Dr Solomon's

Anti-Virus Toolkit

pour station de travail

Dr Solomon's Software Ltd.
Alton House, Gatehouse Way, Aylesbury, Buckinghamshire, HP19 3XU, RU
Tél : +44 (0)1296 318700 Fax : +44 (0)1296 318777
E-mail : support@drsolomon.com

Dr Solomon's Software, Inc.
1 New England Executive Park, Burlington, MA 01803, EU
Tél : +1 781 273 7400 Fax : +1 781 273 7474
E-mail : support@us.drsolomon.com

Dr Solomon's Software GmbH
Luisenweg 40, 20537 Hamburg, Allemagne
Tél : Support +49 (0)1805 237678
E-mail : support@de.drsolomon.com

Dr Solomon's Software Australasia Pty Ltd.
96-98 Market Street, South Melbourne, Victoria 3205, Australie
Tél : +61 3 9690 0455 Fax : +61 3 9690 7349
E-mail : support@au.drsolomon.com

CompuServe : GO DRSOLOMON
World Wide Web : www.drsolomon.com

FR8000F-20-05

Copyright

Limitation de garantie

Marques déposées

Version du logiciel

Ce manuel décrit la version 7.78 de Dr Solomon's Anti-Virus Toolkit.

Edition du manuel

Edition 1.0
Novembre 1997

Table des matières

Préface

Dr Solomon's Anti-Virus Toolkit met à votre disposition tous les outils nécessaires à la détection et suppression de tout virus existant dans votre ordinateur et vous aide à vous prémunir contre des contaminations éventuelles.

Pour vous aider à utiliser votre Toolkit de façon efficace, ce manuel est divisé en chapitres de la façon suivante :

Chapitre 1 : **"Première installation de votre Toolkit"** fournit des instructions détaillées pour l'installation du Toolkit sur votre ordinateur.

Chapitre 2 : **"Mise à jour de votre Toolkit"** explique comment mettre à jour votre Toolkit à partir d'une disquette ou d'un CD-ROM.

Chapitre 3 : **"Balayage"** fournit des explications sur les outils de balayage automatique ou sur demande ainsi que des instructions de base concernant les fonction de balayage.

Chapitre 4 : **"Balayage avancé"** fournit des instructions détaillées pour l'utilisation et la configuration des scanners Dr Solomon's.

Chapitre 5 : **"Utilisation du Scheduler sous Windows 3.x, Windows 95 et Windows NT"** explique comment utiliser Scheduler.

Chapitre 6 : **"Désinfection"** décrit comment désinfecter les fichiers, les secteurs de boot et les secteurs de partition.

Chapitre 7 : **"Documentation en ligne"** explique comment installer Adobe Acrobat Reader à partir d'un CD-ROM et comment l'utiliser pour lire votre manuel en ligne.

Chapitre 8 : **"A propos des virus informatiques"** décrit les virus informatiques et donne des conseils sur les principales précautions à prendre contre les virus.

Chapitre 9 : **"Dépannage et options avancées"** traite des problèmes courants que les utilisateurs peuvent rencontrer ainsi que des options avancées du Toolkit.

A la fin de ce manuel vous trouverez un glossaire comprenant tous les termes importants, ainsi qu'un index complet.

Les conventions du Manuel

Dans ce manuel, un certain nombre de conventions sont utilisées.

Les pages contenant des informations spécifiques à certaines plateformes portent le nom de la plateforme afin de faciliter la consultation du manuel.

Les informations que vous devez saisir sont indiquées en `Courier` Typeface. Exemple :

```
D:\SETUP
```

Les variables sont affichées en police courier, en italique et entre chevrons. Voici par exemple, comment apparaissent les instructions pour l'installation du Toolkit pour OS/2 :

"Entrer la lettre qui représente votre lecteur de CD-ROM suivie de :
<*LANGUAGE*>\PRODUCTS\OS2
et appuyez sur <Entrée>."

Dans ce cas vous devez remplacer <*LANGUAGE*> par le nom de la langue du logiciel que vous désirez installer. Le nom de la langue doit apparaître dans cette langue même. Par exemple, si vous travaillez en anglais mais que vous voulez installer la version française du Toolkit pour OS/2, le nom du répertoire auquel vous désirez accéder est Français et non French.

Les boutons sur lesquels vous devez cliquer ainsi que les options à sélectionner apparaissent en gras.

Les touches à utiliser apparaissent entre chevrons.

<Entrée> est utilisé pour indiquer la touche Retour ou Entrée,

<Echap> est utilisé pour indiquer la touche Echappement.

Dans le texte, des symboles sont utilisés pour attirer votre attention sur des points particuliers. Ces symboles ainsi que leur signification apparaissent de la façon suivante :

Attention 	Signale un avertissement que vous devez lire attentivement.
Conseil 	Signale des informations ou des conseils importants que vous devez lire attentivement.
Aide 	Signale des informations supplémentaires.

Captures d'écran

Dans les sections générales, la plupart des captures d'écran proviennent de la version Windows 95 de l'Anti-Virus Toolkit. Les captures d'écran provenant de versions différentes sont signalées.

Produits annexes

L'encyclopédie des virus

Une copie de l'Encyclopédie des virus est livrée avec le Toolkit. Elle contient non seulement des informations de base sur les virus mais également des descriptions détaillées de la plupart des virus détectables par le Toolkit. Cette encyclopédie classe tous les virus en catégories et décrit leurs effets. En outre, tous les autres noms donnés aux virus y sont répertoriés.

Une version en ligne de l'Encyclopédie des virus accompagne également le Toolkit. Lorsque de nouveaux virus sont découverts ils sont ajoutés à la dernière mise à jour du Toolkit. La version en ligne est toujours plus récente que la copie papier.

Les autres versions de l'Anti-Virus Toolkit

Windows NT Server Management Edition

La version Windows NT Server Management Edition fournit des outils d'installation, de configuration, de mise à jour, de suppression et de gestion des applications de Dr Solomon's Anti-Virus Toolkit pour des ordinateurs distants fonctionnant sur un réseau Windows NT.

Novell NetWare

La version NetWare de l'Anti-Virus Toolkit fournit des outils permettant de protéger les serveurs NetWare des virus. Pour une protection maximale, elle comprend également la version DOS/Windows du Toolkit.

SCO UNIX

La version SCO UNIX de l'Anti-virus Toolkit fournit des outils de détection des virus, de désinfection et de protection pour les ordinateurs fonctionnant sous SCO UNIX. Elle comprend également la version DOS du Toolkit.

Mac OS

La version Mac OS de l'Anti-Virus Toolkit fournit des outils de détection des virus, de désinfection et de protection pour les ordinateurs fonctionnant sous Mac OS.

Enregistrement et mises à jour

Les chercheurs de Dr Solomon's reçoivent entre 300 et 400 nouveaux specimen de virus pour examen chaque mois et le Toolkit est mis à jour mensuellement afin de les intégrer. Dans votre propre intérêt, nous vous conseillons de vous abonner au service de mise à jour régulière. Une mise à jour trimestrielle offre une protection suffisante pour la plupart des utilisateurs, mais si votre système est particulièrement exposé à des risques ou si la sécurité est primordiale, des mises à jour mensuelles sont à votre disposition.

Si vous avez acheté le Toolkit avec un abonnement d'un an de mises à jour, vous bénéficiez automatiquement des mises à jour mensuelles ou trimestrielles pendant douze mois à compter de la date figurant sur votre carte d'enregistrement.

Attention Vous ne pouvez recevoir les mises à jour pour lesquelles vous avez payé que si vous nous renvoyez votre carte d'enregistrement.

Si vous n'avez pas souscrit à un abonnement lors de l'achat, envoyez votre carte d'enregistrement ainsi que la somme correspondante. Tous les détails nécessaires figurent sur la carte.

Vous trouverez une carte d'enregistrement utilisateur à l'intérieur de l'emballage du Toolkit. Veuillez la remplir de manière précise et la renvoyer à Dr Solomon's ou à son représentant dans votre pays.

Attention Vous ne pouvez recevoir les mises à jour de Toolkit que si vous avez enregistré votre achat.

Si vous ne trouvez pas de carte d'enregistrement, contactez Dr Solomon's ou son représentant dans votre pays.

Conseil Envoyez votre carte d'enregistrement.

Si vous avez besoin d'aide

Si vous rencontrez un problème lors de l'installation ou de l'exécution du Toolkit, vous pouvez obtenir de l'aide de différentes manières.

Lisez attentivement la documentation, les fichiers README se trouvant sur le CD-ROM ou les disquettes ainsi que ce manuel et l'aide. Vérifiez que vous avez installé le logiciel correctement. Votre distributeur agréé est également en mesure de vous conseiller.

Si vous ne parvenez toujours pas à résoudre un problème, l'équipe d'assistance de Dr Dolomon's est à votre disposition pour vous aider gratuitement.

Vous pouvez contacter les différents services de Dr Solomon's Software de la manière suivante :

Au Royaume Uni :

Par téléphone :	+44 (0)1296 318700
Par fax :	+44 (0)1296 318734
Par e-mail :	support@drsolomon.com
Par bulletin board :	+44 (0)1296 318810
Par courrier :	Dr Solomon's Software Ltd. Alton House Gatehouse Way Aylesbury Buckinghamshire HP19 3XU Royaume-Uni

Conseil

Si vous téléphonez en dehors des heures de bureau, écoutez attentivement la totalité du message et suivez les instructions.

Aux Etats-Unis

Par téléphone :	+1 781 273 7400
Par fax :	+1 781 273 7474
Par e-mail :	support@us.drsolomon.com
Par bulletin board :	+1 781 229 8804
Par courrier :	Dr Solomon's Software, Inc. 1 New England Executive Park Burlington MA 01803 Etats-Unis

En Allemagne

Par téléphone :	Support +49 (0)1805 237678
Par fax :	Sales +49 (0)1805 237677
Par e-mail :	support@de.drsolomon.com
Par courrier :	Dr Solomon's Software GmbH Luisenweg 40 20537 Hamburg Allemagne

En Australie

Par téléphone :	+61 3 9690 0455
Par fax :	+61 3 9690 7349
Par e-mail :	support@au.drsolomon.com
Par courrier :	Dr Solomon's Software Australasia Pty Ltd. 96-98 Market Street South Melbourne Victoria 3205 Australie

Dans le monde entier

CompuServe :	GO DRSOLOMON
World Wide Web :	www.drsolomon.com

Lorsque vous contactez Dr Solomon's, munissez-vous des informations suivantes :

- Le numéro de série qui figure sur votre carte d'enregistrement.
- La version de Windows 3.x, Windows 95, Windows NT, OS/2 ou DOS sous laquelle vous travaillez.
- Le numéro de la version du Toolkit que vous utilisez (imprimé sur le CD du Toolkit ou sur l'étiquette des disquettes d'installation).
- Le numéro de la version du manuel du Toolkit que vous utilisez. Vous trouverez ce numéro sur la page copyright du manuel.
- La disquette Magic Bullet ou une disquette système DOS saine (non infectée) et protégée en écriture, ou encore un ensemble de disquettes système OS/2 saines et protégées en écriture.
- Dans le cas d'une erreur de l'application, notez tout message d'erreur signalé.

Si cela est possible, soyez à proximité de votre ordinateur lorsque vous nous contactez afin de nous fournir des informations complémentaires ou d'effectuer des tests de diagnostic.

1. Première installation de votre Toolkit

Ce chapitre décrit la procédure à suivre pour effectuer un balayage préliminaire et installer ou désinstaller le Toolkit. Pour obtenir des instructions sur la mise à niveau de votre Toolkit, voir la section “Mise à jour de votre Toolkit” à la page 59.

1.1 Balayage préliminaire

Vous devez vous assurer que votre ordinateur n’est pas déjà infecté avant d’installer un logiciel de Dr Solomon’s. Dr Solomon’s vous propose deux méthodes de balayage de votre ordinateur.

Conseil

Si vous faites fonctionner Windows NT ou OS/2, consultez directement les instructions d’installation relatives à ces plate-formes. Pour une installation sous Windows NT, voir “Windows NT” à la page 36. Pour obtenir des instructions pour une installation sous OS/2, voir “OS/2” à la page 47.

Utilisation de Magic Bullet

Balayage standard

Attention

Si vous avez un lecteur compressé ou tout logiciel spécialisé, vous ne pouvez pas utiliser Magic Bullet pour balayer votre ordinateur en intégralité.

Remarquez que vous ne pouvez pas utiliser Magic Bullet pour balayer un réseau ou si vous utilisez Windows NT ou OS/2. Si vous ne pouvez pas utiliser Magic Bullet, voir “Balayage spécialisé” à la page 2.

1. Mettez votre ordinateur hors tension.

2. Insérez la disquette de Magic Bullet dans le lecteur A: et mettez votre ordinateur sous tension.

   [*Remarque : le message “Starting Magic Bullet...” apparaît brièvement et l’interface de Magic Bullet s’affiche.*]

3. Tapez sur la touche <F2> pour débuter le balayage de tous les fichiers exécutables du ou des disques durs locaux.

4. Si aucun virus n'a été détecté sur votre ordinateur, quittez Magic Bullet à l'aide de la touche <Echap>. Retirez ensuite la disquette et redémarrez votre ordinateur. Si un virus est détecté, poursuivez jusqu'à l'étape 5.

5. Appuyez sur la touche <F4> à partir de l'interface de Magic Bullet pour balayer votre ordinateur et supprimer tout virus connu avant de poursuivre avec l'installation. Lorsqu'aucun virus n'est détecté sur votre ordinateur, quittez Magic Bullet à l'aide de la touche <Echap>. Retirez ensuite la disquette et redémarrez votre ordinateur.

Balayage spécialisé

Si vous possédez un lecteur compressé ou du matériel spécialisé, suivez les instructions suivantes.

Attention Vous ne pouvez pas utiliser cette procédure de balayage de virus sur réseau ou cette procédure si vous faites fonctionner Windows NT ou OS/2.

1. Insérez une disquette système DOS saine (sans virus) et protégée en écriture dans le lecteur A:. Cette disquette système doit correspondre à la version de DOS que vous avez sur le disque dur. Cette disquette doit contenir tous les drivers nécessaires à l'utilitaire de compression de disquettes et de matériel spécialisé que vous utilisez.

   Pour élaborer une disquette système saine, vous devez formater une disquette système. Si vous avez besoin de driver spéciaux pour accéder à votre disque dur, copiez ces derniers sur la disquette et créez un fichier CONFIG.SYS approprié.

Attention Gardez à l'esprit que le fait de formater une disquette supprime toutes les données qu'elle contient.

Par exemple, si vous utilisez Stacker ou SuperStore (compression de disquette ne faisant pas partie du système d'exploitation), vous devez créer une disquette système contenant des copies saines des drivers de compression de disquettes et un fichier CONFIG.SYS permettant de charger ces drivers. Cette disquette système saine vous permet de lire le disque dur et permet à FindVirus de balayer les fichiers stockés sur la disquette.

Par exemple, si vous utilisez l'utilitaire Microsoft's DriveSpace dans la version 6.22 de MS-DOS, vous utilisez les commandes suivantes pour formater votre disquette système saine (cette ligne de commandes considère A: comme le lecteur de disquettes):

```
FORMAT A: /U /S
```

La disquette peut être utilisée pour initialiser l'ordinateur et pour accéder au lecteur compressé.

Lorsqu'une disquette est compressée à l'aide de Microsoft's DoubleSpace ou DriveSpace, un lecteur "hôte" est créé. Il est normalement attribué à la lettre H. Ce lecteur contient le fichier command.com et les fichiers cachés suivants :

```
IO.SYS
MSDOS.SYS
DRVSPACE.BIN
DRVSPACE.000
DRVSPACE.INI
```

Lorsque l'ordinateur est démarré normalement, les fichiers système sont chargés à partir du lecteur H: (le lecteur "hôte"), qui utilise le fichier DRVSPACE.BIN pour monter DRVSPACE.000 sous la forme C:.

Un lecteur de disquette formatée, décrit plus haut, contient les fichiers système normaux, ainsi que le fichier DRVSPACE.BIN qui vous permet d'accéder normalement à la fois au lecteur "hôte" (H:) et au lecteur compressé (C:).

Si vous utilisez un utilitaire de compression de disquettes différent, les noms de fichiers peuvent être différents de ceux dont il est fait référence dans ce manuel.

2. Mettez votre ordinateur sous tension. Une fois que l'invite A:\ apparaît, retirez la disquette système DOS. A ce moment, il est recommandé de vous assurer que vous pouvez accéder normalement à tous les lecteurs. Si vous ne pouvez pas accéder normalement à tous vos lecteurs, cela peut être dû à un problème de configuration survenu sur votre ordinateur.

3. Insérez la disquette Magic Bullet. Tapez maintenant :

   `MB_MENU` <Entrée>

4. A l'apparition de l'interface de Magic Bullet, appuyez sur la touche <F2> pour commencer le balayage de tous les fichiers exécutables sur votre (vos) disque(s) dur(s).

5. Si aucun virus n'est détecté sur votre ordinateur, quittez Magic Bullet à l'aide de la touche <Echap>. Ensuite, retirez la disquette et redémarrez votre ordinateur. Si un virus a été détecté, poursuivez jusqu'à l'étape 6.

6. Appuyez sur la touche <F4> à partir de l'interface de Magic Bullet popur balayer votre ordinateur et supprimer tout virus connu avant de poursuivre l'installation. Lorsqu'aucun virus n'est détecté sur votre ordinateur, quittez Magic Bullet en appuyant sur la touche <Echap>. Retirez ensuite la disquette et redémarrez votre ordinateur.

1.2 Fichiers README

Un fichier README, considéré comme faisant partie de l'installation en elle-même, est copié dans le dossier du Toolkit. Ce fichier contient des rectifications au manuel et fournit des informations relatives aux modifications les plus récentes apportées au Toolkit. Il est recommandé de lire ce fichier attentivement.

Vous êtes invité à consulter le fichier README lors de l'installation du Toolkit. Vous pouvez néanmoins le consulter à tout moment via un programme tel que “Notepad”.

1.3 Windows 3.x

Conditions requises pour le système

Dr Solomon's Anti-Virus Toolkit fonctionne sur tout ordinateur IBM ou sur tout ordinateur compatible avec Windows 3.x. Vous devez avoir :

- DOS 3.3 ou une version ultérieure ; pour connaître la version de DOS que vous utilisez, tapez :

  `VER` <Entrée>

  à partir d'une invite DOS.

Pour l'installation vous devez avoir :

- 5 Mo d'espace disque pour le Toolkit pour Windows et DOS.

