Nye våben

Brug Artikel 1232 i stedet for.

Skrevet den **02. Feb 2009** af **fromsej** I kategorien **Sikkerhed / Virus** | ★★★☆☆

Brug denne, den er noget nyere.
Artikel 1232

Da skidtprogrammørerne hele tiden bliver dygtigere, og efterhånden har lært at skjule sig for de gængse scannere, har jeg (vi) prøvet at sammensætte en ny vejledning.

Denne vejledning dækker Win XP, Win 2000 og delvist Win 98.

Betingelser for hjælp

Der er nogle krav, som vi stiller for overhovedet at ville prøve at rense maskiner.
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.

2. Windows skal være opdateret, XP med min. Servicepack 1, 2000 med Servicepack 4.

`Hvis der er Servicepack 2 på XP, skal den selvfølgelig ikke fjernes.`

Hent følgende programmer

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

Ccleaner
Hijackthis
SuperAntiSpyware

ComboFix

Installation og kørsel af programmerne

Crapcleaner (Manual)

Installer Crapcleaner, husk at fjerne fluebenet udfor installation af Yahoo toolbar.
Start Crapcleaner, fjern evt fluebenet i cookies, da du ellers vil miste dine login-cookies i diverse fora, er det ikke et problem, så lad fluebenet være.

Klik på kør Cleaner og lad den fjerne hvad den finder.
Klik så på Problemer 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.

SuperAntiSpyware
Start programmet, klik på Check for updates, når det er opdateret, luk programmet, du skal ikke scanne endnu.
Genstart i fejlsikret. (tryk på <F8> under opstarten)
Start SuperAntiSpyware, klik på Scan your Computer, sæt flueben i de drev der skal scannes.
(Fixed disk betyder harddisk)
Flyt prikken til Perform complete scan og klik på Næste, så kører scanningen.

Når den er færdig kommer der et vindue med en opsummering, klik på OK, klik så på næste og så på Udfør.

Der kommer et vindue med Quarantine and removal Complete, klik på OK, klik på Udfør.
Luk programmet, genstart normalt.

Hijackthis
Dobbeltklik på Alternativ.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.

Combofix
Kør så combofix.exe, og følg anvisningerne.
Du bør ikke klikke på vinduet imens værktøjet kører, idet det kan få din computer til at fryse.
Når combofix er færdig, og efter det har genstartet, skulle der gerne åbnes en logfil: combofix.txt, indholdet af denne fil må du gerne lægge ind i **Viruskategorien**, sammen med Hijackthislogfilen og loggen fra SuperAntiSpyware.
Start SuperAntiSpyware igen, klik på Preferences, skift til fanebladet Statistics/Logs, i vinduet dobbeltklikker du på SUPERAntiSpyware Scan Log, den åbner i notesblok.

Det vil sige ialt tre logfiler.

> 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.
Kopier denne linie ind i din Browser, 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 Alliance of Security Analysis Professionals

Kommentarer til artikel

Ds-zim , det er muligt, men det er en falsk positiv fra Avast.
Det er Ejvindh TeamSpywarefri der har lavet Rootchk, der er garanteret IKKE spy eller adware i.
Så nej, artiklen skal ikke ændres.

Smashlotus , der er sikkert ikke snavs i alle P2P klienter, og der findes legale ting der kan hentes den vej, men i langt de fleste tilfælde bliver P2P brugt til illegale ting, og der er risikoen for "præmier" kæmpestor, derfor vil jeg ikke spilde tid på at rense maskiner med fildeling.
En browser kan du sikre, og bruge med omtanke, men med P2P lukker du selv skidtet ind, det er forskellen. ;-)

Roenving , du har en pointe, det er rettet nu. ;-)

Kommentar af hojben d. 21. Sep 2007 | 1

Har endnu ikke haft brug for denne guide men ikke desto mindre ville jeg ikke tøve med at benytte den da jeg ved hva fromsej står for :)

Kommentar af ds-zim d. 24. Jul 2007 | 2

"Rootchk" blir dd 24 juli rated som Adware af Avast! AntiVirus!
Overvej at opdatere Artikel

