Prepareer een usb-stick om malware van iedere pc te verwijderen

# Malware verwijderen

Normaal gesproken start uw pc op vanaf een interne harde schijf. Het is echter prima mogelijk uw computer van een cd/dvd of zelfs van een usb-stick of externe harde schijf te starten. Er zijn verschillende scenario's denkbaar die zo'n alternatieve opstartmethode zinvol maken. In deze vijfdelige reeks gaan we precies op zulke scenario's in. In dit eerste deel pakken we malware aan.

Door Ignace de Groot

Tegenwoog elke moderne computer kan van uiteenlopende media opstarten, zoals een cd/dvd of een usb-stick. Wij kiezen voor een usb-stick omdat deze herschrijfbaar, robuuster, duurzamer en sneller is. Bovendien hebben niet alle computers nog een cd/dvd-station (denk aan netbooks). Maar waarom zou u een pc willen opstarten van een medium als een usb-stick?

## Opstarten vanaf usb-stick

Daar kunnen we verschillende redenen voor bedenken. Zo kan het gebeuren dat u een malware-infectie op uw systeem vermoedt, maar dat uw virusscanner niets verdachts aantreft of niet meer functioneert. Een mogelijke verklaring is dat de malware al actief is zodra u Windows opstart. Antivirussoftware opstarten vanuit een schoon systeem (zoals een besturingssysteem op een usb-stick) biedt dan uitkomst.

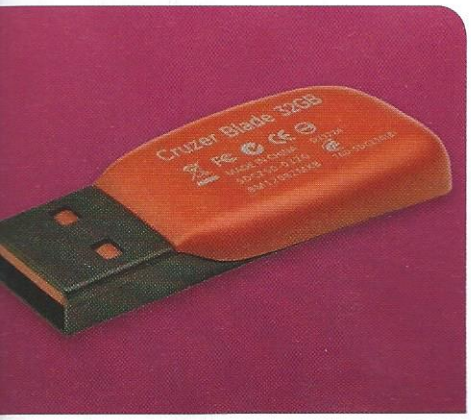
Een ander scenario: om een of andere reden wil Windows niet meer opstarten, zodat ook uw gegevens niet langer bereikbaar zijn. Ook dat laat zich wellicht oplossen met een opstartbare usb-stick. Andere redenen kunnen zijn: surfen en online bankieren zonder dat u hoeft te vrezen voor een besmet of gekaapt systeem, het BIOS of andere firmware 'flashen' met een tool die een DOS-omgeving vereist, een systeemprogramma uitvoeren dat niet werkt vanuit uw reguliere Windows-omgeving (denk aan een partitioneringsprogramma), een Linux-distributie uitproberen zonder die op uw harde schijf te installeren enzovoort.

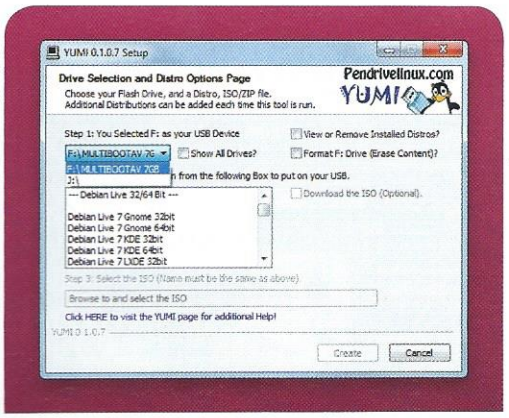
## Reeks

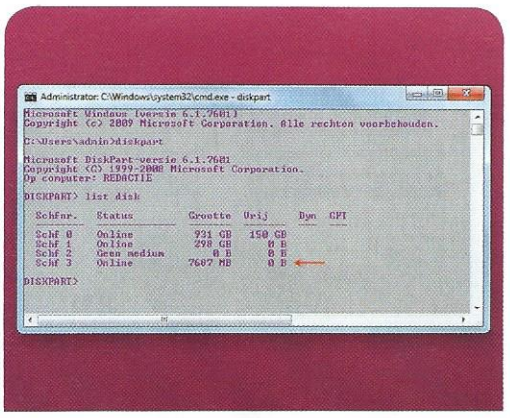
We zullen in de komende nummers verschillende van deze scenario's behandelen. Het opsporen en verwijderen van potentiële malware zoals rootkits is het onderwerp van dit eerste deel. Handig om achter de hand te hebben liggen in geval van narigheid, of wanneer u onverhoopt moet uitrukken om het systeem van familieleden of kennissen op te schonen.

