

MEMENTO

Virus informatiques

SGDN/DCSSI/CERTA

23 juin 2005

1 Toujours la même chose !

Les virus se propagent toujours de la même façon.

1.1 Pièces jointes à un mail

| Date | Nom | Mode de propagation |
|------|-----------|--|
| 1999 | melissa | fichier .doc en P.J. |
| 2000 | ILOVEYOU | fichier .html .vbs en P.J. |
| 2001 | HOME PAGE | fichier .html .vbs en P.J. |
| 2001 | SIRCAM | fichier .jpg.exe ou .com.pif en P.J. |
| 2002 | Myparty | fichier www.myparty.yahoo.com (c.à.d .com) en P.J. |
| 2003 | Sobig.F | fichier .pif ou .scr en P.J. |
| 2004 | mydoom | fichier .pif, .scr, .exe, .cmd, .bat ou .zip en P.J. |

Certains antivirus *même à jour* ont été incapables d'arrêter de tels virus pendant plusieurs heures voire plusieurs jours.

1.2 Exploitation d'une faille de sécurité

| date | Nom | Faille dans | Correctif disponible |
|------|---------|-------------------|------------------------|
| 2001 | CodeRed | IIS | 1 mois avant le virus |
| 2001 | Nimda | IIS | 11 mois avant le virus |
| | | Internet Explorer | 6 mois avant le virus |
| 2002 | Klez-A | Internet Explorer | 9 mois avant le virus |
| 2003 | Slammer | SQLServer | 6 mois avant le virus |
| 2003 | Blaster | RPC DCOM | 1 mois avant le virus |

2 Quels sont les risques encourus ?

- 1° panique (peut faire plus de dégâts que le virus)
- 2° perte d'image (Votre organisme propage des virus)
- 3° fuite d'information (il ne devrait *jamais* y avoir d'information sensible sur une machine en réseau)
- 4° perte d'information (effacement d'un fichier non encore sauvegardé)
- 5° cheval de Troie, mise en place d'une porte dérobée
- 6° perte de temps
- 7° saturation des ressources informatiques

3 Reconnaître un virus dans un mail

C'est un message avec un fichier en pièce jointe. Si la pièce jointe est un fichier dont le nom se termine par (les extensions les plus fréquentes sont en **gras**) :

.ade, .adp, .asx, .bas, **.bat**, .chm, .cmd, **.com**, .cpl, .crt, **.exe**, .hlp, .hta, .inf, .ins, .isp, .js, .jse, **.lnk**, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, **.pif**, .reg, **.scr**, .sct, .shb, .shs, .url, .vb, .vbe, **.vbs**, .wsc, .wsf, .wsh

C'est probablement un virus.

Si la pièce-jointe est une archive (par exemple un fichier .zip) qui contient un fichier avec une telle extension c'est suspect aussi. Les extensions fréquentes de noms de fichiers contenant des archives sont :

.zip, .arj, .rar, .tar, .tar.gz, .tar.bz2, .tgz, .zoo, .lzh, .lha

4 Que faire pour prévenir l'infection

En suivant à la lettre ces recommandations vous ne serez pas contaminés.

4.1 Administration quotidienne de son système

- ne pas activer l'ouverture automatique des pièces jointes
- mettre à jour son ordinateur, c.à.d corriger les failles du système d'exploitation et des applications (penser aux portables). *Il vaut mieux mettre à jour 1 mois avant le virus, que réparer une heure après.*
- faire des sauvegardes

- utiliser un firewall (entrave les chevaux de Troie)
- utiliser et mettre à jour un antivirus.

4.2 Réception d'un mail suspect

- Ne pas baser *toute* sa confiance sur des solutions techniques telles que l'antivirus. Même si l'antivirus ne vous alerte pas, c'est peut-être un virus.
- Si on reçoit une pièce jointe suspecte :
 - 1° ne pas se fier à l'expéditeur (certains virus semblent venir de la hiérarchie, de la famille, de correspondants habituels ou de parfaits inconnus)
 - 2° ne pas cliquer sur la pièce jointe
 - 3° prévenir par téléphone le Service Informatique (SI) ou l'Officier de Sécurité Informatique (OSI)
 - 4° détruire le message

5 Que faire si vous êtes contaminé ?

- Débrancher le câble du réseau (la machine ne contamine personne, personne ne peut utiliser le cheval de Troie)



Fig. 1. Où se branche le câble réseau

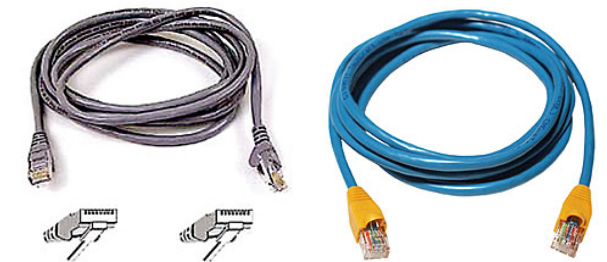


Fig. 2. À quoi ressemble un câble réseau

- Ne pas utiliser de disquettes (ou de clef USB, ...) sur cette machine
- Appeler l'OSI ou le SI (pour aider à nettoyer) téléphone