Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 juin 2005
N° CERTA-2005-REC-002

**Affaire suivie par :**
CERTA

# RECOMMANDATION DU CERTA

## Objet : Attaque ciblée par cheval de Troie

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-2005-REC-002

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2005-REC-002 |
| Titre | Attaque ciblée par cheval de Troie |
| Date de la première version | 24 juin 2005 |
| 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 Introduction

Cette note de recommandation n'est pas destinée à expliquer de façon théorique ce qu'est un cheval de Troie (CERTA-2001-INF-002) mais rappelle les principes généraux pour s'en protéger en particulier sous l'angle des attaques ciblées. Cette recommandation est complétée par un mémento sur les virus émis par le CERTA (CERTA-2005-INF-002). Ces recommandations sont destinées aux responsables de sécurité des systèmes d'information (RSSI) ainsi qu'aux utilisateurs finaux.

Cette recommandation fait suite à des cas de déploiement de chevaux de Troie exploitant le vecteur de l'ingénierie sociale pour s'installer sur les machines des victimes. Pour la plupart des utilisateurs, un code malveillant est nécessairement un virus. Le terme virus étant aussitôt associé :

- à la reproduction immédiate via une infection de fichiers ou l'exploitation d'une vulnérabilité dans les logiciels ;
- à un anti-virus, considéré pour beaucoup comme une sorte d'assurance tout risque sur l'Internet.

Cependant, cette vision s'avère trop réductrice du danger des codes malveillants. En effet, il existe des programmes malveillants qu'on appelle chevaux de Troie et qui peuvent n'avoir aucune capacité de reproduction par eux-mêmes. De plus, s'ils sont employés uniquement dans des attaques dites ciblées, il y a fort peu de chance qu'ils soient détectés par les anti-virus.

Ces programmes infectent la machine (ils peuvent s'assurer par différents moyens d'être toujours résidents en mémoire même si le système est redémarré) mais n'ont pas de capacité de reproduction en dehors du système infecté.

# 2 Principe

Si une attaque ciblée devait se produire, les anti-virus ne seraient pas de grande utilité, au moins dans les premiers temps de l'attaque. Cette période d'inefficacité des anti-virus pouvent s'étendre jusqu'à plusieurs mois. En effet, dans ce type d'attaque il ne s'agit pas de propager à très grande échelle des vers ou des virus ou d'une façon générale du code malveillant, mais bien de conduire des attaques plus ciblées sur certaines victimes sans chercher nécessairement un effet de propagation.

Ces attaques ciblées, du fait entre autres choses de leur propagation limitée, ne peuvent être détectées automatiquement par les anti-virus. De plus, ces chevaux de Troie, ne s'autopropagent pas et n'ont pas intérêt à s'autopropager afin de conserver leur furtivité au regard des anti virus. Une fois installée sur une machine victime, ils ne cherchent pas nécessairement à se diffuser au travers du carnet d'adresses de la victime.

Ces attaques sont ciblées dans la mesure où le vecteur de transport du cheval de Troie est particulièrement soigné et travaillé en fonction de la victime choisie. Cela se traduit par exemple par l'envoi de méls parraissant émaner d'une personne connue du destinataire ; sans titre accrocheur ou texte raccoleur poussant le destinataire à poursuivre son action en cliquant sur la pièce jointe contenant le code malveillant. Ce mail contient en revanche une pièce jointe (avec des extensions qui devraient tout de même alerter le destinataire formé et vigilant : CERTA-2005-INF-002 et CERTA-2002-REC-001).

Ce type d'attaque ciblée utilisant des méthodes d'ingénierie sociale peut aussi prendre d'autres formes comme celle d'un cédérom publicitaire remis par une personne de confiance et contenant un cheval de Troie.

# 3 Défense

## 3.1 Généralités

Il ne faut pas oublier que le seul moyen dont dispose le cheval de Troie pour s'installer dans un système est de ... demander de l'aide à l'utilisateur, en lui proposant une action qui semble anodine comme un simple «clic». Comme souvent en matière de sécurité, la dernière barrière de défense est fondée sur l'état de vigilance et le niveau de sensibilisation des utilisateurs finaux. Il faut donc à nouveau souligner combien le comportement de l'utilisateur est primordial en matière de sécurité des systèmes d'information, en ne faisant pas reposer la confiance sur les seuls logiciels de sécurité.