Pour vérifier que vous avez suffisamment d'espace disque disponible :

Assurez-vous que vous vous trouvez sur l'invite DOS. Tapez la lettre correspondant au lecteur sur lequel vous souhaitez installer le Toolkit et appuyez sur la touche <Entrée>. Par exemple, tapez :

`C:\` <Entrée>

Au retour de l'invite, tapez :

`DIR` <Entrée>

Une liste des répertoires du lecteur apparaît, suivie par le total de l'espace disque utilisé et du total de l'espace disque disponible. Vous devez disposer d'au moins 5 000 000 octets pour pouvoir installer le Toolkit pour Windows et DOS.

VirusGuard, le scanner résidant dans DOS, fonctionne plus rapidement si votre système possède les éléments suivants :

- mémoire d'extension,
- mémoire étendue,
- une unité de mémoire vive.

Si vous souhaitez faire fonctionner le Toolkit en réseau ou sur plusieurs ordinateurs à la fois, renseignez-vous sur une licence de site auprès de Dr Solomon's ou du distributeur le plus proche.

Première installation de votre Toolkit

Avant d'installer Dr Solomon's Anti-Virus Toolkit, vous devez fermer toutes les applications Windows fonctionnant sur votre ordinateur.

Comment éviter les conflits avec d'autres logiciels antivirus

Afin d'éviter tout conflit, il est recommandé de désinstaller tout autre logiciel anti-virus avant d'installer le Toolkit.

Attention

Vous devez en particulier désinstaller tout autre scanner automatique (sur accès) ou résident en mémoire, tel que Scanshield de McAfee, avant d'installer WinGuard.

Installation à partir d'un CD-ROM

Installation rapide

Conseil

Une mise à jour incrémentielle vous permettra d'utiliser la méthode d'installation rapide pour mettre à jour votre version du Toolkit. La mise à jour de votre Toolkit vous permettra de conserver la configuraton de la version précédente de votre Toolkit. Pour obtenir des instructions sur l'installation complète du Toolkit, voir la section "Options d'installation avancées" à la page 9.

1. Démarrez votre ordinateur et chargez Windows 3.x. A l'apparition du bureau de Windows 3.x, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Sélectionnez **Fichier**, puis **Exécuter** à partir du menu.

3. Dans la zone d'entrée qui apparaît, tapez la lettre correspondant au lecteur de CD-ROM et faites-la suivre par deux points. Tapez ensuite :

   ```
   \SETUP
   ```

   et cliquez sur **OK**. Tapez par exemple :

   ```
   D:\SETUP
   ```

4. Un écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

5. Dans la boîte de dialogue suivante, vous êtes invité à confirmer l'installation de Dr Solomon's Anti-Virus Toolkit pour Windows 3.x. Cliquez sur **Aller**.

6. La boîte de dialogue de vérification du disque Magic Bullet apparaît. Si vous avez déjà vérifié votre ordinateur à l'aide du disque Magic Bullet de Dr Solomon's, cliquez sur **OK**. Si tel n'est pas le cas, reportez vous à la section "Balayage préliminaire" à la page 1.

7. La boîte de dialogue "Recherche de l'emplacement de destination" apparaît. Si vous souhaitez installer le Toolkit dans un répertoire différent de celui qui vous est proposé par défaut, cliquez sur **Parcourir**, puis sélectionnez le lecteur et / ou le répertoire sur lequel vous souhaitez le Toolkit. Cliquez sur **Suivant**.

   Vous pouvez annuler l'installation en cliquant sur **Annuler**.

8. Cliquez sur **Oui** pour confirmer l'activation des scanners automatiques (lors de l'accès).

Conseil

Il est recommandé de confirmer l'activation des scanners automatiques (lors de l'accès). Si, pour quelque raison que ce soit, vous choisissez de ne pas le faire, vous pouvez les activer ultérieurement. Pour obtenir des informations sur l'activation de VirusGuard, reportez-vous à la rubrique "VirusGuard" de l'aide en ligne du Toolkit. Pour obtenir des informations sur l'activation de WinGuard. Voir la section "Modification de la configuration de WinGuard" à la page 88.

9. Cliquez sur **Oui** pour confirmer que le Scheduler doit être actif. Si vous cliquez sur **Non**, vous pouvez activer le Scheduler à une date ultérieure. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir la section "Exécution du Scheduler" à la page 134.

   Le Scheduler vous permet de définir des événements à exécuter à des heures prédéterminées. Ces événements peuvent consister en des recherches de virus, des vérifications de fichiers ou l'exécution de n'importe quelle application et qui peut arriver une fois ou à intervalles réguliers.

10. Cliquez sur **Oui** pour consulter le fichier Readme, puis fermez ce fichier pour revenir à l'installation.

11. Cliquez sur **OK** pour commencer une recherche de virus sur votre ordinateur. Le balayage FindVirus débute immédiatement. Si un virus est détecté, reportez-vous à la section "Désinfection des lecteurs" à la page 145.

12. Cliquez sur **OK** dans la boîte de message "Tout est sain - aucun virus détecté" puis sur **Quitter** pour terminer la fenêtre du balayage FindVirus. Enlevez toute disquette du lecteur de disquettes.

Conseil

Il est recommandé de redémarrer immédiatement votre ordinateur, pour activer VirusGuard et WinGuard, ainsi que les scanners automatiques (lors de l'accès) de Dr Solomon's.

13. Sélectionnez l'une des options de la boîte de dialogue **"**Installation terminée" et appuyez sur **Terminé**.

Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi les procédures décrites dans ce manuel et passez en revue la section Dépannage de "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Options d'installation avancées

Conseil

Cette option permet d'installer une version complète du Toolkit, écrasant ainsi la version précédente et les configurations définies pour cette version du Toolkit.

1. Démarrez votre ordinateur et chargez Windows 3.x. Lorsque le bureau de Windows 3.x apparaît, insérez votre CD de station de travail dans le lecteur de CD-ROM.

2. Sélectionnez **Fichier** et choisissez **Exécuter** dans le menu.

3. Dans la zone d'entrée qui apparaît, tapez la lettre correspondant au lecteur de CD-ROM, suivi par deux points. Puis, tapez :

   ```
   \SETUP
   ```

   et cliquez sur **OK**. Par exemple, tapez :

   ```
   D:\SETUP
   ```

4. Un écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Options d'installation avancées** et cliquez sur **Suivant**.

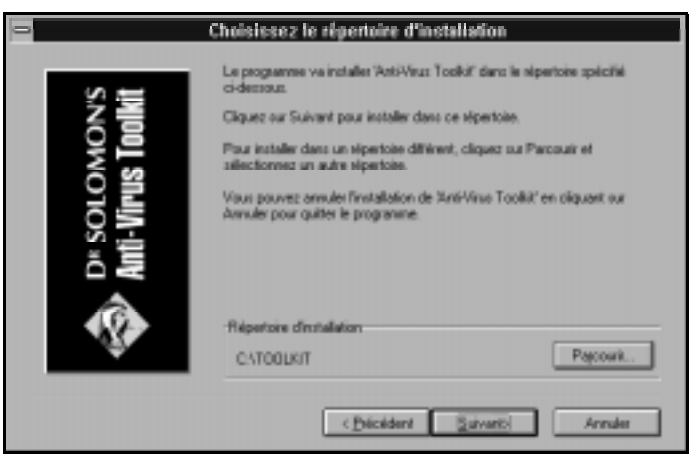
5. Dans la boîte de dialogue suivante, sélectionnez **Installer Dr Solomon's Anti-Virus Toolkit**. Cliquez sur **Suivant**.

6. La boîte de dialogue suivante vous demande confirmation de l'installation de Dr Solomon's Anti-Virus Toolkit pour Windows 3.x. Cliquez sur **Aller**.

7. La boîte de dialogue suivante apparaît :.

Si vous avez déjà vérifié votre ordinateur avec le disque de vérification Magic Bullet de Dr Solomon's, cliquez sur **OK**. Dans le cas contraire, reportez-vous à la section "Balayage préliminaire" à la page 1.

8. La boîte de dialogue "Recherche de l'emplacement de destination" vous permet de sélectionner le lecteur et le répertoire dans lequel vous souhaitez installer votre Toolkit. Si vous souhaitez installer le Toolkit dans un répertoire différent de celui qui vous est suggéré par les paramètres par défaut, cliquez sur **Parcourir** et sélectionnez le lecteur et / ou le répertoire sur lequel vous souhaitez installer le Toolkit. Lorsque vous avez sélectionné le lecteur et le répertoire dans lequel vous souhaitez installer le Toolkit, cliquez sur **Suivant**.



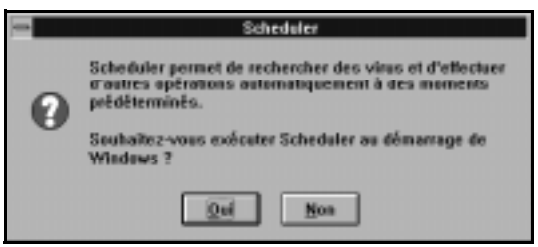
Vous pouvez annuler l'installation en cliquant sur **Annuler**.

9. Cliquez sur **Oui** pour confirmer l'activation des scanners automatiques (lors de l'accès)..

Conseil

Il est recommandé de confirmer l'activation des scanners automatiques (lors de l'accès). Si, pour quelque raison que ce soit, vous choisissez de ne pas le faire, vous pouvez les activer ultérieurement. Pour obtenir des informations sur l'activation de VirusGuard, voir la rubrique "VirusGuard" de l'aide en ligne du Toolkit. Pour obtenir des informations sur l'activation de WinGuard, voir la section "Modification de la configuration de WinGuard" à la page 88.

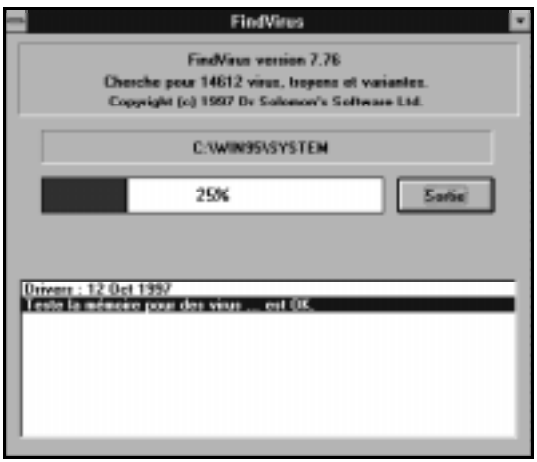
10. Cliquez sur **Oui** pour confirmer l'activation du Scheduler. Si vous cliquez sur **Non**, vous pouvez activer le Scheduler ultérieurement. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir "Exécution du Scheduler" à la page 134.



Le Scheduler vous permet de définir des événements à exécuter à des heures prédéterminées. Ces événements peuvent consister en des balayages de virus, des vérifications de fichiers ou l'exécution de n'importe quelle application et peuvent se produire une fois ou à intervalles réguliers.

11. Cliquez sur **Oui** pour consulter le fichier Readme et fermez le fichier Readme pour revenir à l'installation.

12. Cliquez sur **OK** pour démarrer la recherche de virus sur votre ordinateur. Le balayage de FindVirus commence immédiatement.

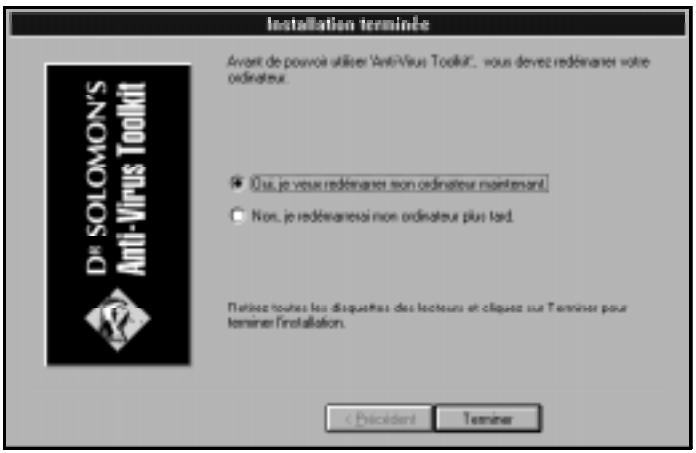


Si un virus est détecté, reportez-vous à la section "Désinfection des lecteurs" à la page 145.

13. Cliquez sur **OK** dans la boîte de dialogue "Tout est sain - aucun virus détecté", puis sur **Quitter** pour fermer la fenêtre de balayage de FindVirus. Retirez tout disque du lecteur de disquettes.

Conseil Il est recommandé de redémarrer votre ordinateur immédiatement afin d'activer VirusGuard et WinGuard, ainsi que les scanners automatiques (lors de l'accès) de Dr Solomon's.

14. Sélectionnez l'une des options de la boîte de dialogue **"**Installation terminée" et cliquez sur **Terminé**.

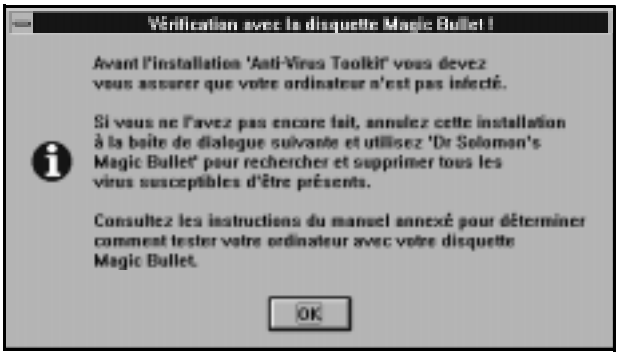


Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi les procédure décrites dans ce manuel et passez en revue la section Dépannage dans "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

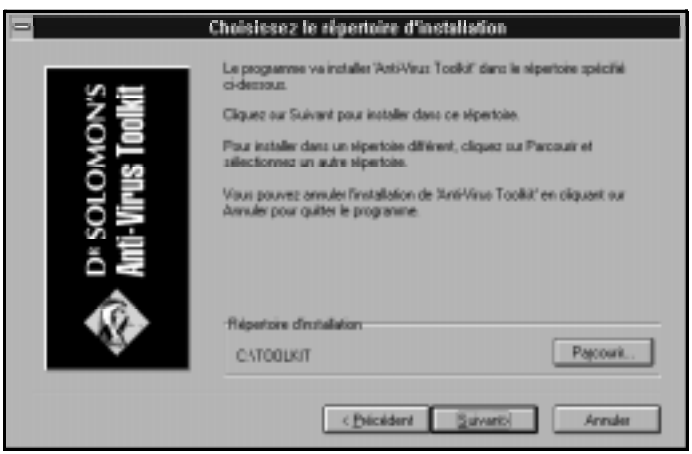
Installation à partir de disquettes

1. Insérez la première disquette d'installation de Dr Solomon's Anti-Virus Toolkit (étiquetée Windows 3.x) dans le lecteur de disquettes.
2. Dans le Gestionnaire de programmes, sélectionnez **Fichier**, puis **Exécuter**.
3. Tapez `A:\Setup` et cliquez sur **OK**.

4. La boîte de dialogue de la disquette de vérification Magic Bullet apparaît. Si vous avez déjà vérifié votre ordinateur avec la disquette de vérification Magic Bullet de Dr Solomon's, cliquez sur **OK**. Si tel n'est pas le cas, reportez-vous à la section "Balayage préliminaire" à la page 1.



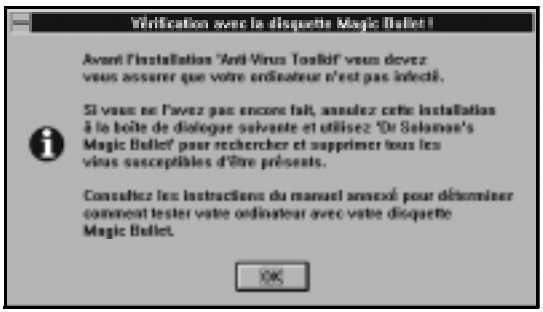
5. La boîte de dialogue "Recherche de l'emplacement de destination" vous permet de sélectionner le lecteur et le répertoire dans lesquels vous souhaitez installer votre Toolkit. Si vous souhaitez installer le Toolkit dans un répertoire différent de celui qui vous est proposé par les paramètres par défaut, cliquez sur **Parcourir** et sélectionnez le lecteur et / ou le répertoire dans lequel vous souhaitez installer le Toolkit. Une fois le lecteur et le répertoire dans lequel vous souhaitez installer le Toolkit sélectionné, cliquez sur **Suivant**.



6. Insérez les disquettes d'installation comme il vous est demandé et cliquez sur **OK**.

Vous pouvez annuler l'installation en cliquant sur **Annuler**.

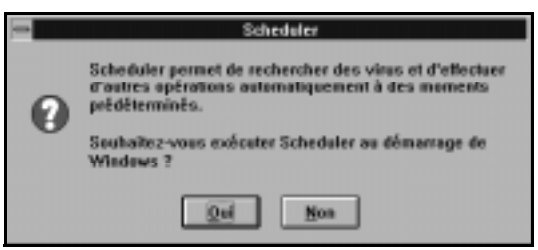
7. Cliquez sur **Oui** pour confirmer l'activation des scanners automatiques (lors de l'accès).



Conseil

Il est recommandé de confirmer l'activation des scanners automatiques (lors de l'accès). Si, pour quelque raison que ce soit, vous choisissez de ne pas le faire, vous pouvez les activer ultérieurement. Pour obtenir des informations sur l'activation de VirusGuard, voir la rubrique "VirusGuard" de l'aide en ligne du Toolkit. Pour obtenir des informations sur l'activation de WinGuard, voir "Modification de la configuration de WinGuard" à la page 88.

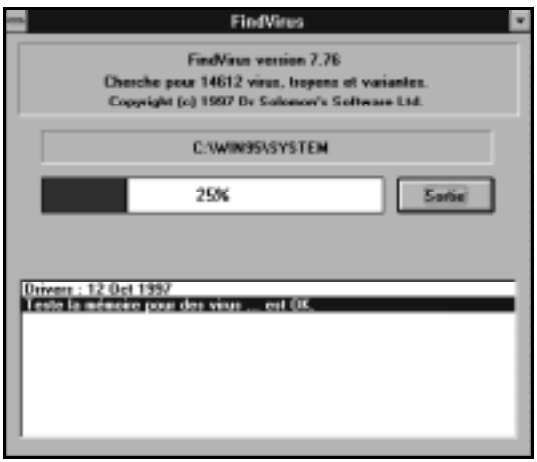
8. Cliquez sur **Oui** pour confirmer l'activation du Scheduler. Si vous cliquez sur **Non**, le Scheduler peut être activé ultérieurement. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir "Exécution du Scheduler" à la page 134.



