



Spybot-Search&Destroy


1. **Downloaden, installeren en gebruiksklaar maken.**
2. **Updaten, immuniseren en scannen.**
3. **Geavanceerde instellingen.**
4. **Spybot-Search & Destroy volledig verwijderen.**
5. **Bijlage.**

Lees eerst dit:

- Door deze handleiding op te slaan heb je ze altijd bij de hand.
- Het zichtbaar maken van de bladwijzers doe je in Adobe Reader of Acrobat door op de tab bladwijzers te klikken links in het venster. In Foxit Reader klik je daarvoor in de menubalk op “Beeld”-> Bladwijzers.
- Deze handleiding is gebaseerd op **versie 1.5.2.20**
- Wie van deze handleiding gebruik maakt, doet dat op eigen risico.

1. Downloaden, installeren en gebruiksklaar maken

a. Downloaden

-  **Download Spybot S&D.** Indien niet bereikbaar, probeer het later eens opnieuw.
- Klik op één van de blauwe "**Download here**" knopjes. Bij voorkeur eentje van **Safer-Networking Ltd.**
- Kies voor "**opslaan**" en sla het bestand "**spybotsd152.exe**" op naar een locatie waar je het makkelijk terugvindt, bv bureaublad. Je kunt dit setup-bestand na het voltooiën van de installatie trouwens gewoon verwijderen.

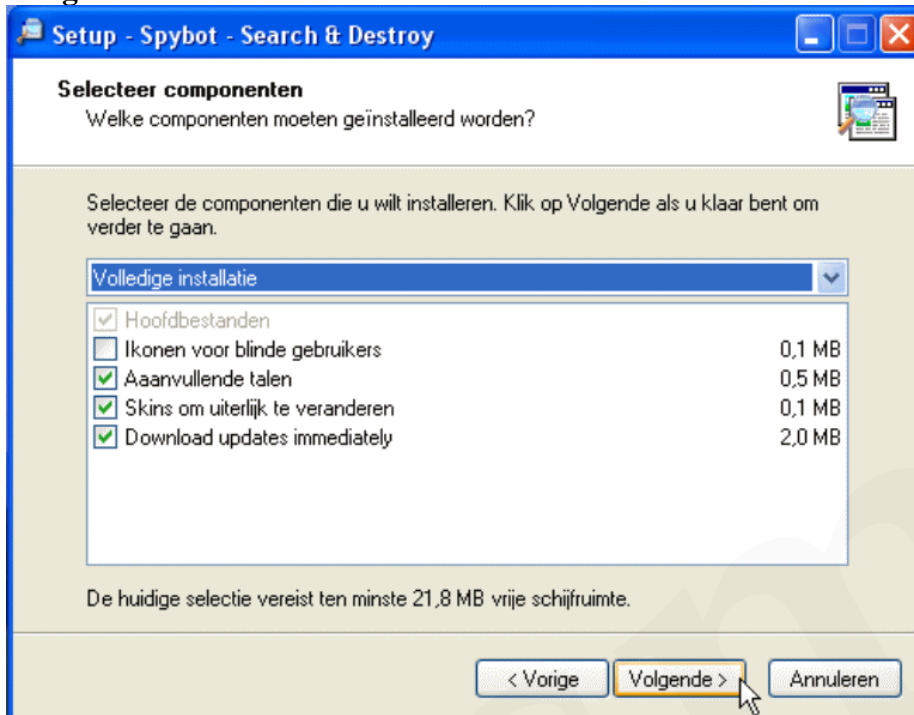
b. Installeren

Indien je een recentere versie wenst te installeren dan degene die je al staan hebt, verwijder dan eerst de oude versie alvorens een nieuwe te installeren. Lees in **hoofdstuk 4** hoe je dat doet.

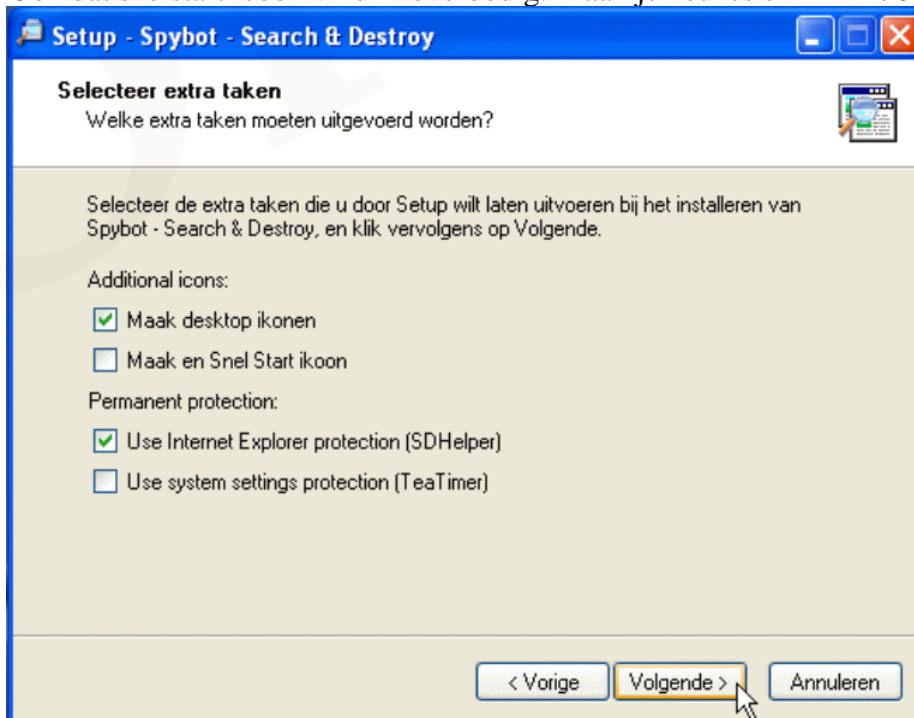
- Maak, naar goede gewoonte, een systeemherstelpunt alvorens je een programma installeert. Klik **hier** om te weten hoe je dat doet.
- Sluit alle geopende toepassingen.
- Dubbelklik op het opgeslagen setup-bestand "**spybotsd152.exe**"
- Selecteer je taalkeuze tijdens de installatie (**Nederlands**) > klik **OK**
- **Welkomstvenster** > klik "**Volgende**"
- **Licentie-overeenkomst** > vink "**Ik accepteer de licentie-overeenkomst**" aan en klik "**Volgende**"
- **Kies de doelmap:** Standaard is dat "**c:\program files\spybot - search & destroy**" (min. 30,7 mb ruimte op de harde schijf vereist) > Klik "**volgende**"
 - Indien er nog een map “Spybot-Search&Destroy” van een vorige installatie staat dan zal je gevraagd worden of je toch naar die map wil installeren. Klik op “**Ja**”

indien je zeker bent dat je eerder de oude versie hebt verwijderd. In het andere geval klik je “**Neen**” om de installatie af te breken. Verwijder de oude versie (zie hoofdstuk 4) en start de installatie opnieuw.

- **Selecteer componenten:** Standaard staat de "**volledige**" installatie" aangeduid. Klik "**volgende**"



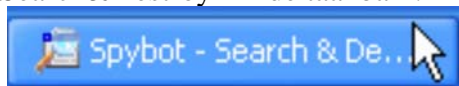
- **Start map:** Standaard "**Spybot - Search & Destroy**" > Klik "**Volgende**"
- **Selecteer extra taken:** Hier kun je o.a. aanvinken om de twee preventieve tooltjes van Spybot S&D te activeren: **SD-helper** en **Teatimer**. Vink de **TeaTimer** nog **niet** aan, je kunt deze ook achteraf nog steeds in het programma zelf instellen (zie hoofdstuk 3). Ook dat snelstart icoon vind ik overbodig. Maak je keuzes en klik "**Volgende**"



- **Het voorbereiden van de installatie is gereed.** Hier zie je een overzicht van de instellingen die je opgegeven hebt. Wil je nog iets veranderen, neem dan het knopje "Vorige". Is alles naar wens, klik dan "Installeren".
- **Spybot S&D** wordt nu geïnstalleerd.
 - Indien je over een Firewall beschikt dan zal deze melden dat Spybot verbinding met het Internet zoekt. Geef daar een permanente toestemming voor.
- Klik op **Voltoeien** om de Installatiewizard af te sluiten. **We gaan nu naadloos over naar het gebruiksklaar maken van het programma.**

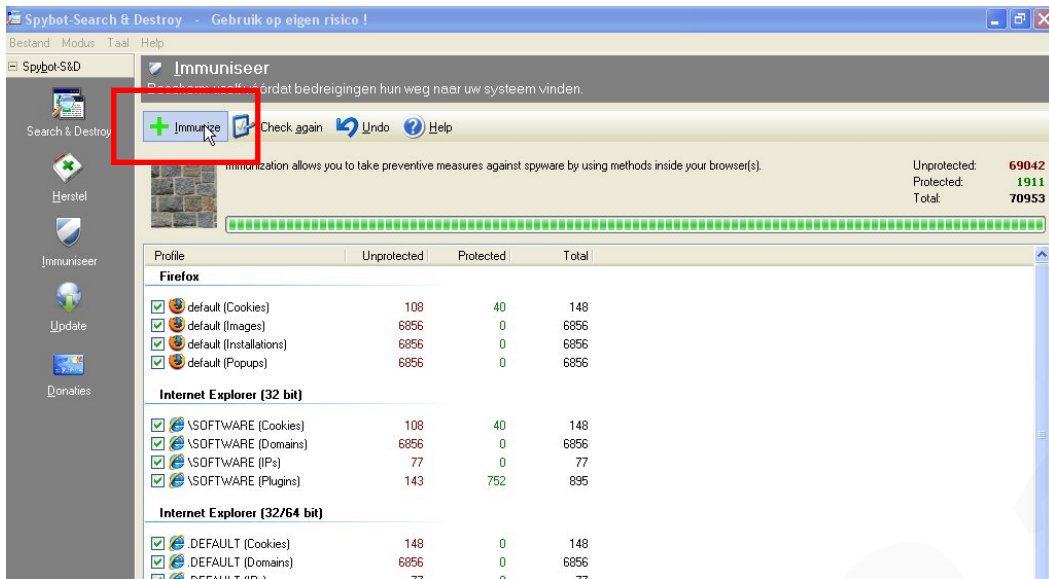
c. Gebruiksklaar maken

- Plaats in het venstertje "**Juridische zaken**" een vinkje bij "**Toon dit bericht niet weer**" en klik op **OK**.
 - **Opgelet:** Dit venster staat mogelijk op de achtergrond open indien je nog een ander venster hebt open staan. Klik dan even op de tab "Spybot-Search&Destroy" in de taakbalk.