In de komende edities van Computer!Totaal zetten we de workshopreeks voort en leggen wij u uit hoe u een usb-stick prepareert voor netwerk- en pc-analyse, veilig internetten, dataherstel en overige portabele apps.


*Een geprepareerde usb-stick: altijd handig om in de kast te hebben liggen!*




## 01 Stick kiezen

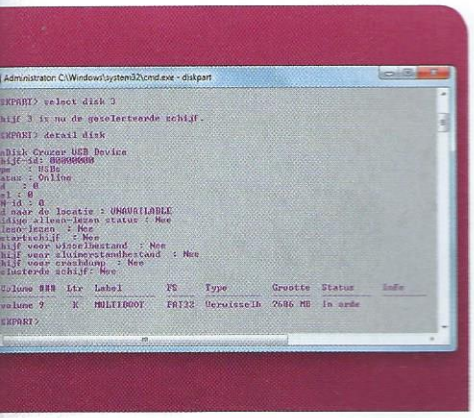
We gaan ervan uit dat u over een usb2.0-stick beschikt. De capaciteit hangt natuurlijk af van wat u op die k wilt plaatsen, maar voor onze doeleinden kiest u best voor een stick van 4 GB of meer (voor de prijs eft u het nauwelijks te laten: zelfs een 32 GB-stick dt u al vanaf circa 12 euro). Snelle leestijden zijn jd welkom en daar kunnen best wel opvallende schillen optreden. Op http://usbspeed.nirsoft.net dt u een overzicht en een tool om zelf de snelheid uw sticks te testen.

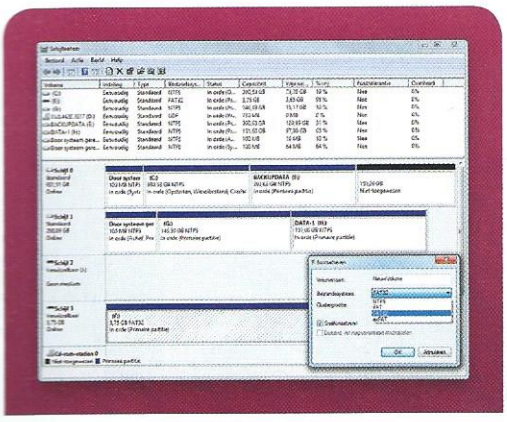
## 02 Opstartbaar maken

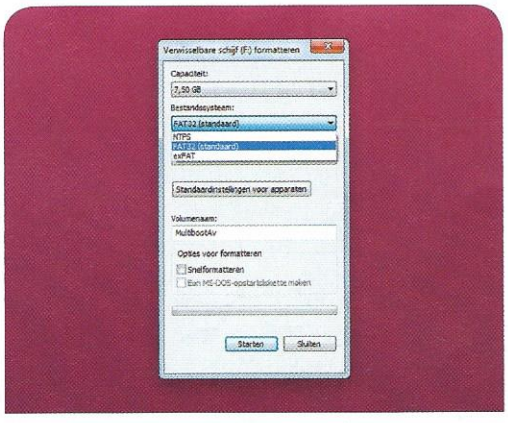
Er zijn diverse tools om een usb-stick opstartbaar mee te maken. Onze voorkeur gaat uit naar YUMI (Your Universal Multiboot Installer), met name vanwege het gebruiksgemak en de flexibiliteit. U vindt YUMI op http://ct.link.idg.nl/ymc. De tool heeft geen installatie nodig. Stop de stick in de pc, start YUMI op, ga akkoord met de gebruiksovereenkomst en verwijs naar de (juiste!) usb-stick in het uitklapmenu. Eventueel plaatst u eerst een vinkje bij **Showing All Drives**. Vink dan de optie bij **Format X: Drive** aan: alle data op de stick wordt gewist, zodat de stick schoon is.