Le Scheduler vous permet de définir des événements à exécuter à des heures prédéterminées. Ces événements peuvent consister en des recherches de virus, des vérifications de fichiers ou des exécutions de n'importe quelle application et peuvent se produire une seule fois ou à intervalles réguliers.

9. Cliquez sur **Oui** pour consulter le fichier Readme et fermer le fichier Readme pour revenir à l'installation.

10. Cliquez sur **OK** pour commencer une recherche de virus sur votre ordinateur. Le balayage FindVirus commence immédiatement.



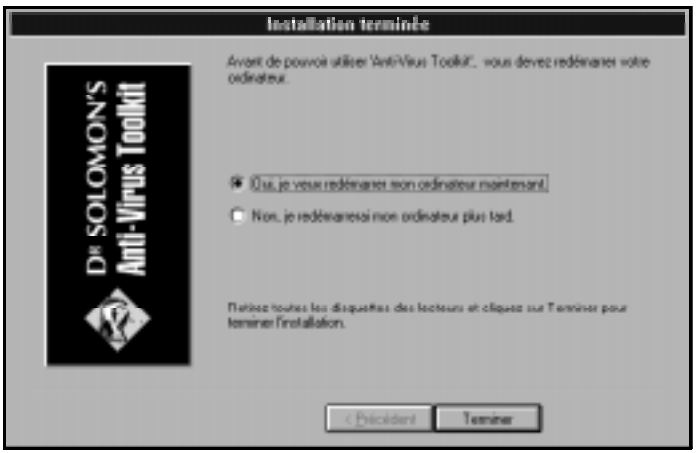
Si un virus est détecté, reportez-vous à la section "Désinfection des lecteurs" à la page 145.

11. Cliquez sur **OK** pour faire apparaître la boîte de dialogue 'Tout est sain - aucun virus détecté", puis sur **Quitter** pour fermer la fenêtre de balayage FindVirus. Retirez toute disquette du lecteur de disquettes.

Conseil

Il est recommandé de redémarrer votre ordinateur immédiatement, ceci afin d'activer VirusGuard et WinGuard, ainsi que les scanners automatiques (lors de l'accès) de Dr Solomon's.

12. Sélectionnez l'une des options de la boîte de dialogue **"**Installation terminée" et cliquez sur **Terminé**.



Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel et passez en revue la section Dépannage dans "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

Désinstallation de votre Toolkit

Attention

Si vous faites passer votre système de Windows 3.x à Windows 95, vous devez tout d'abord désactiver WinGuard. La version de WinGuard pour Windows 3.x n'est pas compatible avec Windows 95.

Conseil

Si vous désinstallez un Toolkit pour Windows 3.x, c'est-à-dire la version 7.75 ou une version antérieure, vous devrez désinstaller le Toolkit manuellement. Pour obtenir des instructions sur la désinstallation manuelle du Toolkit pour Windows 3.x, voir la section "Désinstallation sans un utilitaire de désinstallation" à la page 177.

Pour désinstaller Dr Solomon's Anti-Virus Toolkit pour Windows 3.x :

1. Dans Windows, cliquez deux fois sur le groupe de programmes Dr Solomon's AVTK.

2. Cliquez deux fois sur **Désinstaller Dr Solomon's AVTK**.

3. Dans la boîte de dialogue d'avertissement qui apparaît, cliquez sur **Oui.**

4. Si WinGuard est en cours de fonctionnement, Uninstaller doit réinitialiser votre ordinateur pour désactiver WinGuard. Une boîte de dialogue vous demande si vous souhaitez permettre à Uninstaller de réinitialiser votre ordinateur. Cliquez sur **Oui**. Si vous cliquez sur **Non**, la désinstallation est interrompue.

   L'écran devient vide, Windows redémarre et la désinstallation de Dr Solomon's Anti-Virus Toolkit se poursuit.

5. A ce moment, Uninstaller peut vous demander si vous souhaitez effacer ou déplacer des fichiers, comme par exemple des fichiers journal ou Scheduler. La boîte de dialogue vous propose les options suivantes :

- **Effacer** permet d'effacer uniquement le nom du fichier en cours.
- **Effacer tout** permet d'effacer ce fichier ainsi que tous les autres fichiers dans le répertoire sans invite préalable.
- **Déplacer** permet de déplacer uniquement le nom de fichier en cours. La boîte de dialogue "Enregistrer sous" apparaît. Sélectionnez un nouveau répertoire et / ou un nom de fichier pour le fichier.
- **Déplacer tous** permet de déplacer ce fichier ainsi que tous les autres fichiers dans le répertoire dans invite préalable. La boîte de dialogue "Répertoire de destination" apparaît. Sélectionnez un nouveau répertoire.

   Sélectionnez l'une des options suivantes.

6. Dans la boîte de dialogue, cliquez sur **Terminé** pour terminer la désinstallation de Dr Solomon's Toolkit.

1.4 Windows 95

Conditions requises pour le système

L'Anti-Virus Toolkit pour Windows 95 fonctionne sur tout ordinateur possédant Windows 95.

Environ 5 Mo d'espace disque sont requis.

Si vous souhaitez installer le Toolkit sur plusieurs ordinateurs, vous devez vous renseigner sur les licences de sites auprès de Dr Solomon's ou du distributeur le plus proche.

Première installation du Toolkit

Comment éviter les conflits avec un autre logiciel antivirus

Afin d'éviter tout conflit, il est recommandé de désinstaller tout autre logiciel antivirus avant l'installation du Toolkit.

Attention

Vous devez, en particulier, désinstaller tout autre scanner automatique (sur accès) ou résident en mémoire, tel que Scanshield de McAfee, avant d'installer WinGuard.

Installation à partir d'un CD-ROM

Attention

Si une version du Toolkit pour Windows 3.x est installée, vous devez la supprimer avant d'installer le Toolkit pour Windows 95. Pour savoir comment supprimer le Toolkit pour Windows 3.x, voir "Désinstallation de votre Toolkit" page 17.

Installation rapide

Conseil

Bientôt une mise à jour incrémentielle vous permettra d'utiliser la méthode d'installation rapide pour mettre à jour le Toolkit déjà installé sur votre ordinateur. La mise à jour de votre Toolkit vous permet de conserver les configurations de la version précédente de votre Toolkit. Pour obtenir des informations sur l'installation complète du Toolkit, voir la section "Options d'installation avancées" à la page 23.

1. Démarrez votre ordinateur. Lorsque le bureau de Windows 95 apparaît, insérez le CD d'installation du Toolkit dans le lecteur de CD-ROM.

2. Un écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

3. Dans la boîte de dialogue suivante, on vous demande confirmation pour l'installation de Dr Solomon's Anti-Virus Toolkit pour Windows 95. Cliquez sur **Aller**.

4. Une boîte de dialogue vous invite à continuer ou à abandonner l'installation. Cliquez sur **Continuer**.

5. La boîte de dialogue suivante vous demande à quel emplacement vous souhaitez installer le Toolkit. Tapez un chemin d'accès différent si vous le désirez. Cliquez sur **OK**.

   Si vous le souhaitez, vous pouvez annuler l'installation en cliquant sur **Annuler**.

6. Des options d'exécution de WinGuard apparaissent.

Conseil

Il est fortement recommandé de sélectionner **Exécuter WinGuard automatiquement**. WinGuard est constamment exécuté en arrière-plan. WinGuard vérifie que les fichiers ne sont pas infectés avant de vous permettre d'y accéder. Voir la section "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71 pour plus de détails.

7. Des options vous invitent à exécuter VirusGuard. VirusGuard est la contre-partie DOS de WinGuard. Il vous fournit une protection lorsque Windows 95 n'est pas actif. VirusGuard peut être configuré pour balayer lors d'opérations différentes (copie de fichiers, lancement de fichiers exécutables, etc.)

Aide

Pour plus de détails sur les options de VirusGuard, voir la section "Paramètres de référence" sous la rubrique "VirusGuard" dans l'aide en ligne du Toolkit.

Conseil

Il est fortement recommandé de sélectionner l'une des options **Installer VirusGuard**.... **Sécurité standard** balaie les fichiers lors de toutes les tentatives de copies, alors que **Sécurité minimum** ne balaie que les fichiers que vous tentez de copier à partir de disquettes.

8. Si vous avez choisi d'installer VirusGuard, une boîte de dialogue vous indique que votre fichier AUTOEXEC.BAT a subi des modifications pour pouvoir lancer VirusGuard et que le fichier AUTOEXEC.BAT d'origine a été sauvegardé sous AUTOEXEC.DRS. Cliquez sur **OK** pour continuer.

9. Des options vous invitent à exécuter Dr Solomon's Scheduler. Si vous choisissez **Oui**, le Scheduler est ajouté au dossier Démarrage. Si vous sélectionnez **Non**, vous devez démarrer le Scheduler manuellement chaque fois que vous souhaitez l'utiliser. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir "Exécution du Scheduler" à la page 134.

   Le Scheduler vous permet de définir des événements à exécuter à des moments prédéterminés. Les événements peuvent servir à rechercher des virus éventuels, vérifier des fichiers ou exécuter n'importe quelle application. Ils peuvent se produire une seule fois ou à intervalles réguliers.

10. Une invite vous demande si vous souhaitez installer l'outil DOS 16 bits "CLEANBOO". Cet outil est très utile. Il est donc recommandé de l'installer. Pour plus d'informations sur cet outil, voir la section "CleanBoot" à la page 179 et la rubrique "CleanBoot" de l'aide en ligne du Toolkit.

11. Une fois les fichiers copiés sur le disque dur, un message vous indique le démarrage d'un balayage FindVirus. Cliquez sur **OK** pour continuer.

    Une boîte de dialogue vous indique l'évolution du balayage. Vous pouvez cliquer sur **Quitter** pour arrêter le balayage. Il est recommandé de ne pas l'arrêter car il est possible que des virus ne soient pas détectés sur le disque dur. Si vous l'arrêtez, vous devez effectuer un balayage FindVirus complet dès que l'installation est terminée.

    Lorsque le balayage est terminé, un message vous informe des résultats du balayage. Cliquez sur **OK** pour continuer.

    Pour plus d'informations sur FindVirus, voir "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

12. Cliquez sur **Quitter.**

13. Une invite vous demande si vous souhaitez visualiser les modifications les plus récentes apportées à Dr Solomon's Anti-Virus Toolkit pour Windows 95. Cliquez sur **Oui** pour consulter le fichier ReadMe. Si vous cliquez sur **Non**, vous continuez sans consulter le fichier ReadMe. Il est recommandé de consulter le fichier ReadMe, car il contient des informations sur les nouvelles fonctions et les modifications apportées au logiciel.

14. Une invite vous demande si vous souhaitez redémarrer l'ordinateur. Si vous choisissez **Non**, le Scheduler, VirusGuard et WinGuard ne fonctionneront pas avant le prochain démarrage de l'ordinateur.

Si vous rencontrez des problèmes lors de l'installation de Toolkit, assurez-vous d'avoir suivi les procédures décrites dans ce manuel et passez en revue la section Dépannage dans "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

Options d'installation avancées

Attention

Si la version pour Windows 3.x du Toolkit est installée sur votre ordinateur, vous devez la supprimer avant d'installer le Toolkit pour Windows 95. Pour savoir comment supprimer la version Windows 3.x du Toolkit, voir "Désinstallation de votre Toolkit" page 17.

Conseil

Cette option permet d'installer une version complète du Toolkit, en écrasant la version existante du Toolkit ainsi que toutes les configurations définies pour cette version du Toolkit.

Conseil

Dr Solomon's Anti-Virus Toolkit pour Windows 95 peut être installé via SMS. Voir le fichier Microsoft SMS PDF fournit avec votre Toolkit pour les options d'installation.

1. Démarrez votre ordinateur. Lorsque votre bureau Windows 95 apparaît, insérez le CD de votre Toolkit dans le lecteur de CD-ROM.

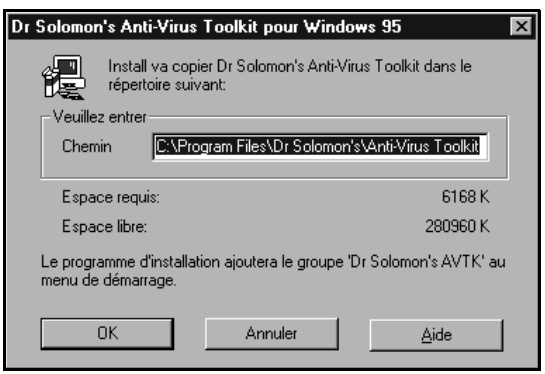
2. Un écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Options d'installation avancées** et cliquez sur **Suivant**.

3. Dans la boîte de dialogue suivante, sélectionnez **Installation de Dr Solomon's Anti-Virus Toolkit** et cliquez sur **Suivant**.

4. La boîte de dialogue suivante vous demande de confirmer si vous souhaitez installer Dr Solomon's Anti-Virus Toolkit pour Windows 95. Cliquez sur **Aller**.

5. Une boîte de dialogue vous invite à poursuivre ou à abandonner l'installation. Cliquez sur **Continuer**.

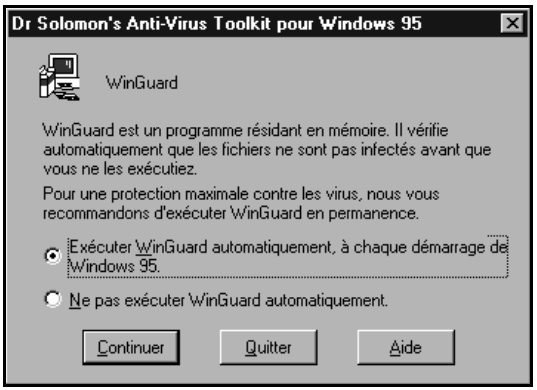
Une boîte de dialogue vous invite à déterminer le chemin d'accès dans lequel vous souhaitez installer le Toolkit.



6. Tapez un second chemin d'accès si vous le souhaitez. Cliquez sur **OK**.

   Si vous souhaitez annuler l'installation cliquez sur **Annuler**.

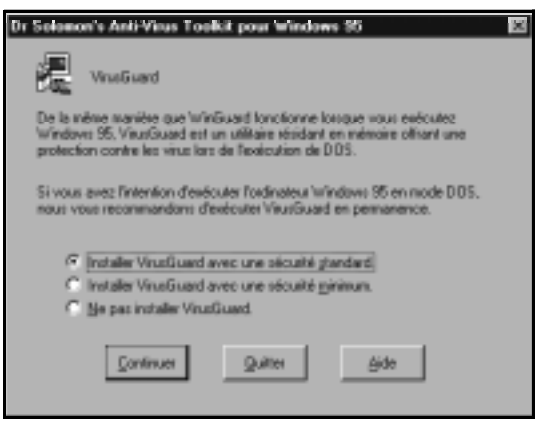
7. Des options vous invitent à exécuter WinGuard.



Conseil

Il est fortement recommandé de sélectionner **Exécuter WinGuard automatiquement**. WinGuard fonctionne constamment en arrière-plan. Il vérifie que les fichiers ne sont pas infectés avant de vous permettre d'y accéder. Voir "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71 pour plus de détails.

8. Des options vous invitent à exécuter VirusGuard.



VirusGuard est la contrepartie DOS de WinGuard. Il fournit une protection lorsque Windows 95 est désactivé. VirusGuard peut être configuré pour balayer lors d'opérations différentes (copie de fichiers, lancement d'exécutables, etc.)

Aide

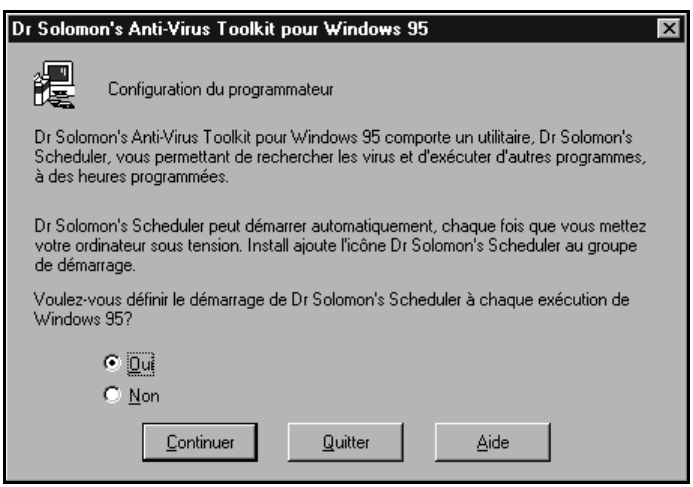
Pour plus de détails sur les options de VirusGuard, voir "Paramètres de référence" sous la rubrique "VirusGuard" de l'aide en ligne du Toolkit.

Conseil

Il est fortement recommandé de sélectionner l'une des options **Installation de VirusGuard**..... **Sécurité standard** balaie les fichiers lors de toutes les tentatives de copies de fichiers, alors que **Sécurité minimum** ne balaie que les fichiers que vous tentez de copier à partir de disquettes.

9. Si vous choisissez d'installer VirusGuard, une boîte de dialogue vous indique que votre fichier AUTOEXEC.BAT a subi des modifications pour pouvoir démarrer VirusGuard et que le fichier AUTOEXEC.BAT d'origine a été sauvegardé sous AUTOEXEC.DRS. Cliquez sur **OK** pour poursuivre.

10. Des options vous invitent à exécuter Dr Solomon's Scheduler.



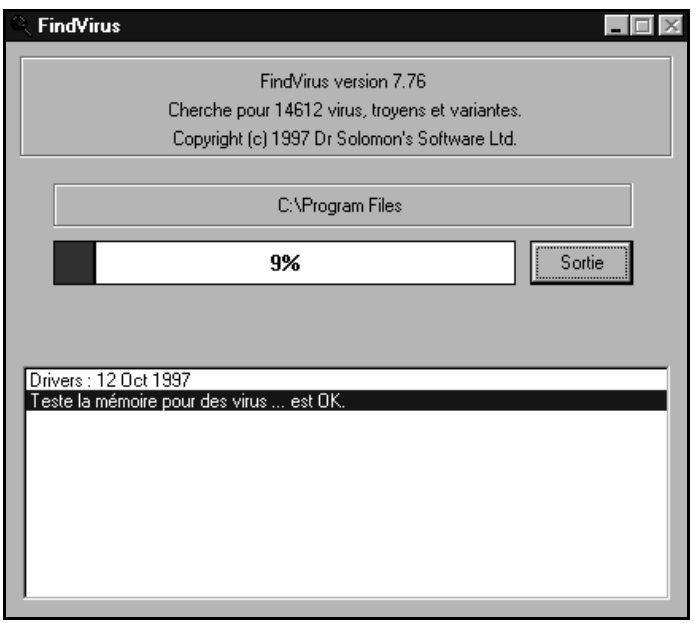
Si vous sélectionnez **Oui**, le Scheduler est ajouté au dossier Démarrage. Si vous sélectionnez **Non**, vous devez démarrer le Scheduler manuellement chaque fois que vous souhaitez l'utiliser. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir "Exécution du Scheduler" à la page 134.

