

## Procédure d'éradication du virus W32.goner.A@mm

### Description (selon Symantec)

Type: Virus, ver

Définitions: 4 décembre 2001

Propagation: niveau 4 (le plus élevé)

Dommages: niveau moyen

### Eradication manuelle

1. Sous Windows 9x: arrêter le poste, attendre au moins 30 sec avant le remettre sous tension. Lancer Windows en mode sans échec

1a. Sous Windows NT/2000 lancer Gestionnaires des tâches, supprimer les processus: gone.scr et pentagone ( si présent)

2. Editer la base de registre

trouver la clé:

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\Current Version\Run

supprimer la valeur: C:\%SYSTEM%\gone.scr C:\%SYSTEM%\gone.scr

3. Quitter l'éditeur de registre et relancer la machine

4. réinstaller Norton AV et relancer la machine

5. Mettre à jour les définitions (04/12/2001 ou supérieures)

6. Lancer le scan de tous les fichier de tous les disques

7. Supprimer tous les fichiers contaminés par >W32.Goner.A@mm (ces fichiers doivent être restaurés çà partir d'une sauvegarde)

### Eradication automatique ( tool FixGoner.exe)

Ce qui fait le tool:

- arrête les processus viraux de W32.Goner.A@mm
- supprime tous les exe de W32.Goner.A@mm
- supprime la modification de registre

1. Télécharger le tool (fixgoner.exe)

2. Terminer tous les programmes.

2a. Si Windows Me - désactiver la sauvegarde Système

3. déconnecter le poste du réseau et arrêter la connexion permanente Internet le cas échéant

4. lancer le tool (double clic sur fixgoner.exe)

5. Cliquer sur Start pour lancer le scan

6. relancer le poste après la fin du scan

7. Si Norton AntiVirus a été altéré par le virus ( ne se lance pas, etc...) , réinstaller le

8. Mettre à jour les définitions

9. Si Windows Me - réactiver la sauvegarde Système

10. Lancer le scan de tous les fichiers du système