## 03 Bij problemen

Meestal gaat u nu rechtstreeks van stap 2 naar stap 7, maar heel soms gaat er iets mis bij het formatteren in stap 2 en duiken er later bij het booten problemen op. In dat geval moet u iets meer moeite doen om de stick handmatig te formatteren. Start de opdrachtprompt als administrator: tik **cmd** in het Windows-startmenu in en bevestig met Ctrl+Shift+Enter. Daarna voert u het commando **diskpart** uit. Achter de nieuwe prompt voert u de opdracht **list disk** uit. Op basis van de grootte identificeert u vervolgens uw stick , het schijfnummer leest u in de kolom **Schfnr**.






## 04 Stick leegmaken

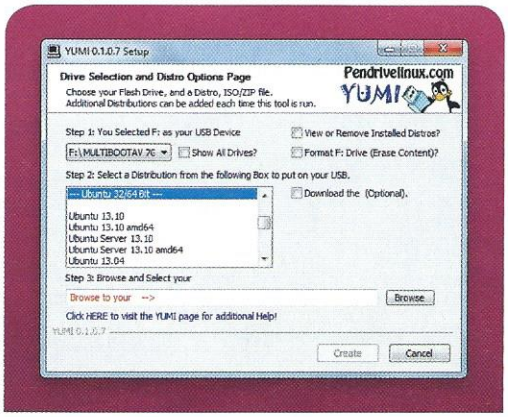
U selecteert uw usb-stick met de opdracht **select disk <schijfnummer>**. U krijgt vervolgens melding **Schijf x is nu de geselecteerde schijf**. ar het commando **detail disk** geeft u veel meer ormatie over uw usb-stick. De volgende stap is het schonen van de stick met het commando **clean** of, ndiger nog, met **clean all**. Met dit laatste commando overschrijft u namelijk alle sectoren, een proces echter lang kan duren.

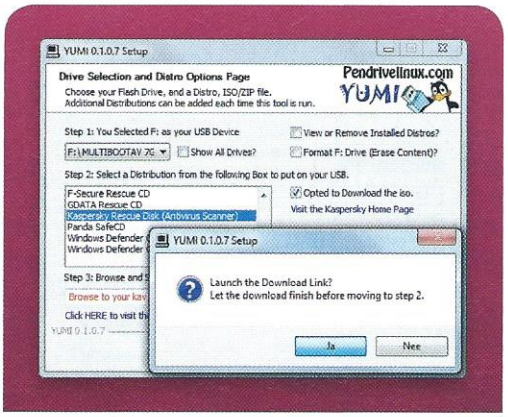
## 05 Bestandssysteem kiezen

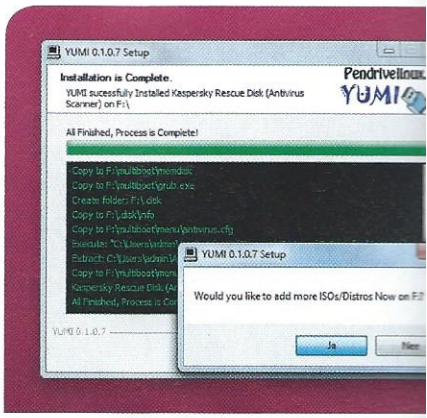
Er zijn verschillende bestandssystemen mogelijk waarin u de usb-stick kunt formatteren, waaronder FAT32 en NTFS. Een voordeel van NTFS is dat het bestanden van meer dan 4 GB aankan. Maar aangezien wij in de volgende stappen in een (grafische) Linux-omgeving werken, is NTFS geen echte optie. Linux vereist namelijk een FAT(32)-medium om te kunnen booten (en ook een UEFI-stick heeft FAT32 nodig, zie kader 'UEFI omzeilen'). Wij kiezen in daarom voor FAT32.

## 06 Stick formatteren

Voer de volgende drie commando's uit (telkens gevolgd een Enter): **create partition primary**, **assign**, **exit**. Er verschijnt nu een Windows-venster waarin u de knop **Schijf formatteren** aanklikt en bij **Bestandssysteem** de optie **FAT32 (standaard)** selecteert. Verwijder bij voorkeur het vinkje bij **Snelformatteren** en bevestig met **Starten**. Is de stick groter dan 32 GB, dan moet u uitwijken naar een gratis tool als FAT32 Format (http://ct.link.idg.nl/ftf). Gebruik tot slot het programma YUMI (stap 2) opnieuw, dit keer zonder vinkje bij de optie **Format X: Drive**.




