Met dit schrijven ontvangt iedereen onze 4de nieuwsbrief van 2009. Laten we eerst beginnen met de laatste vernieuwingen op Antivirus- en Antispywaregebied.

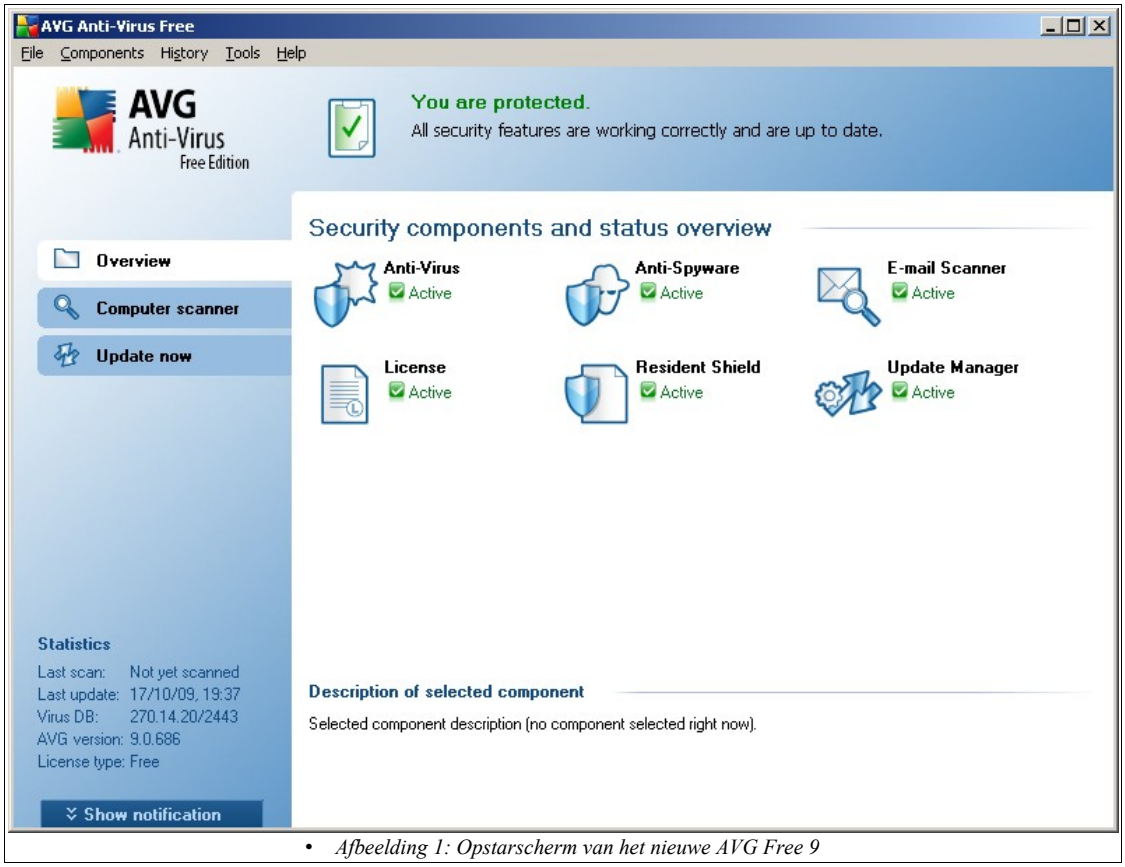
AVG free 9.0

Vanaf 1 December wordt AVG Free 8.5 niet meer verder ontwikkeld. Of er daarna ook nog antivirusdefinities zullen blijven verschijnen voor deze versie is onwaarschijnlijk. Zodoende raden we iedere gebruiker van dit programma aan om voor 1 December al te upgraden naar AVG free 9.

Er is wel 1 probleem. AVG free 8.5 en 9 werken vanaf Windows XP SP2 tot en met de allernieuwste Windows 7. Mensen die vandaag de dag nog steeds met een oudere Windows XP werken zijn nu genoodzaakt om hun versie (XP zonder SP, SP1 en SPS1a) te updaten tot minimaal SP2. Of je blijft AVG free 7 gebruiken zonder allerlaatste virusdefinities. Voor alle duidelijkheid: Windows XP SP3 is de laatste versie van Windows XP.