Kommentar af jps6kb d. 23. Jul 2007 | 3

Jeg synes det er en super idé at lave en, "inden vi begynder" guide. IMO bliver den måske indledt en kende arrogant, men det har jo ikke noget med nytteværdien at gøre. ;)

Kommentar af ogra d. 03. Mar 2008 | 4

http://www.prevx.com/freescan.asp

Et program som virker mod denne virus

ogra

Kommentar af roenving d. 12. Mar 2008 | 5

Som sædvanligt super arbejde fra fromsej/Team Spywarefri !-)
-- og det er herligt at se kvikke reaktioner fra forfatteren !o]

Kommentar af john_stigers (nedlagt brugerprofil) d. 11. Sep 2008 | 6

Som sædvanlig et godt stykke arbejde.

smashlotus: det er derfor der findes antispyware, antivirus m.m. Browserne nu til dags er fyldt med huller,

som disse programmer hjælper med til at få fyldt ud så godt det kan lade sig gøre.
lqnne - du skal selvfølgelig oprette et spørgsmål som indeholder dine logs :)
ohhelpme - en falsk positiv!!! hvilken antivirus bruger du?

Kommentar af marathonmann d. 08. Mar 2008 | 7

Det ser ud til at fungere. Jeg mangler bare nogen der kan kontrollere mine log filer.

Kommentar af victor-1 d. 23. Jul 2007 | 8

Man kan jo ikke forvente andet end ordentligt arbejde fra den kant. :o)

Kommentar af smashlotus d. 17. Aug 2007 | 9

Rolig nu fromsej, det er overkill at afinstallere alle de programmer du nævner øverst. Eksempelvis så indeholder selve programmet Azureus INTET spy/ad/malware overhovedet! Det kan godt være man kan hente filer med spyware gennem denne og lignende fildelingsprogrammer - men det kan man også på resten af Internettet! Skal vi så ikke også afinstallere alle browsere, fordi der bevisligt kommer alverdens skidt ind den vej?! For lige at bruge din egen formulering.. Nej vel?!?! Håber ikke du tager denne kritik alt ofr ilde op - jeg ved godt at din hensigt er god.. :)

Kommentar af levich d. 12. Jul 2008 | 10

Hej Fromsej. Godt arbejde, men linket http://www.spywarefri.dk/downloads1/alternativ.exe er til en gammel version af Hijackthis.

Kommentar af ejvindh d. 09. Aug 2007 | 11

God artikel, selvom jeg personligt ikke er enig i vurderingen af fildelingsklienter. Angående rootchk, så har en bruger på Spywarefri hjulpet mig med at få Avast til at rette deres fejl. Rootchk skulle således ikke blive detekteret mere :-)

Kommentar af sasso d. 22. Jul 2008 | 12

Let forståeligt og superbrugbart. Tak for, at I gider hjælpe alle os andre. :o)
/sasso

Kommentar af kurdo d. 26. Jan 2008 | 13

har lige brugt det og det virkede, jeg kom altid ind i megaupload vis en side var langsom eller ikke fandtes, jeg tror faktisk det var combofix der rettede det, men jeg er ikk sikker! :) fantastisk..

Kommentar af kristianiversen d. 07. Aug 2008 | 14

Rigtig dejlig artikel. Har brugt den flere gange, og er altid top-of-mind når der skal fjernes skidt.

Kommentar af struve_aalborg d. 12. Mar 2008 | 15

Test

Kommentar af lqnne d. 24. Aug 2007 | 16

hvor skal jeg lægge mine logs ind? og hvorfor er der ikke en logfil inde i SUPERAntiSpyware > Preferences > Statistics/logs? (har kørt hele programmet, (40min) men den har ikke lagt en logfil derind)

Kommentar af mark-ch d. 27. Jan 2008 | 17

ok

Kommentar af dyrdal d. 01. Apr 2008 | 18

Hej Jeg har 3 logs... vil i kigge på dem?
ComboFix 08-03-30.5 - Signe Dyrdal 2008-04-01 16:00:01.1 - **FAT32**x86
Microsoft Windows XP Home Edition 5.1.2600.2.1252.1.1030.18.185 [GMT 2:00]
Running from: C:\Documents and Settings\Signe Dyrdal\Skrivebord\ny\ComboFix.exe
* Created a new restore point

WARNING -THIS MACHINE DOES NOT HAVE THE RECOVERY CONSOLE INSTALLED !!
.