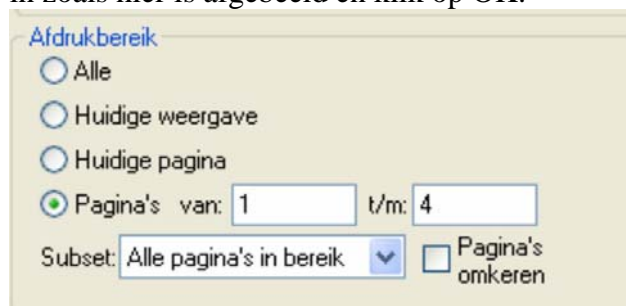
- **Spybot-S&D** wordt op de achtergrond geopend. Op de voorgrond staat het Wizard-venstertje **Stap 3 van 7**
- In het venster **Stap 3 van 7** wordt de mogelijkheid geboden om een **backup van het register** te maken. Omdat we eerder een systeemherstelpunt gemaakt hebben slaan we deze stap over door op de knop "**Volgende**" te klikken. Omdat stap 4 van 7 vreemd genoeg niet bestaat, komen we nu in het venster "stap 5 van 7".
- Klik in het venster **Stap 5 van 7** op de knop "**Zoek naar updates**".
 - Indien je over een Firewall beschikt dan zal deze melden dat Spybot verbinding met het internet zoekt. Geef daar een permanente toestemming voor.
- Er zal een lijst getoond worden van alle servers waarvan men kan updaten. Standaard is willekeurig één van deze voorgeselecteerd. Je hoeft dus enkel maar op "**Continue**" te klikken.
- De beschikbare updates worden nu getoond. Enkel de voor u belangrijke updates zijn standaard aangevinkt. Klik op **Download**. De te downloaden items worden één na één met een wit vinkje in een groen rondje gemarkeerd zodra de download gelukt is.
 - **Ter attentie:** Het kan gebeuren dat de server overbelast is en dat daardoor het downloaden van sommige items mislukt (Dat zie je aan dat wit kruisje in rood rondje). Klik dan op "**Back to mirror list**", selecteer uit de lijst een andere server en klik op "**Continue**" om het downloaden over te doen.
- In een klein **informatievenstertje** wordt je er in het Engels aan herinnerd, na iedere update, het immunisatie- proces uit te voeren en een scan te doen. Beide komen later aan bod. Klik dus op **OK**.
- Zodra het downloaden met succes afgerond is klik je op "**Exit**" en vervolgens, in het venster **stap 5 van 7**, op "**Volgende**".
- Klik, in het venster **stap 6 van 7**, op de knop "**Immuniseer mijn systeem**". Volg het proces in het, op de achtergrond, geopende venster van Spybot S&D. Indien er, na afloop, bij "**Protected**" een NUL staat, klik dan nogmaals op de knop "**Immuniseer mijn systeem**". Misschien heb je de eerste keer niet goed geklikt.
- Indien je daar in de rechterbovenhoek bij "**Unprotected**" een rood getal ziet staan dat groter is dan 0, klik dan op de knop "**Immunize**" (zie groen apothekerskruisje), **in**

afbeelding rood omkaderd. Het rode getal zal op 0 (nul) gezet worden, en zo hoort het te zijn.



- Indien dat rode getal al op nul stond (of staat), klik dan in het venster **stap 6 van 7**, op “**Volgende**”.
- Klik in het venster **Stap 7 van 7** op de knop “**Start het programma**” om alles af te ronden. Je zult hierdoor geen verandering zien omdat het programma al gestart was. **Sluit nu het programma af.**
- Verwijder het overbodig geworden installatiebestand. **Let op !!!** Het icoon van dit bestand lijkt sprekend op het snelkoppelings-icoon van Spybot.
- Spybot S&D is nu klaar voor gebruik. Met de huidige instellingen wil dat zeggen dat:
 - Enkel de **SDHelper** (Internet Explorer slechte downloadblokkeerder) op de achtergrond actief is.
 - Het programma niet is ingesteld om automatisch te updaten. Je moet dat dus regelmatig zelf doen.
 - Er geen automatische scantaak is ingesteld. Je moet het scannen dus regelmatig zelf starten.

Een goede raad: Omdat, tijdens de installatie, alle toepassingen dienen gesloten te zijn doe je er goed aan dit hoofdstuk af te drukken en ter inzage naast je toetsenbord te leggen. Om het aantal afdrukpagina's tot een minimum te beperken is er in dit hoofdstuk zo weinig mogelijk gebruik gemaakt van schermafbeeldingen. Zet je printer aan. Klik in de menubalk op **Bestand -> Afdrukken**. Stel het afdrukbereik in zoals hier is afgebeeld en klik op OK.



Zij die toch alles wensken af te drukken selecteren hier **Alle**.

Ga nu naar **hoofdstuk 2** voor informatie bij het scannen of naar **hoofdstuk 3** voor geavanceerde instellingen.

Naar begin

2. Updaten, immuniseren en scannen

Zij die een automatische scan- en updatetaak hebben ingesteld hoeven dus zelf geen scan- en updateopdracht uit te voeren. Deze instellingen worden toegelicht in **hoofdstuk 3**.

De scantaak wordt dan op het ingestelde tijdstip automatisch uitgevoerd.

De updatetaak wordt continu waargenomen zodra je Internetverbinding hebt.

Er dient hierbij wel rekening mee gehouden te worden dat het scannen de CPU (processor) behoorlijk belast. Je mag rekenen op een CPU gebruik van +/- 32.000 kb. Bij oudere computers kan dan het totale CPU gebruik oplopen tot 90 à 100 %. In een dergelijk geval is het nauwelijks te doen om gelijktijdig nog met een ander programma bezig te zijn. Je scant dan best terwijl je zelf even iets anders doet. In dit geval is dus een automatische scantaak instellen uit den boze.

Dit hoofdstuk is vooral van toepassing voor de gebruikers die handmatig wensen te updaten en te scannen.

Start het programma.

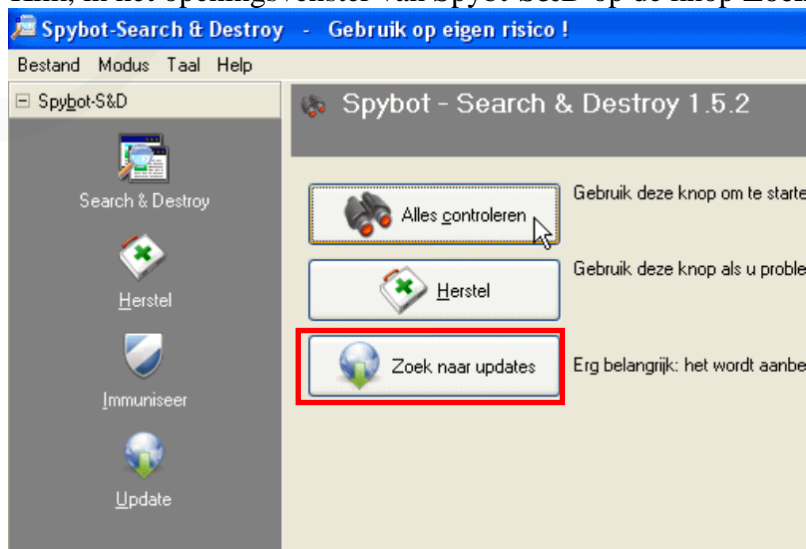
Dat kan door te dubbelklikken op het programma-snelkoppeling op je bureaublad of via Start -> Alle Programma's.

a. Updaten en immuniseren

Indien je automatische updates hebt ingeschakeld staan, dan mag je er vanuit gaan dat je programma Up To Date is. Ga dan verder naar **b. Scannen en fixen**.

De andere gebruikers moeten eerst even nagaan of er nieuwe updates ter beschikking zijn. Doe daarom wat volgt:

- Klik, in het openingsvenster van Spybot-S&D op de knop **Zoek naar updates**.



Het venster **Spybot-S&D Updater** wordt geopend. Er zal een lijst getoond worden van alle servers waarvan men kan updaten. Standaard is willekeurig één van deze voorgeselecteerd. Je hoeft dus enkel maar op “**Continue**” te klikken



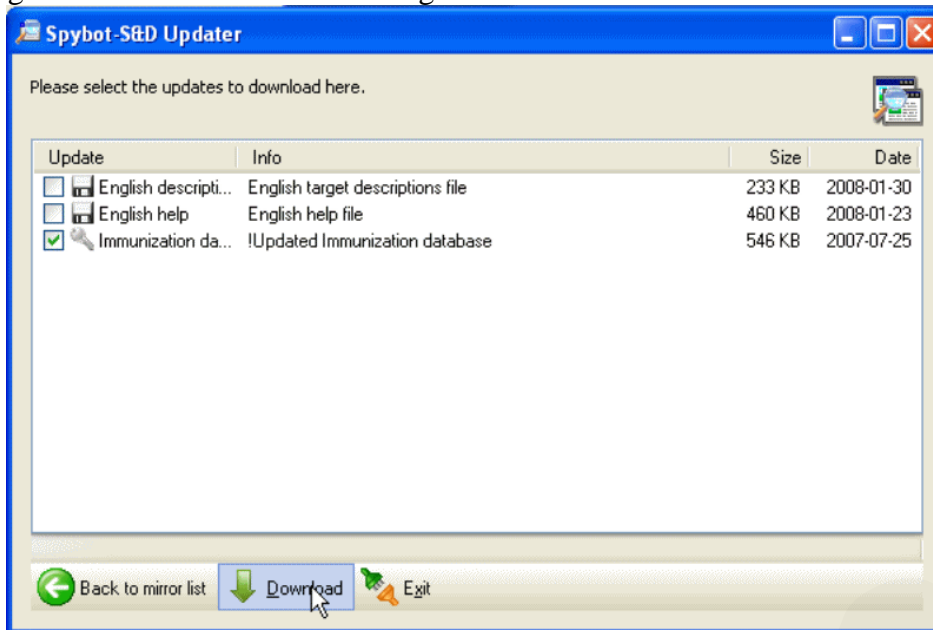
- Indien er helemaal geen updates ter beschikking zijn dan wordt dat als volgt medegedeeld.



Klik dan op **OK**.

