

Doel

Bewustwording waar zijn we mee bezig

Geen bangmakerij

Wel realiteit



**ZO
DAT WAREN
DE REGELS

DAN GAAN WE
NU OVER NAAR
DE REALITEIT**

Wat doet wat

Updates:

- zorgt dat o.a. Windows 10 wordt bijgewerkt naar de laatste versie
- dit geldt voor alle software op de computer

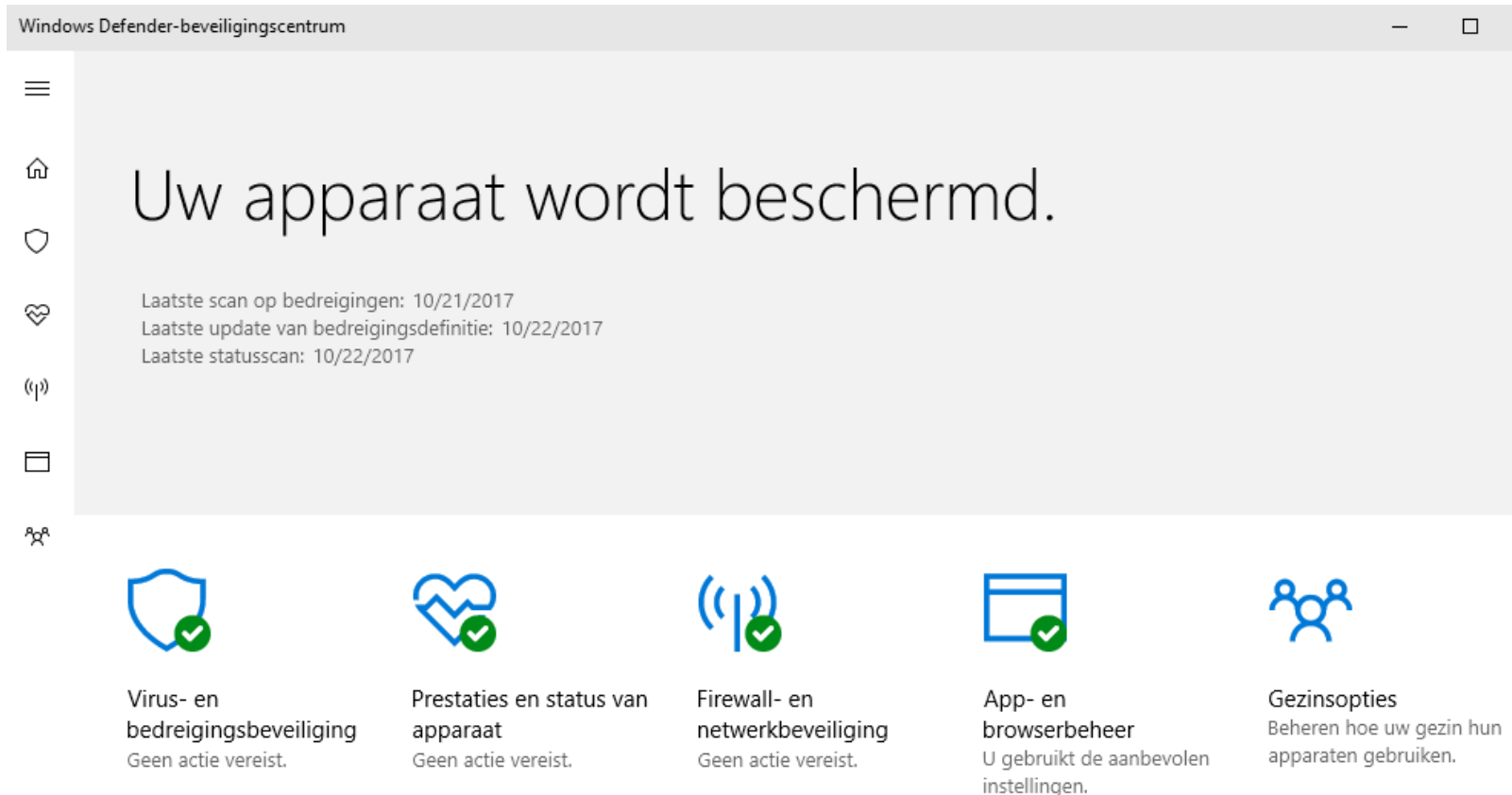
Firewall:

- houdt in de gaten wat er van en naar de computer gaat
- voorkomt niet dat de computer geïnfecteerd raakt met een virus

Antivirussoftware:

- controleert alle inkomende bestanden op virussen en zorgt ervoor dat deze niet voor een besmetting kunnen zorgen door deze voortijdig onschadelijk te maken

“Ideaal” is een moment opname



Windows Defender-beveiligingscentrum

Uw apparaat wordt beschermd.

