Politievirus Verwijderen

Voor het verwijderen van het politievirus is enige computer ervaring benodigd !

Voorwoord

De afgelopen jaren zijn cybercriminelen steeds slimmer geworden op het gebied van malware en virussen. De virussen die vandaag de dag in omloop zijn, zijn steeds moeilijker te verwijderen. Beschikt u over antivirus software, maar bent u toch slachtoffer geworden van het politievirus; hieronder bespreken we hoe u in de meeste gevallen het politie virus kunt verwijderen. Heeft uw antivirus software zijn werk niet goed gedaan en bent u op zoek naar goede antivirus klik dan hier.

Het politievirus zelf

Het politievirus is een Trojan horse dat uw gehele computer blokkeert. U krijgt de melding dat u computer is vergrendeld en dat u een boete moet betalen om de computer te deblokkeren. DOE DIT NOOIT!!! Na betaling is uw computer nog steeds geblokkeerd en cybercriminelen gaan er met uw geld vandoor.

Politievirus verwijderen

Voor het verwijderen van het politievirus is enige computer ervaring benodigd. Zie onderstaande stappen. Als u niet geheel bekend bent met computers is het raadzaam het verwijderen door een specialist te laten uitvoeren. De hierna genoemde stappen zijn als richtlijn en hebben niet altijd succes. Beschikt u over een goede backup dan is het raadzaam om deze terug te zetten.

Het verwijderen van het politievirus is op uw eigen verantwoording.

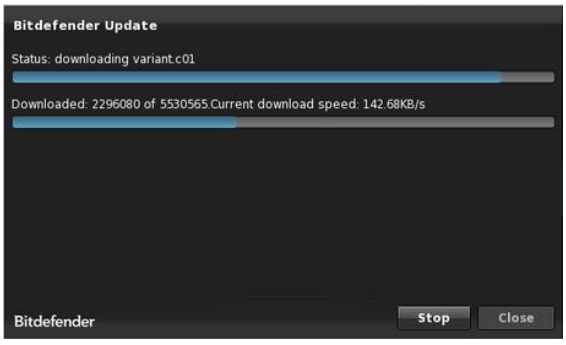
Download met een computer, die niet besmet is, het volgende ISO bestand. Brand het gedownload bestand op een CD. Als de CD gebrand is, is het de bedoeling om de besmette computer op te laten starten van deze CD:

Zet de computer aan, onder in beeld verschijnt de melding: Boot Menu. Dit is per computer merk verschillend. In de meeste gevallen is het toets: F9 of F11 of F12. Sluit de computer aan op de netwerk kabel voordat u deze opstart!

Selecteer de standaard instelling: "Start Bitdefender Rescue CD in English"

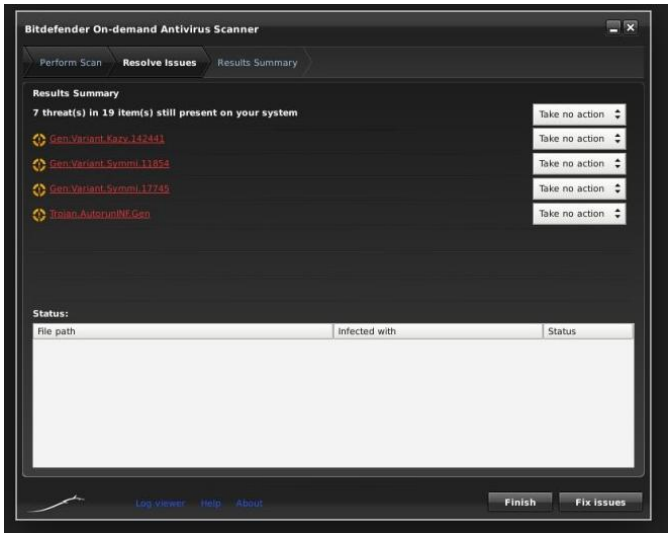
Als de besmette computer is opgestart van de CD, dient u de laatste updates binnen te halen. Dit is nodig zodat de meest recente virussen verwijderd kunnen worden.

Klik op "Continue" als de computer aangesloten is op de netwerk kabel (RJ45 / Internet kabel / UTP kabel) tijdens het opstarten. Dan begint de antivirus met het downloaden van de laatste updates. Dit is zeer belangrijk!



Nadat de updates gedownload zijn begint automatisch de antivirus scan. Dit kan van enkele minuten tot uren duren. Dit is afhankelijk van de snelheid van de computer en de hoeveelheid data die gescand moet worden.

