Ewido Security Suite

1. Wat

Ewido SS is een goede **gratis Malware Scanner, Cleaner en Remover** voor Trojans, Worms, Dialers, Hijackers, Spyware en Keyloggers. Een goede aanvulling dus op de traditionele anti-virus software, die vaak voor deze vormen van malware niet veel in huis heeft of ze gewoonweg niet detecteert of kan verwijderen.
Hier kan je een lijst met beveiligingsprogjes vinden, om te controleren of je eigen beveiligingsoftware wel goed combineerbaar is met Ewido: compatibiliteits-lijst

Ewido is beschikbaar in **2 versies**, een Plus-versie (29,95 €) en een freeware-versie (waarbij je voor 14 dagen ook over alle mogelijkheden van de volledige betalende versie beschikt, als "trail". Na deze 14 dagen worden de "plugins" van de Plus-versie gedeactiveerd en kan je ze dus niet meer verder gebruiken).
De eigenlijke trojanscanner, -cleaner, -remover behoort bij de freeware en blijft dus oneindig bruikbaar en werkzaam.

Citaat:

> Enkele functies van het **Freeware-progje**:
> - Zelf te starten malware scanner, cleaner, remover met quarantaine mogelijkheid.
> - Zelf te starten update van de malware database / definities beschikbaar (via "intelligent" online-update)
> - Analyse- tooltjes (opstart-items, verbindingen en processen)
> - Quarantaine
>
> Enkele bijkomende functies van de **Plus-versie** (14dagen trial)
> - Realtime bescherming (= de guard / bewaker)
> - Memory Scan voor actieve bedreigingen
> - Scannen van de archieven / archief-bestanden
> - Automatische online-update
> - ...

Je kunt naar pagina 3 gaan, indien je het programma al geïnstalleerd hebt.

2. Downloadgegevens

Citaat:

> Homepage: http://www.ewido.net
> Downloadpagina: http://www.ewido.net/en/download/
> of: Directe download : http://download.ewido.net/ewido-setup.exe
>
> Besturingssysteem: Windows **2000** en **XP** (NIET voor oudere Windows-versies)
> Bestandsgrootte: ca. 2,2 Mb
> Versie: 3.5
> Talen: Engels, Duits, Franks, Italiaans, Japans, **Nederlands**, Portugees

Kies bij de download voor "Opslaan" en sla op naar een voor jou gemakkelijk terug te vinden locatie, bv. het bureaublad.

De download omvat de gratis versie met alle (trial) plugins van de "plus" versie van Ewido Security Suite.
Na installatie kan je de plugins van de Plus-versie 14 dagen gratis uitproberen, daarna worden deze gedeactiveerd. De freeware versie zelf blijft verder gratis werken.

3. Installatie

Citaat:

- Open na download het setup-bestand "**ewido-setup.exe**"
- Afhankelijk van je beveiligingsinstellingen krijg je mogelijk eerst nog een melding "Bestand openen - Beveiligingswaarschuwing", kies daarbij voor "**Uitvoeren**"
- Selecteer de **taal** die tijdens de installatie gebruikt moet worden. Standaard is dit op Duits, maar je kunt ook voor Engels kiezen.
- In het volgende venstertje wordt nog even ingegaan op de tijdelijke "**Plus**"-plugins van de betalende versie die je voor 14 dagen gratis mee kan gebruiken als trial. Na deze proefperiode worden de extra-plugins inactief.
  Verder wordt aanbevolen om tijdens de setup van Ewido, alle andere open toepassingen even te sluiten. Klik "Next"
- **Licentie-overeenkomst**. Neem deze even door en klik "I Agree" als je akkoord bent, om verder te gaan.
- Volgend venster gaat over de **locatie** waar Ewido geinstalleerd gaat worden, standaard is dit "C:\Program Files\ewido security suite". Dmv. de knop "browse" kan je deze locatie eventueel veranderen. Klik "Next".
- Hier kan je de naam van de map die voor Ewido in het **startmenu** (standaard "ewido") gezet gaat worden, eventueel aanpassen. Klik "Next"
- Bij het volgende schermpje kan je **extra opties** kiezen die mee geïnstalleerd zullen worden, nl.:
  - Install background guard : de installatie van de "real-time" beschermer die meteen op het moment zelf dat er iets verdachts aan de hand is, een melding geeft en ingrijpt.
  - install scan via context menu : hiermee kan je een verdacht bestand scannen via het "context menu" (rechtermuisklik op het bestand), zie verder bij "Het hoofdprogramma - scanner"

  Standaard staan beide aangevinkt(Trial versie). Indien je nu al weet dat je het bij de Free versie te zullen houden dan mag je die vinkjes verwijderen. Maak je keuze en klik "**Install**"
- Als de installatie "**completed**" is, klik je bij het volgende venstertje op "finish".
  .

Het wordt aangeraden om na de installatie, je pc opnieuw op te starten.

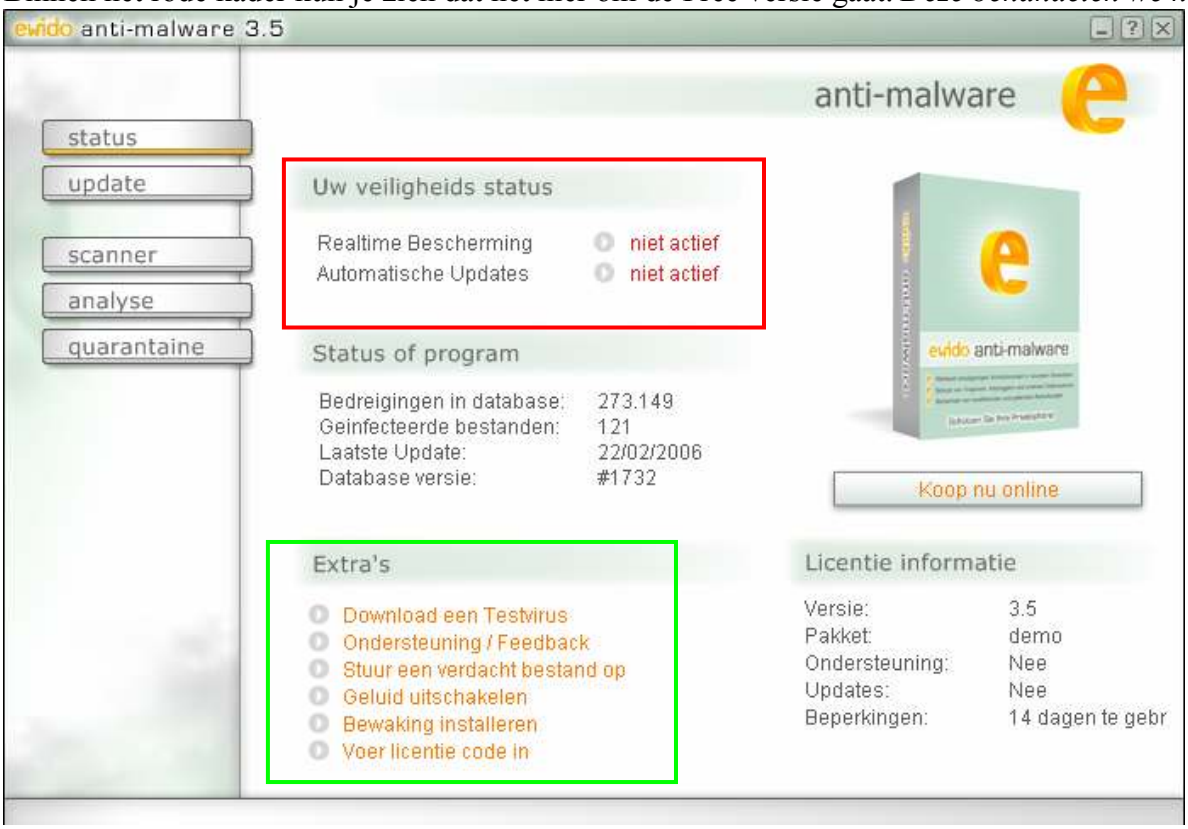
4. Gebruik en Configuratie

Na de heropstart (of na even te wachten) gebeurt er een **update** / installatie van de updates van de Ewido malware-definities. Het is belangrijk dat je deze updates eerst toestaat alvorens te scannen, want het progje bevat vlak na installaties niets aan updates. Indien je het als Free version hebt geïnstalleerd dan zal het Updaten niet automatisch uitgevoerd worden. Doe het dan handmatig (Zie volgende pagina).

Indien je tijdens de installatie voor de Plus-versie (Trial) hebt gekozen, dan zie je dat er intussen een icoontje in de systray-balk (naast de klok) en een snelkoppeling op je bureaublad bijgekomen is.
Via rechtermuisklik op het **ewido-icoontje** (van de guard) in de systray-balk, krijg je ook de mogelijkheid om de Guard en / of de Automatische Updates uit te schakelen.
Opgelet: Niet bij de Free versie.

