FixWareout

Denne artikel hjælper dig med at finde, fjerne og beskytte dig imod Wareout infektionen.

Skrevet den **03. Feb 2009** af **fazli** I kategorien **Sikkerhed / Virus** | ★☆☆☆☆

I min tidligere artikel om Wareout blev jeg overstormet med dårlig kritik osv. Så jeg besluttede at gøre det bedre denne gang, og jeg håber det lykkedes hvis ikke, ja så er det bare surt for mig :).
Denne artikel er beregnet til brugere som er blevet inficeret og er igang med at få hjælp af en ekspert via Hijackthis. Den er også får brugere som vil vide lidt mere om denne infektion og til dem som vil igang med at løse hijackthis logge.

Jeg har delt artiklen op så den er lettere at overskue

1) Hvordan finder jeg Wareout?
2) Hvordan fjerner jeg Wareout?
3) Hvordan forhindrer jeg at Wareout kommer tilbage?

_-_-_-_-_-_

1) Hvordan finder jeg Wareout?

Før vi kan komme til at rense noget overhovedet må vi jo finde den drillende infektion først.
Hvis du er inficeret af Wareout vil der i Hijackthis loggen være en linie ligesom denne eller lignende:

O17 - HKLM\System\CCS\Services\Tcpip\..\{ECFF8F98-69BE-40ED-A311-2965DB08F05D}: NameServer = 69.50.184.84,195.225.176.37

Denne linie fortæller ikke ret meget men hvis du kopierer en af **IP'erne** fra linien f.eks. **"195.225.176.37"** og går ind på: http://www.all-nettools.com/toolbox og skriver **ip'en** ind på "SmartWhois" feltet og der kommer en **Ukrainsk** eller en anden mærkelig IP frem er du helt klart inficeret af denne infektion.
(I dette eksempel kommer der en Ukrainsk fætter frem)

2) Hvordan fjerner jeg Wareout?

Inden vi begynder her vil jeg gerne tilføje at du skal have hjælp af en Hijackthis ekspert til at tyde din logfil.

Nu skal vi igang med den Grove fjernelse af Wareout infektionen
Hent Fixwareout:
<a
href="http://www.bleepingcomputer.com/files/lonny/Fixwareout.exe">http://www.bleepingcomputer.com/files/lonny/Fixwareout.exe

Gem filen på dit Skrivebord og dobbeltklik på den. Klik **Next** -> **Install** og check, at der er et flueben i **"Run fixit"** - klik herefter på **Finish**. Fixet vil nu starte, og du skal blot følge instruktionerne. Du vil blive bedt om at genstarte din computer - gør venligst det. Genstarten vil tage lidt længere tid end normalt

Når dit skrivebord er loadet skal du Kopiere indholdet af **C:\fixwareout\report.txt** ind i dit spørgsmål sammen med en frisk **HijackThis log**.

Nu vil den Hijackthis ekspert du bliver hjulpet af gå videre med Hijackthis rensningen.
Det vil jeg ikke fortælle hvordan man gør da det kan gøres på forskellige måder.

3) Hvordan forhindrer jeg at Wareout kommer tilbage?

Nu har Hijackthis eksperten hjulpet dig til en ren computer, Hvad nu?

Ja hvis du vil forhindre den slags infektioner vil jeg anbefale dig disse programmer:

OBS! Følgende programmer er **gratis** og kan derfor bruges af alle.

http://www.javacoolsoftware.com/spywareblaster.html <- Spywareblaster forhindrer dig i at komme ind i mystiske hjemmesider som indeholder "snavs"

http://www.javacoolsoftware.com/spywareguard.html <- Spywareguard er en realtime beskytter mod Spyware og andet snavs, Den er uunværdlig for folk uden en realtime spywarescanner.

Det er også en god ide at rydde lidt op på din computer det kan CCleaner hjælpe dig med:
http://spywareinfo.dk/#/manualer/ccleaner.htm <- Manual til CCleaner

_-_-_-_-_-_

Skrevet af Fazli

Kommentar af 477 d. 19. Jul 2006 | 1

Intet nyt

Kommentar af nielle d. 19. Jul 2006 | 2

Fra Computerwold: "McAfee forventer, at antallet af registrerede ondsindede programmer vil vokse fra 200.000 til 400.000 i løbet af de næste to år". Jeg håber da ikke at vi skal have en artikel for hver af disse 200000 kommende vira?

Kommentar af magictouch d. 21. Jul 2007 | 3

Wareout kommer ikke fra de IP aresser du nævner. Desuden mangler du, at en ikke opdateret sun java kan være årsagen til infektionen.

Og når jeg går ind og tjekker - 195.225.176.37

Kommer jeg frem til -
IBC Tower Floor 9 PO Box 901-2389
Manuel Espinosa Batista Avenue

Det lyder ikke som Ukrainsk i mine ører

Kommentar af ejvindh d. 07. Aug 2006 | 4

Godt med en understregning af, at man ikke skal køre fixet uden vejledning. Men så synes jeg det bliver lidt overflødigt, idet en god supporter vil vide dette i forvejen. Pkt 2 er rigtig nok (selvom fixwareout faktisk ikke kan tage hele infektionen alene i øjeblikket), men jeg mener at pkt. 1 og 3 ikke er adækvate. En anden vigtig ting: Når man lægger sådanne fixes ud i det offentlige, er det vigtigt at man forpligter sig på at holde sig opdateret om infektionen, idet standardteksterne ofte må skrives om, ved nye udgaver af infektionen. Så medmindre man har tæt forbindelse med udviklerne, bør man være lidt forsigtig med det.

Kommentar af sorensen_123 d. 29. Jul 2006 | 5

Samme som sidst... Ikke noget nyt... Du skriver noget som jeg godt tror alle ved...
En dårlig måde at tjene points på.