Laatste scan op bedreigingen: 10/21/2017
Laatste update van bedreigingsdefinitie: 10/22/2017
Laatste statusscan: 10/22/2017


- Virus- en bedreigingsbeveiliging**
Geen actie vereist.
- Prestaties en status van apparaat**
Geen actie vereist.
- Firewall- en netwerkbeveiliging**
Geen actie vereist.
- App- en browserbeheer**
U gebruikt de aanbevolen instellingen.
- Gezinsopties**
Beheren hoe uw gezin hun apparaten gebruiken.


“Ideaal” is een moment opname

Windows Defender-beveiligingscentrum


Uw apparaat wordt beschermd.


Laatste statusscan: 10/22/2017

- 

Virus- en bedreigingsbeveiliging
U gebruikt andere antivirusproviders.
[Antivirusproviders weergeven](#)
- 

Prestaties en status van apparaat
Geen actie vereist.
- 

Firewall- en netwerkbeveiliging
Geen actie vereist.
- 

App- en browserbeheer
U gebruikt de aanbevolen instellingen.
- 

Gezinsopties
Beheren hoe uw gezin hun apparaten gebruiken.

Welke gevaren ⁽¹⁾

Virus:

- een stukje code dat op de computer achterblijft zich vermenigvuldigd en in principe schade toebrengt

Malware: (wikipedia)

- elke software die gebruikt wordt om de computer te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen
- malware veronderstelt kwade opzet
- software waarmee geen kwaad wordt beoogd, valt hier dus niet onder

Phishing:

- hengelen naar je persoonlijke gegevens

(kijk voor heel veel voorbeelden eens op Seniorweb:

<https://www.seniorweb.nl/onderwerp/spam-en-phishing#/meldingen>



Welke gevaren ⁽²⁾

Ransomware:

- bestand(en) op je computer of de hele computer wordt gegijzeld

Hacken: (wikipedia)

- hiervoor is géén duidelijke definitie te geven
- het toepassen van creativiteit, kennis, vaardigheden en intelligentie om beperkingen en limitaties te overwinnen om bijvoorbeeld een voorwerp (b.v. computer) voor iets anders te gebruiken dan waar het voor bedoeld is

Spyware:

- verzameld allerlei gegevens over het gebruik van de computer

Welke gevaren ⁽³⁾

E-mail spoofing:

- mensen sturen een mail uit naam van iemand anders
- uit naam van een politicus of ministeries
- uit naam van bedrijven o.a. energie bedrijven ect.
-



Virusverzekering tegen digitale schade

- verzekeraar geeft router met extra bescherming en een virusscanner
- Afkomstig van F-Secure
- schade dekking € 5.000,00

Wat merkt u

Bij een besmetting gebeuren de raarste dingen met een computer:

- zoals een trage computer of internetverbinding
- het automatisch wijzigen van de startpagina
- het niet meer kunnen verwijderen van een toolbar
- een firewall die regelmatig met meldingen komt, etc
- afbeeldingen die over het scherm lopen

Het is dan noodzaak het systeem op te schonen / aan te pakken:

- voor dit doel kan gebruik worden gemaakt van

Wat kunt u zelf doen

- controleren of laatste update's geïnstalleerd zijn
- met antivirus software regelmatig uw computer laten scannen
- met hulpprogramma('s) regelmatig de computer laten onderzoeken
(ook deze hulpprogramma's regelmatig updaten)

- Website om te kijken of je mailadres is gehackt:
<https://haveibeenpwned.com>

of

- Website politie
<https://www.politie.nl/themas/controleer-of-mijn-inloggegevens-zijn-gestolen.html>

Antivirus software

- Avg
- Avira
- Avast
- Bitdefender
- Bullguard
- Eset
- F-Secure
- G-Data
- Kaspersky
- Mcafee
- Microsoft
- Normen
- Norton
- Panda
- Symantec
- Trend Micro
- Webroot
- Windows Defender
(WD zit standaard in Windows 10)

AV-Test (antivirus test) <https://www.av-test.org/en/antivirus/>

F-Secure online scan https://www.f-secure.com/nl_NL/web/home_nl/online-scanner

Hulpprogramma's (tools)