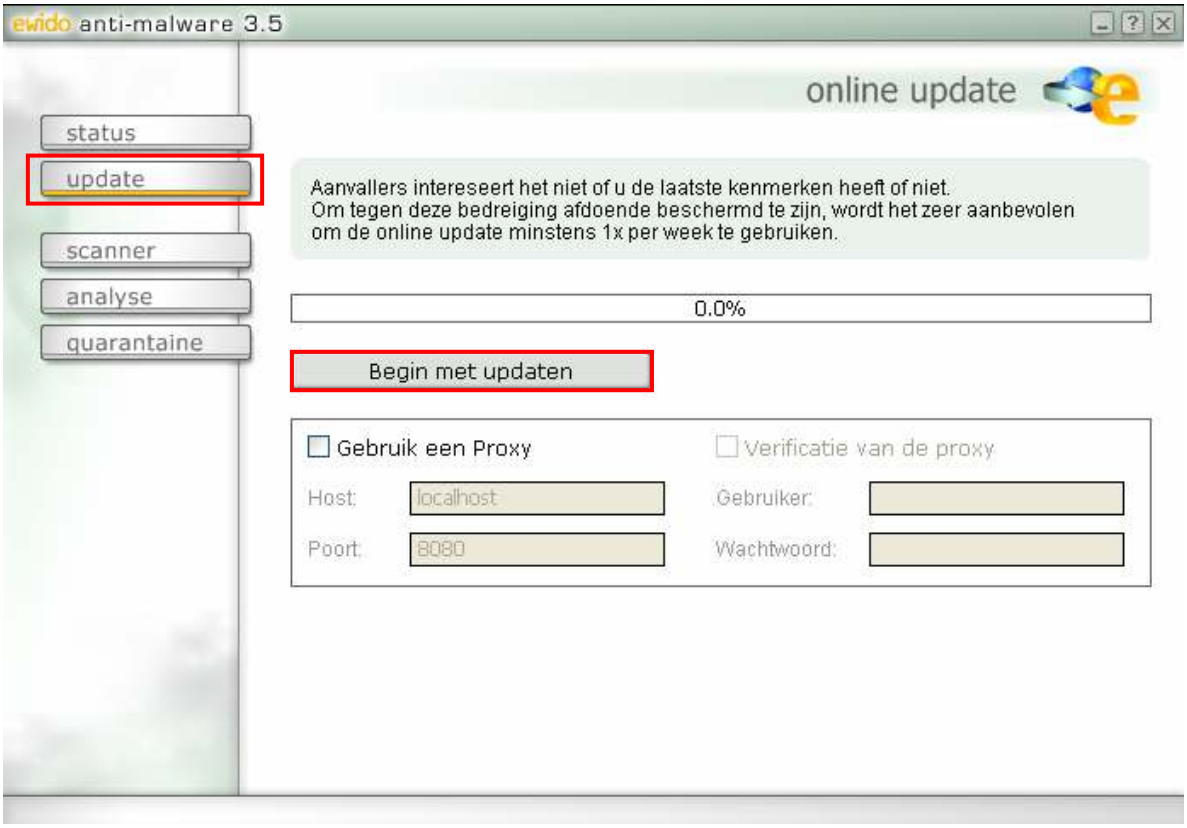
Een dubbele klik op de **snelkoppeling** van Ewido op het bureaublad opent het statusvenster "**anti-malware**". Dit kan je ook tevoorschijn halen via rechtermuisklik op het systray-icoontje of via Start --> Alle programma's --> ewido --> security suite

Binnen het rode kader kun je zien dat het hier om de Free versie gaat. *Deze behandelen we nu.*

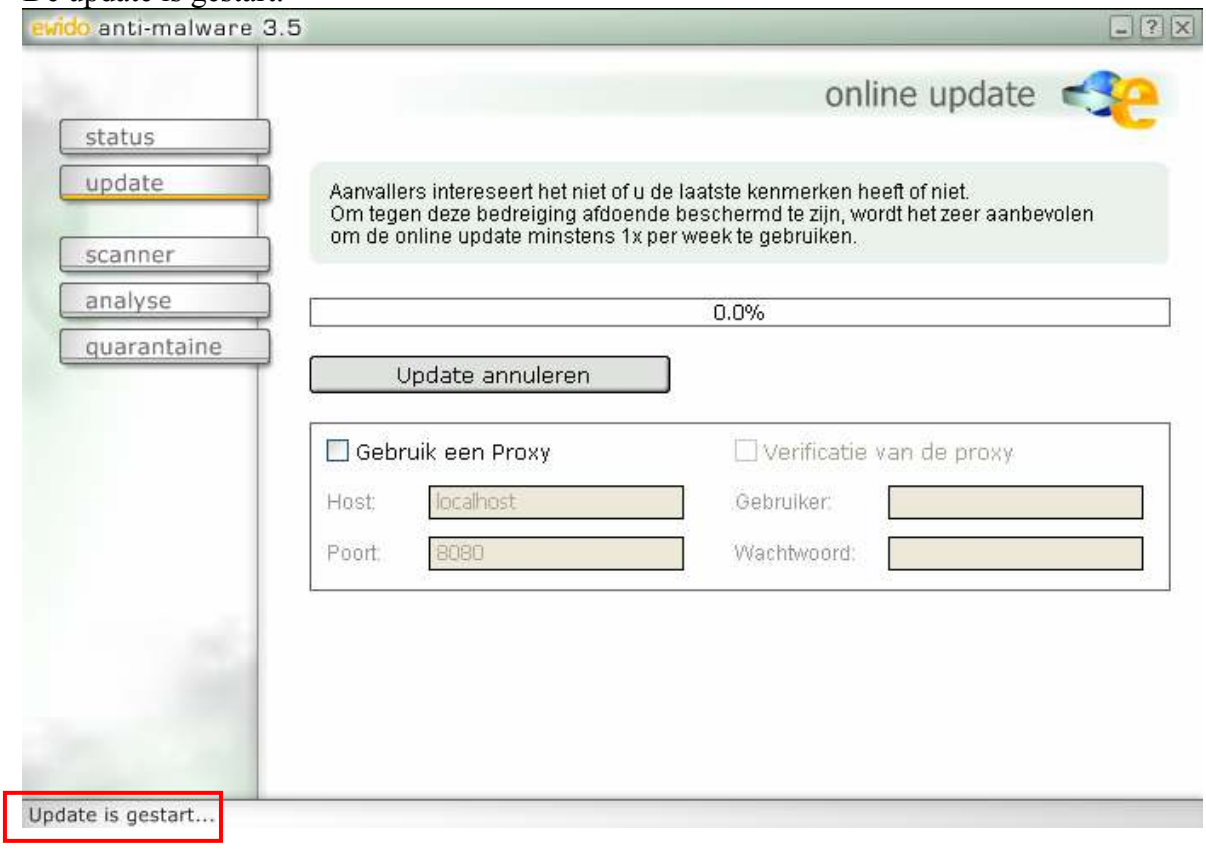


Binnen het groene kader bevinden zich nog een aantal Extra's. Zo kun je ondermeer een bestand dat je zelf verdacht vindt opsturen voor onderzoek.

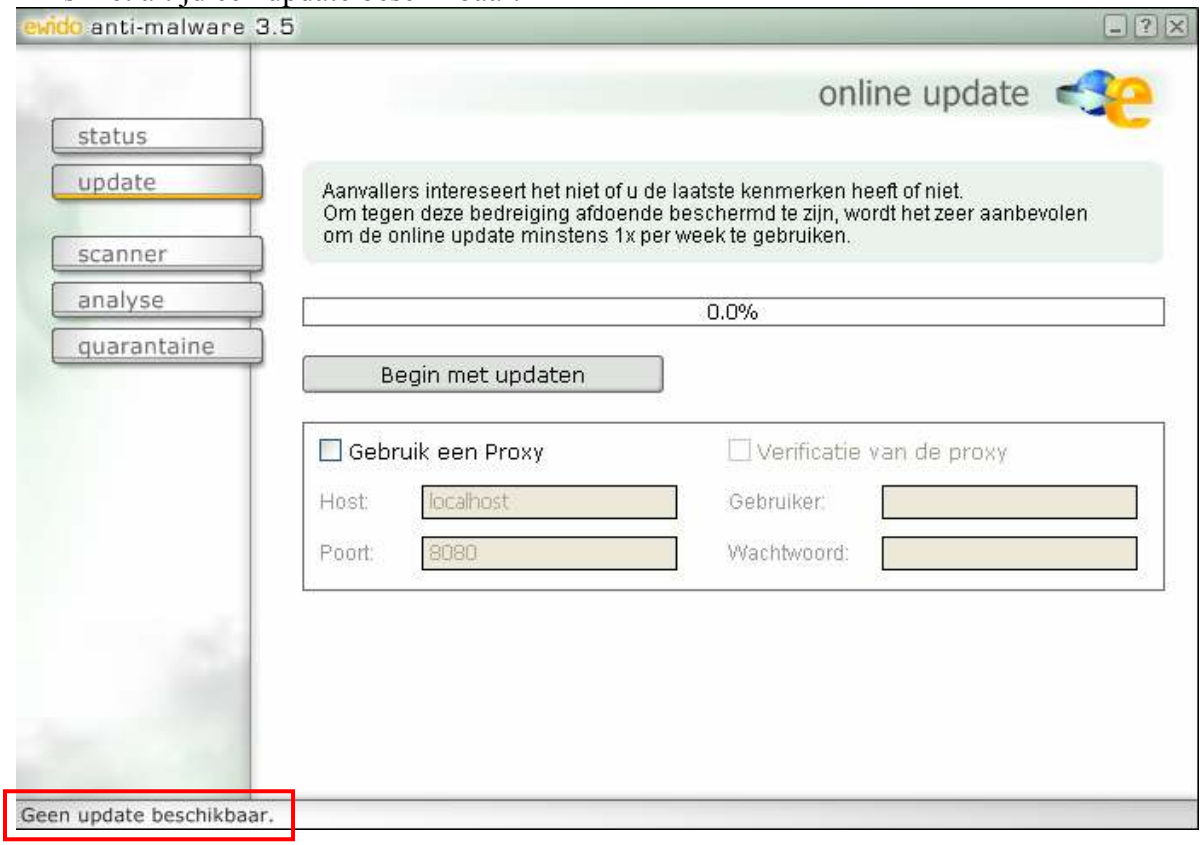
Klik op **update** en vervolgens op **Begin met updaten.**
Zolang de trial van de Plus-versie geldt, gebeurt de **Online-**update automatisch, daarna is het geregeld zelf controleren via dit menu, of er een update is. Haal de updates altijd op vóór je met ewido scant.



