Denne guide er oprindeligt
udgivet på Eksperten.dk

COMPUTERWORLD

Sådan fjerner du virus og malware

Udviklingen går stærkt på "skidt"fronten, så vi har sammensat en ny og effektiv programpakke til fjernelse af det.

Skrevet den **06. nov 2011** af **fromsej** I kategorien **Sikkerhed / Virus** | ⭐⭐⭐⭐☆

Denne vejledning dækker Win XP, Win 2000 og Vista/Win 7.

Betingelser for hjælp

1. Eventuel fildeling skal afinstalleres, alle cracks skal afinstalleres og slettes.
(KaZaA, Bearshare, Emule, Auzereus, Torrentprogrammer osv.)
Dette er ikke for at hjælpe APG eller andre interesseorganisationer, men fordi der bevisligt kommer alverdens skidt ind den vej.
Vi er godt klar over at især Torrentprogrammer bliver brugt til legale formål også, men vi kan altså ikke se det i en log, derfor vil vi gerne have dem fjernet.

2. Windows skal være opdateret, XP med min. Servicepack 2, 2000 med Servicepack 4.
Vista med Servicepack 2, bemærk at Sp 1 skal være installeret før du kan installere Sp 2.
Win7 skal have Servicepack 1

`Hvis der er Servicepack 3 på XP, skal den selvfølgelig ikke fjernes.`

VIGTIGT !!!

Hvis netforbindelsen forsvinder efter Combofix, så tjek Hijackthisloggen for linier der ligner disse:
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = http=127.0.0.1:8484
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *.local;<local>
Er de til stede, så skal de fixes.

En anden variant, som ses hvis det er en zlobinfektion er disse:
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyServer = http=localhost:7171 (tallet kan variere)
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *.local
De skal også fjernes, så burde internettet virke igen efter en genstart.

Hent følgende programmer

Gem dem i en nyoprettet mappe til formålet, de skal ikke installeres endnu.

Vedrørende Vista og Win 7, skal man højreklikke og vælge "Kør som Administrator".

Ccleaner http://www.piriform.com/ccleaner/download/standard
Malwarebytes http://www.besttechie.net/tools/mbam-setup.exe
Malwarebytes alternativ http://www.majorgeeks.com/Malwarebytes_Anti-Malware_d5756.html
ComboFix http://download.bleepingcomputer.com/sUBs/ComboFix.exe
Hijackthis http://www.download.com/Trend-Micro-HijackThis/3000-8022_4-10227353.html

Installation og kørsel af programmerne

Ccleaner

Installer Ccleaner, i øjeblikket får du tilbudt Google chrome, husk at fjerne fluebenene, hvis du ikke ønsker den, eller ikke ønsker den som standardbrowser.
Start Ccleaner, den tilbyder at scanne "intelligent" efter cookies, vælg Ja, da du ellers vil miste dine login-cookies i diverse fora, er det ikke et problem, kan du vælge Nej.

Klik på kør Rens, fjern evt. flueben ved Cookies, vær opmærksom på fanebladet Programmer, her vil der være valgmuligheder for dine evt. andre browsere(Firefox, opera osv.), og lad den fjerne hvad den finder.
Klik så på Register ovre i venstre side (den blå terning), klik på Skan efter problemer, når den er færdig, klik på Udbedre valgte problemer, lav evt. en backup af registreringsdatabasen, klik så på udbedre alle valgte problemer.
Klik på OK, klik på Luk når den er færdig.

Malwarebytes

Installer programmet - når det er gjort skal du lade programmet opdatere sig. Herefter åbner et vindue, hvor du skal flytte prikken til "Kør et fuldstændigt systemscan" - klik på Skan Knappen - lad programmet arbejde. Når det er færdig (det tager tid afhængig af hvor meget du har på computeren).

Derefter - Tryk på "Vis resultater" knappen efter scanningen - og herefter tryk på "Fjern det valgte" - nu åbnes log'en og du skal gemme den et sted, hvor du kan finde den igen.

Combofix

Åbn mappen med Combofix, højreklik, vælg Ny->tekstdokument, åbn tekstdokumentet, kopier følgende ind:

Killall::
Snapshot::

klik på Filer->Gem som, navngiv den CFScript, luk tekstdokumentet.

Tag så fat i den nye fil med musen, og før den hen over Combofix-filen, hvorefter du "giver slip" med musen.
http://www.fromsej.saknet.dk/billeder/cfscript.gif
Så skulle Combofix gerne give sig til at arbejde. Muligvis vil den kræve en genstart, hvilket du skal tillade.
Du bør ikke klikke på vinduet imens værktøjet kører, idet det kan få din computer til at fryse.
Kopier den fremkomne log ind i dit spørgsmål.