Een kleine selectie

- Advanced SystemCare 10 <https://www.iobit.com/nl/advancedsystemcarefree.php>
- Ccleaner <https://www.piriform.com/ccleaner/download>
- Driver Booster <https://www.iobit.com/nl/driver-booster.php>
- IObit Malware Fighter <https://www.iobit.com/nl/store.php>
- Iobit Uninstaller <https://www.iobit.com/nl/advanceduninstaller.php>
- Smart Defrag <https://www.iobit.com/nl/iobitsmartdefrag.php?a>

Let op: kijk altijd of er hokjes aangevinkt staan



die ook andere software mee installeert

Install Yahoo powered Chromium browser

(bij het installeren van gratis software moet je accepteren dat er regelmatig een “soort” advertentie melding komt om je te verleiden om de Pro-versie aan te schaffen, je kan deze meldingen gewoon negeren en sluiten met het kruisje)


Voorkomen van Ransomware

- als je één mail ontvangt welke je niets zegt open deze mail dan **niet** maar verwijder hem direct
- heb je deze mail wel hebt geopend dan is er nog niets aan de hand
- echter als er in deze mail een vermelding staat (lees een link) om hierop te klikken en je doet dit braaf dan ben je **de klos**
- of er wordt gevraagd om de “bijlage” die bij de mail zit te openen, **niet doen** anders en u raad het al, dan ben je de klos

Probleem in de praktijk is natuurlijk dat deze mail niet van de echte mail te onderscheiden is. Denk aan uw eigen bank, energie leverancier of telefoonprovider, enz.