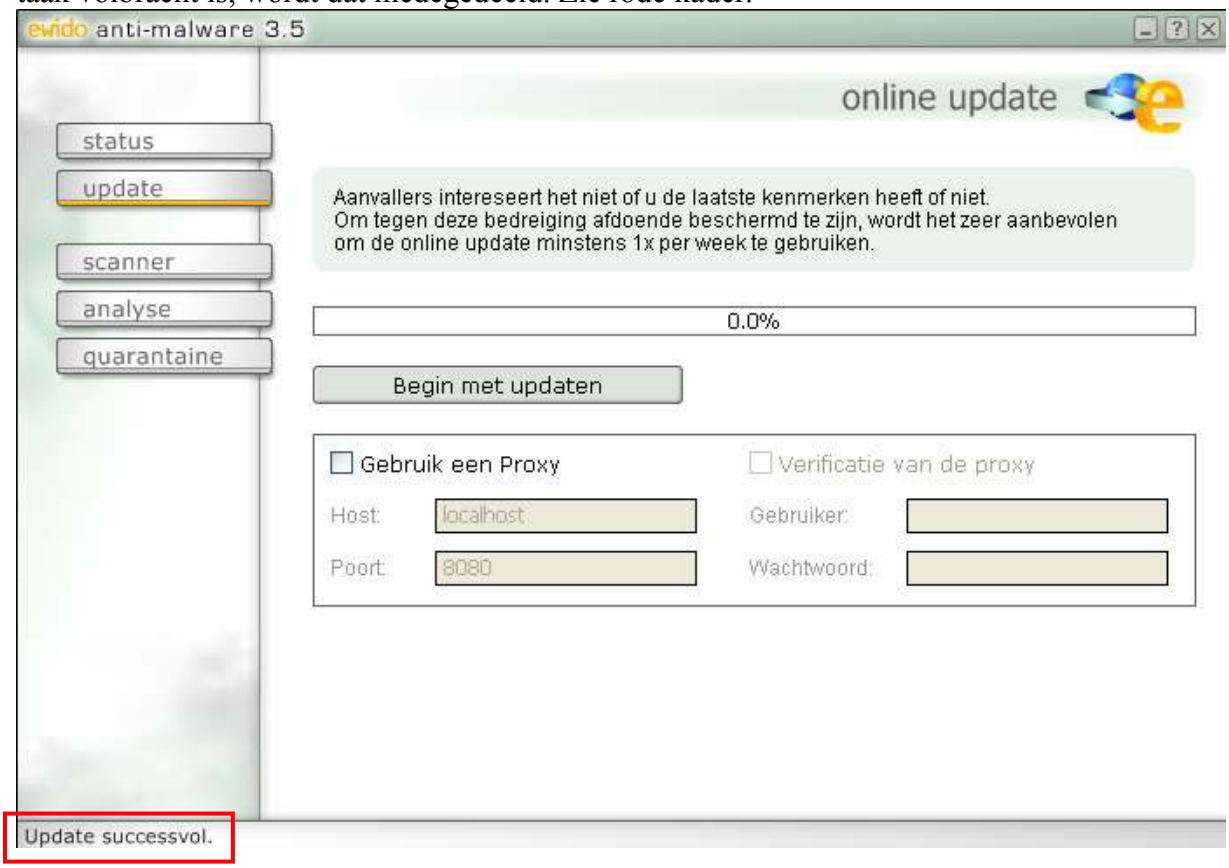
De update is gestart.



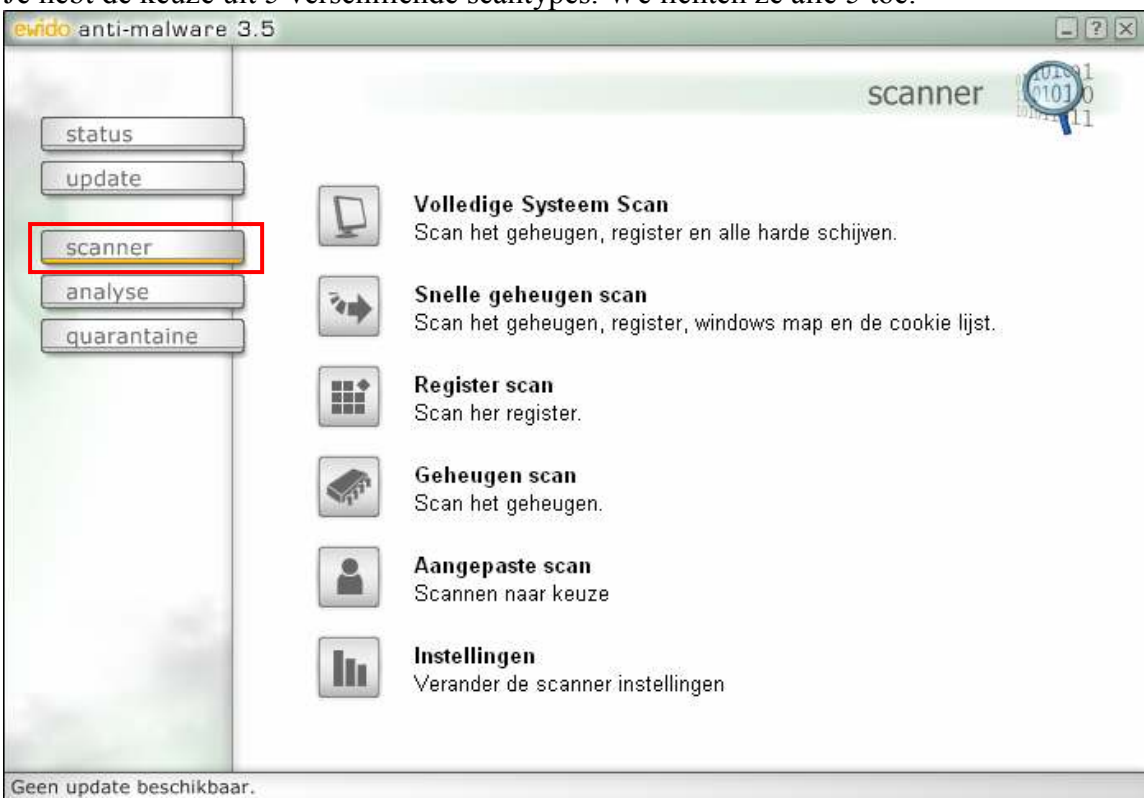
Er is niet altijd een update beschikbaar.



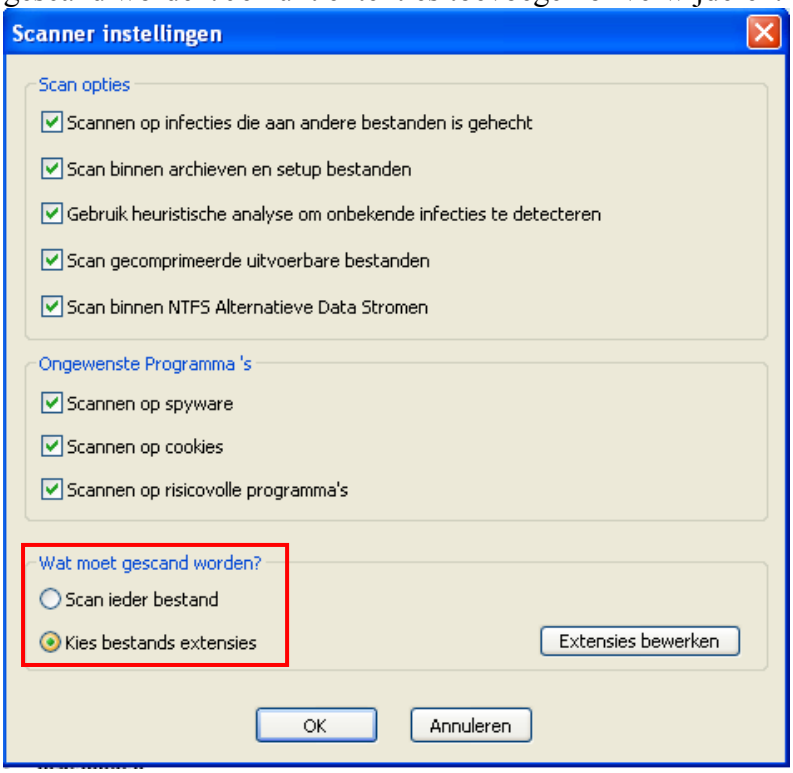
Indien er een update beschikbaar is dan wordt die gedownload en geïnstalleerd. Zodra deze taak volbracht is, wordt dat medegedeeld. Zie rode kader.



Nadat je op **scanner** hebt geklikt krijg je onderstaand keuzevenster.
Je hebt de keuze uit 5 verschillende scantypes. We lichten ze alle 5 toe.