((((((((((((((((((((((((((((((((((((((Other Deletions)))
.

C:\Documents and Settings\Signe Dyrdal\Application Data\FunWebProducts
C:\Documents and Settings\Signe Dyrdal\Application Data\FunWebProducts\Data\Signe Dyrdal\avatar.dat
C:\Programmer\FunWebProducts
C:\Programmer\MyWebSearch
C:\Programmer\MyWebSearch\bar\History\search2
C:\Programmer\MyWebSearch\bar\Settings\s_pid.dat
C:\Programmer\MyWebSearch\bar\Settings\setting2.htm
C:\Programmer\MyWebSearch\bar\Settings\settings.dat
C:\Programmer\outlook
C:\Programmer\outlook\p.zip
C:\WINDOWS\system32\bszip.dll
C:\WINDOWS\system32\cmd.com
C:\WINDOWS\system32\ping.com
C:\WINDOWS\system32\regedit.com
C:\WINDOWS\system32\tasklist.com
C:\WINDOWS\system32\tracert.com
D:\Autorun.inf

.
((((((((((((((((((((((Files Created from 2008-03-01 to 2008-04-01))))))))))))))))))))))))))))))))
.

2008-04-01 15:07 . 2008-04-01 15:08 <DIR> d-------- C:\Programmer\Fælles filer\Wise Installation Wizard
2008-04-01 15:02 . 2008-04-01 15:02 <DIR> d-------- C:\Programmer\CCleaner
2008-04-01 00:38 . 2008-04-01 00:39 <DIR> d-------- C:\Programmer\Trend Micro
2008-03-31 21:23 . 2008-03-31 21:23 <DIR> d-------- C:\Documents and Settings\Signe Dyrdal\DoctorWeb
2008-03-31 20:32 . 2008-03-31 20:32 <DIR> d-------- C:\Programmer\SUPERAntiSpyware
2008-03-31 20:32 . 2008-03-31 20:32 <DIR> d-------- C:\Documents and Settings\Signe Dyrdal\Application Data\SUPERAntiSpyware.com
2008-03-31 20:32 . 2008-03-31 20:33 <DIR> d-------- C:\Documents and Settings\All Users\Application Data\SUPERAntiSpyware.com
2008-03-31 20:30 . 2008-03-31 20:30 <DIR> d-------- C:\Documents and Settings\Signe Dyrdal\Application Data\Grisoft
2008-03-31 20:30 . 2008-03-31 20:30 <DIR> d-------- C:\Documents and Settings\All

Users\Application Data\Grisoft
2008-03-31 20:30 . 2007-05-30 14:10 10,872 --a------ C:\WINDOWS\system32\drivers\AvgAsCln.sys
2008-03-26 14:33 . 2008-03-26 14:33 <DIR> d-------- C:\Documents and Settings\Signe Dyrdal\WINDOWS
2008-03-24 12:22 . 2008-03-24 12:22 <DIR> d-------- C:\Programmer\Alwil Software
2008-03-19 18:56 . 2008-03-19 18:56 <DIR> d-------- C:\Programmer\GamesBar
2008-03-19 18:56 . 2008-03-19 18:56 <DIR> d-------- C:\Programmer\Gamenext
2008-03-19 18:56 . 2008-03-19 18:56 <DIR> d-------- C:\Documents and Settings\All Users\Application Data\TEMP

.
(((((((((((((((((((((((((((((((((((((((Find3M Report))
.
2008-02-27 18:12 --------- d-----w C:\Programmer\Microsoft SQL Server Compact Edition
2008-02-27 18:07 --------- d-sh--w C:\Programmer\Fælles filer\WindowsLiveInstaller
2008-02-27 18:07 --------- d-----w C:\Programmer\Windows Live
2008-02-27 18:06 --------- d-----w C:\Documents and Settings\All Users\Application Data\WLInstaller
2008-02-01 09:17 586,752 ----a-w C:\WINDOWS\WLXPGSS.SCR
2008-01-11 04:40 44,544 ----a-w C:\WINDOWS\system32\dllcache\pngfilt.dll
.

