

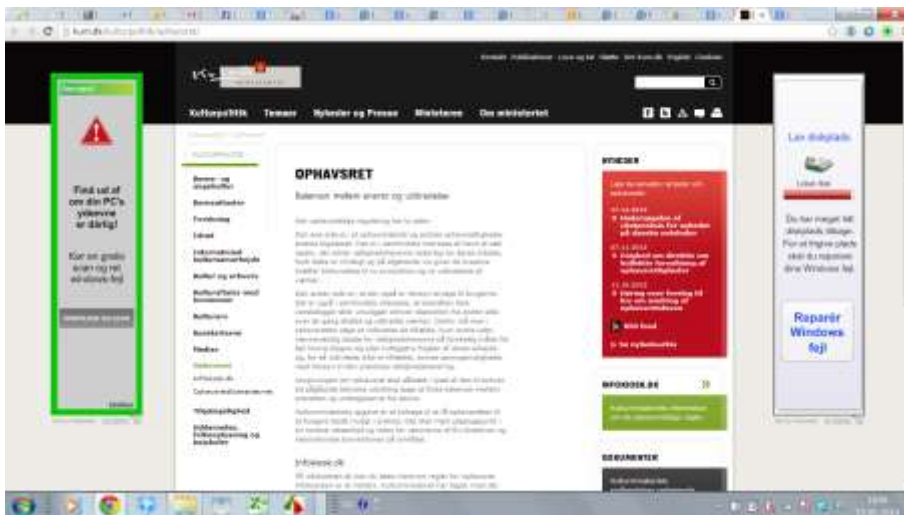
Hjælp – jeg har malware!

Indhold

Malware eller uønskede reklamer på hjemmesider?	1
Rens og styr computeren med Ccleaner	3
Ccleaner: Analyser og slet affaldsfiler	3
Cookies: slette eller gemme?	5
Igangsæt Rens	6
Styr computeren bedre med Ccleaner	6
Hvordan fjerner jeg "Din pc's ydelse er ringe"?	7
Fjern programmet fra computeren	8
Fjern programmet fra Internet Explorer og andre browsere	8
Internet Explorer	8
Chrome	9
Fjern programmet med Malwarebytes	9
Endelig succes igennem afinstallering af Internet Explorer	11
Forklaringer og løsninger	11
En fortsættelse af sagaen, maj 2014:	12

MALWARE ELLER UØNSKEDE REKLAMER PÅ HJEMMESIDER?

Ser dine hjemmesider ofte ud som nedenstående skærmbillede fra Kulturministeriet? Som du nok kan regne ud, har Kulturministeriet her ikke lagt reklamer af denne type på siden, og de er derfor kommet kunstigt pga. et uønsket reklameprogram. Det man kalder "malware". Malware kan være farligt, og skal fjernes. Firmaerne bag tjener penge på reklamerne og den trafik de skaber.



Reklamerne er i sig selv irriterende at se på. Værre er at du – eller andre på din computer – kan komme til at klikke på dem, måske bare for at lukke dem. Det leder derefter til installering af yderligere programmer, som for alvor kan skade maskinen.

Reklamerne stammer som nævnt fra et reklameprogram, der på en eller anden måde har fået sig installeret på din maskine. Det er typisk sket i forbindelse med at du har installeret et andet, mere uskyldigt program, som derefter har installeret reklameprogrammet meget diskret. Hos mig er det vist nok sket gennem programmet BatteryCare, der var installeret på min computer, da jeg købte den.

Der er ikke noget bestemt navn for reklameprogrammet. Det kan optræde under navne som " RightSaver, SafeSaver, DP1815, Video Player, Convert Files for Free, Plus-HD 1.3, BetterSurf, Media Player 1.1, PassShow, LyricsBuddy-1, YoutubeAdBlock 1.2, Media Player 1.1, Savings Bull, Feven Pro 1.1, Websteroids, Savings Bull, HD-Plus 3.5, QuickShare."

Denne vejledning er baseret på mine egne erfaringer med at rense min egen og min datters computer for malware i foråret 2014. Vi har i øvrigt begge installeret udmærkede og opdaterede antivirus-programmer. Af forskellige årsager har de bare ikke reageret på malwaren.

