



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 août 2000
N° CERTA-2000-AVI-036

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Cheval de Troie : Troj/qaz

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-AVI-036>

Gestion du document

Référence	CERTA-2000-AVI-036
Titre	Cheval de Troie : Troj/qaz
Date de la première version	29 août 2000
Date de la dernière version	–
Source(s)	Sophos Symantec
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

- Cheval de Troie ;
- Propagation de virus ;
- Accès aux données.

2 Systèmes affectés

- Microsoft Windows 9x ;
- Microsoft Windows 2000 ;
- Microsoft Windows NT.

3 Description

Troj/Qaz est un cheval de Troie permettant à un utilisateur mal intentionné de pouvoir avoir accès, à distance, à une machine infectée.

Lors de son exécution ce cheval de Troie recherche le fichier « notepad.exe » et le renomme en « note.exe ». Il duplique son propre code dans un nouveau fichier nommé « notepad.exe ».

Lorsque l'utilisateur exécute « notepad.exe », le cheval de Troie s'exécute et lance également l'application « bloc note ». Il modifie également la base de registre afin de se charger au démarrage de la machine.

4 Détection et solution provisoire

Rechercher sur le disque la présence des fichiers suivants :

W32.HLLW.Qaz.A ou Qaz.Trojan

Rechercher la présence de « note.exe » et le renommer en « notepad.exe »

Supprimer dans la base de registre à l'emplacement HKEY_LOCAL_MACHINE\Software\Microsoft\Current\Version\Run la clé : StartIE=notepad.exe

5 Solution

Mettre à jour votre anti-virus

6 Documentation

Site Sophos :

<http://www.sophos.com/virusinfo/analyses/trojgaz.html>

Site Symantec :

<http://www.symantec.com/avcenter/venc/data/qaz.trojan.html>

Gestion détaillée du document

29 août 2000 version initiale.