De volgende vernieuwingen zijn in AVG Free 9 geïmplementeerd. Je hebt niet alleen basis-antivirusbescherming maar vanaf nu eveneens basis anti-spywarebescherming en bovendien basis Rootkit-bescherming. We kunnen dus stellen dat AVG nu een volwaardige (basis) bescherming biedt. Je kan dus eventueel AdAware verwijderen en enkel AVG als bescherming gebruiken. Rootkit bescherming is een functie die voordien enkel in de koopversie van AVG zat.

Zoals gewoonlijk bieden wij een aangepaste versie aan zonder linkscanner en zonder toolbar. Deze versie werkt ietwat sneller dan de “gewone” downloadversie (vooral tijdens het surfen).



- *Afbeelding 1: Opstarscherm van het nieuwe AVG Free 9*

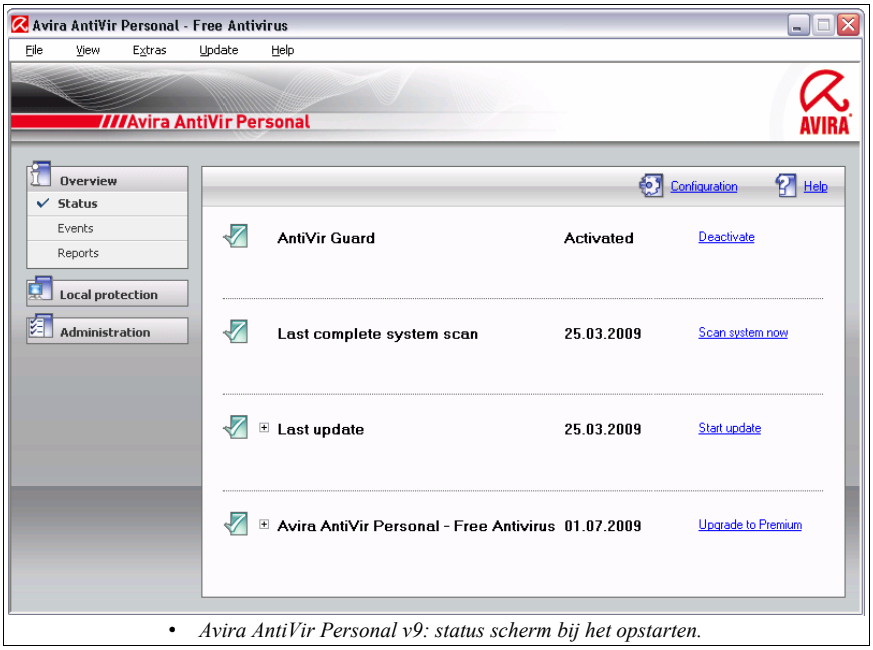
Ad-Aware Free

Ook Lavasoft heeft een nieuwe versie van dit programma uitgebracht. De laatste versie doet eveneens dienst als anti-virusprogramma. Dit is nog steeds een passief programma. Het meeste werk wordt gedaan bij het scannen van Uw PC en niet op de achtergrond zoals een actief Anti-spyware programma dat doet. De kritieken zijn nog steeds goed over Ad-Aware maar gezien vandaag de dag veel programma's elkaar overlappen wat functies betreft lijkt het ons nutteloos om Ad-Aware te gebruiken. Tenzij misschien als "backup-antivirus". De Antivirus motor van Ad-Aware wordt geleverd door Avira (een gekend gratis Antivirus-programma). Er zijn uiteraard nog steeds verschillen met het Avira programma zelf dat zelf nog steeds verkrijgbaar is, en welke in zijn laatste versie net zoals de AVG eveneens Anti-spyware bevat.

