Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 juin 2005
N° CERTA-2005-ALE-004

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver MYTOB

Gestion du document

Référence	CERTA-2005-ALE-004
Titre	Propagation du ver MYTOB
Date de la première version	03 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 Risque

- Exécution de code arbitraire à distance;
- dysfonctionnements du système.

2 Systèmes affectés

Systèmes Windows.

3 Résumé

De nombreuses versions du virus MYTOB ont infecté un certain nombre de machines auprès d'abonnés du CERTA.

4 Description

MYTOB est un ver qui se propage par la messagerie (via une pièce jointe) ou par l'exploitation d'une vulnérabilité de `LSASS` (voir ci-dessous la référence). Les machines infectées se reconnaissent grâce à leurs tentatives de connexion sur la machine `irc.blackcarder.net` (port 7000/TCP). Une fois connectée au serveur

d'`irc.blackarder.net`, la machine infectée peut recevoir l'instruction de télécharger puis d'exécuter des fichiers arbitraires.

Par ailleurs, les machines infectées rencontrent de nombreux dysfonctionnements tels que l'arrêt, dès leur lancement, de certains processus (par exemple le gestionnaire des tâches, l'invite de commande MS-DOS, ...).

5 Solution

Aspects organisationnels . Cette infection rappelle à nouveau l'impérieuse nécessité des mises à jour et d'autre part la nécessaire sensibilisation des utilisateurs sur l'ouverture trop confiante des pièces jointes.

Aspects techniques . Pour déterminer les machines infectées sur les réseaux, l'analyse des journaux en amont des firewalls doit permettre de détecter les machines cherchant une connexion sur les ports 7000/TCP et 445/TCP. En cas d'infection, contactez le CERTA.

6 Documentation

– Alerte CERTA-2004-ALE-007 « Exploitation de la vulnérabilité LSASS sous Windows : apparition du ver Sasser»:

http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-007/index.html

Gestion détaillée du document

03 juin 2005 version initiale.