(((((((((((((((((((((((((((((((((((((((Reg Loading Points))
.
.
Note empty entries & legit default entries are not shown
REGEDIT4

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"CTFMON.EXE"="C:\WINDOWS\system32\ctfmon.exe" [2004-08-27 05:00 15360]
"MsnMsgr"="C:\Programmer\Windows Live\Messenger\MsnMsgr.exe" [ ]
"updateMgr"="C:\Programmer\Adobe\Acrobat 7.0\Reader\AdobeUpdateManager.exe" [2006-03-30 16:45 313472]
"SUPERAntiSpyware"="C:\Programmer\SUPERAntiSpyware\SUPERAntiSpyware.exe" [2008-02-29 16:03 1481968]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"LaunchApp"="Alaunch" []
"SynTPLpr"="C:\Programmer\Synaptics\SynTP\SynTPLpr.exe" [2004-05-20 19:57 98304]
"SynTPEnh"="C:\Programmer\Synaptics\SynTP\SynTPEnh.exe" [2004-05-20 19:57 532480]
"RemoteControl"="C:\Programmer\r\CyberLink\PowerDVD\PDVDServ.exe" [2003-10-21 11:52 40960]
"BluetoothAuthenticationAgent"="bthprops.cpl" [2004-08-27 05:00 110592 C:\WINDOWS\system32\bthprops.cpl]
"IMJPMIG8.1"="C:\WINDOWS\IME\imjp8_1\IMJPMIG.exe" [2004-08-27 05:00 208952]
"MSPY2002"="C:\WINDOWS\system32\IME\PINTLGNT\ImScInst.exe" [2004-08-27 05:00 59392]
"PHIME2002ASync"="C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.exe" [2004-08-27 05:00 455168]
"PHIME2002A"="C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.exe" [2004-08-27 05:00 455168]
"IgfxTray"="C:\WINDOWS\system32\igfxtray.exe" [2004-02-11 01:55 155648]
"HotKeysCmds"="C:\WINDOWS\system32\hkcmd.exe" [2004-02-11 01:51 118784]
"EPM-DM"="c:\acer\epm\epm-dm.exe" [2004-07-14 14:19 151552]
"ePowerManagement"="C:\Acer\ePM\ePM.exe" [2004-09-01 17:38 2876416]
"LManager"="C:\Programmer\Launch Manager\QtZgAcer.EXE" [2004-07-30 11:30 319488]
"SunJavaUpdateSched"="C:\Programmer\Java\jre1.6.0_05\bin\jusched.exe" [2008-02-22 04:25 144784]
"HPDJ Taskbar Utility"="C:\WINDOWS\system32\spool\drivers\w32x86\3\hpztsb12.exe" [2005-03-08 06:42 176128]
"GrooveMonitor"="C:\Programmer\Microsoft Office\Office12\GrooveMonitor.exe" [2006-10-27 00:47 31016]

"!AVG Anti-Spyware"="C:\Programmer\Grisoft\AVG Anti-Spyware 7.5\avgas.exe" [2007-06-11 11:25 6731312]

[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]
"CTFMON.EXE"="C:\WINDOWS\system32\CTFMON.EXE" [2004-08-27 05:00 15360]
"Nokia.PCSync"="C:\Programmer\Nokia\Nokia PC Suite 6\PcSync2.exe" [2007-03-27 15:58 1744896]

C:\Documents and Settings\All Users\Menuen Start\Programmer\Start\
HP Digital Imaging Monitor.lnk - C:\Programmer\HP\Digital Imaging\bin\hpqtra08.exe [2005-05-11 23:23:26 282624]
ZyXEL G-162 Wireless Adapter Utility.lnk - C:\Programmer\ZyXEL\G162\Gcc.exe [2007-09-12 17:23:45 36864]
Adobe Reader Speed Launch.lnk - C:\Programmer\Adobe\Acrobat 7.0\Reader\reader_sl.exe [2005-09-23 22:05:26 29696]

