Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 novembre 2000
N° CERTA-2000-INF-007

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Rappel sur les virus et chevaux de Troie

Gestion du document

Référence	CERTA-2000-INF-007
Titre	Rappel sur les virus et chevaux de Troie
Date de la première version	08 novembre 2000
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

- Perte de données ;
- Propagation de virus et de chevaux de Troie.

2 Systèmes affectés

Principalement Microsoft Windows et plus particulièrement Outlook.

3 Description

Depuis quelques temps, une recrudescence dans la propagation de virus est constatée par les éditeurs d'antivirus. Ces virus sont généralement transmis par courrier électronique à l'insu de l'expéditeur (même principe que le virus ILOVEYOU).

Plusieurs variantes de virus connus sont signalées chaque jour par les éditeurs d'antivirus. Parmis les plus courrants :

- Virus de type VBS (Visual basic), exemple : VBS/LoveLet-BT en date du 7/11/2000 ;

– Virus de type WM (Word Macro), exemple : WM97/Killdll-B en date du 7/11/2000 ;
– Virus de type W32 (Fichier exécutable .exe), exemple Sonic en date du 30/10/2000.

Les conseils mentionnés dans les avis et alertes du CERTA permettent d'éviter l'infection de sa machine et la propagation de ces programmes.

4 Solutions

Rappel sur les mesures à prendre :

– Ne pas se satisfaire des paramétrages par défaut ;
– Mettre régulièrement à jour votre anti-virus ;
– Analyser tout fichier reçu (mél, disquette, CD etc...) ;
– Ne pas faire confiance à l'expéditeur supposé d'un mél ;
– Ne jamais accepter de recevoir des messages au format HTML ou XML et respecter soi-même cette consigne en s'interdisant l'envoi de messages ou de pièces jointes au format HTML ou XML ;
– Ne pas autoriser l'ouverture automatique des pièces jointes dans votre gestionnaire de messagerie ;
– Ne pas autoriser l'exécution systématique des ActiveX, Java et Javascript ;
– Désactiver l'exécution des fichiers VBS ;
– Toujours ouvrir une pièce jointe avec un éditeur de texte.

5 Documentations

– Désactivation de l'exécution des fichiers VBS sous Windows (CERTA-2000-INF-006)
– Mesures de prévention relatives à la messagerie (CERTA-2000-INF-002)
– Retour d'expérience du ver ILOVEYOU (CERTA-2000-INF-001)

Gestion détaillée du document

08 novembre 2000 version initiale.