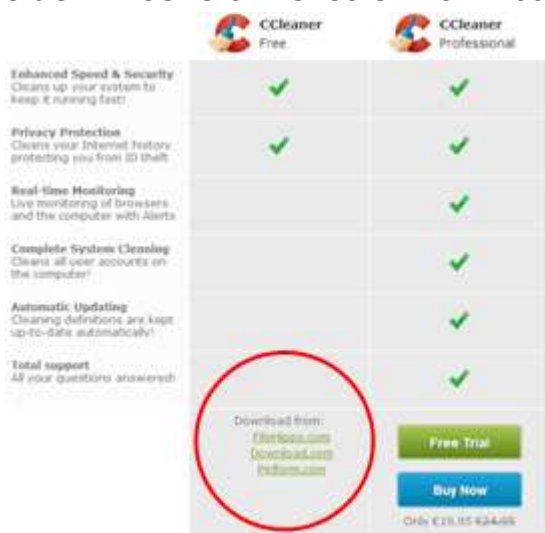
Jeg har fået god hjælp fra flg. hjemmesider:

- <http://www.spywarefri.dk/manualer/manual-for-installation-og-brug-af-cleaner/>
 - En god gennemgang af hvordan Ccleaner fungerer
- <http://malwaretips.com/blogs/>
 - En meget fin hjemmeside med alle mulige malware-tips. Den skrives af Stelian Pilici, som driver en computerbutik i Rumænien.
- <http://www.shouldiremoveit.com/index.aspx>
 - En hjemmeside med struktureret gennemgang af alle mulige programmer. Først kommer producentens tekst, dernæst resultatet af forskellige virustjek – det er det sidste der er det interessante. Der

er også en statistik på hvor mange brugere der fjerner/holder de pågældende programmer.

RENS OG STYR COMPUTEREN MED CCLEANER

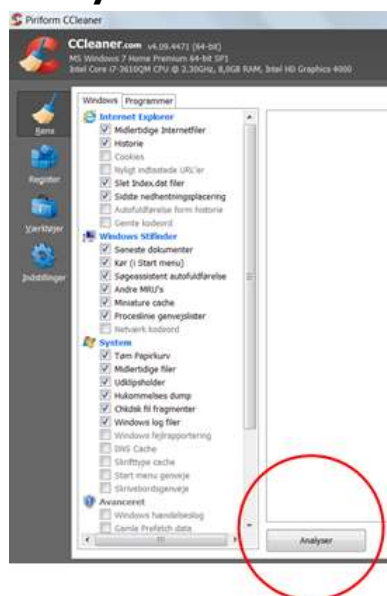
Gå til Ccleaner (<http://www.piriform.com/ccleaner>). Du kan her vælge mellem betalingsversion og den gratis. Vælg den gratis ved at klikke på et af hjemmeside-linksene til venstre. Download går i gang automatisk.



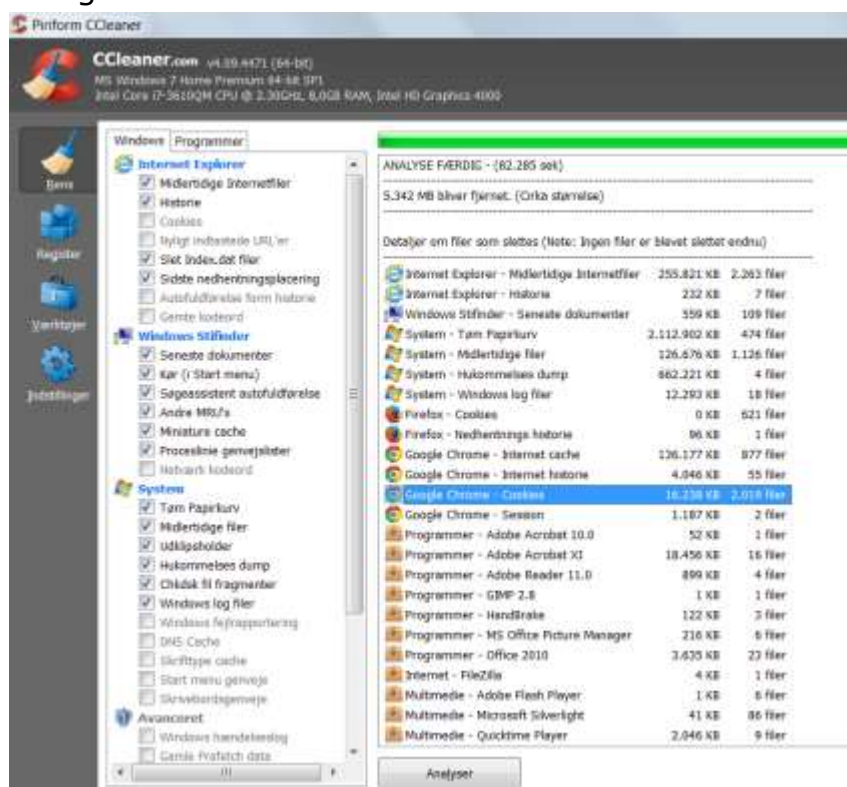
I forbindelse med installeringen af Ccleaner bliver du spurgt om du vil have forskellige ekstra funktioner. Sig bare ja.

