



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2000
N° CERTA-2000-AVI-049

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Virus FunnyStory

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-AVI-049>

Gestion du document

Référence	CERTA-2000-AVI-049
Titre	Virus FunnyStory
Date de la première version	19 septembre 2000
Date de la dernière version	–
Source(s)	Réseau de confiance Sophos Antivirus et Panda Software
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

Propagation d'un ver de messagerie (saturation du serveur de messagerie).
Diffusion d'informations confidentielles et de mots de passes.

2 Systèmes affectés

Tous systèmes Microsoft Windows.

3 Résumé

Le Virus FunnyStory, est un script en VBS, qui se propage, comme beaucoup d'autres (par exemple Melissa et ILoveYou), via le carnet d'adresse du logiciel Outlook. Mais il a la particularité d'installer un cheval de Troie qui envoie à une adresse programmée des données sensibles lues sur le système.

4 Description

Comme ses prédécesseurs, ce virus se recopie dans un répertoire système, et se propage par mél à destination de tous les contacts présents dans le carnet d'adresse d'Outlook.

Il y a plusieurs versions de ce ver, connues sous les noms de VBS/Funny-A, Funny-B, FunnyStory, et il pourrait y en avoir d'autres. Sophos Antivirus et Panda software décrivent une version légèrement différente, mais la base reste approximativement la même.

L'action principale de ce virus est d'installer un cheval de Troie (connu sous le nom de Troj/Hooker-E). Ce dernier, lorsqu'il est exécuté, récupère des données présentes sur le disque dur telles que les noms et mots de passes des utilisateurs du système, et d'autres informations de configuration comme l'adresse IP de la machine, et les envoie à une adresse programmée.

5 Contournement provisoire

Le virus FunnyStory se présente sous la forme d'un courrier électronique intitulé Funny Story.

La partie active du virus est dans l'attachement qui est, selon les versions, un fichier nommé Funny_Story.htm.vbs, ou LIFE_ASSURANCE.HTM.vbs. Notons que selon la configuration, on peut voir l'attachement sous la forme .htm, qui laisse penser que l'attachement est anodin.

Enfin, si le cheval de Troie Troj/Hooker-E est installé, il faut le supprimer en détruisant le fichier nommé mstk32.exe présent dans le répertoire système de Windows, et supprimer la clé nommée mstk32 qui se trouve dans la branche HKLM/Software/Microsoft/Windows/Current/Version/RunOnce de la base des registres. Cette clé sert à Troj/Hooker-E à s'exécuter à chaque démarrage de la machine.

6 Solution

Mettre à jour votre anti-virus.

Il faut se méfier des pièces jointes, ne pas les ouvrir, et en avoir désactivé l'ouverture automatique. De plus, votre lecteur de courrier, doit lire les pages web comme du texte uniquement et ne doit pas exécuter les contrôles Active X, de même votre navigateur internet, comme indiqué dans les avis notes et alertes : CERTA-2000-AVI-002, CERTA-2000-ALE-001 et CERTA-2000-ALE-002, CERTA-2000-INF-002.

7 Documentation

Avis du CERTA :

- CERTA-2000-AVI-002
- CERTA-2000-ALE-001
- CERTA-2000-ALE-002
- CERTA-2000-INF-002

Sophos Antivirus :

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

Gestion détaillée du document

19 septembre 2000 version initiale.