- Indien er wel updates ter beschikking zijn dan worden deze nu getoond. Enkel de voor u belangrijke updates zijn standaard aangevinkt. Klik op **Download**. De te

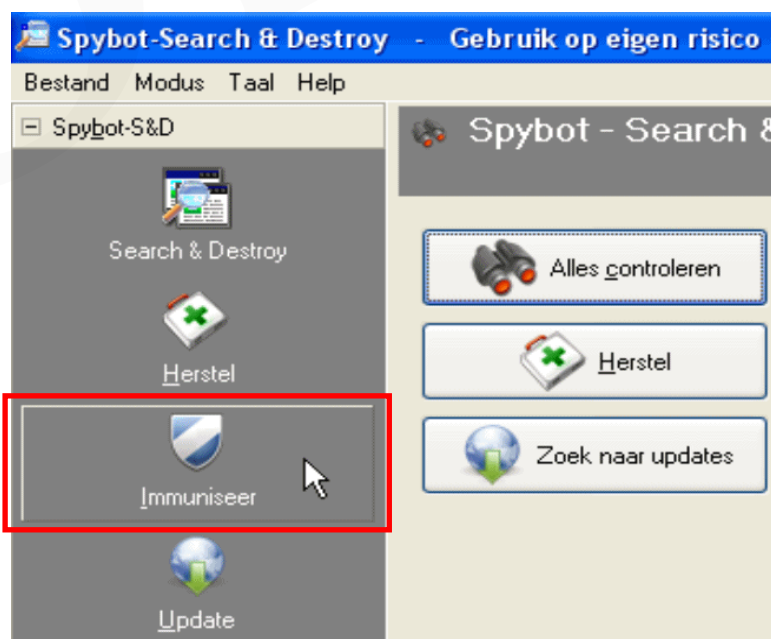
downloaden items worden één na één met een wit vinkje in een groen rondje gemarkeerd zodra de download gelukt is.



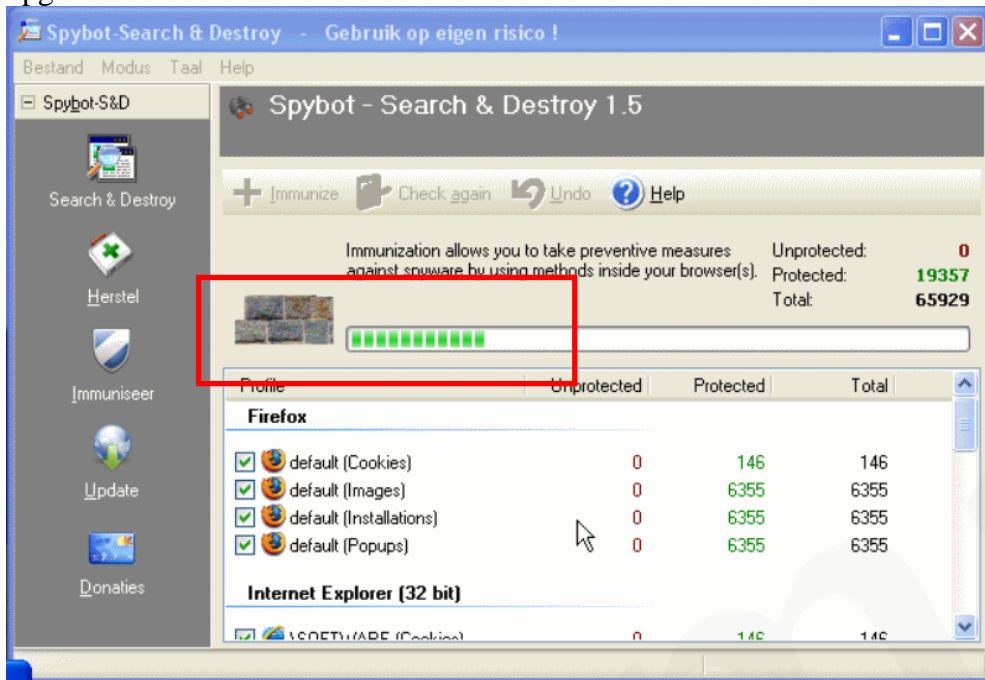
- **Ter attentie:** Het kan gebeuren dat de server overbelast is en dat daardoor het downloaden van sommige items mislukt (Wit kruisje in rood rondje). Klik dan op “**Back to mirror list**”, selecteer uit de lijst een andere server en klik op “**Continue**” om het downloaden over te doen.

Klik op **Exit**, zodra het updaten met succes is voltooid.

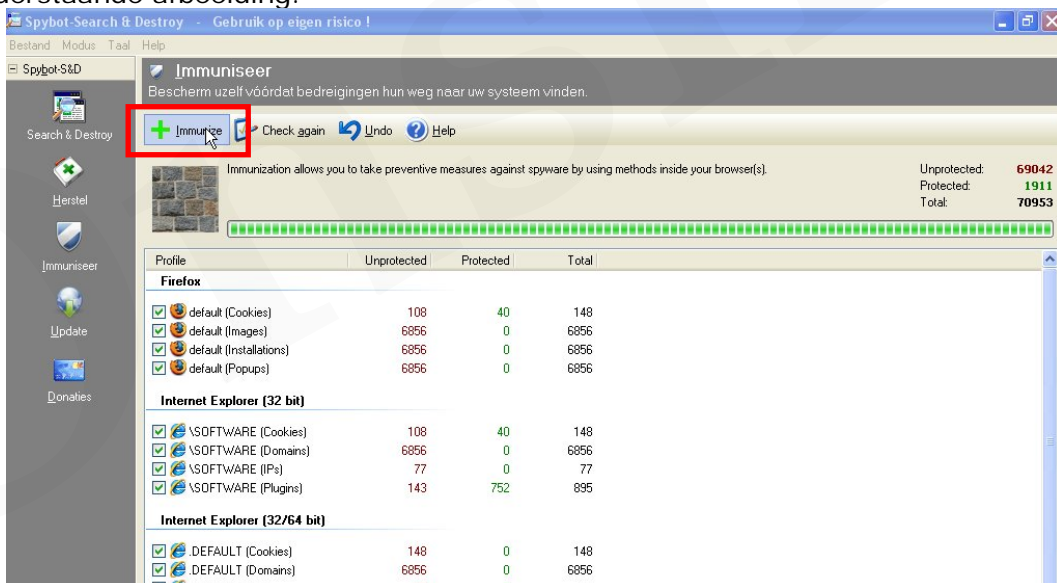
- Indien er enkel voor u onbelangrijke, niet aangevinkte, updates ter beschikking zijn, klik dan op **Exit**.
- Indien er nieuwe updates gedownload zijn dan moeten de nieuwste gekende slechte producten nog geblokkeerd worden. Dat doe je als volgt.
- Klik in het openingsvenster op de knop **Immuniseer**.



- De nieuwste “Includes” betreffende de preventieve bescherming van je browser(s) worden nu geladen. Dat zie je ondermeer aan het muurtje dat symbolisch wordt opgebouwd.



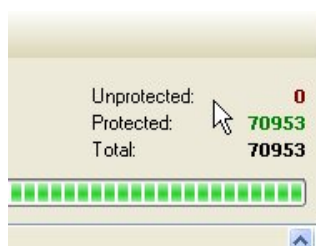
- Zodra dit proces afgelopen is krijg je een overzicht van de actuele situatie. Zie onderstaande afbeelding.



We zien hier in de rechterbovenhoek dat er nog **69042 items** onbeschermd (Unprotected) zijn.

Om dat cijfer op **NUL** te stellen klikken we op de knop “**Immunize**” met het groene kruisje.

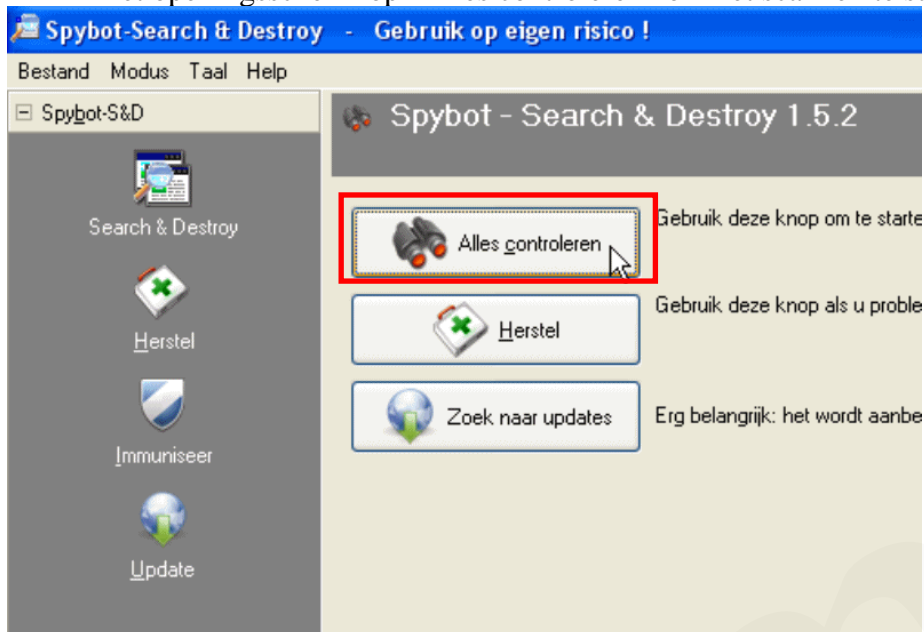
De onbeveiligde (Unprotected) items worden op **NUL** gesteld. Zie onderstaande afbeelding.



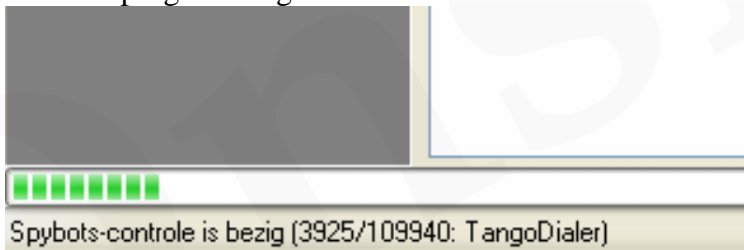
Het programma is nu helemaal klaar om een scan uit te voeren.

b. Scannen en fixen

- Klik in het openingsscherm op “Alles controleren” om het scannen te starten.



- In de balk beneden in het scanvenster zie je de groene vorderingsbalk langzaam naar rechts vollopen. Je kunt ook lezen dat de controle bezig is . Tevens zie je daar naar welke malware er gezocht wordt. Daarom is het zo belangrijk dat je programma Up To Date is alvorens een scan uit te voeren. Zo niet, zijn de meest recente boosdoeners niet door het programma gekend.

