Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 12 mai 2003
N° CERTA-2003-AVI-084

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Rappel sur les virus de messagerie

Gestion du document

Référence	CERTA-2003-AVI-084
Titre	Rappel sur les virus de messagerie
Date de la première version	12 mai 2003
Date de la dernière version	–
Source(s)	
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

Virus informatiques.

2 Systèmes affectés

La plupart des systèmes peuvent être infectés par des virus informatiques véhiculés par la messagerie. Cependant les virus les plus fréquents s'attaquent en général aux systèmes les plus répandus.

3 Description

Il n'y a pas de fatalité vis-à-vis des virus informatiques. Ils se propagent essentiellement en exploitant :

1° de mauvaises configurations des systèmes d'information ;
2° une mauvaise sensibilisation de l'utilisateur.

C'est pourquoi il est en général inutile de faire des alertes systématiques sur chacun des virus qui sortent chaque jour. Le CERTA communique peu sur des virus particuliers et préfère régulièrement faire une note de rappel sur les bonnes pratiques.

3.1 Les virus à la mode

Il n'existe pas de statistiques fiables en matière de virus. Beaucoup de sources d'informations sur les virus, citant le nombre de spécimens en circulation sans parler du montant des dégats imputés aux virus, sont particulièrement fantaisistes. Peu importe, cette information est en général inutile pour mettre en œuvre les mesures de protection nécessaires.

Les sites suivants serviront arbitrairement de référence :

- http://www.wildlist.org
- http://www.messagelabs.com/viruseye/threats/list/default.asp
- http://www.vmyths.com

Beaucoup trop de virus se propagent en exploitant une vulnérabilité du logiciel Internet Explorer utilisé au travers du logiciel de messagerie *Outlook*. Le correctif de cette vulnérabilité a été publié en mars 2001 et fait l'objet de l'avis CERTA-2001-AVI-041.

Une tendance des virus est d'arrêter les antivirus fonctionnant sur l'ordinateur contaminé. Si bien que plus que jamais, c'est la vigilance de l'utilisateur qui protège en dernier ressort.

4 Solution

Il y a quelques règles de base pour se protéger contre les virus de messagerie :

1° Pas de panique : les actions réalisées dans l'urgence, font souvent plus de dégats que les virus.

2° Faites des sauvegardes. Le risque virus ne peut être complètement réduit. Plutôt que limiter la propagation des virus (objectif impossible), il vaut mieux limiter l'impact des virus (en sauvegardant ce qu'ils peuvent détruire).

3° Mettez à jour vos systèmes d'exploitation et logiciels. Il s'agit plus d'appliquer les correctifs de sécurité que d'ajouter de nouvelles fonctionnalités.

4° Utilisez un parefeu. Certains virus installent un cheval de Troie ou un relai (IRC, HTTP, SMTP, ...). Leur action est limitée si un parefeu vous protège. Configurez le pour interdire les protocoles que vous n'utilisez pas. Lisez régulièrement les journaux de votre parefeu pour découvrir les tentatives de connexions suspectes.

5° Ne pas ouvrir les fichiers douteux. Un fichier douteux est un fichier provenant d'une source non sûre :

- les fichiers attachés, quelqu'en soit la source (vos amis vous envoient aussi des virus, puisque les virus utilisent leur carnet d'adresse). Préférez toujours échanger un texte saisi dans le corps du message plutôt que d'attacher une pièce jointe.
- les fichiers attachés exécutables sont quasi-systématiquement des fichiers nuisibles. Ne pas hésiter à les détruire (ou les mettre en quarantaine) dès le serveur de messagerie. (cf. http://www.cnrs.fr/Infosecu/num41.pdf).
- les fichiers téléchargés (ftp, http, disquettes, messagerie instantanée, partage de fichier, ...)

6° Si le fichier vient d'une source connue demandez une confirmation que le fichier attaché a bien été envoyé volontairement.

7° Si la source du fichier est inconnue, si vous avez un doute ... n'ouvrez pas le fichier.

8° Si le titre ou le texte du message est douteux n'ouvrez pas le message. Méfiez vous en particulier des titres qui jouent sur vos affects et en particulier ceux qui exploitent l'actualité. Il peut s'agir d'un virus ou d'un canular.

9° Les logiciels de messagerie sont généralement connus pour faire mauvais ménage avec les anti-virus. Il est toujours préférable de laisser au logiciel de messagerie le soin de gérer (envoyer, recevoir) les messages et de ne lui laisser que la possibilité d'enregistrer la pièce jointe et ne surtout pas l'exécuter. Les antivirus du poste de travail pourront plus aisément traiter le virus une fois sur le disque.

10° Pour cela mettez régulièrement à jour vos antivirus.

11° Dans le doute faîtes appel à votre responsable de sécurité informatique.

5 Documentation

- La revue de la sécurité des systèmes d'information au CNRS publie régulièrement des articles très pertinents sur la lutte contre les virus informatiques :
  http://www.cnrs.fr/Infosecu/Revue.html
- CERTA-2001-AVI-041 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-041/index.html

Gestion détaillée du document

12 mai 2003 version initiale.