verwijderd die niet tijdens het automatisch verwijderen werden verwijderd.

# Basisbeheer

# 2. Aan de slag

Uw computer is beveiligd zodra u BitDefender hebt geïnstalleerd. U kunt het Beveiligingscentrum van BitDefender openen om de status van de systeembeveiliging te controleren, voorzorgsmaatregelen te nemen of op elk ogenblik het product volledig te configureren.

Om toegang te krijgen tot het Beveiligingscentrum van BitDefender, gebruikt u het menu Start van Windows en volgt u het pad **Start → Programma's → BitDefender 2008 → BitDefender Antivirus 2008**. U kunt dit ook sneller doen door te dubbelklikken op het **BitDefender-pictogram** in het systeemvak.


**BitDefender Beveiligingscentrum**

Het Beveiligingscentrum van BitDefender bevat twee gebieden:

- Het gebied **Status**: bevat informatie over en helpt u met het oplossen van de zwakke punten in de beveiliging van uw computer. U kunt gemakkelijk zien hoeveel problemen uw computer kunnen beïnvloeden. Door op de overeenkomende rode knop **Alle probl. herst.** worden de zwakke punten van uw computer ter plaatse

opgelost of wordt u geholpen om ze gemakkelijk op te lossen. Tegelijkertijd zijn vier statusknoppen beschikbaar die overeenkomen met vier beveiligingscategorieën. Groene statusknoppen geven aan dat er geen risico is. Gele of rode knoppen geven gemiddelde of hoge beveiligingsrisico's aan. Om ze op te lossen klikt u op de gele/rode knop en klikt u achtereenvolgens op elke knop **Herstellen** of klikt u op de knop **Alles nu herst** button. Grijs geeft een niet-geconfigureerde component aan.

- Het gebied **Snelle taken**: helpt u uw systeem veilig te houden en uw gegevens te beveiligen.

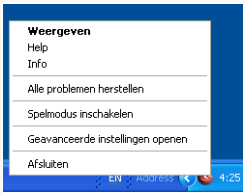
Daarnaast bevat het Beveiligingscentrum van BitDefender meerdere nuttige snelkoppelingen.

| *Koppeling* | *Beschrijving* |
|---|---|
| **Kopen** | Opent een pagina waar u het product kunt komen. |
| **Mijn account** | Opent de pagina van uw BitDefender-account. |
| **Registreren** | Opent de registratiewizard. |
| **Help** | Opent het Help-bestand. |
| **Ondersteuning** | Opent de webpagina van de BitDefender-ondersteuning. |
| **Instellingen** | Opent de console met de geavanceerde instellingen. |
| **Geschiedenis** | Opent een venster met de geschiedenis en gebeurtenissen van BitDefender. |

# 2.1. BitDefender Icon in het Systeemvak

Om het volledige product sneller te beheren, kunt u ook het BitDefender-pictogram in het systeemvak gebruiken.

Als u dubbelklikt op dit pictogram, wordt het Beveiligingscentrum van BitDefender geopend. Door met de rechterknop op het pictogram te klikken, verschijnt een snelmenu waarmee u het BitDefender-product snel kunt beheren.




**BitDefender-pictogram**

- **Weergeven** - opent het Beveiligingscentrum van BitDefender.
- **Help** - opent het Help-bestand.
- **Info** - opent de webpagina van BitDefender.

- **Alle probl. herst.** - helpt u de zwakke punten in de beveiliging te verwijderen.
- **Spelmodus aan/uit** - zet de Spelmodus aan/uit.
- **Geavanceerde instellingen openen** - biedt toegang tot de console met de geavanceerde instellingen.
- **Update nu** - start een directe update. Een nieuw venster verschijnt waarin u de updatestatus kan zien.
- **Afsluiten** - sluit de toepassing af.

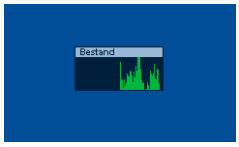
Als de Spelmodus is ingeschakeld, ziet u de letter G boven het BitDefender-pictogram.

Als er kritieke zaken de veiligheid van uw systeem bedreigen, staat er een uitroepteken boven het BitDefender-pictogram. U kunt het aantal problemen dat uw systeem beïnvloedt, zien door de muis op het pictogram te plaatsen.

## 2.2. Balk scanactiviteit

De **balk Scanactiviteit** is een grafische voorstelling van de scanactiviteit op uw systeem.

De groene balken (de **Bestand**) toont het aantal gescande bestanden per seconde op een schaal van 0 tot 50.




**Activiteitenbalk**

*Opmerking*
De balk voor de scanactiviteit zal aangeven wanneer de real time-beveiliging is uitgeschakeld door een rood kruis over de **Bestand** weer te geven

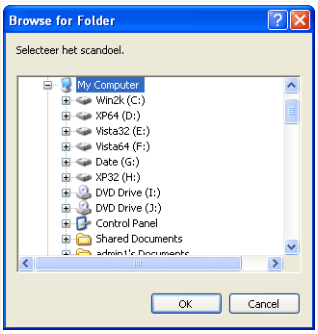
U kunt de **balk Scanactiviteit** gebruiken om objecten te scannen. Sleep de objecten die u wilt scannen en zet ze neer op de balk. Meer informatie vindt u onder "*Scannen door slepen & neerzetten*" (p. 68).

Als u deze grafische voorstelling niet langer wilt zien, klik er dan op met de rechtermuisknop en selecteer **Verbergen**.

## 2.3. BitDefender Handmatig scannen

Als u een bepaalde map snel wilt scannen, kunt u BitDefender Handmatig scannen gebruiken.

Om toegang te krijgen tot BitDefender Handmatig scannen, gebruikt u het menu Start van Windows via het pad **Start → Programma's → BitDefender 2008 → BitDefender Handmatig scannen** Het volgende venster wordt geopend:




**BitDefender Handmatig scannen**

U hoeft alleen maar door de mappen te bladeren, de map die u gescand wilt hebben te selecteren en te klikken op **OK**. De BitDefender Scanner verschijnt en begeleidt u door het scanproces.

## 2.4. Spelmodus

De nieuwe Spelmodus verandert tijdelijk de beveiligingsinstellingen om de snelheid van het systeem zo weinig mogelijk te beïnvloeden. Als u de Spelmodus aanzet, worden de volgende instellingen toegepast:

- Alle BitDefender waarschuwingen en pop-ups zijn uitgeschakeld.
- Het BitDefender real-time beschermingsniveau is ingesteld op **Toegeeflijk**.

Als de Spelmodus is ingeschakeld, ziet u de letter `G` boven het BitDefender-pictogram.

### 2.4.1. Gebruik van de Spelmodus

Gebruik één van de volgende methodes om de Spelmodus aan te zetten:

- Rechtsklik op het BitDefender pictogram in het systeemvak en selecteer **Spelmodus aanzetten**.
- Druk op `Alt+G` (de standaard sneltoets).

***Belangrijk***
Vergeet niet de Spelmodus uit te zetten als u klaar bent. Doe dit op dezelfde manier als bij het aanzetten.

## 2.4.2. Veranderen van de Spelmodus sneltoets

Volg deze stappen als u de sneltoets wilt veranderen:

1. Klik op **Instellingen** in het BitDefender Veiligheidscentrum om de instellingenconsole te openen.

   *Opmerking*
   U kan ook rechtsklikken op BitDefender pictogram in het systeemvak en **Open geavanceerde instellingen** selecteren.

2. Click **Geavanceerd**.
3. Stel de gewenste sneltoets in onder de **Sneltoets voor Spelmodus aan** optie:
   - Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (`Ctrl`), Shift toets (`Shift`) of Alternate toets (`Alt`).
   - Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

   Bijvoorbeeld, als u de `Ctrl+Alt+D` sneltoets wilt gebruiken, kruist u `Ctrl` en `Alt` aan en typt u `D`.

   *Opmerking*
   Door het kruisje naast **Sneltoets voor Spelmodus aan** te verwijderen, schakelt u de sneltoets uit.

# 3. Beveiligingsstatus

De beveiligingsstatus toont een systematisch georganiseerde en gemakkelijk beheerbare lijst van zwakke punten in de beveiliging van uw computer. BitDefender Antivirus 2008 zal u op de hoogte brengen wanneer een probleem de beveiliging van uw computer kan beïnvloeden.

Er zijn vier knoppen voor de beveiligingsstatus:

- **ANTIVIRUS**
- **ANTIPHISING**
- **IDENTITEITSCONTROLE**
- **UPDATE**

Aan de linkerzijde ziet u tegelijkertijd het aantal problemen dat de beveiliging van uw systeem beïnvloedt en een rode knop **Alle probl. herst.**.

De vier statusknoppen kunnen, afhankelijk van het huidige beveiligingsniveau, in het groen, geel, rood of grijs worden weergegeven.

- **Groen** geeft een laag beveiligingsrisico voor uw computer aan.
- **Geel** geeft een gemiddeld beveiligingsrisico voor uw computer aan.
- **Rood** geeft een hoog beveiligingsrisico voor uw computer aan.
- **Grijs** geeft een niet-geconfigureerde component aan.

Het herstellen van beveiligingsproblemen vereist geen inspanningen en kan met één klik op de knop **Alle probl. herst.** worden uitgevoerd. Een nieuw venster wordt weergegeven.


**Beveiligingsproblemen**

U zult een lijst van beveiligingsproblemen en een korte beschrijving van hun status zien.

Om een specifiek probleem te herstellen, klikt u op de overeenkomende knop **Herstellen**. Het probleem wordt onmiddellijk of nadat u de stappen van een wizard hebt gevolgd, opgelost. Als u beslist om ze allemaal op te lossen, klikt u op de knop **Alles nu herst** en volgt u de overeenkomende wizard.

Als u extra help nodig hebt, klik dan op de **Meer Help** knop, onderaan het venster. Een contextafhankelijke helppagina verschijnt het gedetailleerde informatie over deze zaken en hun oplossingen.

***Belangrijk***

Voor elk probleem is er een selectievakje dat standaard is ingeschakeld. Als u wilt dat er geen rekening wordt gehouden met een specifiek probleem tijdens het berekenen van het beveiligingsrisico, moet u het overeenkomende selectievakje uitschakelen. Ga voorzichtig te werk wanneer u deze optie gebruikt. Het is namelijk heel gemakkelijk om het beveiligingsrisico waaraan uw computer is blootgesteld, te verhogen.

Om de problemen op een later tijdstip te herstellen, klikt u op **Sluiten**.

# 3.1. Knop Antivirusstatus

Als de knop voor de antivirusstatus groen is, hoeft u zich geen zorgen te maken. Als de knop geel, rood of grijs is, betekent dit dat de computer is blootgesteld aan een gemiddeld of hoog beveiligingsrisico.

De kleur van de statusknoppen kan niet alleen wijzigen wanneer u de instellingen configureert die de beveiliging van uw computer kunnen beïnvloeden, maar ook wanneer u belangrijke taken vergeet uit te voeren. Als uw laatste systeemscan bijvoorbeeld oud is, zal de knop voor de beveiligingsstatus geel zijn. Als de scan zeer oud is, wordt de knop rood.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

| *Probleem* | *Kleur* |
|---|---|
| De laatste systeemscan is oud | Geel |
| De laatste systeemscan is zeer oud | Rood |
| De real time-beveiliging is uitgeschakeld | Rood |
| Het antivirusbeveiligingsniveau is ingesteld op "Toegeeflijk" | Geel |

Volg deze stappen om de problemen op te lossen:

1. Klik op de statusknop voor de antivirus.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

# 3.2. Knop Antiphishing-status

Als de statusknop voor antiphishing groen is, hoeft u zich geen zorgen te maken. Als de knop rood is, betekent dit dat de computer is blootgesteld aan een hoog beveiligingsrisico.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

| Probleem | Kleur |
|---|---|
| De antiphishing-beveiliging is ingeschakeld | Groen |
| De antiphishing-beveiliging is uitgeschakeld | Rood |

Volg deze stappen om de problemen op te lossen:

1. Klik op de statusknop voor antiphishing.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

## 3.3. Identiteitscontrole statusknop

Als de identiteitscontrole statusknop groen is, hoeft u zich nergens zorgen om te maken. Anderzijds, als de knop rood of grijs is, dan is er een hoog veiligheidsrisico op uw computer aanwezig.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

| Probleem | Kleur |
|---|---|
| De privacybeveiliging is ingesteld op AAN | Groen |
| De privacybeveiliging is ingesteld op UIT | Rood |
| De privacybeveiliging is niet ingesteld | Grijs |

Volg deze stappen om de problemen op te lossen:

1. Klik op de Identiteitscontrole statusknop.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

## 3.4. Knop Updatestatus

Als de statusknop voor de update groen is, hoeft u zich geen zorgen te maken. Als de knop rood is, betekent dit dat de computer is blootgesteld aan een hoog beveiligingsrisico.

De onderstaande tabel biedt u informatie over de elementen waarmee rekening wordt gehouden bij het berekenen van het beveiligingsrisico.

| *Probleem* | *Kleur* |
|---|---|
| Automatische update is ingeschakeld | Groen |
| Automatische update is uitgeschakeld | Rood |
| De laatste update is één dag oud | Rood |

Volg deze stappen om de problemen op te lossen:

1. Klik op de statusknop voor de update.
2. Klik op de knoppen **Herstellen** om de problemen een voor een op te lossen of op de knop **Alles nu herst** om ze allemaal samen op te lossen.
3. Als een probleem niet er plaatse wordt opgelost, moet u de wizard volgen om het op te lossen.

# 4. Snelle taken

Onder de vier statusknoppen vindt u het gebied **Snelle taken**.

## 4.1. Beveiliging

BitDefender wordt geleverd met een beveiligingsmodule waarmee u uw systeem up-to-date en virusvrij houdt.

Klik op het tabblad **Beveiliging** om de beveiligingsmodule te openen.

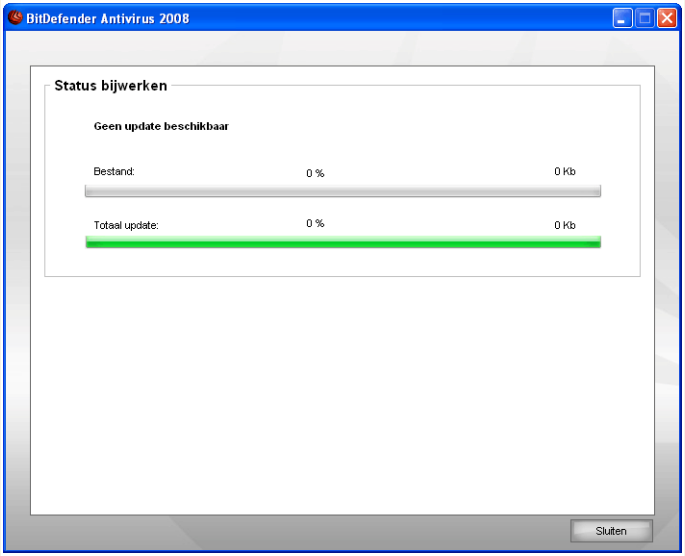
De volgende knoppen zijn beschikbaar:

- **Update nu** - start een directe update.
- **Mijn documenten scannen** - start een snelscan van uw documenten en instellingen.
- **Diepe systeemscan** - start een complete scan van uw computer (inclusief archiefbestanden).
- **Volledige systeemscan** - start een complete scan van uw computer (exclusief archiefbestanden).

### 4.1.1. Updaten BitDefender

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Standaard controleert BitDefender of er updates zijn als u uw computer aanzet en **ieder uur** daarna. Als u echter BitDefender wilt updaten, klik dan op **Update nu**. Het updateproces wordt gestart en het volgende venster verschijnt direct:




**Updaten BitDefender**

In dit venster kan u de status van het updateproces zien.

Het updateproces wordt geleidelijk uitgevoerd, wat betekent dat de te updaten bestanden een voor een worden vervangen. Op deze manier vormt het updateproces geen belemmering voor de werking van het product, en is tegelijk elke kwetsbaarheid uitgesloten.

Als u dit venster wilt sluiten, klik dan op **Sluiten**. Hierdoor stopt het updateproces echter niet.

*Opmerking*
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

**Start de computer indien nodig opnieuw op.** Als het een belangrijke update betreft, wordt u gevraagd de computer opnieuw op te starten: Als u niet telkens gevraagd wilt worden om na een update te herstarten, kruist u **Wacht met herstarten, in plaats van erom vragen**. Op deze manier blijft het product de volgende keer dat na een update een herstart noodzakelijk is, doorwerken met de oude bestanden totdat u zelf het systeem opnieuw opstart.

Klik op **Herstarten** om uw systeem direct opnieuw op te starten.

Als u uw systeem op een later tijdstip wilt herstarten, klik dan op **OK**. Wij adviseren dat u uw systeem zo snel mogelijk opnieuw opstart.

## 4.1.2. Scannen met BitDefender

Om uw computer te scannen op malware, voert u een speciale scantaak uit door te klikken op de overeenkomende knop. In de volgende tabel staan de beschikbare scantaken met hun beschrijving:

| *Taak* | *Beschrijving* |
|---|---|
| **Scan Mijn documenten** | Gebruik deze taak om belangrijke gangbare gebruikersmappen te scannen: `Mijn documenten`, `Bureaublad` en `Opstarten`. Dit garandeert de veiligheid van uw documenten, een veilige werkruimte en schone applicaties bij het opstarten. |
| **Diepe systeemscan** | Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere. |
| **Volledige systeemscan** | Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere. |

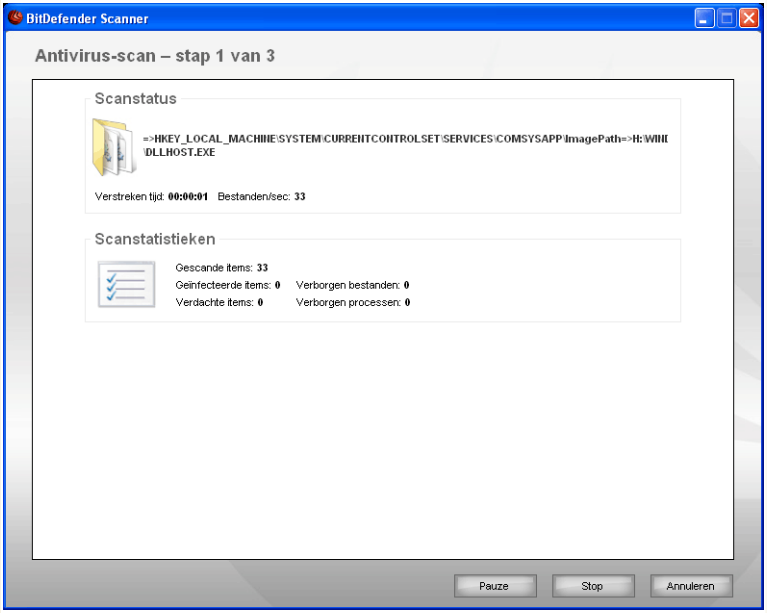
*Opmerking*
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner, ongeacht of het om een snelle of volledige scan gaat.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

### Stap 1/3 - Scannen

BitDefender start het scannen van de geselecteerde objecten.




**Scannen**

U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

***Opmerking***
Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

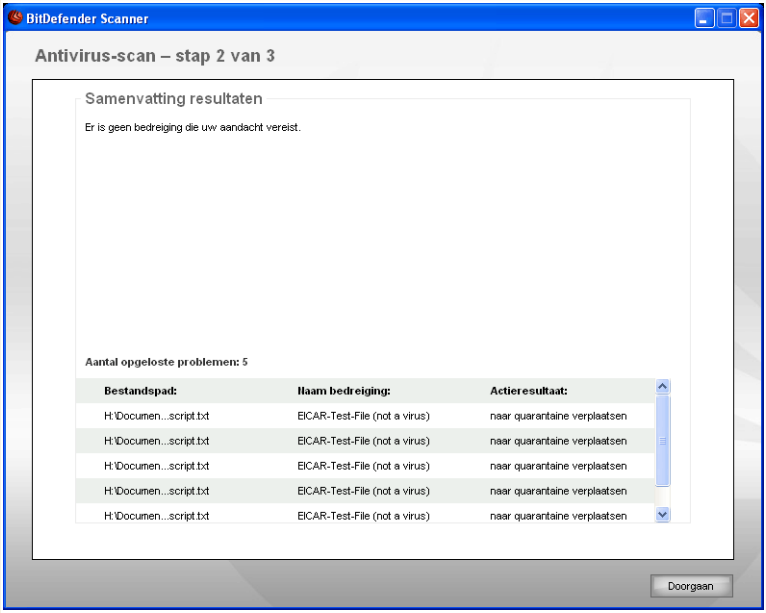
Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

U kunt het scannen op elkogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard.

Wacht tot BitDefender het scannen beëindigt.

## Stap 2/3 - Acties selecteren

Wanneer het scannen is voltooid, verschijnt een nieuw venster waarin u de scanresultaten kunt zien.




**Acties**

U kunt het aantal problemen dat uw systeem beïnvloedt, zien.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de malware waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.

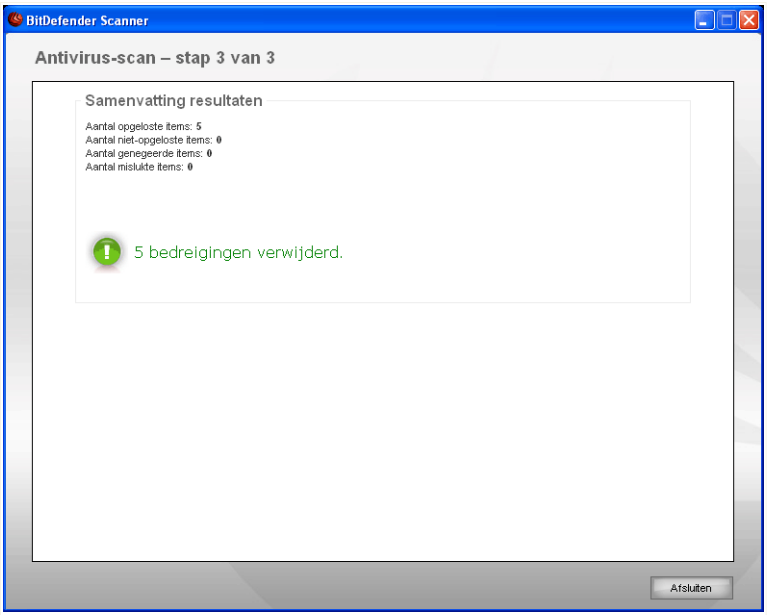
De volgende opties kunnen in het menu verschijnen.

| Actie | Beschrijving |
|---|---|
| **Geen actie nemen** | Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. |
| **Desinfecteren** | Desinfecteert geïnfecteerde bestanden. |
| **Verwijderen** | Verwijdert gedetecteerde bestanden. |
| **Zichtbaar maken** | Maakt verborgen objecten zichtbaar. |

Klik op **Doorgaan** om de aangegeven acties toe te passen.

## Stap 3/3 - Resultaten weergeven

Wanneer BitDefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster.




**Overzicht**

U kunt een samenvatting van de resultaten zien. Het rapportbestand wordt automatisch opgeslagen in het gedeelte Logboeken in het venster **Eigenschappen** van de respectievelijke taak.

***Belangrijk***
U wordt gevraagd uw systeem opnieuw te starten zodat het installatieprogramma de installatie kan voltooien.

Klik op **Afsluiten** om het venster te sluiten.

### *BitDefender kon bepaalde zaken niet oplossen*

In de meeste gevallen desinfecteert BitDefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Niet alle zaken kunnen echter worden opgelost.

In deze gevallen, raden wij u aan contact op te nemen met het ondersteuningsteam van BitDefender op www.bitdefender.com. Onze experts helpen u de problemen op te lossen.

### *BitDefender detecteerde met een wachtwoord beschermde zaken*

De met een wachtwoord beschermde categorie bevat twee types van zaken: archieven en installatieprogramma's. Zij vormen geen echte bedreiging voor de veiligheid van het systeem, tenzij zij geïnfecteerde bestanden bevatten en alleen als zij worden uitgevoerd.

Om zeker te weten dat deze zaken schoon zijn:

- Als de met een wachtwoord beschermde zaak een archief is dat u met een wachtwoord hebt beschermt, pakt u de bestanden die erin staan uit en scant u deze afzonderlijk. Klik erop met de rechtermuisknop en selecteer **BitDefender Antivirus 2008** in het menu.
- Als de met een wachtwoord beschermde zaak een installatieprogramma is, controleer dan of de real-time bescherming is ingeschakeld voordat u het installatieprogramma uitvoert. Als het installatieprogramma is geïnfecteerd, zal BitDefender de infectie detecteren en isoleren.

Als u niet wilt dat deze objecten opnieuw worden gedetecteerd door BitDefender, moet u deze toevoegen als uitzonderingen op het scanproces. Om scanuitzonderingen toe te voegen, klikt u op **Instellingen** om de instellingenconsole te openen en gaat u naar **Antivirus > Uitzonderingen** . Voor meer informatie raadpleegt u de Objecten die zijn uitgesloten van de scan.

