



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 9 juin 2000
N° CERTA-2000-ALE-007

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Virus VBS/LoveLet-AS

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-007>

Gestion du document

Date de la première version	09 juin 2000
Date de la dernière version	–
Source(s)	Sophos

TAB. 1 – gestion du document

1 Risques

- Virus

2 Systèmes concernés

- Windows 9x
- Windows nt

3 Résumé

VBS/LoveLet-AS est un virus VBS de type Loveletter situé dans un pièce jointe et se propageant par le carnet d'adresses d'Outlook.

4 Description

Message type de présentation du virus

Sujet « US PRESIDENT AND FBI SECRETS =PLEASE VISIT=> (<http://WWW.2600.COM>)<= »

Texte « VERY JOKE...! SEE PRESIDENT AND FBY TOP SECRET PICTURE... » ou une chaîne aléatoire de 10 caractères.

Ce virus affiche, le 17 septembre, un message d'avertissement :
« Dedicated to my best brother =>Christiam Julian(C.J.G.S) Att », suivi de 5 lettres aléatoires et de « (M.H.M. Team) ».

Il essaie de démonter les lecteur Z : à E :

Il essaie de télécharger les fichiers MACROMEDIA32.ZIP, LINUX321.ZIP et LINUX322.ZIP via Internet Explorer.

Ces fichiers ne sont pas des fichiers compressés mais un fichier texte et deux fichiers d'images.

MACROMEDIA32.ZIP est copié dans le répertoire Windows, sous le nom important_note.txt et le met en mode *RUN* dans la base de registre.

Les deux autres fichiers sont également copiés dans le répertoire Windows sous les noms respectifs de logos.sys et logw.sys.

Le virus se duplique sous deux noms différents : LINUX32.VBS et reload.vbs et les rends exécutables au démarrage.

Il se duplique également dans le répertoire system avec un nom commençant par 5 à 8 caractère choisi au hasard suivi des extensions .GIF.VBS ou .JPG.VBS.

C'est ce fichier qui est envoyé à toutes les adresses du carnet d'adresses d'outlook.

5 Solution

- Mettre à jour votre antivirus
- Suivre les conseils de la notre d'information CERTA-2000-INF-002

Documentation

Site Sophos

<http://www.sophos.com>