

Besmet?

Doe de check

Is je Windows-pc besmet met malware of weet je het niet zeker? Ons stappenplan biedt uitkomst.



Herken de 5 symptomen

Malware en advertentiesoftware kunnen hardnekkig zijn. Met ons stappenplan heb je een goede kans dat je er vanaf komt. Soms merk je niet dat die ongewenste software actief is, dus we raden aan om sowieso af en toe dit stappenplan te doorlopen. Doe het in elk geval als je pc een of meer van onderstaande symptomen vertoont:

1 Een trage pc. Malware die op de achtergrond zijn werk doet kan de computer vertragen.

2 Browseraanpassingen. Vreemde veranderingen in je browser, zoals een andere startpagina of zoekmachine of rare werkbalken wijzen erop dat de pc ongewenste software bevat.

3 Pop-upschermpjes. Vensters met reclame of nepwaarschuwingen die tevoorschijn schieten zijn een sterke aanwijzing voor een besmette pc.

4 Uitgeschakelde virus-scanner. Is je virusscanner om onduidelijke redenen uitgeschakeld? Dan kan dit het werk zijn van malware.

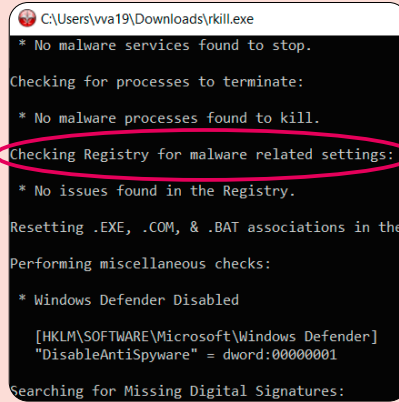
5 Versleutelde bestanden en een melding waarin loggeld wordt geëist. Je pc is besmet met ransomware (gijzelsoftware). Volg dan het speciale stappenplan op pagina 16.

STAP 1

Stop ongewenste processen met RKill

Sluit eerst mogelijk ongewenste software die momenteel actief is. Dan is de kans groter dat die software straks verwijderd kan worden. Het gratis RKill doet dit voor je. Ga naar bleepingcomputer.com/download/rkill en kies de downloadknop linksboven.

Als je het programma start, verschijnt het Windows-opdrachtvenster (zie rechts) en voert het automatisch zijn werk uit. Na afloop zie je of RKill processen heeft afgesloten. Ga verder met de volgende stappen zonder de pc te herstarten.



STAP 3

Voer een scan uit met Malwarebytes

Voer, behalve met je virusscanner, ook een scan uit met een tweede malwareverwijderaar. Virusscanners zijn namelijk vooral goed in het blokkeren van virussen. Maar als je pc tóch besmet is, lukt het ze niet altijd om die op te schonen. Ook de minder kwaadaardige ongewenste software (de zogeheten POP's, zie kader op pagina 17) missen ze nog wel eens. Wij hebben goede ervaringen met Malwarebytes.

N.B.: Kaspersky geeft aan dat Malwarebytes niet samengaat met zijn virusscanners, maar het gratis deel van Malwarebytes zou probleemvrij moeten werken.

1 Ga naar nl.malwarebytes.com/free en download en installeer Malwarebytes. De browserextensie Browser Guard mag je weigeren. Negeer het betaalde Premium-deel (eerste 14 dagen

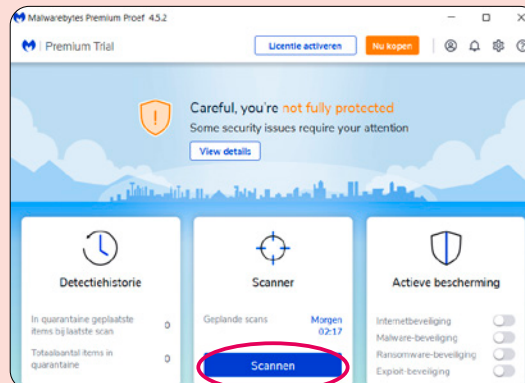
gratis), het gaat ons om het gratis deel dat handmatig besmettingen opspoot en verhelpt.

2 Klik op > **Beveiliging**.

3 Schakel **Opstarten van Windows** uit, en schakel in het hoofdscherm alle onderdelen uit bij 'Actieve bescherming', dit doet je gewone virusscanner immers al.