## 07 Distributies bekijken

YUMI mag uw stick dan wel opstartbaar maken (lees: van een geschikte bootloader als grub en syslinux voorzien), daar hebt u natuurlijk niets aan als daar niet een of ander besturingssysteem aan gekoppeld is. Ook daarin voorziet YUMI. Meer zelfs, u kunt uit tientallen live-distributies kiezen, opgedeeld in diverse rubrieken. Zo tellen we bijvoorbeeld 76 Ubuntu-varianten, 35 systeemtools en 13 antivirustools. En wie heeft nagedacht over de 'M' in YUMI (van Multiboot) heeft wellicht begrepen dat we verschillende distributies op dezelfde stick kwijt kunnen.

## 08 Distributie selecteren

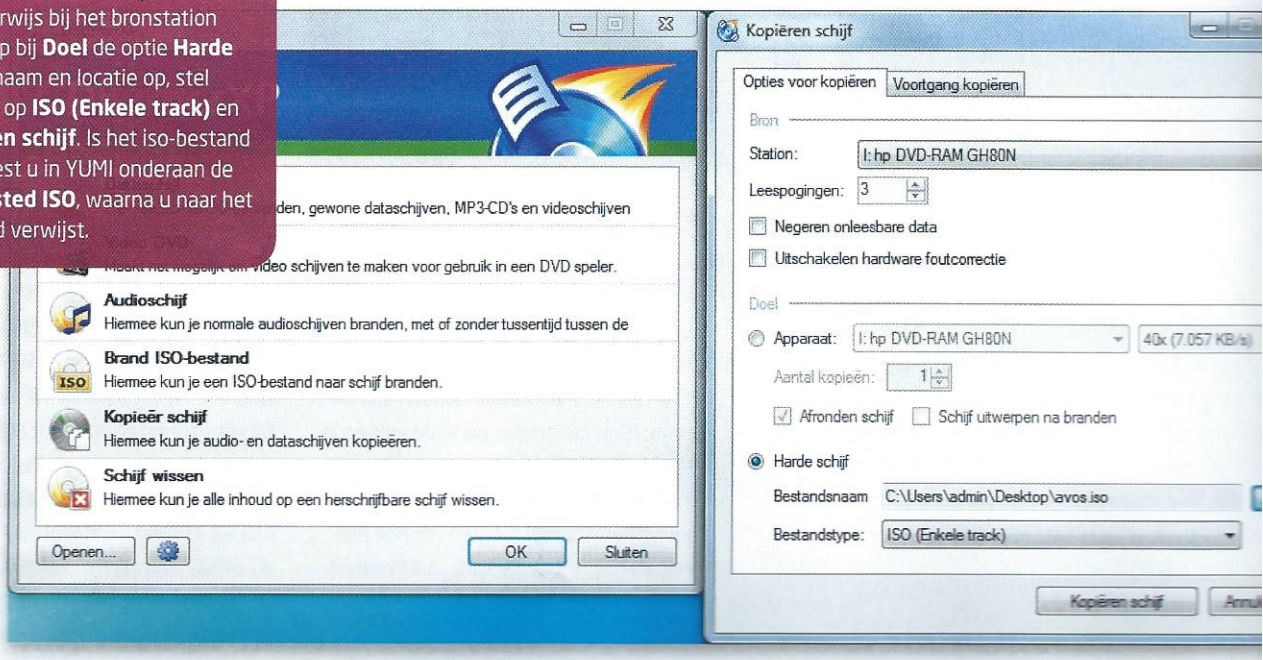
Bij het detecteren van potentiële malware is het zinvol meerdere antivirustools te proberen. Immers, wat de ene antivirustool mist, wordt wellicht opgepikt door de andere. Scrol dus naar de rubriek **Antivirus Tools** en selecteer alvast één antimalwaredistributie. Tot onze favorieten horen AVG Rescue CD, BitDefender Rescue Disk en Kaspersky Rescue Disk, maar het staat u vrij een andere distributie te selecteren. Wij beginnen met Kaspersky, waarna we een vinkje plaatsen bij **Download the iso**. Immers, het bijhorende iso-bestand staat nog niet op onze schijf.