Le Scheduler vous permet de définir des événements à exécuter à des moments prédéterminés. Les événements peuvent servir à rechercher des virus, vérifier des fichiers ou exécuter n'importe quelle application. Ils peuvent se produire une seule fois ou à intervalles réguliers.

11. Une invite vous demande si vous souhaitez installer l'outil DOS 16 bits "CLEANBOO". Cet outil est très utile. Il est donc recommandé de l'installer. Pour plus d'informations sur cet outil, voir la section "CleanBoot" à la page 179 et la rubrique "Cleanboot" dans l'aide en ligne du Toolkit.

12. Une fois que les fichiers sont copiés sur le disque dur, un message vous indique qu'un balayage FindVirus est sur le point de démarrer. Cliquez sur **OK** pour poursuivre.

    Une boîte de dialogue indique l'évolution du balayage :



Vous pouvez cliquer sur **Quitter** pour arrêter le balayage. Il est déconseillé de le faire car il est possible que des virus ne soient pas détectés sur le disque dur. Si vous l'arrêtez, vous devez effectuer un balayage FindVirus complet dès que l'installation est terminée.

13. Une fois le balayage terminé, un message vous indique les résultats du balayage. Cliquez sur **OK** pour poursuivre.

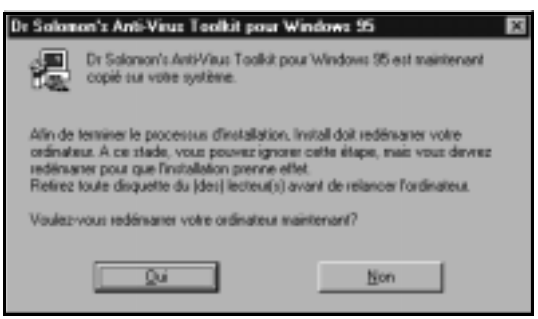
    Pour plus d'informations sur FindVirus, voir "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

14. Cliquez sur **Quitter.**

15. Une invite vous demande si vous souhaitez visualiser les modifications les plus récentes apportées à Dr Solomon's Anti-Virus Toolkit pour Windows 95.

    Cliquez sur **Oui** pour consulter le fichier ReadMe. Si vous cliquez sur **Non**, vous poursuivez sans consulter le fichier ReadMe. Il est recommandé de consulter le fichier ReadMe car il contient des informations sur les nouvelles fonctions et toutes les modifications apportées au logiciel.

16. Une invite vous demande si vous souhaitez redémarrer votre ordinateur.



Si vous choisissez **Non**, le Scheduler, VirusGuard et WinGuard ne fonctionneront pas avant le prochain démarrage de l'ordinateur.

Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous que vous avez suivi la procédure décrite dans ce manuel et passez en revue la section Dépannage dans "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

Installation à partir de disquettes

Attention

Si le Toolkit installé est la version pour Windows 3.x, vous devez le supprimer avant d'installer la version pour Windows 95. Pour savoir comment supprimer la version pour Windows 3.x, voir "Désinstallation de votre Toolkit" page 17.

Une fois que vous savez que l'ordinateur n'est pas infecté et que vous avez désinstallé la version pour Windows 3.x (si cette dernière était installée), vous pouvez installer la version pour Windows 95 du Toolkit.

1. Démarrez Windows 95 et insérez la première disquette d'installation de Dr Solomon's Anti-Virus Toolkit (étiquetée Windows 95) dans le lecteur de disquettes.

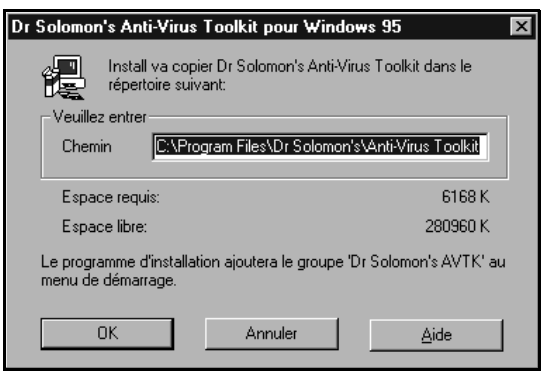
2. Cliquez sur **Démarrer**, puis sur **Exécuter**. Dans la zone "Ouvrir", tapez :

   ```
   A:\SETUP
   ```

3. Cliquez sur **OK**.

4. Une boîte de dialogue vous invite à poursuivre ou à abandonner l'installation. Cliquez sur **Continuer**.

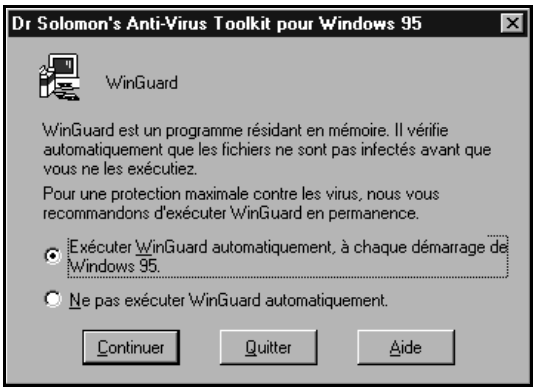
Une boîte de dialogue vous invite à taper le chemin d'accès dans lequel vous souhaitez installer le Toolkit.



5. Tapez un second chemin d'accès si vous le souhaitez. Cliquez sur **OK**.

6. Suivez les invites pour insérer les disquettes suivantes. Si vous le souhaitez, vous pouvez annuler l'installation en cliquant sur **Annuler**.

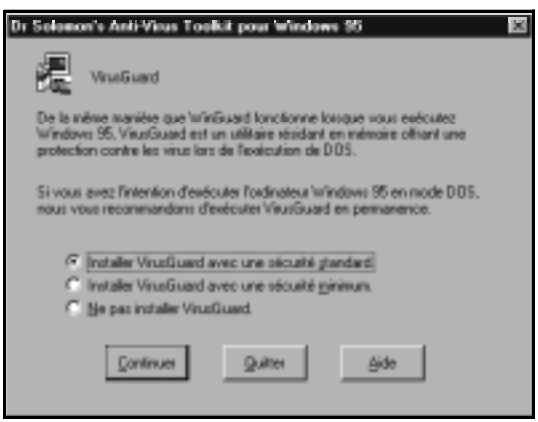
7. Des options vous invitent à exécuter WinGuard.



Conseil

Il est fortement recommandé de sélectionner **Exécuter WinGuard automatiquement**. WinGuard fonctionne constamment en arrière-plan. Il vérifie que les fichiers ne sont pas infectés avant de vous permettre d'y accéder. Voir "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71 pour plus de détails.

8. Des options vous invitent à exécuter VirusGuard.



VirusGuard est la contrepartie DOS de WinGuard. Il fournit une protection lorsque Windows 95 n'est pas actif. VirusGuard peut être configuré pour balayer lors de différentes opérations (copie de fichiers, lancement d'exécutables, etc.)

Aide

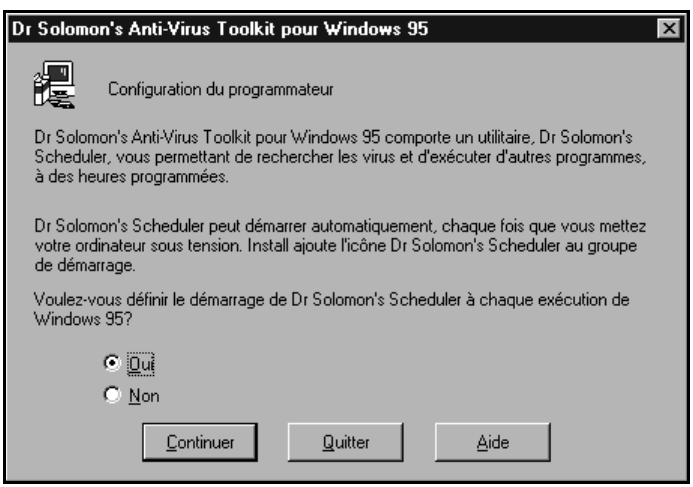
Pour plus de détails sur les options de VirusGuard, voir "Paramètres de référence" sous la rubrique "VirusGuard" de l'aide en ligne du Toolkit.

Conseil

Il est fortement recommandé de sélectionner l'une des options **Installer VirusGuard**..... **Sécurité standard** balaie les fichiers lors de toutes les tentatives de copies alors que **Sécurité minimum** ne balaie les fichiers que lors de tentatives de copies à partir de disquettes.

9. Si vous choisissez d'installer VirusGuard, une boîte de dialogue vous indique que votre fichier AUTOEXEC.BAT a subi des modifications pour pouvoir démarrer VirusGuard et que votre fichier AUTOEXEC.BAT d'origine a été sauvegardé sous AUTOEXEC.DRS. Cliquez sur **OK** pour poursuivre.

10. Des options vous invitent à exécuter Dr Solomon's Scheduler.



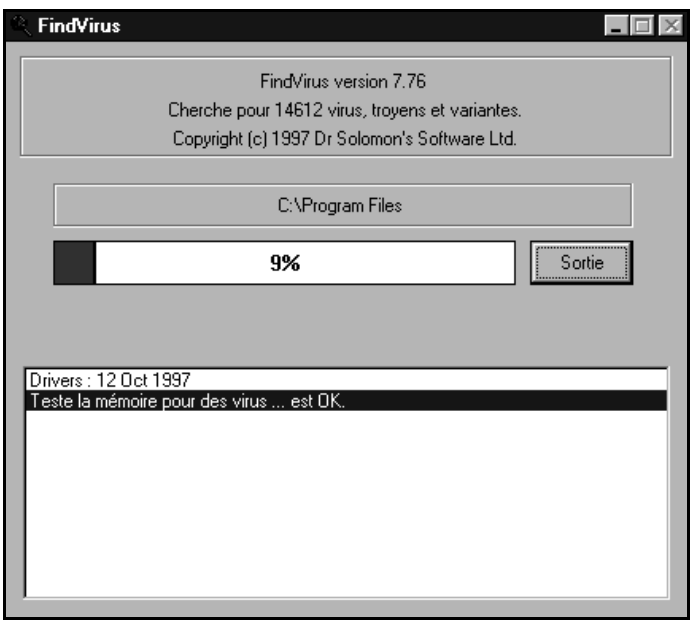
Si vous sélectionnez **Oui**, le Scheduler est ajouté au dossier Démarrage. Si vous sélectionnez **Non**, vous devrez démarrer le Scheduler manuellement chaque fois que vous souhaiterez l'utiliser. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir "Exécution du Scheduler" à la page 134.

Le Scheduler vous permet de définir des événements à exécuter à des moments prédéterminés. Ces événements peuvent servir à rechercher des virus, vérifier des fichiers ou exécuter n'importe quelle application et peuvent se produire une seule fois ou à intervalles réguliers.

11. Une invite vous demande si vous souhaitez installer l'outil DOS 16 bits "CLEANBOO". Cet outil est très utile. Il est donc recommandé de l'installer. Pour plus d'informations à propos de cet outil, voir la section "CleanBoot" à la page 179 et la rubrique "CleanBoot" de l'aide en ligne du Toolkit.

12. Une fois que les fichiers sont copiés sur le disque dur, un message vous indique qu'un balayage FindVirus est sur le point de démarrer. Cliquez sur **OK** pour poursuivre.

    Une boîte de dialogue indique l'évolution du balayage :



Vous pouvez cliquer sur **Quitter** pour arrêter le balayage. Il est déconseillé de procéder de cette manière car il est possible que des virus ne soient pas detectés sur le disque dur. Si vous l'arrêtez, vous devez effectuer un balayage FindVirus complet dès que l'installation est terminée.

13. Une fois le balayage terminé, un message apparaît vous indiquant les résultats du balayage. Cliquez sur **OK** pour poursuivre.

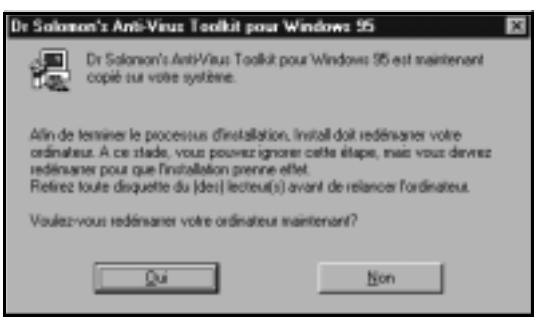
    Pour plus d'informations sur FindVirus, voir "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

14. Cliquez sur **Quitter.**

15. Une invite vous demande si vous souhaitez visualiser les modifications les plus récentes apportées à Dr Solomon's Anti-Virus Toolkit pour Windows 95.

    Cliquez sur **Oui** pour consulter le fichier readme. Si vous cliquez sur **Non**, vous poursuivez sans consulter le fichier ReadMe. Il est recommandé de consulter le fichier ReadMe car il contient des informations sur les nouvelles fonctions ainsi que toutes les modifications apportées au logiciel.

16. Une invite vous demande si vous souhaitez redémarrer votre ordinateur.



Si vous choisissez **Non**, le Scheduler, VirusGuard et WinGuard ne fonctionneront pas avant le prochain démarrage de l'ordinateur.

Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel et consultez la section Dépannage dans "Dépannage et options avancées" à la page 177. Si vous ne pouvez pas résoudre ce problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

Désinstallation de votre Toolkit

Conseil

Si Dr Solomon's Anti-Virus Toolkit n'est pas répertorié sous l'option Ajout/Suppression de programmes dans le Panneau de configuration, vous devez désinstaller le Toolkit manuellement. Pour obtenir des informations sur la désinstallation manuelle de votre Toolkit, voir "Désinstallation sans un utilitaire de désinstallation" à la page 177.

Pour désinstaller le Toolkit :

1. A partir du menu **Démarrer**, sélectionnez **Paramètres** puis **Panneau de configuration**.
2. Cliquez sur **Ajout/Suppression de programmes** dans le Panneau de configuration.
3. Sélectionnez **Dr Solomon's Anti-Virus Toolkit** dans la liste.
4. Cliquez sur **Ajout/Suppression**.
5. A l'invite, confirmez la suppression du programme.
6. Répondez à l'invite pour déplacer ou supprimer tout fichier qui a été ajouté au répertoire du Toolkit depuis l'installation (tel que des fichiers rapport).

1.5 Windows NT

Conseil

Dr Solomon's Anti-Virus Toolkit pour Windows NT peut être installé via SMS. Voir le fichier PDF de Microsoft SMS fourni pour les options d'installation de votre Toolkit.

Conditions requises pour le système

Matériel requis

L'anti-virus Toolkit pour Windows NT fonctionne sur des ordinateurs fonctionnant sous Windows NT Workstation ou Server. Il requiert un processeur Intel et ne fonctionne sur aucune autre plate-forme que Windows NT.

Environ 5 Mo d'espace disque sont requis.

WinGuard NT est également disponible pour les machines Digital Alpha. Contactez Dr Solomon's Software ou le distributeur le plus proche pour plus de détails.

Logiciel requis

L'anti-virus Toolkit pour Windows NT nécessite la version 3.51 de Windows NT ou une version ultérieure.

Il est recommandé de rester informé des dernières nouveautés de Microsoft Windows NT.

Si vous souhaitez faire fonctionner le Toolkit en réseau ou sur plusieurs ordinateurs en même temps, renseignez-vous à propos des licences de site auprès de Dr Solomon's ou du distributeur le plus proche.

Dr Solomon's met également à votre disposition l'Anti-Virus Toolkit Management Edition pour Windows NT Server. Ce Management Edition Toolkit propose une diffusion logicielle et vous permet de configurer à distance.

Première installation de votre Toolkit

Comment évitez des conflits avec d'autres logiciels antivirus

Afin d'éviter tout conflit, il est recommandé de désinstaller tout autre lociciel antivirus avant l'installation du Toolkit.

Attention

Vous devez, en particulier, désinstaller tout scanner automatique (lors de l'accès) ou résident en mémoire, tel que Scanshield McAfee, avant d'installer WinGuard NT.

Installation à partir d'un CD-ROM

Installation rapide

Conseil

Une mise à jour incrémetielle du logiciel vous permettra d'utiliser la méthode d'installation rapide et de mettre à jour votre Toolkit. Pour obtenir des instructions sur l'installation complète du Toolkit, voir la section "Options d'installation avancées" à la page 39.

1. Démarrez votre ordinateur et lancez Windows NT en tapant un mot de passe défini dans le groupe des administrateurs. Insérez le CD d'installation du Toolkit dans le lecteur de CD-ROM.

2. Un écran de démarrage du CD du Toolkit apparaît sous la version 4 de Windows NT.

Utilisateurs de la version 3.51 de Windows NT :
Après avoir inséré le CD du Toolkit dans le lecteur de CD-ROM, sélectionnez **Fichier**, puis **Exécuter** à partir du menu.

Dans la zone d'entrée qui apparaît, tapez la lettre correspondant au lecteur de CD-ROM, suivie de deux points. Tapez ensuite :

```
\SETUP
```

et cliquez sur **OK**. Par exemple, tapez :

```
D:\SETUP
```

L'écran de démarrage du CD du Toolkit apparaît alors.

3. Dans la boîte de dialogue qui apparaît, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

4. Dans la boîte de dialogue suivante, vous êtes invité à confirmer l'installation de Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Aller**.

5. Vous êtes également invité à confirmer le chemin d'accès de l'installation. Tapez un autre chemin d'accès si vous le désirez et cliquez sur **Continuer**. L'installation démarre.

   Vous pouvez annuler l'installation à tout moment en appuyant sur **Annuler**. Si vous décidez par la suite de l'installer à nouveau, supprimez tout fichier du répertoire du Toolkit créé lors de la première installation.