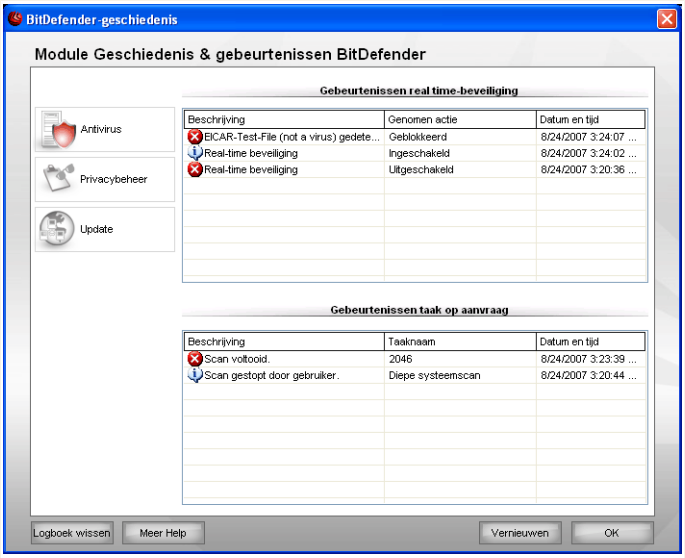
### *BitDefender detecteerde verdachte bestanden*

Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse en die mogelijk geïnfecteerd zijn met malware waarvan de signatuur nog niet bekend is.

Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het BitDefender Lab te sturen. Klik op **OK** om deze bestanden naar het BitDefender laboratorium te verzenden voor verdere analyse.

# 5. Geschiedenis

De koppeling **Geschiedenis** onderaan in het venster van het Beveiligingscentrum van BitDefender opent een ander venster met de Geschiedenis en gebeurtenissen van BitDefender. Dit venster biedt u een overzicht van gebeurtenissen die betrekking hebben op de beveiliging. U kunt bijvoorbeeld gemakkelijk controleren of de update is gelukt, of er malware op uw computer is gevonden, of uw back-uptaken worden uitgevoerd zonder fouten, enz.




**Gebeurtenissen**

Om u te helpen de geschiedenis en gebeurtenissen van BitDefender te filteren, worden de volgende categorieën aan de linkerzijde weergegeven:

- **Antivirus**
- **Privacybeheer**
- **Update**

Voor elke categorie is een lijst gebeurtenissen beschikbaar. Elke gebeurtenis biedt de volgende informatie: een korte beschrijving, de actie die BitDefender heeft genomen

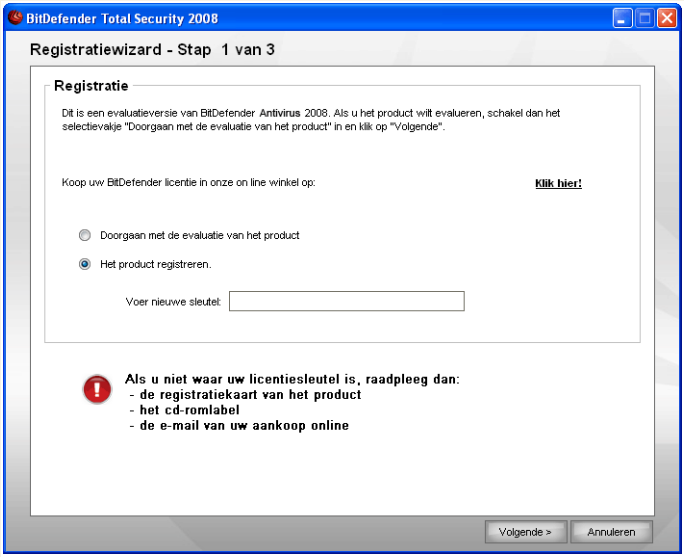
wanneer de gebeurtenis is opgetreden en de datum en het tijdstip van de gebeurtenis. Als u meer informatie over een specifieke gebeurtenis in de lijst wilt krijgen, dubbelklikt u op die gebeurtenis.

Klik op **Logboek wissen** als u de oude logboeken wilt verwijderen of klik op **Vernieuwen** om zeker te zijn dat de recentste logboeken worden weergegeven.

# 6. Registratie

BitDefender Antivirus 2008 begint met een 30-dagen proefperiode. Voor het registreren van BitDefender Antivirus 2008, het veranderen van de licentiesleutel of het maken van een BitDefender-account, klikt u op de **Registreren** link, aan de bovenkant van het BitDefender Veiligheidscentrum venster. De registratiewizard verschijnt.

## 6.1. Stap 1/3 - BitDefender Antivirus 2008 registreren




**Registratie**

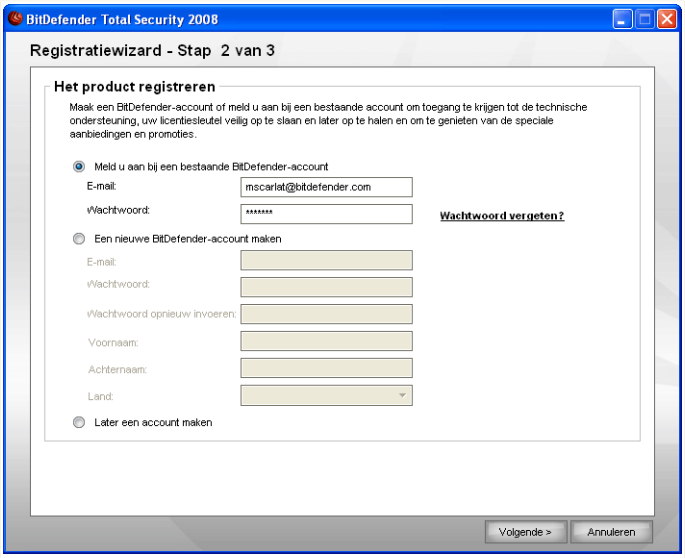
Als u geen BitDefender licentie hebt, klik dan op de aanwezige link om naar de BitDefender on line winkel te gaan en een licentiesleutel te kopen.

Voor het registreren van BitDefender Antivirus 2008, selecteert u **Registreer het product** en typt u de licentiesleutel in het **Nieuwe sleutel invoeren** veld.

Als de proefperiode nog niet is verstreken en u het product nog verder wilt evalueren, selecteert u **Doorgaan met de evaluatie van het product**.

Klik op **Volgende** om door te gaan.

## 6.2. Stap 2/3 - Een BitDefender-account maken




**Account maken**

## Ik heb geen BitDefender-account

Om van de gratis technische ondersteuning en andere gratis diensten van BitDefender te kunnen genieten, moet u een account maken.

***Opmerking***
Als u later een account wilt maken, selecteert u de overeenkomende optie.

Voor het maken van een BitDefender-account, selecteert u **Een nieuwe BitDefender-account maken** en geef de vereiste informatie op. De gegevens die u hier opgeeft blijven vertrouwelijk.

- **E-mail** - voer uw e-mailadres in.
- **Wachtwoord** - voer een wachtwoord voor uw BitDefender-account in.

> *Opmerking*
> Het wachtwoord moet minstens vier tekens bevatten.

- **Wachtwoord opnieuw** - voer het zojuist gebruikte wachtwoord opnieuw in.
- **Voornaam** - voer uw voornaam in.
- **Achternaam** - voer uw achternaam in.
- **Land** - selecteer het land waar u woont.

> *Opmerking*
> Gebruik het door u ingevoerde e-mailadres en wachtwoord om in te loggen op uw account op http://myaccount.bitdefender.com.

Om een account te kunnen maken, moet u eerst uw e-mailadres activeren. Controleer uw e-mailadres en volg de instructies in de e-mail die u van de registratieservice van BitDefender hebt ontvangen.

Klik op **Volgende** om door te gaan.

## Ik heb al een BitDefender-account

BitDefender detecteert automatisch of u al een BitDefender-account hebt geregistreerd op uw computer. In dit geval, klikt u alleen maar op **Volgende**.

Als u al een actieve account hebt, maar BitDefender deze niet detecteert, selecteer dan **Inloggen op een bestaande BitDefender Account** en vul het e-mailadres en het wachtwoord van uw account in.

> *Opmerking*
> Als u een verkeerd wachtwoord hebt ingevuld, kunt u het opnieuw invullen nadat u hebt geklikt op **Next**. Klik op **Ok** om het wachtwoord opnieuw in te vullen of op **Annuleren** om het programma te verlaten.

Als u uw wachtwoord hebt gegeven, klikt u op **Wachtwoord vergeten?** en volgt u de instructies.

Klik op **Volgende** om door te gaan.

## 6.3. Stap 3/3 - BitDefender Antivirus 2008 registreren


**Overzicht**

Selecteer **Mijn BitDefender-account openen** om naar uw BitDefender-account te gaan. Internetverbinding vereist.

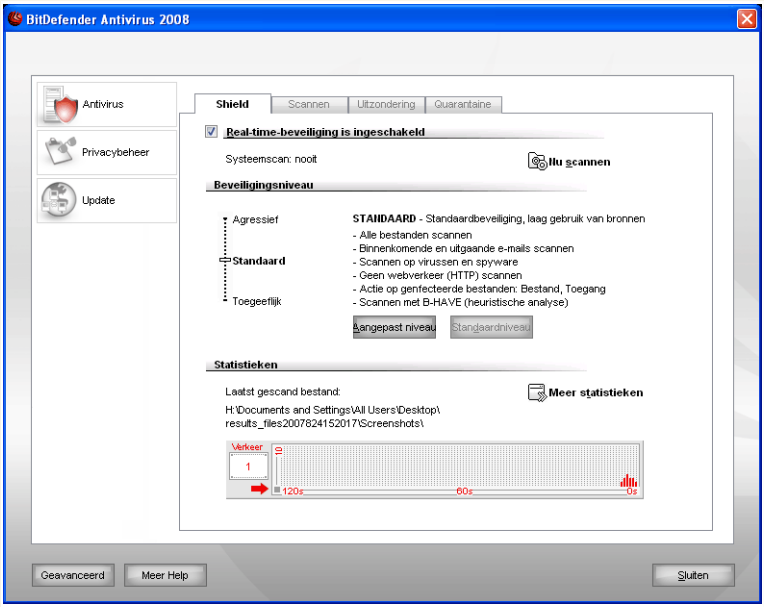
Klik op **Voltooien** om het venster te sluiten.

# Geavanceerd beveiligingsbeheer

# 7. Instellingsconsole

**BitDefender Antivirus 2008** wordt geleverd met een gecentraliseerde instellingsconsole waarmee geavanceerde configuratie en geavanceerd beheer van BitDefender mogelijk is.

Open de instellingsconsole en klik onderaan in het Beveiligingscentrum op de koppeling **Instellingen**.




**Instellingsconsole**

De instellingsconsole is onderverdeeld in modules: **Antivirus**, **Identiteitscontrole** en **Update**. Hiermee kunt u BitDefender gemakkelijk beheren op basis van het type beveiligingsprobleem dat wordt aangepakt.

Aan de linkerzijde van de instellingsconsole ziet u de moduleselector:

- Antivirus - in deze sectie kunt u de **Antivirus**-module configureren.
- Identiteitscontrole - in deze sectie kunt u de module **Identiteitscontrole** configureren.

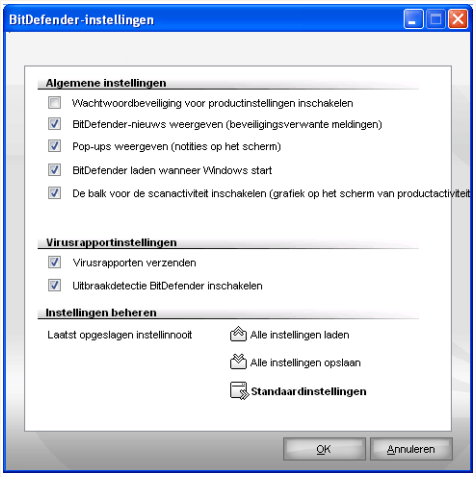
■ Update - in deze sectie kunt u de **Update**-module configureren.

Aan de onderkant van de instellingenconsole, bevindt zich een **Meer Help** knop die een contextafhankelijke helppagina opent. Klik op deze knop om meer informatie te lezen over de sectie waarin u zich bevindt.

Als u extra help nodig hebt, klik dan op de **Meer Help** knop, onderaan het venster. Er verschijnt een contextafhankelijke helppagina met gedetailleerde informatie over de sectie waarin u zich bevindt.

# 7.1. Algemene instellingen configureren

Om de algemene instellingen te configureren voor BitDefender Antivirus 2008 en zijn instellingen te beheren, klikt u op **Geavanceerd**. Een nieuw venster wordt weergegeven.




**Algemene instellingen**

Hier kunt u de algemene gedragingen van BitDefender instellen. BitDefender wordt standaard geladen bij het opstarten van Windows en wordt vervolgens geminimaliseerd uitgevoerd in de taakbalk.

## 7.1.1. Algemene instellingen

- **Wachtwoord voor productinstellingen aan** - maakt het gebruik van een wachtwoord mogelijk om de BitDefender configuratie te beschermen.

*Opmerking*
Als u niet de enige persoon met beheermachtigingen bent die deze computer gebruikt, raden wij u aan uw BitDefender-instellingen te beveiligen met een wachtwoord.

Als u deze optie selecteert, verschijnt het volgende venster:


**Wachtwoord invoeren**

Typ het wachtwoord in het **Wachtwoord** veld, typ het nogmaals in het **Wachtwoord herhalen** veld en klik op **OK**.

Zodra u het wachtwoord hebt ingesteld, zal er elke keer om gevraagd worden als u de instellingen van BitDefender wilt veranderen. De andere systeembeheerders (als die er zijn) moeten dit wachtwoord ook invullen om de instellingen van BitDefender te kunnen veranderen.

*Belangrijk*
Als u uw wachtwoord vergeten bent, zult u het product moeten repareren om de BitDefender-configuratie te wijzigen.

- **BitDefender-nieuws weergeven (berichten i.v.m. beveiliging)** - toont af en toe beveiligingsberichten die door de BitDefender-server zijn verzonden met betrekking tot de uitbraak van virussen.
- **Pop-ups weergeven (notities op het scherm)** - toont pop-upvensters die betrekking hebben op de productstatus.
- **BitDefender laden wanneer Windows start** - start BitDefender automatisch wanneer het systeem wordt opgestart. Wij raden u aan deze optie ingeschakeld te houden.
- **De balk voor de scanactiviteit inschakelen (grafiek op het scherm van productactiviteit)** - toont de Scanactiviteit balk als u inlogt op Windows. Maak dit vakje leeg als u de Scanactiviteit balk niet langer wilt zien.

*Opmerking*
Deze optie kan alleen worden geconfigureerd voor de huidige Windows gebruiker.

- **Sneltoets voor Spelmodus inschakelen** - staat het gebruik toe van een combinatie van toetsen (sneltoets) voor het aanzetten/uitzetten van de Spelmodus. De standaard sneltoets is `Alt+G`.

  U kan deze sneltoets op de volgende manier wijzigen:

  1. Kies de gewijzigde toetsen die u wilt gebruiken door één van de volgende aan te kruisen: Control toets (`Ctrl`), Shift toets (`Shift`) of Alternate toets (`Alt`).
  2. Typ in het invulveld de letter van de normale toets die u wilt gebruiken.

## 7.1.2. Virusrapportinstellingen

- **Virusrapporten verzenden** - verzendt rapporten met betrekking tot virussen die op uw computer werden geïdentificeerd naar de BitDefender Labs. Hierbij helpt u ons virusuitbraken op te volgen.

  De rapporten zullen geen vertrouwelijke gegevens, zoals uw naam, IP-adres of andere bevatten, en zullen niet worden gebruikt voor commerciële doeleinden. De geleverde informatie zal alleen de naam van het virus bevatten en zal uitsluitend worden gebruikt voor het maken van statistische rapporten.
- **Uitbraakdetectie BitDefender inschakelen** - verzendt rapporten met betrekking tot potentiële virusuitbraken naar de BitDefender Labs.

  De rapporten zullen geen vertrouwelijke gegevens, zoals uw naam, IP-adres of andere bevatten, en zullen niet worden gebruikt voor commerciële doeleinden. De geleverde informatie zal alleen de naam van het potentiële virus bevatten en zal uitsluitend worden gebruikt om nieuwe virussen te detecteren.

## 7.1.3. Instellingen beheren

Gebruik de knoppen **Alle instellingen opslaan** / **Alle instellingen laden** om de instellingen die u hebt gedefinieerd voor BitDefender op de gewenste locatie op te slaan / te laden. Op deze manier kunt u dezelfde instellingen gebruiken nadat u uw BitDefender-product opnieuw hebt geïnstalleerd of hebt gerepareerd.

***Belangrijk***
Alleen gebruikers met beheermachtigingen kunnen instellingen opslaan en laden.

Om de standaardinstellingen te laden, klikt u op **Standaardinstellingen**.

# 8. Antivirus

BitDefender beveiligt uw computer tegen alle types malware (virussen, Trojanen, spyware, rootkits, enz.).

Naast het klassieke scannen op basis van malware-handtekeningen, zal BitDefender ook een heuristische analyse uitvoeren op de gescande bestanden. Heuristisch scannen heeft het doel nieuwe virussen te identificeren op basis van bepaalde patronen en algoritmen, voordat een virusdefinitie wordt gevonden. In dat geval zijn valse alarmberichten mogelijk. Wanneer een dergelijk bestand wordt gedetecteerd, wordt het beschouwd als verdacht. In deze gevallen raden wij u aan het bestand te verzenden naar het BitDefender lab voor analyse.

De BitDefender-bescherming is ingedeeld in twee categorieën:

- **Scannen bij toegang** - verhindert dat nieuwe malware-bedreigingen uw systeem binnenkomen. Dit wordt ook real time bescherming genoemd. De bestanden worden gescand op het ogenblik dat u ze gebruikt - bij toegang. BitDefender zal bijvoorbeeld een Worddocument scannen op bekende gevaren wanneer u het opent, en een e-mailbericht wanneer u het ontvangt.
- **Scannen op aanvraag** - hiermee kunt u malware die al op uw systeem aanwezig is, detecteren en verwijderen. Dit is de klassieke scan die door de gebruiker wordt geactiveerd. U selecteert het station, de map of het bestand dat BitDefender moet scannen, en BitDefender doet dat - op aanvraag. Met de scantaken kunt u aangepaste scanroutines maken en ze kunnen op regelmatige basis worden uitgevoerd.

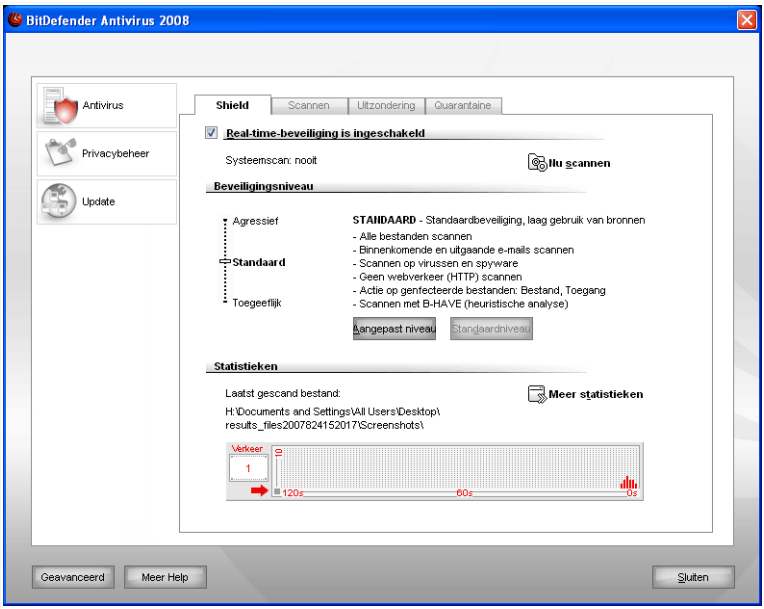
Het gedeelte **Antivirus** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Scannen bij toegang
- Scannen op aanvraag
- Objecten die zijn uitgesloten van de scan
- Quarantaine

## 8.1. Scannen bij toegang

Scannen bij toegang, ook bekend als real time-beveiliging, houdt u computer beveiligd tegen alle types malware-bedreigingen door alle geopende bestanden, e-mailbestanden en communicatie via toepassingen voor instant messaging (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) te scannen.

Om de real time-beveiliging te configureren en te controleren, klikt u in de instellingsconsole op **Antivirus>Shield**. Het volgende venster wordt geopend:




**Real-time-beveiliging**

***Belangrijk***
Om te verhinderen dat uw computer door virussen wordt geïnfecteerd, moet u de **Real-time-beveiliging** ingeschakeld houden.

In het onderste gedeelte van het venster kunt u de statistieken van de **Real-time-beveiliging** over de gescande bestanden en e-mailberichten bekijken. Klik op de knop **Meer statistieken** om een venster weer te geven met meer informatie over deze statistieken.

Om een snelle systeemscan te starten, klikt u op **Nu scannen**.

## 8.1.1. Het beveiligingsniveau configureren

U kunt het beveiligingsniveau kiezen dat beter voldoet aan uw beveiligingsbehoeften. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen.

Er zijn 3 beveiligingsniveaus:

| Beveiligingsniveau | Beschrijving |
|---|---|
| **Toegeeflijk** | Dekt de basisbehoeften aan beveiliging. Het verbruiksniveau van de bron is zeer laag.<br>Programma's en binnenkomende e-mailberichten worden alleen op virussen gescand. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren. |
| **Standaard** | Biedt standaardbeveiliging. Het verbruiksniveau van de bron is laag.<br>Alle bestanden en binnenkomende/uitgaande e-mailberichten worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren. |
| **Agressief** | Biedt een hoge beveiliging. Het verbruiksniveau van de bron is gemiddeld.<br>Alle bestanden, binnenkomende/uitgaande e-mailberichten en webverkeer worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. De volgende acties worden ondernomen op geïnfecteerde bestanden: bestand opruimen/toegang weigeren. |

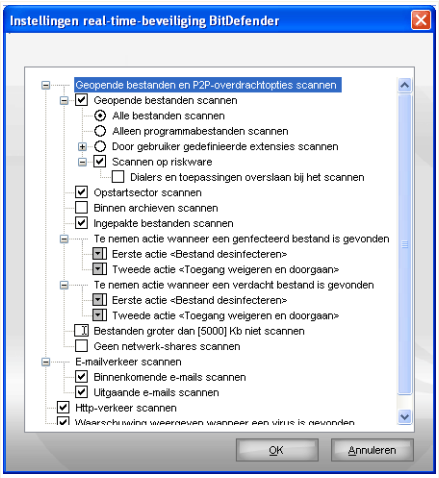
Om de standaard real time beveiligingsinstellingen toe te passen, klikt u op **Standaard**.

## 8.1.2. Het beveiligingsniveau aanpassen

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. De scanner kan worden ingesteld om alleen

specifieke bestandsextensies te scannen, specifieke malware-bedreigingen te zoeken of archieven over te slaan. Dat kan de duur van het scannen aanzienlijk verkorten en de reactie van uw computer tijdens het scannen verbeteren.

U kunt de **Real-time-beveiliging** inschakelen door op **Aangepast** te klikken. Het volgende venster wordt geopend:




**Shield-instellingen**

De scanopties zijn georganiseerd als een uitbereidbaar menu, vergelijkbaar met de menu's die in Windows gebruikt worden. Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

*Opmerking*

U zult merken dat sommige scanopties toch niet kunnen worden geopend, zelfs indien het teken "+" wordt weergegeven. De reden hiervoor is dat deze optie nog niet werd geselecteerd. Wanneer u deze selecteert, zult u merken dat ze nu wel kunnen worden geopend.