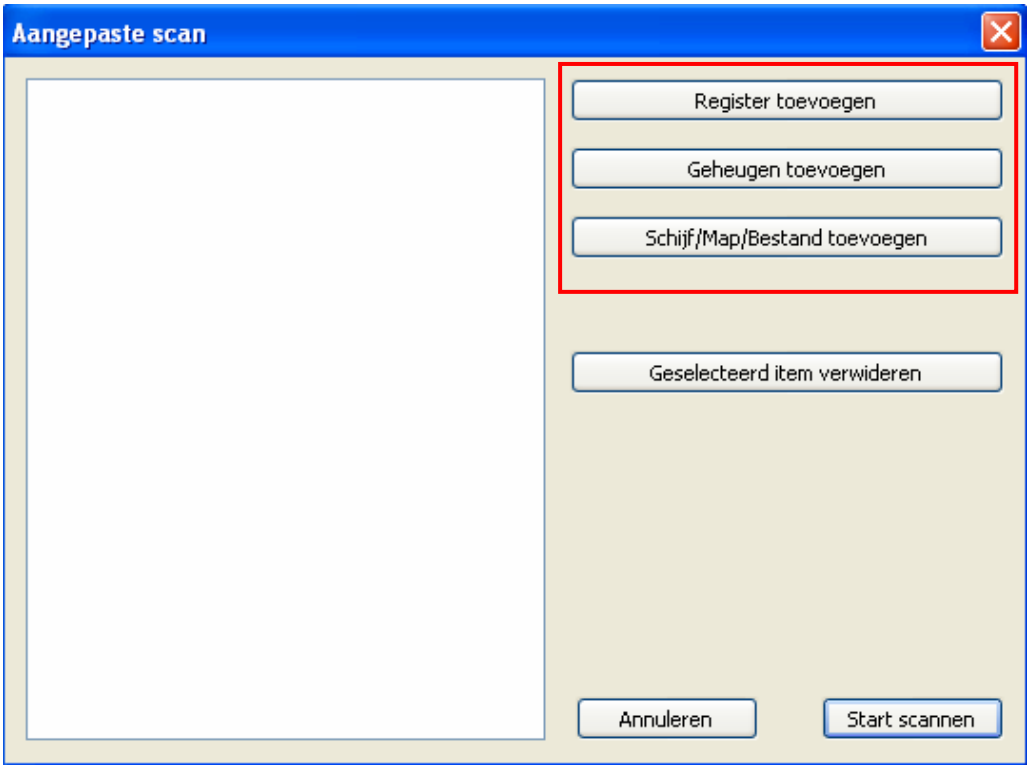


Laten we echter beginnen bij de **Instellingen**. Onderstaand venster geeft de standaard instellingen weer. Je kunt er ondermeer voor kiezen (zie rode kader) om ieder bestand te scannen of om enkel bestanden met een bepaalde (risicovolle) extentie. Via de knop **Extenties bewerken** wordt een standaard lijst met extenties getoond waarvan de bestanden gescand worden. Je kunt extenties toevoegen of verwijderen.



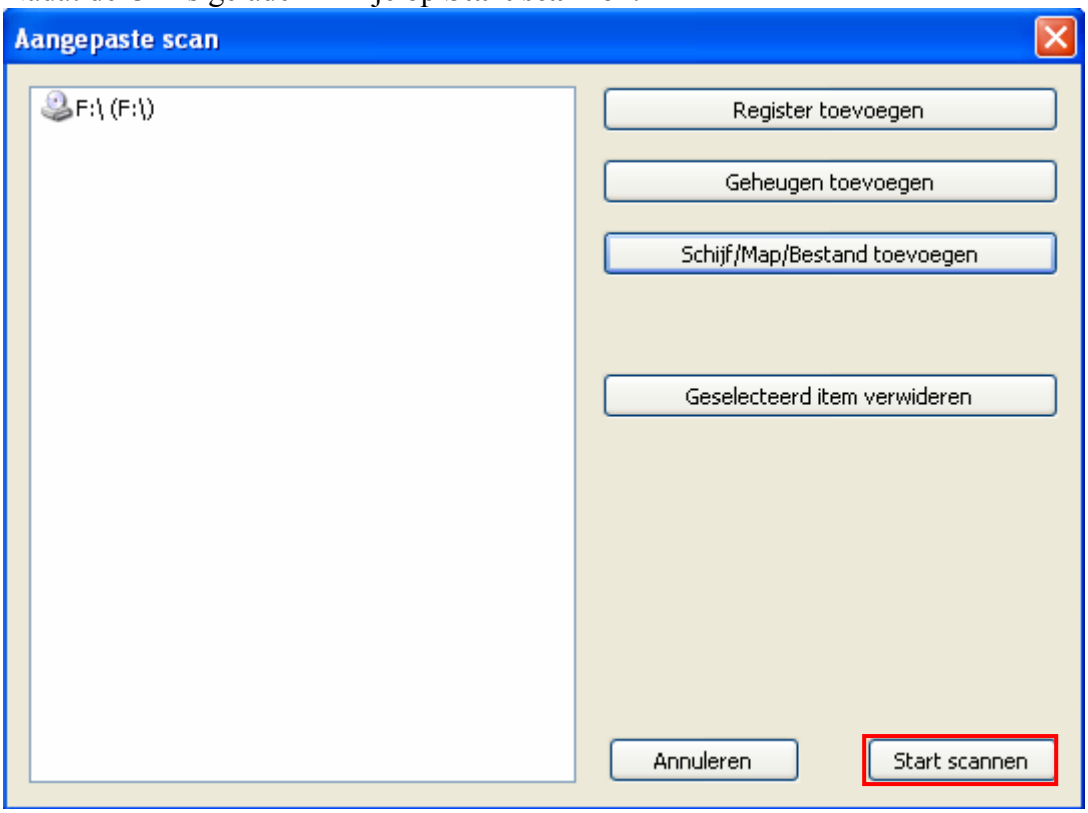
OPMERKING: Het scannen zelf vraagt bij momenten wel redelijk veel van het geheugen.Het is sterk aan te raden om zoveel mogelijk andere (niet-noodzakelijke) lopende programma's, open internetsites, ... te sluiten voor je gaat scannen !

1) Aangepaste scan, maakt het mogelijk zeer gericht te scannen door het (de) beoogde item(s) toe te voegen. Je selectie zal in het witte venster getoond worden. Je kunt een item uit de lijst verwijderen door het te selecteren en dan op de knop **Geselecteerd item verwijderen** te klikken.



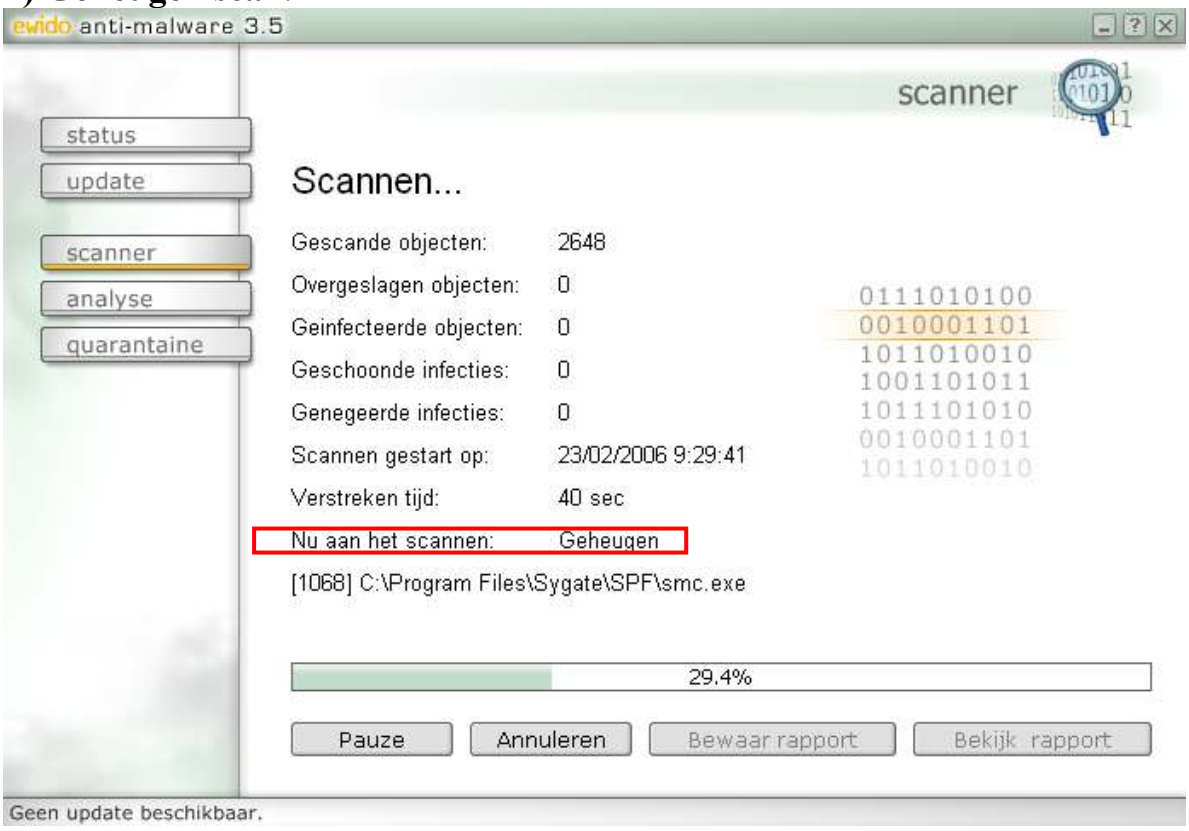
Indien je, bijvoorbeeld, in bovenstaand venster op de knop **Schijf/Map/Bestand toevoegen** klikt, dan kom je in onderstaand venster terecht. Ga naar het gewenste item en klik op **OK**.

In dit voorbeeld is het CD-rom station F:\ toegevoegd om een CD te scannen.
Nadat de CD is geladen klik je op **Start scannen**.



