

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Rappels concernant les virus

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2001-ALE-012>

Gestion du document

Référence	CERTA-2001-ALE-012
Titre	Rappels concernant les virus
Date de la première version	13 septembre 2001
Date de la dernière version	09 janvier 2002
Source(s)	Réseau de confiance
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Augmentation du trafic sur le réseau ;
- perte de confidentialité ;
- destruction de données ;
- perte de contrôle et endommagement des systèmes.

2 Systèmes affectés

Indépendant de la plate-forme.

3 Résumé

Rappel de quelques mesures d'hygiène lié à la recrudescence de vers tels que Magistr.b et autres virus en tout genre.

4 Description

Au vu de l'augmentation du nombre de contaminations par les vers Sircam et Magistr, il apparaît nécessaire d'affermir et de revoir les mesures de protection contre la propagation des virus.

Méfiez-vous des pièces jointes ! Même si le message provient d'une personne que vous connaissez. Les virus se propagent souvent en s'envoyant aux adresses de messagerie se trouvant dans le carnet d'adresses.

N'ouvrez pas une pièce jointe dont vous n'attendiez pas la réception.

Analysez tous les fichiers reçus en pièce jointe, par disquette, par CD-ROM ou par tout autre moyen, avant leur ouverture. Soyez encore plus méfiant en ce qui concerne les fichiers qui permettent l'exécution de code (Tous ceux qui ont une extension en : .exe, .com, .bat, .cmd, .pif, .htm, .html, .hta, .reg, .lnk, .vbs, .js, .shs, .shb, par exemple). Soyez d'autant plus vigilant s'il y a une double extension telle que .doc.pif, .txt.vbs, ou .htm.shs, ce n'est pas normal.

N'oubliez pas que même des documents (WORD ou EXCEL par exemple) peuvent permettre l'exécution de code par l'exécution des macros. Désactivez l'exécution des macros au démarrage de ces logiciels.

N'affichez pas les messages au format HTML, forcez votre logiciel de messagerie à les convertir en texte simple.

De même, forcez-le à n'envoyer que des messages en texte seul, ce qui permet à vos correspondants de ne pas abaisser leur niveau de sécurité pour les lire.

Désactivez l'exécution du Java, des Javascript et surtout des contrôles ActiveX de vos logiciels de messagerie et de vos navigateurs.

Relisez les recommandations que nous avons faites dans nos notes d'information, avis et alertes précédents : CERTA-2000-INF-002, CERTA-2000-ALE-001, CERTA-2000-ALE-002, CERTA-2000-REC-002, CERTA-2000-REC-003 de 2000, ainsi que les alertes récentes de l'année 2001 : CERTA-2001-ALE-006, CERTA-2001-ALE-009 et ses mises à jour.

Mettez immédiatement et quotidiennement à jour votre antivirus.

Nota : l'antivirus MacAfee pourrait ne pas détecter le virus *Magitr.b* si la mise à jour a été effectuée de façon automatisée. Pour pouvoir détecter la présence du virus *W32/MAGISTR.b@MM*, suivez la procédure décrite dans le paragraphe Cas particulier de la mise à jour manuelle de VirusScan.

5 Cas particulier de la mise à jour manuelle de VirusScan

Téléchargez manuellement le fichier DAILYDAT.ZIP situé dans dans le tableau nommé *VirusScan Version 4.x Daily Updates* sur le site de MacAfee :

<http://www.mcafee2b.com/naicommon/avert/avert-research-center/virus-4d.asp>

Puis arrêtez Vshield (ceci peut être fait à l'aide de la console VirusScan) le temps de remplacer les fichiers de configuration Clean.dat, Names.dat et Scan.dat situés dans le répertoire suivant :

C:\Program Files\Fichiers communs\Network Associates\VirusScan Engine\4.0.xx
(si l'antivirus se trouve dans C:\Program Files\) par ceux qui sont compressés dans le fichier téléchargé.

6 Solution

Mettre à jour fréquemment et régulièrement les bases de signatures des logiciels anti-virus.

7 Documentation

– Le site web du CERTA :

- Note d'information CERTA-2000-INF-002 : « Mesures de prévention relatives à la messagerie » ;
- Alertes CERTA-2000-ALE-001 et CERTA-2000-ALE-002 concernant « I Love You » et « New Love » ;
- Recommandation CERTA-2000-REC-002 : « Retour d'expérience du ver ILOVEYOU » ;
- L'alerte CERTA-2001-ALE-006 et CERTA-2001-ALE-009 « Propagation importante du virus SirCam » et « Prolifération en Europe du virus HOMEPAGE » ;

– Le site web de Sophos :

<http://www.sophos.com>

- Le site web de Symantec (Norton Antivirus) :
<http://ww.sarc.com>
<http://www.symantec.com>
- le site web de MacAfee :
<http://www.mcafee2b.com/avert/virus-alerts/defaults>

Gestion détaillée du document

13 septembre 2001 version initiale.

09 janvier 2002 seconde version : correction des erreurs typographiques.