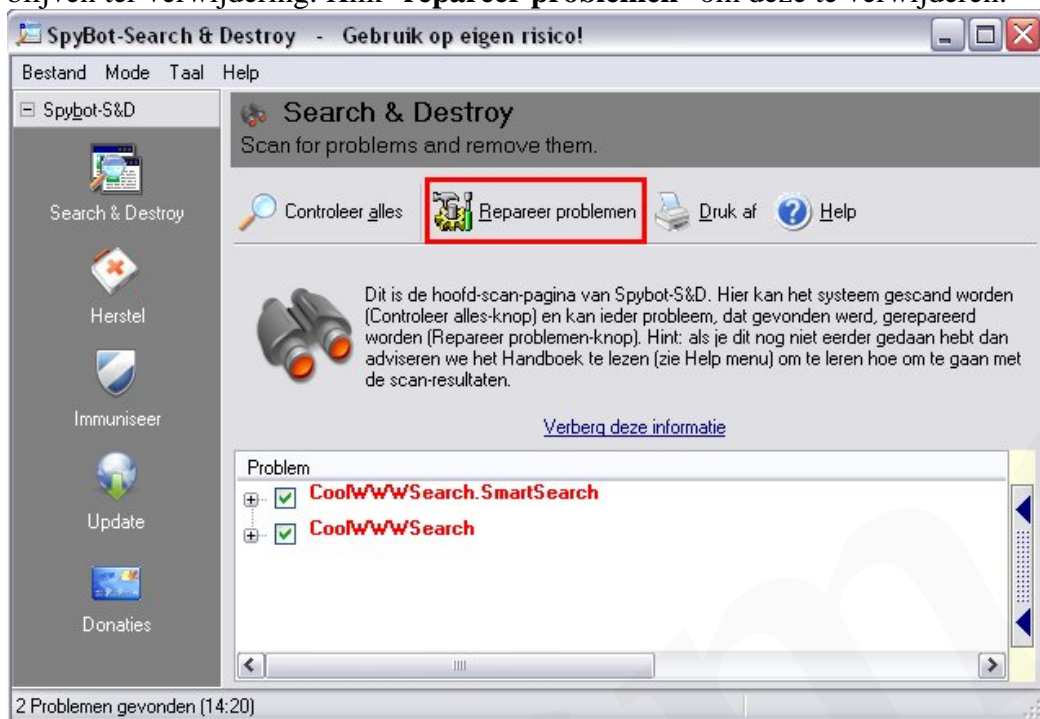


- Zodra de scan voltooid is, wordt het resultaat getoond. Hopelijk ziet er dat zo uit.



Er zijn hier geen bedreigingen gevonden. Je kunt dus het programma sluiten.

- Maar het is niet uitgesloten dat er wel degelijk malware gevonden wordt. Onderstaande afbeelding is daar een voorbeeld van. Alle problemen in het **rood** weergegeven worden beschouwd als **werkelijke bedreigingen** en mogen aangevinkt blijven ter verwijdering. Klik "**repareer problemen**" om deze te verwijderen.



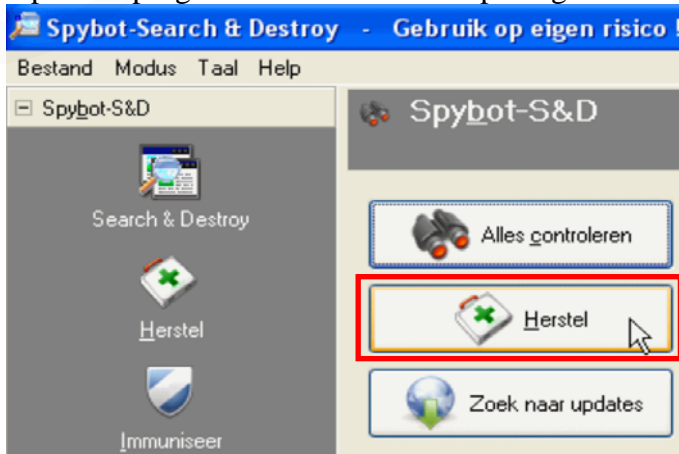
Spybot S&D zal, voor alle zekerheid, van de verwijderde items een backup maken en deze opslaan. Hierover dadelijk meer in "**Goed om weten**".

- Bevestig dat je de aangekruiste items wil verwijderen en laat het programma rustig zijn werk doen. Wanneer de problemen gefixt zijn krijg je een bevestiging. Klik "**OK**".
- **Herstart** de computer en doe eventueel nogmaals een scan met Spybot S&D.

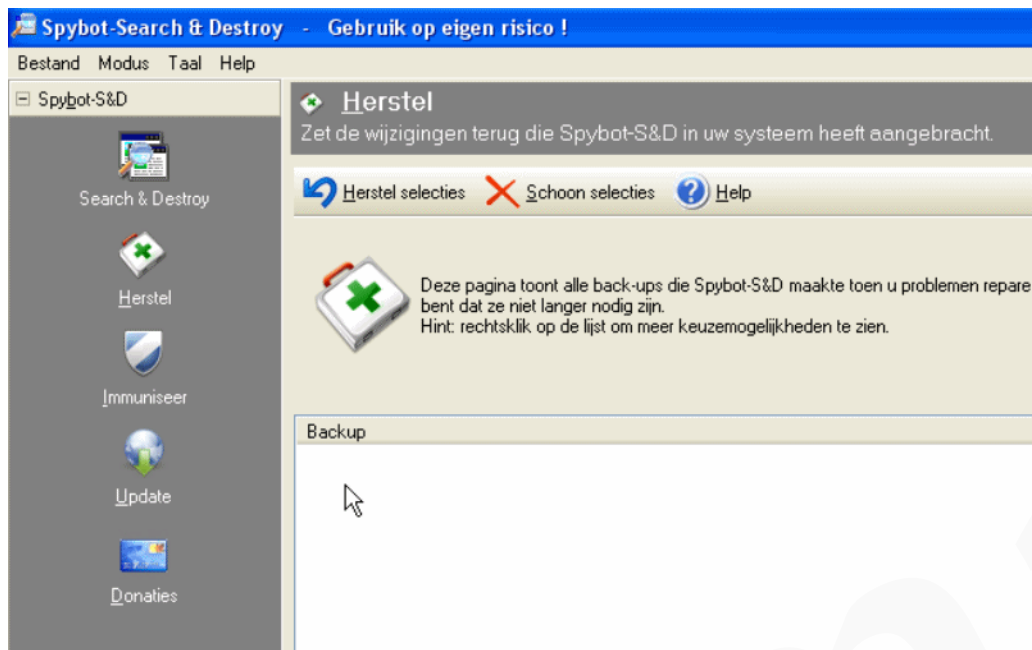
Goed om weten:

Bij iedere bewerking op een computer kan er iets fout gaan. Dat risico is zeker aanwezig bij het verwijderen van malware. Heb je toevallig iets te veel verwijderd waardoor bijvoorbeeld een bepaald programma niet meer functioneert, dan kan je die verwijdering ongedaan maken. Dat doe je zo.

- Open het programma en klik in het openingsvenster op **Herstel**.



- Een venster met beschikbare backups zal getoond worden.



Gelukkig voor mij, maar helaas niet voor deze handleiding, is de databank leeg. Indien je echter in je laatste scan items verwijderd hebt dan zal hier (bij de muisaanwijzer) minstens één backupbestand te zien zijn. In feite is enkel de recentste backup waardevol. De overige mag je verwijderen door ze te selecteren (éénmaal op klikken) en vervolgens op de knop **Schoon selectie** te klikken. Om zo een backup terug te zetten selecteer je deze en klik vervolgens op **Herstel selectie**. In het daarop volgend waarschuwingsvenster klik je op **OK**.

Naar begin

Terug naar “Spybot verwijderen”

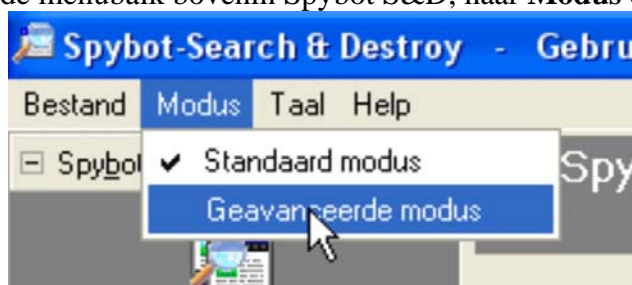
3. Geavanceerde instellingen.

Spybot S&D is niet enkel een spyware scan- en verwijder programma, maar heeft heel wat extra opties in zich, waaronder de “waakhond” **TeaTimer**.

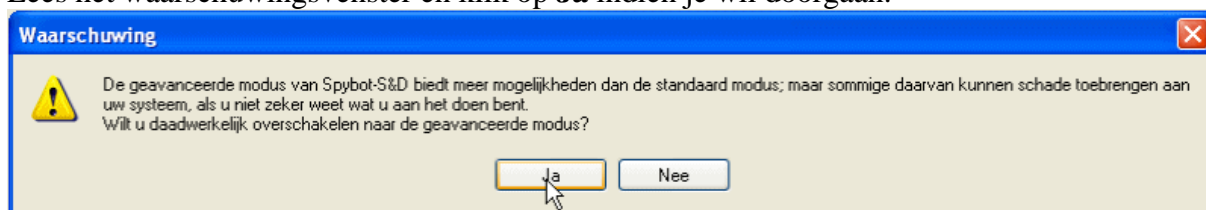
Het grootste deel van deze extra's is ter beschikking in de **Geavanceerde modus**. Deze modus is, in zijn geheel gezien, een complex instrument en vraagt daarom heel wat computerkennis om daar gepast mee te kunnen omgaan. Daarom doen de meeste gebruikers er goed aan in de **Standaard modus** te werken.

Omdat ik me in deze handleiding niet richt tot de echte computerkenners en perfectionisten worden slechts enkele, toch wel interessante, mogelijkheden van de **Geavanceerde modus** toegelicht. Je beslist dus zelf, en op eigen verantwoordelijkheid, of je de hierna volgende voorstellen wenst uit te voeren.

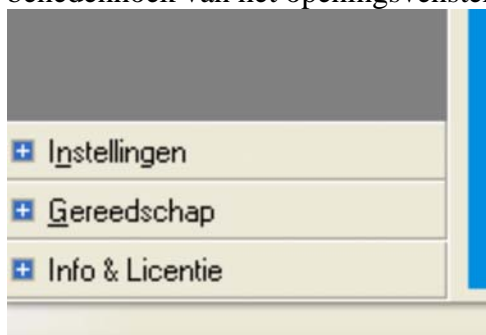
Ga, in de menubalk bovenin Spybot S&D, naar **Modus** en klik op **Geavanceerde modus**.



Lees het waarschuwingsvenster en klik op **Ja** indien je wil doorgaan.



De geavanceerde modus is nu actief. Dat zie je aan de extra tabbladen in de linker benedenhoek van het openingsvenster.



We behandelen deze in aflopende volgorde.

a. Instellingen:

Klik op de functieknop “**Instellingen**”.

