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 juillet 2000
N° CERTA-2000-AVI-019

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Virus sous Autocad2000

Gestion du document

Référence	CERTA-2000-AVI-019
Titre	Virus sous Autocad2000
Date de la première version	27 juillet 2000
Date de la dernière version	–
Source(s)	Réseau de Confiance Infomations Virus de McAfee
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

Selon McAfee, pour le moment aucun car cette version ne contient pas de code malfaisant... Ce virus se contente uniquement de se propager.

2 Systèmes affectés

Logiciel Autocad 2000. Autocad LT n'est pas atteint car il ne supporte pas le VBA.

3 Résumé

Un virus d'une nouvelle génération a été détecté. Il doit son originalité à son environnement de développement : Autocad 2000.

4 Description

Ce virus nommé AC97M/Star est aussi connu sous le nom de ACAD/Star, ACAD.Star, Autocad2k/Star, ou encore AC2KM/Star, il peut être classé dans la catégorie des virus de macro.

Il se loge dans les dessins Autocad (Autocad Drawings), et se base sur la technique de W97M/Marker pour déceler s'il est déja présent dans un document ou non. C'est à dire qu'il recherche une chaîne de caractères types dans les fichiers qu'il peut infecter.

Il contient aussi une part de code provenant de V5M/Radiant.

5 Détection

Il ne se manifeste pas par une action, mais est repérable par le fait qu'un dessin non modifié vous proposera quand même d'enregistrer les changements à sa fermeture. La procédure de fermeture peut aussi durer un peu plus longtemps que normalement à cause de l'exécution du code du virus.

Ce virus possède une signature typique, il contient les chaînes de caractères suivantes :

```
'[Autocad2k\Star]
'[A.s.T]
'Big Greetz to some0ne really special
'"You'll always be a star in my sky"
```

6 Solution

Utiliser un antivirus à jour. Actuellement, seul Viruscan de McAfee semble détecter ce virus.

7 Documentation

Site McAfee :
http://vil.nai.com/villib/dispVirus.asp?virus_k=98745

Gestion détaillée du document

27 juillet 2000 version initiale.