6. Des options vous invitent à exécuter le Scheduler de Dr. Solomon's. Le Scheduler vous permet de définir des événements à exécuter à des heures prédéfinies. Ces événements peuvent consister en des recherches de virus, des vérifications de fichiers ou l'exécution de n'importe quelle application et peuvent se produire une seule fois ou à intervalles réguliers.

   Choisissez **Oui** pour confirmer l'activation du Scheduler. Si vous choisissez **Non**, vous pourrez tout de même activer le Scheduler ultérieurement. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir la section "Exécution du Scheduler" à la page 134.

7. Des options vous invitent à exécuter WinGuard NT.
   WinGuard NT fonctionne constamment en arrière plan. Il vérifie que les fichiers ne sont pas infectés avant d'en autoriser l'accès ; voir la section "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71 pour plus de détails. Il est fortement recommandé de sélectionner l'option **Oui**.

8. Une invite vous demande si vous souhaitez visualiser les modifications les plus récentes apportée à Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Oui** pour pouvoir consulter le fichier Readme. Si vous cliquez sur **Non**, vous poursuivez sans consulter le fichier ReadMe. Il est recommandé de consulter le fichier ReadMe, car il vous informe des nouvelles fonctions et des modifications apportées au logiciel.

9. FindVirus est exécuté automatiquement afin de rechercher tout virus situé sur votre disque dur. Pour plus d'informations sur FindVirus, voir la section "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

Attention

Si FindVirus détecte un virus sur votre ordinateur, ne paniquez pas ! Consultez le chapitre 6 "Désinfection", pour obtenir des informations sur la procédure à suivre.

Vous serez sans doute invité à réinitialiser votre ordinateur à ce moment.

L'installation est terminée et les virus situés sur votre ordinateur ont été détectés. Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Options d'installation avancées

Conseil

La méthode d'installation avancée permet d'installer une version intégrale du Toolkit. Une mise à jour incrémentielle vous permettra d'utiliser la méthode d'installation rapide pour mettre à jour votre Toolkit.

1. Démarrez votre ordinateur et entrez votre mot de passe pour Windows NT en utilisant un nom d'administrateur. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Un écran de démarrage du CD du Toolkit apparaît si la version 4 de Windows NT fonctionne sur votre ordinateur.

Utilisateurs de la version 3.51 de Windows NT :
Après avoir inséré le CD d'installation du Toolkit dans le lecteur de CD-ROM, sélectionnez **Fichier**, puis **Exécuter** à partir du menu.

Dans la zone d'entrée qui apparaît, tapez la lettre correspondant au lecteur de CD-ROM, suivie de deux points. Tapez ensuite :

```
\SETUP
```

et cliquez sur **OK**. Par exemple, tapez :

```
D:\SETUP
```

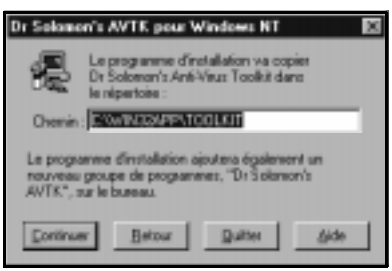
Un écran de démarrage du CD d'installation du Toolkit apparaît.

3. Dans la boîte de dialogue suivante qui apparaît, sélectionnez **Options d'installation avancées** et cliquez sur **Suivant**.

4. Dans la boîte de dialogue suivante, sélectionnez **Installer Dr Solomon's Anti-Virus Toolkit** et cliquez sur **Suivant**.

5. Dans la boîte de dialogue qui suit, on vous demande de confirmer l'installation de Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Aller**.

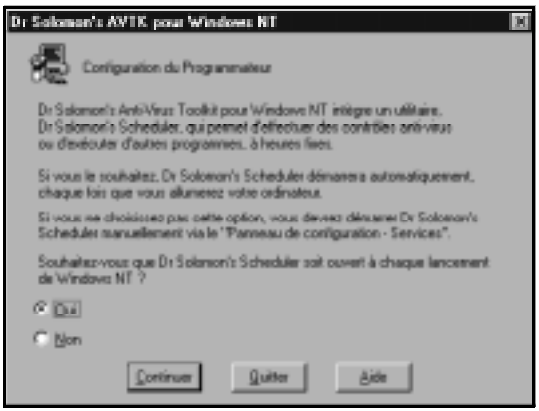
6. Vous êtes invité à confirmer le chemin d'accès de l'installation :



7. Tapez un autre chemin d'accès si vous le souhaitez et cliquez sur **Continuer**. Le processus d'installation commence.

   Vous pouvez annuler l'installation à tout moment en cliquant sur **Annuler**. Si vous souhaitez l'installer à nouveau, supprimez tous les fichiers du répertoire Toolkit créés lors de la première installation.

8. Des options vous invitent à exécuter Dr. Solomon's Scheduler.



Le Scheduler vous permet de définir des événements à des heures prédéfinies. Les événements peuvent consister en des recherches de virus, des vérifications de fichiers ou l'exécution de n'importe quelle application et peuvent se produire une seule fois ou à intervalles réguliers.

Choisissez **Oui** pour confirmer l'activation de Scheduler. Si vous choisissez **Non**, vous pouvez tout de même activer le Scheduler ultérieurement. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir la section "Exécution du Scheduler" à la page 134.

9. Des options vous invitent à exécuter WinGuard NT.

WinGuard NT fonctionne constamment à l'arrière-plan. Il vérifie si les fichiers sont infectés avant d'autoriser leur accès ; voir la section "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71

pour plus de détails. Il est fortement recommandé de sélectionner l'option **Oui**.

10. Une invite vous demande si vous souhaitez consulter les modifications les plus récentes apportées à Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Oui** pour consulter le fichier readme. Si vous cliquez sur **Non**, vous poursuivez sans consulter le fichier ReadMe. Il est recommandé de consulter de fichier ReadMe, car il vous informe des nouvelles fonctions et des modifications apportées au logiciel.

11. FindVirus fonctionne automariquement pour rechercher les virus situés sur votre disque dur. Pour plus d'informations sur FindVirus, voir la section "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

Attention

Si FindVirus détecte un virus sur votre ordinateur, ne paniquez pas ! Voir le chapitre 6, "Désinfection", pour obtenir des informations sur la procédure à suivre.

Vous pouvez être invité à réinitialiser votre ordinateur à ce moment.

L'installation est désormais terminée et une recherche de virus a été effectuée sur votre ordinateur. Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Installation à partir de disquettes

1. Démarrez votre ordinateur normalement. Connectez-vous avec un nom d'utilisateur de la liste des administrateurs.

2. Insérez la première disquette d'installation du Dr Solomon's Anti-Virus Toolkit (étiquetée Windows NT) dans le lecteur de disquettes.

3. Sélectionnez **Exécuter** à partir du menu **Fichier** du Gestionnaire de programmes ou du menu **Démarrer**.

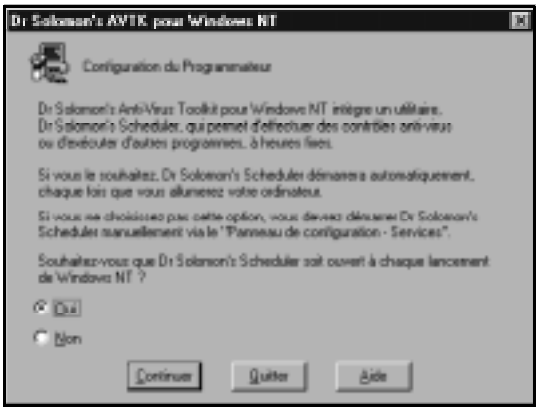
4. A l'invite, tapez `A:\SETUP` et appuyez sur la touche <Entrée>. Suivez les instructions à l'écran.

5. Vous êtes invité à confirmer le chemin d'accès de l'installation :

6. Tapez un autre chemin d'accès si vous le souhaitez et cliquez sur **Continuer**. Le processus d'installation commence.

7. Suivez les messages vous invitant à insérer les disquettes suivantes. Vous pouvez annuler l'installation à tout moment en cliquant sur **Annuler**. Si vous souhaitez une nouvelle installation, supprimez tout fichier se trouvant dans le répertoire du Toolkit, créé lors de la première installation.

8. Des options vous invitent à exécuter Dr. Solomon's Scheduler.



Le Scheduler vous permet de définir des événements pour le Toolkit qui peuvent être exécutés à des heures prédéterminées. Les événements peuvent consister en des recherches de virus, des vérifications de fichiers ou l'exécution de n'importe quelle application et peuvent se produire une seule fois ou à intervalles réguliers.

Choisissez **Oui** pour confirmer l'activation du Scheduler. Si vous choisissez **No**n, vous pouvez tout de même activer le Scheduler ultérieurement. Pour savoir comment démarrer le Scheduler après l'installation du Toolkit, voir la section "Exécution du Scheduler" à la page 134.

9. Des options vous invitent à exécuter WinGuard NT.

. WinGuard NT fonctionne constamment à l'arrière-plan. Il vérifie les fichiers infectés avant d'en autoriser l'accès ; voir la section "WinGuard pour Windows 3.x, Windows 95 et Windows NT" à la page 71 pour plus de détails. Il est fortement recommandé de sélectionner l'option **Oui**.

10. Une invite vous demande si vous souhaitez visualiser les modifications les plus récentes relatives à Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Oui** pour consulter le fichier readme. Si vous cliquez sur **Non**, vous poursuivez sans consulter le fichier ReadMe. Il est recommandé de consulter le fichier ReadMe, car il contient des informations sur les nouvelles fonctions et les modifications apportées au logiciel.

11. FindVirus fonctionne automatiquement pour rechercher tout virus situé sur votre disque dur. Pour plus d'informations sur FindVirus, voir la section "FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 69.

Attention

Si FindVirus détecte un virus sur votre ordinateur, ne paniquez pas ! Voir le chapitre 6, "Désinfection", Pour obtenir des informations sur la procédure à suivre.

Vous serez sans doute invité à réinitialiser à ce moment.

L'installation est désormais terminée et une recherche de virus a été effectuée sur votre ordinateur. Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir "Si vous avez besoin d'aide" à la page xiv.

Désinstallation de votre Toolkit (version 4 de Windows NT)

1. A partir du menu **Démarrer**, sélectionnez **Paramètres** puis **Panneau de configuration**.
2. Cliquez sur **Ajouter/Supprimer des programmes** à partir du Panneau de configuration.
3. Sélectionnez **Dr Solomon's Anti-Virus Toolkit** à partir de la liste.
4. Cliquez sur **Ajouter/Supprimer**.
5. A l'invite, confirmez la suppression du programme.
6. Répondez à l'invite pour déplacer ou supprimer tout fichier ayant été ajouté au répertoire du Toolkit depuis l'installation (tels que les fichiers rapport).

Désinstallation de votre Toolkit (version 3.51 Windows NT)

1. A partir du groupe de programmes Dr Solomon's AVTK, sélectionnez l'élément **Uninstaller**.
2. A l'invite, confirmez la suppression du programme.
3. Répondez à l'invite pour déplacer ou supprimer tout fichier ayant été ajouté au répertoire du Toolkit lors de l'installation (tels que les fichiers rapport).

1.6 OS/2

Conditions requises pour le système

L'Anti-virus Toolkit pour OS/2 fonctionne sur n'importe quel ordinateur fonctionnant sous la version 2 de OS/2 ou une version ultérieure.

Environ 2.5 Mo d'espace disque sont requis.

Si vous souhaitez installer le Toolkit sur plusieurs ordinateurs, renseignez-vous sur les licences de site auprès de Dr Solomon's Software ou du distributeur le plus proche.

Première installation de votre Toolkit

Installation à partir d'un CD-ROM

1. Démarrez votre ordinateur. Une fois que le bureau du Gestionnaire d'amorçage apparaît, insérez votre CD-ROM dans le lecteur de CD-ROM.

2. Ouvrez une session de commandes OS/2.

   Tapez la lettre correspondant au lecteur de CD-ROM, suivie de deux points, puis appuyez sur la touche Retour. Par exemple, tapez :

   `D:` <Entrée>

   Puis :

   `CD <`*`LANGUE`*`>\PRODUCTS\OS2\AVTK` <Entrée>

   Par exemple, si vous installez la version en anglais du Toolkit pour OS/2, vous devez taper :

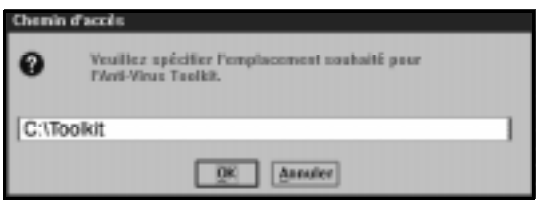
   `CD ENGLISH\PRODUCTS\OS2\AVTK` <Entrée>

Remarquez que le nom de la langue utilisée doit apparaître dans la langue elle-même. Par exemple, si vous travaillez en anglais mais que vous souhaitez installer une version en français du Toolkit pour OS/2, le nom du répertoire par lequel vous devez accéder est FRANÇAIS et non pas FRENCH.

Au retour de l'invite, tapez :

SETUP <Entrée>

3. Une boîte de dialogue vous indique le chemin d'accès d'installation du Toolkit. Tapez un autre chemin d'accès si vous le souhaitez. Cliquez sur **OK**.



Si vous le souhaitez, vous pouvez interrompre l'installation en cliquant sur **Pause** et la poursuivre en sélectionnant **OK**. Vous pouvez annuler l'installation à tout moment en cliquant sur **Quitter**.

Si vous annulez l'installation et que vous souhaitez installer le Toolkit ultérieurement, vous devez tout d'abord supprimer tous les fichiers déjà installés. Pour savoir comment supprimer un Toolkit partiellement installé, voir la section "Désinstallation de votre Toolkit" à la page 50.

Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Installation à partir de disquettes

1. Démarrez votre ordinateur. Une fois que le Gestionnaire d'amorçage apparaît, insérez la première disquette d'installation de Dr Solomon's Anti-Virus Toolkit (étiquetée OS/2) dans le lecteur approprié.

2. Ouvrez une session de commandes de OS/2.

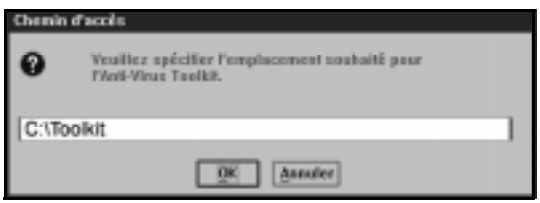
   Tapez la lettre correspondant au lecteur de disquettes suivie de deux points et appuyez sur la touche Retour. Tapez par exemple :

   A: <Entrée>

   Au retour de l'invite, tapez :

   SETUP <Entrée>

3. Une boîte de dialogue vous indique le chemin d'accès de l'installation du Toolkit. Vous pouvez taper un autre chemin d'accès si vous le souhaitez. Cliquez sur **OK**.



   Si vous le souhaitez, vous pouvez interrompre l'installation en cliquant sur **Pause** et poursuivre l'installation en sélectionnant **OK**. Vous pouvez annuler l'installation à tout moment en cliquant sur **Quitter**.

   Si vous annulez l'installation et que vous souhaitez installer le Toolkit ultérieurement, vous devez tout d'abord supprimer tous les fichiers déjà installés. Pour savoir comment supprimer un Toolkit partiellement installé, voir la section "Désinstallation de votre Toolkit" à la page 50.

   Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Désinstallation de votre Toolkit

Pour désinstaller le Toolkit :

1. Ouvrez une session de commande de OS/2.
2. Changez le lecteur et/ou le répertoire contenant le répertoire du Toolkit.
3. Au retour de l'invite, tapez :

   `DEL TOOLKIT` <Entrée>

   Vous êtes invité à confirmer la suppression du répertoire du Toolkit. Tapez :

   `Y` <Entrée>

4. Au retour de l'invite, tapez :

   `RD TOOLKIT` <Entrée>

5. Revenez au bureau. Cliquez avec le bouton droit de la souris sur l'icône du Toolkit et sélectionnez **Effacer** à partir du menu qui apparaît. Dans les boîtes de dialogue qui suivent, confirmez la suppression de l'icône du Toolkit de votre bureau.

1.7 DOS

Conditions requises pour le système

Dr Solomon's Anti-Virus Toolkit fonctionne sur tout ordinateur IBM ou compatible. Vous devez disposer de :

- la version 3.3 de DOS ou ultérieure. Pour connaître la version de DOS que vous utilisez, tapez :

  `VER` <Entrée>

  à partir de l'invite DOS.

Pour l'installer, vous devez disposer de :

- 2,5 Mo d'espace disque pour le Toolkit pour DOS.

VirusGuard, le scanner résidant dans DOS, fonctionne plus rapidement si votre système possède l'un des éléments suivants :

- une mémoire étendue,
- une mémoire d'expansion,
- une unité de mémoire vive.

Si vous souhaitez faire fonctionner le Toolkit en réseau ou sur plusieurs ordinateurs en même temps, renseignez-vous sur les licences de site auprès de Dr Solomon's ou du distributeur le plus proche.

Première installation de votre Toolkit

Installation à partir d'un CD-ROM

1. Démarrez votre ordinateur et assurez-vous que vous vous trouvez à l'invite DOS. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

   Tapez la lettre correspondant au lecteur de CD-ROM suivie de deux points et appuyez sur la touche <Entrée>. Par exemple, tapez :

   `D:` <Entrée>

Tapez maintenant :

`CD <LANGUAGE>\PRODUCTS\DOS\AVTK` <Entrée>

Par exemple, si vous installiez la version en anglais du Toolkit pour DOS, vous taperiez :

`CD ENGLISH\PRODUCTS\DOS\AVTK` <Entrée>

Remarquez que le nom de la langue doit apparaître sous la forme dans laquelle il apparaît dans sa propre langue. Par exemple, si vous travaillez en anglais et que vous souhaitez installer une version française du Toolkit pour DOS, le nom du répertoire auquel vous devez accéder est FRANÇAIS et non pas FRENCH.

Au retour de l'invite, tapez :

`INSTALL` <Entrée>

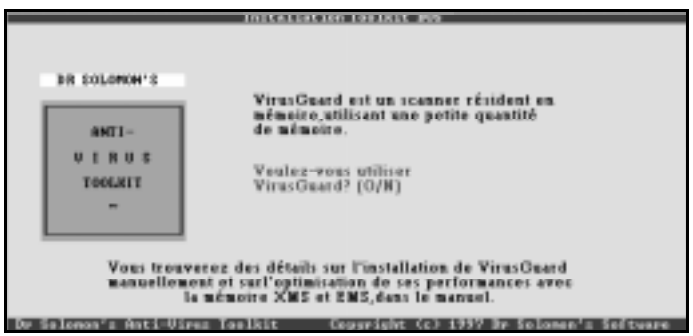
2. Dans le premier écran qui apparaît, vous êtes invité à sélectionner le lecteur sur lequel vous souhaitez installer le Toolkit. Appuyez sur les flèches droite et gauche pour sélectionner un lecteur et appuyez sur la touche <Entrée> pour confirmer la sélection. Cet écran vous indique le total de l'espace disque disponible, le total de l'espace disque utilisé par le Toolkit, ainsi que le total de l'espace restant après l'installation du Toolkit.

