Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 janvier 2007
N° CERTA-2007-ALE-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Filoutage contre le site voyages-sncf.com

Gestion du document

Référence	CERTA-2007-ALE-003
Titre	Filoutage contre le site voyages-sncf.com
Date de la première version	15 janvier 2007
Date de la dernière version	22 janvier 2007
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

– atteinte à la confidentialité des données.

2 Résumé

Un courriel électronique est actuellement diffusé sur l'Internet, et comporte un lien vers un site de filoutage, ou `phishing`. Il permettrait à une personne malveillante de voler des données personnelles, des identifiants de connexion et des coordonnées bancaires.

3 Description

Un courriel électronique est actuellement diffusé sur l'Internet.

Dans sa configuration actuelle, il se présente comme un message provenant de `AdminSNCF@sncf-voyages.com`, avec pour titre : « Urgent : Vérification de vos données ».

Le corps du message ressemble à s'y méprendre à un courrier authentique de la SNCF, avec le logo et un texte en français. Ce dernier, sous un faux prétexte ironique ("vol de votre identité pour acheter sur un site Internet"), exige avec beaucoup de sérieux ("information chiffrée et protégée avec le meilleur logiciel de *chiffrement* dans l'industrie"), à la victime de fournir ses coordonnées bancaires, des données personnelles (adresse, date de naissance, numéro de téléphone), et un mot de passe.

Le lien affiché dans le corps du message ressemble à celui de la SNCF : `http://www.sncf-voyages.com` mais dirige la victime vers un site factice (imitation d'un site officiel de la SNCF).

4 Solution

4.1 Origine du problème

Les courriers électroniques, tout comme les lettres postales, sont un moyen de communication aisé pour transmettre de l'information. Cependant, le processus standard pour les transmettre n'offre pas, sans service complémentaire, certaines garanties. Pour les lettres postales, l'expéditeur n'est pas vérifié, et l'entête du courrier (adresses, téléphone, dates) peut être falsifié. Il en va de même pour la messagerie électronique.

Ces problèmes sont à la source des attaques de filoutage (ou *phishing*), ou servent à conduire les utilisateurs vers des pages Web malveillantes.

4.2 Recommandations

Comment réagir pour ne pas se faire voler d'informations ?

Il n'est pas aisé de déterminer si un courriel a été envoyé à des fins malveillantes. Quelques bons réflexes permettent cependant, malgré la difficulté d'estimer le risque, de limiter les impacts d'une telle attaque :

- être circonspect quand l'expéditeur ou le destinataire affiché est inconnu, ou quand le style ou la syntaxe sont approximatifs ;
- être vigilant lorsqu'un courriel demande des actions urgentes, propose de l'argent facile ou des produits peu chers ;
- éviter de fournir de l'information sur le site Internet qui s'affiche après un clic dans un courriel, en remplissant par exemple un formulaire ou en renseignant un mot de passe ;
- faites appel à un correspondant informatique ou de sécurité s'il y a le moindre doute sur la nature d'u n courriel reçu ou sur une page Internet visitée suite au clic depuis un courriel.

Quelques mesures plus techniques :

- vérifier pour tout échange de coordonnées confidentielles que le mot `https` figure devant l'adresse du site dans la barre du navigateur et/ou un cadenas existe dans la barre d'état (bas droit de l'écran) ;
- taper directement dans le navigateur Internet l'adresse indiquée par le courrier électronique, sans cliquer dessus, et après l'avoir vérifiée. En effet le lien qui s'affiche à l'écran n'est pas nécessairement la véritable adresse Internet cible ;
- configurer le client de messagerie pour lire tous les courriers électroniques au format texte ;
- configurer le navigateur Internet pour qu'il n'interprète pas les ActiveX, Java et le Javascript par défaut ;
- consulter le code source du courrier électronique pour vérifier les adresses incluses dans les liens HTML.

5 Documentation

- Note CERTA-2005-INF-004, « Limiter l'impact du *SPAM* » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-004/
- Note CERTA-2000-INF-002, « Mesures de prévention relatives à la messagerie » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/

Gestion détaillée du document

15 janvier 2007 version initiale.