

Date: Jeudi 07 octobre 2004 à 20:12:43

Sujet: 3 Sécurité et Hacking

Le virus Sobig.B (Mankx, Palyh)

Palyh est un virus plus précisément un ver, comme tant d'autres qui se propage par email et via les dossiers partagés.

Palyh est un virus plus précisément un ver, comme tant d'autres qui se propage par email et via les dossiers partagés. La seule chose qui vous incite à l'ouvrir c'est le nom de l'expéditeur qui est support@microsoft.com. Il est facilement repérable car il est accompagné d'une pièce jointe en .PIF. 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. 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 d'autres noms comme I-Worm.Palyh (Kaspersky), W32/Palyh@MM (Mc Afee), W32.Sobig.B@mm (Symantec), W32.HLLW.Mankx@mm (Symantec), W32/Palyh-A (Sophos) et WORM_PALYH.A (Trend Micro). En fait il a juste été légèrement remanié. Il pèse 52.898 octets.

Le titre de l'e-mail et le nom du fichier joint sont aléatoires. On a pu pour l'instant voir Your details, Approved (Ref: 38446-263), Re: Approved (Ref: 3394-65467), Your password, Re: My details, Screensaver, Cool screensaver, Re: Movie et Re: My application.

Mais attention si vous recevez un e-mail comportant les caractéristiques citées ne l'ouvrez pas même si le titre est différent de ceux cités.

Le corps du message est toujours "All information is in the attached file". La pièce jointe possède une extension en .PIF comme, your_details.pif, ref-394755.pif, approved.pif, password.pif, doc_details.pif, screen_temp.pif, screen_doc.pif, movie28.pif et application.pif.

Dans sa version actuelle, Palyh est conçu pour ne plus s'activer à compter du 31/05/03 et ne devrait donc plus se propager à partir de cette date. Mais là encore attention certains petits malins prennent un virus puis le modifient ou renomment seulement le titre du message comme cela a été le cas pour le virus "I love you" qui a été rediffusé sous le titre de "Bonne fête maman".

Pour terminer si vous avez eu le malheur d'exécuter la pièce jointe en .PIF alors téléchargez [l'utilitaire](#) [pour le détecter et le détruire](#).

Quelques exemples de mail :

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=29>