Denne guide er oprindeligt
udgivet på Eksperten.dk

MSN virus

En foreløbelig vejledning.

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

> Foreløbeligt våben mod MSN virus

Når vi finder die "endloesung" bliver artiklen rettet til.

> Afinstaller MSN i Tilføj/Fjern programmer

Virussen smadrer exefilen til programmet.
C:\Programmer\MSN Messenger\msnmsgr.exe -> Worm.Licat.c : Renset med backup.
Fra Ewido.

Hent denne scanner.
Dr.Web
Billedvejledning

Alternativt link, hvis du ikke kan hente fra FTP:
Dr.Web

Hent denne scanner:
Ewido
Direkte download.
Installer og kør Ewido
Opdater straks efter installationen programmet (men lad være med at scanne endnu).

Hent og installer denne scanner:
SAS

Start superantispyware, klik på Check for updates, når det er opdateret, luk programmet og genstart i fejlsikret.

Dobbeltklik på drweb-cureit.exe, den vil køre en expressscan, det siger du ja til.
Når den skriver Done nederst til venstre, skal du klikke på Options->Change settings.
Skift til fanebladet Scan, fjern fluebenet ved Heuristic analysis.
Skift til fanebladet Actions, her skal alle punkter under Malware sættes til Rename.
Klik så på det eller de drev du vil have scannet, der kommer en rød prik for at vise det/de er valgt.

Klik så på den grønne pil ovre til højre på siden, så starter scanningen.
Første gang Dr.Web finder noget, klik "Yes to All", så fjerner den hvad den finder.
Når scanningen er færdig, gå op i file - Tryk på- Save Report list.
Så ligger der en en fil der her hedder "drweb.csv" på skrivebordet.
Luk Programmet.

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.

Stadig i fejlsikret:
Kør en fuld scanning med Ewido. Programmet laver en lille log, som du skal kopiere herind.

Genstart normalt.

Start superantispyware igen, klik på Preferences, skift til fanebladet Statistics/Logs, i vinduet dobbeltklikker du på SUPERAntiSpyware Scan Log, den åbner i notesblok, kopier resultatet herind.
Dobbeltklik på drweb.csv og kopier teksten fra den herind.

Gå ind her og hent Hijackthis.

Kør Hijackthis, scan, save log og kopier logfilen herind, så kigger vi på den.
Opret et spørgsmål i Virus kategorien, der er chancen størst for hjælp.
Lad være med at slette noget selv med Hijackthis, det kan skade mere end det gavner.

Gør dig selv den tjeneste at tjekke Karma og hvilke spørgsmål den bruger der vejleder dig har deltaget i, på Eksperten er der frit slag, risikoen ved dette er at man får forkert rådgivning, det er ikke sikkert at en af os der er vant til logløsning ser det, før det er for sent.

Hvad gør scannerne

Dr.Web har gang på gang vist sig effektiv til diverse infektioner.
Den gode doktor er "engangs", skal man bruge den igen, bør man hente en frisk.
Hovedsiden.

SuperAntiSpyware (SAS) er et nyt produkt, som har vist sig helt uhyggelig effektiv, overfor selv de sværeste infektioner, Spywarequake, Spyfalcon osv. altså Smitfraud familien snupper den, desuden rydder den godt op i en Lop infektion, og tilsyneladende også med hensyn til CWS.
Wareout kan den desværre ikke snuppe, men det er der heller ingen andre scannere der kan i øjeblikket.
Hovedsiden.

Abovergaard har lavet en mere udførlig vejledning, som kan findes her.

Hvis man ønsker "realtime" beskyttelse, så skal man købe programmet, men som scanner alene kan man klare sig med den gratis version.
(Programmet er fuldt på højde med SpySweeper)
Køb det f.eks hos Spywarefri.

Firmaet Ewido Networks blev grundlagt i 2002. Produktet Ewido Security Suite er et godt supplement til enhver virusscanner.
Ewido er en god spywarescanner, men især stærk over for trojanske heste. Hvor virusscannere ofte kan

finde og sætte trojanere i karantæne, så kan Ewido i langt de fleste tilfælde slette dem.

Undgå at blive inficeret

Virussen spreder sig via inficerede maskiners Messenger kontakter, den videresender en besked til alle kontaktpersoner.
En MSN besked fra ormen kan se ud som følgende:
"lol check http://w w w.uglyphotos.net/*****.PIF"**

Så får man et link over Messenger, lad være med at klikke på det, medmindre man selv har bedt om at få et link, og stoler 100% på den person der sender det.

Kommentarer til artiklen

Mobius6 >> Det er med nu, igår(19/9) havde vi mere travlt med at hjælpe med at fjerne den, end at finpudse artiklen. ;-)

Kommentar af eric-pedersen d. 14. May 2007 | 1

Kanon artikel :-)

Kommentar af john_stigers (nedlagt brugerprofil) d. 21. Sep 2006 | 2

Som altid godt arbejde fra sølvræven :)

Kommentar af kklm d. 20. Sep 2006 | 3

Super godt initiativ... Ekspert-hjælp når det er bedst

Kommentar af serverservice d. 01. Oct 2006 | 4

Jeg har hjulpet en privat for et par dage siden med at rense hans MNS virus ud. Maskinen blev scannet efter alle kunstens regler og fixet med Hijackthis (som forøvrigt Fromsej har lært mig i sin tid , og et par andre).
Men der var et par filer tilbage som ikke kunne slettes i fejlsikret - heller ikke med dr.delete. Det endte med at jeg måtte bruge denne metode fra Ejvind/Magic - og så kunne jeg endelig slette filerne
http://www.spywarefri.dk/forum/topic.asp?TOPIC_ID=29940
Men vil da kraftigt anbefale at man henvender sig til en ekspert , da den er temmelig hård at få renset ud- kan anbefale Fromsej eller en anden fra spywarefri - som jeg mener er landets bedste til den slags.

Kommentar af bredker d. 18. Sep 2006 | 5

let forståelig og fin detaljeret vejledning

Kommentar af mobius6 d. 20. Sep 2006 | 6

god artikel, jeg saver dog at vide HVORDAN jeg uds¿tter mig for den
downloades den via filer, eller anden måde? et er at have den, andet er at undgå den :-)
----------20/9 aktikkel rettet til så den er top :-)

Kommentar af uso d. 08. Feb 2007 | 7

Jeg kan kun sige tak!

Kommentar af psycosoft-funware d. 20. Sep 2006 | 8

som altid, et godt stykke arbejde fra fromsej. en Anti spyware/virus guru her på E :D
/psycosoft-funware

Kommentar af webstuff d. 21. Sep 2006 | 9

Lige en tilføjelse..
Der er kommet en ny version af virusen.
Den siger:
http://peopleonline.pe.funpic.de/*******.PIF

//webstuff

Kommentar af fazli d. 18. Sep 2006 | 10

Ja jeg vil også kalde det en forløbig artikel, Lad os nu se ad. Indtil videre er den meget fin

Kommentar af nikolaj2300 d. 25. Mar 2007 | 11

tak for informationen !! :D

Kommentar af profits d. 24. Apr 2008 | 12

Jeg aner ikke hvad jeg skal gøre. Jeg er ikke computergeni eller noget i den retning.. Jeg kan ikke hente Ewido deroppe via dét link.. Aner ikke hvad jeg skal gøre. Hjælp mig venligst..