Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2000
N° CERTA-2000-REC-002

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Mise en garde au sujet des messages de voeux

Gestion du document

Référence	CERTA-2000-REC-002
Titre	Mise en garde au sujet des messages de voeux
Date de la première version	21 décembre 2000
Date de la dernière version	–
Source(s)	CERTA
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

- Compromission ;
- exécution de code arbitraire ;
- chevaux de Troie ;
- propagation de virus et de vers ;
- dénis de services.

2 Systèmes affectés

Tout système.

3 Résumé

A l'approche des fêtes de fin d'année, la réception de messages de voeux, plus ou moins évolués dans leur présentation, est courante et leur diffusion tentante pour tous. Malheureusement, c'est un vecteur de propagation des virus, chevaux de Troie, ou autres contenus malicieux. Il est donc nécessaire d'augmenter la vigilance et de sensibiliser les utilisateurs.

4 Description

Il est de tradition d'envoyer des cartes de voeux à l'approche des fêtes de fin d'année et Internet est devenu un moyen d'échanger ces voeux sous la forme de messages électroniques. Pour présenter ces messages de voeux de façon amusante, jolie ou attractive, les moyens sont multiples : courriers au format HTML (avec ou sans scripts), liens vers un site web de voeux, fichiers exécutables ou animations en pièces jointes, petits jeux, etc.

Mais c'est aussi une période fort intéressante pour les courrier malicieux (techniciens ou administrateurs en congés). Les pages HTML peuvent contenir des scripts malicieux, sous un aspect attractif ou égayant, les fichiers exécutables peuvent être des chevaux de Troie, les documents, peuvent servir à exécuter du code (macro Word, dépassements de mémoire sous Acrobat Reader ou dans les images JPG, séquence Quick Time ou Flash, etc.).

C'est aussi, malheureusement, un moment propice pour les chaînes de courriers. Les « boules de neige » portent un nom significatif de leur effet.

Il est donc nécessaire de rappeler aux utilisateurs les dangers liés à ce type de propagation, et en particulier les recommandations suivantes (CERTA-2000-AVI-002, CERTA-2000-ALE-001, CERTA-2000-ALE-002, CERTA-2000-INF-002 et CERTA-2000-INF-005) :

- Bien paramétrer les navigateurs, ou les logiciels de messagerie ;
- ne pas suivre systématiquement les liens qui sont donnés dans les courriers ;
- ne pas ouvrir les fichiers attachés sans toutes les précautions nécessaires ;
- détruire tout courrier d'origine inconnue sans l'ouvrir ;
- se méfier des pièces jointes mêmes quand elles proviennent d'un ami ou collègue proche ;
- maintenir les logiciels antivirus à jour et ne pas hésiter à en abuser.
- se méfier des chaînes et des canulars par messagerie ;
- pour envoyer des voeux par messagerie, se contenter de simples textes ;
- une jolie carte de voeux par la poste fait parfois autant plaisir !

5 Documentation

- Concernant la messagerie, les contenus HTML et les pièces jointes :
  CERTA-2000-INF-002 : Mesures de prévention relatives à la messagerie
- Concernant la messagerie et les contenu de pages web :
  - CERTA-2000-ALE-001 : Alerte de virus LOVE-LETTER-FOR-YOU
  - CERTA-2000-ALE-002 : Alerte de virus NEWLOVE
  - CERTA-2000-REC-001 : Retour d'expérience du ver ILOVEYOU
- Concernant les pièces jointes :
  - CERTA-2000-AVI-002 : Vulnérabilités dans Office 2000
  - CERTA-2000-AVI-077 : Vulnérabilités dans le lecteur multimédia Windows
  - CERTA-2000-AVI-020 : Vulnérabilité sous Adobe Acrobat
  - CERTA-2000-AVI-018 : Vulnérabilité sous Netscape 4.73 et antérieures
- Concernant les messages en HTML et les pages web pour netscape :
  CERTA-2000-AVI-026 : Vulnérabilité de Netscape avec Java
- Concernant les messages en HTML et les pages web pour Microsoft :
  CERTA-2000-AVI-032 : Vulnérabilité dans la machine virtuelle Java de Microsoft.
- Concernant l'éxecution des scripts VBS ou SHS par les systèmes Microsoft :
  CERTA-2000-INF-006 : Désactivation de l'exécution des fichiers VBS sous Windows
- Concernant les chaînes et les boules de neige :
  CERTA-2000-INF-005 : Les canulars par messagerie

Gestion détaillée du document

21 décembre 2000 version initiale.