Ccleaner: Analyser og slet affaldsfiler

Ccleaner starter op med nedenstående skærbillede, hvor du først skal vælge **Analyser**.



Det gav næste skærmbillede:

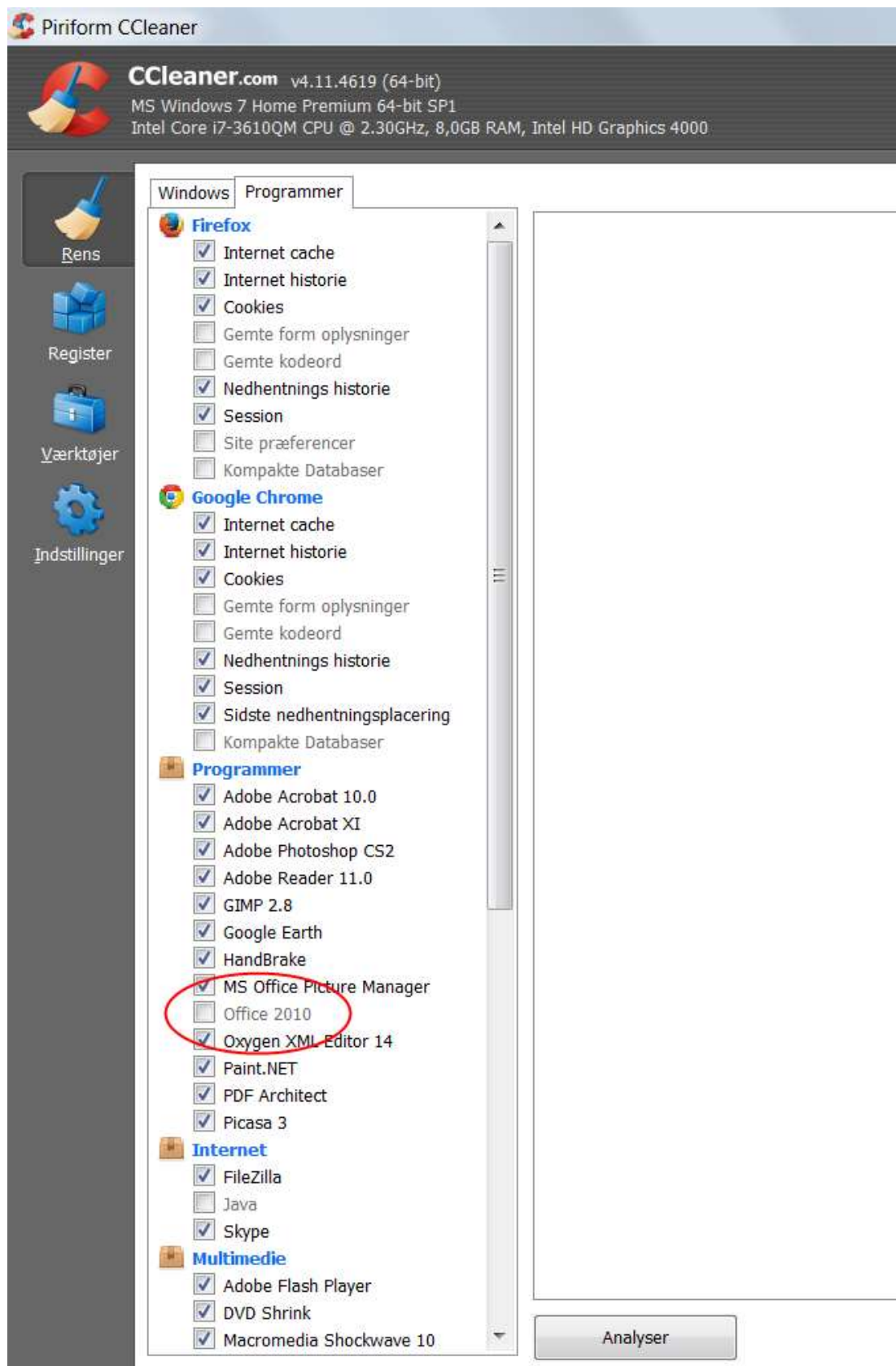


Som du kan se, kan der fjernes en del filer. Bl.a. fylder min papirkurv tilsyneladende 2 gigabyte.