- *Ad-Aware Free: dit is het statusscherm dat U ziet bij het opstarten.*

Avira AntiVir Personal Edition

Hierboven is al wat geschreven over dit alternatieve anti-virusprogramma. Net zoals de nieuwste AVG Free heeft vanaf nu ook Antivir spyware en rootkitbescherming. Waardoor je vanaf nu in feite maar 1 programma nodig hebt voor zowel uw virus- als spywarebescherming. Avira staat bekend als een snel programma dat het systeem niet te zwaar belast. Alleen de updating van virusdefinities is soms wat traag bij de free-versie. Dit zou met deze nieuwe versie (v9.0.407) sterk verbeterd moeten zijn. Ook met dit antivirusprogramma heb je voor Windows XP minstens Service Pack 2 (SP2) nodig.



- *Avira AntiVir Personal v9: status scherm bij het opstarten.*

Het lijkt erop dat het voor sommige mensen stilaan tijd wordt om hun oude PC te vervangen door een ietwat moderne PC met op zijn minst Windows XP SP2. Al is het alleen maar omwille van de beveiliging.

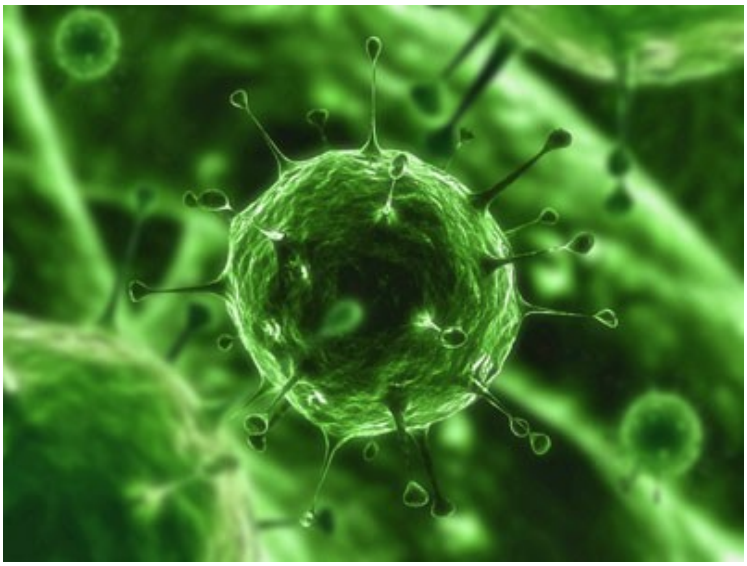
Ook deze versie kan men via Computerhelp bekomen. Voor meer informatie of om een afspraak te maken om uw beveiliging op punt te stellen kan U ons steeds contacteren op volgend nr.: **0495 22 19 74**

Polymorfische virussen

Onlangs stootten we op een nieuw soort virus. Een zogenaamd **polymorfisch virus**. Dit is een virus dat zichzelf (volgens een geprogrammeerd patroon) steeds veranderd. De eerste variant is **Vurit** ook bekend als **win32:virut** of **W32.Virut.A.** Er bestaan ondertussen ook al meerdere varianten zoals **W32.Virut.CF**. Dit virus werkt zoals een Rootkit-virus. Het plaatst zich op speciale plaatsen die worden geactiveerd tijdens het opstarten (o.a. in de Prullenbak). Het beschermt zichzelf via een aantal satellietprocessen en zorgt het er ook voor dat Antivirus programma's niet meer kunnen werken. Intussen worden allerlei programma's en bestanden aangetast. Bij verwijdering van een aantal geïnfecteerde bestanden zie je ineens een hele hoop virusprocessen in actie schieten waardoor er nog meer gevaar binnenkomt. Het probleem is des te erger aangezien geïnfecteerde bestanden op zulke wijze worden beschadigd dat cleaning niet meer helpt.

