support@globalsp.com
+33 1 44 70 48 41
du lundi au vendredi de 8h à 19h

Restrictions pour les pièces jointes

Si des pièces jointes ne respectent pas la politique de sécurité, elles sont remplacées par un fichier texte explicatif qui vous informe des raisons du refus des pièces jointe. Les emails ne sont pas rejetés. Les fichiers de type exécutable (DOS/Windows/ELF) sont interdits.

Les noms des pièces jointes suivants sont interdits :

- les noms de fichier de 150 caractères et plus
- les noms de fichier contenant 10 espaces ou plus
- les noms de fichier contenant un CLSID (MS Class Identifier)
- les noms de fichiers portant des doubles extensions sauf .zip .bz2 .gz .Z .pdf
- les fichiers nommés webpage.rar car utilisés par le virus I-Worm.Yanker
- les fichiers portant les extensions .ceo utilisés virus WinEvar
- .com Windows/DOS Executable
- .exe Windows/DOS Executable
- .reg Attaque possible via la base de registre de Windows
- .chm Attaque possible via les fichiers d'aide compilés
- .cnf Attaque possible via SpeedDial
- .hta Attaque possible via les archives Microsoft HTML
- .ins Attaque possible via les paramétrages Microsoft Internet Comm.
- .js ou .jse Attaque possible via Microsoft JScript
- .lnk Attaque possible via la faille Eudora *.lnk
- .ma[dfgmqrstvw] Attaque possible via les raccourcis Microsoft Access
- .pif Attaque possible via MS-Dos program shortcut
- .scf Attaque possible via Windows Explorer Command
- .sct Attaque possible via Microsoft Windows Script Component
- .shb Attaque possible via document shortcut
- .shs Attaque possible via Shell Scrap Object
- .vb[es] Attaque possible via Microsoft Visual Basic script
- .ws[cfh] Attaque possible via Microsoft Windows Script Host
- .xnk Attaque possible via Microsoft Exchange Shortcut
- .scr Attaque possible via screensaver (économiseur d'écran)
- .bat Attaque possible via malicious batch file script
- .cmd Attaque possible via malicious batch file script
- .cpl Attaque possible via malicious control panel item
- .mhtml Attaque possible via Eudora meta-refresh

Les pièces jointes interdites sont remplacées par un message d'avertissement. En pratique, pour recevoir ou transmettre un exécutable, il est recommandé de l'archiver en zip. Les messages sont analysés par SpamAssassin pour détecter s'il s'agit de SPAM. Le traitement du message s'effectue selon le SPAM score selon la politique par défaut suivante:

- si le score est inférieur à 5, le message n'est probablement pas un SPAM, le message passe sans altération
- si le score est entre 5 et 10, le sujet est préfixé par [SPAM ?]
- si le score supérieur à 10, le sujet est préfixé par [SPAM]

Il est recommandé aux utilisateurs d'utiliser une règle déplaçant automatiquement les messages considérés comme des SPAMs dans un dossier spécial de leur messagerie, de consulter régulièrement ce dossier pour d'éventuels faux positifs et d'y effectuer le ménage.