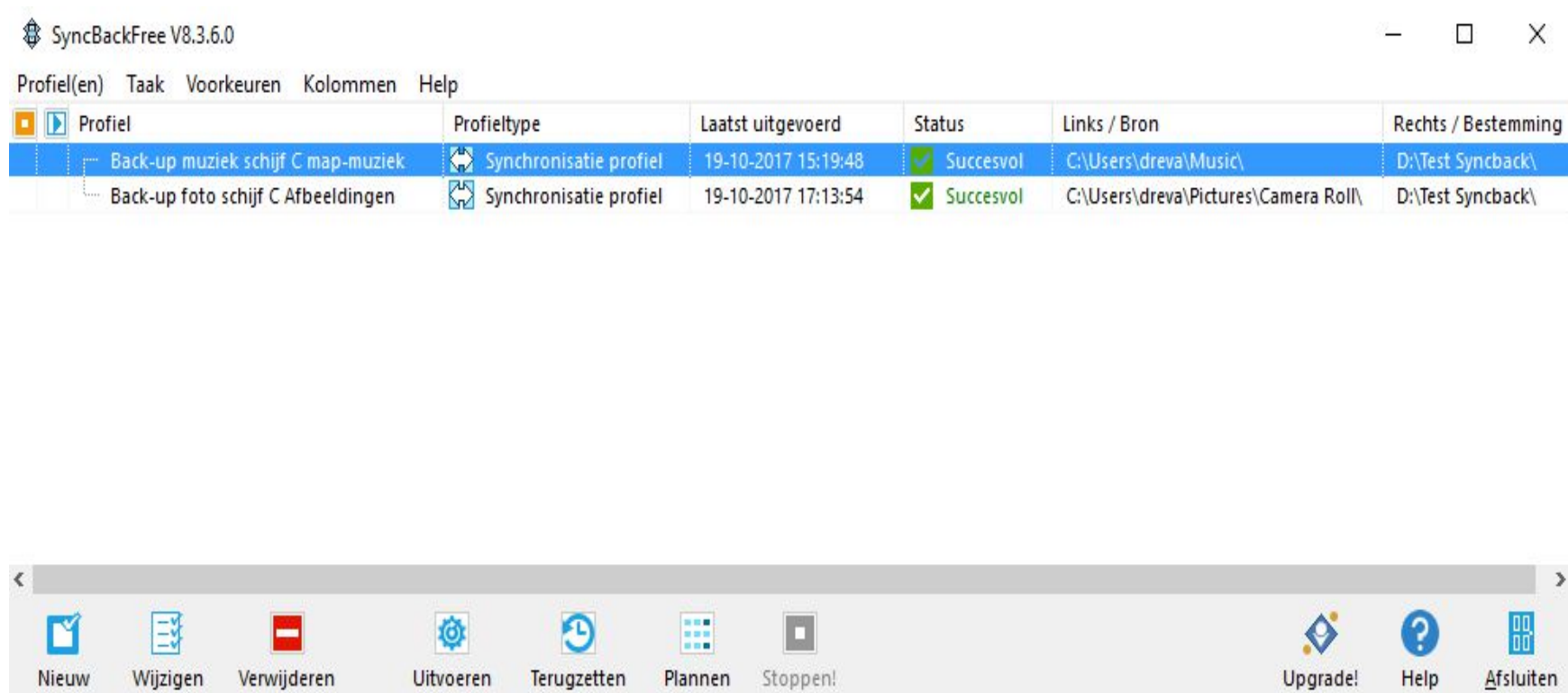
Vorzorgsmaatregel bij Ransomware

Als je wordt gegijzeld probeer dan meer ellende te voorkomen door:

- maak met regelmaat een back-up van je persoonlijke bestanden
- natuurlijk maak je deze back-up op een externe geheugenopslag (2x)
- laat deze externe geheugenopslag niet altijd aan de computer aangekoppeld
- geheugenopslag netjes loskoppelen via stick-afbeelding  in de taakbalk

Back-up software (1)

- SyncBackFree: <https://www.2brightsparks.com/freeware/index.html>



SyncBackFree V8.3.6.0

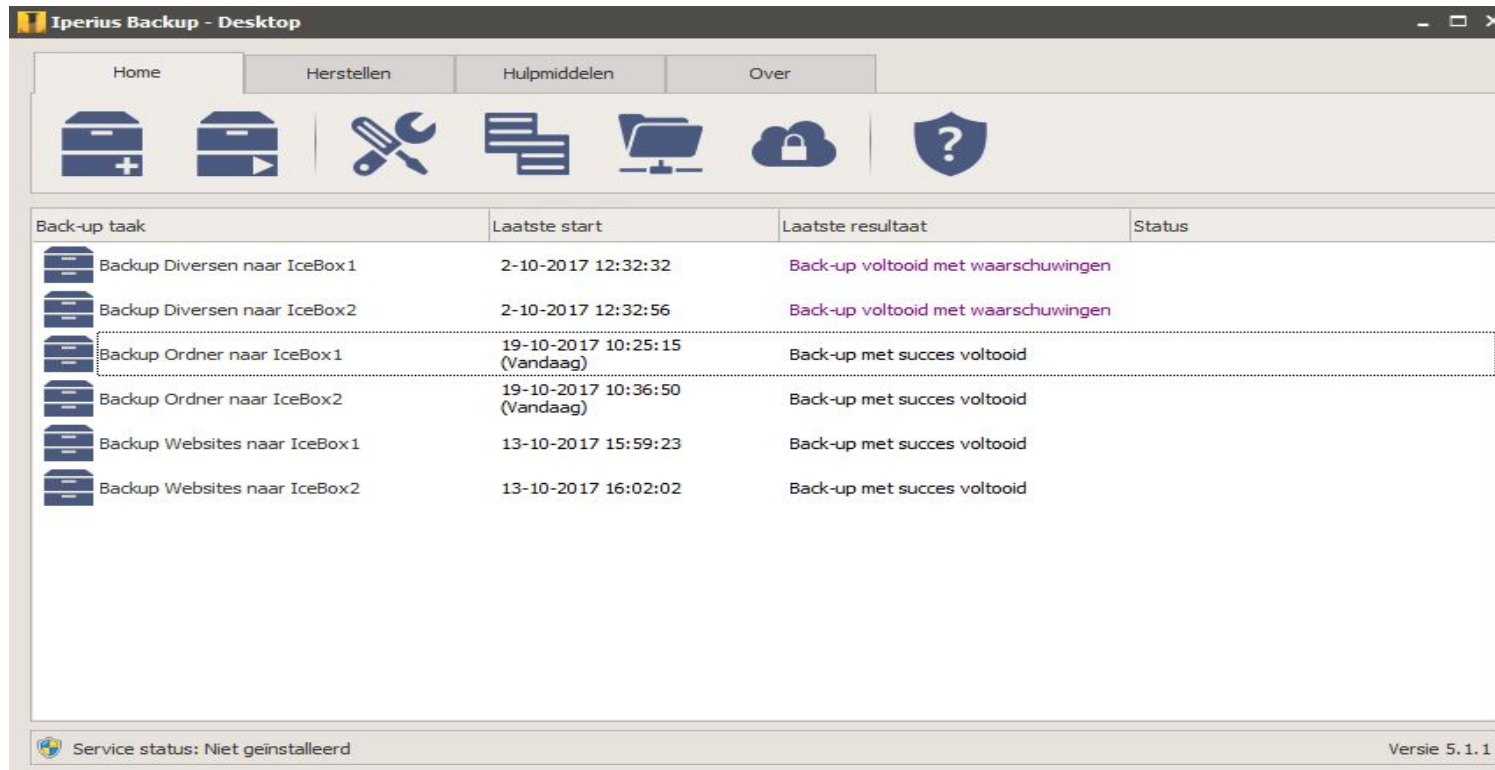
Profiel(en) Taak Voorkeuren Kolommen Help