Wat Virut zelf betreft dit plakt zich vast aan executables (**EXE**-bestanden), screensavers (**SCR**-bestanden) en **HTML**-bestanden. Het begint al wanneer het zich kopieert in een tijdelijk-bestand (**VRT7.tmp**) dat op een plaats word gezet waar normaal geen tijdelijke bestanden horen te zitten (SYTEM32). Het injecteert extra threads in het winlogon-process (het gedeelte dat voor het inloggen op de PC zorgt) en begint dan met andere tijdelijke bestanden te downloaden (**8.tmp en 9.tmp**). Van dan af gaat het zeer vlug. Het begint code van zichzelf in andere lopende processen en programma's te injecteren. Zoekt toegang tot bepaalde websites (de meeste zijn chinese websites en een paar uit polen) en probeert eveneens via bepaalde IRC-servers (o.a. irc.zief.pl uit polen) extra rootkit-virussen (zoals dit hier uit china “PRIVMSG [blocked] :!get http://horobl.cn/[blocked]/**0034.exe**”) binnen te halen.

De laatste varianten die eveneens HTML-pagina's aantasten injecteren extra data in het zogenaamde “iframe script”. Je kan deze pagina's wel herstellen door de extra script data uit het iframe te verwijderen maar andere bestanden opnieuw in orde te krijgen is heel wat moeilijker. Gezien dit virus bekend staat om bestanden zodanig kapot te maken dat ze zelfs na het verwijderen van het virus onherstelbaar beschadigt zijn. In de meeste gevallen zal Windows niet meer normaal of zelfs helemaal niet opstarten. Een volledig formattering van de harde schijf en herinstallatie is uiteindelijk de beste oplossing. Ook data die je nog probeert te “back-uppen” zal in vele gevallen besmet zijn. Let er vooral op dat wanneer je toch nog gegevens probeert te redden, je deze eerst met een goed werkende anti-virusscanner behandeld, voordat je deze begint terug te plaatsen.



Ik heb zelf gezien dat op de duur zelfs mijn eigen USB-stick zodanig was besmet geraakt, dat ik deze eveneens volledig heb moeten formatteren. **Dit virus is ZEER schadelijk**. De enige oplossing die garantie biedt dat het echt weg is, is een zeer drastische formattering met Windows-herinstallatie.

De onderstaande links geven nog meer informatie over dit virus (dat we dus zelf ook al tegenkwamen).

http://miekiemoes.blogspot.com/2009/02/virut-and-other-file-infectors-throwing.html#idc-ctools
http://www.symantec.com/security_response/writeup.jsp?docid=2009-020411-2802-99

en zelfs bij Microsof is dit polymorfisch virus bekend.

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=virus:win32/virut.bm

Solid State Disks

We eindigen met een positieve noot. Hierbij enige informatie over een nieuw fenomeen in het land van de opslagmedia, de Solid State Disc of afgekort SSD.

Jarenlang zijn mechanische vaste schijven de vaste partner geweest van menig PC. Doch daar begint langzaam aan verandering in te komen. Enerzijds doordat vaste mechanische schijven toch nog altijd kwetsbaar zijn. Dit valt vooral op bij notebooks en netbooks gezien harde schijven hierin meer te verduren krijgen dan hun neefjes in vaste PC's. En anderzijds omdat op dit moment de processor-, videokaart- en geheugenperformance zo ver vooruit zijn dat de klassieke vaste schijf een serieuze bottleneck aan het worden is. Een sneller en vooral minder kwetsbaar medium moest gevonden worden. Nu zijn solid state schijven niet echt een nieuwigheid. Ze bestaan al jaren in de muziekwereld. Alle bekende synthesizers maakten (en maken) gebruik van solid state disks om hun data op te slaan. De naam “solid” staat hier voor solide wat vooral op een podium bij een optreden belangrijk is. Langzamerhand zijn ze ook beginnen doordringen op de PC markt. Namelijk bij de introductie van de Netbook laptop, amper 2 jaar geleden, die eerste modellen waren uitgerust met compacte Solid State Discs (SSD). Compact in de zin van zeer beperkte opslagcapaciteit (4GB) ten opzichte van traditionele mechanische harde schijven.