Zo krijgen we dit te zien:

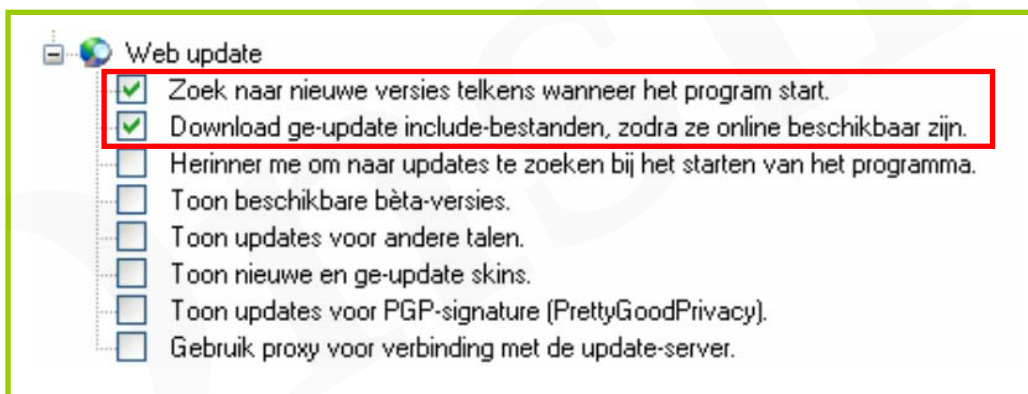
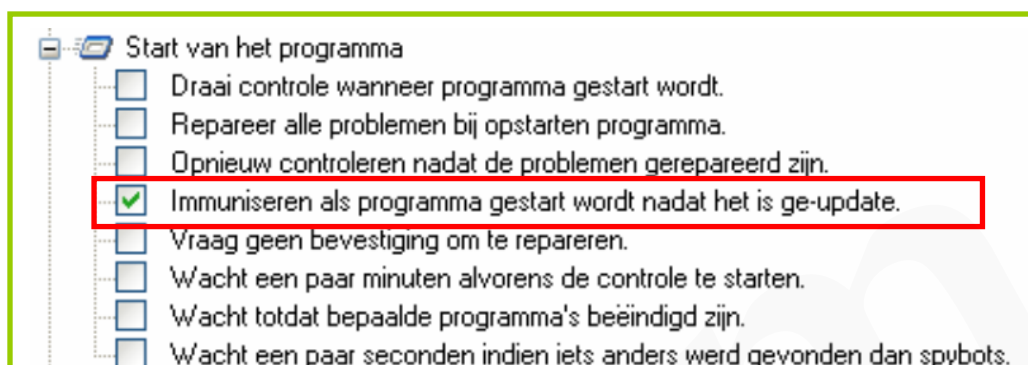
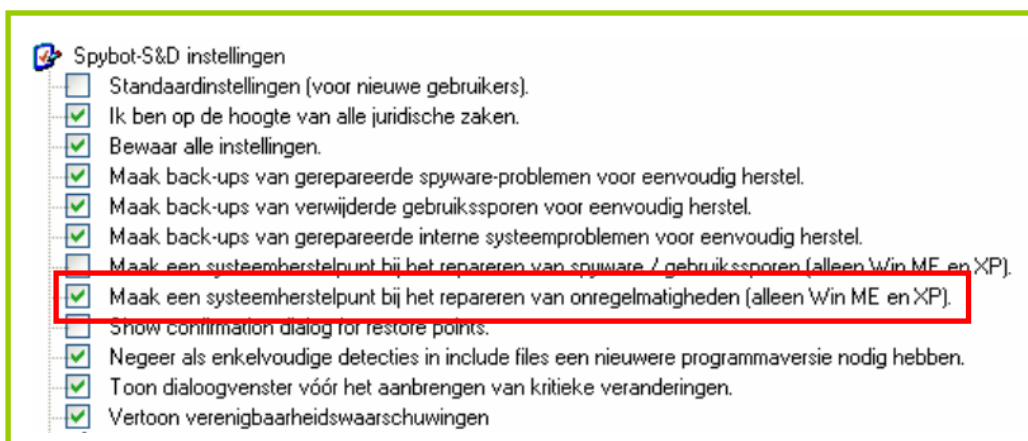


Hiervan behandelen we de onderdelen **Instellingen**, **Mappen** en **Taakplanner**.

Je kunt deze onderdelen openen door ze, links in de donkere balk, aan te klikken.

Instellingen:

Standaard staan hier die instellingen goed. Er kunnen echter nog enkele handige functies extra aangevinkt worden. In onderstaande afbeelding zijn deze herkenbaar aan de **rode** omkadering.



Deze laatste twee items zorgen er voor dat er, bij het starten van Spybot, automatisch naar updates wordt gezocht. Indien er beschikbaar zijn dan zullen deze ook gedownload worden. Bij het selecteren van het eerste item krijg je de waarschuwing dat dit enkel zinvol is indien je over een permanente Internetverbinding beschikt. Klik op **JA** om door te gaan.

Indien er een **volledige nieuwe versie** ter beschikking is dan zal deze automatisch aangeboden worden, ook al zijn bovenstaande items niet aangevinkt. Vaak komt dat op een ongelegen moment. Druk in dergelijk geval in de setupwizard op **Cancel** en vervolgens op **Ja**, om de Upgrade nog niet te laten doorgaan. Download en installeer de nieuwe versie, op een voor u geschikter ogenblik. Zie hoofdstuk 1: [Downloaden, installeren en gebruiksklaar maken](#).

Mapperen

Standaard worden de bestanden die je download, zowel via Internet Explorer als via Firefox, op je bureaublad geplaatst. **Spybot S&D** biedt je de mogelijkheid om die

locatie hier toe te voegen zodat Spybot hierop een installeerscan uitvoert. **P2P programma's**, zoals bv LimeWire, hebben hun eigen downloadmap. Ook deze kun je aan de lijst toevoegen.

Klik met de rechtermuisknop in het witte veld en kies “**Voeg een map toe aan deze lijst**”.



Selecteer “**Bureaublad**” en klik op **OK**



Zie hier het resultaat:



Je kunt deze lijst op dezelfde wijze uitbreiden door andere mappen, waar gedownloadde bestanden in opgeslagen worden, aan deze lijst toe te voegen.

Om een map uit de lijst te verwijderen klik je met de rechtermuisknop op dat bestand kies voor “**Verwijder de geselecteerde map uit de lijst**”.

Taakplanner.

Deze functie biedt de mogelijkheid om een scantaak te plannen zodat deze automatisch wordt uitgevoerd in overeenstemming met de instelling die je gedaan hebt. De instellingsmogelijkheden zijn zeer uitgebreid. Laten we het in dit voorbeeld bij een eenvoudige instelling houden.

Klik op toevoegen om een taak in te stellen.



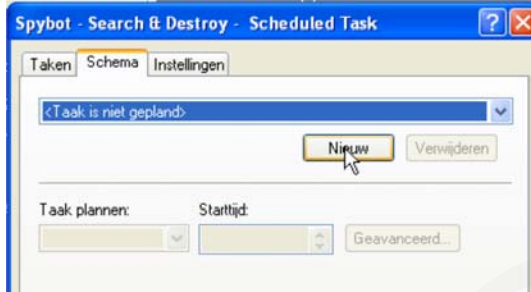
Vink deze twee items aan, zoals in onderstaande afbeelding is weergegeven:



Klik op “**Bewerken**”.



Klik op het tabblad “**Schema**” op “**Nieuw**”.



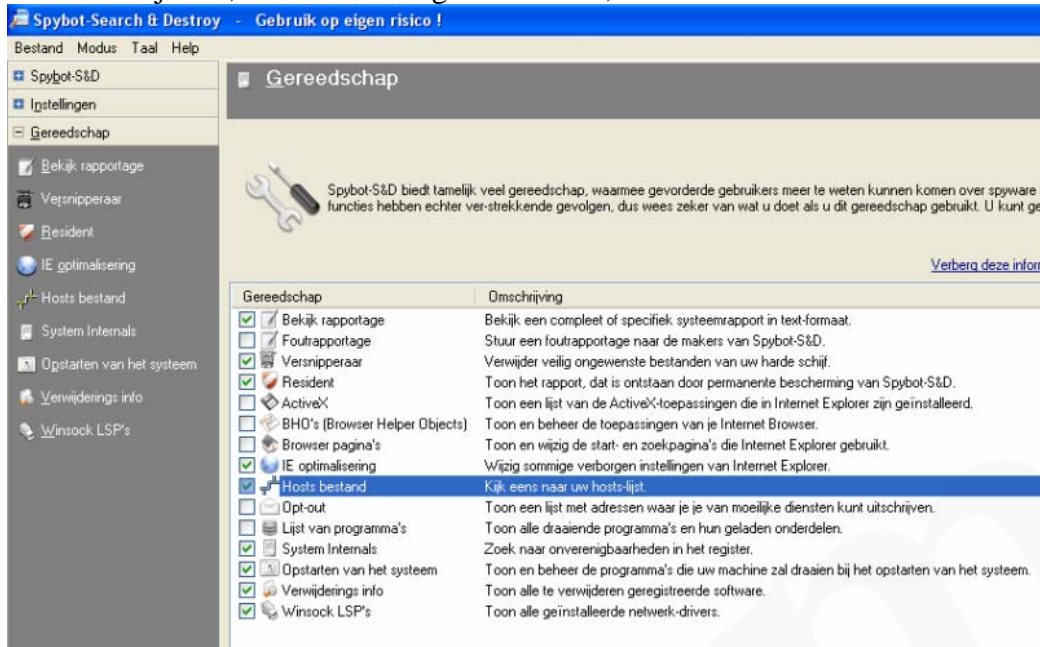
Stel de taak in naar eigen voorkeur en klik op “**Toepassen**” en vervolgens op **OK**. Hier een voorbeeld van een wekelijkse scantaak.



De taak is nu ingesteld.

b. Gereedschap:

Klik op de functieknop “Gereedschap”. Aan de standaard instellingen voegen we er nog één toe. Namelijk het, hier als blauw geselecteerde, **Host bestand**.



