Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 février 2001
N° CERTA-2001-INF-002

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Les chevaux de Troie

Gestion du document

Référence	CERTA-2001-INF-002
Titre	Les chevaux de Troie
Date de la première version	19 février 2001
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.

Introduction

Un cheval de Troie est un programme, installé le plus souvent à l'insu de l'utilisateur, qui permet à un attaquant de se connecter à l'ordinateur de sa victime. Un tel programme est en général composé d'un serveur (installé sur la machine de la victime), et d'un client qu'utilise l'attaquant pour prendre la la main sur la machine.

Nous nous intéresserons plus particulièrement dans cette note à Back Orifice 2000, un cheval de Troie pour Windows.

1 Risques

Les risques encourus pour un utilisateur dont la machine est infectée sont considérables. Toutes les opérations faites sur une machine en local peuvent être exécutées par le biais de BO 2000. Par exemple, un attaquant peut :

- télécharger un fichier sur le poste victime ;
- rebooter l'ordinateur ;
- enregistrer la frappe au clavier ;
- visualiser l'écran ;
- prendre le contrôle de la souris et du clavier ;

...

Il n'est pas étonnant dans ces conditions que BO 2000 soit largement utilisé par les administrateurs systèmes pour l'administration distante.

Le principal danger vient de l'extrême facilité à se servir de BO 2000. Son utilisation ne requiert aboslument aucune compétence particulière, et ne semble donc pas réservée à certains spécialistes.

Il suffit pour un attaquant de faire exécuter par un utilisateur le binaire d'installation su serveur BO 2000. Cet exécutable peut porter n'importe quel nom, se trouver en pièce jointe à un mél (il a une taille comprise entre 160 et 200 Ko), et même être incorporé à un autre exécutable.

2 Détecter un cheval de Troie

Il n'est pas aisé de détecter une compromission par un cheval de Troie, en particulier par BO 2000. En effet, tous les paramètres sont modifiables par l'attaquant : le nom du serveur, sa valeur dans la base des registres, le protocole réseau utilisé pour communiquer entre le client et le serveur, le numéro de port sur lequel se fait la connexion, ...

Par défaut, le serveur sera installé dans le répertoire `c:\windows\system` sous le nom `UMGR32.EXE`. Les communications se feront par défaut avec le protocole TCP sur le port 54320.

3 Eradication

Si vous soupçcoonez une compromission, voici les étapes à suivre pour une machine sous Windows 98 :

- éditer la base de registres ;
- vérifier les entrées de la clef `HKEY\LOCAL\MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices` ;
- supprimer celle qui correspond à Back Orifice 2000 (par défaut `umgr32.exe`) ;
- supprimer l'exécutable du serveur (par défaut `c:\windows\system\Umgr32.exe`) ;
  si windows refuse de supprimer l'exécutable, il faut le supprimer par une commande DOS ;
- redémarrer la machine.

Conclusion

La puissance et la facilité d'utilisation des chevaux de Troie en font une menace particulièrement sérieuse.
Afin d'éviter tout risque de contamination, il convinet de respecter les consignes suivantes :

- mettre régulièrement à jour l'antivirus ;
- analyser tout fichier reçu ;
- ne pas autoriser l'ouverture automatique des pièces jointes avec votre gestionnaire de messagerie ;
- toujours ouvrir une pièce jointe avec un éditeur de texte.

Gestion détaillée du document

19 février 2001 version initiale.