De volledige interne werking van een SSD gaan we hier niet uitleggen maar het komt erop neer dat een SSD geen bewegende delen heeft zoals een mechansiche harde schijf. Er zit zelfs helemaal geen schijf in, geen motors die de schijf doen draaien of de lees/schrijfkop moeten bewegen. In feite bestaan SSD's uit geheugen. De huidige generatie bestaat uit: NAND-flash-chips (zoals bij een USB geheugenstick). Je kan flash-based Solid State Discs in 2 categorieën indelen. SLC (Single Level Cell) en MLC (Multi Level Cell). SLC slaan hun data op in 1 bit per cel terwijl MLC meer bits per cel kunnen bevatten. Hierdoor zijn MLC SSD's goedkoper te fabriceren dan SLC SSD's. Jammergenoeg ligt ook de performance wat lager hoewel daar de laatste tijd verandering in komt. SLC chips zijn veel duurder omdat je meer cellen nodig hebt voor eenzelfde MLC capaciteit. Daar staat tegenover dat SLC-chips een langere levensduur hebben dan MLC-chips. Doch met de laatste generatie MLC lijken de grenzen tussen SLC en MLC te vervagen wat prestaties en levensduur betreft.

Wat is het voordeel van een SSD?

Eerst doordat er geen bewegende onderdelen meer zijn, zal het apparaat minder snel defect gaan. Als je weet dat fabrikanten doorgaans een MTBF (Mean Time Before Failure = gemiddelde tijd voordat er fouten optreden) aanrekenen tussen 300'000 en 750'000 uren voor een mechanische harde schijf en dat bv. de OCZ Vertex 60GB Solid State Disc een MTBF heeft van 1'500'000 uren. Dan weet je dat het wel goed zit met de duurzaamheid.

Ten tweede doordat geheugen zeer snel toegankelijk is zijn er praktisch geen zoektijden (seek) noch accestijden. Ter vergelijking de gemiddelde seektime van een goede harde schijf is tussen de 14 en 10 milliseconden, De snelste mechanische schijf op dit moment haalt seektimes van rond 4.5 milliseconden maar die van de hierboven genoemde Solid State Disc heeft een seek-time van **minder dan 0.1 milliseconden**! Dat is onvoorstelbaar snel.

Bovendien verbruiken SSD's minder energie waardoor bijvoorbeeld de batterij van je laptop iets langer meegaat. Ter vergelijking. De snelste mechanische harde schijf verbruikt +6 watt terwijl de Vertex SSD ongeveer 2 Watt verbruikt.

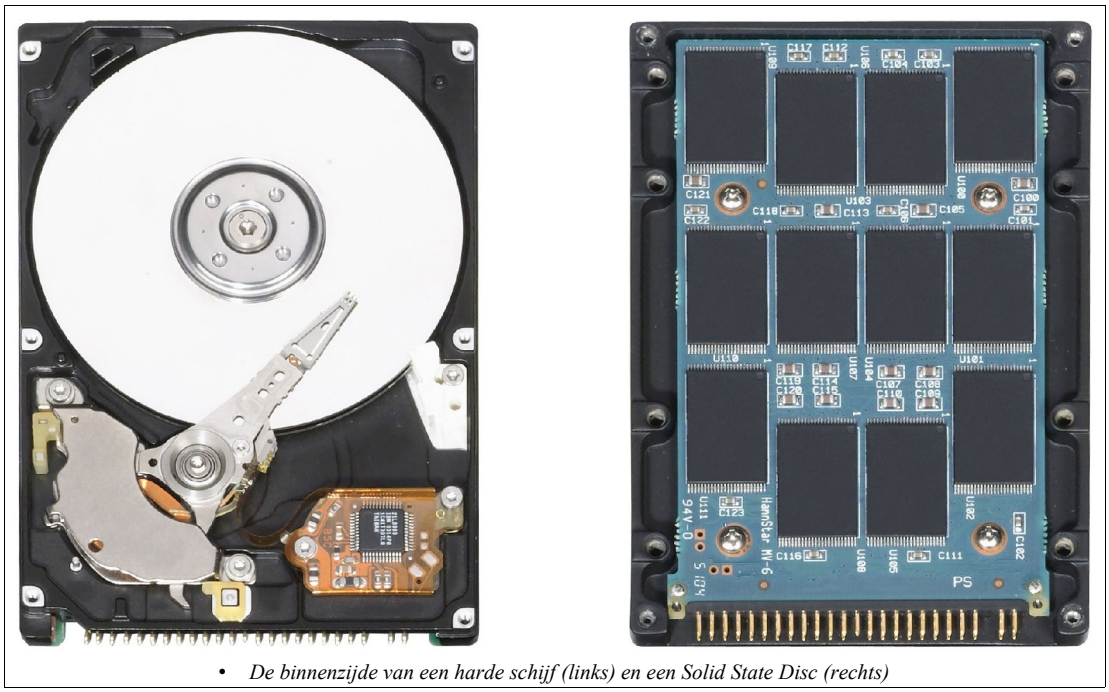
En dan zijn er nog de lees/schrijfsnelheden.

