

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Trojan Simpson

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-011>

Gestion du document

| | |
|-----------------------------|--------------------|
| Référence | CERTA-2000-ALE-011 |
| Titre | Trojan Simpsons |
| Date de la première version | 29 juin 2000 |
| Date de la dernière version | – |
| Source(s) | Sophos Symantec |
| 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

Cheval de Troie

2 Systèmes affectés

Windows 9x

3 Résumé

Simpson est un cheval de Troie qui se propage par un fichier compressé (zip) auto-extractible nommé SIMPSONS.EXE

4 Description

Ce cheval de Troie proposé sous forme de fichier exécutable contient deux fichiers SIMPSONS.BAT et SIMPSONS.BMP.

Lorsque le fichier SIMPSONS.EXE est lancé il extrait les fichiers et exécute automatiquement SIMPSONS.BAT.

SIMPSONS.BAT utilise la commande DELTREE . EXE pour effacer les disques de A: à D:.
Ce cheval de Troie n'affecte pas Windows NT ni Windows 2000 car la commande Deltree n'existe plus sur ces versions.

5 Solution

Mettre à jour votre anti-virus

6 Documentation

Site Sophos

<http://www.sophos.com/virusinfo/analyses/trojsimpsons.html>

Site Symantec

<http://www.sarc.com/avcenter/venc/dat/simpsons.trojan.html>

Gestion détaillée du document

29 juin 2000 version initiale.