- **Geopende bestanden en P2P-overdrachten scannen** - scant de geopende bestanden en de communicatie via Instant Messaging-software (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). Selecteer vervolgens het type bestanden dat u wilt scannen.

| Optie | | Beschrijving |
|---|---|---|
| **Geopende bestanden scannen** | **Alle bestanden scannen** | Alle geopende bestanden worden gescand, ongeacht hun type. |
| | **Alleen programmabestanden scannen** | Alleen de programmabestanden worden gescand. Dit betekent alleen bestanden met de volgende extensies: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml en .nws. |
| | **Door gebruiker gedefinieerde extensies scannen** | Alleen de bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden gescand. Deze extensies moeten worden gescheiden door ";". |
| | **Scannen op riskware** | Scannen op riskware. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld.<br><br>Selecteer **Dialers en toepassingen overslaan bij scan** als u dit type bestanden wilt uitsluiten van het scannen. |
| **Opstartsector scannen** | | Scant de opstartsector van het systeem. |
| **Binnen archieven scannen** | | De geopende archieven worden gescand. Wanneer u deze optie inschakelt, zal de computer langzamer werken. |
| **Ingepakte bestanden scannen** | | Alle ingepakte bestanden worden gescand. |
| **Eerste actie** | | Selecteer de eerste actie die moet worden genomen op geïnfecteerde en verdachte bestanden in het vervolgkeuzemenu. |

| Optie | | Beschrijving |
|---|---|---|
| | **Toegang weigeren en doorgaan** | Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd. |
| | **Bestand opruimen** | Desinfecteert geïnfecteerde bestanden. |
| | **Bestand verwijderen** | Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing. |
| | **Bestand verplaatsen naar quarantaine** | Verplaatst de geïnfecteerde bestanden naar de quarantaine. |
| **Tweede actie** | | Selecteer in het vervolgkeuzemenu de tweede actie die moet worden genomen op geïnfecteerde bestanden in het geval de eerste actie mislukt. |
| | **Toegang weigeren en doorgaan** | Wanneer een geïnfecteerd bestand is gedetecteerd, zal de toegang tot dit bestand worden geweigerd. |
| | **Bestand verwijderen** | Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing. |
| | **Bestand verplaatsen naar quarantaine** | Verplaatst de geïnfecteerde bestanden naar de quarantaine. |
| **Bestanden groter dan [x] Kb niet scannen** | | Voer de maximale grootte in van de bestanden die moeten worden gescand. Als u de grootte instelt op 0 Kb, worden alle bestanden gescand, ongeacht hun grootte. |
| **Geen netwerk-shares scannen** | | Als deze optie is ingeschakeld, zal BitDefender de netwerk-shares niet scannen, zodat u sneller toegang krijgt tot het netwerk.<br>Wij raden u aan deze optie alleen in te schakelen als het netwerk waarvan u deel uitmaakt, door een antivirusoplossing is beveiligd. |

- **E-mailverkeer scannen** - scant het e-mailverkeer.

De volgende opties zijn beschikbaar:

| Optie | Beschrijving |
|---|---|
| **Binnenkomende e-mails scannen** | Scant alle binnenkomende e-mailberichten. |
| **Uitgaande e-mails scannen** | Scant alle uitgaande e-mailberichten. |

- **Http-verkeer scannen** - scant het http-verkeer.
- **Waarschuwing weergeven wanneer een virus is gevonden** - opent een waarschuwingsvenster wanneer een virus wordt gevonden in een bestand of in een e-mailbericht.

  Voor een geïnfecteerd bestand zal het waarschuwingsvenster de naam van het virus bevatten, het pad naar het virus, de actie die door BitDefender wordt ondernomen en een koppeling naar de BitDefender-site waar u meer informatie over het virus kunt vinden. Voor een geïnfecteerde e-mail zal het waarschuwingsvenster ook informatie over de afzender en de ontvanger bevatten.

  Als een verdacht bestand is gedetecteerd, kunt u een wizard starten vanaf het waarschuwingsvenster. Deze wizard zal u helpen bij het verzenden van dat bestand naar BitDefender Labs voor verdere analyse. U kunt uw e-mailadres invoeren om informatie te ontvangen over dit rapport.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## 8.1.3. Real time-beveiliging uitschakelen

Als u de real time-beveiliging wilt uitschakelen, verschijnt een waarschuwingsvenster.


**Real time-beveiliging uitschakelen**

U moet uw keuze bevestigen door in het menu te selecteren hoelang u de real time-beveiliging wilt uitschakelen. U kunt de real time-beveiliging uitschakelen

gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.

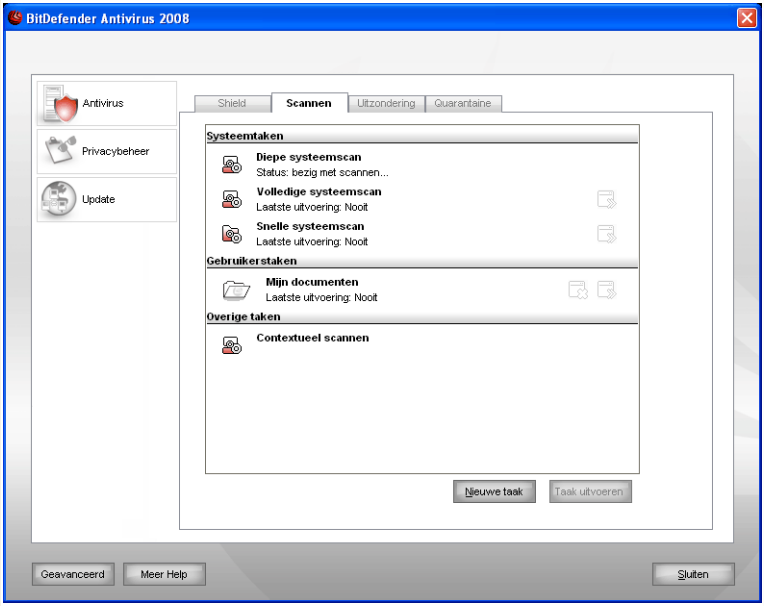
***Waarschuwing***
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de real time-beveiliging zo kort mogelijk uit te schakelen. Als de real time-beveiliging is uitgeschakeld, wordt u niet beveiligd tegen malware-bedreigingen.

## 8.2. Scannen op aanvraag

BitDefender heeft als hoofddoel uw computer vrij te houden van virussen. Dit wordt in de eerste plaats gedaan door nieuwe virussen uit uw computer weg te houden en door uw e-mailberichten en alle nieuwe bestanden, die u downloadt of kopieert naar uw systeem, te scannen.

Het risico bestaat dat een virus zich reeds in uw systeem heeft genesteld voordat u BitDefender installeert. Het is dan ook een bijzonder goed idee uw computer meteen te scannen op aanwezige virussen nadat u BitDefender hebt geïnstalleerd. En het is zeker ook een goed idee om uw computer frequent te scannen op virussen.

Om Scannen op aanvraag te configureren en te starten, klikt u in de instellingsconsole op **Antivirus>Scannen**. Het volgende venster wordt geopend:




**Scantaken**

Scannen op aanvraag is gebaseerd op scantaken. Scantaken bepalen de scanopties en de objecten die moeten worden gescand. U kunt de computer scannen wanneer u dat wilt door de standaardtaken of uw eigen scantaken (door gebruiker gedefinieerde taken) uit te voeren. U kunt ook een planning instellen om taken regelmatig uit te voeren of wanneer het systeem inactief is zodat uw niet wordt gehinderd in uw werk.

## 8.2.1. Scantaken

BitDefender wordt geleverd met meerdere taken die standaard zijn gemaakt en de gebruikelijke beveiligingsproblemen dekken. U kunt ook uw eigen aangepaste scantaken maken.

Elke taak heeft een venster **Eigenschappen** waarmee u de taak kunt configureren en de scanresultaten kunt weergeven. Meer informatie vindt u onder "*Scantaken configureren*" (p. 57).

Er zijn drie categorieën scantaken:

- **Systeemtaken** - bevat de lijst van standaard systeemtaken. De volgende taken zijn beschikbaar:

| Standaardtaak | Beschrijving |
|---|---|
| **Diepe systeemscan** | Scant het volledige systeem. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere. |
| **Volledige systeemscan** | Scant het volledige systeem, behalve archieven. In de standaardconfiguratie wordt er gescand op alle types malware die de beveiliging van uw systeem bedreigen, zoals virussen, spyware, adware, rootkits en andere. |
| **Snelle systeemscan** | Scant de mappen `Windows`, `Program Files` en `All Users`. In de standaardconfiguratie wordt gescand op alle types malware, behalve rootkits, maar het geheugen, het register en de cookies worden niet gescand. |

*Opmerking*
Omdat de taken **Diepe systeemscan** en **Volledige systeemscan** analyseren het volledige systeem. Het scannen kan enige tijd in beslag nemen. Wij raden u daarom aan deze taken uit te voeren met een lage prioriteit, of bij voorkeur wanneer uw systeem inactief is.

- **Gebruikerstaken** - bevat de door de gebruiker gedefinieerde taken.

  Er wordt een taak geleverd met de naam `Mijn documenten`. Gebruik deze taak om belangrijke mappen van de huidige gebruiker te scannen. `Mijn documenten`, `Bureaublad` en `Opstarten`. Dit zal de veiligheid van uw documenten, een veilige werkruimte en opgeruimde toepassingen bij het opstarten garanderen.
- **Diverse taken** - bevat een lijst van diverse scantaken. Deze scantaken verwijzen naar alternatieve scantypes die vanaf dit venster kunnen worden uitgevoerd. U kunt alleen hun instellingen wijzigen of de scanrapporten weergeven.

Rechts van elke taak zijn drie knoppen beschikbaar:

- **Planning** - geeft aan dat de geselecteerde taak voor later is gepland. Klik op deze knop om het venster **Eigenschappen** te openen. Klik op het tabblad Planner waar u de taakplanning kunt bekijken en wijzigen.

- **Verwijderen** - verwijdert de geselecteerde taak.

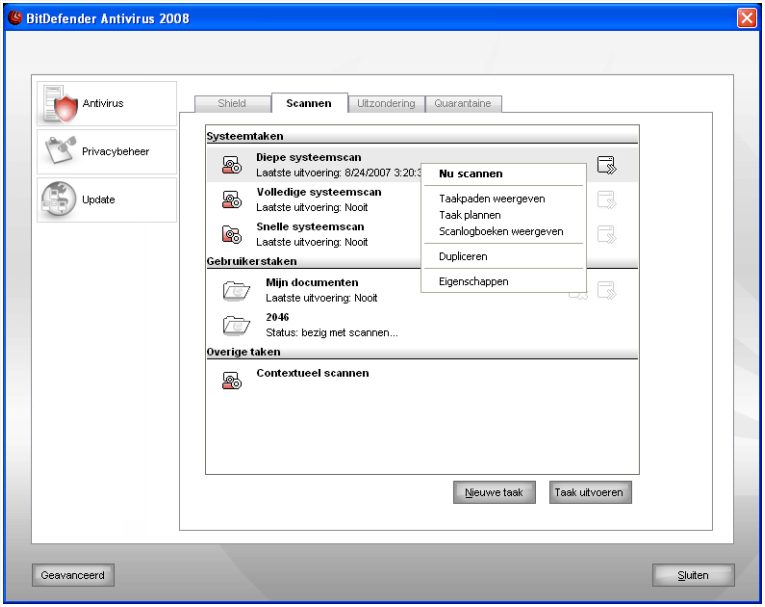
> ***Opmerking***
> Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

- **Nu scannen** - voert de geselecteerde taak uit en start de optie Onmiddellijk scannen.

Links naast elke taak ziet u de knop **Eigenschappen** waarmee u de taak kunt configureren en de scanlogs kunt weergeven.

## 8.2.2. Het snelmenu gebruiken

Voor elke taak is een




**Snelmenu**

snelmenu beschikbaar. Klik met de rechtermuisknop op de geselecteerde taak om deze te openen.

De volgende opdrachten zijn beschikbaar in het snelmenu:

- **Nu scannen** - voert de geselecteerde taak uit en start een onmiddellijke scan.
- **Scandoel wijzigen** - opent het venster **Eigenschappen**. Klik op het tabblad Scanpad waar u het scandoel van de geselecteerde taak kunt wijzigen.

*Opmerking*
In het geval van systeemtaken wordt deze optie vervangen door **Taakpaden weergeven** omdat u alleen hun scandoel kunt zien.

- **Taak plannen** - opent het venster **Eigenschappen**. Klik op het tabblad Planner waar u de geselecteerde taak kunt plannen.
- **Log weergeven** - opent het venster **Eigenschappen**. Klik op het tabblad Scanlogboeken waar u de rapporten kunt bekijken die werden gegenereerd nadat de geselecteerde taak werd uitgevoerd.
- **Kopiëren** - dupliceert de geselecteerde taak.

*Opmerking*
Dit is nuttig wanneer u nieuwe taken maakt omdat u de instellingen van een duplicaat van de taak kunt wijzigen.

- **Verwijderen** - verwijdert de geselecteerde taak.

*Opmerking*
Niet beschikbaar voor systeemtaken. U kunt geen systeemtaak verwijderen.

- **Eigenschappen** - opent het venster **Eigenschappen**. Klik op het tabblad Overzicht waar u de instellingen van de geselecteerde taak kunt wijzigen.

*Opmerking*
Door de specifieke aard van de categorie **Overige taken**, zijn in dit geval alleen de opties **Eigenschappen** en **Scanlogboeken weergeven** beschikbaar.

## 8.2.3. Scantaken maken

Gebruik een van de volgende methoden om een scantaak te maken:

- Kopieer een bestaande taak, wijzig de naam van de taak en breng de nodige wijzigingen aan in het venster Eigenschappen.
- Klik op **Nieuwe taak** om een nieuwe taak te maken en te configureren.

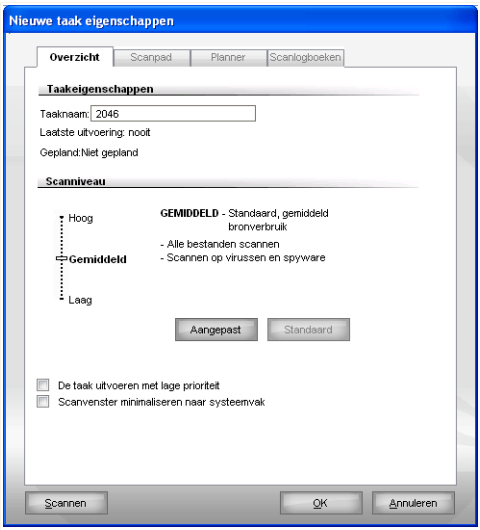
## 8.2.4. Scantaken configureren

Elke scantaak heeft zijn eigen venster **Eigenschappen** waarin u de scanopties kunt configureren, het scandoel kunt instellen, de taak kunt plannen of rapporten kunt weergeven. Om dit venster te openen, klikt u op de knop **Openen** die zich rechts van de taak bevindt (of klik met de rechtermuisknop op de taak en klik daarna op **Openen**).

*Opmerking*
Meer informatie over het weergeven van logboeken en het tabblad **Logboeken**, vindt u onder "*Scanlogboeken weergeven*" (p. 74).

### Scaninstellingen configureren

Om de scanopties van een specifieke scantaak te configureren, klikt u met de rechtermuisknop en selecteert u **Openen**. Het volgende venster wordt geopend:




**Overzicht**

Hier ziet u informatie over de taak (naam, laatste uitvoering en status van de planning) en de scaninstellingen definiëren.

### *Het scanniveau selecteren*

U kunt de scaninstellingen gemakkelijk configureren door het scanniveau te kiezen. Sleep de schuifregelaar langs de schaal om het geschikte scanniveau in te stellen.

Er zijn 3 scanniveaus:

| *Beveiligingsniveau* | *Beschrijving* |
|---|---|
| **Laag** | Biedt een redelijke detectie-efficiëntie. Het verbruiksniveau van de bron is laag.<br>Alleen programma's worden gescand op virussen. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. |
| **Gemiddeld** | Biedt een goede detectie-efficiëntie. Het verbruiksniveau van de bron is gemiddeld.<br>Alle bestanden worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. |
| **Hoog** | Biedt een hoge detectie-efficiëntie. Het verbruiksniveau van de bron is hoog.<br>Alle bestanden en archieven worden gescand op virussen en spyware. Naast de klassieke op handtekeningen gebaseerde scan, wordt ook de heuristische analyse gebruikt. |

Er is ook een reeks algemene opties beschikbaar voor het scanproces.

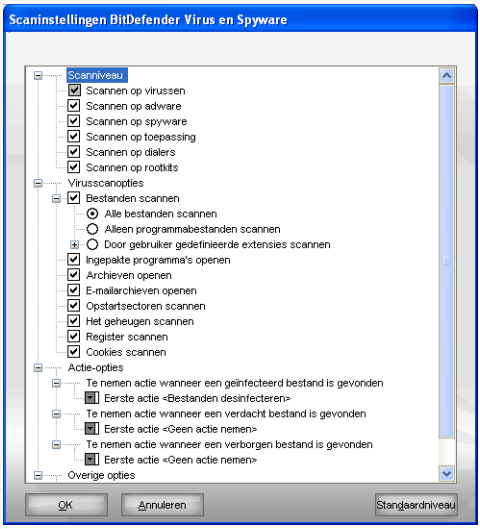
| *Optie* | *Beschrijving* |
|---|---|
| **De taak uitvoeren met lage prioriteit** | Verlaagt de prioriteit van het scanproces. U zult andere programma's sneller kunnen uitvoeren en de tijd die nodig is om het scanproces te voltooien, verlengen. |
| **Scanvenster naar systeemvak minimaliseren bij opstarten** | Minimaliseert het scanvenster naar het systeemvak. Dubbelklik op het pictogram BitDefender om het programma te openen. |

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

### *Het scanniveau aanpassen*

Gevorderde gebruikers willen wellicht voordeel halen uit de scaninstellingen die door BitDefender worden aangeboden. De scanner kan worden ingesteld om alleen specifieke bestandsextensies te scannen, specifieke malware-bedreigingen te zoeken of archieven over te slaan. Dat kan de duur van het scannen aanzienlijk verkorten en de reactie van uw computer tijdens het scannen verbeteren.

Klik op **Aangepast** om uw eigen scanopties in te stellen. Een nieuw venster wordt weergegeven.




**Scaninstellingen**

De scanopties zijn georganiseerd als een uitbereidbaar menu, vergelijkbaar met de menu's die in Windows gebruikt worden. Klik op het vakje met een "+" om een optie te openen of op het vakje met een "-" om een optie te sluiten.

De scanopties zijn gegroepeerd in vijf categorieën:

- **Scanniveau**
- **Virusscanopties**
- **Actie-opties**
- **Overige opties**

- Geef het type malware op waarop BitDefender moet scannen door de geschikte opties te selecteren in de categorie **Scanniveau**.

  De volgende opties zijn beschikbaar:

| Optie | Beschrijving |
|---|---|
| **Scannen op virussen** | Scant op bekende virussen.<br>BitDefender detecteert ook onvolledige virussen waardoor elke mogelijke bedreiging die de beveiliging van uw systeem kan beïnvloeden, wordt verwijderd. |
| **Scannen op adware** | Scant op adware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die adware-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld. |
| **Scannen op spyware** | Scant op bekende spyware-bedreigingen. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. |
| **Scannen op toepassing** | Scant toepassingen (`.exe`- en `.dll`-bestanden). |
| **Scannen op dialers** | Scant op toepassingen die dure nummers belt. Gedetecteerde bestanden zullen worden behandeld als geïnfecteerd. Software die dialer-componenten bevat, zal mogelijk niet meer werken als deze optie is ingeschakeld. |
| **Scannen op rootkits** | Scant op verborgen objecten (bestanden en processen), algemeen bekend als rootkits. |

- Geef het type objecten op dat moet worden gescand (archieven, e-mailberichten, enz.) en definieer andere opties. Selecteer hiervoor bepaalde opties van de categorie **Virusscanopties**.

  De volgende opties zijn beschikbaar:

| Optie | | Beschrijving |
|---|---|---|
| **Bestanden scannen** | **Alle bestanden scannen** | Alle geopende bestanden worden gescand, ongeacht hun type. |

| Optie | | Beschrijving |
|---|---|---|
| | **Alleen programmabestanden scannen** | Alleen de programmabestanden worden gescand. Dit betekent alleen bestanden met de volgende extensies: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml en nws. |
| | **Door gebruiker gedefinieerde extensies scannen** | Alleen de bestanden met de extensies die door de gebruiker zijn gedefinieerd, worden gescand. Deze extensies moeten worden gescheiden door ";". |
| **Ingepakte programma's openen** | | Scant ingepakte bestanden. |
| **Archieven openen** | | Scant binnen archieven. |
| **E-mailarchieven openen** | | Scant binnen e-mailarchieven. |
| **Opstartsectoren scannen** | | Scant de opstartsector van het systeem. |
| **Geheugen scannen** | | Scant het geheugen op virussen en andere malware. |
| **Register scannen** | | Scant registergegevens. |
| **Cookies scannen** | | Scant cookiebestanden. |

- Geef de acties op die moeten worden genomen voor de geïnfecteerde, verdachte of verborgen bestanden die in de categorie **Actie-opties** zijn gedetecteerd. U kunt een verschillende actie voor elke categorie opgeven.
  - Selecteer de actie die moet worden genomen voor de geïnfecteerde bestanden. De volgende opties zijn beschikbaar:

| Actie | Beschrijving |
|---|---|
| **Geen (logboekobjecten)** | Er wordt geen actie ondernomen voor geïnfecteerde bestanden. Deze bestanden zullen verschijnen in het rapportbestand. |
| **Bestanden desinfecteren** | Desinfecteert geïnfecteerde bestanden. |

| Actie | Beschrijving |
|---|---|
| **Bestanden verwijderen** | Verwijdert onmiddellijk de geïnfecteerde bestanden, zonder enige waarschuwing. |
| **Bestanden verplaatsen naar quarantaine** | Verplaatst de geïnfecteerde bestanden naar de quarantaine. |

- Selecteer de actie die moet worden genomen voor de verdachte bestanden die zijn gedetecteerd. De volgende opties zijn beschikbaar:

| Actie | Beschrijving |
|---|---|
| **Geen (logboekobjecten)** | Er wordt geen actie ondernomen voor verdachte bestanden. Deze bestanden zullen verschijnen in het rapportbestand. |
| **Bestanden verwijderen** | Verwijdert onmiddellijk de verdachte bestanden, zonder enige waarschuwing. |
| **Bestanden verplaatsen naar quarantaine** | Verplaatst de verdachte bestanden naar de quarantaine. |

*Opmerking*
De bestanden worden gedetecteerd als verdacht door de heuristische analyse. Wij raden u aan deze bestanden naar het BitDefender Lab te sturen.

- Selecteer de actie die moet worden genomen voor de verborgen objecten (rootkits) die zijn gedetecteerd. De volgende opties zijn beschikbaar:

| Actie | Beschrijving |
|---|---|
| **Geen (logboekobjecten)** | Er wordt geen actie ondernomen voor verborgen bestanden. Deze bestanden zullen verschijnen in het rapportbestand. |
| **Bestanden verplaatsen naar quarantaine** | Verplaatst de verborgen bestanden naar de quarantaine. |
| **Zichtbaar maken** | Maakt verborgen bestanden zichtbaar. |

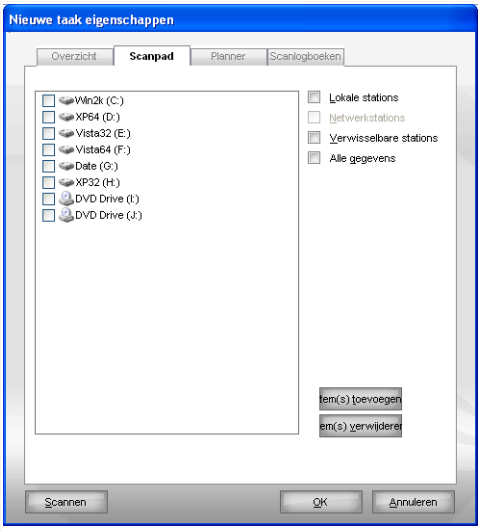
*Opmerking*
Als u de gedetecteerde bestanden wilt negeren of als de gekozen actie mislukt, moet u een actie selecteren in de scanwizard.

- Om te worden gevraagd alle verdachte bestanden naar het BitDefender lab te sturen nadat het scanproces is voltooid, schakelt u het selectievakje **Verdachte bestanden verzenden naar BitDefender Lab** in de categorie **Andere opties** in.

Als u op **Standaard** klikt, worden de standaardinstellingen geladen. Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

## Het scandoel instellen

Om het scandoel in te stellen van een scantaak van een specifieke gebruiker, klikt u rechts op de taak en selecteert u **Scandoel wijzigen**. Het volgende venster wordt geopend:




**Scandoel**

U kunt de lijst van lokale, netwerk en verwisselbare stations evenals de bestanden of mappen die eventueel eerder werden toegevoegd, weergeven. Alle ingeschakelde items zullen worden gescand tijdens het uitvoeren van de taak.

Dit onderdeel bevat de volgende knoppen:

- **Item toevoegen** - opent een zoekvenster waarin u de bestanden/mappen die u wilt scannen, kunt selecteren.

  *Opmerking*
  U kunt ook slepen & neerzetten gebruiken om bestanden/mappen toe te voegen aan de lijst.

- **Item verwijderen** - verwijdert bestanden/mappen die vooraf werden geselecteerd in de lijst van objecten die moeten worden gescand.

  *Opmerking*
  Alleen de bestanden/mappen die achteraf werden toegevoegd, kunnen worden verwijderd. Dat is niet mogelijk met de bestanden/mappen die automatisch door BitDefender werden "gezien".

Naast de knoppen die hierboven zijn toegelicht, zijn er ook enkele opties waarmee u de scanlocaties snel kunt selecteren.