---

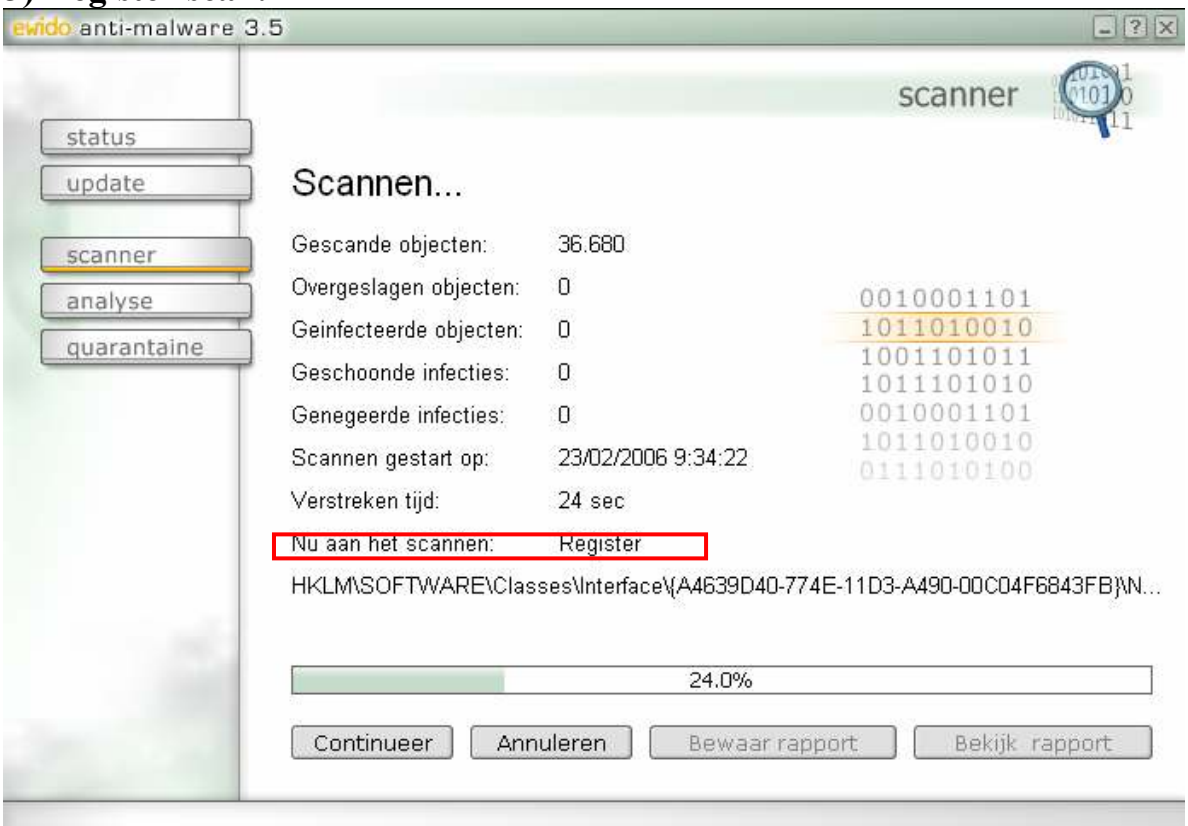
2) Geheugen scan.



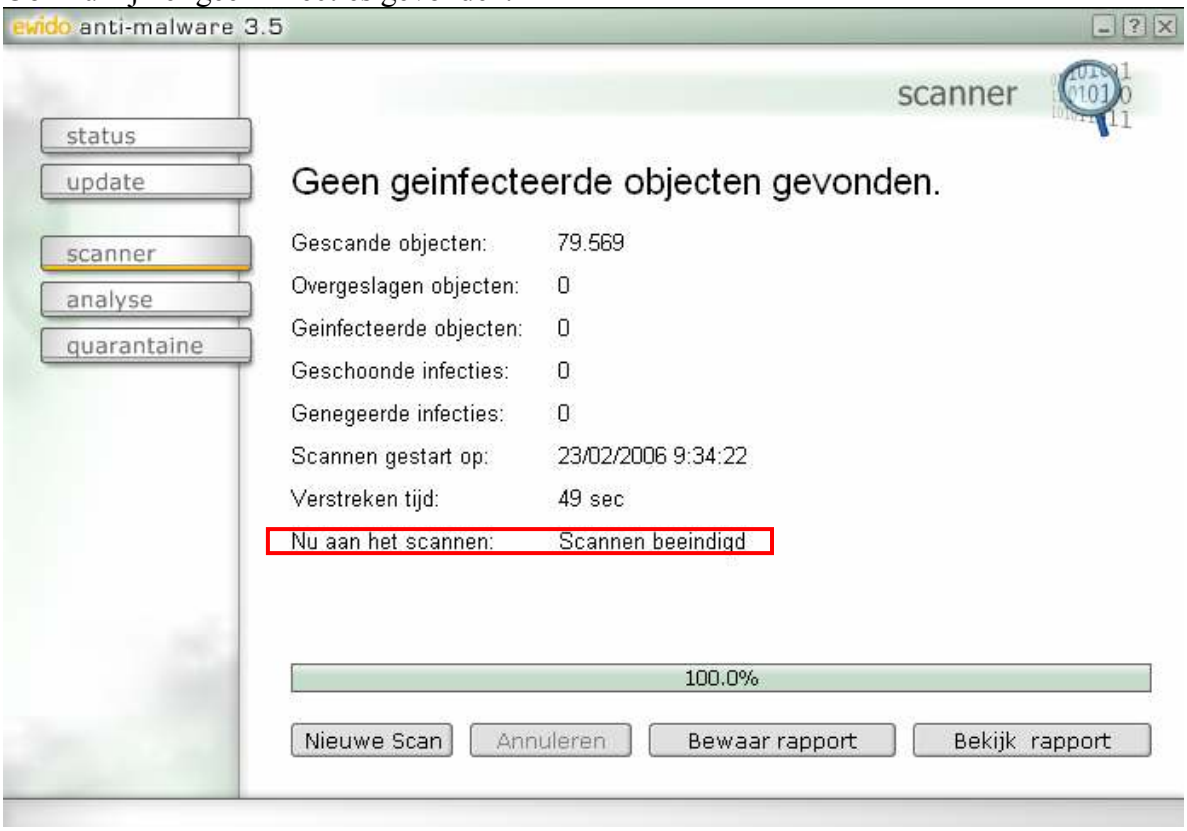
De geheugen scan is beëindigd en er zijn geen infecties gevonden.

---

3) Register scan.

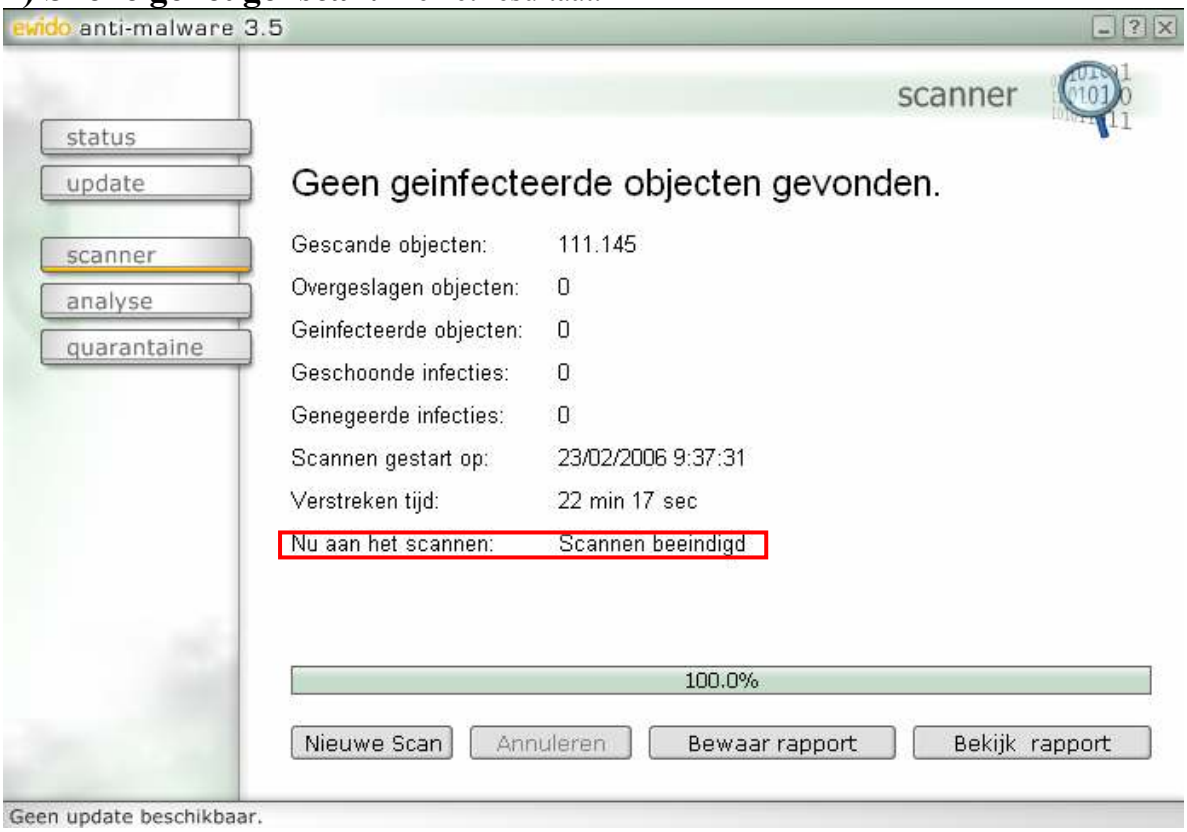


Ook nu zijn er geen infecties gevonden.