Der er også nævnt en del programfiler – her er det altså ikke selve programmet der fjernes, kun de midlertidige filer i forbindelse med installeringen af programmet eller andet.

De midlertidige filer fra mine tre browsere fylder en del. Mest fylder Internet Explorer, nok fordi jeg ser YouTube dér.

Hvis du klikker på fanen **Programmer**, kan du se mere om hvad der kan fjernes. Læg mærke til at jeg har fjernet fluebenet i Office 2010, da jeg har læst at netop Office kan være følsom for rensning.



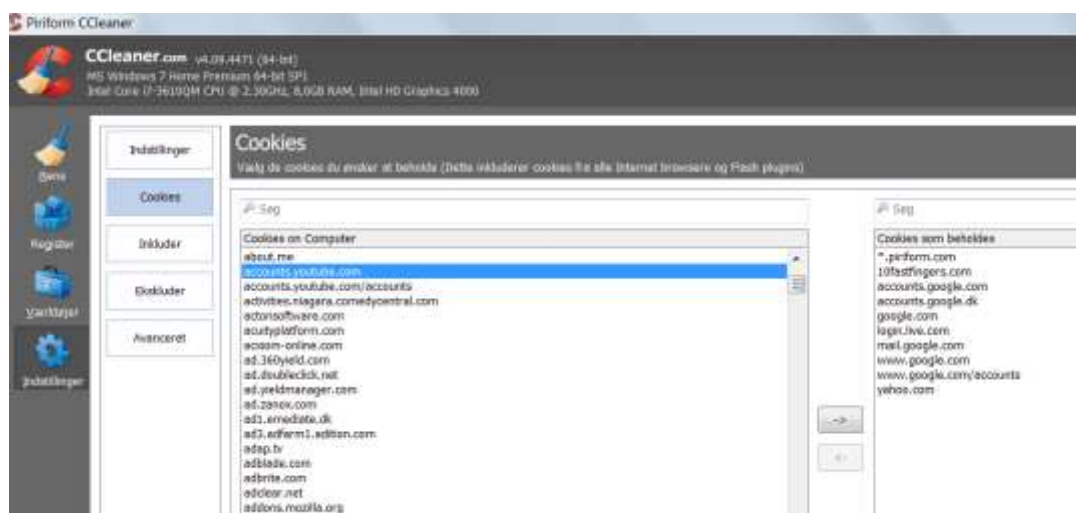
Cookies: slette eller gemme?

Som du kan se, bliver Internet cache, historie og cookies automatisk slettet. Gemte kodeord o.l. bliver ikke slettet, men du må være forberedt på at sletningen af cookies gør det nødvendigt at genindtaste en del oplysninger rundt om-

kring. Samtidig er du nødt til at slette dem, for det er tit her at de farlige reklamelinks ligger gemt.

Ved at klikke på **Indstillinger** og vælge **Cookies** i venstre side kan du dog gemme de bedste cookies.

Som du måske kan ane på nedenstående billede, har jeg en hel del cookies. Den markerede cookie (accounts.youtube.com) kunne måske være smart at beholde, og det gør jeg ved at trække den over i højre side. Mange cookies er nemlig nyttige, og det er derfor godt at kigge listen igennem.



I skærbilledet optræder imidlertid en cookie fra ad.doubleclick.net. Det er en kendt reklamevirus, der skaber reklamer fx hver gang man klikker på en Google-søgning. Den kommer ikke med. Det gør heller ikke cookien længere nede fra *Russian Girls* og fra *Ryan Air*. Jeg ved ikke hvordan *Russian Girls* er kommet, men ved at jeg tit får underlige reklamer fra interesserede russiske piger på min Facebook, så mon ikke den har noget med det at gøre.

