COMPUTERWORLD

Ny Farlig Messenger Orm

Læs denne artikkel hvis du ikke allerede har hørt om den nye messenger orm. Koden er yderst skadelig og vanskelig at fjerne fra et inficeret system.

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

Ormen spreder sig især via messenger ved at man klikker på et meget "uskyldigt-udseende" link som automatisk popper op som en besked fra en af dine kontaktpersoner i messenger. Klikkes der på linket går det galt.

Ormen er meget ondsindet, den sørger bl.a. for automatisk at blive brændt ud på de cd'er du laver via Windows CD-brænder software! Den sørger også for at dræbe alle sikkerhedsrelaterede programmer såsom norton, mcafee, kaspersky osv. ligesom den lukker for REGEDIT.EXE, TASKMGR.EXE og MSCONFIG.EXE. m.fl.

Programmet gør det muligt for hackere at overtage kontrollen af den inficerede maskine. Derudover ændrer ormen i hostfilen så det bliver umuligt at tilgå en række sikkerhedsrelaterede hjemmesider heriblandt symantec.com, samtidig med at dit sikkersniveau i Internet Explorer bliver nedsat.

Jeg finder det forkert blot at copy paste en hel masse derfra hvor jeg har læst det. Så her er link til mere info på dansk:

[b](link dødt)
<<Update>> - <<Se i stedet symantecs link længere nede>>

og

[b](link dødt)
<<Update>> - <<Se i stedet symantecs link længere nede>>

Ormen spreder sig enormt hurtigt - jeg kender mange der allerede har haft besøg.

Removal tool kan gratis hentes fra symantec her:

http://securityresponse.symantec.com/avcenter/FixSflog.exe

Da ormen som førnævnt ændrer i hostfilen er det ikke muligt at hente denne fix fra symantecs side via den inficerede pc. Den skal hentes fra en anden computer og så overføres til den inficerede pc.

Der kan i øvrigt også læses mere om ormen hos symantec her:

http://securityresponse.symantec.com/avcenter/venc/data/w32.serflog.a.html

For at undgå inficering gennem messenger skal man undlade at klikke på "uskyldige" links såsom:

See my lesbian friends.pif
LOL that ur pic!.pif
My new photo!.pif
Me on holiday!.pif
The Cat And The Fan piccy.pif

Disse er nogle af ormens fantasifulde alias. Som hovedregel kan man sige, at når filnavnet har endelsen *.pif skal man være yderst varsom.

Bemærk, at ormen også spredes via p2p fildeling da den automatisk lægger kopier af sig selv i mapper såsom "My shared folder" med filnavne som eksempelvis "Messenger plus".

Mvh.
Peter/Smashlotus

PS.: Tak for al den positive respons for initiativet til denne "artikkel"... Jeg er fuldt ud enig i at det ikke er en egentlig artikkel, men jeg synes alligevel at informationen i artiklen er meget relevant og derfor mener jeg at dette var den mest åbenlyse metode til at få informationen spredt ud til så mange brugere som muligt, så vi kan begrænse spredningen af denne ondsindede virus mest muligt.

Endnu engang,
Mvh. Peter/Smashlotus

Kommentar af freeman5 d. 18. Mar 2005 | 1

Rar nok artikel :)

Kommentar af ysubhi d. 14. Mar 2005 | 2

har også selv oplevet at få sådan nogen beskeder. godt at nogen gør opmærksom på det.

Kommentar af the_email d. 10. Mar 2005 | 3

Godt råd, men ikke en artikel. Eksperten skulle næsten have et Tips og Tricks-system :-)

Kommentar af beorn d. 15. Mar 2005 | 4

Kommentar af mtrolle d. 08. Aug 2005 | 5

Kommentar af fredie89 d. 13. Mar 2005 | 6

Til jeres information kan man ikke hente dette lille værktøj fra symantec da denne side er blokeret når man har virusen.. ligger derfor en op www.fredie89.dk/FixSflog.exe her om lidt..

