Fejl efter spyware: Windows logger af med det samme

Lille hurtig vejledning til recovery

Skrevet den **03. Feb 2009** af **plx** I kategorien **Styresystemer / Generelt** | ⭐⭐⭐☆☆

Historie:
V1.1 - tilføjet ny metode

Hvis du lider af problemet med, at Windows logger af med det samme du forsøger at logge på, så er dette en mulig løsning.

Problemet skyldes at en bestemt fil og/eller værdi i registreringsdatabasen bliver ændret. Det drejer sig om:

c:\windows\system32\userinit.exe

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\userinit = c:\windows\system32\userinit.exe,

(På dit system kan Windows naturligvis være installeret på et andet drev end c:)

Metode 1:

Boot på din Windows CD og start en recovery console. Kopier userinit.exe fra cden:

X:\I386>expand userinit.ex c:\windows\system32

(X: er dit cdrom drev)

Skift bibliotek til:

C:\WINDOWS\SYSETM32\CONFIG

Omdøb din nuværende software hive (her gemmes oplysningen om userinit):

ren software software.old

Slet trygt disse to:

del software.sav
del software.log

Kopier den hive som blev lavet ved installation af Windows over i config-biblioteket:

copy c:\windows\repair\software

Genstart Windows normalt og start regedit.

Marker HKEY_LOCAL_MACHINE

Og load den gamle hive (software.old):

File > load hive

Som navn kan du give den 'old'

Under old kan du nu finde

Microsoft\Windows NT\CurrentVersion\Winlogon

Ændre 'userinit' til

c:\windows\system32\userinit.exe,

Genstart igen maskinen i en recovery console. Du skal igen starte med den oprindelige software hive:

slet 'software'
og omdøb 'software.old' til 'software'

Efter ny genstart skulle Windows gerne kunne logge på normalt igen.

Metode 2:

Jeg har set flere, som med fordel kunne gøre brug af en meget mere simpel metode: redigering af registry over netværk.

Hvis du har administrative rettigheder på den syge maskine, og den er konfigureret til at tillade redigering af registry over netværk (standard konfiguration), kan du blot gøre følgende:

I regedit > file > connect network registry

når du har opnået adgang, finder du blot den defekte registreringsværdi og laver den om.

Hvis du har adgang til registry over netværk, har du sikkert også adgang til de administrative shares, og af denne vej sikre at userinit.exe er på plads.

Kommentar af tonnybrandt d. 19. Apr 2005 | 1

Flot og gennemført arbejde. Jeg satta harddisken over som slave i en anden computer og brugte hovedelementerne i artiklen til at få den op at køre igen. Så jeg nøjedes med at restore userinit.exe og lave tricket med "load Hive" og rette værdien til den rigtige, hvorefter hd'en blev smidt tilbage i den gamle maskine igen og bootede som om den aldrig havde haft et problem. Det var så blot en 3 måde at gøre det på. Men tricket med Load Hive kendte jeg ikke, så det havde ikke været muligt uden din artikel. Tak for flot

arbejde !

Kommentar af smikkel d. 15. Apr 2005 | 2

Kommentar af serverservice d. 07. Jun 2005 | 3

Kanon - løste problemet første gang med noget repair og ændrede brugerkonto samt oprettede en ekstra bruger med admin - Men her er da den rigtige geniale IT-løsning - tak for det

Kommentar af sorenbs d. 25. Mar 2005 | 4

Har ikke prøvet, men dejlig information hvis det virker. Jeg har brugt mange timer på præcist det problem. Det skyldtes at jeg havde installeret to antivirusprogrammer samtidigt, og det brød den sig åbenbart ikke om. Jeg fik hjælp i denne tråd: http://www.eksperten.dk/spm/563509
Og linket der gjorde tricket var dette: http://support.microsoft.com/?kbid=307545

Kommentar af aa_1234 d. 31. Mar 2005 | 5

God artikel. kunne bare godt have brugt den lidt før :p

Kommentar af talrinys d. 27. Mar 2005 | 6

Har ikke selv haft problemet, men lyder godt hvis det virker, godt formuleret.

Kommentar af psycosoft-funware d. 20. Apr 2006 | 7

rigtig god artikel :D thumbs up/keep up the good work... /psycosoft-funware

Kommentar af patrion d. 24. Mar 2005 | 8

Fint

Kommentar af no1dane d. 29. Mar 2006 | 9