Si vous souhaitez annuler l'installation, appuyez sur la touche <Echap>.

3. L'écran suivant vous invite à confirmer dans quel répertoire vous souhaitez installer le Toolkit. Vous pouvez taper un autre répertoire si vous le souhaitez. Appuyez sur la touche <Entrée> pour continuer l'installation.

Si vous souhaitez annuler l'installation, appuyez sur la touche <Echap>.

4. Un écran apparaît vous indiquant l'état de l'installation. L'écran suivant vous demande si vous souhaitez activer VirusGuard. Tapez **O** pour activer VirusGuard.



Conseil

Il est fortement recommandé d'activer VirusGuard. Si, pour une raison ou pour une autre, vous choisissez de ne pas le faire, vous pouvez tout de même l'activer ultérieurement.

Si vous choisissez d'installer VirusGuard, un écran apparaît vous invitant à confirmer que le programme peut modifier les fichiers AUTOEXEC.BAT et CONFIG.SYS. Si des modifications sont effectuées, des copies de sauvegarde de ces fichiers sont placées dans le répertoire racine du lecteur contenant ces fichiers. Tapez **O** pour continuer.

5. Le prochain écran vous invite à sélectionner les paramètres de sécurité pour VirusGuard. Sélectionnez les paramètres à l'aide des flèches haut et bas, puis appuyez sur la touche <Entrée> pour confirmer le paramètre choisi.

6. Un écran récapitulatif apparaît. Dans l'écran qui suit, le programme d'installation vous indique le nom de votre fichier de sauvegarde AUTOEXEC.BAT.

7. L'écran final confirme que l'installation est terminée et que FindVirus va effectuer une recherche de virus sur votre (vos) disque(s) dur(s).

   Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Conseil Il est recommandé d'effectuer une autre recherche complète de virus, une fois l'installation terminée.

Installation à partir de disquettes

1. Démarrez votre ordinateur et vérifiez que vous vous trouvez sur une invite DOS.

2. Insérez la première disquette d'installation de Dr Solomon's Anti-Virus Toolkit (étiquetée DOS) dans le lecteur de disquettes.

3. Tapez la lettre correspondant au lecteur de disquettes, suivie de deux points et appuyez sur la touche <Entrée>. Tapez par exemple :

   `A:` <Entrée>

4. A l'invite `A:`, tapez `INSTALL` et appuyez sur la touche <Entrée>.

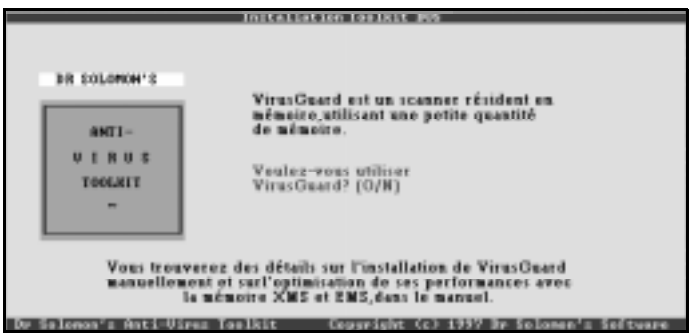
5. Dans le premier écran qui apparaît, vous êtes invité à sélectionner le lecteur sur lequel vous souhaitez installer le Toolkit. Sélectionnez un lecteur à l'aide des flèches droite et gauche et appuyez sur la touche <Entrée> pour confirmer votre sélection. L'écran vous indique également le total de l'espace disque disponible, le total de l'espace disque utilisé par le Toolkit et le total de l'espace disque dont vous disposerez après l'installation du Toolkit.

   Si vous souhaitez annuler l'installation, appuyez sur la touche <Echap>.

6. L'écran qui suit vous demande de confirmer dans quel répertoire vous souhaitez installer le Toolkit. Tapez le nom d'un autre répertoire si vous le souhaitez. Appuyez sur la touche <Entrée> pour poursuivre l'installation.

Si vous souhaitez annuler l'installation, appuyez sur la touche <Echap>.

7. Un écran apparaît vous indiquant l'état de l'installation. L'écran suivant vous invite à activer VirusGuard. Tapez **O** pour activer VirusGuard.



Conseil

Il est fortement recommandé d'activer VirusGuard. Si, pour une raison quelconque, vous choisissez de ne pas le faire, vous pouvez tout de même l'activer ultérieurement.

Si vous choisissez d'installer VirusGuard, un écran apparaît vous demandant confirmation des modifications apportées aux fichiers AUTOEXEC.BAT et CONFIG.SYS. Si des modifications sont apportées,

des copies de sauvegarde de ces fichiers sont placées dans le répertoire racine du lecteur contenant ces fichiers. Tapez **0** pour poursuivre.

8. L'écran qui suit vous invite à sélectionner votre paramètre de sécurité pour VirusGuard. Sélectionnez un paramètre à l'aide des flèches haut et bas et appuyez sur la touche <Entrée> pour confirmer la sélection du paramètre.

9. Un écran récapitulatif apparaît. Dans l'écran suivant, le programme vous indique le nom du fichier de sauvegarde de AUTOEXEC.BAT.

10. L'écran final confirme que l'installation est terminée et que FindVirus va effectuer une recherche de virus sur votre (vos) disque(s) dur(s).

    Si vous rencontrez des problèmes lors de l'installation du Toolkit, assurez-vous d'avoir suivi la procédure décrite dans ce manuel. Si vous ne pouvez pas résoudre le problème, contactez le support technique de Dr Solomon's. Pour savoir comment contacter Dr Solomon's Software, voir la section "Si vous avez besoin d'aide" à la page xiv.

Conseil Il est recommandé d'effectuer une autre recherche complète de virus, une fois l'installation terminée.

Désinstallation de votre Toolkit

1. Basculez vers le lecteur et/ou le répertoire dans lequel se trouve le Toolkit.

2. Supprimez tous les fichiers du Toolkit situés dans le répertoire du Toolkit.

Si, par exemple, vous avez installé le Toolkit dans le répertoire qui vous est proposé par défaut, C:\TOOLKIT, vous devez supprimer les fichiers du Toolkit comme il vous est décrit dans les instructions suivantes. A partir de l'invite C:\ , tapez :

```
CD TOOLKIT <Entrée>
```

pour modifier les fichiers dans le répertoire du Toolkit. A l'invite C:\Toolkit, tapez :

```
DEL *.* <Entrée>
```

Vous êtes invité à confirmer la suppression des fichiers du Toolkit. Tapez :

```
Y <Entrée>
```

3. Supprimez le répertoire du Toolkit en tapant :

   ```
   DEL TOOLKIT <Entrée>
   ```

   Vous êtes invité à confirmer la suppression le répertoire du Toolkit. Tapez :

   ```
   Y <Entrée>
   ```

4. Au retour de l'invite, tapez :

   ```
   RD TOOLKIT <Entrée>
   ```

5. Ouvrez le fichier `AUTOEXEC.BAT` et supprimez la ligne contenant la commande VirusGuard. Le fichier de VirusGuard est intitulé GUARD.COM. Si vous avez installé VirusGuard sous C:\TOOLKIT, la ligne que vous devez supprimer est :

   ```
   C:\TOOLKIT\GUARD.COM
   ```

6. Réinitialisez votre ordinateur.

2. Mise à jour de votre Toolkit

Le Toolkit est mis à jour tous les mois afin de pouvoir traiter les nouveaux virus, et les versions mises à niveau sont disponibles sur une base mensuelle ou trimestrielle. Il est recommandé de conserver une souscription au service de mise à niveau pour vous assurer une protection complète des virus. Voir la section “Enregistrement et mises à jour” à la page xii.

2.1 Windows 3.x

Mise à jour à partir du CD-ROM

Installation rapide

Conseil

Un logiciel de mise à jour incrémentielle vous permettant d’utiliser la méthode d’installation rapide pour mettre à jour votre Toolkit va bientôt être mis sur le marché. La mise à jour de votre Toolkit vous permettra de maintenir sa configuration à partir de la version précédente. Pour plus de détails sur la manière d’effectuer une installation complète du Toolkit, voir la section “Options d’installation avancées” à la page 39.

1. Démarrez votre ordinateur et chargez Windows 3.x. Lorsque le bureau de Windows 3.x apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Sélectionnez le menu **Fichier**, puis la commande **Exécuter**.

3. Dans la boîte d’entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points. Tapez ensuite :

   ```
   \INSTALLATION
   ```

   et cliquez sur **OK**. Par exemple, tapez :

   ```
   D:\INSTALLATION
   ```

4. L'écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

5. Dans la boîte de dialogue suivante, il vous faut confirmer que vous souhaitez mettre à jour Dr Solomon's Anti-virus Toolkit pour Windows 3.x. Cliquez sur **Aller**.

6. Suivez les instructions qui s'affichent à l'écran.

Mise à jour à partir d'une disquette

1. Démarrez votre ordinateur et chargez Windows 3.x. Lorsque le bureau de Windows 3.x apparaît, insérez la disquette 1 (étiquetée Windows 3.x) d'installation du Dr Solomon's Anti-Virus Toolkit dans votre lecteur de disquettes.

2. Dans le Gestionnaire de fichiers, sélectionnez le menu **Fichier** puis la commande **Exécuter**.

3. Dans la zone Ouvrir, tapez `A:\INSTALLATION` et cliquez sur **OK**.

4. Suivez les instructions qui s'affichent à l'écran.

2.2 Windows 95

Mise à jour à partir d'un CD-ROM

Installation rapide

Conseil

Un logiciel de mise à jour incrémentielle vous permettant d'utiliser la méthode d'installation rapide pour mettre à jour votre Toolkit va bientôt être mis sur le marché. La mise à jour de votre Toolkit vous permettra de maintenir sa configuration à partir de la version précédente. Pour plus de détails sur la manière d'effectuer une installation complète du Toolkit, voir la section "Options d'installation avancées" à la page 23.

1. Démarrez votre ordinateur. Lorsque le bureau de Windows 95 apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L'écran de démarrage du CD apparaît. Dans la boîte de dialogue suivante, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

3. Dans la boîte de dialogue suivante, il vous faut confirmer que vous souhaitez mettre à jour Dr Solomon's Anti-Virus Toolkit pour Windows 95. Cliquez sur **Aller**.

4. Suivez les instructions qui s'affichent à l'écran.

Mise à jour à partir d'une disquette

1. Démarrez votre ordinateur et chargez Windows 95. Lorsque le bureau de Windows 95 apparaît, insérez la disquette 1 (étiquetée Windows 95) d'installation du Dr Solomon's Anti-Virus Toolkit dans votre lecteur de disquettes.

2. Cliquez sur **Démarrer**, puis sur **Exécuter**.

3. Dans la zone "Ouvrir", tapez `A:\INSTALLATION` et cliquez sur **OK**.

4. Suivez les instructions qui s'affichent à l'écran.

2.3 Windows NT

Mise à jour à partir d'un CD-ROM

Installation rapide

Conseil

Un logiciel de mise à jour incrémentielle vous permettant d'utiliser la méthode d'installation rapide pour mettre à jour votre Toolkit va bientôt être mis sur le marché. Pour les instructions sur la manière d'effectuer une installation complète du Toolkit, voir la section "Options d'installation avancées" à la page 23.

1. Démarrez votre ordinateur et connectez-vous à votre bureau de Windows NT avec un nom d'utilisateur faisant partie de la liste des administrateurs. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L'écran de démarrage du CD du Toolkit apparaît si vous êtes sous Windows NT version 4.

Pour les utilisateurs de Windows NT version 3.51 :
Après avoir inséré le CD du Toolkit dans le lecteur de CD-ROM, sélectionnez le menu **Fichier** puis la commande **Exécuter**.

Dans la boîte d'entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points. Tapez ensuite :

```
\INSTALLATION
```

et cliquez sur **OK**. Par exemple, tapez :

```
D:\INSTALLATION
```

Vous allez voir apparaître l'écran de démarrage du CD du Toolkit.

3. Dans la boîte de dialogue qui apparaît, sélectionnez la méthode d'installation rapide et cliquez sur **Suivant**.

4. Dans la boîte de dialogue suivante, il vous faut confirmer que vous souhaitez mettre à jour Dr Solomon's Anti-Virus Toolkit pour Windows NT. Cliquez sur **Aller**.

5. Suivez les instructions qui s'affichent à l'écran.

Mise à jour à partir d'une disquette

1. Démarrez votre ordinateur et connectez-vous à votre bureau de Windows NT avec un nom d'utilisateur faisant partie de la liste des administrateurs. Insérez la disquette 1 (libellée Windows NT) d'installation du Dr Solomon's Anti-Virus Toolkit dans votre lecteur de disquettes.

2. Sélectionnez la commande **Exécuter** dans le menu **Fichier** du Gestionnaire de programmes ou à partir du menu **Démarrer**.

3. Lorsque l'invite apparaît, tapez `A:\INSTALLATION` et appuyez sur la touche <Entrée>.

4. Suivez les instructions qui s'affichent à l'écran.

2.4 OS/2

Mise à jour à partir d'un CD-ROM

1. Démarrez votre ordinateur. Une fois que le bureau du gestionnaire d'amorçage apparaît, insérez votre CD-ROM dans le lecteur de CD-ROM.

2. Ouvrez une session de commandes OS/2.

   Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `D:` <Entrée>

   Tapez ensuite :

   `CD <`*`LANGUE`*`>\PRODUCTS\OS2\AVTK` <Entrée>

   Par exemple, si vous étiez en train de mettre à jour la version anglaise du Toolkit pour OS/2, vous taperiez :

   `CD ENGLISH\PRODUCTS\OS2\AVTK` <Entrée>

   Veuillez noter que le nom de la langue doit apparaître sa propre langue. Par exemple, si vous travaillez en anglais mais que vous souhaitez mettre à jour la version française du Toolkit pour OS/2, le nom du répertoire auquel vous avez besoin d'accéder est FRANÇAIS, et non pas FRENCH.

   Au retour de l'invite, tapez :

   `INSTALLATION` <Entrée>

3. Suivez les instructions qui s'affichent à l'écran.

Mise à jour à partir d'une disquette

1. Démarrez votre ordinateur. Une fois que le bureau du gestionnaire d'amorçage apparaît, insérez la disquette 1 (étiquetée OS/2) d'installation du Dr Solomon's Anti-Virus Toolkit dans votre lecteur de disquettes.

2. Ouvrez une session de commandes OS/2.

   Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `A:` <Entrée>

   Au retour de l'invite, tapez :

   `INSTALLATION` <Entrée>

3. Suivez les instructions qui s'affichent à l'écran.

2.5 DOS

Mise à jour à partir d'un CD-ROM

1. Démarrez votre ordinateur et assurez-vous que vous recevez bien une invite DOS. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

   Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `D:` <Entrée>

   Tapez maintenant :

   `CD <`*`LANGUE`*`>\PRODUCTS\DOS\AVTK` <Entrée>

   Par exemple, si vous deviez mettre à jour la version anglaise du Toolkit pour DOS, vous taperiez :

   `CD ENGLISH\PRODUCTS\DOS\AVTK` <Entrée>

   Veuillez noter que le nom de la langue doit apparaître dans sa propre langue. Par exemple, si vous travaillez en anglais mais que vous souhaitez mettre à jour la version française du Toolkit pour DOS, le nom du répertoire auquel vous avez besoin d'accéder est FRANÇAIS, et non pas FRENCH.

   Au retour de l'invite, tapez :

   `INSTALL` <Entrée>

2. Suivez les instructions qui apparaissent à l'écran.

Mise à jour à partir d'une disquette

1. Démarrez votre ordinateur et assurez-vous que vous recevez bien une invite DOS. Insérez la disquette 1 (étiquetée DOS) d'installation du Dr Solomon's Anti-Virus Toolkit dans votre lecteur de disquettes.

2. Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `A:` <Entrée>

3. A l'invite `A:`, tapez `INSTALL` et appuyez sur la touche <Entrée>.

4. Suivez les instructions qui s'affichent à l'écran.

3. Balayage

3.1 Scanners sur demande

Dr Solomon's Toolkit fournit deux scanners sur demande, FindVirus et Viverify.

FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS

Dès qu'un nouveau virus est découvert, il est analysé pour en connaître ses caractéristiques. Lorsque celles-ci sont connues, elles sont programmées dans un outil de recherche qui peut alors identifier ce virus dans un ordinateur.

L'outil de recherche de virus de Dr Solomon's est le scanner "FindVirus". FindVirus est contamment mis à jour à l'aide d'informations sur les virus nouvellement découverts.

FindVirus peut également désinfecter des fichiers, des secteurs de boot et de partition. Lorsqu'un virus de secteur de boot ou de partition du disque dur est découvert, la contamination est signalée mais le balayage est interrompu. Ceci fournit une sécurité supplémentaire. Vous devez alors exécuter la fonction de désinfection puis effectuer un nouveau balayage du disque dur. Des fichiers image de secteur de boot peuvent également contenir des fichiers infectés.

Les paramètres par défaut des options de FindVirus sont définis afin d'être efficaces dans la plupart des situations. Les fichiers susceptibles d'être contaminés par virus sont vérifiés. Vous pouvez exécuter un balayage basé sur ces paramètres ou modifier les options afin d'optimiser le balayage selon vos besoins.