Kommentar af vaco d. 09. Mar 2005 | 7

Takker for oplysningen :-)

Kommentar af jih d. 09. Mar 2005 | 8

topkarakter! tak for tippet! :)

Kommentar af norbert d. 09. Mar 2005 | 9

Tja - det er jo ingen artikel, men til gengæld et knaldgodt initiativ til at hjælpe andre. Så derfor fuld støtte fra mig. :-)

Kommentar af afro_05 d. 09. Mar 2005 | 10

Lige hvad jeg søgte efter. Perfekt. Fuld karakter fra mig.

Kommentar af serverservice d. 14. Aug 2005 | 11

Smart idé at bruge artikler til nyt om de værste virus. Måske et lille tip til at lave en default hostfil? - vigtig ting for at kunne komme vidre skulle man blive inficeret.

Kommentar af michaelb.dk d. 13. Mar 2005 | 12

Er blevet tilbudt op imod 7-8 af disse omtalte filer, og det er da indlysende at man ikke skal tage imod dem :) Alligevel rigtig god ide du skrev artiklen, den orm er åbenbart meget udbredt nu!

Kommentar af ironmaiden d. 15. Mar 2005 | 13

Har også selv fået en fil tilsendt med teksten "LOL that ur pic!.pif" og tænkte det ku ske at være noget dirty virus-skidt så vist meget godt jeg ikke åbnede... men vidste slet ikke d ku la sig gøre før jeg selv så det :S

Kommentar af busschou d. 08. Sep 2005 | 14

Jeg synes det er fint nok at gøre opmærksom på sådanne vira. Men jeg synes omvendt også at folk der klikker på noget som lyder skummelt og oven i købet ender på .pif , ja så burde alarmklokken altså ringe hos folk

Kommentar af htmlkongen d. 09. Mar 2005 | 15

Tak for et godt tip :) /Htmlkongen

Kommentar af ddd_dendummedreng (nedlagt brugerprofil) d. 10. Mar 2005 | 16

Jeg syntes at det er godt at du kaster fatakt ud til os andre.
Når det er sådanne nogle ting skal vi alle være med på hvad der sker.
Og nu ved jeg det.

Kommentar af plazm d. 10. Mar 2005 | 17

Kommentar af the_ghost d. 10. Mar 2005 | 18

Rigtig godt initativ.

Kommentar af lund_dk d. 09. Mar 2005 | 19

Kommentar af da9el d. 16. Mar 2005 | 20

Kommentar af wicez (nedlagt brugerprofil) d. 09. Mar 2005 | 21

Godt initiativ, men dog som drillepinden heller ikke at det er en artikel.
Men anyways, topkarakter for det gode råd om at være varsom!

Kommentar af uso d. 18. Mar 2005 | 22

Kommentar af rhandersen d. 14. Mar 2005 | 23

Godt at få det at vide // RHandersen

Kommentar af maijen d. 09. Mar 2005 | 24

DET ER VIRKELIG UHYGGELIGT AT NOGLE FÅR NOGET UD AF AT ØDELÆGGE ANDRES PC'ER
DET ER JO UFATTELIG MANGE MENNESKER SOM BERØRES AF DETTE/DENNE PEST...
GODT AT NOGLE GIDER ULEJLIGHED MED AT GØRE OS ANDRE BRUGERE OPMÆRKSOM PÅ DISSE/DETTE...

Kommentar af klubba d. 10. Mar 2005 | 25

Kommentar af kdjweb d. 10. Apr 2005 | 26

har prøvet den :) det skal bare sendes vidre ;D inden det går galt

Kommentar af sorenknudsen d. 10. Mar 2005 | 27

Sgu nogle gode oplysninger som folk kan bruge til noget :)~

Kommentar af serverag d. 13. Mar 2005 | 28

Har os undret mig over at nogen fra min MSN liste prøver at sende mig nogle filer..
Men der er oz en fil som hedder noget med : frog chashed of train eller sådan noget..

Kommentar af zeff d. 09. Apr 2005 | 29

Kommentar af rambuk d. 01. Aug 2005 | 30