[hkey_local_machine\software\microsoft\windows\currentversion\explorer\shellexecutehooks]
"{5AE067D3-9AFB-48E0-853A-EBB7F4A000DA}"= C:\Programmer\SUPERAntiSpyware\SASSEH.DLL [2006-12-20 12:55 77824]

[HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\winlogon\notify\!SASWinLogon]
C:\Programmer\SUPERAntiSpyware\SASWINLO.dll 2007-04-19 12:41 294912
C:\Programmer\SUPERAntiSpyware\SASWINLO.dll

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\Adobe Photo Downloader]
--a------ 2005-06-06 23:46 57344 C:\Programmer\Adobe\Photoshop Album Starter Edition\3.0\Apps\apdproxy.exe

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\BullGuard]
C:\Programmer\BullGuard Ltd\BullGuard\bullguard.exe

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\HP Software Update]
--a------ 2005-05-11 23:12 49152 C:\Programmer\HP\HP Software Update\HPWuSchd2.exe

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\startupreg\PCSuiteTrayApplication]
--a------ 2007-03-23 13:20 227328 C:\Programmer\Nokia\Nokia PC Suite 6\LaunchApplication.exe

[HKEY_LOCAL_MACHINE\software\microsoft\shared tools\msconfig\services]
"BsMailProxy"=2 (0x2)
"BsFire"=2 (0x2)
"BsFileScan"=2 (0x2)
"BgMainSvc"=2 (0x2)
"BgLiveSvc"=2 (0x2)

[HKEY_LOCAL_MACHINE\software\microsoft\security center]
"AntiVirusOverride"=dword:00000001

[HKLM\~\services\sharedaccess\parameters\firewallpolicy\standardprofile\AuthorizedApplications\List]
"%windir%\\system32\\sessmgr.exe"=
"C:\\Programmer\\Messenger\\msmsgs.exe"=
"C:\\Programmer\\LimeWire\\LimeWire.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpqtra08.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpqste08.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpofxm08.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hposfx08.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hposid01.exe"=

"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpqscnvw.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpqkygrp.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpqCopy.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpfccopy.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpzwiz01.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\Unload\\HpqPhUnl.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\Unload\\HpqDIA.exe"=
"C:\\Programmer\\HP\\Digital Imaging\\bin\\hpoews01.exe"=
"C:\\Programmer\\Microsoft Office\\Office12\\OUTLOOK.EXE"=
"C:\\Programmer\\Microsoft Office\\Office12\\groove.exe"=
"C:\\Programmer\\Microsoft Office\\Office12\\ONENOTE.EXE"=
"%windir%\\Network Diagnostic\\xpnetdiag.exe"=

R1 SMBHC;Driver til Microsoft SM Bus-værtscontroller;C:\WINDOWS\system32\DRIVERS\SMBHC.sys [2001-08-17 21:57]
R2 EpmPsd;Acer EPM Power Scheme Driver;C:\WINDOWS\system32\drivers\epm-psd.sys [2004-07-19 13:10]
R2 EpmShd;Acer EPM System Hardware Driver;C:\WINDOWS\system32\drivers\epm-shd.sys [2004-08-14 20:59]
R3 CBTNDIS5;CBTNDIS5 NDIS Protocol Driver;C:\WINDOWS\system32\CBTNDIS5.SYS [2003-07-16 22:28]
R3 odysseyIM3;Odyssey Network Services Miniport;C:\WINDOWS\system32\DRIVERS\odysseyIM3.sys [2003-05-14 16:01]
R3 SMBBATT;Driver til Microsoft Smart Battery;C:\WINDOWS\system32\DRIVERS\SMBBATT.sys [2004-08-03 23:07]
R3 TNET1130x;ZyXEL 802.11g Wireless Card;C:\WINDOWS\system32\DRIVERS\tnet1130x.sys [2004-06-10 17:14]