La sécurité des systèmes d'information (SSI) repose sur une démarche de défense en profondeur. Ce concept propose une approche globale et dynamique de la SSI, en s'intéressant à la maîtrise de l'information de l'environnement du poste de travail jusqu'aux environnements de réseau. Il s'agit de coordonner plusieurs lignes de défense dans toute la profondeur des organisations (chaîne fonctionnelle SSI, relais SSI auprès des utilisateurs, PSSI, etc.) mais également dans les procédures (remontée d'incidents, cycle de vie, etc.) et dans les techniques employées (cryptologie, évaluation et certification, etc.).

Les attaques ciblées ne peuvent être détectées par la simple mise en place d'une ligne de défense technique (l'anti-virus), il est nécessaire pour se protéger d'associer la ligne de défense technique à une ligne de défense procédurale qui peut prendre la forme d'une politique de remontée d'incidents ou d'un meilleur filtrage sur les pièces jointes et de compléter cette défense par une ligne organisationnelle qui permet de sensibiliser les utilisateurs à l'usage de la messagerie et de la navigation sur l'Internet.

## 3.2 Meilleures pratiques

Le document du CERTA (CERTA-2005-INF-002) propose sous forme de mémento, les meilleures pratiques pour se protéger des virus. Les pratiques retenues ci-dessous constituent une synthèse en terme de pratiques d'organisation et de procédures.

- Prendre connaissance et diffuser les différentes publications du CERTA (voir le chapitre Documentation ci-dessous).

- Rester vigilant si un correspondant que vous connaissez bien et avec qui vous échangez régulièrement du courrier en français, vous fait par exemple parvenir un message avec un titre en anglais (ou tout autre langue). En cas de doute, il est toujours possible de confirmer le message en téléphonant.

- Habituer vos correspondants à votre style personnel : pour compliquer la tâche des attaquants, prenez l'habitude quand vous envoyez un message d'ajouter dans le corps du message l'objet précis de la pièce jointe (par exemple compte rendu de la réunion du ..). Ainsi un message ne comportant pas une indication de ce type sera suspect pour votre interlocuteur qui pourra alors se méfier de la pièce jointe.
- Privilégier l'envoi de pièce jointe au format plus neutre comme RTF ou PDF par exemple. N'ouvrir jamais les pièces jointes dont les extensions dangeureuses comme « .exe » ; « .vbs » ; « .lnk » (CERTA-2005-INF-002 pour une liste plus exhaustive).
- Mettre à jour quotidiennement les anti-virus. Mettre en œuvre des anti-virus distincts sur les passerelles de messagerie et sur les postes utilisateur.
- Appliquer sans attendre les correctifs des éditeurs de systèmes d'exploitation et d'applications.
- Sensibiliser les utlisateurs sur les dangers de la messagerie en leur expliquant leur rôle dans la politique de défense. Adapter et diffuser largement un document comme le mémento du CERTA (CERTA-2005-INF-002).

### 3.3 Règles de filtrage

Les règles générales de filtrage données ci-dessous ne constituent que des exemples. Leur application reste dépendante des architectures.

Une fois infectée par un cheval de Troie, la machine victime cherchera en général à sortir du réseau interne afin d'aller se connecter sur un serveur. Pour se protéger, il convient d'appliquer la règle de sécurité suivante pour les connexions sortantes : «tout est interdit sauf...». Par exemple, si les machines des utilisateurs ne sont autorisées qu'à la navigation et à la messagerie, on pourra alors appliquer les règles suivantes (en complément des règles sur d'autres protocoles comme par exemple ICMP ou DNS) :

- ports autorisés en sortie : 80/TCP et 443/TCP afin de permettre les flux HTTP et HTTPS ;
- ports autorisés en sortie : 25/TCP et 110/TCP vers vos services de messagerie uniquement.

Cependant, cette règle peut s'avérer insuffisante si le cheval de Troie utilise un des ports autorisés (par exemple le port 80). Dans ce cas, il est préconisé de mettre en œuvre un filtrage applicatif (reverse proxy) qui vérifiera que seules les applications autorisées peuvent accéder à l'Internet (par exemple un navigateur ou un client de messagerie).

Ainsi, la règle précédente concernant les ports 80 et 443 pourrait être remplacée par la suivante :

- port autorisé : 3128/TCP vers le proxy uniquement.

Dans cet exemple, les postes utilisateur ne sont jamais autorisés à aller sur l'Internet directement sans passer par des serveurs sous contrôles.

## 4 Documentation

- Référence CERTA sur l'usage de la messagerie instantanée ou de l'IRC
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-001/index.html
- Référence CERTA sur les chevaux de Troie
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-002/index.html
- Référence CERTA sur le vulnérabilité de type « Cross Site Scripting »
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-001/index.html
- Référence CERTA sur les virus de messagerie
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-001/index.html

## Gestion détaillée du document

**23 juin 2005** version initiale.