4 Kies in het hoofdscherm voor **Scannen**.

5 Klik na het scannen bij de scanresultaten rechtsonder op **Quarantaine** om gevonden items te verwijderen.



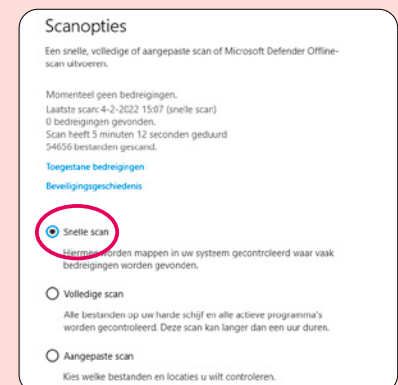
STAP 2

Doe een uitgebreide scan

Je virusscanner controleert alle binnenkomende bestanden, maar kan toch een (nieuw) virus over het hoofd zien. Als de virusscanner na een update de volgende dag het virus wel kan herkennen, wordt het virus nog niet direct onschadelijk gemaakt. Je virusscanner controleert uit zichzelf namelijk alleen bestanden die je downloadt of opent (tussen de automatische scans die je hebt ingepland). Voer daarom nu een handmatige scan uit:

1 Open het hoofdmenu van je virus-scanner door op de taakbalk rechtsonder op het virusscanner-icoontje te dubbelklikken. Vaak zie je het icoontje pas nadat je op het pijltje (^) klikt.

2 Gebruik je Windows Defender, de standaard virusscanner van Windows? Dubbelklik dan in de taakbalk op het schildicoontje > **Virus- en bedreigingsbeveiliging** > **Scanopties** > **Volledige scan**.



3 Gebruik je een eigen virusscanner? Zoek daar dan naar de optie volledige (systeem)scan uitvoeren. In Bitdefender ga je bijvoorbeeld in het hoofdmenu naar 'Antivirus' en kies je voor 'Systeemscan'.





Hoe verwijder ik ransomware?

Een van de vervelendste digitale gevaren is gijzelsoftware of ransomware. Criminelen zetten je bestanden op slot en vragen een betaling van een grote som geld om ze weer vrij te geven. Actie vooraf is cruciaal, zoals back-ups en een goede virus-scanner. Zonder back-up zijn je bestanden vaak niet meer te redden.

Doorloop bij een ransomware-besmetting de volgende stappen:

- 1 Verbreek de internetverbinding** op de pc. Dubbelklik op het wifi-icoontje op de taakbalk > kies voor vliegtuigstand of trek de netwerkkabel uit de pc om verdere schade te voorkomen.
- 2 Betaal geen losgeld.** Je houdt hiermee deze vorm van criminaliteit in stand en bovendien heb je geen garantie dat je na betaling je bestanden terugkrijgt.
- 3 Maak een foto of screenshot** van het losgeldbericht. De informatie kan nodig zijn voor het ontsleutelen.
- 4 Voer virusscans uit.** Volg stap 1 tot 4 en eventueel 7 uit ons stappenplan.
- 5 Heb je een back-up?** Plaats deze pas terug als de malware is verwijderd.
- 6 Heb je geen back-up, ga dan naar nomoreransom.org** om te controleren of je apparaat geïnfecteerd is met een ransomware-variant waarvoor gratis ontsleutelsoftware (decrypter) beschikbaar is. Bijvoorbeeld doordat de politie 'de sleutels' heeft buitgemaakt of de bende heeft opgerold. De informatie in het losgeldbericht kan helpen de juiste variant te achterhalen.
- 7 Doe aangifte** bij de politie. Met meerdere aangiftes is de kans groter dat de politie de bende achter de ransomware (internationaal) kan aanpakken.

STAP 4

Verwijder adware met AdwCleaner

Voor specifieke hardnekkige advertentie-software (adware) kan AdwCleaner uitkomst bieden. Het programmaatje is gemaakt door de makers van Malwarebytes en verwijdert soms net wat andere hardnekkige items. Bovendien werkt de scan erg snel.

1 Ga naar nl.malwarebytes.com/adwcleaner en download en installeer AdwCleaner.

2 Klik na openen op **Scan nu** om een scan te starten.

3 Klik na de scan in het resultaten-scherm op **Volgende**.

4 Geeft AdwCleaner meldingen over 'voorgeïnstalleerde software' dan kun je deze beter niet zomaar aanvinken om te verwijderen. Dit kan nuttige software van de pc-fabrikant zijn.

5 Klik rechtsonder op **Quarantaine** om de gevonden items te verwijderen.

STAP 5

Voer een scan uit met Zemana

Vindt Malwarebytes niets? Probeer dan ook nog Zemana, een vergelijkbare scanner.

1 Ga naar zemana.com/antimalware en download en installeer Zemana. Vink daarbij 'Run Zemana AntiMalware at Windows startup' uit. Net als Malwareby-

tes heeft Zemana een betaald deel dat je kunt negeren.