- **Lokale stations** - om de lokale stations te scannen.
- **Netwerkstations** - om alle netwerkstations te scannen.
- **Verwisselbare stations** - om de verwisselbare stations (cd-rom, diskettestation) te scannen.
- **Alle gegevens** - om alle stations te scannen, ongeacht of ze lokaal, in het netwerk of verwisselbaar zijn.

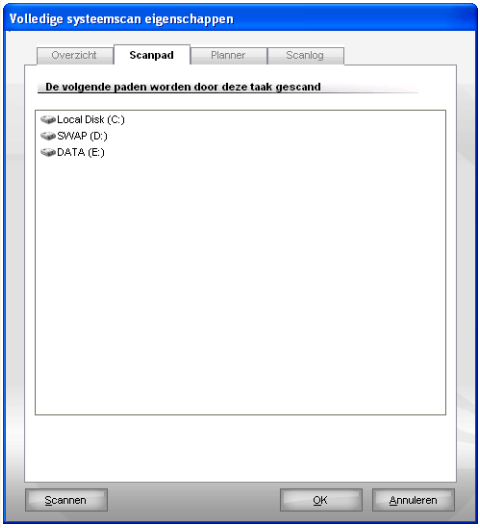
*Opmerking*
Activeer het selectievakje naast **Alle gegevens** als u uw volledige computer wilt scannen op virussen.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

### *Scandoel van systeemtaken bekijken*

U kunt het scandoel van de scantaken niet wijzigen via de categorie **Systeemtaken**. U kan alleen het scandoel ervan zien.

Om het scandoel te tonen van een scantaak van een specifieke systeem, klikt u rechts op de taak en selecteert u **Taakpaden weergeven**. Voor een **Volledige systeemscan**, bijvoorbeeld, verschijnt het volgende venster:




**Scandoel van Volledige systeemscan**

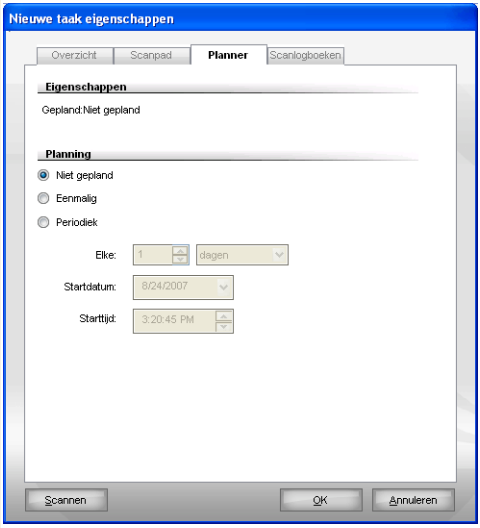
**Volledige systeemscan** en **Diepe systeemscan** scannen alle lokale schijven, terwijl **Snelle systeemscan** alleen de `Windows` en `Program Files` mappen scant.

Klik op **OK** om het venster te sluiten. Om deze taak uit te voeren, klikt u op **Scan**.

## *Scantaken plannen*

Bij complexe taken zal het scanproces enige tijd in beslag nemen en zal het proces het beste werken als u alle andere programma's afsluit. Daarom is het aan te raden dergelijke taken te plannen op tijdstippen waarop u de computer niet gebruikt en naar de inactieve stand is overgeschakeld.

Om de planning van een specifieke taak weer te geven of te wijzigen, klikt u met de rechtermuisknop op de taak en selecteert u **Planning**. Het volgende venster wordt geopend:




**Planner**

Als er een taakplanning is, kunt u deze bekijken.

Wanneer u een taak plant, moet u een van de volgende opties kiezen:

- **Niet gepland** - start de taak alleen wanneer de gebruiker dit vraagt.
- **Eenmalig** - start het scannen eenmalig op een bepaald ogenblik. Geef de startdatum en het starttijdstip op in de velden **Startdatum/Starttijd**.
- **Periodiek** - start de scan periodiek, met bepaalde tijdintervallen (uren, dagen, weken, maanden, jaren) vanaf een opgegeven datum en tijdstip.

  Selecteer **Periodiek** als u wilt dat het scannen met bepaalde intervallen wordt herhaald en geef het aantal minuten/uren/dagen/weken/maanden/jaren op in het bewerkingsvak **Elke** om de frequentie van dit proces aan te geven. U moet ook de startdatum en het starttijdstip opgeven in de velden **Startdatum/Starttijd**.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

## 8.2.5. Objecten scannen

Voordat u het scanproces start, moet u controleren of de malware-handtekeningen up-to-date zijn in BitDefender. Het scannen van uw computer met een oude handtekeningendatabase kan verhinderen dat BitDefender nieuwe malware die sinds de laatste update is gevonden, detecteert. Om te controleren wanneer de laatste update is uitgevoerd, klikt u in de instellingsconsole op **Update>Update** .

***Opmerking***
Als u wilt dat BitDefender een volledige scan uitvoert, moet u alle geopende programma's afsluiten. Het is vooral belangrijk dat u uw e-mail-client afsluit (Outlook, Outlook Express of Eudora).

### Scanmethoden

BitDefender biedt u vier types voor het scannen op aanvraag:

- Onmiddellijk scannen - voer een scantaak uit van de systeem-/gebruikerstaken.
- Contextueel scannen - klik met de rechtermuisknop op een bestand of een map en selecteer BitDefender Antivirus 2008.
- Scannen door slepen & neerzetten - sleep een bestand of map naar de balk Scanactiviteit.
- Handmatig scannen - gebruik BitDefender Handmatig scannen om de bestanden of mappen die moeten worden gescand, rechtstreeks te selecteren.

#### *Onmiddellijk scannen*

Om uw computer volledig of gedeeltelijk te scannen, kunt u de standaard scantaken of uw eigen scantaken uitvoeren. Dit wordt Onmiddellijk scannen genoemd.

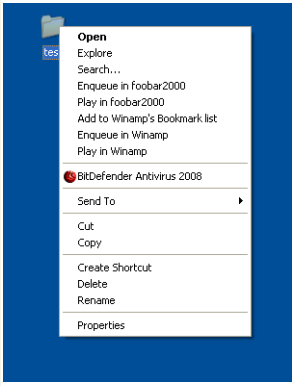
Gebruik een van de volgende methoden om een scantaak uit te voeren:

- dubbelklik op de gewenste scantaak in de lijst.
- klik op de knop **Nu scannen** die overeenkomt met de taak.
- selecteer de taak en klik vervolgens op **Taak uitvoeren**.

BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 69).

#### *Contextueel scannen*

Om een bestand of een map te scannen zonder een nieuwe scantaak te configureren, kunt u het contextmenu gebruiken. Dit wordt Contextueel scannen genoemd.




**Contextueel scannen**

Klik met de rechtermuisknop op het bestand of de map die u wilt scannen en selecteer **BitDefender Antivirus 2008**.

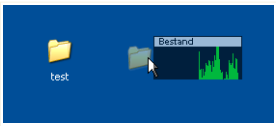
BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 69).

U kunt de scanopties wijzigen en de rapportbestanden weergeven door het venster **Eigenschappen** van de taak **Contextmenuscan** te openen.

### *Scannen door slepen & neerzetten*

Sleep het bestand of de map die u wilt scannen naar de **balk Scanactiviteit** zoals hieronder weergegeven.


**Bestand slepen**




**Bestand neerzetten**

BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 69).

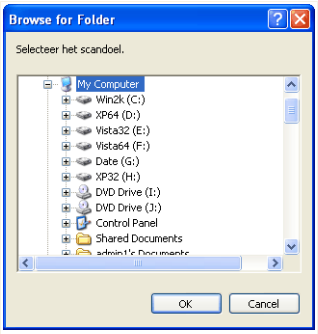
### Handmatig scannen

Handmatig scannen bestaat uit het rechtstreeks selecteren van het object dat moet worden gescand door middel van de optie Handmatig scannen van BitDefender in de programmagroep BitDefender in het menu Start.

**Opmerking**
Het handmatig scannen is zeer nuttig omdat het ook kan worden uitgevoerd wanneer Windows in de veilige modus werkt.

Om het object dat door BitDefender moet worden gescand te selecteren, gebruikt u het menu Start van Windows en volgt u het pad **Start → Programma's → BitDefender 2008 → BitDefender Handmatig scannen**.

Het volgende venster wordt geopend:




**Handmatig scannen**

Selecteer het object dat u wilt scannen en klik op **OK**.

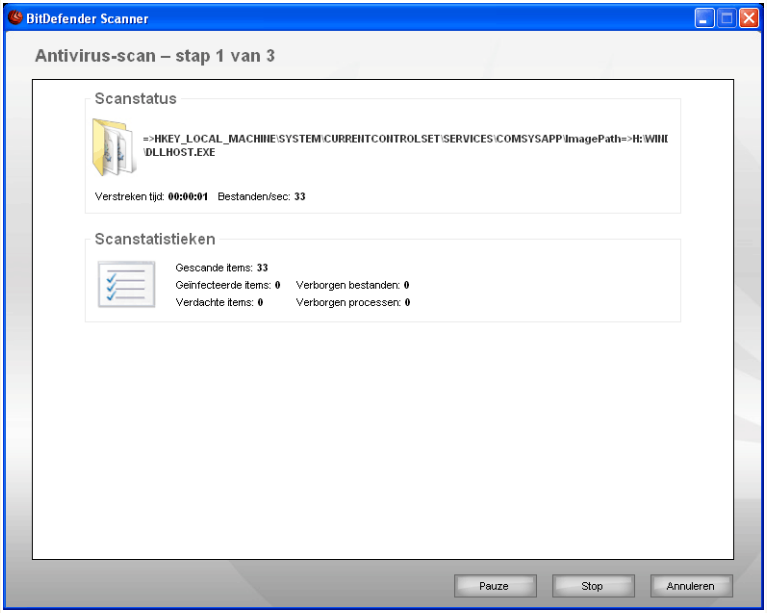
BitDefender Scanner verschijnt en het scannen wordt gestart. Meer informatie vindt u onder "*BitDefender Scanner*" (p. 69).

## BitDefender Scanner

Wanneer u een proces Scannen op aanvraag start, verschijnt BitDefender Scanner. Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

### Stap 1/3 - Scannen

BitDefender start het scannen van de geselecteerde objecten.




**Scannen**

U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

***Opmerking***
Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

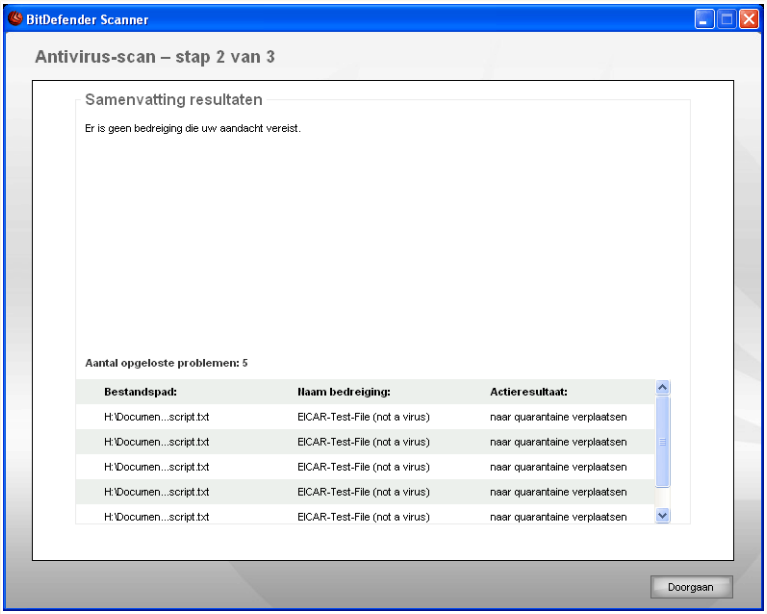
Klik op **Pauze** om het scanproces tijdelijk te stoppen. Om het scannen te hervatten, klikt u op **Hervatten**.

U kunt het scannen op elkogenblik stoppen door op **Stop&Ja** te klikken. U gaat dan rechtstreeks naar de laatste stap van de wizard.

Wacht tot BitDefender het scannen beëindigt.

### *Stap 2/3 - Acties selecteren*

Wanneer het scannen is voltooid, verschijnt een nieuw venster waarin u de scanresultaten kunt zien.




**Acties**

U kunt het aantal problemen dat uw systeem beïnvloedt, zien.

De geïnfecteerde objecten worden weergegeven in groepen, die zijn gebaseerd op de malware waarmee ze zijn geïnfecteerd. Klik op de link van de bedreiging voor meer informatie over de geïnfecteerde objecten.

U kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.

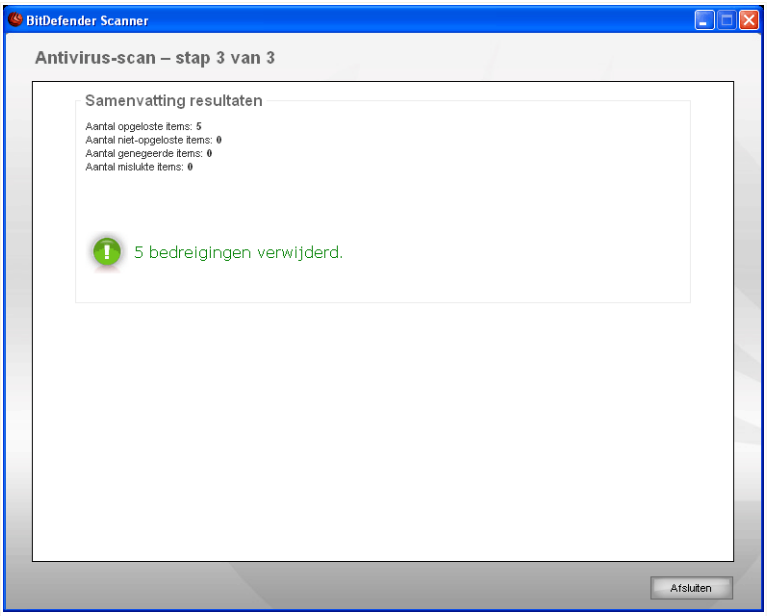
De volgende opties kunnen in het menu verschijnen.

| Actie | Beschrijving |
|---|---|
| **Geen actie nemen** | Er wordt geen actie ondernomen voor de geïnfecteerde bestanden. |
| **Desinfecteren** | Desinfecteert geïnfecteerde bestanden. |
| **Verwijderen** | Verwijdert gedetecteerde bestanden. |
| **Zichtbaar maken** | Maakt verborgen objecten zichtbaar. |

Klik op **Doorgaan** om de aangegeven acties toe te passen.

### *Stap 3/3 - Resultaten weergeven*

Wanneer BitDefender het oplossen van de problemen heeft voltooid, verschijnen de scanresultaten in een nieuw venster.




**Overzicht**

U kunt een samenvatting van de resultaten zien. Het rapportbestand wordt automatisch opgeslagen in het gedeelte Logboeken in het venster **Eigenschappen** van de respectievelijke taak.

***Belangrijk***
U wordt gevraagd uw systeem opnieuw te starten zodat het installatieprogramma de installatie kan voltooien.

Klik op **Afsluiten** om het venster te sluiten.

***BitDefender kon bepaalde zaken niet oplossen***

In de meeste gevallen desinfecteert BitDefender met succes de geïnfecteerde bestanden die het detecteert of isoleert het de infectie. Niet alle zaken kunnen echter worden opgelost.

In deze gevallen, raden wij u aan contact op te nemen met het ondersteuningsteam van BitDefender op www.bitdefender.com. Onze experts helpen u de problemen op te lossen.

***BitDefender detecteerde met een wachtwoord beschermde zaken***

De met een wachtwoord beschermde categorie bevat twee types van zaken: archieven en installatieprogramma's. Zij vormen geen echte bedreiging voor de veiligheid van het systeem, tenzij zij geïnfecteerde bestanden bevatten en alleen als zij worden uitgevoerd.

Om zeker te weten dat deze zaken schoon zijn:

- Als de met een wachtwoord beschermde zaak een archief is dat u met een wachtwoord hebt beschermt, pakt u de bestanden die erin staan uit en scant u deze afzonderlijk. Klik erop met de rechtermuisknop en selecteer **BitDefender Antivirus 2008** in het menu.
- Als de met een wachtwoord beschermde zaak een installatieprogramma is, controleer dan of de real-time bescherming is ingeschakeld voordat u het installatieprogramma uitvoert. Als het installatieprogramma is geïnfecteerd, zal BitDefender de infectie detecteren en isoleren.

Als u niet wilt dat deze objecten opnieuw worden gedetecteerd door BitDefender, moet u deze toevoegen als uitzonderingen op het scanproces. Om scanuitzonderingen toe te voegen, klikt u op **Instellingen** om de instellingenconsole te openen en gaat u naar **Antivirus > Uitzonderingen** . Voor meer informatie raadpleegt u de Objecten die zijn uitgesloten van de scan.

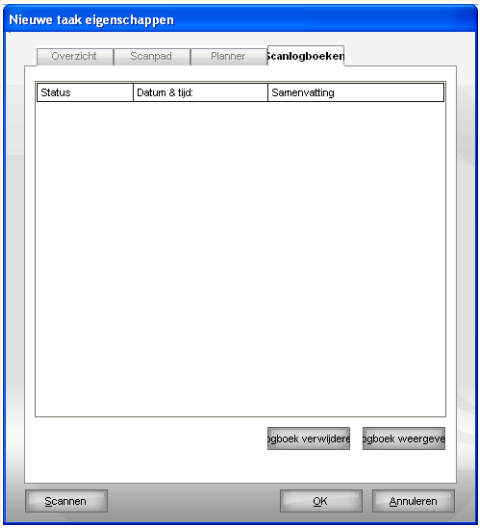
*BitDefender detecteerde verdachte bestanden*

Verdachte bestanden zijn bestanden die zijn gedetecteerd door de heuristische analyse en die mogelijk geïnfecteerd zijn met malware waarvan de signatuur nog niet bekend is.

Als er tijdens het scannen verdachte bestanden zijn gedetecteerd, wordt u gevraagd ze naar het BitDefender Lab te sturen. Klik op **OK** om deze bestanden naar het BitDefender laboratorium te verzenden voor verdere analyse.

## 8.2.6. Scanlogboeken weergeven

Om de scanresultaten te zien nadat een taak is uitgevoerd, klikt u met de rechtermuisknop op de taak en selecteert u **Logboeken**. Het volgende venster wordt geopend:




**Scanlogs**

Hier ziet u de rapportbestanden die zijn gegenereerd bij het uitvoeren van de taak.

Van elk bestand krijgt u informatie over de status van het gevolgde scanproces, de datum en tijd waarop de scan is uitgevoerd en een samenvatting van de scanresultaten.

Er zijn twee knoppen beschikbaar:

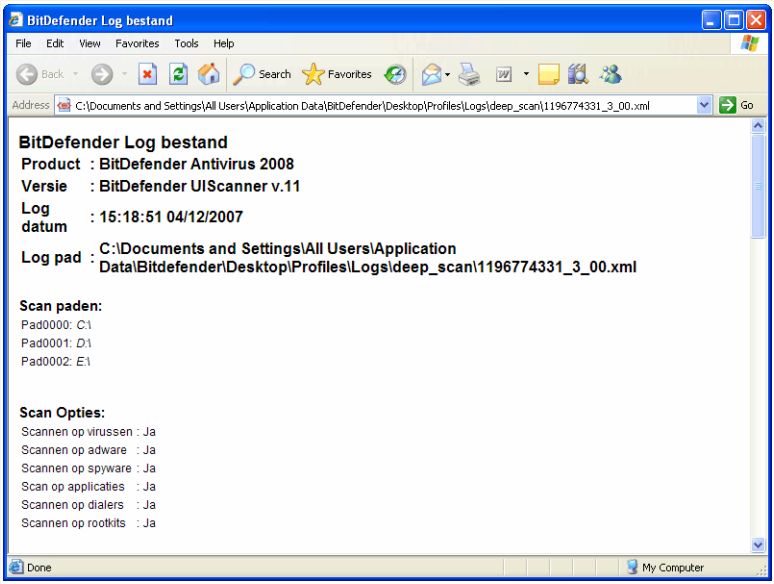
- **Log verwijderen** - om het geselecteerde scanlog rapportbestand te verwijderen.
- **Log weergeven** - om het geselecteerde scanlog rapportbestand weer te geven. Het scanlog rapportbestand wordt geopend in uw standaard webbrowser.

*Opmerking*
Om een bestand weer te geven of te verwijderen, kunt u ook met de rechtermuisknop op de overeenkomende optie klikken in het snelmenu.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten. Klik op **Scannen** om de taak uit te voeren.

## Scanlogs

De volgende afbeelding is een voorbeeld van een scanlog rapportbestand:




**Scanlogs**

Het scanlog bevat gedetailleerde informatie over het gevolgde scanproces, zoals de scanopties, het scandoel, de gevonden bedreigingen en de hierop uitgevoerde acties.

# 8.3. Objecten die zijn uitgesloten van het scannen

Er zijn situaties waarbij u bepaalde bestanden zult willen uitsluiten van het scannen. U zult bijvoorbeeld een EICAR-testbestand willen uitsluiten van een Scan bij toegang of `.avi`-bestanden van een Scan op aanvraag.

Met BitDefender kunt u objecten uitsluiten van een Scan bij toegang, een Scan op aanvraag, of beide. Deze functie is bedoeld om de scantijden te verkorten en onderbreking in uw werk te vermijden.

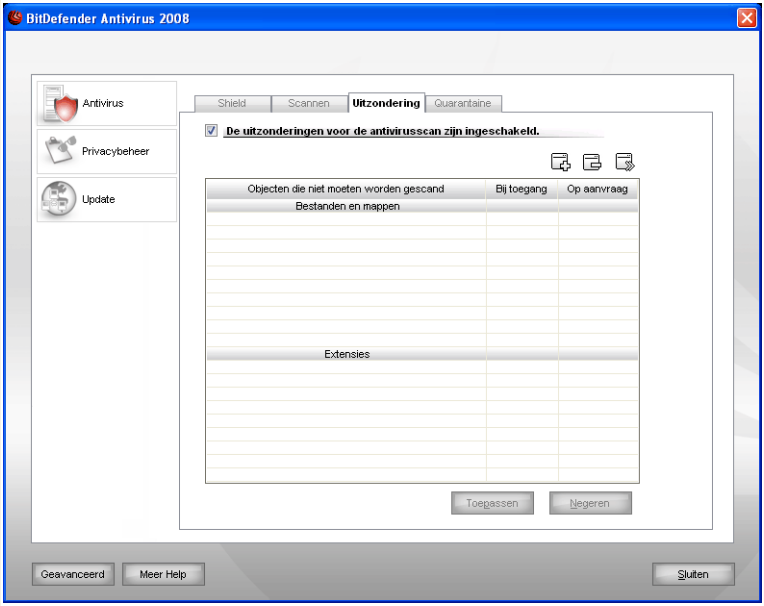
Er kunnen types objecten worden uitgesloten van het scannen.

- **Paden** - het bestand of de map (inclusief alle objecten die erin zijn opgenomen) die is aangegeven door een opgegeven pad, wordt uitgesloten van het scannen.
- **Extensies** - alle bestanden met een specifieke extensie zullen worden uitgesloten van de scan.

*Opmerking*

De objecten die zijn uitgesloten van scannen bij toegang, worden niet gescand, ongeacht of ze door u of door een toepassing zijn geopend.

Om de objecten die zijn uitgesloten van het scannen, weer te geven en te beheren, klikt u op **Antivirus>Uitzonderingen** in de instellingsconsole. Het volgende venster wordt geopend:




**Uitzonderingen**

U kunt de objecten (bestanden, mappen, extensies) zien die van het scannen zijn uitgesloten. Voor elk object kunt u zien of het is uitgesloten van scannen bij toegang, scannen op aanvraag of beide.

*Opmerking*
De uitzonderingen die hier zijn opgegeven, zullen NIET van toepassing zijn voor contextueel scannen.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Om een gegeven in de tabel te bewerken, selecteert u het gegeven en klikt u op de knop **Bewerken**. Er verschijnt een nieuw venster. Hier kunt u de extensie of het pad dat moet worden uitgesloten en het type scan waarvoor u ze wilt uitsluiten, wijzigen volgens uw voorkeur. Breng de nodige wijzigingen aan en klik op **OK**.

*Opmerking*
U kunt ook met de rechtermuisknop op een object klikken en de opties in het snelmenu gebruiken om het object te bewerken of te verwijderen.

U kunt klikken op **Negeren** om de wijzigingen aan de regeltabel ongedaan te maken, op voorwaarde dat u ze niet hebt opgeslagen door op **Toepassen** te klikken.

## 8.3.1. Paden uitsluiten van het scannen

Om paden uit te sluiten van het scannen, klikt u op de knop **Toevoegen**. De configuratiewizard die verschijnt, zal u begeleiden doorheen het proces voor het uitsluiten van paden van de scan.

