



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juin 2000
N° CERTA-2000-ALE-009

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Ver VBS/Stages-A, Mirc/Stages-A, pIRC/Stages-A

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-2000-ALE-009>

Gestion du document

Référence	CERTA-2000-ALE-009
Titre	Ver VBS/Stages-A, Mirc/stages-a, pIRC/Stages-A
Date de la première version	20 juin 2000
Date de la dernière version	-
Source(s)	Sophos
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

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

1 Risques

- Propagation de Virus
- Perte de données

2 Systèmes affectés

- Windows NT;
- Windows 2000;
- Windows 95 et 98.

3 Résumé

Stages-A est un ver contenu dans un fichier SHS (Shell Scrap Objet) qui se propage par e-mail (Carnet d'adresses Outlook), par IRC (Logiciels Mirc ou Pirch) et par partage de volume sur le réseau.

4 Description

Stages-A est transmis par une pièce jointe de type LIFE_STAGES.TXT.SHS. Le ver s'active à l'ouverture de ce fichier et montre un texte contenant des plaisanteries sur les étapes de la vie des hommes et des femmes. Parallèlement le ver s'installe sur la machine puis se propage via le carnet d'adresse d'Outlook et les logiciels Mirc ou Pirch. Enfin il détruit le fichier REGEDIT.EXE en le déplaçant vers la poubelle du système.

Le fait d'utiliser l'extension SHS risque de rendre moins méfiant les utilisateurs par rapport à une extension VBS.

Principe d'un fichier SHS : le contenu du presse-papier peut être sauvegarder par « cliquer-déposer » dans un fichier de type SHS (Shell Scrap Objet). Ce fichier peut contenir des données Word, Excel mais également un fichier exécutable. L'exécution du fichier SHS entraîne automatiquement l'ouverture des applications correspondantes (Word, Excel...) ou le lancement du fichier exécutable.

5 Contournement provisoire

Détection du ver : présentation du message reçu

- Objet : « Funny » , « Funny » , « Funny test » , « Life stages text »
- Corps du message : « The male and female stages of life »
- Pièce jointe : LIFE_STAGES.TXT.SHS

6 Solution

- Mettre à jour votre anti-virus;
- Suivre les recommandations de la note CERTA-2000-INF-002.

7 Documentation

Site Sophos
<http://www.sophos.com/virusinfo/analyses/vbsstagesa.html>

Gestion détaillée du document

20 juin 2000 version initiale.