## 09 Distributie toevoe

Bevestig de vraag of u de loadlink wilt lanceren met wacht tot de download is rond. Vervolgens klikt u op **Browse** en wijst u de weg naar het gedownloade iso-bestand. St dat eenmaal klaar, dan drukt u op de knop **Cre** bevestigt u uw beslissing. Het iso-bestand wo automatisch uitgepakt en aan uw stick toegev Na afloop drukt u op **Next** en bevestigt u met nog andere distro's aan uw stick wilt toevoege herhalen de procedure alvast voor AVG en Bit der. Na afloop sluit u YUMI af met **Finish**.

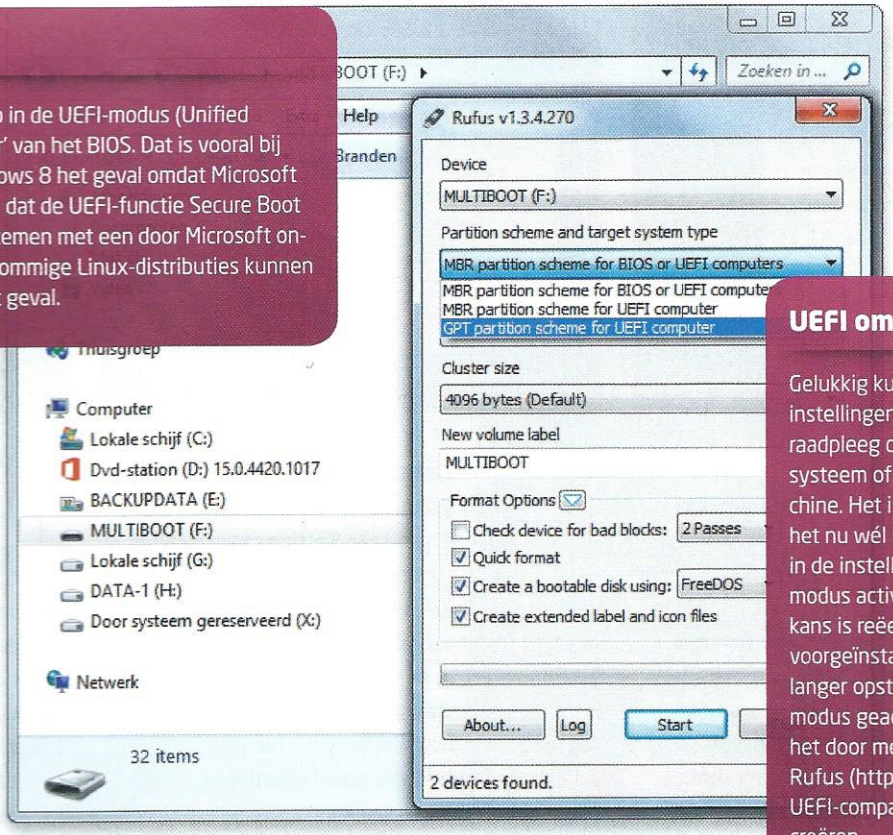
### Van dvd naar iso-bestand

YUMI kan zelf geen image maken van een opstartbare cd/dvd. Hiervoor hebt u een ander programmaatje nodig: CDBurnerXP (http://cdburnerxp.se). Stop de cd/dvd in het station, start de tool op en kies **Kopieer schijf** uit het menu. Druk op **OK**, verwijs bij het bronstation naar uw cd/dvd en stip bij **Doel** de optie **Harde schijf** aan. Geef een naam en locatie op, stel het **Bestandstype** in op **ISO (Enkele track)** en bevestig met **Kopiëren schijf**. Is het iso-bestand eenmaal klaar, dan kiest u in YUMI onderaan de lijst voor **Try an Unlisted ISO**, waarna u naar het gewenste iso-bestand verwijst.