Een gewone harde schijf heeft leessnelheden tot ongeveer 50MB/s terwijl een SSD tot +200MB/s kan. Bovendien doordat er geen zoektijden meer zijn is data sneller gevonden waardoor alles veel sneller reageert, opstart en afsluit. Het verschil is fenomenaal. We hebben uitgemeten dat een goede SSD een Windows 7 systeem op ongeveer 45seconden opstart (inclusief het antivirusprogramma). Dezelfde PC met een mechanische schijf op 7200rpm en 8MB cache heeft voor dezelfde opstart bijna 2 minuten nodig (van aan/uitknop tot werkend bureaublad). Niet alleen het opstarten van je PC gaat sneller, ook het starten van programma's, bewaren van documenten, printen; alles waarbij je opslag nodig hebt gaat vliegensvlug.

Dit lijkt bijna te mooi om waar te zijn.

Er zijn natuurlijk ook nadelen aan SSD's. Enerzijds de hoge prijzen (de OCZ Vertex 60GB kost ongeveer 270 euro) en de grootste capaciteit die je op dit moment (moeizaam) kan verkrijgen is 250GB. En dan is nog het typische probleem van flash-geheugen. Namelijk je kan flash-geheugen maar beperkt volledig wissen en volledig beschrijven. Een harde schijf kan je miljoenen keer volledig opvullen en wissen, een flash geheugen (MLC) kan je maar 10'000 keer volledig opvullen en wissen. Dit ligt 10x hoger bij SLC Flash geheugen maar het probleem blijft. Je moet beseffen dat een SSD compleet anders werkt dan een mechanische harde schijf en ook in het gebruik zal je je moeten aanpassen. Natuurlijk zijn er allerlei mechanismes die dit probleem aanpakken. 1 ervan is het zogenaamde TRIM-commando dat o.a. vanaf Windows 7 wordt ondersteund. Een complexe berekening leert ons dat de levensuur alsnog 50jaar is (dit is veel langer dan de levensduur van andere componenten binnen in je PC). Bovendien wordt dit type geheugen al jaren gebruikt in GSM's, MP3-spelers (met flash geheugen) en niet te vergeten de eerste generatie van Netbooks die ondertussen ook al ruim 2 jaar meegaan (U weet wel die allereerste Asus Eee-PC 701 met 8 inch scherm).

We kunnen echt stellen dat een goede SSD de beste upgrade is die kan doen samen met Windows 7 (welke speciale functies heeft ingebouwd om de levensduur van een solid state disc nog te verbeteren; het zogenaamde TRIM-commando. De meeste SSD's zijn trouwens in 2.5” uitvoering. Ideaal om de huidige schijf van je laptop te vervangen door dit type van schijf. Voor desktop PC's bestaan er speciale 3.5” adapters zodat U de 2.5” SSD's ook in je desktop PC kan inbouwen. Wij kunnen U uiteraard alle informatie hierover verschaffen. Bel gerust: **0495 22 19 74**



- *De binnenzijde van een harde schijf (links) en een Solid State Disc (rechts)*