Cookien fra Ryan Air er sikkert fin nok. Men mange mener at Ryan Air holder øje med dine søgninger på billige flybilletter, således at prisen stiger jo flere gange du søger på samme afgang.

Derfor får den heller ikke lov at komme med...

Igangsæt Rens

Og så er det bare at klikke på knappen **Kør rens**.

Du får i første omgang en advarsel om at der bliver slettet filer permanent. Hvis du har tjekket dine cookies og fjernet markeringen i Office-pakken, skal du ignorere advarslen.

Hos mig fik jeg fjernet over 5 gigabyte.

Styr computeren bedre med Ccleaner

Klik på **Register** til venstre under de forskellige værktøjer. Vælg **Skan efter problemer**. Klik derefter på **Udbedre valgte problemer**. Du bliver spurgt om du vil oprette en sikkerhedskopi af ændringer i registrerings-databasen – sig hellere ja. Derefter bliver computeren rensed for endnu flere affaldsfil.

formance is poor". Den forblev trods grundig rensning og poppede op overalt, specielt i Youtube-videoer.



Den er naturligvis malware eller adware som de øvrige programmer, men svære at fjerne. Her er hvad jeg gjorde – det er en lang historie...

Fjern programmet fra computeren


Afinstaller først det oprindelige program der installerede "Din PC's ydelse". Det kan være svært at finde. Brug Ccleaner eller gå til Kontrolpanel. Når programoversigten er åbnet, kan du klikke på søjlen to gange for at få de sidst installerede programmer øverst. Kig dem igennem. Hvis du kan huske hvornår du begyndte at se annoncen, kan det hjælpe.

Mulige programnavne kan være: RightSaver, SafeSaver, DP1815, Video Player, Convert Files for Free, Plus-HD 1.3, BetterSurf, Media Player 1.1, PassShow, LyricsBuddy-1, YoutubeAdBlock 1.2, Media Player 1.1, Savings Bull, Feven Pro 1.1, Websteroids, Savings Bull, HD-Plus 3.5, QuickShare.

Muligvis er der ikke engang installeret noget program... Det hele kan nemlig ske via webbrowsere.

Fjern programmet fra Internet Explorer og andre browsere

Internet Explorer

Klik på  (Funktioner) og vælg Internet Indstillinger. Klik her på fanen Avanceret og på knappen Nulstil. Sig ja til at fjerne personlige indstillinger. Gem og luk IE.

Hos mig virkede dette dog ikke. Som vist senere viste det sig at jeg havde to versioner af Internet Explorer installeret, og at "Din pc's ydeevne"-programmet

havde gemt sig i den anden version. Se sidst i denne vejledning for nærmere beskrivelse af dette.

Chrome

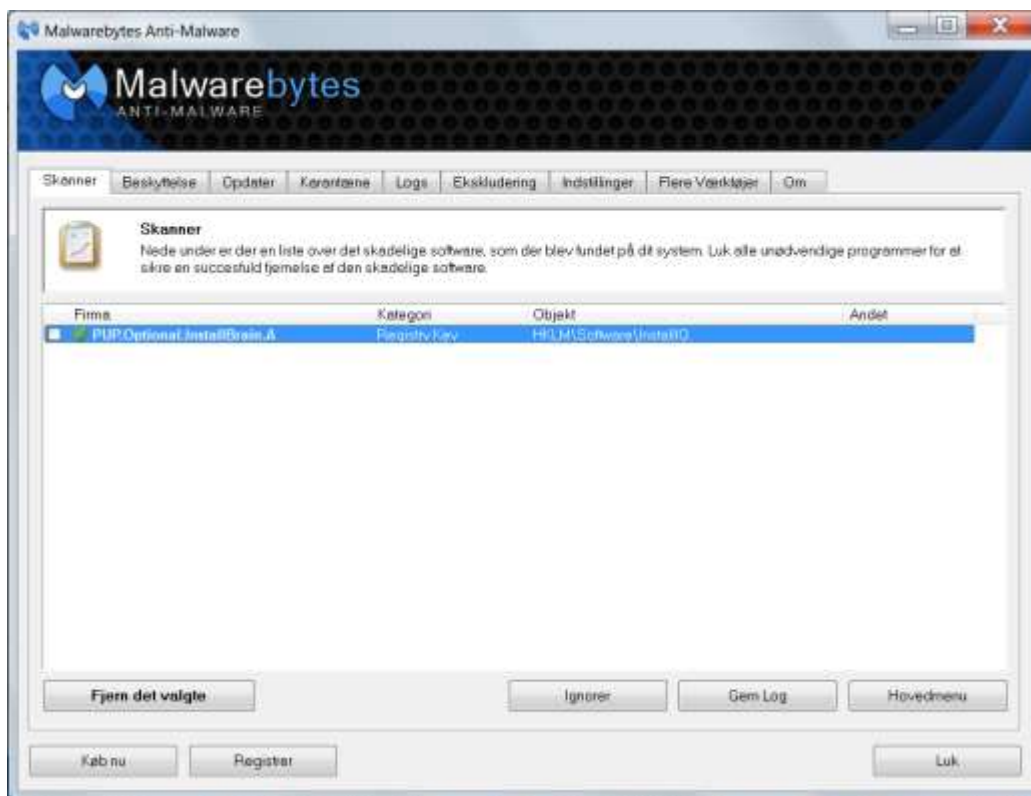
Klik på menuen øverst til højre ☰ og vælg Værktøjer/Udvidelser. Kig her efter mistænkelige udvidelsesprogrammer. Fjern dem.