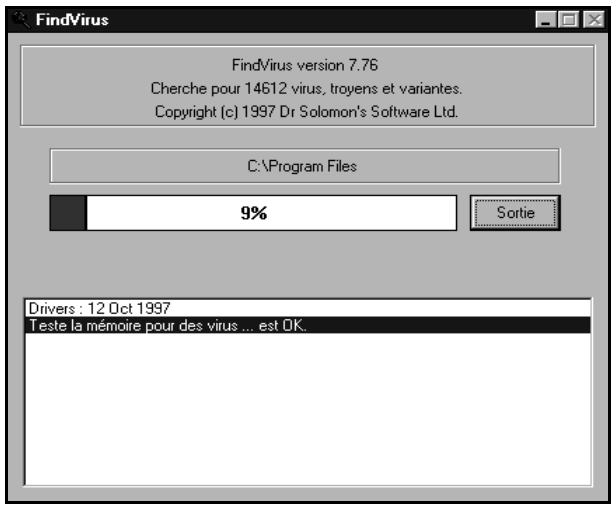
Recherche des virus par balayage

Afin de rechercher des virus en utilisant les paramètres d'option initiaux ou les paramètres définis grâce au menu "Balayer", utilisez l'écran principal :

1. Sélectionnez le(s) lecteur(s) que vous recherchez dans la zone "Lecteurs".

2. Cliquez sur le bouton **Trouver**.

3. Une boîte de dialogue apparaît indiquant en premier lieu la progression du balayage, puis les résultats.



   Vous pouvez interrompre la recherche à tout moment en cliquant sur le bouton **Exit**. Un rapport détaillé décrit tous les virus trouvés jusqu'au moment où la recherche a été interrompue. Si aucun virus n'a été découvert, la boîte de dialogue "Trouver virus" est affichée.

4. Lorsque la recherche est terminée, notez les résultats puis cliquez sur **Exit** pour retourner à la boîte de dialogue "Trouver virus".

Attention

Pour les utilisateurs de Windows NT : si votre nom d'utilisateur (nom de connexion) ne figure pas dans la liste des administrateurs, FindVirus ne peut pas balayer les secteurs de boot et de partition du disque. Dans ce cas, les messages "Impossible de lire le secteur de boot" et "Impossible de lire le secteur de partition" s'affichent. Si vous devez procéder à un balayage de ces secteurs, contactez l'administrateur du système.

Si une contamination par virus est signalée, utilisez l'option "Désinfecter" de FindVirus ; voir la section "Désinfection des lecteurs" à la page 145. Voir également la rubrique "Stratégie pour l'utilisation du Toolkit" dans l'aide du Toolkit.

Aide

Pour plus d'informations sur l'exécution de FindVirus à partir d'une commande en ligne, voir la rubrique "FindVirus" dans l'aide en ligne de Toolkit.

ViVerify pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS

ViVerify est le scanner avancé sur demande de Dr Solomon's. Pour plus d'informations sur ViVerify, voir "Balayage avancé avec ViVerify pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS" à la page 80.

3.2 Scanners Automatiques (activés au démarrage)

Les Toolkits Dr Solomon's pour Windows 3.x, Windows 95 et Windows NT disposent d'un scanner automatique (activé au démarrage) appelé WinGuard. VirusGuard est le scanner automatique (activé au démarrage) fonctionnant sous DOS.

WinGuard pour Windows 3.x, Windows 95 et Windows NT

WinGuard vous permet d'établir une surveillance en arrière plan permanente de recherche de virus .

WinGuard s'exécute automatiquement lors du démarrage de Windows. Lorsque vous effectuez une opération susceptible de propager un virus, WinGuard peut procéder à un balayage du fichier, du secteur de boot ou du secteur de partition concerné. Si un virus est détecté, l'opération est interrompue et vous êtes averti par un message d'alerte. Vous pouvez également opter pour une suppression automatique des virus.

Il existe des options permettant de modifier le fonctionnement de WinGuard. Les paramètres initiaux de ces options (les paramètres d'installation) ont été définis afin de fonctionner dans la plupart des situations.Vous pouvez toutefois modifier ces paramètres afin qu'ils correspondent à vos propres besoins.

Vous pouvez, par exemple, spécifier quelles actions vont déclencher le balayage et quels types de fichiers vont être balayés. Pour plus d'informations sur la modification de la configuration standard de WinGuard, voir la section “Balayage avancé avec WinGuard pour Windows 3.x et Windows 95” à la page 87“Balayage avancé avec WinGuard pour Windows NT” à la page 101.

Conseil Seuls les administrateurs peuvent modifier les paramètres d'options de WinGuard dans Windows NT.

Utilisation quotidienne de WinGuard

WinGuard s'exécute lors du démarrage de Windows. Afin de vous assurer que WinGuard est activé, une icône apparaît sur l'écran de Windows 3.x et Windows NT (version 3.51) ou sur la barre de menus de Windows 95 et Windows NT (version 4).

L'icône WinGuard n'apparaît pas si vous avez choisi de ne pas installer WinGuard lors de l'installation du Toolkit ou lorsque WinGuard est désactivé ; voir la section “Options de balayage” à la page 91.

WinGuard fonctionne automatiquement dès son activation. A part la présence de l'icône, rien n'indique le fonctionnement de WinGuard tant qu'un virus n'est pas découvert.

VirusGuard pour Windows 3.x, Windows 95 et DOS

VirusGuard est l'équivalent DOS de WinGuard. Si vous avez opté pour l'activation de VirusGuard lors de l'installation du Toolkit (voir chapitre 1), VirusGuard fournit alors une protection automatique sous DOS. WinGuard prend le relai lors du démarrage de Windows.

Sans la présence deVirusGuard, le système DOS risque d'être infecté.WinGuard détecterait un virus lors du démarrage suivant de Windows (et accèderait au fichier infecté dans le cas d'un virus de fichier). Cependant, le virus risque de se déclencher et de provoquer des dégâts avant le lancement de Windows.

Le logiciel Dr Solomon's vous recommande d'exécuter WinGuard et VirusGuard en permanence pour une protection maximale contre les virus si vous utilisez Windows 3.x ou Windows 95.

Conseil

VirusGuard ne peut prendre en charge des fichiers extra driver.

Démarrage de VirusGuard

Conseil

Si vous avez choisi de ne pas activer VirusGuard lors de l'intallation du Toolkit, vous pouvez l'activer par la suite en utilisant la / les commande(s) décrite(s) dans cette section et dans l'aide en ligne de Toolkit.

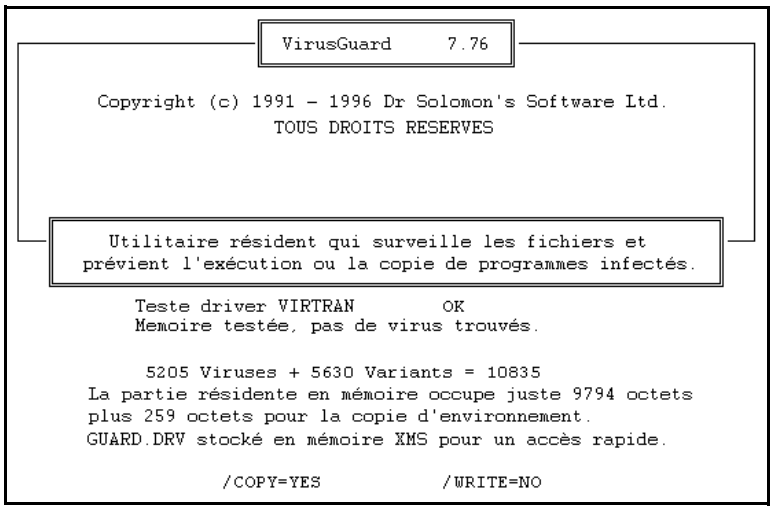
A l'invite DOS, tapez la commande de lancement de VirusGuard. Cette commande respecte la syntaxe suivante :

```
GUARD [/paramètres]...
```

Aide

Les détails concernant les commandes sont fournis dans "Paramètres de référence" dans la rubrique "VirusGuard" de l'aide en ligne du Toolkit.

Lors du démarrage de VirusGuard, l'écran suivant apparaît brièvement :



Conseil

Remarquez que lorsque VirusGuard est lancé, il ne peut être interrompu.

Si VirusGuard découvre un virus

Si VirusGuard découvre un virus:

- L'action en cours est interrompue.
- Une alarme sonore se déclenche.
- Un message d'alerte apparaît sur l'écran devant le programme que vous exécutez.

Appuyez sur la touche <CTRL> et supprimez l'infection immédiatement en utilisant FindVirus, à partir de l'interface utilisateur ou à partir de la disquette Magic Bullet disk (voir "Utilisation de Magic Bullet" à la page 1).

4. Balayage avancé

4.1 Balayage avancé avec FindVirus pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS

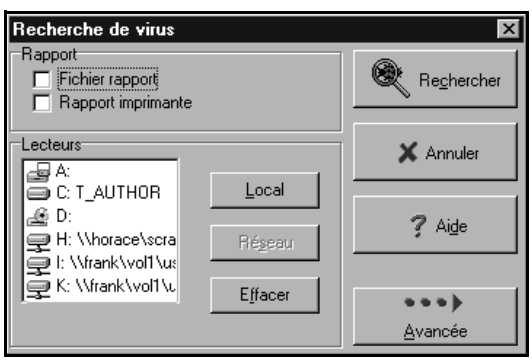
Conseil Veuillez noter que toutes les options décrites dans ce chapitre ne sont pas disponibles pour toutes les plateformes.

Vous pouvez commencer un balayage à la recherche de virus en utilisant le menu **Balayer**. Ce menu fournit des options permettant de modifier le mode de fonctionnement du balayage.

Balayages configurés par l'utilisateur

1. Si vous souhaitez choisir vos propres options de balayage, sélectionnez la commande **Rechercher les virus** dans le menu **Balayer**.

   La boîte de dialogue "Recherche de virus" apparaît.



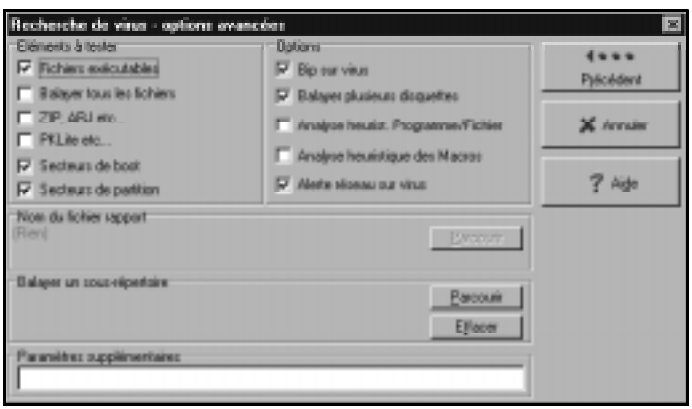
2. Sélectionnez les lecteurs à balayer dans la zone "Lecteurs".

3. Si vous avez des exigences de rapport spécifiques, sélectionnez l'option **Fichier rapport** ou **Rapport imprimante**.

Conseil Remarquez que les options de cette boîte de dialogue s'appliquent également aux balayages de désinfection lancés à l'aide de la commande **Désinfecter le lecteur** ou du bouton **Désinfecter**.

4. Si vous avez des exigences particulières sur la façon dont le balayage doit s'effectuer, cliquez sur **Avancé**.

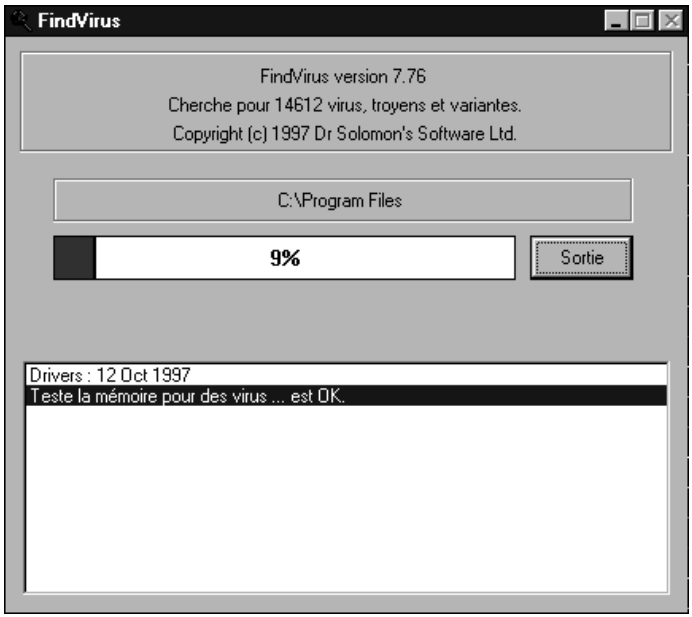
   La boîte de dialogue "Options avancées" apparaît.



   Après avoir défini les options, cliquez sur **Retour** pour revenir à la boîte de dialogue "Recherche de virus".

5. Cliquez sur **Rechercher**.

6. Une boîte de dialogue s'affiche, indiquant d'abord la progression du balayage, puis les résultats de la recherche.



   Vous pouvez interrompre la recherche à n'importe quel moment en cliquant sur **Quitter**. Le rapport affiche les détails relatifs aux virus identifiés pendant la recherche jusqu'au moment où celle-ci a été interrompue. Si aucun virus n'a été détecté, la boîte de dialogue "Recherche de virus" apparaît.

7. Une fois la recherche terminée, prenez connaissance des résultats, puis cliquez sur **Quitter** pour revenir à la boîte de dialogue "Recherche de virus".

Attention

Pour les utilisateurs de Windows NT : si votre nom d'utilisateur (nom de connexion) ne se trouve pas dans le groupe des administrateurs, FindVirus ne peut pas balayer les secteurs de partition et les secteurs de boot du disque dur. Les messages "Ne peut lire le secteur de boot" et "Ne peut lire le secteur de partition" apparaissent. Si vous désirez effectuer un balayage de ces secteurs, contactez l'administrateur du système.

Si un virus est détecté, supprimez-le en utilisant l'option **Désinfecter** de FindVirus. Reportez-vous également à la rubrique "Stratégies d'utilisation de Toolkit"dans l'aide en ligne du Toolkit.

4.2 Balayage avancé avec ViVerify pour Windows 3.x, Windows 95, Windows NT, OS/2 et DOS

Conseil

Veuillez noter que toutes les options décrites dans ce chapitre ne sont pas disponibles pour toutes les plateformes.

ViVerify

Un fichier exécutable reste généralement inchangé. Si des modifications y ont été apportées, il est possible qu'il soit infecté par un virus. En effectuant un balayage indiquant quels fichiers ont été modifiés, il est possible de déterminer les fichiers qui sont probablement infectés.

L'outil de Dr Solomon's servant à rechercher les fichiers modifiés est un scanner appelé ViVerify. ViVerify recherche également les modifications présentes dans les secteurs de boot et de partition.

Pour vérifier un fichier, ViVerify génère une nouvelle "empreinte" pour ce fichier et la compare à celle générée et enregistrée (ou calculée) au préalable. Si le fichier a été modifié, les empreintes ne correspondent plus.

Il n’est pas nécessaire de calculer les empreintes régulièrement, il suffit de le faire de temps en temps, par exemple lorsque vous installez Toolkit pour la première fois ou lorsque vous installez un nouveau logiciel. Une fois que vous avez généré les empreintes, vous pouvez “tester pour modifications” à intervalles réguliers.

Les fichiers contenant les empreintes enregistrées sont codés de sorte à être protégés des virus. Vous entrez ce code lors du calcul des empreintes.

Vous pouvez accéder au programme ViVerify à partir de l’interface utilisateur ou d’une ligne de commande.

Vous disposez d’options qui vous permettent de changer le mode d’opération de ViVerify. Vous pouvez par exemple changer les options suivantes :

- vérification des modifications ou calcul des empreintes,
- lecteurs à balayer.

Vous disposez d’options avancées qui vont seront utiles si vous souhaitez affiner la fonction de balayage de sorte qu’elle réponde à des besoins spécifiques. Les paramètres par défaut de ces options avancées s’appliquent à la plupart des situations.

Base de données de réparation

ViVerify dispose d’une option de “base de données de réparation”. La base de données de réparation est générée en même temps qu’un fichier d’empreintes et est associée à ce fichier. Elle contient une copie des parties du fichier qui semblent affectées par les dommages causés par le virus.

Dans le rapport généré à la fin du balayage de vérification des modifications, vous êtes invité à réparer les fichiers modifiés. Si vous sélectionnez cette option, les parties du fichier apparaissant dans la base de données de réparation sont recopiés dans le fichier, rétablissant ainsi son contenu d’origine.

Fichiers exclus

ViVerify vérifie uniquement les fichiers exécutables. Bien que la plupart des fichiers exécutables restent inchangés, certains peuvent être modifiés et se trouvent donc exclus de la vérification des modifications de ViVerify. Ces fichiers sont les suivants :

```
CONFIG.SYS
WPQUE.SYS
WPSYSD.SYS
BOOTCONF.SYS
TELIX.FON
```

Il est recommandé d'utiliser FindVirus pour vérifier ces fichiers régulièrement. ViVerify n'effectue pas de balayage dans la Corbeille.

Recherche des fichiers modifiés

A l'inverse des fichiers de données, la plupart des fichiers exécutables doivent rester inchangés. Si le système détecte des modifications dans un fichier exécutable, il est possible que ce dernier soit infecté par un virus.

Génération d'empreintes

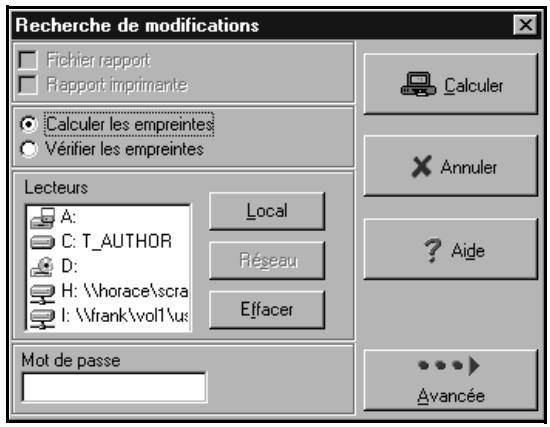
Avant de pouvoir vérifier les modifications survenues dans un fichier, vous devez générer des "empreintes". Une empreinte représente l'état d'un fichier à l'enregistrement. Un changement dans l'empreinte d'un fichier indique une modification dans le fichier.

Lorsque vous installez un nouveau programme logiciel, il est recommandé de régénérer toutes les empreintes de sorte à enregistrer celles contenues dans les nouveaux fichiers.

