

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : The Serbian Badman Trojan (TSB)

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-2000-ALE-008>

Gestion du document

Date de la première version	13 juin 2000
Date de la dernière version	–
Source(s)	Sophos

TAB. 1 – *gestion du document*

1 Risque

Cheval de Troie

2 Systèmes concernés

- Windows 95
- Windows 98

3 Résumé

Serbian.trojan (également nommé Troj/Downloader ou W95/Loader Trojan) est un cheval de Troie qui s'est propagé par l'intermédiaire d'un fichier téléchargé depuis certains forums.

4 Description

Ce cheval de Troie a été proposé sur des forums pour adultes sous la forme d'un fichier Quickflick.mpg.exe ou Mysissy.mpg.exe se faisant ainsi passer pour un fichier vidéo (.mpg).

Une fois ce fichier exécuté sur la machine, il installe discrètement un cheval de Troie téléchargé depuis un autre site (dont l'adresse semble actuellement inaccessible), qui permet à un utilisateur distant de prendre le contrôle de la machine et de l'impliquer dans un éventuel Déni de Service par Outils Répartis. Il utilise également des ports de communications dont certains correspondent à ceux utilisés lors de connexions IRC.

5 Solution

– Détection :

Lister les ports ouverts via la commande `netstat -a` et s'assurer que les ports 2221, 2222, 6669 et 7000 ne sont pas utilisés.

Le cheval de troie ajoute les lignes de commandes suivantes :

- `system.ini: shell=Explorer «trojan.exe»`
- `win.ini: run=«trojan.exe»`

Il ajoute également une entrée dans la base de registre à l'emplacement :

`HKEY_USERS\Microsoft\Windows\CurrentVersion\Explorer`

– Solution :

- Filtrer les ports 2221, 2222, 6669 et 7000 sur le firewall;
- Mettre à jour votre anti-virus;
- Suivre les recommandations de la note d'information CERTA-2000-INF-002 concernant les pièces jointes.

Documentation

- Site Sophos :
<http://www.sophos.com>
- Site Netsec :
<http://www.netsec.net/advisory.htm>
- Site CNN :
<http://www.cnn.com/2000/TECH/computing/06/09/hacker.attack/index.html>

Gestion détaillée du document

13 juin 2000 version initiale.