2 Zet in het hoofdmenu het schuifje op **diep** voor het beste resultaat.

3 Klik op **Scannen**. Kies in ieder geval de C-schijf in de volgende stap.

4 Na de scan kies je voor **Acties uitvoeren** om de gevonden items te verwijderen.

STAP 6

Reset de browser

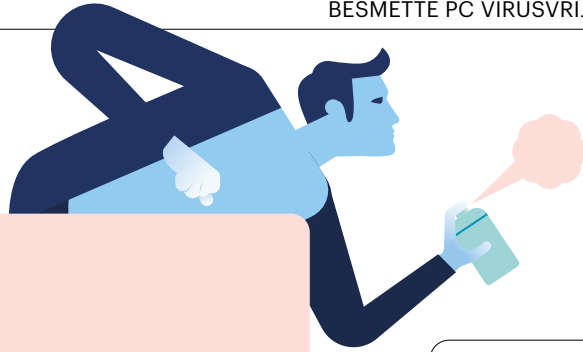
Merkte je vreemde wijzigingen in je browser, zoals een andere startpagina (symptoom 2) en zijn die er nog steeds? Reset de browser dan. In de browser opgeslagen wachtwoorden en favorieten blijven bewaard, maar al het andere wordt teruggezet naar begininstellingen (zoals startpagina, werkbalken en browseruitbreidingen).

► **Chrome:** ☰ > Instellingen > Geavan-

ceerd > **Resetten en opruimen** > **Instellingen terugzetten naar de oorspronkelijke standaardwaarden** > **Instellingen resetten**.

► **Firefox:** typ **about:support** in de web-adresbalk bovenaan, druk op Enter en klik rechtsboven op **Firefox opfrissen**.

► **Edge:** ☰ > Instellingen > Instellingen opnieuw instellen.



STAP 7

Specifieke maatregelen

Hebben stappen 1 t/m 6 nog niet geholpen? Dan kun je op internet soms nog oplossingen vinden voor de specifieke problemen die je ondervindt.

Zoek niet op algemene problemen zoals 'trage pc' of 'pop-ups verwijderen', want dan kom je uit bij algemene of zelfs dubieuze oplossingen (zie 'Trap niet in nepadvies').

Waar je wel op kunt zoeken, is bijvoorbeeld de naam van een verdacht proces dat RKill heeft gevonden (stap 1). Of zoek op namen van mappen en bestanden of webadressen die spontaan verschijnen, of steeds weer opduiken na verwijdering.

Trap niet in nepadvies

► **Klik niet op pop-upschermpjes** met waarschuwingen of virussen die niet van je virus-scanner afkomstig zijn. Die komen vaak voor op (onbetrouwbare) websites en kunnen juist voor besmetting zorgen of leiden naar onbetrouwbare 'hulpsoftware'.

► **Pas op voor online stappenplannen:** als je op internet zoekt op algemene problemen zoals 'trage pc' of 'pop-ups verwijderen', kun je uitkomen op onbetrouwbare stappenplannen en dubieuze 'hulpsoftware'. Een flink deel van die adviezen is opgezet om betaalde software te promoten, zoals Combo Cleaner. Vaak zijn er gratis oplossingen en zo'n betaalprogramma werkt lang niet altijd. Een van de weinige betrouwbare sites met geavanceerde stappenplannen en extra software voor virusverwijdering is bleepingcomputer.com/virus-removal

Wat zijn POP's?

Virussen en andere kwaadaardige software vallen onder de noemer 'malware'. Ze zijn gevaarlijk en stelen bijvoorbeeld je wachtwoorden. Er is ook software die in een grijs gebied opereert: Potentieel Ongewenste Programma's (POP's). Ze komen soms stiekem mee met gewenste software. POP's kunnen bijvoorbeeld reclame tonen of je surfgedrag verzamelen. Let daarom altijd op vinkjes en kleine lettertjes bij het installeren van software. Of installeer het gratis programmaatje Unchecky (unchecky.com), dat dit soort vinkjes uitzet. Virusscanners blokkeren POP's niet altijd, en soms moet je dat apart inschakelen.


STAP 8


Zet Windows terug naar fabrieksinstellingen



Hebben alle voorgaande maatregelen niet geholpen of vind je het te veel gedoe, dan kun je als paardenmiddel Windows terugzetten naar de fabrieksinstellingen. Je behoudt dan je persoonlijke bestanden, maar je moet wel alle instellingen opnieuw aanpassen en programma's en browserextensies opnieuw installeren. Maak vooraf een lijstje van die programma's, zodat je snel weer alles in werkbare staat hebt. Weet je zeker dat je systeem met malware besmet is? Dan raden we aan Windows helemaal opnieuw te installeren, dus

zonder je bestanden te behouden. Zet daarna je data uit een virusvrije back-up terug.

Windows 10 terugzetten:  > **Instellingen** > **Bijwerken en beveiliging** > **Systeemherstel** > **Aan de slag** bij 'Deze pc opnieuw instellen'. Maak een keuze of je bestanden wilt behouden.

Windows 11 terugzetten:  > **Instellingen** > **Systeem** > **Systeemherstel** > **Pc opnieuw instellen**. Maak een keuze of je bestanden wilt behouden.

Hier download je de software

- **AdwCleaner**
nl.malwarebytes.com/adwcleaner
- **Malwarebytes**
nl.malwarebytes.com/free
- **RKill**
bleepingcomputer.com/download/rkill/
- **Zemana AntiMalware**
zemana.com/antimalware

Meer info: consumentenbond.nl/veilig-internetten

Digitaal blijblijven?

In de DigitaalGids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding

