Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 juin 2000
N° CERTA-2000-INF-005

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Les canulars par messagerie

Résumé

Ce document s'adresse à tous les utilisateurs de la messagerie. Il met en garde contre certaines formes de rumeurs diffusées par Internet et apprend à les reconnaître. Ce document pourrait être repris par les responsables informatiques sous la forme d'une note interne.

Gestion du document

Date de la première version	29 mai 2000
Date de la dernière version	–
Source(s)	http://www.hoaxbuster.com

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Systèmes concernés

- la messagerie ;
- les forums de discussions.

2 Risque

- divulgation de l'organisation interne, voire de la liste des personnes les plus crédules ;
- déni de service sur les outils de messagerie ;
- participation à son insu à une attaque de déni de service ;
- banalisation du risque de sécurité ;
- recommandations de fausses mesures de sécurités pouvant causer des dégats.

3 Description

Des messages circulent sur la messagerie qui invitent le lecteur à les faire suivre au plus grand nombre de destinataires possible. Ces messages diffusent des rumeurs parfois fondées souvent non fondées.

3.1 Incitation à la propagation

Ces messages canulars jouent sur les sentiments du destinataire pour le pousser à faire suivre le message au plus grand nombre de personne possible. Ils poussent le destinataire à faire une « bonne action » : aider un enfant malade, être le héros qui arrêtera la prochaine épidémie de virus informatiques, ... ou bien à acquérir à bon compte des objets convoités (un téléphone portable, une image attrayante, ...).

Les messages jouent souvent d'arguments d'autorités pour inciter les destinataires à le propager. Par exemple, le message prétend ne pas être un canular (ou *hoax* en anglais), il prétend que l'information a été vérifiée par une autorité reconnue (FBI, éditeur d'antivirus, hôpital, fournisseur d'accès à Internet, le service informatique, Microsoft ou tout autre grand éditeur de logiciel, etc.)

Une autre méthode classique pour laisser croire à la véracité du message est de le présenter comme le témoignage direct d'une personne impliquée.

Pour paraître vrai le message peut citer des éléments d'actualité. Le destinataire sera d'autant plus enclin à croire au bien fondé de la démarche à laquelle il est poussé si il peut la rattacher à un contexte d'évènements qu'il connaît par ailleurs.

Le message invite le destinataire à le propager le plus rapidement possible en invoquant l'urgence de la situation. Le destinataire est invité à prendre une décision rapide concernant l'envoi du message. Tout est fait pour qu'il juge que le meilleur choix est d'envoyer rapidement (il vaut mieux diffuser une fausse nouvelle plutôt que de laisser arriver une catastrophe).

Le message vient de quelqu'un qui a été lui-même victime de la rumeur et qui vous connaît. Ce mode de diffusion du message tend à faire baisser votre niveau de vigilance. « Puisque je reçois une invitation à propager un message de la part de quelqu'un que je connais, je suppose qu'il s'est assuré du bien fondé de la démarche et je me dispense de le faire ».

3.2 Danger de ce type de messages

3.2.1 Surcharge de votre réseau

Le premier risque concerne la surchage de vos réseaux et de vos serveurs de messagerie. Lorsqu'un message est diffusé à n personnes qui chacune le diffusent à n personnes. Pour $n = 10$ et 4 niveaux de redirection on peut aller jusqu'à 10 000 messages.

3.2.2 Diffusions de messages parasites

Lorsque le texte du message est exprimé en HTML par le biais de balises malveillantes, il est possible d'envoyer systématiquement un message à la réception du canular.

Parfois ce même mécanisme se fait de façon manuelle lorsque le destinataire est invité à ajouter un destinataire particulier à la liste de diffusion (l'argumentaire du message vise à justifier pourquoi il est nécessaire d'ajouter ce destinataire).

Ceci peut avoir de nombreux effets, dont :

1° lorsque le destinataire de ce message est une victime, il est noyé sous un flot de messages qui lui sont envoyés automatiquement. Dans ce cas, le fait de lire le message et de le faire suivre s'apparente à de la complicité dans une opération de déni de service sur un tiers ;

2° lorsque le destinataire de ce message envoyé automatiquement est la personne malicieuse, elle reçoit la liste de vos correspondants ce qui lui permet d'imaginer la structure de votre entité et les réseaux de personnes à l'intérieur.

   De surcroît, elle reçoit la liste des personnes les plus crédules (celles qui font suivre les mèls). Cette information pourrait être exploitée ultérieurement pour obtenir à moindre risque des informations plus sensibles.

   Il faut noter qu'il existe une variante, où l'on obtient l'organigramme de votre entité en vous demandant d'envoyer vos carte de visites à un enfant gravement malade dont c'est la seule passion. Quelqu'un malintentionné peut, par exemple, avec vos carte de visite prétendre vous connaître et avoir travaillé avec vous voire se faire passer pour vous.

3.2.3 Autres effets nuisibles

Parfois le message vous demande de faire des actions réputées être les seules pertinentes étant donné l'urgence. Ces actions sont dangereuses. Par exemple, vous êtes invités à :

– débrancher l'ordinateur sans l'éteindre proprement pour éviter d'être contaminé par un virus ;

– effacer tous vos documents de bureautiques probablement déjà contaminés ;
– isoler votre réseau sans précaution. En vous isolant totalement vous perdez toute possibilité d'apprendre qu'il s'agit d'un canular.

3.3 Exemples

Fausses alertes de virus Un message annonce la propagation éclair d'un nouveau Virus aux propriétés destructrices extraordinaires. Le message se présente comme une information issue d'un éditeur d'antivirus bien connu. Par exemple :

```
*=====================================*
COMMUNIQUE DU SERVICE INFORMATIQUE
*=====================================*

IBM et Aol ont annoncé l'arrivée d'un nouveau virus : << wobbler >>
Semblable à << I love You >>, d'après IBM il peut être encore plus
dangereux car il arrive à détruire toutes les données du disque dur
ainsi que celles de Netscape et Microsoft Internet explorer. Il
n'existe pas à ce jour d'antivirus capable de le détruire.  Il peut
vous parvenir sous la forme suivante : << How to Give a Cat a Colonic >>.
Si vous recevez par Mail un message avec comme fichier joint un écran
de veille screensaver intitulé BUDDLY SIP ne l'ouvrez en aucun cas.
Annulez le immédiatement.  En l'ouvrant, vous allez perdre toutes les
données de votre disque dur.  Tout ce que l'on sait, c'est que ce
virus a été lancé il y a 10 jours et il s'agit d'un tout nouveau virus
extrêmement dangereux.  Faites suivre ce message à tout votre carnet
d'adresse. Si tout le monde est au courant, le lancement de ce virus
aura été un échec.  MICROSOFT, LINUX, AOL ainsi que WANADOO a confirmé
jusqu'à quel point ce virus est dangereux. Aucun programme ne peut le
détruire.  Veuillez prendre toutes les précautions et communiquer ce
message à un maximum de personnes.

Ci-dessous une liste de virus qui sont particulièrement virulents si
vous les recevez surtout ne pas ouvrir il peuvent venir en annexe de
l'un de vos e-mails

      1)  buddylst.exe
      2)  calcu18r.exe
      3)  deathpr.exe
      4)  einstein.exe
      5)  happ.exe
      6)  girls.exe
      7)  happy99.exe
      8)  japanese.exe
      9)  keypress.exe
      10) kitty.exe
      11) monday.exe
      12) teletubb.exe
      13) The Phantom Menace
      14) prettypark.exe
      15) UP-GRADE INTERNET2
      16) perrin.exe

      17) EAT SHIT (c'est le plus dangereux
      il attaque le système (notament "Regegit")
      il se présente sous la forme d'un message
      intitulé "FreePizza"
```

On voit dans cet exemple que :

- argument d'autorité : l'information est vraie puisqu'elle viendrait du service informatique et qu'elle serait confirmée par MICROSOFT, AOL, WANADOO et *LINUX* suggéré ici comme étant une improbable société.
- rôle gratifiant : les spécialistes ne savent rien faire, il faut donc prévenir tout le monde. Je participe à l'éradication d'un virus ;
- référence à l'actualité : on parle d'`I LOVE YOU`, dont on a entendu parler par la presse. C'est donc grave.
- Urgence : au vu de la vitesse de propagation et des dégâts occasionnés il faut faire suivre le plus rapidement possible.

Action généreuse vers un enfant malade Un message informe du drame vécu par un jeune enfant devant se faire opérer ou bien étant traité pour une longue maladie. Le destinataire du message est invité à réaliser une action qui vise à permettre le succès de l'opération ou bien à combler un souhait qui semble anodin de cet enfant. Par exemple :

```
================================================================
MESSAGE IMPORTANT A TRANSMETTRE AU PLUS GRAND NOMBRE DE PERSONNE
================================================================
Mesdames, Messieurs,

Il y a actuellement, une petite fille de 12 ans, à l'hôpital Necker,
qui doit se faire opérer pour la seconde fois du foie mi-juin.

Elle recherche du sang B-, en quantité importante. Je ne peux hélas
pas lui donner le mien, ayant accouché il y a 4 mois. Le don du sang
étant anonyme et le receveur aussi, la démarche à suivre est donc la
suivante : le donneur doit aller dans un hôpital qui a un service
"Don du sang anonyme". Donnez son sang. Appelez la maman de la petite
fille (dont vous trouverez le N de tél, ci-dessous) pour lui indiquer
le lieu du don.

Elle contactera Necker, qui contactera l'hôpital en question pour
récupérer le sang. C'est un peu compliqué, mais c'est comme ça.

Pour confirmation, vous pouvez contacter sa maman au 06.70.02.41.75.
LE SANG B- EST RARE, VOUS QUI EN AVEZ, DONNEZ-LE, MERCI.


Merci de renvoyer ce message au plus grand nombre de personne possible

        Emmanuelle FLAHAULT
```

On voit dans cet exemple que :

- argument d'autorité : L'information est vraie puisqu'elle provient d'un grand hôpital ;
- témoignage direct : le message provient d'une personne qui aurait bien voulu donner son sang, mais qui n'a pas pu. De plus la mère de la petite fille a fourni son numéro de téléphone. Imagine-t-on que quelqu'un ait pris le risque de *bluffer* en donnant son numéro de téléphone ?
- rôle gratifiant : En envoyant ce message à tous vos correspondants on augmente la chance de trouver des donneurs de sang du groupe B- et de sauver la petite fille ;
- urgence : L'opération de la petite fille a lieu mi-juin, il faut trouver rapidement le plus grand nombre de donneurs étant donné les démarches à entreprendre.

Ce type de message est assez courant. Il gêne le travail des hôpitaux qui ont bien d'autres choses à faire que de répondre à des canulars.
On peut imaginer que le propriétaire du téléphone va recevoir plusieurs appels qui le dérangeront puisque toute cette histoire est inventée.

Acquisition d'un objet attrayant Un message vous invite à le faire suivre à 8 ou 20 de vos amis afin de gagner un téléphone portable. Ce canular a débuté avec un message venant soit disant de Nokia. Un second message de même type à suivi mais cette fois ci avec le constructeur Ericsson. Une troisième version cite maintenant Alcatel.

```
Cher client,


Nos concurrents Nokia et Ericsson, donnent des mobiles gratuits sur
leur site Internet et nous, ALCATEL, voulons résister à leur offre.


Donc nous donnons aussi nos téléphones One Touch VIEW DB derniers
modèles qui sont tout particulièrement développés pour l'internet
et nos heureux clients trouvent ces appareils très avancés
technologiquement. En donnant des téléphones gratuits, nous obtenons
donc de la part de nos clients de bons retours et des effets
importants de bouche à oreilles.

Tout que vous devez faire, c'est expédier ce message à 8 amis. Après
un délai de livraison de deux semaines, vous recevrez un
ALCATEL One Touch MAX DB.

Si vous l'envoyer à 20 amis, vous recevrez le tout dernier
ALCATEL One Touch CLUB DB.

N'oubliez juste pas d'envoyer une copie à : jean.market@alcatel.com ;
c'est, pour nous, la seule façon de vérifier que vous avez expédié ce
message à 20 personnes.


                                Bonne chance
                                Jean market
                                Directeur marketing
```

On voit dans cet exemple que :

- témoignage direct : l'information est vraie puisqu'elle vient du directeur marketing (jean.market@alcatel.com) (sic) qui ne prendrait pas le risque de donner son mèl si toute cette affaire était fausse ;
- référence à l'actualité : des messages identiques ont circulé sur Nokia et Ericsson. C'est donc une pratique courante de cette industrie que de donner les objets qu'elle fabrique ;
- attrait du gain : on va obtenir un objet que l'on imagine très convoité (le tout dernier modèle de la marque) sans trop d'effort puisqu'il suffit de transmettre ce message à 20 amis.
- urgence : Plus tôt le message est envoyé, plus on a de chance d'obtenir son gain. Cette opération pourrait ne pas durer.

Il n'y a qu'une chose dont on peut être sûr, c'est que le serveur de courrier de chez Alcatel va être saturé. Le votre aussi.

4 Solution

Il ne faut jamais chercher à savoir si de tels rumeurs véhiculées par la messagerie sont fondées ou non. C'est une fausse piste. La décision doit se prendre de façon objective sur ce que le message veut vous pousser à faire.

Dès que vous recevez un message :

1° avec beaucoup de destinataires ;

2° dont le texte véhicule une forte charge émotive ;

3° qui inspire un sentiment d'urgence ;

4° qui vous invite à faire quelque chose que vous ne faites pas spontanément

vous êtes en droit de supposer que vous êtes en présence d'un canular.

Que la rumeur soit fondée ou non, la diffusion massive d'un message par tous les usagers de la messagerie, ne constitue jamais la bonne démarche.

Il faut faire suivre le message à son responsable de la sécurité informatique qui est le seul habilité à juger des suites à donner.

Gestion détaillée du document

29 mai 2000 version initiale.