Date: Samedi 16 juin 2007 à 20:54:36
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 envoyer ce fichier a 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 puissez enfin réutiliser 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 :p
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 Espangol :
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 téléchargé alors suivait les procédures de désinfection suivantes :
Supprimer le virus MSN Photo.zip (Backdoor.Win32.IRCBot.acd)
Téléchargez MSNFix.zip sur votre bureau:
MSNFix.zip Décompressez-le (clic droit >> Extraire ici) et double cliquer sur le fichier MSNFix.bat. Exécutez l'option R. Si l'infection est détectée, exécutez l'option proposée.
Si MSNFix vous demande d'éxecuter le scan en mode sans échec alors :
Redémarrez votre ordinateur Au démarrage de l'ordinateur appuyez la touche F8 de votre clavier jusqu'à ce que les options de démarrage apparaissent. A l'aide des touches de votre clavier descendez jusque "Mode sans échec" puis valide par la touche [entrée] Si le choix est proposé choisis le même nom d'utilisateur qu'en mode normal. Puis relancez le Fix comme décrit plus haut.

Si tout se déroule normalement, vous aurez desinfecté et votre ordinateur et le virus aura été supprimé, sinon vous avez peut été infecté par le nouveau virus photo8.com. Dans ce cas là essayez également la procédure suivante.

Supprimer le virus Photo8.com (Trojan-Downloader.Win32.Agent.btu)
Téléchargez VundoFix.exe Double-cliquez sur l'executable VundoFix.exe que vous venez de télécharger
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 supprimé les fichiers, redémarrez votre PC.
Si le virus n'a toujours pas été détecté :
Téléchargez Antivir
Installez Antivir que vous venez de télécharger en suivant les étapres indiquées
Quand Antivir vous demandera Do you want to start an update now ?, cliquez sur oui
Une fois la mise à jour faites, rédémarrez votre PC en mode sans échec Pour accéder au mode sans échec, appuyez sur la touche F8 de votre clavier juste après le démarrage de votre ordinateur. Appuyez sur F8 plusieurs fois pour etre sur de lancer le choix, vous devriez avoir alors le choix entre

démarrer 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 complêt, 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 mette 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 reussi a supprimé le virus après avoir suivit ces 3 procédures de désinfection sont invités a poster leur probleme sur le forum Sécurité de manière claire et argumentée.
Précisez bien le nom du fichier que vous avez ouvert, quelle phrases accompagnée le fichier, et ce qui n'a pas fonctionné dans les procédures de désinfections précédentes.