### Stap 1/3 - Objecttype selecteren


**Objecttype**

Selecteer de optie om een pad uit te sluiten van de scan.

Klik op **Volgende**.

## Stap 2/3 - Uitgesloten paden opgeven


**Uitgesloten paden**

Om de paden die moeten worden uitgesloten van de scan op te geven, gebruikt u een van de volgende methoden.

- Klik op **Bladeren**, selecteer het bestand of de map die u wilt uitsluiten van de scan en klik vervolgens op **Toevoegen**.
- Voer het pad in dat u wilt uitsluiten van de scan in het bewerkingsveld en klik op **Toevoegen**.

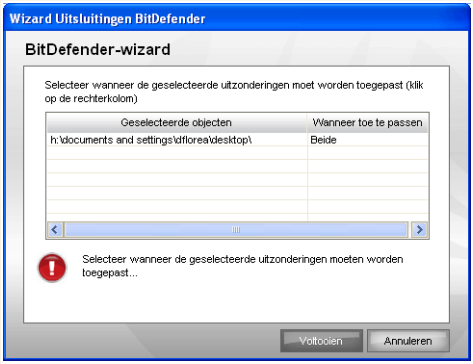
> ***Opmerking***
> Als het opgegeven pad niet bestaat, verschijnt een foutbericht. Klik op **OK** en controleer het pad op geldigheid.

De paden verschijnen in de tabel wanneer u ze toevoegt. U kunt zoveel paden toevoegen als u wilt.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Klik op **Volgende**.

### Stap 3/3 - Scantype selecteren




**Scantype**

U ziet een tabel met de paden die moeten worden uitgesloten van de scan en het type scan waarvan ze zijn uitgesloten.

De geselecteerde paden worden standaard uitgesloten van Scan bij toegang en van Scan bij aanvraag. Om te wijzigen wanneer de uitzondering moet worden toegepast, klikt u op de rechterkolom en selecteert u de gewenste optie in de lijst.

Klik op **Voltooien**.

Klik op **Toepassen** om de wijzigingen op te slaan.

## 8.3.2. Extensies uitsluiten van het scannen

Om extensies uit te sluiten van het scannen, klikt u op de knop **Toevoegen**. De configuratiewizard die verschijnt, zal u begeleiden doorheen het proces voor het uitsluiten van extensies van de scan.

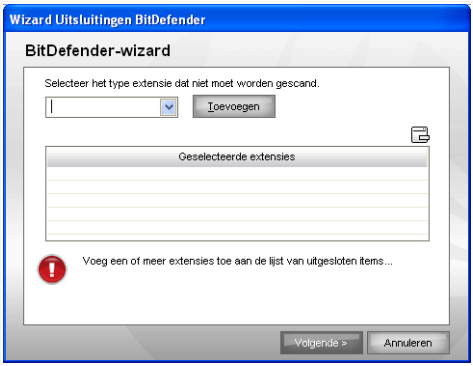
## Stap 1/3 - Objecttype selecteren


**Objecttype**

Selecteer de optie om een extensie uit te sluiten van de scan.

Klik op **Volgende**.

## Stap 2/3 - Uitgesloten extensies opgeven




**Uitgesloten extensies**

Om de extensies die moeten worden uitgesloten van de scan op te geven, gebruikt u een van de volgende methoden.

- Selecteer de extensie die u wilt uitsluiten van de scan in het menu en klik vervolgens op **Toevoegen**.

> ***Opmerking***
> Het menu bevat een lijst met alle extensies die op uw systeem zijn geregistreerd. Wanneer u een extensie selecteert, kunt u de beschrijving zien, indien deze beschikbaar is.

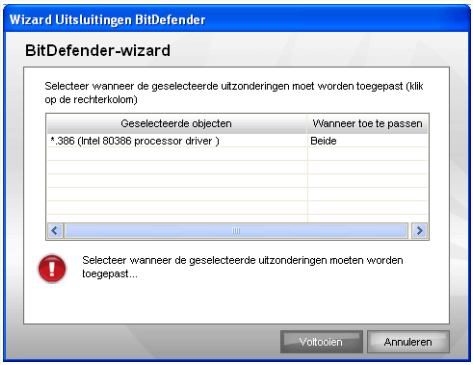
- Voer de extensie in die u wilt uitsluiten van de scan in het bewerkingsveld en klik op **Toevoegen**.

De extensies verschijnen in de tabel wanneer u ze toevoegt. U kunt zoveel extensies toevoegen als u wilt.

Om een gegeven uit de tabel te verwijderen, selecteert u het gegeven en klikt u op de knop **Verwijderen**.

Klik op **Volgende**.

## *Stap 3/3 - Scantype selecteren*




**Scantype**

U ziet een tabel met de extensies die moeten worden uitgesloten van de scan en het type scan waarvan ze zijn uitgesloten.

De geselecteerde extensies worden standaard uitgesloten van Scan bij toegang en van Scan bij aanvraag. Om te wijzigen wanneer de uitzondering moet worden toegepast, klikt u op de rechterkolom en selecteert u de gewenste optie in de lijst.

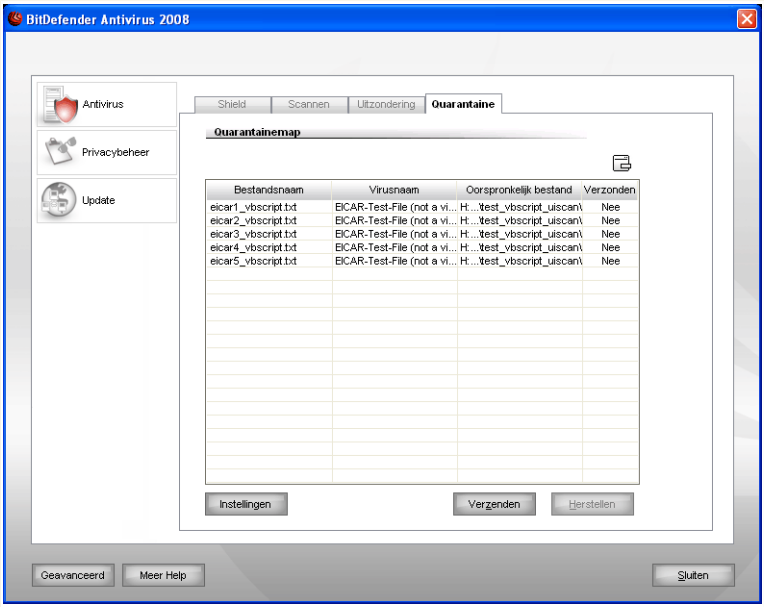
Klik op **Voltooien**.

Klik op **Toepassen** om de wijzigingen op te slaan.

# 8.4. Quarantainegebied

BitDefender biedt u de mogelijkheid geïnfecteerde of verdachte bestanden te isoleren in een beveiligd gebied, de quarantaine. Door deze bestanden te isoleren in de quarantaine verdwijnt het risico op infecties, maar hebt u tegelijk ook de mogelijkheid deze bestanden voor verdere analyse te verzenden naar het BitDefender lab.

Om de bestanden in quarantaine te zien en te beheren en om de quarantaine-instellingen te configureren, klikt u op **Antivirus>Quarantaine** in de instellingsconsole.




**Quarantaine**

## 8.4.1. Bestanden in quarantaine beheren

Zoals u wellicht zult merk, bevat het onderdeel **Quarantaine** een lijst van alle bestanden die tot nog toe werden geïsoleerd. Elk bestand bevat zijn naam, grootte, isolatiedatum en verzendingsdatum.

*Opmerking*
Wanneer het virus in quarantaine is, kan het geen schade berokkenen, aangezien het niet kan worden uitgevoerd of gelezen.

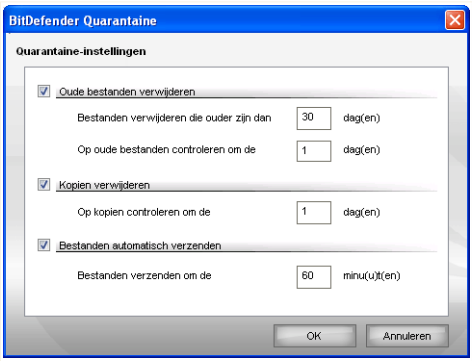
Om een geselecteerd bestand uit de quarantaine te verwijderen, klikt u op de knop **Verwijderen**. Als u een geselecteerd bestand wilt terugzetten op zijn oorspronkelijke locatie, klikt u op **Herstellen**.

U kunt elk geselecteerd bestand van de quarantaine verzenden naar het BitDefender Lab door op **Verzenden** te klikken.

**Contextmenu.** Er is een snelmenu beschikbaar waarmee u de bestanden in quarantaine gemakkelijk kunt beheren. Dezelfde opties zoals eerder vermeld, zijn beschikbaar. U kunt ook **Vernieuwen** selecteren om het gebied Quarantaine te vernieuwen.

## 8.4.2. Quarantaine-instellingen configureren

Klik op **Instellingen** om de quarantaine-instellingen te configureren. Een nieuw venster wordt weergegeven.




**Quarantaine-instellingen**

Met de quarantaine-instellingen, kunt u BitDefender instellen om de volgende acties automatisch uit te voeren.

**Oude bestanden verwijderen.** Om oude bestanden in quarantaine automatisch te verwijderen, schakelt u de overeenkomende optie in. U moet opgeven na hoeveel dagen de bestanden in quarantaine moeten worden verwijderd en de frequentie instellen waarmee BitDefender oude bestanden zou moeten controleren.

*Opmerking*
BitDefender zal standaard elke dag controleren op oude bestanden en bestanden die ouder zijn dan 10 dagen verwijderen.

**Kopieën verwijderen.** Om dubbele bestanden in quarantaine automatisch te verwijderen, schakelt u de overeenkomende optie in. U moet het aantal dagen tussen twee opeenvolgende controles op kopieën opgeven.

*Opmerking*
Standaar zal BitDefender dagelijks controleren op dubbele bestanden in de quarantaine.

**Bestanden automatisch verzenden.** Om bestanden in quarantaine automatisch te verzenden, schakelt u de overeenkomende optie in. U moet de frequentie waarmee de bestanden moeten worden verzonden, opgeven.

*Opmerking*
Standaard zal BitDefender de bestanden in quarantaine elke 60 minuten automatisch verzenden.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

# 9. Privacybeheer

BitDefender controleert tientallen potentiële "hotspots" in uw systeem waar spyware kan optreden en controleert ook alle wijzigingen aan uw systeem en software. Hij is bijzonder efficiënt bij het blokkeren van Trojaanse paarden en andere programma's die worden geïnstalleerd door hackers, die proberen uw privacy in gevaar te brengen en uw persoonlijke informatie, zoals kredietkaartnummers, verzenden van uw computer naar de hacker.

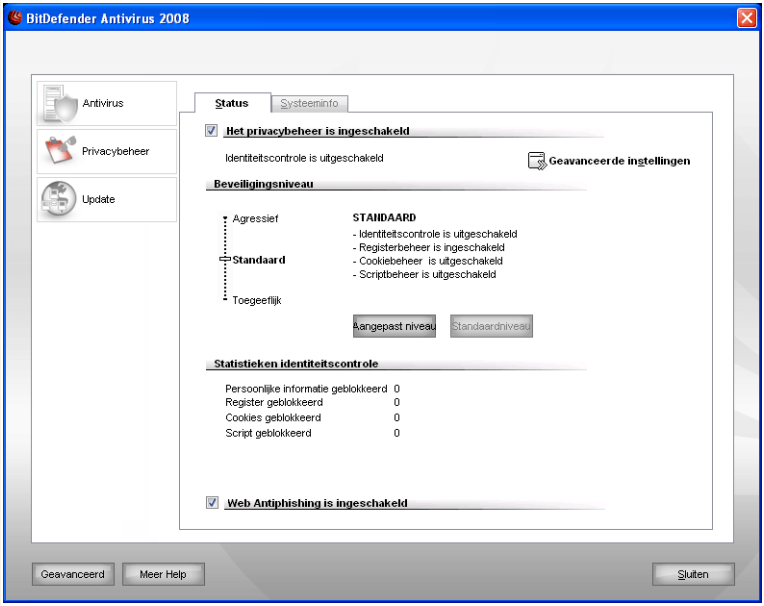
BitDefender scant ook de websites die u bezoekt en waarschuwt u als er een phishing-bedreiging is gedetecteerd.

Het gedeelte **Privacybeheer** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Status Privacybeheer
- Geavanceerde instellingen - Identiteitscontrole
- Geavanceerde instellingen - Registerbeheer
- Geavanceerde instellingen - Cookiebeheer
- Geavanceerde instellingen - Scriptbeheer
- Systeeminformatie
- Antiphishing-werkbalk

## 9.1. Status Privacybeheer

Om het Privacybeheer te configureren en informatie met betrekking tot zijn activiteit te bekijken, klikt u op **Privacybeheer>Status** in de instellingsconsole. Het volgende venster wordt geopend:




**Status Privacybeheer**

## 9.1.1. Privacybeheer

***Belangrijk***
Om diefstal van data te voorkomen en om uw privacy te beschermen, moet u **Privacycontrole** ingeschakeld laten.

Het Privacybeheer beveiligt uw computer met 5 belangrijke beveiligingselementen:

- Identiteitscontrole - beschermt uw vertrouwelijke gegevens door al het uitgaande HTTP- en SMTP-verkeer te filteren volgens de regels die u in de sectie Identiteit hebt gemaakt.

***Opmerking***
Aan het eind van de sectie ziet u de **Identiteitscontrole statistieken**.

- Registerbeheer - vraagt uw toestemming wanneer een programma probeert een registergegeven te wijzigen om te worden uitgevoerd bij het opstarten van Windows.
- Cookiebeheer - vraagt uw toestemming wanneer een nieuwe website een cookie probeert te plaatsen.
- Scriptbeheer - vraagt uw toestemming wanneer een website een script of andere actieve inhoud probeert te activeren.

Om de instellingen voor deze beheeropties te configureren, klikt u op Geavanceerde instellingen.

### *Het beveiligingsniveau configureren*

U kunt het beveiligingsniveau kiezen dat beter voldoet aan uw beveiligingsbehoeften. Sleep de schuifregelaar langs de schaal om het geschikte beveiligingsniveau in te stellen.

Er zijn 3 beveiligingsniveaus:

| *Beveiligingsniveau* | *Beschrijving* |
|---|---|
| **Toegeeflijk** | Alleen **Registerbeheer** is ingeschakeld. |
| **Standaard** | **Registerbeheer** en **Identiteitcontrole** zijn ingeschakeld. |
| **Agressief** | **Registerbeheer**, **Identiteitscontrole** en **Scriptbeheer** zijn ingeschakeld. |

U kan het beveiligingsniveau aanpassen door te klikken op **Aangepast niveau**. In het venster dat verschijnt, selecteert u de beveiligingen die u wilt inschakelen en klikt u op **OK**.

Klik op **Stand.niveau** om de schuifregelaar op het standaardniveau in te stellen.

## *9.1.2. Antiphishing-beveiliging*

Phishing is een criminele activiteit op het internet dat sociale technieken gebruikt om mensen door een list te overhalen persoonlijke informatie te geven.

In de meeste gevallen bestaan phishing-pogingen uit het verzenden van grote hoeveelheden e-mailberichten die valselijk beweren dat ze van een gevestigde, wettelijke onderneming afkomstig zijn. Deze valse berichten worden verzonden in de hoop dat er minstens enkele ontvangers die overeenkomen met het profiel van het phishing-doel, zullen worden overgehaald om persoonlijke informatie vrij te geven.

Een phishing-bericht vermeldt doorgaans een probleem met betrekking tot uw online rekening. Het probeert u te overtuigen om op een koppeling in het bericht te klikken om toegang te krijgen tot een zogenaamde wettelijke website (die in feite een vervalste site is) waar persoonlijke gegevens vereist zijn. U kunt bijvoorbeeld worden gevraagd de gegevens van uw rekening, zoals de gebruikersnaam en het wachtwoord, te bevestigen en het nummer van uw bankrekening of uw nummer bij de sociale zekerheid op te geven. Om nog overtuigender over te komen, kan het bericht soms doen alsof uw rekening al werd of mogelijk zal worden opgeschort als u de bijgeleverde koppeling niet gebruikt.

Phishing maakt ook gebruik van spyware, zoals Trojaanse paarden met toetsenregistratie, om de rekeninginformatie rechtstreeks van uw computer te stelen.

De belangrijkste doelwitten van phishing-pogingen zijn klanten van online betalingsdiensten, zoals eBay en Paypal, evenals banken die online diensten aanbieden. Onlangs werden ook gebruikers van websites van sociale netwerken belaagd door phishing om persoonlijke identificatiegegevens te verkrijgen die worden gebruikt voor identiteitsdiefstal.

Om u tegen phishing-pogingen te beveiligen, moet u **Antiphishing** ingeschakeld houden. Op deze manier zal BitDefender elke website scannen voordat u deze kunt bezoeken en wordt u op de hoogte gebracht van het bestaan van elke phishing-bedreiging. U kunt een Witte lijst configureren van websites die niet door BitDefender moeten worden gescand.

Om de antiphishing-beveiliging en de Witte lijst gemakkelijk te beheren, kunt u de werkbalk van BitDefender Antiphishing gebruiken die in Internet Explorer is geïntegreerd. Meer informatie vindt u onder “*Antiphishing-werkbalk*” (p. 105).

## 9.2. Geavanceerde instellingen - Identiteitscontrole

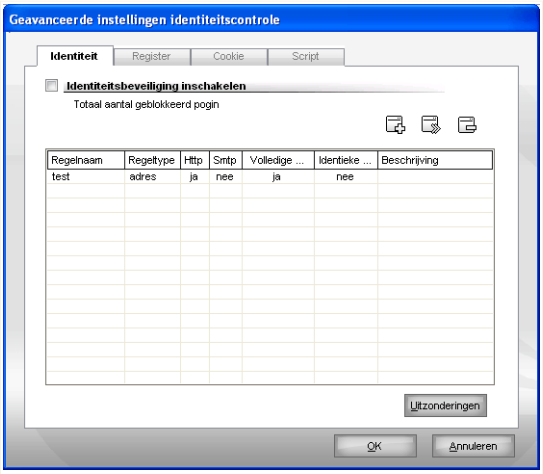
Het veilig houden van vertrouwelijke gegevens is een belangrijke kwestie die ons allen aanbelangt. Gegevensdiefstal is de ontwikkeling van internetcommunicatie gevolgd en maakt gebruik van nieuwe methoden om mensen te misleiden zodat ze persoonlijke gegevens vrijgeven.

**Identiteitscontrole** helpt u vertrouwelijke gegevens veilig te houden. Hiermee wordt HTTP-, SMTP-verkeer, of beide gescand op bepaalde tekenreeksen die u hebt gedefinieerd. Als een overeenkomst is gevonden, wordt de desbetreffende webpagina of e-mail geblokkeerd.

Er is ondersteuning voorzien voor meerdere gebruikers, zodat geen enkele andere gebruiker van het systeem de regels die u hebt geconfigureerd, kan zien.

De privacyregels kunnen worden geconfigureerd in de sectie **Identiteit**. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Identiteit**.

*Opmerking*
Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.



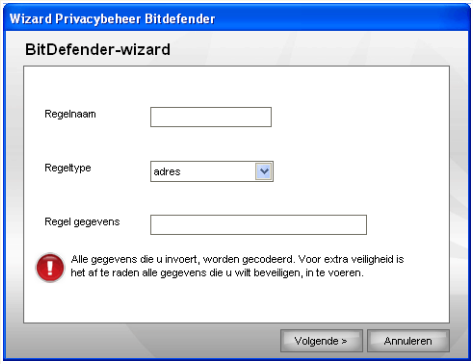

**Identiteitscontrole**

## 9.2.1. Privacyregels maken

De regels moeten handmatig worden ingevoerd (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

De configuratiewizard is een procedure die uit 3 stappen bestaat.

## Stap 1/3 - Type en gegevens van de regel instellen




**Type en gegevens van de regel instellen**

Voer de naam in van de regel in het bewerkingsveld.

U moet de volgende parameters instellen:

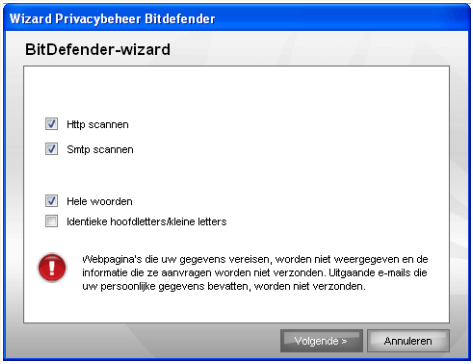
- **Regeltype** - kies het type regel (adres, naam, creditcard, PIN, SSN, enz.).
- **Regelgegevens** - voer de gegevens voor de regel in.

> ***Opmerking***
> Als u minder dan drie tekens invoert, wordt u gevraagd de gegevens te valideren. Wij raden u aan minstens drie tekens in te voeren om te vermijden dat berichten en webpagina's verkeerdelijk worden geblokkeerd.

Alle gegevens die u invoert, worden gecodeerd. Voor extra veiligheid mag u niet alle gegevens invoeren die u wilt beschermen.

Klik op **Volgende**.

## Stap 2/3 - Verkeer selecteren




**Verkeer selecteren**

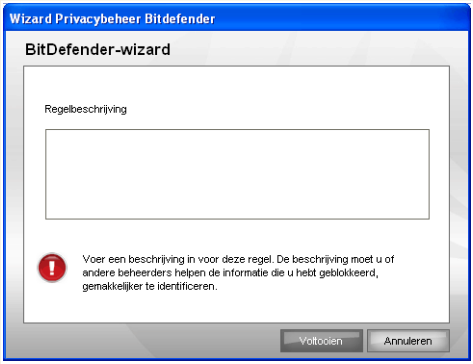
Selecteer het verkeer dat u door BitDefender wilt laten scannen. De volgende opties zijn beschikbaar:

- **HTTP scannen** - scant het HTTP-verkeer (web) en blokkeert uitgaande gegevens die overeenkomen met de regelgegevens.
- **SMTP scannen** - scant het SMTP-verkeer (e-mail) en blokkeert uitgaande e-mailberichten die de regelgegevens bevatten.

U kunt ervoor kiezen de regels alleen toe te passen als de regelgegevens overeenkomen met volledige woorden of als de regelgegevens en de gedetecteerde tekenreeks overeenkomen.

Klik op **Volgende**.

### Stap 3/3 - Regel beschrijven




**Regel beschrijven**

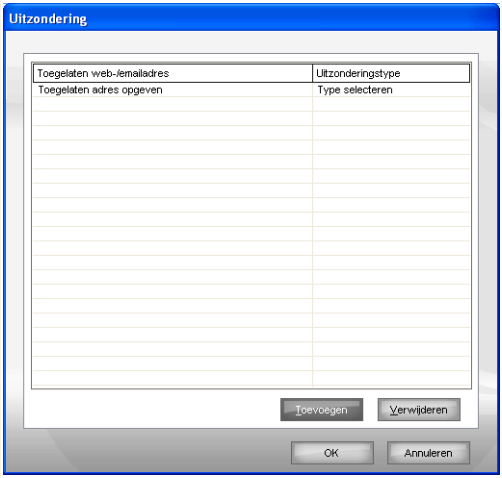
Voer een korte beschrijving in van de regel in het bewerkingsveld.

Klik op **Voltooien**.

## 9.2.2. Uitzonderingen definiëren

Er zijn situaties waarin u uitzonderingen op specifieke identiteitsregels moet definiëren. Laten we even een situatie bekijken waarbij u een regel hebt gemaakt die verhindert dat uw creditcardnummer via HTTP (het web) wordt verzonden. Telkens wanneer uw creditcardnummer vanaf uw gebruikersaccount naar een website wordt verzonden, wordt de desbetreffende pagina geblokkeerd. Als u bijvoorbeeld schoenen wilt kopen in een online winkel (waarvan u zeker bent dat deze veilig is), moet u een uitzondering op de respectievelijke regel opgeven.

Klik op **Uitzonderingen** om het venster te openen waarin u de uitzonderingen kunt beheren.




**Uitzonderingen**

Volg deze stappen om een uitzondering toe te voegen:

1. Klik op **Toevoegen** om een nieuw gegeven in de tabel toe te voegen.
2. Dubbelklik op **Toegelaten adres opgeven** en geef het webadres of het e-mailadres op dat u wilt toevoegen als uitzondering.
3. Dubbelklik op **Type selecteren** en selecteer de optie die overeenkomt met het eerder opgegeven adrestype in het menu.
   - Selecteer **HTTP** als u een webadres hebt opgegeven.
   - Selecteer **SMTP** als u een e-mailadres hebt opgegeven.

Om een uitzondering uit de lijst te verwijderen, selecteert u deze en klikt u op **Verwijderen**.