---

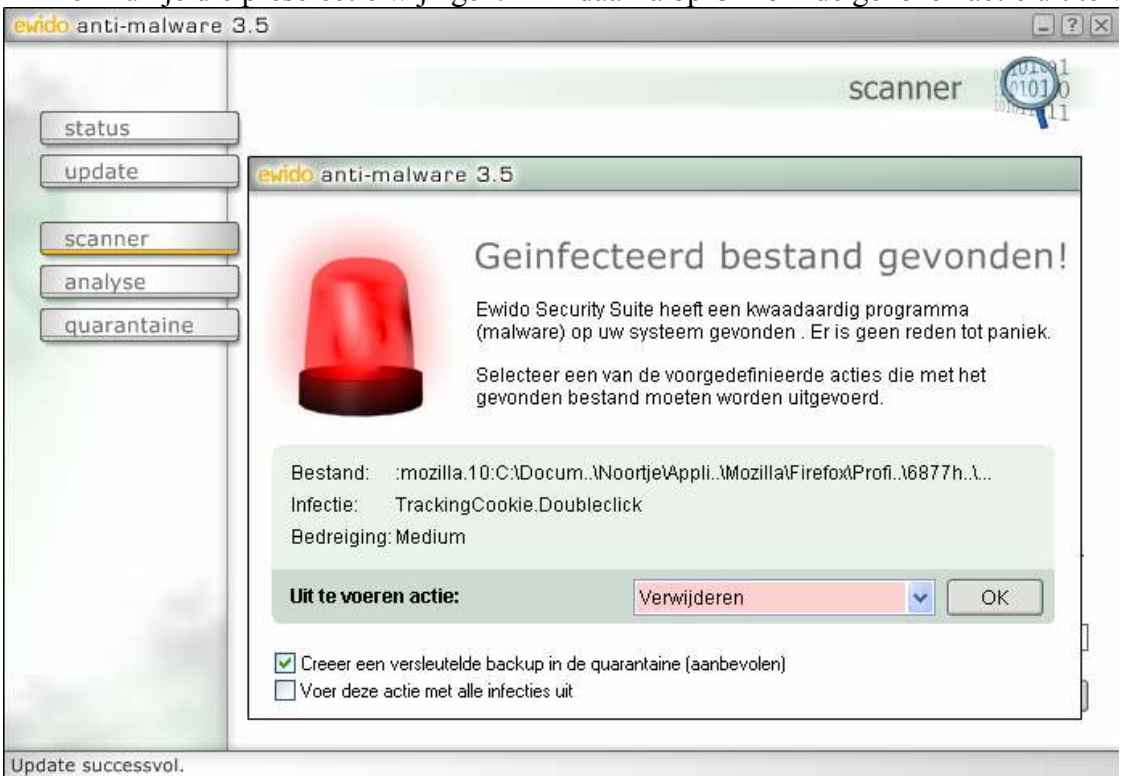
4) Snelle geheugenscan. Zie het resultaat.



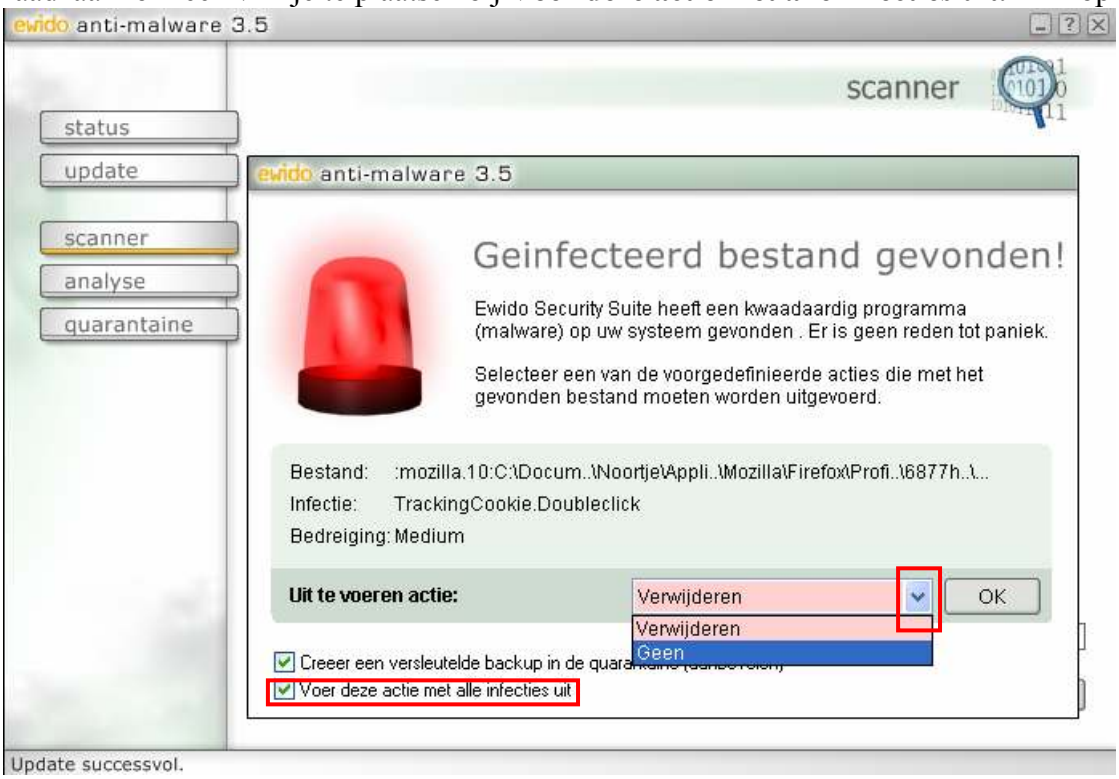
---

5) Volledige systeem scan.

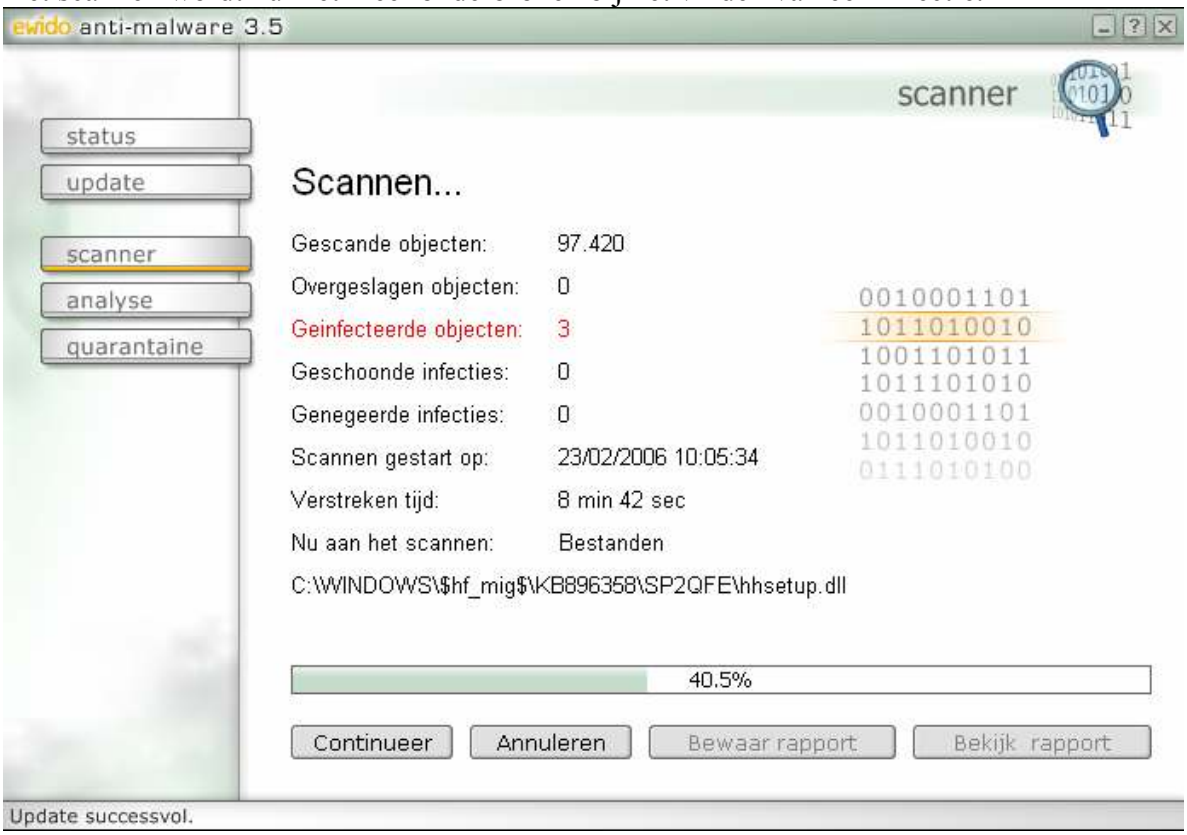
Zodra de eerste infectie is gevonden, wordt je gevraagd wat er mee moet gebeuren. Het programma formuleert een voorstel (zie rose achtergrond). Door op het zwarte pijltje te klikken kun je die preselectie wijzigen. Klik daarna op OK om de gekozen actie uit te voeren.



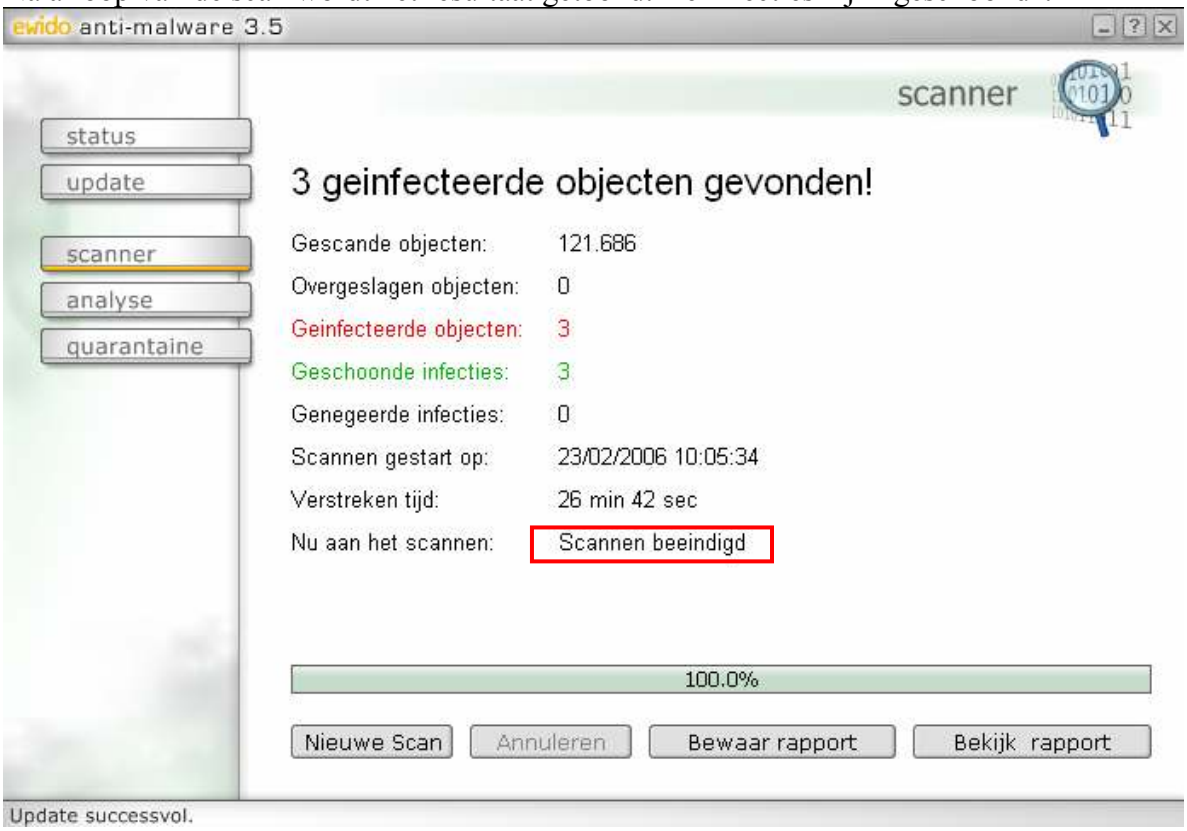
Vermits je te maken kunt hebben met tientallen, zo niet honderdtallen, infecties, is het raadzaam om een vinkje te plaatsen bij **Voer deze actie met alle infecties uit.** Klik op **OK**