Profiel	Profieltype	Laatst uitgevoerd	Status	Links / Bron	Rechts / Bestemming
Back-up muziek schijf C map-muziek	Synchronisatie profiel	19-10-2017 15:19:48	✓ Succesvol	C:\Users\dreva\Music\	D:\Test Syncback\
Back-up foto schijf C Afbeeldingen	Synchronisatie profiel	19-10-2017 17:13:54	✓ Succesvol	C:\Users\dreva\Pictures\Camera Roll\	D:\Test Syncback\

Nieuw Wijzigen Verwijderen Uitvoeren Terugzetten Plannen Stoppen! Upgrade! Help Afsluiten

Back-up software (2)

- Iperius Backup: <https://www.iperiusbackup.com/software-backup-free.aspx>



Indien toch gegijzeld Ransomware

Indien slachtoffer van Ransomware ga dan eerst naar de website's:

- www.nomoreransom.org (samenwerking tussen politie, Europol en beveiligingsbedrijf Kaspersky)

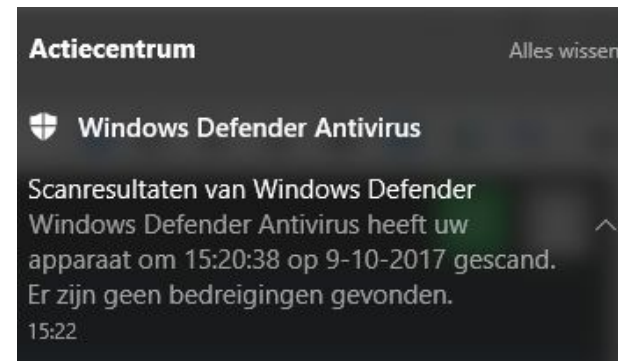
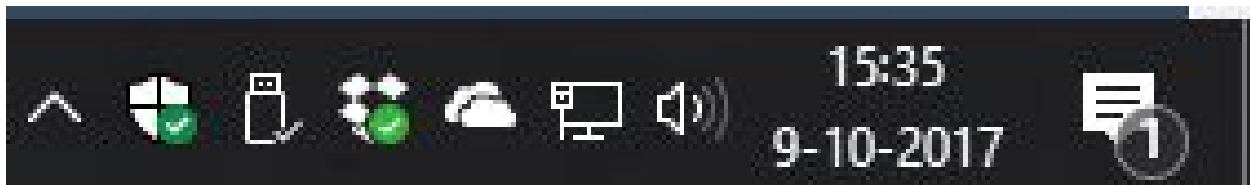
of

- <http://support.eset.com/kb6274/> en <http://support.eset.com/kb6051/> beveiligingsbedrijf ESET biedt een decryptietool aan



Beide website's bieden hulp aan d.m.v. een decryptietool.
Verder staat er heel veel informatie over Ransomware.

Windows Defender ⁽¹⁾



Windows Defender (5)

Uw apparaat wordt beschermd.

Laatste scan op bedreigingen: 10/9/2017
Laatste update van bedreigingsdefinitie: 10/8/2017
Laatste statusscan: 10/9/2017



**Virus- en
bedreigingsbeveiliging**
Geen actie vereist.



**Prestaties en status van
apparaat**
Geen actie vereist.



**Firewall- en
netwerkbeveiliging**
Geen actie vereist.



**App- en
browserbeheer**
U gebruikt de aanbevolen
instellingen.








Gezinsopties
Beheren hoe uw gezin hun
apparaten gebruiken.

Windows Defender (2)

Uw apparaat wordt beschermd.