Als de antivirus scan niet automatisch start klikt u op: "Scan Now"



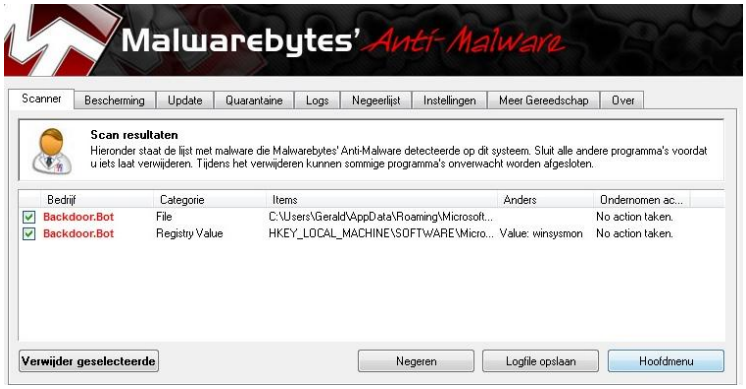
Als de gehele computer is gescand krijgt u het resultaat. Achter de gevonden virussen staat: "Take no action". Hier klikt u op en selecteert u "verwijderen". Soms wil dit niet lukken, dan selecteert u "desinfecteren". Als dit niet lukt selecteert u "Rename".

Als bovenstaande handelingen zijn uitgevoerd, herstart u de "besmette" computer. De computer is nog niet volledig virus vrij. Voordat we hiervan uit kunnen gaan dienen er nog paar handelingen en scans uitgevoerd te worden.

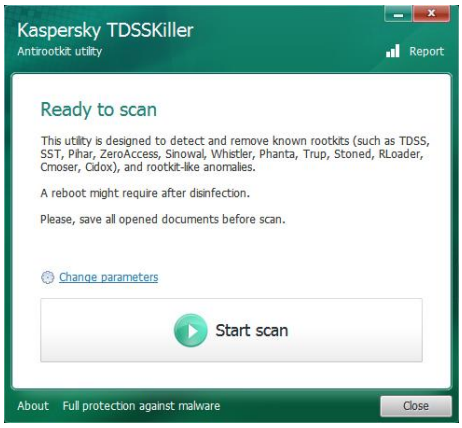
Malware en rootkit scan

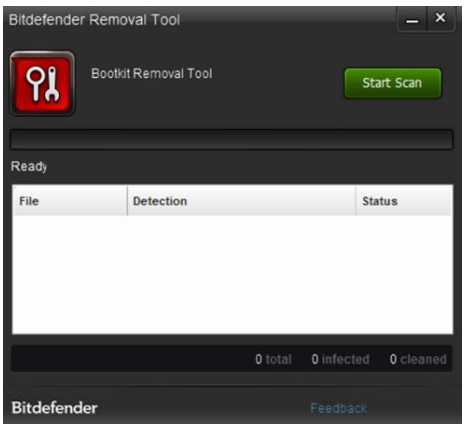
Download de gratis anti-malware tool Malwarebytes. Als de software gedownload is installeert u deze op de besmette computer. Update de software. Als de software up to date is start u de computer op in de veilige modus. Meestal is dit Toets F8. Dit is ook per computer merk verschillend.

Als de computer is opgestart in de veilige modus dan start u de antimalware scan. Aan het einde van de scan kunt u de gevonden bedreigingen selecteren en verwijderen via "Verwijderder Geselecteerde". Niet alle gevonden meldingen vormen per definitie een bedreiging. Let dus op wat je verwijderd!



Als de scan klaar is en de bedreigingen verwijderd, start u de computer opnieuw op. Download de Kaspersky TDSSKiller of de Rootkit remover van Bitdefender. Deze tool is speciaal ontwikkeld voor het herkennen en verwijderen van rootkit's.





Een Rootkit is een stukje software dat zich diep in de computer nestelt. Dit stukje software zorgt ervoor dat hackers toegang krijgen tot uw computer. Daarnaast download deze software nieuwe virussen op uw computer.

Als laatste laat u uw computer nogmaals volledig scannen op virussen. Beschikt u computer al over antivirus software dan installeert u de laatste updates en start u de volledige scan. Beschikt u computer nog niet over antivirus software dan raden wij u deze pagina aan. Hier vindt u een overzicht van de beste antivirus software en ziet u in een oogopslag welke software voor u het meest geschikt is.

Mocht na bovenstaande handelingen uw computer nog steeds problemen ondervinden, dan adviseren wij uw computer te voorzien van een nieuw besturingssysteem. Hiermee weet u zeker dat uw computer virus vrij is.

(Antivirus)