Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 novembre 2001
N° CERTA-2001-ALE-016

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver badtrans - variante B

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-2001-ALE-016`

Gestion du document

Référence	CERTA-2001-ALE-016
Titre	Propagation du ver badtrans - variante B
Date de la première version	27 novembre 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.

1 Risque

- Exécution de code arbitraire ;
- Compromission des données introduites au clavier ;
- Virus.

2 Systèmes affectés

Microsoft Internet Explorer, Outlook et Outlook express.

3 Résumé

Une variante du ver `badtrans`, se présentant sous la forme d'un texte écrit au format HTML, se propage actuellement sur Internet. Ce ver utilise une vulnérabilité d'Internet Explorer décrite dans l'avis : CERTA-2001-AVI-041 du 30 mars 2001.

4 Description

`badtrans` se présente sous la forme d'une pièce jointe contenant un cheval de Troie. Ce ver est activé si l'utilisateur clique sur la pièce jointe.

Une variante de ce ver, (`badtransB`), qui se propage depuis quelques jours, utilise une vulnérabilité de Outlook lors de la réception de messages au format HTML. L'exécution de la pièce jointe est alors réalisée automatiquement, sans que l'utilisateur ai à ouvrir la pièce jointe.

Une fois activé, `badtransB` enregistre les frappes de l'utilisateur sur le clavier de la machine infectée.

Il est à noter que cette variante utilise une vulnérabilité signalée depuis plusieurs mois. Il est donc nécessaire, pour se protéger de telles attaques, d'appliquer les correctifs proposés par les éditeurs dès leurs publications.

Ce type de ver ne peut se propager que si l'on autorise l'affichage des messages au format HTML. Nous vous recommandons d'appliquer les conseils concernant le paramètrage de votre messagerie (cf. CERTA-2000-INF-002).

5 Contournement provisoire

Bloquer le téléchargement automatique de fichiers dans les paramètres d'Internet Explorer (cf. Avis CERTA-2001-AVI-041)

6 Solution

- Télécharger le correctif Microsoft :
  http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp
- Mettre à jour votre logiciel d'anti-virus.
- Changer par précaution les mots de passe du poste de travail.

7 Documentation

- Site du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-041/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html
- Bulletin Microsoft MS01-020 :
  http://www.microsoft.com/technet/security/bulletin/MS01-020.asp
- Site Sophos :
  http://www.sophos.com/virusinfo/analyses/w32badtransb.html
- Site Symantec :
  http://www.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html
- Site F-Secure :
  http://www.europe.f-secure.com/v-descs/badtrs_b.shtml
- Site NAI :
  http://vil.nai.com/vil/virusSummary.asp?virus_k=99069

Gestion détaillée du document

27 novembre 2001 version initiale.