Newly Created Service - CATCHME
.
****

catchme 0.3.1344 W2K/XP/Vista - rootkit/stealth malware detector by Gmer, http://www.gmer.net
Rootkit scan 2008-04-01 16:01:36
Windows 5.1.2600 Service Pack 2 FAT NTAPI

scanning hidden processes ...

scanning hidden autostart entries ...

scanning hidden files ...

scan completed successfully
hidden files: 0

****
.
Completion time: 2008-04-01 16:02:05
ComboFix-quarantined-files.txt 2008-04-01 14:02:04
Pre-Run: 6,600,949,760 byte ledig
Post-Run: 6,590,578,688 byte ledig
.
2008-03-13 18:47:11   --- E O F ---

Logfile of HijackThis v1.99.1
Scan saved at 15:57:29, on 01-04-2008
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v7.00 (7.00.6000.16608)

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Acer\eManager\anbmServ.exe
C:\Programmer\Grisoft\AVG Anti-Spyware 7.5\guard.exe
C:\Programmer\Fælles filer\Microsoft Shared\VS7DEBUG\mdm.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\Explorer.EXE
C:\Programmer\Synaptics\SynTP\SynTPLpr.exe
C:\Programmer\Synaptics\SynTP\SynTPEnh.exe
C:\Programmer\r\CyberLink\PowerDVD\PDVDServ.exe
C:\WINDOWS\system32\rundll32.exe
C:\WINDOWS\system32\igfxtray.exe
C:\WINDOWS\system32\hkcmd.exe
C:\acer\epm\epm-dm.exe
C:\Programmer\Launch Manager\QtZgAcer.EXE
C:\Programmer\Java\jre1.6.0_05\bin\jusched.exe
C:\WINDOWS\system32\spool\drivers\w32x86\3\hpztsb12.exe
C:\Programmer\Microsoft Office\Office12\GrooveMonitor.exe
C:\Programmer\Grisoft\AVG Anti-Spyware 7.5\avgas.exe
C:\WINDOWS\system32\ctfmon.exe
C:\Programmer\SUPERAntiSpyware\SUPERAntiSpyware.exe
C:\Programmer\HP\Digital Imaging\bin\hpqtra08.exe
C:\Programmer\HP\Digital Imaging\bin\hpqSTE08.exe
C:\Programmer\ZyXEL\G162\Gcc.exe
C:\Programmer\HP\Digital Imaging\Product Assistant\bin\hprblog.exe
C:\Programmer\ZyXEL\G162\OdHost.exe
C:\Programmer\Internet Explorer\iexplore.exe
C:\Documents and Settings\Signe Dyrdal\Skrivebord\ny\alternativ.exe

R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.google.dk/
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =
http://go.microsoft.com/fwlink/?LinkId=69157
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =
http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =
http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =
http://go.microsoft.com/fwlink/?LinkId=69157
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Hyperlinks
O2 - BHO: Adobe PDF Reader Link Helper - {06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} -
C:\Programmer\Adobe\Acrobat 7.0\ActiveX\AcroIEHelper.dll
O2 - BHO: Groove GFS Browser Helper - {72853161-30C5-4D22-B7F9-0BBC1D38A37E} -
C:\PROGRA~1\MICROS~2\Office12\GRA8E1~1.DLL
O2 - BHO: SSVHelper Class - {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} -