Firefox har en tilsvarende indstilling. Øvrige browsere sikkert også.

Fjern programmet med Malwarebytes

Som nævnt virkede det ikke hos mig. Jeg gik derfor videre med det avancerede program Malwarebytes. Hent og installer Malwarebytes fra dette link: <http://www.malwarebytes.org/free/>. Ligesom med Ccleaner er der både en gratis og en betalingsversion. Du behøver ikke betale.

Malwarebytes anbefaler at man starter med en **Hurtig scanning**. Hos mig gav det følgende resultat:



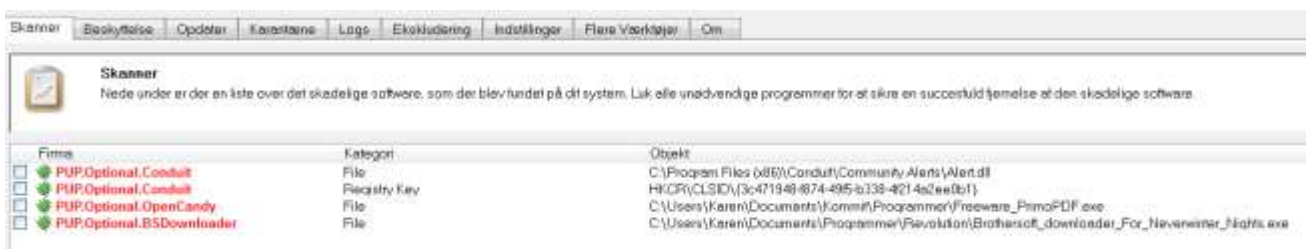
Ved at højreklikke på den markerede fil får man adgang til **"Vælg alle objekter"**, der udvider søgningen på filer fra kilden. Gør det og klik derefter på **Fjern det valgte**.



Umiddelbart efter jeg havde gjort dette, kom mit antivirus-program Avira med følgende advarsel:



Jeg går dog ud fra at Avira bare registrerede at Malwarebytes gik ind og fjernede filer. Men måske lykkedes det ikke at fjerne filen. Der var i hvert fald stadig problemer, og jeg valgte derfor at køre en **Fuld scanning**. Den gav følgende resultat:



Jeg højreklikkede først på filerne og valgte **Fjern alt fra dette firma**, før jeg gik videre til helt at fjerne dem. Endelig genstartede jeg computeren.

Tilsyneladende var rensningen en succes. I hvert fald var "Din pc's ydelse" væk fra Chrome. Men på Internet Explorer fortsatte den.

Endelig succes igennem afindstilling af Internet Explorer

Jeg fandt det interessant at Chrome fungerede, men ikke Internet Explorer, og bestemte mig derfor – meget frustreret – for at afinstallere Internet Explorer.

I **Kontrolpanel** kan man imidlertid ikke se Internet Explorer. Det kunne jeg først da jeg valgte **Vis installerede Opdateringer**. Det viste sig at jeg havde to Internet Explorer'ere installeret. Den ene hed bare Internet Explorer. Den anden hed Internet Explorer 10 da-DK Language Pack.

Jeg fjernede den første version og beholdt den anden.

Dernæst genstartede jeg computeren.

Og så åbnede jeg Internet Explorer.

Ingen mistænkelige reklamer. Ingen "Din pc's ydeevne er ringe".