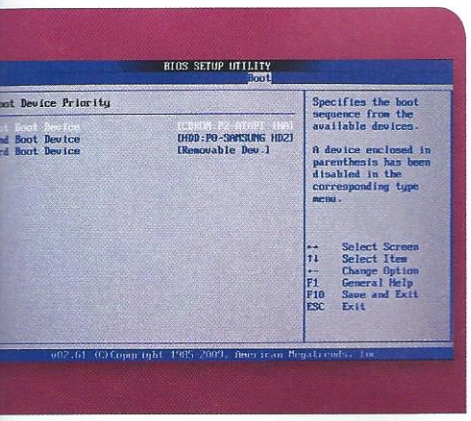
## UEFI-perikelen

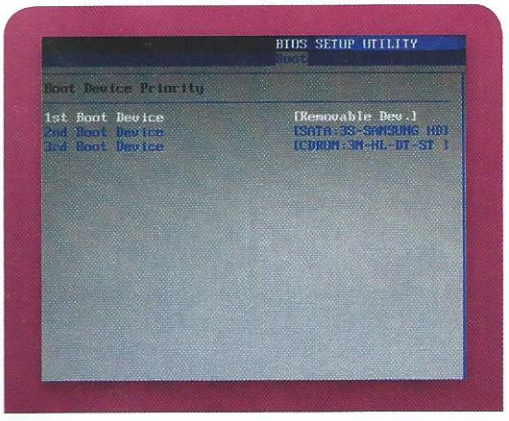
Veel nieuwe systemen starten standaard op in de UEFI-modus (Unified Extensible Firmware Interface), de 'opvolger' van het BIOS. Dat is vooral bij systemen met een voorgeïnstalleerde Windows 8 het geval omdat Microsoft dat zo voorschrijft. Microsoft eist bovendien dat de UEFI-functie Secure Boot is ingeschakeld, zodat alleen besturingssystemen met een door Microsoft ondertekende bootloader kunnen opstarten. Sommige Linux-distributies kunnen daarmee overweg, maar dat is niet altijd het geval.

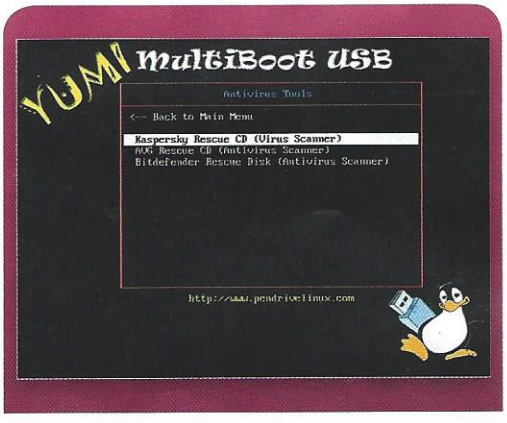



## UEFI omzeilen

Gelukkig kunt u Secure Boot in de instellingen van UEFI uitschakelen, raadpleeg de handleiding bij uw systeem of gebruik een zoekmachine. Het is echter niet zeker dat het nu wél lukt: mogelijk moet u in de instellingen tijdelijk de BIOS-modus activeren. Tijdelijk, want de kans is reëel dat in die modus een voorgeïnstalleerde Windows niet langer opstart. Of u laat de UEFI-modus geactiveerd en probeert het door met het programmaatje Rufus (http://rufus.akeo.ie) een UEFI-compatibele bootstick te creëren.




## 10 Bootmenu openen

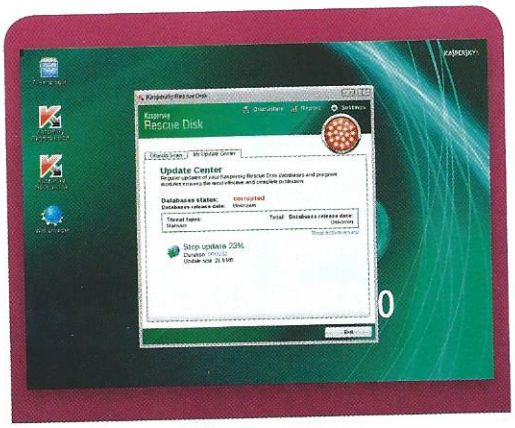
Het is nu de bedoeling dat u uw pc met deze usb-stick opstart. Afhankelijk van het systeem, vereist dat bepaalde handelingen. Bij de meeste moderne temen dient u tijdens het opstarten een of andere ts(combinatie) in te drukken om een speciaal bootnu op te roepen, waarin u dan te kennen geeft het araat vanaf de usb-stick te willen booten. Vaak is een functietoets als F10 of F12, maar de handling bij uw systeem vertelt u ongetwijfeld wat u cies hoort te doen.