Het scannen wordt nu niet meer onderbroken bij het vinden van een infectie.

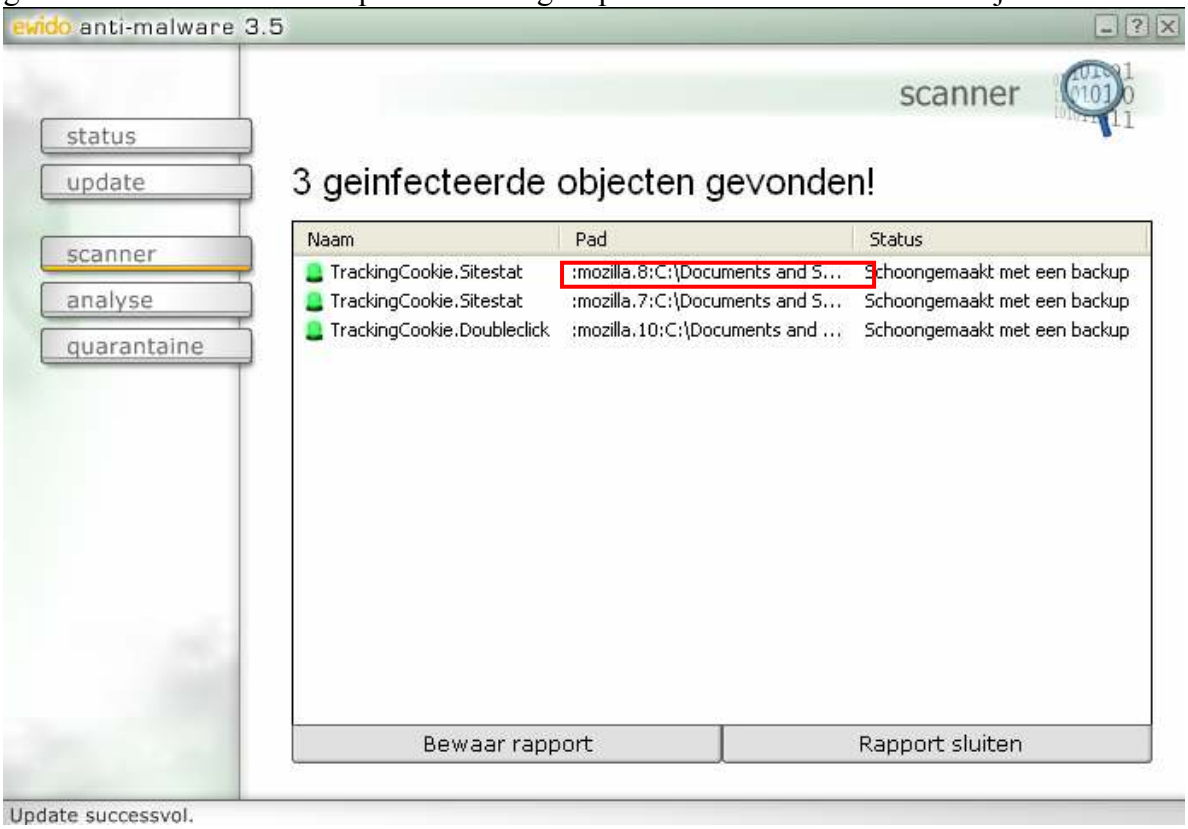


Na afloop van de scan wordt het resultaat getoond. De infecties zijn “geschoond”.

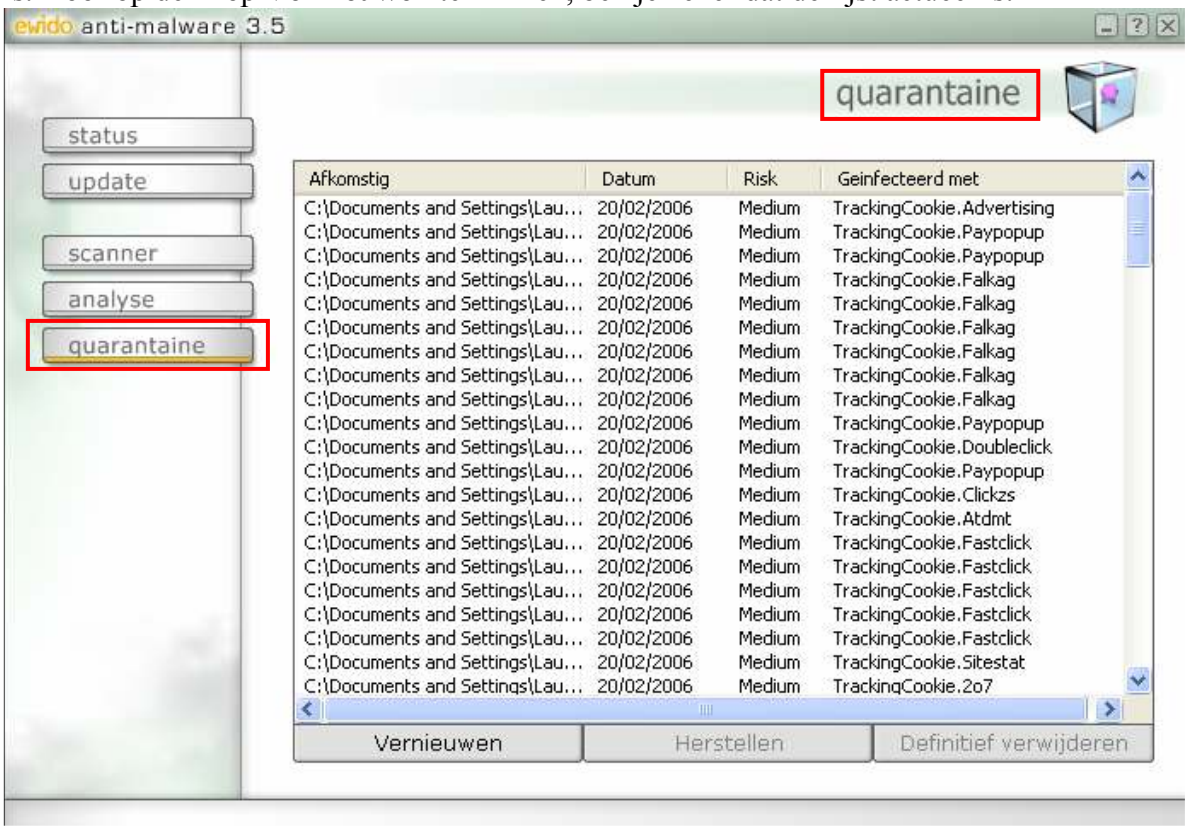


Indien gewenst, kun je het rapport bekijken en bewaren. Klik bv eens op **Bekijk rapport.**