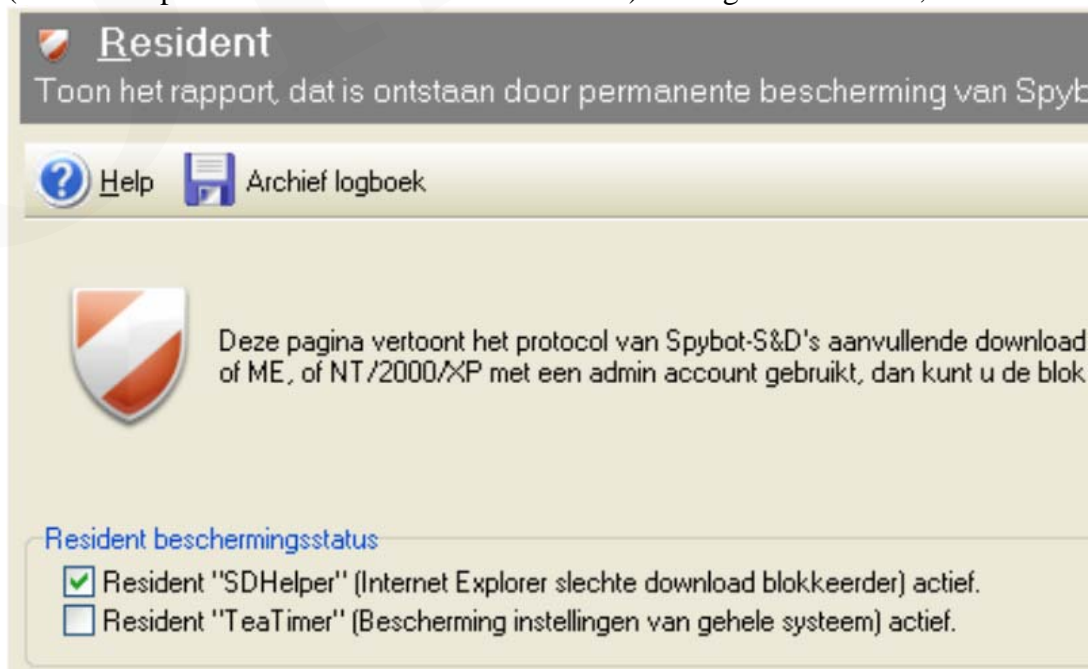
Van de onderliggende onderdelen gaan we er drie behandelen. **Resident**, **IE Optimalisering** en **Host bestand**. De overige zijn voor de experts onder U.

Je kunt deze onderdelen openen door ze, links in de donkere balk, aan te klikken.

Resident

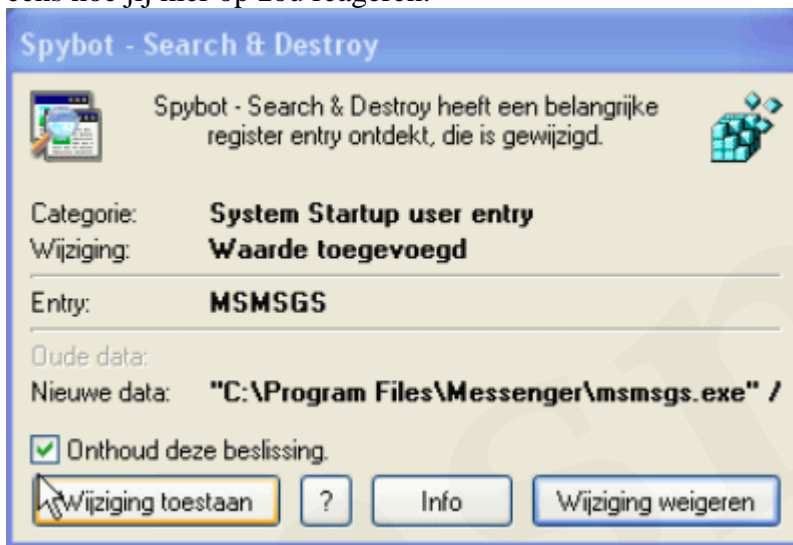
Hier zijn twee functies ter beschikking

Indien je de installatiehandleiding goed gevolgd hebt dan staat de “SDhelper” (Internet Explorer slechte download blokkeerder) al aangevinkt. Zoniet, vink deze aan.

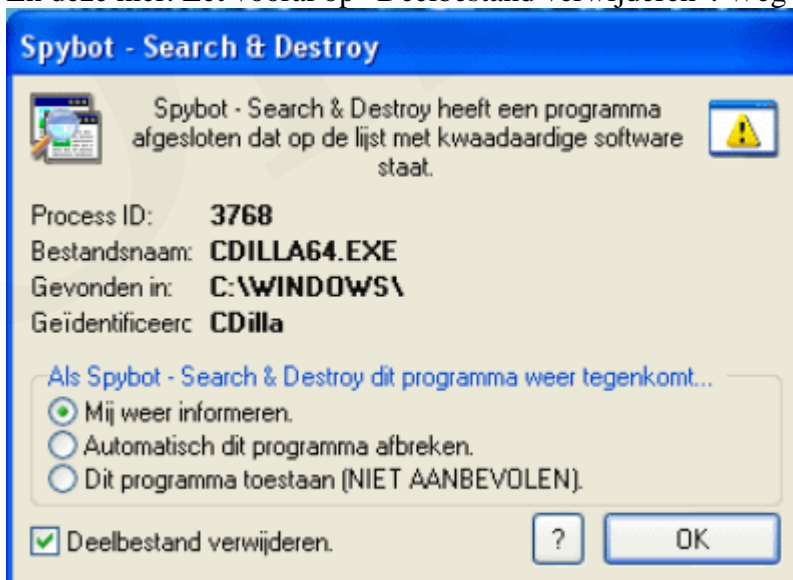


Tijdens de installatie heb ik het advies gegeven om de **TeaTimer** niet in te schakelen. Daarom staat deze hier nu ook niet aangevinkt. **TeaTimer** is de real-time protectie van Spybot-Search & Destroy. Er wordt dan permanent gescand op kwaadaardige processen die willen opstarten

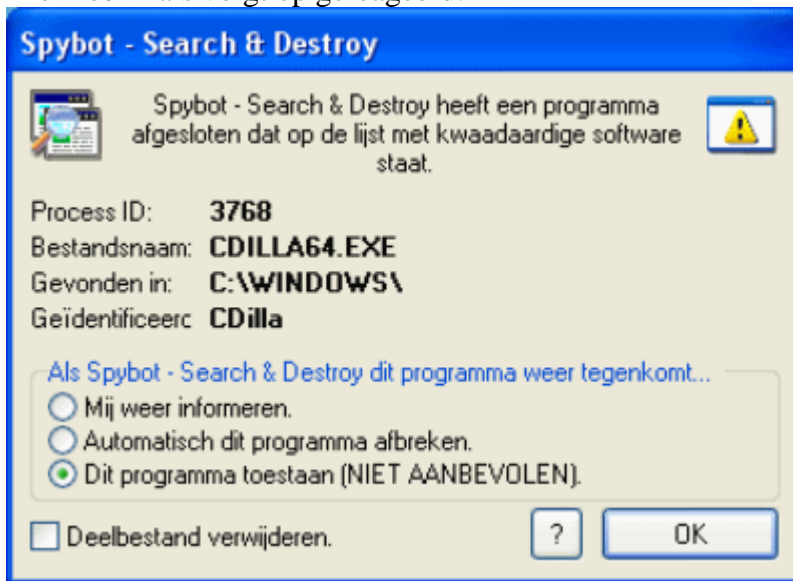
Wanneer TeaTimer ingeschakeld is krijg je namelijk een melding wanneer bepaalde registersleutels gewijzigd worden. Het gaat om registersleutels die vaak (niet altijd dus !!!) door malware gebruikt worden. Je krijgt de keuze om deze registerwijzingen toe te staan of te weigeren. Hetzij eenmalig, of voor altijd (Zie "Onthoud deze beslissing"). Het is voor velen echter altijd niet gemakkelijk om hier de juiste beslissing te nemen, want het gaat niet altijd om een kwaadaardige registerwijziging. Indien je een goedaardige registerwijziging blokkeert dan gaat de betreffende toepassing vaak niet meer werken. Hier enkele voorbeelden van TeaTimer-meldingen. Oordeel zelf maar eens hoe jij hier op zou reageren.



En deze hier. Let vooral op "Deelbestand verwijderen". Weg is weg hé !!!



Hier heb ik als volgt op gereageerd:



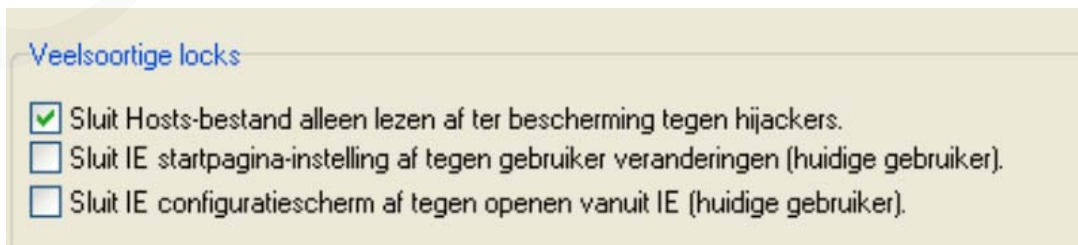
Indien ik dit niet toegestaan had dan zou het programma AutoCAD niet meer gewerkt hebben.

In dit geval wist ik “toevallig” dat deze met AutoCAD te maken had, hoewel CDILLA soms ook kwaadaardig kan zijn.

Een andere reden om TeaTimer NIET in te schakelen kan zijn dat je computer al real-time beschermd is via een ander programma, zoals bv SpywareBlaster, SpywareGuard, WinPatrol, Windows Defender, enz. Het is bekend dat real-time functies van verschillende programma's met elkaar kunnen conflicteren. Welke wel, en welke niet goed samen gaan is moeilijk te zeggen omdat die programma's voortdurend wijzigingen ondergaan. Op dit ogenblik werkt TeaTimer bv goed samen met SpywareBlaster en in Vista zeker ook met Windows Defender.

Opgelet: TeaTimer kan veranderingen die je op je systeem zelf aanbrengt (bv het fixen in hijackthis) terug ongedaan maken. Daarom is het soms nodig om deze functie tijdelijk uit te schakelen om registerwijzigingen door te laten. Klik [hier](#) om te weten hoe je dat doet.

IE Optimalisering

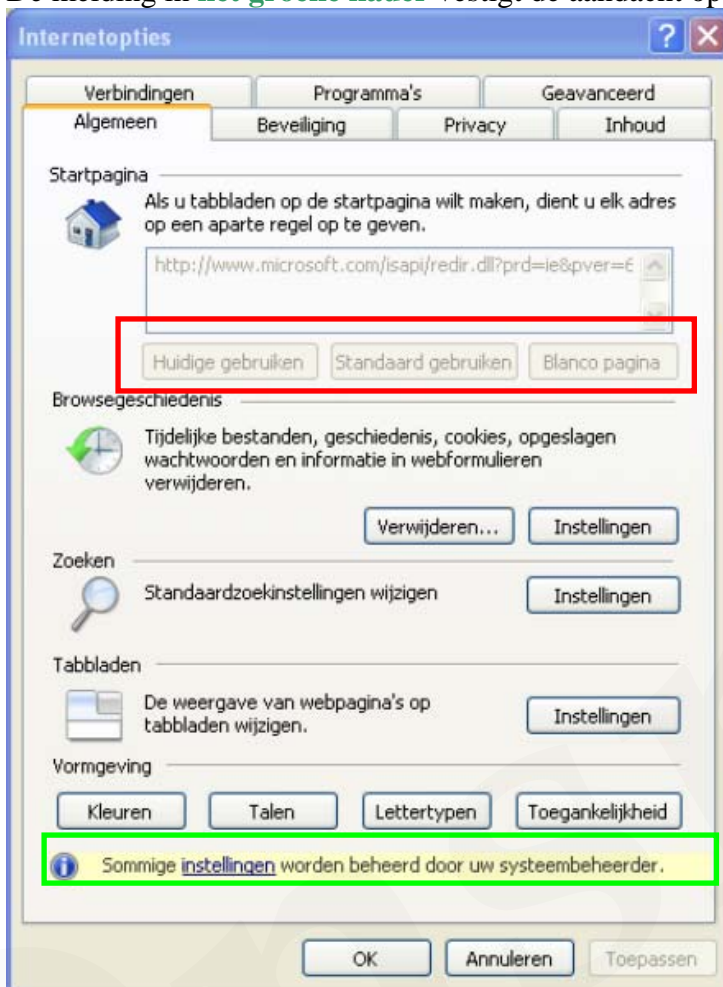


Deze functie is dus enkel van toepassing voor Internet Explorer (IE).