## 11 Bootsequentie aanpassen

Het valt vooral bij oudere systemen niet uit te sluiten dat u het BIOS in moet om uw pc van een alternatief medium te laten opstarten. Meestal komt u in het BIOS door tijdens het opstarten op de Delete-toets te drukken. Eenmaal binnen gaat u op zoek naar een optie om de opstartvolgorde (boot sequence) aan te passen. Niet zelden is dat bij **Advanced BIOS features**. U zorgt er dan voor dat het usb-apparaat als eerste in de rij staat. Mogelijk omschrijft uw eigen bios dat als 'removable device' of 'external device'. Beschikt u over een UEFI-systeem? Lees dan het kader 'UEFI-perikelen' door.

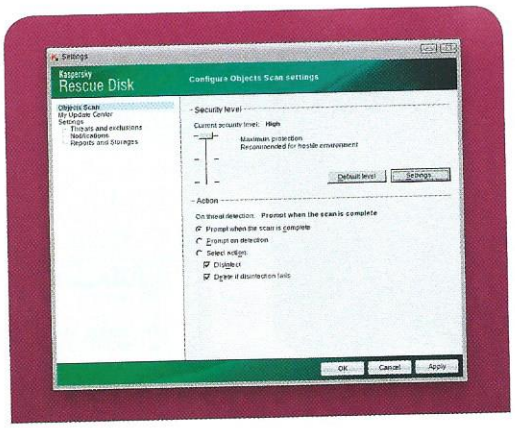
## 12 YUMI-stick opstarten

We gaan ervan uit dat u verschillende antimalware-distributies op uw stick hebt staan. Als het goed is, krijgt u dan een grafisch opstartmenu te zien waarin u als eerste optie alsnog de kans krijgt gewoon naar uw harde schijf door te starten. Dat is hier niet de bedoeling en dus kiest u voor de rubriek **Antivirus Tools**. Hier ziet u dan de geïnstalleerde distributies en hoeft u de gewenste distributie alleen maar te selecteren. Verder in dit artikel leggen we kort de werking van Kaspersky, AVG en BitDefender uit.



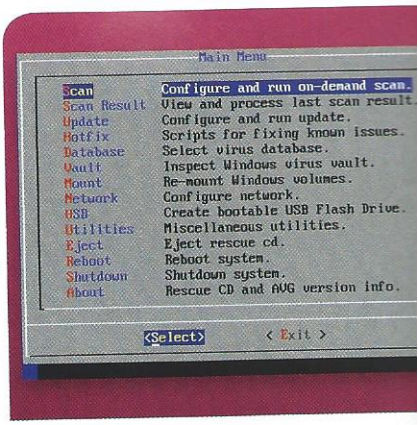

## 13 Kaspersky (1)

Na de keuze voor Kaspersky krijgt u meerdere mogelijkheden, waaronder de optie een hardware-informatietool te draaien of om Kaspersky in 'text mode' op te starten. Wij kiezen echter de bovenste optie: **Run Kaspersky Rescue Disk from this USB**. Even later start de tool op in een grafische desktopomgeving. Start hier Kaspersky Rescue Disk op en laat de tool eerst zijn databases updaten, via het tabblad **My Update Center**. Vervolgens hoeft u enkel de locaties aan te duiden die u wilt laten scannen. Dat doet u op het tabblad **Object Scan**, via de knop **+Add**.