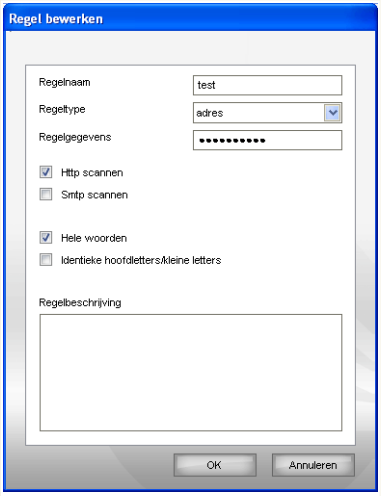
Klik op **OK** om de wijzigingen op te slaan.

## 9.2.3. Regels beheren

De regels worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen**. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

Om een regel te bewerken, selecteert u de regel en klikt u op de knop **Bewerken** of dubbelklikt u op de regel. Een nieuw venster wordt weergegeven.




**Regel bewerken**

Hier kunt u de naam, de beschrijving en de parameters van de regel wijzigen (type, gegevens en verkeer). Klik op **OK** om de wijzigingen op te slaan.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

# 9.3. Geavanceerde instellingen - Registerbeheer

Een bijzonder belangrijk onderdeel van het Windows-besturingssysteem wordt het **Register** genoemd. Dit is de plaats waar Windows zijn instellingen, geïnstalleerde programma's, gebruikersinformatie en heel wat andere gegevens bijhoudt.

Het **Register** wordt ook gebruikt om te definiëren welke programma's automatisch moeten worden gestart wanneer Windows wordt gestart. Virussen maken er dan ook vaak gebruik van om automatisch te worden geactiveerd, zodra de gebruiker zijn computer opnieuw opstart.

Het **Registerbeheer** houdt de gebeurtenissen in het Register van Windows in het oog. Hierdoor is het ook een nuttig middel om Trojaanse paarden te detecteren. U wordt gewaarschuwd zodra een programma probeert een registergegeven te wijzigen, zodat het wordt uitgevoerd bij het opstarten van Windows.


**Registerwaarschuwing**

U kunt deze wijziging weigeren door op **Nee** te klikken of toestaan door op **Ja** te klikken.

Als u wilt dat BitDefender uw antwoord onthoudt, schakelt u de optie **Deze actie altijd toepassen voor dit programma** in. Hierdoor wordt een regel gemaakt en zal dezelfde actie telkens worden toegepast wanneer dit programma een registergegeven probeert te wijzigen zodat het moet worden uitgevoerd bij het opstarten van Windows.

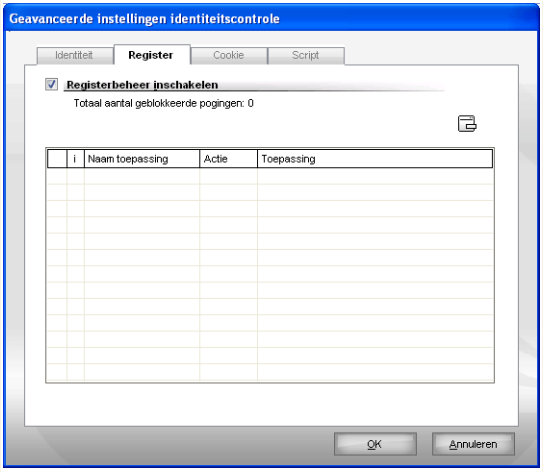
*Opmerking*

BitDefender zal u doorgaans waarschuwen wanneer u nieuwe programma's installeert die moeten worden uitgevoerd nadat u de computer de volgende keer opstart. In de meeste gevallen zijn deze programma's rechtmatig en kunnen ze worden vertrouwd.

U kunt elke regel die werd onthouden in het gedeelte **Register** openen om deze verder fijn af te stemmen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Register**.

*Opmerking*

Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.




**Registerbeheer**

De regels die tot nog toe zijn gemaakt, worden weergegeven in de tabel.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen**. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

Om de actie van een regel te wijzigen, dubbelklikt u op het actieveld en selecteert u de geschikte optie in het menu.

Klik op **OK** om het venster te sluiten.

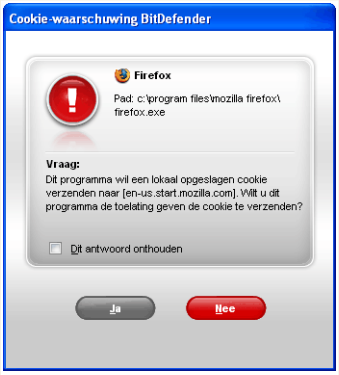
# 9.4. Geavanceerde instellingen - Cookiebeheer

Cookies zijn een bijzonder gangbaar fenomeen op het Internet. Het zijn kleine bestanden die op uw computer worden opgeslagen. Websites maken deze cookies om specifieke informatie over u bij te houden.

Cookies zijn meestal ontwikkeld om u het leven te vergemakkelijken. Ze kunnen de website bijvoorbeeld helpen uw naam en voorkeuren te onthouden, zodat u ze niet telkens opnieuw moet invoeren wanneer u de site bezoekt.

Cookies kunnen echter ook worden gebruikt om uw privacy in gevaar te brengen door de patronen van uw surfgedrag op te sporen.

Dit is het punt waarop het **Cookiebeheer** ingrijpt. Wanneer u het **Cookiebeheer** inschakelt, zal het telkens uw toestemming vragen wanneer een nieuwe website een cookie probeert te plaatsen:




**Cookie-waarschuwing**

U ziet de naam van de toepassing die u probeert het cookiebestand te zenden.

Schakel de optie **Dit antwoord onthouden** in en klik op **Ja** of **Nee**. Een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels. U zult niet langer op de hoogte worden gebracht wanneer u de volgende keer een verbinding maakt met dezelfde site.

Dit zal u helpen een keuze te maken van de websites die u wel of niet vertrouwt.

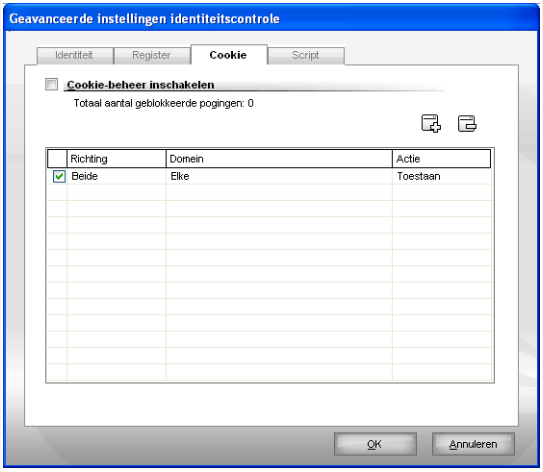
*Opmerking*

Gezien het grote aantal cookies dat tegenwoordig op het Internet wordt gebruikt, kan het **Cookiebeheer** aanvankelijk nogal hinderlijk zijn. Het zal u eerst veel vragen stellen over sites die proberen cookies te plaatsen op uw computer. Zodra u uw gebruikelijke sites toevoegt aan de regellijst, zult u opnieuw even gemakkelijk kunnen surfen als voorheen.

U kunt elke regel die werd onthouden, openen in het onderdeel **Cookie** om deze fijner in te stellen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Cookie**.

*Opmerking*

Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.




**Cookiebeheer**

De regels die tot nog toe zijn gemaakt, worden weergegeven in de tabel.

***Belangrijk***
De regels worden vanaf boven weergegeven in volgorde van prioriteit, wat betekent dat de eerste regel de hoogste prioriteit heeft. U kunt de regels slepen & neerzetten om hun prioriteit te wijzigen.

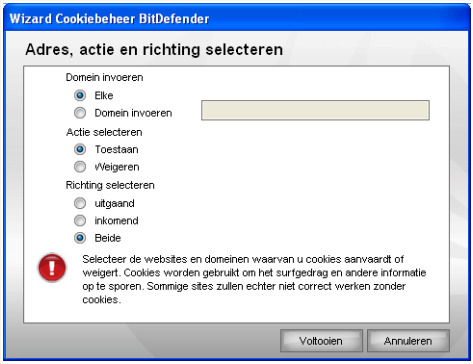
Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een parameter van een regel te wijzigen, dubbelklikt u op zijn veld en brengt u de gewenste wijziging aan. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

De regels kunnen automatisch worden ingevoerd (via het waarschuwingsvenster) of handmatig (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

## 9.4.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

## Stap 1/1 - Adres, actie en richting selecteren




**Adres, actie en richting selecteren**

U kunt de volgende parameters instellen:

- **Domeinadres** - voer het domein in waarop de regel moet worden toegepast.
- **Actie** - selecteer de actie van de regel.

| Actie | Beschrijving |
|---|---|
| **Toestaan** | De cookies op dat domein zullen worden uitgevoerd. |
| **Weigeren** | De cookies op dat domein zullen niet worden uitgevoerd. |

- **Richting** - selecteer de richting voor het verkeer.

| Type | Beschrijving |
|---|---|
| **Uitgaand** | De regel zal alleen worden toegepast op cookies die worden teruggezonden naar de verbonden site. |
| **Binnenkomend** | De regel zal alleen worden toegepast op cookies die worden ontvangen van de verbonden site. |
| **Beide** | De regel zal in beide richtingen worden toegepast. |

Klik op **Voltooien**.

*Opmerking*
U kunt cookies aanvaarden, maar ze nooit terugsturen. Stel hiervoor de actie in op **Weigeren** en de richting op **Uitgaand**.

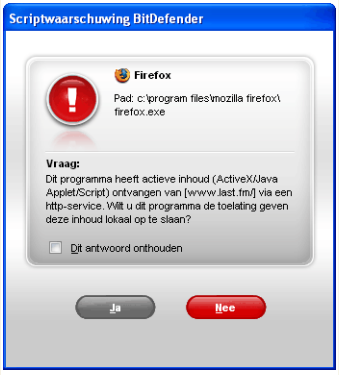
Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

# 9.5. Geavanceerde instellingen - Scriptbeheer

Scripts en andere codes, zoals ActiveX-besturingselementen en Java-applets, die worden gebruikt om interactieve webpagina's te maken, kunnen worden geprogrammeerd om schadelijke effecten te veroorzaken. ActiveX-elementen kunnen bijvoorbeeld de volledige toegang verkrijgen tot uw gegevens en kunnen gegevens lezen van uw computer, informatie verwijderen, wachtwoorden overnemen en berichten onderscheppen terwijl u on line bent. Wij raden u dan ook aan alleen actieve inhoud te aanvaarden van sites die u volledig kent en vertrouwt.

Met BitDefender kunt u beslissen of u deze elementen wilt uitvoeren of als u het uitvoeren wilt blokkeren.

Met het **Scriptbeheer** bepaalt u zelf welke websites u vertrouwt en welke niet. BitDefender zal telkens uw toestemming vragen wanneer een website een script of andere actieve inhoud probeert te activeren.



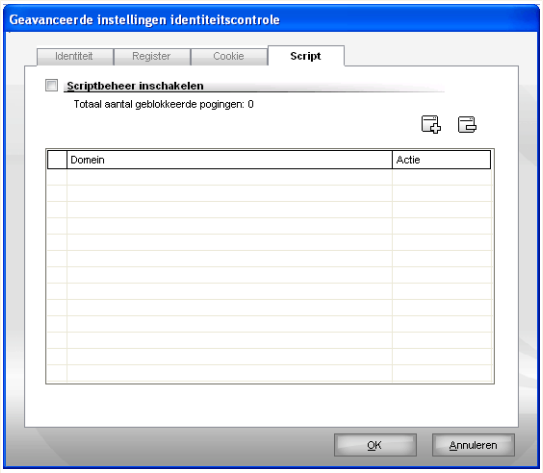

**Script-waarschuwing**

De naam van de bron wordt weergegeven.

Schakel de optie **Dit antwoord onthouden** in en klik op **Ja** of **Nee**. Een regel wordt gemaakt, toegepast en weergegeven in de tabel met regels. U wordt niet langer op de hoogte gebracht wanneer dezelfde site probeert u actieve inhoud te zenden.

U kunt elke regel die werd onthouden, openen in het onderdeel **Script** om deze fijner in te stellen. Om toegang te krijgen tot deze sectie, opent u het venster **Geavanceerde instellingen Privacybeheer** en klikt u op het tabblad **Script**.

*Opmerking*
Om het venster **Geavanceerde instellingen Privacybeheer** te openen, klikt u op **Privacybeheer>Status** in de instellingsconsole en klikt u op **Geavanceerde instellingen**.




**Scriptbeheer**

De regels die tot nog toe zijn gemaakt, worden weergegeven in de tabel.

*Belangrijk*
De regels worden vanaf boven weergegeven in volgorde van prioriteit, wat betekent dat de eerste regel de hoogste prioriteit heeft. U kunt de regels slepen & neerzetten om hun prioriteit te wijzigen.

Om een regel te verwijderen, selecteert u de regel en klikt u op de knop **Verwijderen** Om een parameter van een regel te wijzigen, dubbelklikt u op zijn veld en brengt u de gewenste wijziging aan. Als u een regel tijdelijk wilt uitschakelen zonder deze te verwijderen, moet u het overeenkomende selectievakje uitschakelen.

De regels kunnen automatisch worden ingevoerd (via het waarschuwingsvenster) of handmatig (klik op de knop **Toevoegen** en kies de parameters voor de regel). De configuratiewizard wordt geopend.

## 9.5.1. Configuratiewizard

De configuratiewizard is een procedure die uit 1 stap bestaat.

### Stap 1/1 - Adres en actie selecteren


**Adres en actie selecteren**

U kunt de volgende parameters instellen:

- **Domeinadres** - voer het domein in waarop de regel moet worden toegepast.
- **Actie** - selecteer de actie van de regel.

| Actie | Beschrijving |
|---|---|
| **Toestaan** | De scripts op dat domein zullen worden uitgevoerd. |
| **Weigeren** | De scripts op dat domein zullen niet worden uitgevoerd. |

Klik op **Voltooien**.

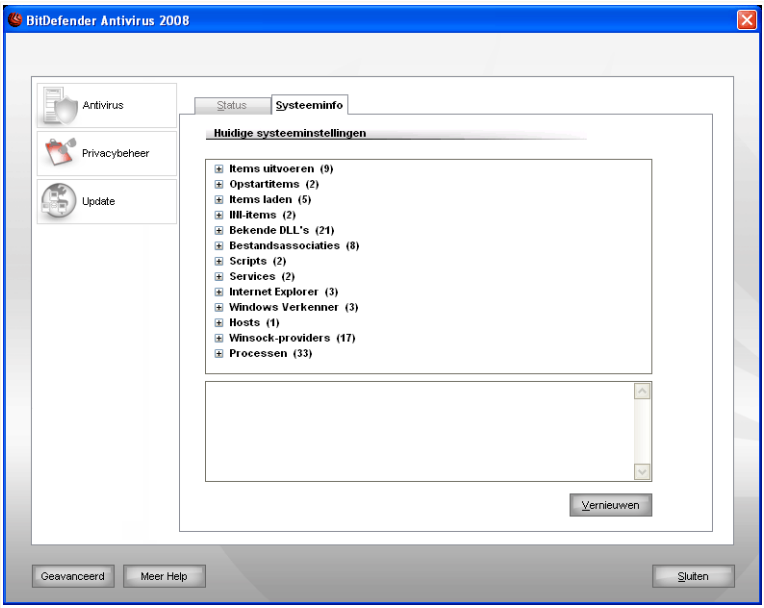
Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

# 9.6. Systeeminformatie

Met BitDefender kunt u vanaf één locatie alle systeeminstellingen bekijken, samen met de toepassingen die zijn geregistreerd om te worden uitgevoerd bij het opstarten.

Hierdoor kunt u de activiteit controleren van het systeem en de toepassingen die op het systeem zijn geïnstalleerd en kunt u mogelijke systeeminfecties identificeren.

Om systeeminformatie te verkrijgen, klikt u op **Privacybeheer>Systeeminfo** in de instellingsconsole. Het volgende venster wordt geopend:




**Systeeminformatie**

De lijst bevat alle items die zijn geladen bij het opstarten van het systeem, maar ook de items die door de verschillende toepassingen zijn geladen.

Er zijn drie knoppen beschikbaar:

- **Verwijderen** - verwijdert het geselecteerde item. U moet op **Ja** klikken om uw keuze te bevestigen.

> ***Opmerking***
> Als u tijdens de huidige sessie niet opnieuw wilt worden gevraagd uw keuze te bevestigen, moet u het selectievakje **Mij niet meer vragen tijdens deze sessie** inschakelen.

- **Ga naar** - opent een venster waar het geselecteerde item is geplaatst (bijvoorbeeld **Register**).
- **Vernieuwen** - opent het gedeelte **Systeeminfo** opnieuw.

*Opmerking*
Afhankelijk van het geselecteerde item, kan één of beide knoppen **Verwijderen** of **Ga naar** misschien niet verschijnen.

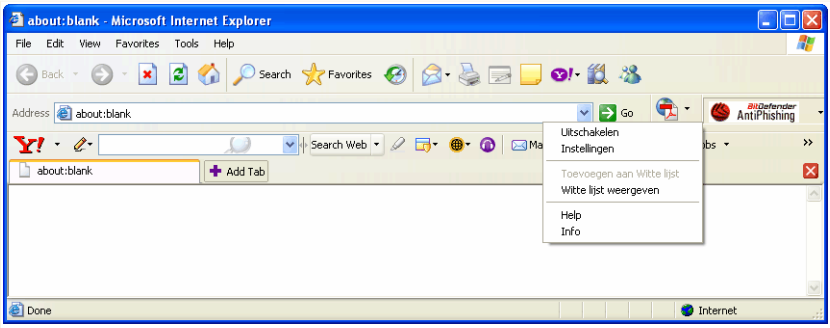
## 9.7. Antiphishing-werkbalk

BitDefender beveiligt u tegen phishing-pogingen terwijl u op het internet surft. Het programma scant de bezochte websites en waarschuwt u als er phishing-bedreigingen zijn. U kunt een Witte lijst configureren van websites die niet door BitDefender moeten worden gescand.

U kunt de antiphishing-beveiliging en de Witte lijst gemakkelijk en efficiënt beheren met de werkbalk van BitDefender Antiphishing die in Internet Explorer is geïntegreerd.

De antiphishing-werkbalk die wordt voorgesteld door het **BitDefender-pictogram**, bevindt zich bovenaan in Internet Explorer. Klik op dit pictogram om het werkbalkmenu te openen.

*Opmerking*
Als u de werkbalk niet kunt zien, opent u het menu **Weergave**, wijst u **Werkbalken** aan en selecteert u **Werkbalk BitDefender**.




**Antiphishing-werkbalk**

De volgende opdrachten zijn beschikbaar in het werkbalkmenu:

- Met **Inschakelen / Uitschakelen** - wordt de Antiphishing-werkbalk van BitDefender in- of uitgeschakeld.

*Opmerking*
Als u ervoor kiest de antiphishing-werkbalk uit te schakelen, bent u niet langer beveiligd tegen phishing-pogingen.

- **Instellingen** - opent een venster waarin u de instellingen voor de antiphishing-werkbalk kunt opgeven.

  De volgende opties zijn beschikbaar:
  - **Scannen inschakelen** - schakelt het scannen van antiphishing in.
  - **Vragen vóór toevoegen aan witte lijst** - vraagt uw bevestiging voordat een website aan de witte lijst wordt toegevoegd.
- **Toevoegen aan Witte lijst** - voegt de huidige website toe aan de Witte lijst.

*Opmerking*
Wanneer een site wordt toegevoegd aan de Witte lijst, betekent dit dat BitDefender de site niet langer zal scannen op phishing-pogingen. Wij raden u aan alleen sites die u volledig vertrouwt toe te voegen aan de Witte lijst.

- **Witte lijst tonen** - opent de Witte lijst.

  U kunt de lijst weergeven van alle websites die niet door de antiphishing-engines van BitDefender worden gecontroleerd.

  Als u een site uit de Witte lijst wilt verwijderen, zodat u op de hoogte wordt gebracht van eventuele phishing-bedreigingen op die pagina, klikt u op de knop **Verwijderen** naast de naam van de site.

  U kunt de sites die u volledig vertrouwt toevoegen aan de Witte lijst, zodat ze niet langer worden gescand door de antiphishing-engines. Om een site toe te voegen aan de Witte lijst, geeft u het adres van de site op in het overeenkomende veld en kikt u op **Toevoegen**.
- **Help** - opent het Help-bestand.
- **Info** - opent een venster waar u informatie over BitDefender kunt bekijken en waar u hulp kunt zoeken wanneer er zich een onverwachte gebeurtenis voordoet.

# 10. Update

Elke dag wordt nieuwe malware gevonden en geïdentificeerd. Het is dan ook heel belangrijk dat u BitDefender up-to-date houdt met de meest recente malware handtekeningen.

Als u via breedband of DSL verbonden bent met het Internet, zal BitDefender deze taak op zich nemen. Het programma controleert standaard op updates wanneer u uw computer inschakelt en daarna om het **uur**.

Als een update wordt gevonden, wordt u, afhankelijk van de opties die zijn ingesteld in het gedeelte Automatische update-instellingen, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

Het updateproces wordt "on the fly" uitgevoerd. Dit betekent dat de bestanden die moeten worden bijgewerkt, progressief worden vervangen. Hierdoor zal het updateproces de productwerking niet beïnvloeden wordt tegelijkertijd elk zwak punt uitgeschakeld.

Updates worden op de volgende manieren beschikbaar gesteld:

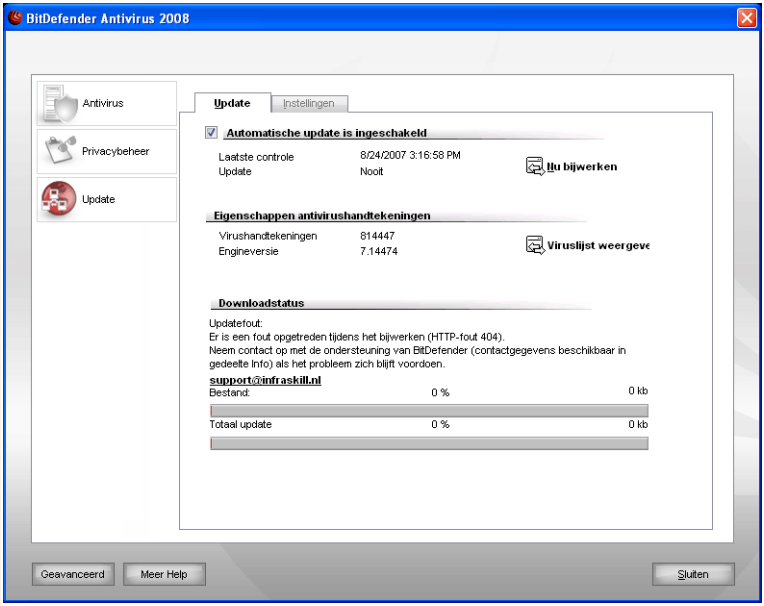
- **Updates voor antivirus-engines** - aangezien er steeds nieuwe virussen dreigen, moeten de bestanden met de virushandtekeningen voortdurend worden bijgewerkt om een permanente up-to-date beveiliging te garanderen. Dit type update is ook bekend als **Update virusdefinities**.
- **Updates voor de antispyware-engines** - er worden nieuwe spyware-handtekeningen toegevoegd aan de database. Dit type update is ook bekend als **Antispyware -update**.
- **Product upgrades** - Bij de lancering van een nieuwe productversie worden nieuwe functies en scantechnieken ingevoerd met het oog op een betere prestatie van het product. Dit type update is ook bekend als **Product-update**.

Het gedeelte **Update** in deze gebruiksaanwijzing bevat de volgende onderwerpen:

- Automatische update
- Update-instellingen

# 10.1. Automatische update

Om informatie met betrekking tot de update weer te geven en automatische updates uit te voeren, klikt u op **Update>Update** in de instellingsconsole. Het volgende venster wordt geopend:




**Automatische update**

Hier kunt u zien wanneer de laatste controle op updates en de laatste update werd uitgevoerd. Daarnaast vindt u hier ook informatie over de laatst uitgevoerde update (indien gelukt of als er fouten zijn opgetreden). Ook informatie over de huidige engine-versie en het aantal handtekeningen wordt weergegeven.

U kunt de malware-handtekeningen van BitDefender ophalen door te klikken op **Viruslijst weergeven**. Er wordt een HTML-bestand gemaakt dat alle beschikbare handtekeningen bevat. Dit bestand wordt geopend in een webbrowser. U kunt in de database zoeken naar een specifieke malware-handtekening of op **Viruslijst BitDefender** klikken om naar de online handtekeningendatabase van BitDefender te gaan.

Als u deze sectie opent tijdens een update, kunt u de downloadstatus zien.

***Belangrijk***
Houd **Automatische update** ingeschakeld om tegen de meest recente gevaren te worden beschermd.

## 10.1.1. Een update aanvragen

De automatische update kan ook op elk gewenst ogenblik worden uitgevoerd door te klikken op **Nu bijwerken**. Dit type update is ook bekend als de **Update op aanvraag van de gebruiker**.

