

Date: Jeudi 07 octobre 2004 à 19:49:07

Sujet: 3 Sécurité et Hacking

Le virus Sobig.C : le successeur de Sobig.B

Tout sur le virus Sobig.C et les moyens de s'en débarrasser.

Sobig.C est un virus qui se propage par email et via les dossiers partagés comme [Sobig.B](#) (Mankx, Palyh). Mais le nom de l'expéditeur change ce n'est plus support@microsoft.com mais bill@microsoft.com. Il est accompagné d'un fichier joint dont l'extension est .PIF ou .SCR. La pièce jointe pèse environ 59.211 octets. Si sans méfiance vous exécutez ce fichier, le virus s'envoie à tous les correspondants présents dans votre carnet d'adresses Windows, ainsi qu'aux adresses email collectées dans les fichiers .DBX, .HTM, .HTML, .EML ou .TXT de votre ordinateur.

Comme [Sobig.B](#) ce virus est un ver qui se multiplie et s'envoie à votre carnet d'adresse Windows.

Les systèmes concernés par ce virus sont Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000 et Windows XP. Vous n'avez pas de soucis à vous faire si vous êtes sur Linux ou Mac.

Ce virus est déjà connu sous les noms de :

- Worm.Sobig.c (KAV)
- W32/Sobig.c@MM (Mc Afee)
- W32.Sobig.C@mm (Symantec)
- WORM_SOBIK.C (Trend Micro)

Mais attention si vous recevez un e-mail comportant les caractéristiques citées ne l'ouvrez pas même si le titre et les différents de ceux cités. Sobig.C comme [Sobig.B](#) se présente sous la forme d'un message dont le titre, le corps et le nom du fichier joint sont aléatoires. Quelques titres de messages :

- Re: Movie
- Re: Submitted (004756-3463)
- Re: 45443-343556
- Re: Approved Approved
- Re: Your application
- Re: Application

Le corps du message est toujours "Please see the attached file."

La pièce jointe possède une extension en .PIF ou .SCR. Quelques noms de pièces jointes :

- screensaver.scr movie.pif
- submitted.pif
- 45443.pif
- documents.pif
- approved.pif
- application.pif
- document.pif

Dans sa version actuelle, Sobig.C est conçu pour ne plus s'activer à compter du 08/06/03 et ne devrait donc plus se propager à partir de cette date. Mais souvenez-vous que [Sobig.B](#) ne devait plus se propager jusqu'au 31/05/03 et que Sobig.C est apparu le 31/05/03

donc une personne a tres legerement ameliorer [Sobig.B](#) pour propager Sobig.C. Les utilisateurs qui ont executé ce fichier doivent mettre à jour leur antivirus. Et on ne redira jamais assez n'ouvrez pas les e-mails d'utilisateurs inconnus surtout lorsqu'il accompagné d'une piece jointe suspecte, même si le sujet de l'e-mail est attrayant il ne faut pas exécuter un fichier joint sans l'avoir au préalable analysé avec un antivirus mis à jour régulièrement.

Pour éliminer ce virus vous pouvez telecharger [l'utilitaire de desinfection de Sobig.C.](#)

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

URL de cette publication
<http://www.zmaster.fr/modules.php?name=News&file=article&sid=26>