C:\Programmer\Java\jre1.6.0_05\bin\ssv.dll
O4 - HKLM\..\Run: [LaunchApp] Alaunch
O4 - HKLM\..\Run: [SynTPLpr] C:\Programmer\Synaptics\SynTP\SynTPLpr.exe
O4 - HKLM\..\Run: [SynTPEnh] C:\Programmer\Synaptics\SynTP\SynTPEnh.exe
O4 - HKLM\..\Run: [RemoteControl] C:\Programmer\r\CyberLink\PowerDVD\PDVDServ.exe
O4 - HKLM\..\Run: [BluetoothAuthenticationAgent] rundll32.exe
bthprops.cpl,,BluetoothAuthenticationAgent
O4 - HKLM\..\Run: [IMJPMIG8.1] "C:\WINDOWS\IME\imjp8_1\IMJPMIG.EXE" /Spoil /RemAdvDef /Migration32
O4 - HKLM\..\Run: [MSPY2002] C:\WINDOWS\system32\IME\PINTLGNT\ImScInst.exe /SYNC
O4 - HKLM\..\Run: [PHIME2002ASync] C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.EXE /SYNC
O4 - HKLM\..\Run: [PHIME2002A] C:\WINDOWS\system32\IME\TINTLGNT\TINTSETP.EXE /IMEName
O4 - HKLM\..\Run: [IgfxTray] C:\WINDOWS\system32\igfxtray.exe
O4 - HKLM\..\Run: [HotKeysCmds] C:\WINDOWS\system32\hkcmd.exe
O4 - HKLM\..\Run: [EPM-DM] c:\acer\epm\epm-dm.exe
O4 - HKLM\..\Run: [ePowerManagement] C:\Acer\ePM\ePM.exe boot
O4 - HKLM\..\Run: [LManager] C:\Programmer\Launch Manager\QtZgAcer.EXE
O4 - HKLM\..\Run: [SunJavaUpdateSched] "C:\Programmer\Java\jre1.6.0_05\bin\jusched.exe"
O4 - HKLM\..\Run: [HPDJ Taskbar Utility] C:\WINDOWS\system32\spool\drivers\w32x86\3\hpztsb12.exe
O4 - HKLM\..\Run: [GrooveMonitor] "C:\Programmer\Microsoft Office\Office12\GrooveMonitor.exe"
O4 - HKLM\..\Run: [!AVG Anti-Spyware] "C:\Programmer\Grisoft\AVG Anti-Spyware 7.5\avgas.exe"
/minimized
O4 - HKCU\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\ctfmon.exe
O4 - HKCU\..\Run: [MsnMsgr] "C:\Programmer\Windows Live\Messenger\MsnMsgr.Exe" /background
O4 - HKCU\..\Run: [updateMgr] C:\Programmer\Adobe\Acrobat 7.0\Reader\AdobeUpdateManager.exe
AcRdB7_0_9
O4 - HKCU\..\Run: [SUPERAntiSpyware] C:\Programmer\SUPERAntiSpyware\SUPERAntiSpyware.exe
O4 - Global Startup: HP Digital Imaging Monitor.lnk = C:\Programmer\HP\Digital Imaging\bin\hpqtra08.exe
O4 - Global Startup: ZyXEL G-162 Wireless Adapter Utility.lnk = C:\Programmer\ZyXEL\G162\Gcc.exe
O4 - Global Startup: Adobe Reader Speed Launch.lnk = C:\Programmer\Adobe\Acrobat
7.0\Reader\reader_sl.exe
O8 - Extra context menu item: E&ksporter til Microsoft Excel -
res://C:\PROGRA~1\MICROS~2\Office12\EXCEL.EXE/3000
O9 - Extra button: (no name) - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} -
C:\Programmer\Java\jre1.6.0_05\bin\ssv.dll
O9 - Extra 'Tools' menuitem: Sun Java Console - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} -
C:\Programmer\Java\jre1.6.0_05\bin\ssv.dll
O9 - Extra button: Send til OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} -
C:\PROGRA~1\MICROS~2\Office12\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: S&end til OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} -
C:\PROGRA~1\MICROS~2\Office12\ONBttnIE.dll
O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} -
C:\PROGRA~1\MICROS~2\Office12\REFIEBAR.DLL
O9 - Extra button: (no name) - {e2e2dd38-d088-4134-82b7-f2ba38496583} - %windir%\Network
Diagnostic\xpnetdiag.exe (file missing)
O9 - Extra 'Tools' menuitem: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7-f2ba38496583} -
%windir%\Network Diagnostic\xpnetdiag.exe (file missing)
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Programmer\Messenger\msmsgs.exe
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} -
C:\Programmer\Messenger\msmsgs.exe
O11 - Options group: [INTERNATIONAL] International*
O16 - DPF: {1D4DB7D2-6EC9-47A3-BD87-1E41684E07BB} -
http://ak.exe.imgfarm.com/images/nocache/funwebproducts/ei/WebfettiInitialSetup1.0.0.15-3.cab
O16 - DPF: {5F8469B4-B055-49DD-83F7-62B522420ECC} (Facebook Photo Uploader Control) -
http://upload.facebook.com/controls/FacebookPhotoUploader.cab