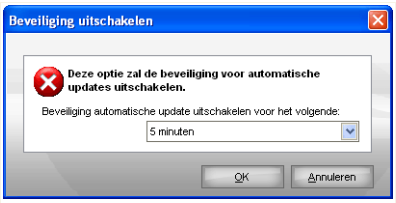
De module **Update** zal een verbinding maken met de updateserver van BitDefender en controleren of er een update beschikbaar is. Als een update wordt gevonden, wordt u, afhankelijk van de opties die zijn ingesteld in het gedeelte Handmatige update-instellingen, gevraagd de update te bevestigen of wordt de update automatisch uitgevoerd.

***Belangrijk***
Het kan noodzakelijk zijn de computer opnieuw op te starten wanneer de update is voltooid. We bevelen aan dit zo snel mogelijk te doen.

***Opmerking***
Als u met het internet bent verbonden via een inbelverbinding, dan adviseren wij BitDefender regelmatig handmatig te updaten.

## 10.1.2. Automatisch update uitschakelen

Als u de automatische update wilt uitschakelen, verschijnt een waarschuwingsvenster.




**Automatische update uitschakelen**

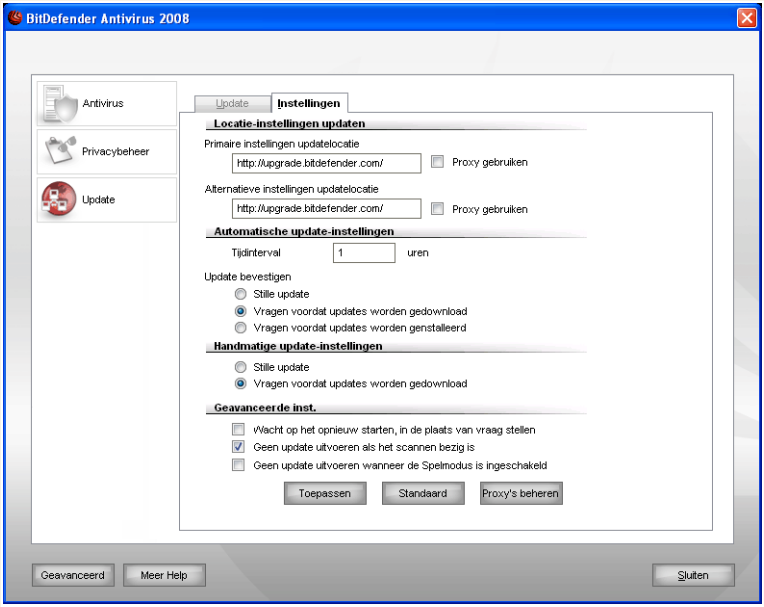
U moet uw keuze bevestigen door in het menu te selecteren hoelang u de automatische update wilt uitschakelen. U kunt de automatische update uitschakelen gedurende 5, 15 of 30 minuten, 1 uur, definitief of tot het systeem opnieuw wordt opgestart.

***Waarschuwing***
Dit is een kritiek beveiligingsprobleem. Wij raden u aan de automatische update zo kort mogelijk uit te schakelen. Als BitDefender niet regelmatig wordt bijgewerkt, zal het programma niet in staat zijn u te beschermen tegen de nieuwste bedreigingen.

# 10.2. Update-instellingen

De updates kunnen worden uitgevoerd vanaf het netwerk, via het Internet, rechtstreeks of via een proxyserver. BitDefender zal standaard elk uur via het internet controleren op updates en de beschikbare updates zonder enige waarschuwing installeren.

Om de update-instellingen te configureren en de proxy's te beheren, klikt u in de instellingsconsole op **Update>Instellingen**. Het volgende venster wordt geopend:




**Update-instellingen**

De update-instellingen zijn gegroepeerde in 4 categorieën (**Updatelocatie-instellingen**, **Automatische update-instellingen**, **Handmatige update-instellingen** en **Geavanceerde instellingen**). Elke categorie wordt afzonderlijk beschreven.

## 10.2.1. De updatelocaties instellen

Gebruik de opties in de categorie **Updatelocatie-instellingen** om de updatelocaties in te stellen.

*Opmerking*
Configureer deze instellingen alleen als u verbonden bent met een lokaal netwerk dat de malware-handtekeningen van BitDefender lokaal opslaat of als u via een proxyserver met het internet bent verbonden.

Voor betrouwbaardere en snellere updates kunt u twee updatelocaties configureren: een **Primaire updatelocatie** en een **Alternatieve updatelocatie**. Deze locaties zijn standaard dezelfde: `http://upgrade.bitdefender.com`.

Om een van de updatelocaties te wijzigen, geeft u de URL van de lokale spiegel op in het **URL**-veld dat overeenkomt met de locatie die u wilt wijzigen.

*Opmerking*
Wij raden u aan de lokale spiegel in te stellen als een primaire updatelocatie en de alternatieve updatelocatie ongewijzigd te laten als een back-upplan in het geval de lokale spiegel onbeschikbaar wordt.

Als het bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, schakelt u het selectievakje **Proxy gebruiken** in en klikt u vervolgens op **Proxy's beheren** om de proxy-instellingen te configureren.

*Opmerking*
Meer informatie vindt u onder "*Proxy's beheren*" (p. 113)

## 10.2.2. Automatische update configureren

U kunt het automatisch uitvoeren van de update door BitDefender instellen met de opties in de categorie **Automatische update-instellingen**.

In het veld **Tijdinterval** kunt u het aantal uren tussen twee opeenvolgende controles op updates opgeven. Het tijdinterval voor de update is standaard ingesteld op 1 uur.

Selecteer een van de volgende opties om op te geven hoe de automatische update moet worden uitgevoerd:

- **Stille update** - BitDefender downloadt en implementeert automatisch de update.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.

*Opmerking*
U wordt de vraag gesteld voordat de updates worden gedownload, zelfs als u het Beveiligingscentrum afsluit.

- **Vragen voordat updates worden geïnstalleerd** - telkens wanneer een update is gedownload, wordt uw bevestiging gevraagd voordat de update wordt geïnstalleerd.

*Opmerking*
U wordt de vraag gesteld voordat de updates worden geïnstalleerd, zelfs als u het Beveiligingscentrum afsluit.

## 10.2.3. Handmatige update configureren

Selecteer een van de volgende opties in de categorie **Handmatige update-instellingen** om op te geven hoe de handmatige update (update op aanvraag van gebruiker) moet worden gebruikt:

- **Stille update** - de handmatige update wordt automatisch uitgevoerd op de achtergrond, zonder enige tussenkomst van de gebruiker.
- **Vragen voordat updates worden gedownload** - telkens wanneer een update beschikbaar is, wordt uw bevestiging gevraagd voordat de update wordt gedownload.

*Opmerking*
U wordt de vraag gesteld voordat de updates worden gedownload, zelfs als u het Beveiligingscentrum afsluit.

## 10.2.4. Geavanceerde instellingen configureren

Om te verhinderen dat het updateproces van BitDefender uw werk hindert, moet u de opties in de categorie **Geavanceerde instellingen** configureren:

- **Wacht op het opnieuw starten, in de plaats van vraag te stellen** - Als een update het opnieuw opstarten vereist, zal het product blijven werken met de oude bestanden tot het systeem opnieuw wordt opgestart. De gebruiker wordt niet gevraagd om opnieuw op te starten. Daarom zal het updateproces van BitDefender geen invloed hebben op het werk van de gebruiker.
- **Geen update uitvoeren als het scannen bezig is** - BitDefender zal geen update uitvoeren als een scanproces wordt uitgevoerd. Hierdoor zal het updateproces van BitDefender de scantaken niet hinderen.

*Opmerking*
Als de update van BitDefender wordt uitgevoerd terwijl het scannen bezig is, wordt het scanproces afgebroken.

- **Geen update uitvoeren wanneer de spelmodus is ingeschakeld** - BitDefender zal geen update uitvoeren wanneer de spelmodus is ingeschakeld. Hierdoor kunt u de invloed van het product op de systeemprestaties beperken tijdens het spelen van spelletjes.

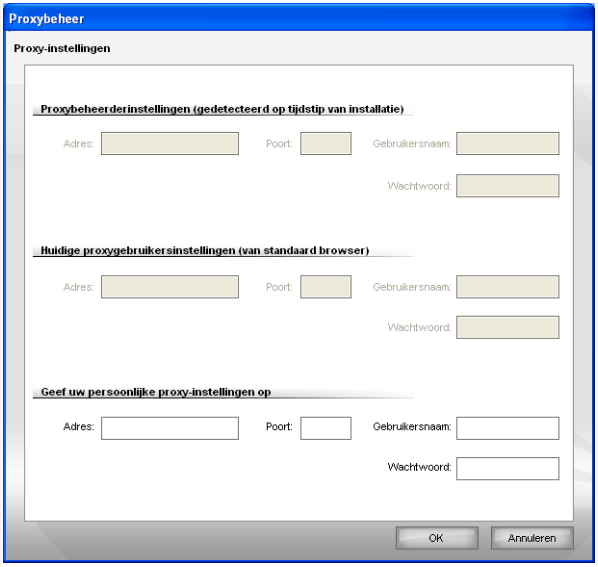
## 10.2.5. Proxy's beheren

Als uw bedrijf een proxyserver gebruikt om een verbinding te maken met het internet, moet u de proxy-instellingen opgeven zodat BitDefender zichzelf kan updaten. Anders zal het programma gebruik maken van de proxy-instellingen van de beheerder die het product heeft geïnstalleerd of van de eventuele standaardbrowser van de huidige gebruiker.

*Opmerking*

De proxy-instellingen kunnen alleen worden geconfigureerd door gebruikers met beheerdersrechten op de computer of door hoofdgebruikers (gebruikers die het wachtwoord voor de productinstellingen kennen).

Klik op **Proxy's beheren** om de proxy-instellingen te beheren. Het venster **Proxybeheer** wordt weergegeven.




**Proxybeheer**

Er zijn drie reeksen proxy-instellingen:

- **Proxybeheerderinstellingen (gedetecteerd op tijdstip van installatie)** - proxy-instellingen die tijdens de installatie op de beheerdersaccount zijn gedetecteerd en die alleen kunnen worden geconfigureerd wanneer u bij die account bent aangemeld. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.
- **Huidige proxygebruikersinstellingen (van standaard browser)** - proxy-instellingen van de huidige gebruikers, opgehaald van de standaard browser. Als de proxyserver een gebruikersnaam en wachtwoord vereist, moet u deze gegevens opgeven in de overeenkomende velden.

> ***Opmerking***
> De ondersteunde webbrowsers zijn Internet Explorer, Mozilla Firefox en Opera. Als u standaard een andere browser gebruikt, zal BitDefender de proxy-instellingen van de huidige gebruiker niet kunnen ophalen.

- **Uw persoonlijke reeks proxy-instellingen** - proxy-instellingen die u kunt configureren als u bent aangemeld als beheerder.

  U moet de volgende instellingen definiëren:
  - **Adres** - voer het IP-adres van de proxyserver in.
  - **Poort** - Voer de poort in die BitDefender gebruikt om een verbinding te maken met de proxyserver.
  - **Gebruikersnaam** - voer een gebruikersnaam in die wordt herkend door de proxy.
  - **Wachtwoord** - voer het geldige wachtwoord voor de eerder opgegeven gebruiker in.

Wanneer u een verbinding probeert te maken met het internet, wordt elke reeks proxy-instellingen achtereenvolgens geprobeerd, tot BitDefender erin slaagt een verbinding te maken.

Eerst wordt de reeks met uw persoonlijke proxy-instellingen gebruikt om een verbinding te maken met het internet. Als dat niet werkt, worden daarna de proxy-instellingen die op het tijdstip van de installatie zijn gedetecteerd, geprobeerd. Als dat evenmin werkt, worden tot slot de proxy-instellingen van de huidige gebruiker overgenomen van de standaard browser en gebruikt om een verbinding te maken met het internet.

Klik op **OK** om de wijzigingen op te slaan en het venster te sluiten.

Klik op **Toepassen** om de wijzigingen op te slaan of klik op **Standaard** om de standaardinstellingen te laden.

# BitDefender reddingsschijf

# 11. Overzicht

**BitDefender Antivirus 2008** wordt geleverd met een opstartbare CD (BitDefender reddingsschijf) die in staat is alle bestaande harde schijven te scannen en te desinfecteren voordat uw besturingssysteem opstart.

Gebruik telkens de BitDefender reddingsschijf wanneer uw besturingssysteem niet correct werkt door de virusinfecties. Dit gebeurt doorgaans wanneer u geen antivirusproduct gebruikt.

Telkens wanneer u de BitDefender reddingsschijf opstart, wordt de update van de virushandtekeningen automatisch uitgevoerd, zonder tussenkomst van de gebruiker.

De BitDefender reddingsschijf is een geremasterde Knoppix-distributie van BitDefender, die de nieuwste BitDefender voor Linux-beveiligingsoplossing integreert in de GNU/Linux Knoppix Live CD en een desktopantivirus biedt die bestaande harde schijven kan scannen en desinfecteren (inclusief Windows NTFS-partities). Op hetzelfde ogenblik kunt u de BitDefender reddingsschijf gebruiken om uw waardevolle gegevens te herstellen wanneer u Windows niet kunt opstarten.

*Opmerking*
De BitDefender reddingsschijf kan worden gedownload van deze locatie: http://download.bitdefender.com/rescue_cd/

## 11.1. Systeemvereisten

Voordat u de BitDefender reddingsschijf opstart, moet u eerst controleren of uw systeem voldoet aan de volgende vereisten.

**Processortype**
x86-compatibel, minimum 166 MHz, maar verwacht geen hoge prestaties in dit geval. Een processor van de i686-generatie met 800 MHz is een betere keuze.

**Geheugen**
Minimum 512 MB RAM-geheugen (1 GB aanbevolen)

**Cd-rom**
De BitDefender reddingsschijf wordt uitgevoerd vanaf een cd-rom. Daarom is een cd-rom en een BIOS waarvan kan worden opgestart vereist.

**Internetverbinding**
Hoewel de BitDefender reddingsschijf kan werken zonder internetverbinding, is er toch een actieve http-verbinding vereist voor de updateprocedure, zelfs via

een proxyserver. Voor een up-to-date beveiliging is een internetverbinding dus een MUST.

**Grafische resolutie**
Standaard SVGA-compatibele grafische kaart.

## 11.2. Bijgeleverde software

De BitDefender reddingsschijf bevat de volgende softwarepakketten.

**Xedit**
Dit is een tekstbestandseditor.

**Vim**
Dit is een krachtige tekstbestandseditor die syntaxmarkering, een GUI en veel meer bevat. Meer informatie vindt u op de Vim-startpagina.

**Xcalc**
Dit is een rekenmachine.

**RoxFiler**
RoxFiler is een snel en krachtig grafisch bestandsbeheer.

Meer informatie vindt u op de RoxFiler-startpagina.

**MidnightCommander**
GNU Midnight Commander (mc) is een beheerprogramma voor tekstmodusbestanden.

Meer informatie vindt u op de MC-startpagina.

**Pstree**
Pstree toont de actieve processen.

**Top**
Top toont Linux-taken.

**Xkill**
Xkill vernietigt een client door middel van zijn X-bronnen.

**Partition Image**
Met Partition Image kunt u partities in de bestandssysteemformaten EXT2, Reiserfs, NTFS, HPFS, FAT16 en FAT32 opslaan naar een imagebestand. Dit programma kan nuttig zijn voor back-updoeleinden.

Meer informatie vindt u op de Partimage-startpagina.

**GtkRecover**

GtkRecover is een GTK-versie van het consoleprogrammaherstel. Het helpt u een bestand te herstellen.

Meer informatie vindt u op de GtkRecover-startpagina.

**ChkRootKit**

ChkRootKit is een hulpprogramma dat u helpt uw computer te scannen op rootkits.

Meer informatie vindt u op de ChkRootKit-startpagina.

**Nessus Network Scanner**

Nessus is een externe beveiligingsscanner voor Linux, Solaris, FreeBSD en Mac OS X.

Meer informatie vindt u op de Nessus-startpagina.

**Iptraf**

Iptraf is een programma voor IP-netwerkbewaking.

Meer informatie vindt u op de Iptraf-startpagina.

**Iftop**

Iftop toont het bandbreedtegebruik op een interface.

Meer informatie vindt u op de Iftop-startpagina.

**MTR**

MTR is een netwerkdiagnosehulpprogramma.

Meer informatie vindt u op de MTR-startpagina.

**PPPStatus**

PPPStatus toont statistieken over het binnenkomende en uitgaande TCP/IP-verkeer.

Meer informatie vindt u op de PPPStatus-startpagina.

**Wavemon**

Wavemon is een bewakingstoepassing voor draadloze netwerkapparaten.

Meer informatie vindt u op de Wavemon-startpagina.

**USBView**

USBView toont informatie over apparaten die zijn aangesloten op de USB-bus.

Meer informatie vindt u op de USBView-startpagina.

**Pppconfig**

Pppconfig helpt bij het automatisch tot stand brengen van een ppp-inbelverbinding.

**DSL/PPPoe**

DSL/PPPoe configureert PPPoE-verbinding (ADSL).

**I810rotate**

I810rotate schakelt de video-uitvoer op i810-hardware door middel van de i810switch(1).

Meer informatie vindt u op de I810rotate-startpagina.

**Mutt**

Mutt is een krachtige, op tekst gebaseerde MIME-e-mailclient.

Meer informatie vindt u op de Mutt-startpagina.

**Mozilla Firefox**

Mozilla Firefox is een bekende webbrowser.

Meer informatie vindt u op de Mozilla Firefox-startpagina.

**Elinks**

Elinks is een webbrowser in tekstmodus.

Meer informatie vindt u op de Elinks-startpagina.

# 12. De BitDefender reddingsschijf gebruiken

Dit hoofdstuk bevat informatie over het starten en stoppen van de BitDefender reddingsschijf, het scannen van uw computer op malware en het opslaan van gegevens vanaf uw aangetaste Windows-pc naar een verwisselbaar apparaat. Wanneer u de softwaretoepassingen die op de cd zijn geleverd gebruikt, kunt u echter heel wat meer taken uitvoeren dan binnen het bereik van deze handleiding kunnen worden beschreven.

## 12.1. BitDefender reddingsschijf starten

Om de cd te starten, stelt u de BIOS van uw computer in om te starten vanaf de cd, plaatst u de cd in het cd-romstation en start u de computer opnieuw op. Controleer of uw computer kan opstarten vanaf een cd.

Wacht tot het volgende scherm wordt getoond en volg de instructies op het scherm om de BitDefender reddingsschijf te starten.


**Splash-opstartscherm**

Bij het opstarten wordt de update van de virushandtekeningen automatisch uitgevoerd. Dit kan even duren.

Wanneer het opstartproces is voltooid, ziet u het volgende bureaublad. U kunt nu starten met het gebruik van de BitDefender reddingsschijf.

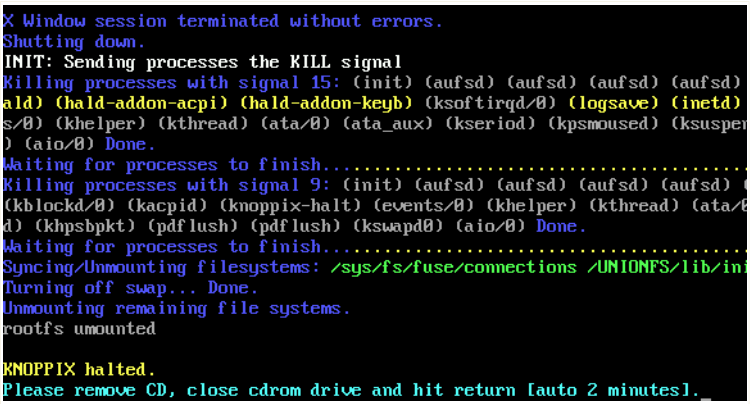
Het bureaublad

## 12.2. BitDefender reddingsschijf stoppen

Daarna kunt u de computer veilig afsluiten door **Afsluiten** te selecteren in het snelmenu van de BitDefender reddingsschijf (klikken met de rechtermuisknop om het te openen) of door de opdracht **stoppen** te selecteren op een werkstation.


Kies "AFSLUITEN"

Wanneer de BitDefender reddingsschijf alle programma's met succes heeft afgesloten, wordt een scherm weergegeven zoals in de volgende afbeelding. U kunt de cd verwijderen om opnieuw op te starten vanaf uw harde schijf. U kunt nu uw computer veilig uitschakelen of opnieuw opstarten.




**Wacht op dit bericht wanneer u afsluit.**

# 12.3. Hoe kan ik een antivirusscan uitvoeren?

Nadat het opstartproces is voltooid, verschijnt een wizard waarmee u een volledige scan van uw computer kunt uitvoeren. Hiervoor hoeft u alleen op de knop **Start** te klikken.

*Opmerking*
Als uw schermresolutie niet hoog genoeg is, wordt u gevraagd het scannen te starten in de tekstmodus.

Volg de begeleide procedure van drie stappen om het scanproces te voltooien.

1. U kunt de scanstatus en de statistieken zien (scansnelheid, verstreken tijd, aantal gescande/geïnfecteerde/verdachte/verborgen objecten en andere).

   *Opmerking*
   Afhankelijk van de complexiteit van de scan, kan het scanproces enige tijd in beslag nemen.

2. U kunt het aantal problemen dat uw systeem beïnvloedt, zien.

   De problemen worden weergegeven in groepen. Klik op het vakje "+" om een groep te openen of op het vakje "-" om een groep te sluiten.

U kunt een algemene actie selecteren die moet worden genomen voor elke groep problemen of u kunt afzonderlijke acties voor elk probleem selecteren.
3. U kunt een samenvatting van de resultaten zien.

Als u slechts één bepaalde map wilt scannen, gaat u als volgt te werk:

Blader door uw mappen, klik met de rechtermuisknop op een bestand of map en selecteer **Verzenden naar**. Kies vervolgens **BitDefender Scanner**.

U kunt ook de volgende opdracht als hoofdmap opgeven vanaf een terminal. De **BitDefender Antivirusscanner** zal starten met het geselecteerde bestand of de map als de standaardlocatie voor het scannen.

```
# bdscan /path/to/scan/
```

## 12.4. Hoe kan ik BitDefender updaten over een proxy?

Als er een proxy server is tussen uw computer en het Internet, moeten een paar configuraties worden uitgevoerd om de virussignaturen te kunnen updaten.

Doe het volgende BitDefender om te updaten over een proxy:

1. Rechtsklik op het Bureaublad. Het BitDefender reddingsschijf contextmenu verschijnt.
2. Selecteer **Werkstation (als root)**.
3. Typ het commando: **cd /ramdisk/BitDefender-scanner/etc**.
4. Typ het commando: **mcedit bdscan.conf** om dit bestand te wijzigen met behulp van GNU Midnight Commander (mc).
5. Verwijder de toelichting van de volgende regel: `#HttpProxy =` (verwijder alleen het `#` teken) en geef het domein, gebruikersnaam, wachtwoord en serverpoort van de proxy server aan. De betreffende regel kan er, bijvoorbeeld, als volgt uitzien:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Druk op **F2** om het actuele bestand op te slaan, bevestig het opslaan, en druk dan op **F10** om het te sluiten.
7. Typ het commando: **bdscan update**.

# 12.5. Hoe kan ik mijn gegevens opslaan?

Laten we veronderstellen dat u uw Windows-pc door enkele onbekende problemen niet meer kunt opstarten. U moet echter tegelijkertijd absoluut toegang krijgen tot enkele belangrijke gegevens op uw computer. Dit is het ogenblik waarop de BitDefender reddingsschijf in actie komt.

Volg deze stappen om gegevens van de computer op te slaan naar een verwisselbaar apparaat, zoals een USB-geheugenstick:

1. Plaats de BitDefender reddingsschijf in het cd-romstation. Stop de geheugenstick in het USB-station en start de computer opnieuw op.
2. Wacht tot de BitDefender reddingsschijf volledig is opgestart. Het volgende venster wordt geopend.

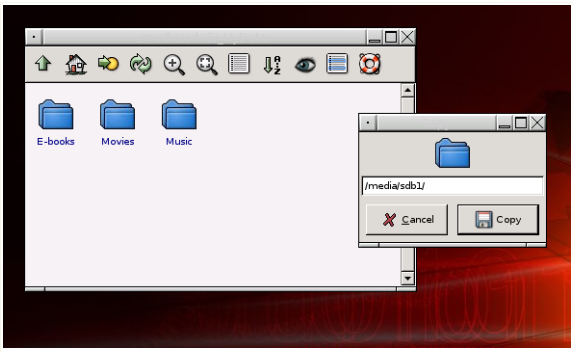
**Bureaubladscherm**

3. Dubbelklik op de partitie die de gegevens die u wilt opslaan, bevat (bijv. `[sda3]`).

> ***Opmerking***
> Wanneer u met de BitDefender reddingsschijf werkt, zult u te maken hebben met partitienamen van het Linux-type. Zo zal `[sda1]` waarschijnlijk overeenkomen met de `(C:)`-partitie van het Windows-type, `[sda3]` met `(F:)` en `[sdb1]` met de geheugenstick.