Standaard is alleen de eerste lock (blokkering) aangevinkt.

Ook de tweede lock is onze aandacht waard. Indien je deze aanvinkt dan wordt het wijzigen van je startpagina, door kapers, in IE onmogelijk gemaakt. **Maar ook voor jezelf !!!**

Onderstaand zie je dat bij **Internetopties /Startpagina** de knoppen voor het instellen van de startpagina niet meer ter beschikking zijn. **Zie in rood kader.** De melding in **het groene kader** vestigt de aandacht op deze beperking.

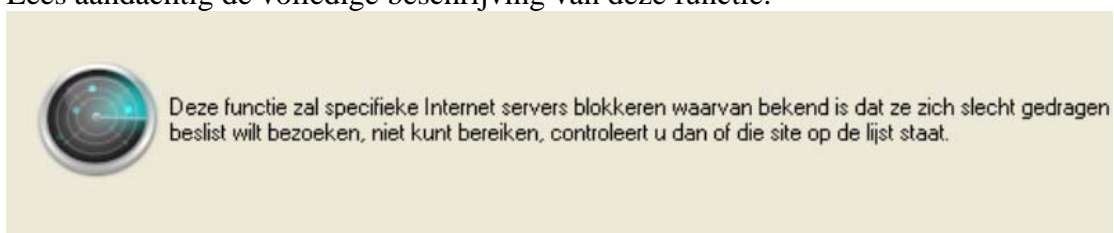


Je zult dus die startpagina-blokkering, tijdelijk moeten uitvinken wanneer je zelf graag je startpagina wenst te wijzigen. Dus uitvinken en Spybot afsluiten.

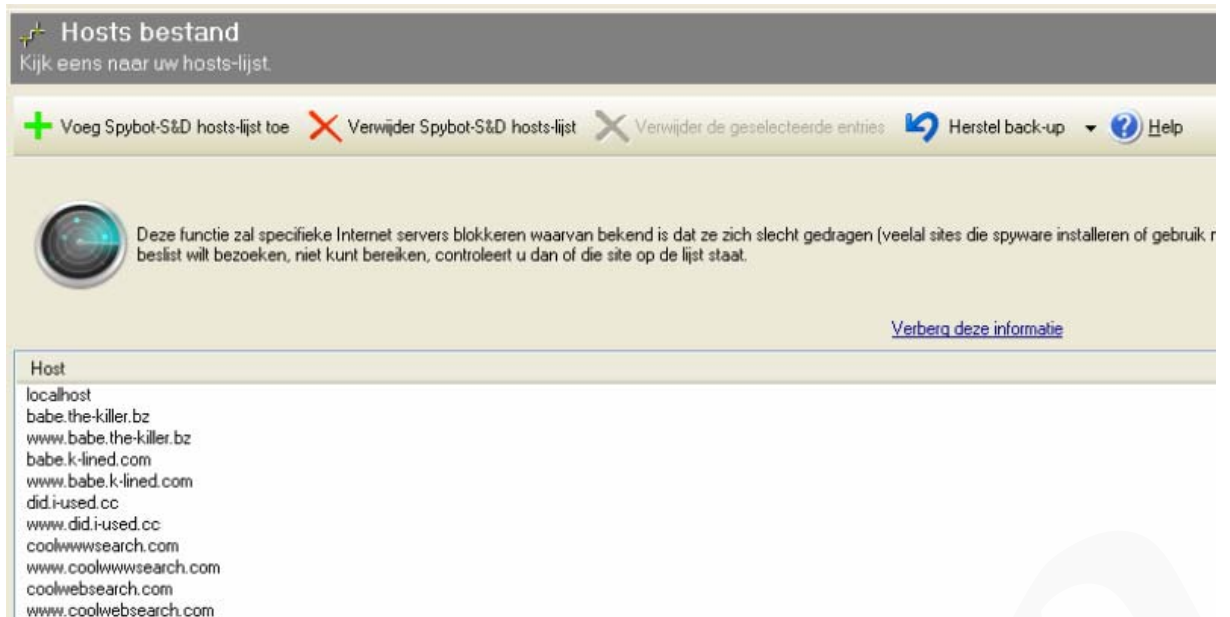
Opgelet: Indien je startpagina al door een ander beveiligingsprogramma bewaakt wordt, is het niet verstandig hier van deze optie gebruik te maken. Populaire startpagina bewakers zijn bv **StartPage Guard** en **SpywareGuard**.

Host bestand

Lees aandachtig de volledige beschrijving van deze functie.



Om aan de bestaande lijst van gevaarlijke websites ook deze die door Spybot als zodanig gekend zijn toe te voegen klik je op de knop “**Voeg Spybot-S&D host-lijst toe**”



Goed om weten: Indien ook andere, minder deskundige, personen toegang hebben tot dit programma, dan doe je er goed aan om terug te keren naar de **Standaard modus**. Je instellingen blijven hoe dan ook van kracht.

c. Info & Licentie

Dit is enkel leesvoer.

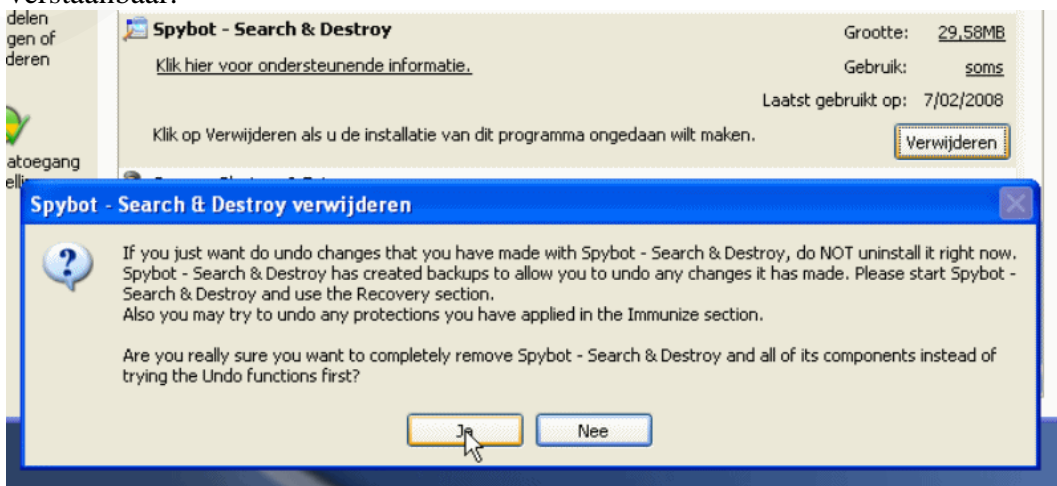
Naar begin

Naar "Scannen"

4. Spybot-Search&Destroy volledig verwijderen.

a. Vooraf uit te voeren !!!

- Maak een systeemherstelpunt. Klik [hier](#) om te weten hoe je dat doet.
- Sluit alle geopende toepassingen en vensters.
- **Waarschuwing:** Zodra je het programma wil verwijderen verschijnt er echter een waarschuwingsvenster. Helaas helemaal in het Engels en dus niet voor iedereen verstaanbaar.



Hier de vertaling:

Indien je met Spybot-S&D wijzingen hebt aangebracht aan uw systeem, verwijder het dan nu nog niet.

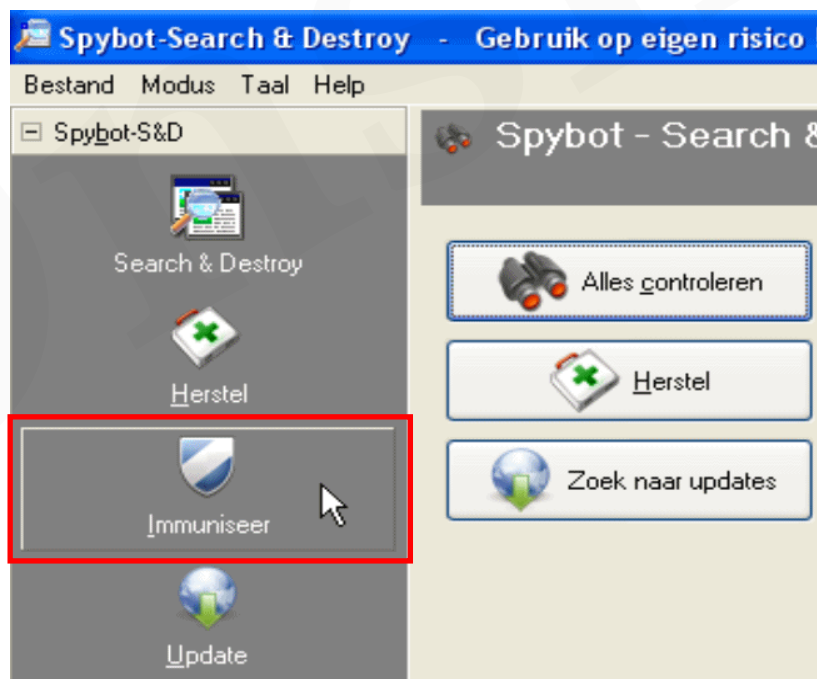
Spybot-S&D heeft backups gemaakt waarmee je eerder gemaakte wijzingen kunt herstellen. Start a.u.b. Spybot-S&D en gebruik de Herstel functie.

Schakel tevens de beveiligingen die je ingesteld hebt in Immuniseren uit.