## 14 Kaspersky (2)

Voor u de scan laat uitvoeren, doet u er goed aan **Settings** te selecteren. U kunt hier bijvoorbeeld de beveiliging verhogen en via de knop **Settings** duidelijk maken welke bestanden u wilt laten scannen. Op het tabblad **Additional** kunt u de scanmethode kiezen (**Signature** en/of **Heuristic Analysis**) en bij de heuristische scan de grondigheid instellen. Verder is het verstandig de optie **Prompt when the scan is complete** geselecteerd te laten, zodat u zelf kunt beslissen wat er met potentiële malware moet gebeuren: in quarantaine plaatsen, desinfecteren of desnoods verwijderen.

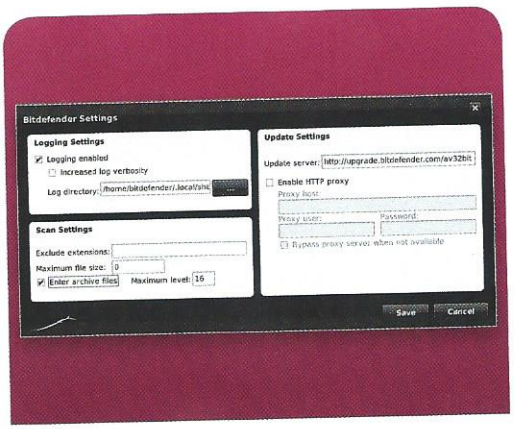



## 15 AVG (1)

Twee weten meer dan één gebruiken we ook nog AVG. de bovenste optie, **AVG Res** problemen te geven, dan kunt u het nog me de twee andere proberen (**with Disabled F buffer** en **with Resolution Selection**). Eve verschijnt dan een menu waar u de eerste o lecteert: **Scan**. Stelt AVG een update voor, g zeker op in. Kies in dat geval **Online / Upda the Internet**. Vervolgens geeft u aan wat u wilt laten scannen: specifieke volumes of m bootsectoren of het Windows-register.

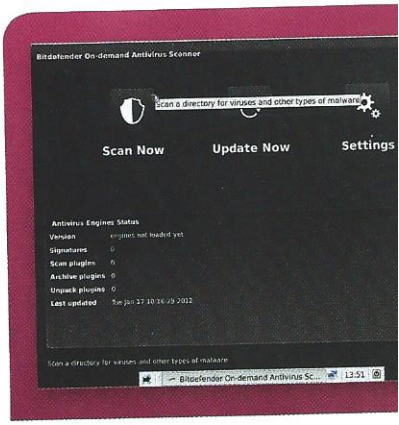

## 16 AVG (2)

AVG toont u nu het **Options**-menu waarin u via de spatiebalk alle gewenste scanopties kunt activeren. Naast de standaardopties raden we u aan ook **Scan inside archives** aan te stippen. Levert de normale scanronde niets op en vermoedt u toch een infectie, dan kunt u de scan eventueel opnieuw uitvoeren in **Paranoid Mode**. Na afloop van de scanronde krijgt u dan een beknopt rapport. Bij malware-detectie kunt u dan zelf bepalen wat er met de geïnfecteerde bestanden (individueel of in groep) moet gebeuren: overslaan, hernoemen of verwijderen.




## 17 BitDefender (1)

We laten nog een derde scanner los op ons systeem, die van BitDefender. Die neemt u vriendelijk met een wizard aan de hand. Allereerst haalt de wizard de nodige updates op. Vervolgens belandt u in de antivirusmodule waarin u naast de knop **Update Now** nog de knoppen **Scan Now** en **Settings** aantreft. In dit **Settings**-menu kunt u echter weinig aanpassingen doen. Wel kunt u hier bepaalde schijfonderdelen uitsluiten, de maximale grootte van te scannen bestanden aangeven en duidelijk maken dat BitDefender ook archiefbestanden moet doorzoeken.




## 18 BitDefender (2)

Standaard begint BitDefe meteen aan een complete maar desgewenst kunt u onderbreken. Via de **Scan Now**-knop krijg de gelegenheid aan te duiden welke locat wilt laten scannen. Naderhand krijgt u dan rapport te zien en kunt u per geval aange actie u wilt ondernemen. Desinfecteren li meest plausibele optie. Als dat niet lukt, c u altijd nog de besmette bestanden herno verwijderen. De gevraagde acties voert u knop **Fix issues**.