

Date: Samedi 16 juin 2007 à 21:54:36
Sujet: 3 Sécurité et Hacking

Supprimer le virus MSN Album Photo.zip

Vous avez reçu un fichier compressé intitulé:
"Album photo.zip" ou "photo.zip", vous l'avez ouvert et un virus a envoyé ce fichier à tous vos contacts avec un message du type "Il faut que tu télécharges ces photos". Je vais vous expliquer comment supprimer ce virus pour que vous puissiez enfin utiliser MSN sans envoyer des messages à tout le monde.

Le virus se transmet par msn en envoyant à tous vos contacts des messages comme ceux ci-dessous et en proposant de télécharger un fichier de photo.zip (il existe sous plusieurs noms).

En Français :

hey regarde les tof de notre bande de fous. :p
va voire ces photos de toi et moi !
hey c'est toi dans ces tof!?!??
hey regarde les tof, c'est moi et mes copains entrain de.... :D
j'ai fais pour toi cet album de photos tu dois le voire :p
stp regarde cet album de photos je lai fais specialement pour toi et mes amis... mes photos chaudes :D
t'as pas encore vu ces tof???

En Anglais :

Here are my very secret pictures for you.
Here are my pictures from my vacation
hmm is this you on the photo ?
Check out my pics from my workplace.
Nice new photos of me and my friends and stuff...
ahh look this is my greatest picture made on vacation 2007, take a look
Check out my nice photo album. :D

En Néerlandais :

hey kijk eens naar mijn nieuwe foto album
hey bekijk eens mijn nieuwe foto album
hmm ben jij dit op de foto ?
hey kijk ! dit is een lijst van mijn nieuwste fotos !
ahh kijk mijn mooiste foto album van vakantie 2007 bekijk ze eens
kijk dit zijn fotos van mij werkplek! :)
hmm ben jij dit op de foto ?

En Allemand :

meine hei en Fotos ! :p

En Italien :
le mie foto calde :p

En Espagnol :
mis fotos calientes
mi fotografas :p
Mi amigo tom?las fotos agradables de m?:p
el lol mi hermana quisiera que le enviara este album de foto
Si vous l'avez t?l?charg? alors suivait les
proc?dures de d?sinfection suivantes :
Supprimer le virus MSN Photo.zip (Backdoor.Win32.IRCBot.acd)
T?l?chargez [MSNFix.zip](#) sur votre bureau:
[MSNFix.zip](#) D?compressez-le (clic droit >> Extraire
ici) et double cliquer sur le fichier MSNFix.bat. Ex?cutez l'option
R. Si l'infection est d?tect?e, ex?cutez
l'option propos?e.
Si MSNFix vous demande d'?xecuter le scan en mode sans
&?chec alors :
Red?marrez votre ordinateur Au d?marrage de
l'ordinateur appuyez la touche F8 de votre clavier jusqu'? ce que les
options de d?marrage apparaissent. A l'aide des touches de
votre clavier descendez jusque "Mode sans ?chec" puis
valide par la touche [entr?e] Si le choix est propos?
choisis le m?me nom d'utilisateur qu'en mode normal. Puis
relancez le Fix comme d?crit plus haut.

Si tout se d?roule normalement, vous aurez desinfect? et
votre ordinateur et le virus aura ?t? supprim?, sinon
vous avez peut ?t? infect? par le nouveau virus
photo8.com. Dans ce cas l'? essayez ?galement la
proc?dure suivante.

Supprimer le virus Photo8.com (Trojan-Downloader.Win32.Agent.btu)
T?l?chargez [VundoFix.exe](#) Double-cliquez sur
l'ex?cutable [VundoFix.exe](#) que vous venez de t?l?charger
Cliquez sur le bouton Scan for Vundo Si le programme vous
demande de supprimer des fichiers, faites oui Lorsque le scan de votre
ordinateur est fini et que vous avez supprim? les fichiers,
red?marrez votre PC.
Si le virus n'a toujours pas ?t? d?tect? :
T?l?chargez [Antivir](#)
Installez [Antivir](#) que vous venez de
t?l?charger en suivant les ?tapes indiqu?es
Quand [Antivir](#) vous demandera Do you want to start an update now ?,
cliquez sur oui
Une fois la mise ? jour faites, red?marrez votre
PC en mode sans ?chec Pour acc?der au mode sans
&?chec, appuyez sur la touche F8 de votre clavier juste apr?s
le d?marrage de votre ordinateur. Appuyez sur F8 plusieurs fois pour
etre sur de lancer le choix, vous devriez avoir alors le choix entre

démarrez en mode normal ou en mode sans échec, choisissez le mode sans échec. Une fois dans le mode sans échec de Windows, lancez [Antivir](#) depuis l'icône du Bureau, cliquez ensuite sur l'onglet Scanner. Cochez tous vos disques durs pour que le scan soit complet, et lancez le scan. Si [Antivir](#) détecte un fichier infecté sur votre PC et qu'il vous propose soit de le supprimer soit de le mettre en quarantaine, je vous conseille de choisir la suppression. Lorsque le scan de votre ordinateur est fini et que vous avez supprimé les fichiers, redémarrez votre PC en mode normal cette fois. Votre ordinateur devrait être alors clean.

Tout ceux qui n'ont pas réussi à supprimer le virus après avoir suivi ces 3 procédures de désinfection sont invités à poster leur problème sur le [forum Sécurité](#) de manière claire et argumentée. Précisez bien le nom du fichier que vous avez ouvert, quelle phrase accompagne le fichier, et ce qui n'a pas fonctionné dans les procédures de désinfections précédentes.

Publication de Tout sur l'informatique - Programmation C#, Sécurité, Divx, P2P:
<http://www.zmaster.fr>

URL de cette publication
<http://www.zmaster.fr/modules.php?name=News&file=article&sid=210>