

**La procédure est différente pour un poste autonome et pour un poste en réseau**

## **I. Mono poste**

1. Quitter toutes les applications
2. Lancer le poste en mode sans échec
  - sous Windows 98 - appuyer sur la touche "Ctrl" au démarrage pour obtenir le menu
  - sous Windows 95 - appuyer sur la touche F8 au démarrage pour obtenir le menu
3. Lancer le système en mode sans échec
4. Exécuter l'utilitaire Fixirc.com  
cet utilitaire supprime les fichiers contaminés et "nettoie" la base de registre
5. Lancer Commandes MS-DOS
6. Lancer Edit c:\autoexec.bat  
supprimer les lignes faisant référence au fichier SIRC32.EXE  
par exemple: **win \recycled\sirc32.exe**  
sauvegarder le fichier autoexec.bat et quitter EDIT
7. Relancer le système en mode "normal"
8. Mettre à jour les définitions virales ( via Cité Expert ou [services.ccmx.com/majav](http://services.ccmx.com/majav))
9. Lancer l'analyse du système

## **II. Réseau**

La procédure est à appliquer pour tous les postes du réseau

1. Quitter toutes les applications
2. Lancer le poste en "mode sans échec":
  - sous Windows 98 - appuyer sur la touche "Ctrl" au démarrage pour obtenir le menu
  - sous Windows 95 - appuyer sur la touche F8 au démarrage pour obtenir le menu
3. Lancer le système en mode sans échec ( **le poste sera déconnecté du réseau**)
4. Exécuter l'utilitaire Fixirc.com  
cet utilitaire supprime les fichiers contaminés et "nettoie" la base de registre
5. Lancer Commandes MS-DOS
6. Lancer Edit c:\autoexec.bat  
supprimer les lignes faisant référence au fichier SIRC32.EXE  
par exemple: win \recycled\sirc32.exe  
sauvegarder le fichier autoexec.bat et quitter EDIT  
**Ne pas relancer le poste avant d'effectuer cette procédure sur tous les postes du réseau.**  
Suite de la procédure (après avoir traité tous les postes du réseau):
7. Si les définitions ne sont pas à jour pour ce virus (inférieures à 17/07/2001)  
Relancer un poste en mode "normal"  
mettre à jour des définitions du dossier de distribution du serveur (via Cité Expert ou [services.ccmx.com/majav](http://services.ccmx.com/majav))  
mettre à jour les définitions sur le serveur ( fermer et ouvrir une session sur le serveur NT ou redémarrer le serveur OS/2 )
8. Dans tous les cas:
  - lancer l'analyse du serveur (NT et OS/2)
  - lancer l'analyse des volumes du serveur Novell à partir du poste "contrôleur"  
S'il y a des fichiers contaminés les mettre en quarantaine.
9. Relancer les postes du réseau ( les définitions seront mises à jour et l'analyse sera lancée)

Attention: si le virus persiste il est possible que la contamination a été effectuée plusieurs fois (plusieurs lignes dans le fichier autoexec.bat). Dans ce cas la il faut se procurer la version saine du fichier RUNDLL32.EXE ( à partir du CD ROM Windows ou des fichiers cabs)