O16 - DPF: {67DABFBF-D0AB-41FA-9C46-CC0F21721616} - http://download.divx.com/player/DivXBrowserPlugin.cab
O16 - DPF: {D6E7CFB5-C074-4D1C-B647-663D1A8D96BF} (Facebook Photo Uploader 4) - http://upload.facebook.com/controls/FacebookPhotoUploader4_5.cab
O18 - Protocol: grooveLocalGWS - {88FED34C-F0CA-4636-A375-3CB6248B04CD} - C:\PROGRA~1\MICROS~2\Office12\GR99D3~1.DLL
O18 - Protocol: ms-help - {314111C7-A502-11D2-BBCA-00C04F8EC294} - C:\Programmer\Fælles filer\Microsoft Shared\Help\hxds.dll
O18 - Protocol: wlmailhtml - {03C514A3-1EFB-4856-9F99-10D7BE1653C0} - C:\Programmer\Windows Live\Mail\mailcomm.dll
O18 - Filter hijack: text/xml - {807563E5-5146-11D5-A672-00B0D022E945} - C:\PROGRA~1\FÆLLES~1\MICROS~1\OFFICE12\MSOXMLMF.DLL
O20 - Winlogon Notify: !SASWinLogon - C:\Programmer\SUPERAntiSpyware\SASWINLO.dll
O20 - Winlogon Notify: igfxcui - C:\WINDOWS\SYSTEM32\igfxsrvc.dll
O20 - Winlogon Notify: WgaLogon - C:\WINDOWS\SYSTEM32\WgaLogon.dll
O23 - Service: Notebook Manager Service (anbmService) - OSA Technologies Inc. - C:\Acer\eManager\anbmServ.exe
O23 - Service: Ati HotKey Poller - Unknown owner - C:\WINDOWS\system32\Ati2evxx.exe
O23 - Service: AVG Anti-Spyware Guard - GRISOFT s.r.o. - C:\Programmer\Grisoft\AVG Anti-Spyware 7.5\guard.exe
O23 - Service: Pml Driver HPZ12 - HP - C:\WINDOWS\system32\HPZipm12.exe
O23 - Service: ServiceLayer - Nokia. - C:\Programmer\PC Connectivity Solution\ServiceLayer.exe

SUPERAntiSpyware Scan Log
http://www.superantispyware.com

Generated 04/01/2008 at 03:46 PM

Application Version : 4.0.1154

Core Rules Database Version : 3428
Trace Rules Database Version: 1420

Scan type : Complete Scan
Total Scan Time : 00:31:05

Memory items scanned : 181
Memory threats detected : 0
Registry items scanned : 5272
Registry threats detected : 0
File items scanned : 13025
File threats detected : 3

Adware.Tracking Cookie
C:\Documents and Settings\Signe Dyrdal\Cookies\signe_dyrdal@doubleclick[1].txt
C:\Documents and Settings\Signe Dyrdal\Cookies\signe_dyrdal@statse.webtrendslive[1].txt
C:\Documents and Settings\Signe Dyrdal\Cookies\signe_dyrdal@atdmt[2].txt

Håber i kan hjælpe....

Kommentar af snif12 (nedlagt brugerprofil) d. 23. Apr 2008 | 19

Vil lige gøre opmærksom på at det link til SUPERANTISPYWARE er til PRO versionen, burde det ikke rettes til FREEversionen???

Kommentar af ohhelpme d. 02. Sep 2008 | 20

hvorfor siger mit antivirus program at combofix er vira?

Kommentar af thomas_bork d. 20. Jul 2008 | 21

Jeg har et spørgsmål. Når jeg dobbeltklikker på ikonet til Combofix.exe, bliver jeg bedt om at finde et program at åbne filen med. Hvilket program skal jeg åbne den med?