COMPUTERWORLD

Hårdt ramt af virus

Målet med denne artikel er hjælp til selvhjælp, ment som at kan man ikke udføre de normale renseprocedurer pga. at maskinen er for hårdt angrebet, så er der stadig muligheder med diverse værktøjer, inden håndklædet kastes i ringen.

Skrevet den **14. sep 2009** af **fromsej** I kategorien **Sikkerhed / Virus** | ⭐⭐⭐⭐☆

Jeg tillader mig at linke til min forrige artikel, hvor man finder standardvejledningen til at påbegynde rensningen.
http://www.eksperten.dk/guide/1232

Når man har prøvet guide1232 uden held, er der flere angrebsvinkler.

Redde vigtige data

Når maskinen er så inficeret at man ikke kan køre nogle værktøjer, er der en ret stor risiko for at man mister alle data, så dette punkt må være det første man gennemfører.

Til det formål vil jeg anbefale en Linux Live CD (her PuppyLinux), i hovedtrækkene henter man en ISO-fil på nettet og brænder den med sit brænderprogram, derefter sætter man CDén i den syge maskine og starter op på den.
Der er en skridt for skridt vejledning med billeder her:
Fremstilling af Puppylinux CD - http://bjergs.net/boot_iso.html
Vejledning i brugen - http://bjergs.net/puppy_live.html - Her er også downloadlink.
Vejledningen er lavet af Rookie fra Spywarefri.

Scanne fra CD

Kaspersky Rescue CD kan bruges, hvis du slet ikke kan komme ind i Windows, eller hvis du ikke kan få installeret andre værktøjer. Du kan brænde den ISO-fil, du henter fra Kaspersky og derefter starte computeren fra CD'en.

Hent ISO-filen herfra:
http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk/
Download den f.eks. til Skrivebordet på en velfungerende pc, så ISO-filen er let at finde, når du er færdig med at downloade den. Den fylder ca. 100 MB, så det tager nogen tid.

Dobbelt-klik på den downloadede fil. Nu skulle dit brænderprogram gerne starte op og klare brændingen.
Du skal bruge en tom cd til at brænde på.
Når cd'en er færdig, kan du tage den ud og lægge den i din problem-computer.

Genstart maskinen. Nu skulle den gerne starte Kaspersky-programmet op.
Ellers skal du ændre bootrækkefølgen i BIOS.
Lad programmet opdatere sig over Nettet, hvis du kan. (kræver en kabel-forbindelse)
Ellers prøv at køre programmet alligevel. Forhåbentlig kan vi få "hul" på infektionen på denne måde.
Når den er færdig, pil CDén ud og genstart.
Prøv så om du kan gennemføre guide1232.

Der findes selvfølgelig flere muligheder, her er en ufuldstændig liste:

http://www.techmixer.com/free-bootable-antivirus-rescue-cds-download-list/

Malwarebytes opdatering

Malwarebytes er en virkelig effektiv scanner, men hvis man ikke kan opdatere definitionerne pga. virusangreb, kan de hentes manuelt på en fungerende maskine, og derefter overføres på en CDR, hvorfra man så installerer program og opdateringer på "patienten".
(Lad være med at bruge en USB"pind", den kan blive inficeret, så problemet spreder sig)

Hent Malwarebytes Anti-Malware herfra:
http://www.besttechie.net/tools/mbam-setup.exe
Eller herfra ->
http://www.majorgeeks.com/Malwarebytes_Anti-Malware_d5756.html
Hent også opdateringen her:
http://www.gt500.org/malwarebytes/mbam-rules.exe
Eller her:
http://www.gt500.org/mbam-rules/database.jsp
Kopier de to exe filer over på patienten.
Installer malwarebytes luk det igen- når det er gjort dobbeltklik på mbam-rules. Start så Malwarebytes, flyt prikken til **Kør et fuldstændigt systemscan** - klik på **Skan Knappen** - lad programmet arbejde. Når det er færdig (det tager lidt tid afhængig af hvor meget du har på computeren).

Derefter - Tryk på **Vis resultater** knappen efter scanningen - og herefter tryk på **Fjern det valgte** - nu åbnes en txtfil(logfilen) og du skal gemme den et sted, hvor du kan finde den igen.

Genstart, se om du nu kan køre resten af programmerne i guide 1232.

Fejl i windows

Man kan være så uheldig at angrebet går målrettet efter windows eksekverbare filer (notesblok, paint, regedit osv.), opdager man at disse ikke fungerer, eller får en "file not found", er det et tegn på store og mange gange uoverstigelige problemer.
En infektion der opfører sig således er virut, den er i praksis umulig at rense for, så ser vi den i en Combofixlog, eller en Hijackthislog, vil vi altid anbefale formatering og nyinstallation.
Samtidig må man ikke gemme nogle former for exe eller scr -filer, dette gælder også selvom de er i et pakket zip eller rar arkiv, virut blæser lige igennem indpakningen, den er virkelig ondskabsfuld.
Læs mere her:
http://www.spywarefri.dk/artikel/ramt-af-virut/

Jeg håber ikke at der bliver meget brug for vejledningen her, men nu er den lavet.
Har i spørgsmål til den, eller når så langt at i får logfilerne fra guide1232, så spørg i forum(viruskategorien) her på Eksperten, eller i vores eget forum på www.spywarefri.dk
Begge steder sidder der kvalificerede personer der kan hjælpe.
(Det gør der sikkert også andre steder, men de to kender jeg)
I kan også spørge mig direkte pr. mail, men så må i forvente en vis svartid.

fromsej snabel-a spywarefri.dk

Mvh:
Fromsej

Kommentar af joker73arb d. 29. aug 2011 | 1

Super godt.. og som en evt. indledning eller afslutning:

Lad nu være med at åbne ting som man ikke ved hvad er!!
-at man modtager et link per mail, betyder ikke at man skal klikke på det..
-at man modtager en vedhæftet fil per mail, betyder ikke at man skal åbne den..
-at moster Karen pludseligt skriver engelsk skal da undre en!!
-at links ikke altid er hvad de udgiver sig for at være (til tider kan man holde musen over linket og se den aktuelle sti i bunden af mail klienten, alt efter hvilken klient der bruges)
-at PBS sender en mail på dårligt dansk!?!(det gør de så ikke)

BRUG nu den sunde fornuft derude.. det er den bedste antivirus...