Og sådan er det stadig.

Forklaringer og løsninger

Jeg skal ikke kunne sige præcist hvordan jeg har fået den dejlige reklame-virus. Men mens jeg tænkte, poppede mit batteri-program "Battery Care" op med en besked om at det skulle opdateres. Jeg har altid tænkt at det var et smart program der forlængede mit batteris levetid med de jævnlige påmindelser om at jeg skal huske at kalibrere det (dvs. først oplade computeren fuldt, dernæst lade den stå med strøm på i to timer, dernæst fjerne strømmen og lade computeren gå i dvale af sig selv i mindst 5 timer, hvorefter batteriet skulle fungere bedre).

Men nu klikkede jeg så på opdateringslinket og gik i gang med at downloade opdateringen. Tidligere er jeg ikke blevet spurgt om opdateringer, så jeg tror at jeg har fået fjernet den automatiske opdatering, da jeg rensede min computer med Ccleaner.

Undervejs gik det op for mig at BatteryCare meget diskret spurgte mig om lov til at installere en "toolbar", som jeg ikke kendte. Jeg sagde nej. I næste dialogboks var der endnu et program (Conduit), som jeg også aktivt skulle sige nej til.

Jeg tjekkede Conduit og BatteryCare ud på nettet og fandt adskillige oplysninger om at især Conduit er et malware-program, hvis eneste formål er at lukke andre, skadelige programmer ind på din computer. BatteryCare selv ser ud til at være nyttesløst.

Jeg fjernede selvfølgelig BatteryCare. Men der kommer sikkert noget andet på et andet tidspunkt. Så er det bare at komme i gang igen med rensningen.

Hvis du læser dette, er det nok fordi du selv har problemer. Hvis ikke min vejledning hjalp dig, så prøv at besøge Malwaretips, nævnt i indledningen:

<http://malwaretips.com/blogs/>

EN FORTSÆTTELSE AF SAGAEN, MAJ 2014:

På et eller andet tidspunkt i marts eller april fik jeg trods alle forsigtighedsregler alligevel virus. Jeg mener det kom i forbindelse med at jeg installerede det uskyldige program Geogebra fra den knap så uskyldige side Softonic.com. Aldrig brug den. Adlød Malwarebytes og slettede diverse programmer, men slettede så også den oprindelige installationsfil til Geogebra. Måske var det det. I hvert fald blev halvdelen af mine programmer saboteret, sådan uden videre. Jeg ved ikke hvad der skete, ikke andet end at ikonerne på computeren fra det ene øjeblik til det næste fik det der kedelige udseende, der signalerer at genvejen ikke virker længere. Og altså heller ikke programmet.

Jeg kørte så systemgendannelse, men fik desværre ikke valgt en dato langt nok tilbage i tiden (tror jeg da). Jeg fik de fleste programmer igen, men vedblev at have problemer med at starte fx Skype. Jeg var tæt på at formattere hele computeren, men turde ikke.

Nu, i maj, var jeg så kommet over på den anden side igen. Og så begynder den fordømte reklame at poppe op igen. Jeg havde netop installeret Jaws (en skærmlæser), som jeg ikke mistænkte, Wise Cleaner og Wise Uninstaller (som jeg egentlig heller ikke mistænker) samt nogle opdateringer, som havde vedligeholdt sig selv. Men de så heller ikke mistænkelige ud: Sentinel System Driver Installer (noget Microsoft noget) og Microsoft Visual Basics C++.

For en sikkerheds skyld afinstallerede jeg Jaws (7 underprogrammer!) og Wise-programmerne. Så læste jeg min egen vejledning og genkendte navnet Conduit. Klikkede på Windows-knappen (Start-knappen), skrev Conduit i skrivefeltet. Forskellige resultater væltede frem: Conduit-mapper, NCH-mapper med Conduit i sig.

Jeg lavede en søgning (ikke længere Google – kan ikke bruges til den slags søgninger, da kunstige sider vælter op i søgeresultaterne. Brugte i stedet DuckDuckGo). Fandt at de to ting hænger sammen, altså NCh og Conduit, og at begge er kendt for at indeholde malware.

I NCH-mappen fandt jeg mere: Express Zip, Prism, VideoPad. Alt sammen programmer jeg ikke rigtig har fået til at virke, men som jeg ikke har forbundet med noget specielt. Nu ved jeg det så.