Hijackthis

Dobbeltklik på Hijackthis.exe, klik på "Do a system scan and save a logfile", luk programmet når logfilen er kommet frem.
Det kan godt tage sin tid når den scanner O15 og O23 linier (kan ses øverst i HJT vinduet), men den skal nok blive færdig.

indholdet af denne fil må du gerne lægge ind i **Viruskategorien**, sammen med Malwarebytes og loggen fra Combofix.
Rækkefølgen skal helst være denne:
1. Malwarebytes
2. Combofix
3. Hijackthis
Hvis Combofixloggen er meget lang, så læg den i et indlæg for sig selv.
Vi skal under INGEN omstændigheder se loggen fra Ccleaner!

> Hvad så nu?

Nu venter du på at en tjekker dine logs, det kan godt tage tid, da der for det første ikke er så mange der kan, for det andet skal vi lige se indlægget først.

Når du har fået et løsningsforslag, så gør dig selv den tjeneste at tjekke om den person der har lagt forslaget har forstand på det, det gør du ved at tjekke hvilke spørgsmål personen ellers har deltaget i, og i vedkommendes karma.
Klik på linket, så kan du se min profil:
http://www.eksperten.dk/bruger.phtml?navn=fromsej
Hvis du udskifter **fromsej** med **ejvindh** kan du se Ejvindh´s profil (han har bl.a lavet Rootchk).
På Eksperten.dk er der frit slag for hvem der må svare, hvilket er både en svaghed og en styrke, men i tydning af logfiler skal man være ekstrem varsom, da der ikke skal meget forkert til, før maskinen er ubrugelig, hvilket vil resultere i formatering og tab af data, samt besværet med en geninstallation.

Mvh:
Fromsej TeamSpywarefri
Member of Alliance of Security Analysis Professionals
http://asap.maddoktor2.com/
(Jeg kan altid kontaktes via mail >> fromsej (at) spywarefri . dk <<)

Kommentar af kalp d. 23. okt 2008 | 1

Jeg synes den er fin:)
Bed dog lige mærke i følgende:
"husk at fjerne fluebenet udfor installation af Yahoo toolbar."
under punktet: Ccleaner.

Du antager man har den installeret:)
Desværre tror jeg, at der er en del brugere herinde (ikke for, at tale om deres intelligens), som måske vil sidde og lede efter den toolbar (selv om den ikke er der), så de kan fjerne fluebenet:)
Det skal nok bare rettes til "hvis du har ..":)

Kommentar af dr.big d. 04. jan 2009 | 2

Super artikel, godt arbejde fromsej

Kommentar af corleonedk d. 17. nov 2008 | 3

Rigtig god artikel fromsej

Kommentar af jorgenveisig d. 31. okt 2008 | 4

Hej Fromsej

Fin artikel/vejledning, som giver fine instrukser til hvordan man kan få tjekket sin pc for alskens skidt og møg.

Jeg har 2 spørgsmål: 1: Hvad betyder Torrentprogrammer, jeg kan ikke finde et svar på dette nogen steder, udover at der måske er fildelingsprogrammer?
2: Hvordan ved eksperterne hvilke linier fra hijackloggen der kan fixes? Er der en slags register eller??

Kommentar af borkhardt d. 16. dec 2008 | 5

Det var virkelig gennemført lavet, mange tak den har hjulpet Meget!

Kommentar af nicolain d. 21. sep 2010 | 6

Hej! Tak for hjælpen. Kan det passe at ComboFix ikke virker på Windows 7?

Kommentar af treatmenice d. 16. nov 2010 | 7

ja ikke rigtig som den skal
den ødelægger i flere tilfælde højre kliks menuen så der ikke kan oprettes ny genvej bagefter

der er en løsning på det

http://peter.mpbrun.dk/tips-og-tricks/

http://www.mydigitallife.info/2008/06/22/reset-and-fix-broken-windows-vista-file-ext-and-type-associations-include-exe-com-sys-zip-lnk-folder-drive/

Kommentar af fromsej d. 06. jan 2011 | 8

Combofix kører nu på Win 7 og Vista 64 bit.

Kommentar af Blueeyez d. 01. dec 2011 | 9

Interessant guide, lad os se om den finder noget på mine systemer :)

Kommentar af Novice-1 d. 08. dec 2011 | 10

Jeg kan se enkelte elsker deres fildelingssystemer.
I givet fald må de jo kunne afinstallerer programmerne imedens sikkerhedsprogrammerne køres
og HVIS!!! / i det omfang
at snavset ikke har med fildelingsprogrammerne at gøre
så kan folk vel få fjernet den del af det !?
medmindre det i sin tid er kommet ind sammen med fildelingsprogrammerne, for så er man jo nærmest lige vidt!!

Kommentar af john_stigers (nedlagt brugerprofil) d. 01. jan 2012 | 11

#20

Kørsel af guiden kræver at man kender til Combofix, og ved hvordan man læser dennes log!!!
Det er ikke en færdig løsning som sådan...

Kommentar af Chickencry d. 05. aug 2012 | 12

Åbn mappen med Combofix, højreklik, vælg Ny->tekstdokument, åbn tekstdokumentet, kopier følgende ind:
(Hvad er det for en mappe?)

Kommentar af amfro d. 24. feb 2014 | 13

Smuk vejledning. Kan den mon også få has på awesomehp?
Din mor eller amfro