4. Blader door uw mappen en open de gewenste map. Bijvoorbeeld: `Mijn gegevens` dat de submappen `Films`, `Muziek` en `E-boeken` bevat.

5. Klik met de rechtermuisknop op de gewenste map en selecteer **Kopiëren**. Het volgende venster wordt geopend.




**Gegevens opslaan**

6. Voer `/media/sdb1/` in het overeenkomende tekstvak in en klik op **Kopiëren**.

# Hulp vragen

# 13. Ondersteuning

Als gewaardeerd provider streeft BitDefender ernaar zijn klanten een ongeëvenaard niveau van snelle en nauwkeurige ondersteuning te bieden. Het Ondersteuningscentrum (dat u kunt bereiken op de onderstaande adressen) houdt voortdurend de laatste bedreigingen bij. Hier worden al uw vragen zo snel mogelijk beantwoord.

Bij BitDefender is het onze absolute prioriteit wij onze klant te helpen tijd en geld te besparen, door hem de meest geavanceerde producten te bieden voor de eerlijkste prijs. Bovendien zijn wij ervan overtuigd dat een succesvol bedrijf gebaseerd is om goede communicatie en een inzet voor uitmuntendheid in klantenondersteuning.

U kunt op elk ogenblik hulp vragen op support@bitdefender.com. Voor een snel antwoord raden wij u aan zoveel mogelijk details over BitDefender en uw systeem te vermelden in uw e-mail en het probleem waarmee u te kampen hebt zo nauwkeurig mogelijk te omschrijven.

## 13.1. BitDefender Knowledge Base

De BitDefender Knowledge Base is een online opslagplaats van informatie over BitDefender-producten. Hier worden rapporten bijgehouden in een gemakkelijk toegankelijk formaat over de doorlopende technische ondersteuning en activiteiten voor foutoplossingen van de ondersteunings- en ontwikkelingsteams van BitDefender. Daarnaast vindt u hier ook meer algemene artikels over viruspreventie, het beheer van BitDefender-oplossingen met gedetailleerde uitleg en talrijke andere artikels.

De BitDefender Knowledge Base is toegankelijk voor het publiek en kan vrij worden doorzocht. De uitgebreide informatie die de database bevat is nog een middel om BitDefender-klanten de technische kennis en het inzicht te bieden die ze nodig hebben. Alle geldige aanvragen voor informatie of foutrapporten die van BitDefender-klanten komen, vinden uiteindelijk hun weg naar de BitDefender Knowledge Base als rapporten over het oplossen van problemen, "spiekbriefjes" om een probleem te omzeilen of informatieve artikels om de helpbestanden van het product aan te vullen.

De BitDefender Knowledge Base is altijd beschikbaar op http://kb.bitdefender.com.

## 13.2. Hulp vragen

### 13.2.1. Ga naar Web-selfservice

Hebt u vragen? Onze beveiligingsexperts staan 24/7 gratis tot uw dienst via telefoon, e-mail of chat.

Volg de onderstaande koppelingen:

#### Engels

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

#### Duits

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

#### Frans

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

#### Roemeens

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

#### Spaans

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

### 13.2.2. Een ondersteuningsticket openen

Als u een ondersteuningsticket wilt openen en hulp via e-mail wilt ontvangen, volgt u een van deze koppelingen:

Engels: http://www.bitdefender.com/site/Main/contact/1/
Duits: http://www.bitdefender.de/site/Main/contact/1/
Frans: http://www.bitdefender.fr/site/Main/contact/1/
Roemeens: http://www.bitdefender.ro/site/Main/contact/1/
Spaans: http://www.bitdefender.es/site/Main/contact/1/

## 13.3. Contactinformatie

Efficiënte communicatie is de sleutel naar het succes. Gedurende de laatste 10 jaar heeft BITDEFENDER een onberispelijke reputatie opgebouwd door voortdurend te streven naar een betere communicatie om de verwachtingen van onze klanten en partners steeds opnieuw te overtreffen. Aarzel niet contact op te nemen met ons als u eventuele vragen hebt.

### 13.3.1. Webadressen

Verkoopsafdeling: sales@bitdefender.com
Technische ondersteuning support@bitdefender.com
Documentatie: documentation@bitdefender.com
Partnerprogramma: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Perscontact: pr@bitdefender.com
Carrièremogelijkheden: jobs@bitdefender.com
Virusverzendingen: virus_submission@bitdefender.com
Spamverzendingen: spam_submission@bitdefender.com
Misbruikmeldingen: abuse@bitdefender.com
Website product: http://www.bitdefender.com
FTP-archieven product: ftp://ftp.bitdefender.com/pub
Lokale verdelers: http://www.bitdefender.com/partner_list
BitDefender Knowledge Base: http://kb.bitdefender.com

### 13.3.2. Bijkantoren

De BitDefender-kantoren zijn altijd paraat om te reageren op aanvragen met betrekking tot hun bedrijfsgebied, zowel op commercieel als algemeen vlak. Hun respectievelijke adressen en contactpersonen worden hieronder weergegeven:

#### V.S.A.

**BitDefender, LLC**
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Technische ondersteuning

- E-mail: support@bitdefender.com

- Telefoon:
  - 1-888-868-1873 (alleen geregistreerde gebruikers; alleen bereikbaar in de Verenigde Staten)
  - 1-954-776-6262 (alleen geregistreerde gebruikers)

Klantenservice:

- E-mail: customerservice@bitdefender.com
- Telefoon:
  - 1-888-868-1873 (alleen geregistreerde gebruikers; alleen bereikbaar in de Verenigde Staten)
  - 1-954-776-6262 (alleen geregistreerde gebruikers)

## Duitsland

**BitDefender GmbH**
Hoofdkantoor West-Europa
Karlsdorferstrasse 56
88069 Tettnang
Duitsland
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
E-mail: info@bitdefender.com
Verkoop: sales@bitdefender.com
Web: http://www.bitdefender.com
Technische ondersteuning: support@bitdefender.com

## UK en Ierland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 845 130 5096
Fax: +44 845 130 5069
E-mail: info@bitdefender.com
Verkoop: sales@bitdefender.com
Web: http://www.bitdefender.co.uk
Technische ondersteuning support@bitdefender.com

## Spanje

**Constelacion Negocial, S.L**
C/ Balmes 195, 2a planta, 08006
Barcelona
Technische ondersteuning: soporte@bitdefender-es.com
Verkoop: comercial@bitdefender-es.com
Telefoon: +34 932189615
Fax: +34 932179128
Website product: http://www.bitdefender-es.com

## Roemenië

**BITDEFENDER**
5th Fabrica de Glucoza St.
Boekarest
Technische ondersteuning support@bitdefender.com
Verkoop: sales@bitdefender.com
Telefoon: +40 21 4085600
Fax:
Website product: http://www.bitdefender.com

# Woordenlijst

**ActiveX**

ActiveX is een model voor het schrijven van programma's zodat andere programma's en het besturingssysteem ze kunnen oproepen. De ActiveX-technologie wordt gebruikt bij Microsoft Internet Explorer om interactieve Webpagina's te maken die eruitzien en zich gedragen als computerprogramma's in plaats van statische pagina's. Met ActiveX kunnen gebruikers vragen stellen of beantwoorden, drukknoppen gebruiken en op andere manieren interactief omgaan met de Webpagina. ActiveX-besturingselementen zijn vaak geschreven met de hulp van Visual Basic.

ActiveX is bekend voor een compleet tekort aan beveiligingscontroles; experts op het vlak van computerbeveiliging raden het gebruik ervan via het Internet sterk af.

**Adware**

Adware wordt vaak gecombineerd met een hosttoepassing die gratis wordt aangeboden op voorwaarde dat de gebruiker akkoord gaat met het uitvoeren van de adware. Omdat adware-toepassingen doorgaans worden geïnstalleerd nadat de gebruiker een licentieovereenkomst die het doel van de toepassing vermeldt heeft geaccepteerd, wordt er geen inbreuk gepleegd.

Pop-upadvertenties kunnen echter irritant worden en in sommige gevallen de systeemprestaties negatief beïnvloeden. De gegevens die door sommige van deze toepassingen worden verzameld, kunnen bovendien privacy-problemen veroorzaken voor gebruikers die niet volledig op de hoogte waren van de voorwaarden van de licentieovereenkomst.

**Archief**

Een schijf, tape, of map die bestanden bevat waarvan een back-up werd gemaakt.

Een bestand dat één of meer bestanden bevat in een gecomprimeerd formaat.

**Achterdeur**

Een gat in de beveiliging van een systeem, dat opzettelijk werd achtergelaten door ontwikkelaars of beheerders. De motivatie voor dergelijke gaten is niet altijd boosaardig. Sommige besturingssystemen worden bijvoorbeeld geleverd met bevoegde accounts die bedoeld zijn voor gebruik door technici voor service ter plaatse of onderhoudsprogrammeurs van verkopers.

**Opstartsector**

Een sector aan het begin van elke schijf die de architectuur van de schijf identificeert (sectorgrootte, clustergrootte, enz.) Bij opstartdiskettes bevat de opstartsector ook een programma dat het besturingssysteem laadt.

**Opstartsectorvirus**

Een virus dat de opstartsector van een vaste schijf of een diskette infecteert. Wanneer u probeert op te starten vanaf een diskette die geïnfecteerd is met een opstartsectorvirus, zal het virus actief worden in het geheugen. Wanneer u vanaf dat ogenblik uw systeem opstart, zal het virus telkens in het geheugen geactiveerd zijn.

**Browser**

De korte naam voor Webbrowser, een softwaretoepassing die wordt gebruikt op Webpagina's te zoeken en weer te geven. De twee populairste browsers zijn Netscape Navigator en Microsoft Internet Explorer. Beide zijn grafische browsers. Dit betekent dat ze zowel grafische beelden als tekst kunnen weergeven. Bovendien kunnen de meeste moderne browsers ook multimedia-informatie voorstellen met geluid en video, hoewel voor sommige formaten plug-ins vereist zijn.

**Opdrachtregel**

In een opdrachtregelinterface typt de gebruiker opdrachten in opdrachttaal rechtstreeks op het scherm in de ruimte die hiervoor wordt geboden.

**Cookie**

Binnen de Internetindustrie worden cookies beschreven als kleine programma's die informatie bevatten over individuele computers, die door adverteerders wordt geanalyseerd en gebruikt om uw on line interesse en smaak op te volgen. De cookietechnologie wordt in dit kader nog steeds verder ontwikkeld met het doel reclameberichten rechtstreeks te richten op de interesses die u hebt meegedeeld. Dit is voor veel mensen een mes dat aan twee kanten snijdt. Aan de ene kant is het efficiënt en relevant aangezien u alleen reclames ontvangt voor zaken waarvoor u interesse hebt. Aan de andere kant betekent het ook dat elke plaats die u bezoekt en alles wat u aanklikt wordt "opgespoord" en "gevolgd". Het is dan ook te begrijpen dat er heel wat wordt gedebatteerd over privacy. Bovendien zijn veel mensen verontwaardigd omdat ze het gevoel hebben dat ze als een "SKU-nummer" worden beschouwd (u weet wel, de barcode op de verpakkingen die bij de kassa van het warenhuis wordt gescand). Hoewel dit standpunt misschien nogal extreem is, is het vaak een bijzonder nauwkeurige omschrijving.

**Schijfstation**

Dit is een apparaat dat gegevens leest van en schrijft naar een schijf.

Een harde-schijfstation leest en schrijft harde schijven.

Een diskettestation opent diskettes.

Schijfstations kunnen intern (binnen de behuizing van een computer) of extern zijn (in een afzonderlijke behuizing die op de computer wordt aangesloten).

**Downloaden**

Om gegevens (meestal een volledig bestand) te kopiëren van een hoofdbron naar een randapparaat. De term wordt vaak gebruikt om het proces te beschrijven waarbij een bestand van een on line-service wordt gekopieerd naar de eigen computer. Downloaden kan ook verwijzen naar het kopiëren van een bestand van een netwerkbestandsserver naar een computer in het netwerk.

**E-mail**

Elektronische post. Een dienst die berichten naar computers verzendt via lokale of globale netwerken.

**Gebeurtenissen**

Een actie of gebeurtenis die door een programma wordt gedetecteerd. Gebeurtenissen kunnen gebruikersacties zijn, zoals het klikken met de muis of het indrukken van een toets, of systeemgebeurtenissen, zoals een tekort aan geheugen.

**False positive**

Doet zich voor wanneer een scanner een bestand ten onrechte beschouwt als geïnfecteerd.

**Bestandsextensie**

Het gedeelte van een bestandsnaam na het eindpunt, waarmee het gegevenstype dat in het bestand is opgeslagen wordt aangeduid.

Heel wat besturingssystemen, zoals Unix, VMS en MS-DOS, maken gebruik van bestandsextensies. Ze gebruiken doorgaans één tot drie letters (sommige betreurenswaardige oude besturingssystemen ondersteunen niet meer dan drie letters). Voorbeelden hiervan zijn "c" voor C-broncode, "ps" voor PostScript, "txt" voor tekst zonder opmaak.

**Heuristisch**

Een methode voor het identificeren van nieuwe virussen op basis van regels. Deze scanmethode steunt niet op specifieke virussignatures. Het voordeel van de heuristische scan is dat hij zich niet laat misleiden door een nieuwe variant van een bestaand virus. Dit type kan echter af en toe een verdachte code rapporteren in normale programma's, zodat de zogenoemde "valse positieve" rapporten worden gegenereerd.

**IP**

Internet Protocol - Een routeerbaar protocol in de TCP/OP-protocolreeks die verantwoordelijk is voor de IP-adressering, routing en de fragmentatie en defragmentatie van IP-pakketten.

**Java-applet**

Een Java-programma dat is ontwikkeld om alleen op een webpagina te worden uitgevoerd. Om een applet op een webpagina te gebruiken, zou u de naam van het applet opgeven en de grootte (lengte en breedte in pixels) die het applet kan gebruiken. Wanneer de webpagina wordt geopend, downloadt de browser het applet van een server en voert hij het uit op de computer van de gebruiker (de client). Applets onderscheiden zich van toepassingen omdat ze worden beheerd door een streng beveiligingsprotocol.

Zelfs wanneer applets bijvoorbeeld op de client worden uitgevoerd, kunnen ze geen gegevens lezen van of schrijven naar de computer van de client. Bovendien worden applets verder beperkt zodat ze alleen gegevens kunnen lezen van en schrijven naar hetzelfde domein waarvan ze worden bediend.

**Macrovirus**

Een type computervirus dat is gecodeerd als een macro die in een document is ingesloten. Talrijke toepassingen, zoals Microsoft Word en Excel, ondersteunen krachtige macrotalen.

Met deze toepassingen kunt u een macro in een document insluiten, en die macro telkens laten uitvoeren wanneer het document wordt geopend.

**E-mailclient**

Een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

**Geheugen**

Interne opslaggebieden in de computer. De term geheugen staat voor gegevensopslag die in de vorm van chips wordt geleverd. Het woord opslag wordt gebruikt voor geheugen dat aanwezig is op tapes of schijven. Elke computer wordt geleverd met een bepaalde hoeveelheid fysiek geheugen, dat meestal het hoofdgeheugen of RAM wordt genoemd.

**Niet-heuristisch**

Deze scanmethode steunt op specifieke virussignatures. Het voordeel van de niet-heuristische scan is dat hij zich niet laat misleiden door iets dat kan lijken op een virus en dat hij geen vals alarm genereert.

**Ingepakte programma's**

Een bestand in een gecomprimeerd formaat. Talrijke besturingssystemen en toepassingen beschikken over opdrachten waarmee u bestanden kunt inpakken, zodat ze minder geheugen in beslag nemen. Veronderstel bijvoorbeeld dat u een tekstbestand hebt dat tien opeenvolgende spatietekens bevat. Normaal zou dit tien bytes opslagruimte vereisen.

Een programma dat bestanden inpakt zou echter de spatietekens vervangen door een speciaal spatiereeks-teken, gevolgd door het aantal spaties dat wordt vervangen. In dit geval zouden de tien spaties slechts twee bytes nodig hebben. Dit is slechts één inpaktechniek, maar er zijn er veel meer.

**Pad**

De exacte weg naar een bestand op een computer. Deze weg wordt doorgaans beschreven door middel van het hiërarchische archiveringssysteem vanaf het begin.

De route tussen twee willekeurige punten, zoals het communicatiekanaal tussen twee computers.

**Phishing**

Het onder valse voorwendselen verzenden van een e-mail aan een gebruiker, waarbij de indruk wordt gewekt dat het bericht afkomstig is van een bestaande onderneming, in een poging de gebruiker persoonlijke gegevens te ontfutselen die zullen worden gebruikt voor identiteitsroof. In het e-mailbericht wordt de gebruiker doorverwezen naar een website waar persoonlijke gegevens kunnen worden bijgewerkt, zoals wachtwoorden en creditcard-, sofi- en bankrekeningnummers, die reeds in het bezit zijn van de rechtmatige organisatie. De website is echter nep en alleen opgezet om de gebruikersgegevens te stelen.

**Polymorf virus**

Een virus dat zijn vorm wijzigt bij elk bestand dat hij infecteert. Aangezien ze geen consequent binair patroon hebben, zijn dergelijke virussen moeilijk te identificeren.

**Poort**

Een interface op een computer waarop u een apparaat kunt aansluiten. PC's hebben verschillende types poorten. Intern zijn er verschillende poorten voorzien voor het aansluiten van schijfstations, beeldschermen en toetsenborden. Extern beschikken PC's over poorten voor het aansluiten van modems, printers, muizen en andere randapparatuur.

Bij TCP/IP- en UDP-netwerken, zijn ze een eindpunt voor een logische verbinding. Het poortnummer duidt aan over welk type poort het gaat. Poort 80 wordt bijvoorbeeld gebruikt voor HTTP-verkeer.

**Rapportbestand**

Een bestand dat de acties weergeeft die zich hebben voorgedaan. BitDefender houdt een rapportbestand bij met het gescande pad, het aantal gescande mappen, archieven en bestanden, en het aantal gevonden geïnfecteerde en verdachte bestanden.

**Rootkit**

Een rootkit is een set softwarehulpprogramma's die toegang biedt tot een systeem op beheerniveau. Deze term werd voor het eerst gebruikt voor UNIX-besturingssystemen en verwees naar opnieuw gecompileerde hulpprogramma's die indringers beheerrechten verleende, zodat ze hun aanwezigheid konden verbergen zodat ze onzichtbaar bleven voor systeembeheerders.

De belangrijkste rol van rootkits is het verbergen van processen, bestanden, aanmeldingen en logboeken. Ze kunnen ook gegevens onderscheppen van terminals, netwerkverbindingen of randapparaten als ze de geschikte software bevatten.

Rootkits zijn in wezen niet kwaadaardig. Systemen en zelfs sommige toepassingen verbergen kritieke bestanden met de hulp van rootkits. Ze worden echter het vaakst gebruikt om malware of de aanwezigheid van een indringer op het systeem te verbergen. In combinatie met malware, vormen rootkits een ernstige bedreiging voor de integriteit en beveiliging van een systeem. Ze kunnen het verkeer controleren, achterpoortjes in het systeem maken, bestanden en logboeken wijzigen en detectie vermijden.

**Script**

Script, een andere term voor een macro of batchbestand, is een lijst opdrachten die kunnen worden uitgevoerd zonder tussenkomst van de gebruiker.

**Spam**

Elektronische junkmail of berichten van junknieuwsgroepen. Algemeen bekend als ongewenste e-mail.

**Spyware**

Elke software die heimelijk gebruikersgegevens verzamelt via de internetverbinding van de gebruikers zonder dat hij/zij zich hiervan bewust is, doorgaans voor reclamedoeleinden. Spywaretoepassingen worden doorgaans gebundeld als een verborgen onderdeel van freeware- of sharewareprogramma's die kunnen worden gedownload van het internet. We moeten echter wel vermelden dat de meeste shareware- en freewaretoepassingen geen spyware bevatten. Zodra de spyware is geïnstalleerd, worden de activiteiten van de gebruiker op het Internet gevolgd en wordt deze informatie op de achtergrond naar iemand anders doorgestuurd.

Spyware kan ook informatie verzamelen over e-mailadressen en zelfs wachtwoorden en creditcardnummers.

Spyware is vergelijkbaar met een Trojaans paard omdat gebruikers ook in dit geval het product onbewust installeren wanneer ze een ander programma installeren. Een veel voorkomende manier om slachtoffer te worden van spyware is bepaalde P2P-bestandsuitwisselingsprogramma's te downloaden.

Naast het feit dat deze methode onethisch is en een inbreuk op de privacy van de gebruiker betekent, steelt spyware van de gebruiker door de geheugenbronnen van de computer te gebruiken en bandbreedte te verbruiken wanneer de informatie naar de thuisbasis van de spyware wordt verzonden via de internetverbinding van de gebruiker. Aangezien spyware geheugen- en systeembronnen gebruikt, kunnen de toepassingen die op de achtergrond worden uitgevoerd leiden tot systeemfouten of een algemene systeeminstabiliteit.

**Opstartitems**

Elk bestand in deze map wordt geopend wanneer de computer wordt gestart. Een opstartitem kan bijvoorbeeld een opstartscherm zijn, een geluidsbestand dat moet worden afgespeeld wanneer de computer voor de eerste maal opstart, een herinneringsagenda of een toepassingsprogramma. In normale omstandigheden wordt een alias van een bestand in deze map geplaatst, en niet het bestand zelf.

**Systeemvak**

Het systeemvak, dat met Windows 95 werd ingevoerd, bevindt zich in de taakbalk van Windows (doorgaans onderaan naast de klok) en bevat miniatuurpictogrammen die systeemfuncties zoals fax, printer, modem, volume en meer, gemakkelijk toegankelijk maken. Dubbelklik of klik met de rechtermuisknop op een pictogram om de details en de besturingselementen te bekijken en te openen.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - Een reeks netwerkprotocollen, wijdverspreid gebruikt op het Internet, die communicatie bieden tussen onderling verbonden computernetwerken met verschillende hardware-architecturen en diverse besturingssystemen. TCP/IP bevat standaarden voor de manier waarop computers communiceren en regels voor het aansluiten van netwerken en het routeren van het verkeer.

**Trojaans paard**

Een destructief programma dat zich voordoet als een goedaardige toepassing. In tegenstelling tot virussen, maken ze geen kopie van zichzelf, maar ze kunnen wel even vernietigend zijn. Een van de meest verraderlijke types van de Trojaanse

paarden is een programma dat beweert dat het uw computer kan bevrijden van virussen, maar dat in werkelijkheid virussen op uw computer installeert.

De term komt uit een verhaal uit de Illias van Homerus, dat vertelt over de Grieken die hun vijanden, de Trojanen een reusachtig houten paard schonken, zogenaamd als een vredesgebaar. Maar nadat de Trojanen het paard binnen de stadsmuren hadden gesleept, kwamen de Griekse soldaten, die in de holle romp van het paard verborgen zaten te voorschijn en openden ze de poorten van de stad, zodat hun landgenoten Troje konden binnendringen en veroveren.

**Update**

Een nieuwe versie van een software- of hardwareproduct, dat werd ontwikkeld om een oudere versie van hetzelfde product te vervangen. Daarnaast zullen de installatieroutines voor updates vaak controleren of er reeds een oudere versie van het product op uw computer is geïnstalleerd. Is dat niet het geval, dan kunt u de update niet installeren.

BitDefender heeft zijn eigen updatemodule waarmee u handmatig kunt controleren op updates of die het product automatisch kan updaten.

**Virus**

Een programma of een deel van een code die op uw computer wordt geladen zonder uw medeweten en tegen uw wil wordt uitgevoerd. De meeste virussen kunnen zichzelf ook dupliceren. Alle computervirussen zijn door de mens gemaakt. Een eenvoudig virus dat zichzelf steeds opnieuw kan dupliceren is relatief eenvoudig te maken. Zelfs een dergelijke eenvoudig virus is gevaarlijk aangezien het snel al het beschikbare geheugen zal opgebruiken en het systeem zal blokkeren; Een nog gevaarlijker type is een virus dat in staat is zichzelf te verzenden via netwerken en beveiligingssystemen te omzeilen.

**Virusdefinitie**

Het binaire patroon van een virus, dat wordt gebruikt door het antivirusprogramma om het virus te detecteren en uit te schakelen.

**Worm**

Een programma dat zich verspreidt via een netwerk en zichzelf ondertussen reproduceert. Dit type kan zich niet vasthechten aan andere programma's.