ZaCker vous souhaite une mauvaise année 2002

On ne change pas une recette qui marche : on l'améliore. Le premier virus cuvée 2002 ressemble à ses prédécesseurs mais se révèle encore plus pernicieux...

Ce matin, la tête encore dans le réveillon de la Saint Sylvestre, vous avez allumé votre ordinateur. Surprise, votre bête à puces a changé de nom et s'appelle ZaCker.
Mauvaise, mais alors très mauvaise surprise : le ver ZaCker vous a frappé. Arrêtez tout et procurez-vous immédiatement le correctif adéquat. Sinon vous risquez de très graves tourments, notamment la suppression des fichiers portant les extensions -accrochez-vous - : htm, PHP, HTML, COM, BAT, MDB, SLQ, DOC, LNK, PPT, JPG, MPEG, INI, DAT, ZIP, TXT.

Ce n'est pas tout, l'infâme lombric va également tenter de détruire les fichiers utilisés par les anti-virus et autres logiciels de sécurité situés dans différents répertoires (Par exemple Program Files FindVirus ou Program FilesNorton AntiVirus ...).

Découvert en fin de semaine dernière par les principaux éditeurs, ZaCker porte également le nom de W32/Maldal.D@mm, ou encore W32.Maldal.E.

Les fidèles lecteurs de silicon.fr auront reconnu le type : il s'agit d'un ver Win32 qui se propage par l'intermédiaire de la messagerie Outlook via un fichier .exe d'une taille de 27 Ko(en réalité il s'agit d'un programme Visual Basic compressé avec Aspack).
Notons qu'il porte pratiquement le même nom - Maldal - que le ver signalé juste avant Noël (voir article en référence, ci-dessous), mais son mode d'infection et les dommages potentiels sont très différents.

Une fois de plus : rappelons que l'on ne transforme pas sa messagerie en "clicodrome" et on ne clique pas impunément sur n'importe quel message. Pourtant, en l'espèce, certains ont pu être trompés par l'intitulé et/ou le sujet du message. En effet, l'intitulé et/ou le sujet portent les noms d'une machine. Dans de très nombreux cas, la machine porte le nom de l'utilisateur. Lors de sa première exécution, la larve numérique renommera le nom du fichier attaché. Par exemple, vous pourrez recevoir un message électronique intitulé ZaCker accompagné d'un message sibyllin (par exemple Surprise !!!) et d'un exécutable portant le nom de la personne qui vous a infecté (par exemple pierre.exe). Le texte d'accompagnement est choisi au hasard parmi une trentaine. Tous sont en anglais mais sont suffisamment vagues pour pouvoir induire en erreur des utilisateurs peu méfiants ("Test this game", "I have got this file for you", "Test your mind" ...). La liste complète des possibilités est disponible sur les sites anti-virus de Sophos (www.sophos.com) et Symantec (www.sarc.com), notamment. Panda Software signale également que ZaCker contient des messages encryptés à caractère anti-sémite.
Répétons-le, ZaCker est une véritable sal...rie. Sortez couverts car le fait de renommer votre ordinateur en ZaCker constitue la dernière étape dans sa cascade de dégâts. Estimez-vous heureux d'avoir pu démarrer. Téléchargez immédiatement le correctif.

Par Stéphane Larcher pour :
Silicon

Par

Publié sur Cafeduweb - Archives le jeudi 3 janvier 2002
Consultable en ligne : http://archives.cafeduweb.com/lire/958-zacker-vous-souhaite-mauvaise-annee-2002.html