Laatste scan op bedreigingen: Niet beschikbaar
Laatste update van bedreigingsdefinitie: 10/8/2017
Laatste statusscan: 10/9/2017

				
Virus- en bedreigingsbeveiliging Snelle scan is nodig	Prestaties en status van apparaat Geen actie vereist.	Firewall- en netwerkbeveiliging Geen actie vereist.	App- en browserbeheer U gebruikt de aanbevolen instellingen.	Gezinsopties Beheren hoe uw gezin hun apparaten gebruiken.

[Nu scannen](#)

Klik op geel uitroepteken

Windows Defender ⁽³⁾



Windows Defender (4)

Snelle scan wordt uitgevoerd...
Verstreken tijd: 00:00:03
3659 bestanden gescand

Annuleren


 Scangeschiedenis

Geen bedreigingen gevonden.

0	19511
Bedreigingen gevonden	Bestanden gescand

Snelle scan

[Geavanceerde scan](#)

 Scanresultaten van Windows Defender
Windows Defender Antivirus heeft uw apparaat om 15:20:38 op 9-10-2017 gescand. Er zijn geen bedreigingen gevonden.

Windows Defender ⁽⁶⁾



Windows Defender-beveiligingscentrum

Virus- en bedreigingsbeveiliging

Geschiedenis van bedreigingen bekijken, scannen op virussen en andere bedreigingen, beveiligingsinstellingen opgeven en beveiligingsupdates ontvangen.

Scangeschiedenis
Geen bedreigingen gevonden.