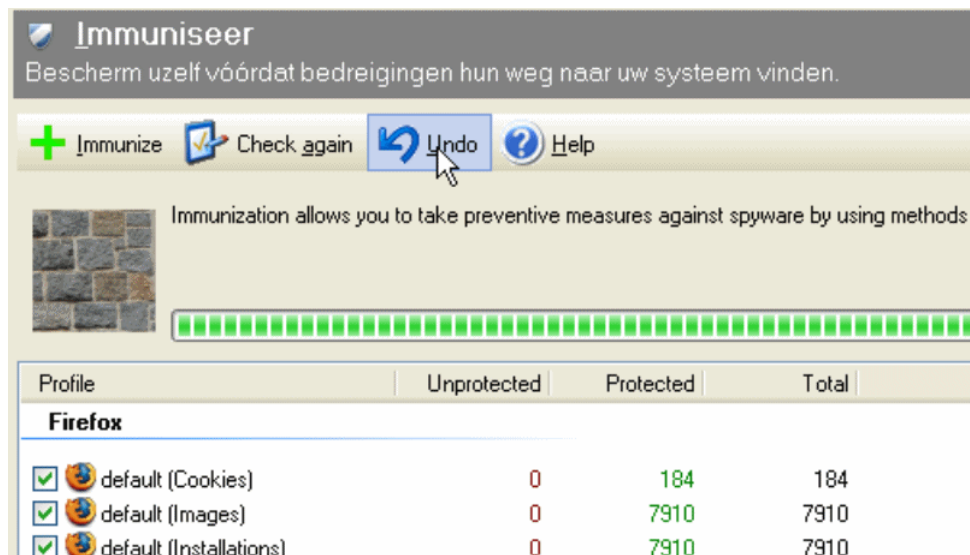
Ben je er zeker van dat je Spybot-S&D volledig wil verwijderen, met inbegrip van al zijn onderdelen en zonder rekening te houden met bovenstaande?

Hoe gaan we met deze waarschuwing om?

1. Het terugplaatsen van een backup is slechts aan te raden indien je nog maar net, na het runnen van een scan, gevonden bedreigingen hebt verwijderd en je nog niet de gelegenheid hebt gehad om na te gaan of deze actie slechte nevenwerkingen heeft op het algemeen functioneren van je computer (Windows en alle programma's). Indien je van oordeel bent dat je de laatste backup maar best eerst terugplaatst, ga dan naar **Goed om weten**, om te zien hoe je dat doet.
2. Het is zeker aan te bevelen om in de functie **Immuniseren** de beveiligingen op te heffen. Dat doe je zo:
 - Open Spybot-S&D.
 - Klik in het openingsvenster op de knop **Immuniseer**.



- Klik, in onderstaand venster, op de knop **Undo**.



- De beveiliging (Protected) zal op 0 gezet worden.



- Sluit Spybot-S&D

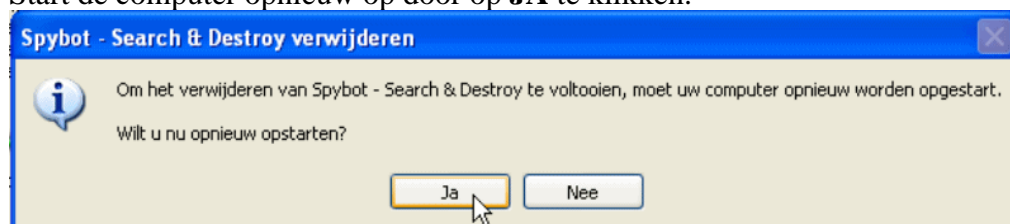
b. Verwijder het programma

Spybot-S&D kun je via verschillende wegen verwijderen. Ik geef hier enkel de twee mogelijkheden die Windows XP biedt.

Voer één van beide uit.

1. De minder gebruikte weg is deze: Ga naar Start -> Alle programma's -> Spybot-Search&Destroy -> **Uninstall Spybot-S&D**. Volg de aanwijzingen op het scherm.
2. De meest gangbare weg is deze: Ga naar Start -> Configuratiescherm -> Software. Selecteer in de lijst van geïnstalleerde programma's **Spybot-Search&Destroy** en klik op verwijderen.

Start de computer opnieuw op door op **JA** te klikken.



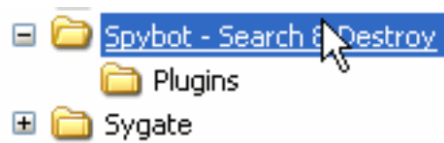
c. Verwijder achtergelaten sporen van het programma

Gebruik een betrouwbaar Clean programma, zoals bv CCleaner, om het register op te schonen. Volg daarvoor de handleiding van het programma.

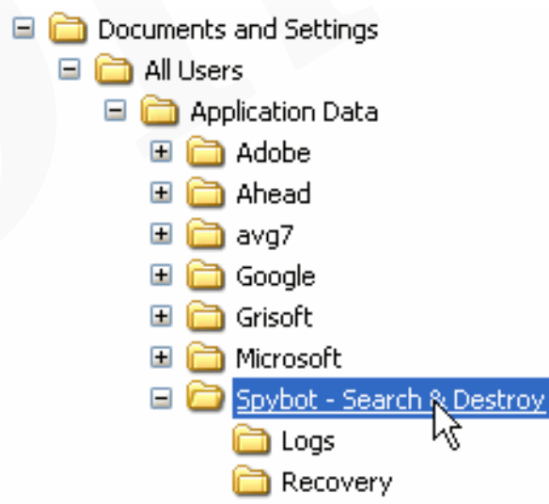
Dit volstaat om een nieuwe versie te kunnen installeren.

Voer wat volgt uit (Windows XP) indien je geen nieuwe versie van het programma wenst te installeren en dus definitief afstand doet van Spybot-S&D.

- Ga naar **Start** -> Deze computer -> Je Windows-schijf (meestal **C**) -> Program Files. Zoek de map **Spybot-Search&Destroy**.(zie afbeelding) en verwijder ze met de volledige inhoud. Indien dat niet lukt, verwijder dan eerst de inhoud van die map (Plugins enz.) en vervolgens de hoofdmap zelf. (In afbeelding met blauwe achtergrond)



- Maar er zit nog één en ander in een verborgen map wat ook nog moet verwijderd worden. Daarvoor moet je die map eerst zichtbaar maken. Klik [hier](#) om te weten hoe je dat doet.
- Ga nu naar **Start** -> Deze Computer -> Je Windows schijf (meestal **C**) -> Documents and Settings -> All Users -> Application Data. Zoek de map **Spybot-Search&Destroy**.(zie afbeelding) en verwijder ze met de volledige inhoud. Indien dat niet lukt, verwijder dan eerst de inhoud van die map (Logs enz.) en vervolgens de hoofdmap zelf. (In afbeelding met blauwe achtergrond)



- Maak nu de verborgen bestanden en mappen terug onzichtbaar. Kijk [hier](#) hoe je dat doet.
- Gebruik nogmaals een Clean programma om het register op te schonen.

Naar begin

5. Bijlage.

Een systeemherstelpunt maken.

In Windows XP

Klik op **START** -> Alle programma's- > Bureau-accessoires -> Systeemwerkset -> Systeemherstel.

Zet een vinkje (puntje) vóór "**Een herstelpunt maken**".

In de invoerbalk onder "Beschrijving van herstelpunt" geef je een herkenbare benaming in en klik op "**Maken**".

In Windows Vista

Klik op **STARTEN** (Vista logo, links onder) > Klik met de rechter muisknop op "**Computer**" -> Eigenschappen -> Klik, in de linker(blauw/gele) kolom, op "Systeembeveiliging".

Klik in het beveiligingsvenstertje op "**Doorgaan**".

Nu wordt het tabblad "systeembeveiliging" in het venster "Systeemeigenschappen" getoond.

Zorg er voor dat er een vinkje staat vóór de schijven of partitie's waarvan je een herstelpunt wil maken (Zie opmerkingen).

Klik op de knop "**Maken**". Geef het herstelpunt een herkenbare naam door deze in het invoerveld te typen en klik op de knop "**Maken**".

Zodra je de melding krijgt "Het maken van het herstelpunt is voltooid", klik je op **OK** om de procedure af te sluiten.

Sluit het venster "Systeemeigenschappen" door op **OK** te klikken.

Opmerkingen:

- Selecteer enkel de schijven of partities die bij de geplande actie betrokken zijn. Dat zal zeker al de partitie zijn waarop Vista geïnstalleerd is (meestal de je C-partitie) en mogelijk ook je DATA-partitie.

- Systeemherstel biedt geen bescherming voor FAT32- en andere FAT-schijven omdat FAT-schijven het gebruik van schaduwkopieën niet ondersteunen.

- Als u een eerdere versie van Windows (bv Win XP) start op een systeem waarop u gebruikmaakt van een dual-bootconfiguratie, worden de herstelpunten die door de huidige versie van Windows (Vista) zijn aangemaakt door de eerdere versie verwijderd.

Naar begin

Naar "spybot verwijderen"

Verborgene bestanden en mappen weergeven (zichtbaar maken).

Ga naar Start en klik op Deze computer.

In de menubalk selecteer je Extra en dan Mapopties.

Selecteer de tab "Weergave".

Haal het vinkje weg bij "Beveiligde besturingssysteembestanden verbergen (aanbevolen)".

Klik in het waarschuwingsvenstertje op JA om dit te bevestigen.

Scroll nu naar beneden naar het gele mapje "Verborgene bestanden en mappen".

Selecteer (groen puntje plaatsen bij) Verborgene bestanden en mappen weergeven.

Klik achtereenvolgens op "Toepassen" en op "OK."

Naar begin

Naar spybot verwijderen

Verborgen bestanden en mappen terug onzichtbaar maken.

Ga naar Start en klik op Deze computer.

In de menubalk selecteer je Extra en dan Mapopties.

Selecteer de tab “Weergave”.

Plaats een vinkje bij “Beveiligde besturingssysteembestanden verbergen (aanbevolen)”.

Scroll nu naar beneden naar het gele mapje “Verborgen bestanden en mappen”

Selecteer (groen puntje plaatsen bij) “Verborgen bestanden en mappen niet weergeven”.

Klik achtereenvolgens op “Toepassen” en op “OK.”

[Naar begin](#)

[Naar spybot verwijderen](#)

TeaTimer uitschakelen

1. De functie uitschakelen
 - Start Spybot-S&D.
 - Enkel indien deze uitgeschakeld is. Ga naar Modus -> selecteer Geavanceerde modus.
 - Ga naar **Gereedschap** en klik op het **Resident** in de lijst.
 - Haal het vinkje weg bij Resident “TeaTimer”.
 - Sluit Spybot-S&D.
2. Herstart je PC.
3. Download vervolgens [ResetTeaTimer.bat](#) naar je Bureaublad.
Opgelet: Deze koppeling werkt mogelijk niet indien Internet Explorer je standaard browser is. Klik eventueel met de rechter muisknop op de koppeling en kies “Koppelingslocatie kopiëren”. Plak deze in de adresbalk van Internet Explorer en klik ENTER.
Dubbelklik op het bestandje **ResetTeaTimer.bat** om alle entries (geschiedenis) in TeaTimer te verwijderen.

[Naar “Gereedschap/TeaTimer”](#)

[Naar begin](#)