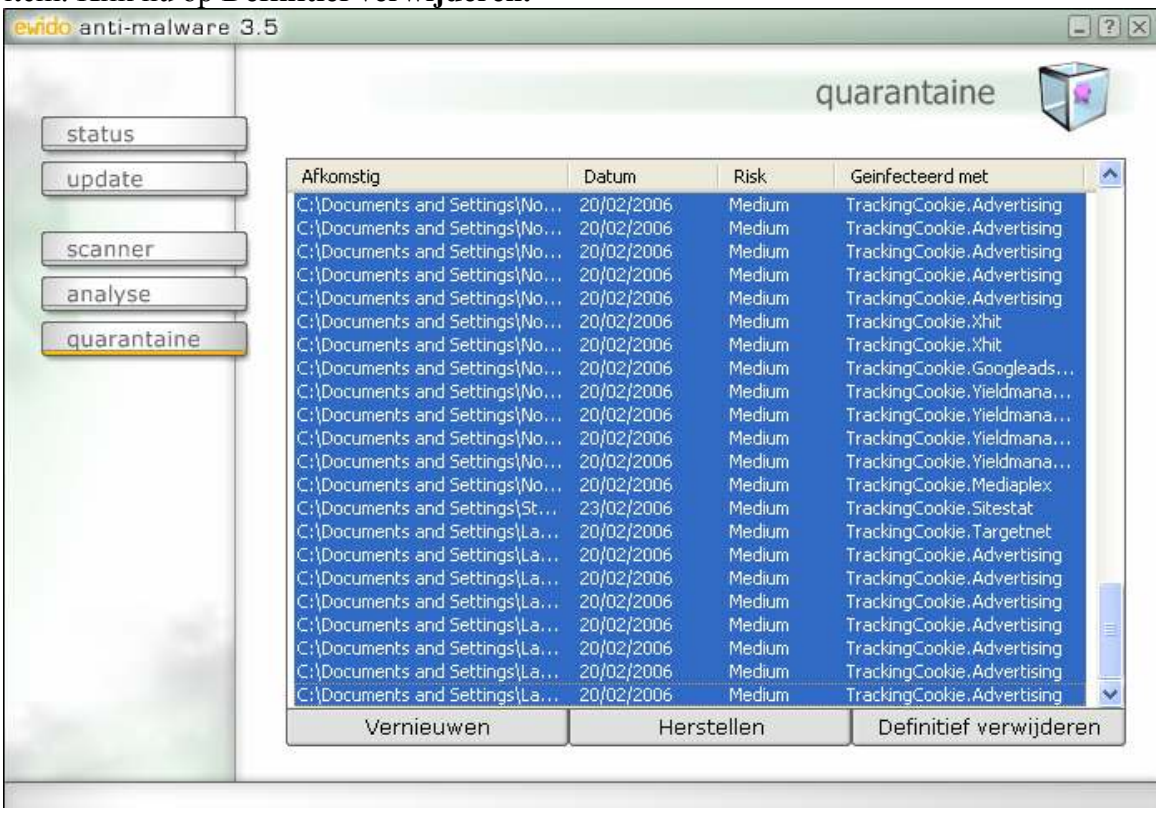
Ziehier het rapport. Door met de muisaanwijzer op het pad van een item te gaan staan zal het volledige pad getoond worden. “Schoongemaakt met een backup” wil zeggen dat het geïnfecteerde item naar de quarantaine is gekopieerd alvorens het werd verwijderd.



Quarantaine. We zien hier dat deze, mede tengevolge van vorige scans, behoorlijk gevuld is. Door op de knop **Vernieuwen** te klikken, ben je zeker dat de lijst actueel is.



Indien je een item vanuit de quarantaine wil terugzetten, dan moet je het selecteren alvorens op de knop **Herstellen** te klikken.
Je doet er goed aan zo nu en dan de quarantaine leeg te maken. Selecteer de volledige inhoud door op het eerste item te klikken. Klik vervolgens, met ingedrukte Shift-toets, op het laatste item. Klik nu op **Definitief verwijderen.**



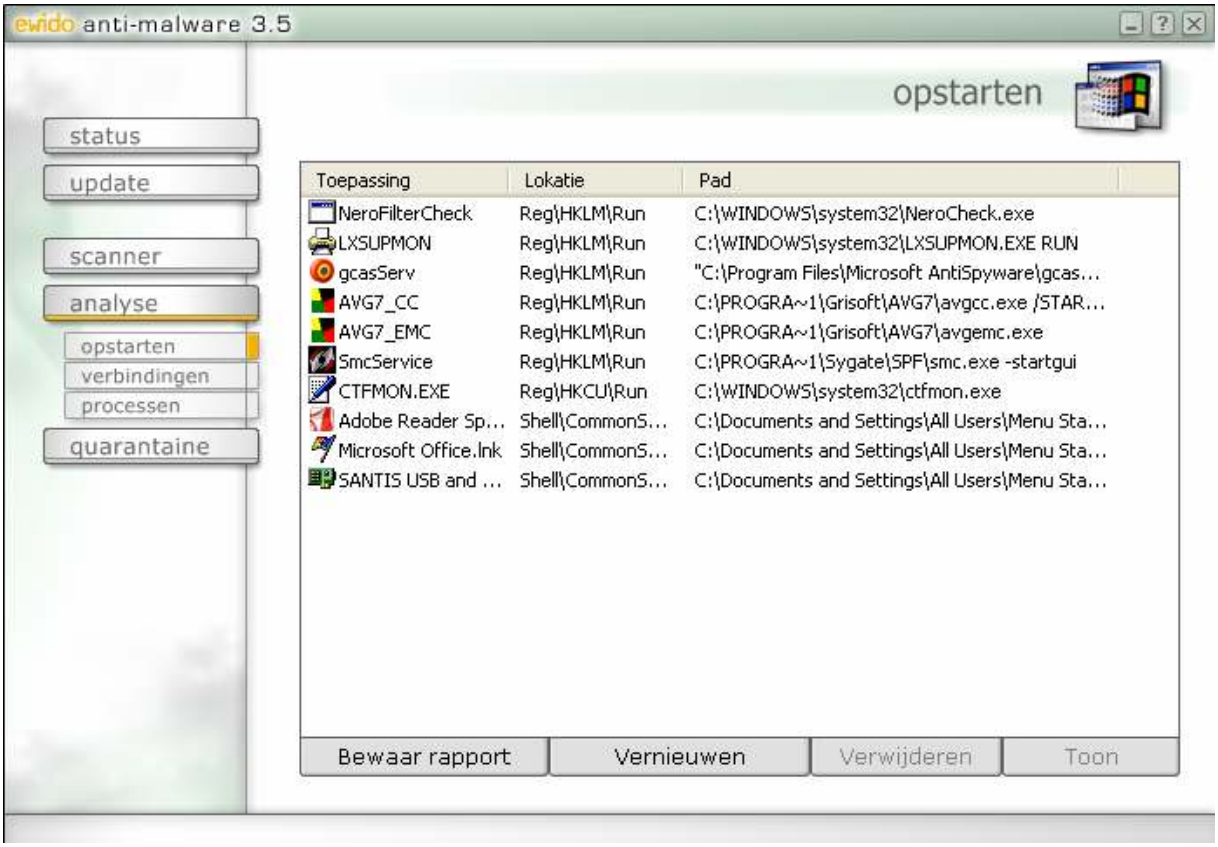
Analyse. Hier zijn 3 overzichten beschikbaar met telkens enkele functies.

We lichten hier de 3 analyse functies toe.

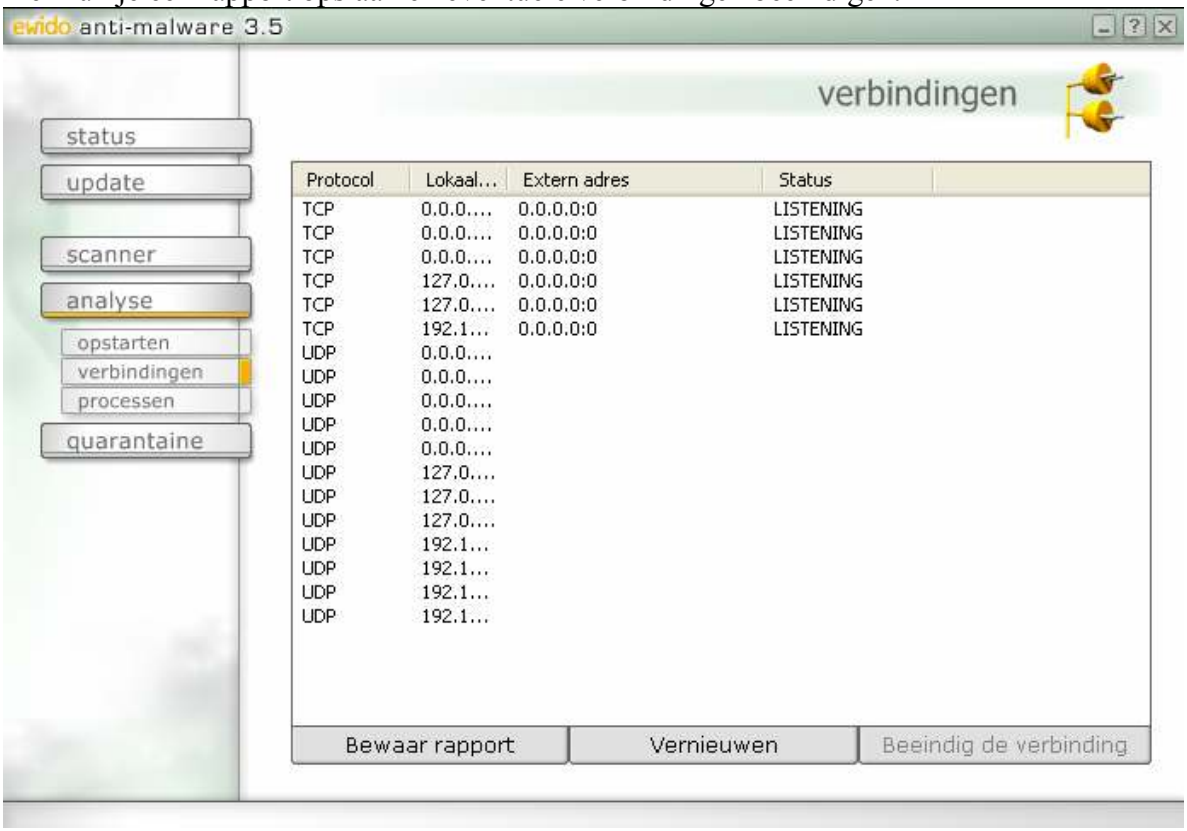
Opstarten.

Er wordt een lijst getoond van alle programma's die bij het opstarten van Windows mee opgestart worden.

- Je kunt de lijst opslaan door op **Bewaar rapport** te klikken.
- Door op **vernieuwen** te klikken, wordt de lijst geactualiseerd.
- Je kunt een opstart-item verwijderen door het te selecteren en vervolgens op **Verwijderen** te klikken.
- Door een regel te selecteren en vervolgens op de knop **Toon** te klikken, opent zich het register bij dat item of de locatie in het Menu Start.



Verbindingen. Geeft een overzicht weer van de lopende verbindingen en hun status. Ook hier kun je een rapport opslaan en eventuele verbindingen beëindigen.



Processen. Toont de lopende processen. Ook hier weer de mogelijkheid om een rapport op te slaan, te vernieuwen en om processen te beëindigen.