0 Bedreigingen gevonden 0 Bestanden gescand

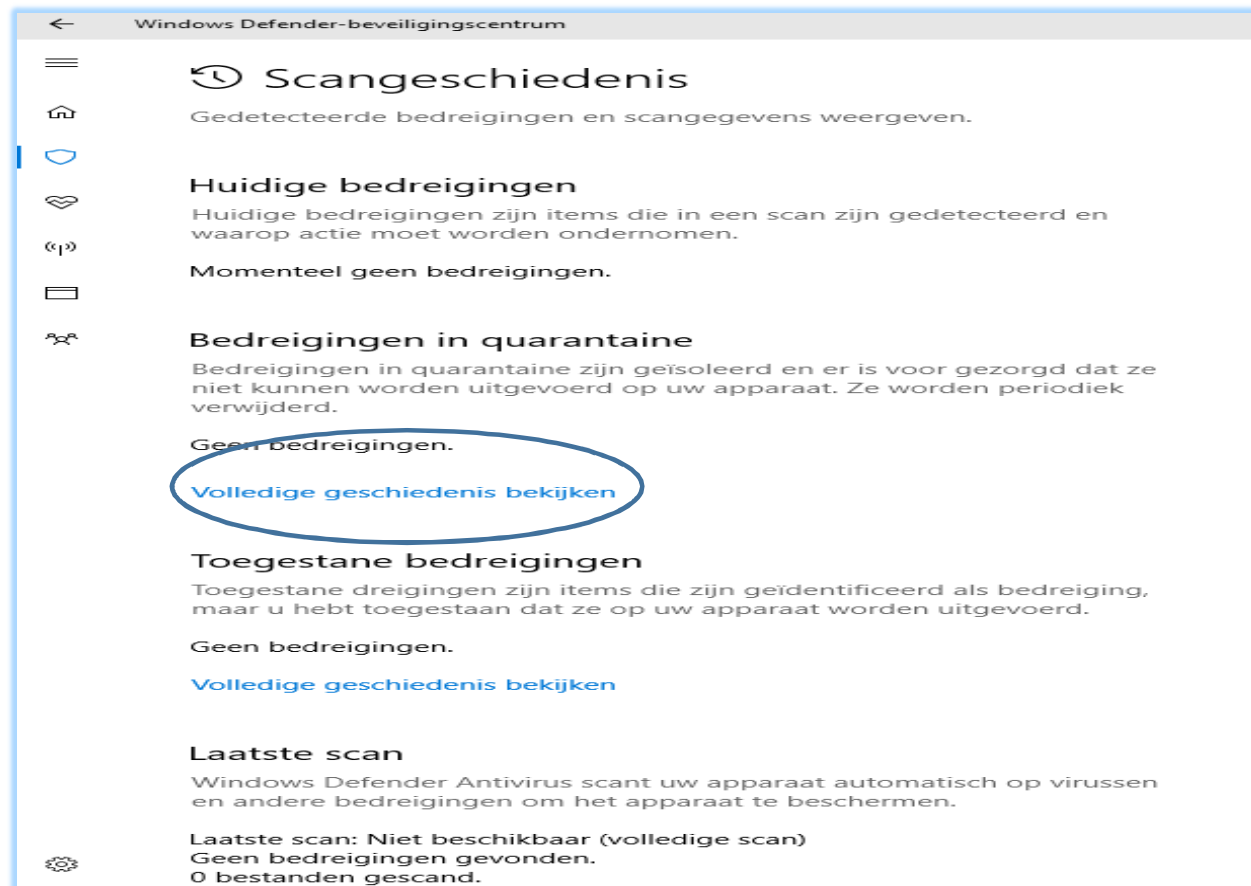
Snelle scan

[Een nieuwe snelle scan uitvoeren](#)
[Geavanceerde scan](#)

Instellingen voor virus- en bedreigingsbeveiliging
U gebruikt de door Microsoft aanbevolen instellingen.

Beveiligingsupdates
Beveiligingsdefinities zijn bijgewerkt.

Windows Defender (7)



Windows Defender-beveiligingscentrum

Scangeschiedenis

Gedetecteerde bedreigingen en scangegevens weergeven.

Huidige bedreigingen

Huidige bedreigingen zijn items die in een scan zijn gedetecteerd en waarop actie moet worden ondernomen.

Momenteel geen bedreigingen.

Bedreigingen in quarantaine

Bedreigingen in quarantaine zijn geïsoleerd en er is voor gezorgd dat ze niet kunnen worden uitgevoerd op uw apparaat. Ze worden periodiek verwijderd.

Geen bedreigingen.

[Volledige geschiedenis bekijken](#)

Toegestane bedreigingen

Toegestane dreigingen zijn items die zijn geïdentificeerd als bedreiging, maar u hebt toegestaan dat ze op uw apparaat worden uitgevoerd.

Geen bedreigingen.

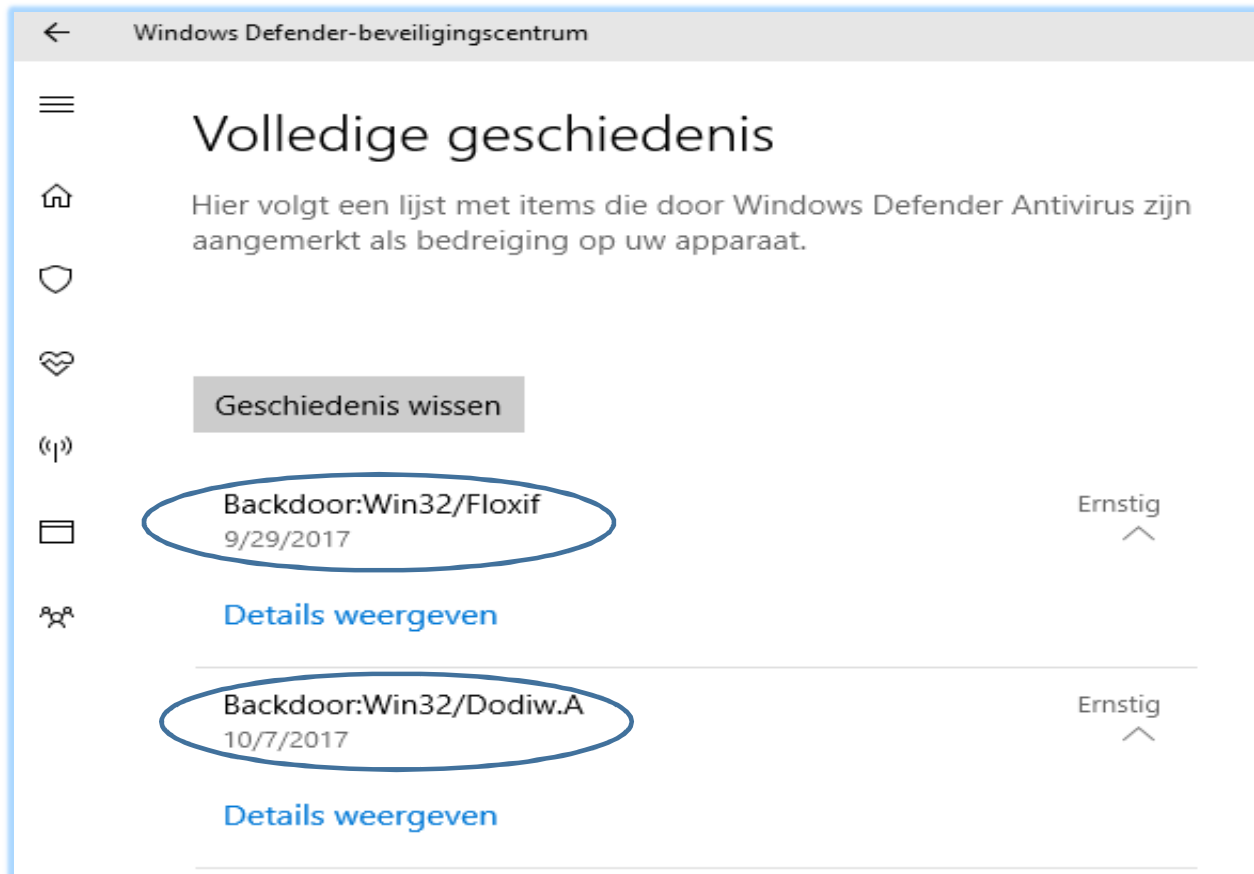
[Volledige geschiedenis bekijken](#)

Laatste scan

Windows Defender Antivirus scant uw apparaat automatisch op virussen en andere bedreigingen om het apparaat te beschermen.

Laatste scan: Niet beschikbaar (volledige scan)
Geen bedreigingen gevonden.
0 bestanden gescand.

Windows Defender ⁽⁸⁾



← Windows Defender-beveiligingscentrum

Volledige geschiedenis

Hier volgt een lijst met items die door Windows Defender Antivirus zijn aangemerkt als bedreiging op uw apparaat.

[Geschiedenis wissen](#)

Backdoor:Win32/Floxif 9/29/2017	Ernstig ^
Details weergeven	
Backdoor:Win32/Dodiv.A 10/7/2017	Ernstig ^
Details weergeven	

Windows Defender ⁽⁹⁾

Backdoor:Win32/Dodiv.A

Waarschuwingsniveau: Ernstig
Status: In quarantaine geplaatst
Datum: 10/7/2017

Aanbevolen actie: Bedreiging nu verwijderen.

Categorie: Achterdeur

Details: Dit programma biedt externe toegang tot de computer waarop het

[Meer informatie](#)

Betrokken items:

file: C:\Users\dreva\AppData\Local\Temp\161649746.exe

OK

Windows Defender (10)



Na de laatste update versie 1709 heeft Windows Defender een tweetal extra beveiligingen toegevoegd:

Controlled Folder Access

Hiermee worden respectievelijk de mappen met persoonlijke bestanden beschermd

Exploit Protection

Windows beschermen tegen wijzigingen

Windows Defender (11)



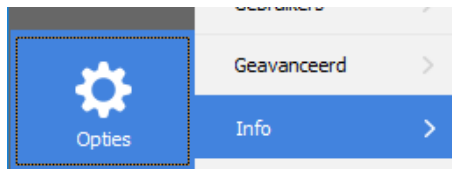
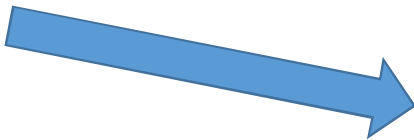
Ccleaner

 artikel 18-09-2017

32-bitsversies

Volgens Piriform zijn alleen de 32-bits-versies van CCleaner en CCleaner Cloud besmet. Het [bedrijf adviseert](#) om met spoed de huidige versie (5.33.6162) te verwijderen en per direct te upgraden naar de [nieuwste versie van CCleaner](#).

Laatste versie
29-10-2017



Lees het complete artikel op:

<http://www.computeridee.nl/nieuws/malware-infecteert-installatiebestanden-ccleaner/>

Wifinetwerken zo lek als een mandje 17-10-2017

1) **Wat is er precies mis?**

Er zit een beveiligingslek in de standaardtechnologie die een veilige verbinding tot stand moet brengen, WPA2. Door de fout was verke.....

2) **Wie zijn kwetsbaar?**

Volgens de Belgische onderzoekers zijn alle wifiverbindingen potentieel kwetsbaar, maar zijn verbindingen via Android-apparaten extra gevoelig voor inbraa.....

3) **Wat is eraan te doen?**

Een standaard zoals WPA2 is het product van uitgebreid overleg tussen fabrikanten en experts, er is dan ook niemand direct verantwoordel.....

Lees het complete artikel op:

<https://www.hcc.nl/kennis/1945-wifinetwerken-zo-lek-als-een-mandje>

Bedankt voor uw aandacht