1. Dans le menu **Balayer**, sélectionnez **Test pour modif**. La boîte de dialogue "Test pour modifications" s'affiche.

2. Sélectionnez **Calculer empreintes**.

La boîte de dialogue ressemble alors à l'illustration ci-dessous :



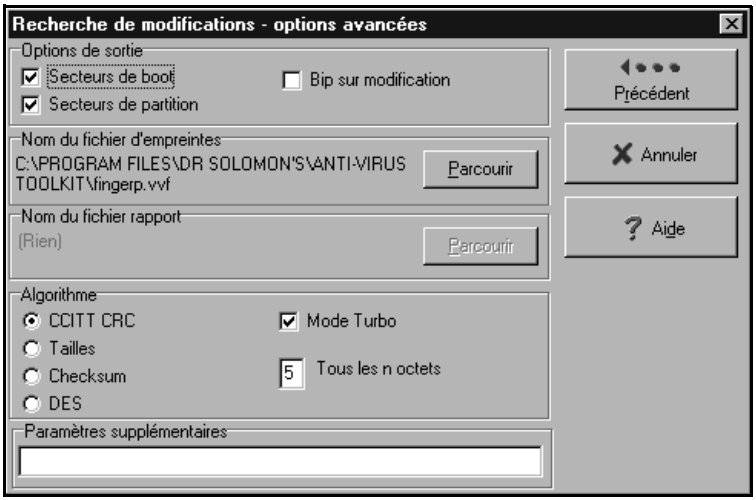
3. Sélectionnez les lecteurs sur lesquels vous souhaitez effectuer une vérification des modifications.

4. Dans la zone "Mot-clé", tapez une combinaison d'au moins 8 caractères alphanumériques. Ce mot-clé est utilisé pour coder le fichier d'empreintes afin de le protéger d'une éventuelle contamination par des virus (il ne s'agit pas d'un mot de passe).

5. Si vous n'avez aucune exigence particulière sur la façon dont les empreintes doivent être générées, vous pouvez alors générer les empreintes sur la base des paramètres actifs des options (les paramètres par défaut conviennent généralement) et passer directement à l'étape 8. Si vous avez des exigences spécifiques en ce qui concerne la fonction de recherche, passez à l'étape suivante.

6. Si vous avez des exigences particulières sur la façon dont les empreintes doivent être générées, cliquez sur **Avancé**.

La boîte de dialogue “Options avancées” apparaît.



Aide

Pour plus d’informations sur les options de cette boîte de dialogue, reportez-vous à la rubrique “Boîte de dialogue Test pour modifications - Options avancées” de l’aide en ligne du Toolkit.

Conseil

A l’aide de cette boîte de dialogue, vous pouvez créer plusieurs fichiers d’empreintes avec les noms de votre choix, de sorte que chaque fichier corresponde à un lecteur spécifique.

7. Après avoir défini les options, cliquez sur **Retour** pour revenir à la boîte de dialogue “Test pour modifications”.

8. Cliquez sur **Calculer** ou appuyez sur <Entrée>.

9. Il se peut que le message “Le fichier d’empreintes existe déjà. L’écraser ?“ s’affiche. Si vous ne souhaitez pas écraser le fichier d’empreintes, vous pouvez spécifier un autre fichier dans la boîte de dialogue “Options avancées” (voir étape 6).

10. Une boîte de dialogue indiquant la progression de la génération des empreintes apparaît, suivie du message “Empreintes créées”. Cliquez sur **Quitter** pour revenir à la boîte de dialogue “Test pour modifications”.

Vous pouvez désormais vérifier les modifications des fichiers. Seuls les fichiers possédant une empreinte sont vérifiés lorsque vous effectuez un test pour modifications.

Vérification de fichiers

Une fois que vous avez calculé les empreintes, vous pouvez les utiliser pour vérifier les modifications :

1. Dans la boîte de dialogue “Test pour modifications”, sélectionnez **Vérifier empreintes**.

2. Sélectionnez les lecteurs à vérifier.

3. Dans la zone “Mot-clé”, tapez le mot-clé utilisé lors de la génération des empreintes (voir étape 4 à la page 83).

4. Cliquez sur le bouton **Vérifier** ou appuyez sur <Entrée>.

5. Une boîte de dialogue indique la progression de la recherche. Vous pouvez cliquer sur **Annuler** à n’importe quel moment. Si tel est le cas, vous êtes ensuite invité à confirmer l’annulation, puis un message affichant les résultats de la recherche jusqu’au moment où elle a été interrompue apparaît.

6. Dès qu’un balayage est terminé, une boîte de dialogue affiche les résultats de la recherche. Cette boîte de dialogue classe les fichiers en trois catégories :

- “Fichiers qui ont été modifiés et qui sont réparables”,
- “Fichiers qui ont été modifiés mais qui ne sont pas réparables”,
- “Nouveaux fichiers” (fichiers détectés dont il n’existe aucune empreinte dans le fichier des empreintes).

7. Si ViVerify détecte des modifications sur un fichier, cela ne signifie pas forcément que ce dernier est infecté. Vérifiez le fichier à l’aide de FindVirus en activant l’option **Scanner heuristique**.

8. Si des fichiers sont modifiés, cliquez sur l'un d'entre eux. Le bouton **Mettre à jour** devient activé (il n'apparaît plus en "grisé") et, pour les fichiers réparables, le bouton **Réparer** devient également accessible.

9. Cliquez sur **Mettre à jour** pour inclure les empreintes récemment générées pour le fichier modifié dans le fichier d'empreintes (afin que le fichier ne soit pas signalé comme modifié à la prochaine vérification). Cliquez sur **Réparer** pour le fichier à réparer (voir la section "Base de données de réparation" à la page 81 pour plus de détails sur le mode de réparation des fichiers).

10. S'il y a des nouveaux fichiers, utilisez FindVirus pour les vérifier. Après vous être assuré que les fichiers ne comportent pas de virus, cliquez sur l'un d'entre eux. Le bouton **Mettre à jour** devient actif (il n'apparaît plus en "grisé"). Certains fichiers peuvent être signalés comme "Nouveaux" si vous avez sélectionné un lecteur différent de celui sélectionné lors de la génération des empreintes ou si les fichiers ont été copiés sur le lecteur après la génération des empreintes.

11. Cliquez sur **Mettre à jour** pour inclure les empreintes récemment générées pour le nouveau fichier dans le fichier des empreintes (pour que le fichier ne soit pas signalé comme nouveau à la prochaine vérification).

4.3 Balayage avancé avec VirusGuard pour Windows 3.x, Windows 95 et DOS

Test de VirusGuard

Les instructions contenues dans cette section décrivent la procédure à suivre pour tester VirusGuard en déclenchant une alerte VirusGuard. Vous pouvez déclencher cette alerte en créant un fichier qui s'apparente à un virus pour VirusGuard. Vous pouvez utiliser cette procédure pour tester le fonctionnement de VirusGuard et pour avoir une idée de ce qui se produit lors d'une alerte au virus. Cette procédure déclenche VirusGuard avec ses paramètres de sécurité standard.

Pour déclencher une alerte VirusGuard :

1. Eteignez l'ordinateur et redémarrez-le en mode DOS.
2. Tapez :

   `COPY CON TRYGUARD.COM` <Entrée>

   Puis :

   `ZQZXJVBVT` <Entrée>

   Remarquez que toutes ces commandes doivent apparaître en majuscules.

   Puis :

   `CTRL Z` <Entrée>

3. Copiez le fichier "TRYGUARD.COM" que vous avez créé vers n'importe quel autre fichier. VirusGuard doit déclencher une alerte (voir "Si VirusGuard découvre un virus" à la page 75).

Supprimez le fichier TRYGUARD.COM après le test pour éviter une éventuelle confusion.

4.4 Balayage avancé avec WinGuard pour Windows 3.x et Windows 95

Test de WinGuard

Il existe une procédure de déclenchement d'une alerte WinGuard. Vous pouvez utiliser cette procédure pour tester WinGuard et pour visualiser les événements qui se produisent lors d'une alerte au virus.

Pour déclencher une alerte WinGuard :

1. Ouvrez un nouveau fichier dans un éditeur de texte tel que Notepad.
2. Tapez "`ZQZXJVBVT`". Remarquez que ces caractères sont en majuscules.

3. Enregistrez ce fichier sur une disquette. Vous pouvez utiliser n'importe quel nom de fichier avec une extension de type exécutable. Utilisez par exemple "TRYGUARD.COM" ou "TRYGUARD.EXE".

4. Si l'option **Teste les écritures** est sélectionnée (voir page 93), WinGuard déclenche une alerte (voir "Si WinGuard détecte un virus" à la page 99). WinGuard ne peut pas désinfecter ce fichier test et déclenche donc une alerte comme si l'option **Désinfection automatique** était désactivée (voir page 93), qu'elle soit en fait désactivée ou non.

5. Si WinGuard ne déclenche pas d'alerte, renommez le fichier en lui attribuant une autre extension de type exécutable. Si vous avez appelé le fichier "TRYGUARD.COM" par exemple, changez le nom en "TRYGUARD.EXE". WinGuard doit désormais déclencher une alerte.

6. Supprimez le fichier après le test, si tant est que WinGuard vous permette de l'enregistrer, afin d'éviter une éventuelle confusion.

Modification de la configuration de WinGuard

Il existe des options que vous pouvez définir pour modifier le mode d'opération de WinGuard. Les paramètres standard (par défaut) de ces options conviennent à la plupart des utilisateurs mais vous pouvez les modifier afin de répondre à vos besoins spécifiques.

Pour modifier les options de WinGuard, vous devez utiliser le programme de configuration qui lui est consacré.

Vous pouvez modifier la configuration de balayage de WinGuard ainsi que les messages qui s'affichent lors d'une alerte au virus. Vous pouvez également définir un mot de passe afin d'empêcher d'autres modifications des options.

Conseils généraux

Comme il est mentionné ci-avant, la configuration standard de WinGuard convient pour la plupart des situations.

Les principales exceptions sont les suivantes :

- Vous souhaitez échanger des fichiers pouvant comporter des objets OLE intégrés (documents Microsoft Word par exemple). Dans ce cas, il est recommandé d'activer l'option **Balayer tous les fichiers OLE** (voir page 92).

- Vous souhaitez télécharger des fichiers à partir d'Internet ou des services télématiques ou échanger des fichiers compressés. Dans ce cas, il est recommandé d'activer l'option **Teste les écritures** (voir page 93).

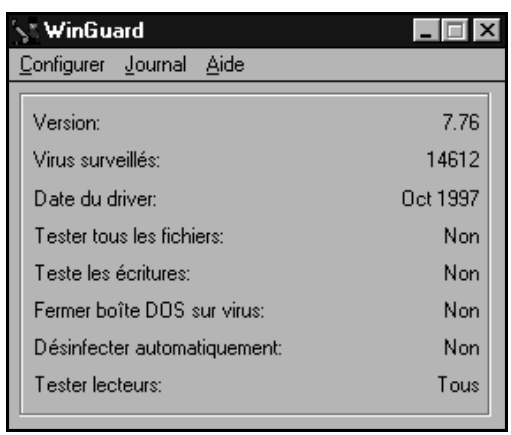
Modification de la configuration de balayage

Pour modifier les options de balayage de WinGuard :

1. Ouvrez WinGuard en cliquant deux fois sur l'icône WinGuard de votre bureau (Windows 3.x) ou en cliquant sur l'icône WinGuard de votre barre des tâches (Windows 95) :

   Si WinGuard a été désactivé, l'icône n'est pas affichée. Dans ce cas, vous devez lancer le programme à partir du groupe de programmes "Anti-Virus Toolkit" (pour Windows 3.x) ou du groupe de programmes "Dr Solomon's AVTK" (pour Windows 95).

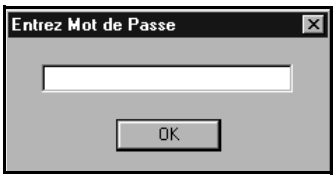
   La boîte de dialogue représentée ci-dessous apparaît :



Vérifiez la configuration et déterminez si vous souhaitez la modifier. Si WinGuard n'est pas activé, le message "WinGuard NON chargé" apparaît.

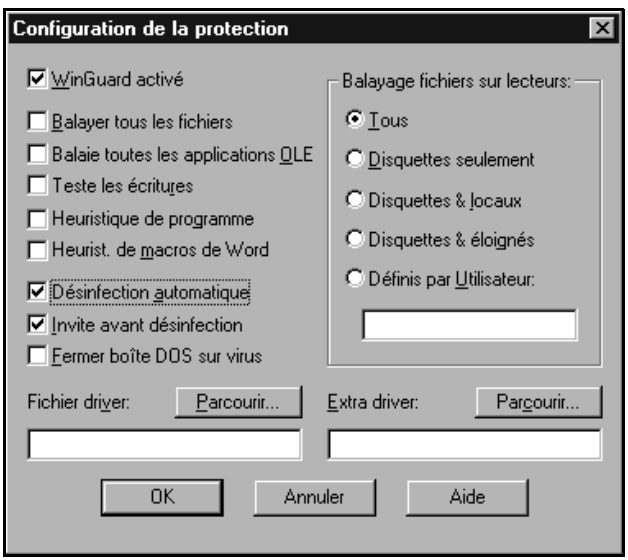
2. Si vous souhaitez modifier la configuration ou activer WinGuard, sélectionnez **Protection** dans le menu **Configurer**.

3. Tapez le mot de passe à l'invite.



Si aucun mot de passe n'existe, vous pouvez en définir un. Si vous connaissez le mot de passe, vous pouvez le modifier (voir à la page 96 pour plus de détails).

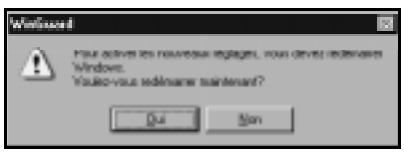
La boîte de dialogue suivante apparaît :



4. Effectuez les modifications de configuration désirées.

5. Lorsque vous avez terminé, cliquez sur **OK**. Un message de confirmation apparaît :

6. Cliquez sur **OK** pour confirmer vos modifications. Cliquez sur **Annuler** pour ignorer vos modifications. Si vous cliquez sur **OK**, un message vous invitant à redémarrer Windows afin que les modifications entrent en vigueur apparaît :



7. Cliquez sur **Oui** pour redémarrer Windows. Cliquez sur **Annuler** si vous ne souhaitez pas redémarrer Windows. Si vous ne relancez pas votre système immédiatement, les modifications entreront en vigueur à la prochaine réinitialisation de votre ordinateur.

Options de balayage

La boîte de dialogue de configuration de WinGuard est illustrée à la page 90.

Les options sont les suivantes :

- **WinGuard activé** : lorsque cette option est sélectionnée, WinGuard est actif. Si vous désactivez cette option, WinGuard n'est pas lancé automatiquement.

Attention Si vous désactivez WinGuard, vous exposez votre système aux infections.

Balayer tous les fichiers : activez cette option pour balayer tous les fichiers à la recherche de virus.

Lorsque cette option est désactivée, seuls les fichiers qui sont le plus susceptibles d'être infectés sont vérifiés. Ces fichiers sont sélectionnés en fonction de l'extension qu'ils portent, sur la base du fait que seuls les fichiers comportant un code exécutable peuvent être infectés, par exemple les fichiers de programmes portant l'extension .EXE ou .COM ou les fichiers de macros. Les fichiers qui ne comportent pas de code exécutable, tels que les fichiers de données enregistrant les résultats de votre travail sur l'ordinateur, ne peuvent pas être infectés.

Si l'option **Balayer tous les fichiers** est désactivée, seuls les fichiers portant l'une des extensions suivantes sont balayés :

APP	DOC	OVR	XLB
BIN	DOT	SCR	XLS
COM	EXE	SYS	XTP
DLL	OVL	XLA	

Le balayage de tous les fichiers prend plus de temps et il est donc recommandé de ne choisir cette option que si, par exemple, vous avez des fichiers exécutables que vous avez renommés et dont la nouvelle extension ne figure pas dans la liste.

La sélection de cette option active automatiquement l'option **Balayer tous les fichiers OLE**.

- **Balayer tous les fichiers OLE** : activez cette option pour vous assurer que tous les fichiers contenant des objets OLE (objets liés et incorporés) sont vérifiés.

  Cette option est automatiquement activée si l'option **Balayer tous les fichiers** est sélectionnée.

  Vous avez la possibilité de choisir cette option car les fichiers de données, tels que les documents Microsoft Word par exemple, peuvent être infectés s'ils contiennent un code exécutable sous la forme d'une macro.

  Il existe des mesures de protection même sans cette option. En effet, la liste des extensions utilisée pour sélectionner les fichiers lorsque l'option **Balayer tous les fichiers** est désactivée (comme il est décrit plus haut) comprend les extensions .DOC et .DOT de Microsoft Word ainsi que l'extension .XL? d' Excel. Toutefois, l'option **Balayer tous les fichiers OLE**

offre une protection pour les fichiers comportant des objets OLE et dotés d'une autre extension.

- **Teste les écritures :** activez cette option pour balayer les fichiers juste après qu'ils aient été enregistrés sur disque ou disquette.

  Cette option offre une protection lorsque, par exemple, vous téléchargez des fichiers à partir d'Internet.

Conseil

Il est recommandé d'activer cette option si vous utilisez des utilitaires d'archivage ou de compression de fichiers tels que PKZIP. Si l'option **Teste les écritures** est activée, les fichiers sont vérifiés immédiatement après leur décompression.

- **Heuristique de programme** : activez cette option si vous souhaitez inclure dans le balayage une recherche des éventuels nouveaux codes (non identifiés) de virus de programme (fichier). Cette option accroît la sécurité mais également la durée du balayage.

- **Heuristique de macros Word** : activez cette option si vous souhaitez inclure dans le balayage une recherche des éventuels nouveaux codes (non identifiés) de virus de macro Word. Cette option accroît la sécurité mais également la durée du balayage.

- **Désinfection automatique** : activez cette option pour que WinGuard supprime automatiquement les virus à mesure qu'ils sont détectés (voir également "Si WinGuard détecte un virus" à la page 99).

- **Invite avant désinfection** : activez cette option pour que WinGuard vous demande confirmation avant de supprimer automatiquement le virus détecté. Cette option apparaît en grisé si l'option **Désinfection automatique** est désactivée.

- **Fermer la boîte DOS sur virus** : activez cette option pour que les actions d'alerte au virus de WinGuard comprennent la fermeture de la session DOS, si vous travaillez sous DOS (sans cette option, la session DOS est uniquement réduite sous forme d'icône).

- **Fichier driver :** les fichiers driver contiennent des informations sur les virus connus qui permettent ensuite de les détecter. WinGuard utilise par défaut le fichier driver "FINDVIRU.DRV".

Si vous souhaitez utiliser cette option, vous devez contacter le support technique de Dr Solomon's.

- **Extra driver :** il se peut que Dr Solomon's mette sur le marché des fichiers driver supplémentaires. Ces derniers contiennent des détails sur des nouveaux virus qui ne sont pas inclus dans le fichier driver standard et élargissent ainsi la gamme des virus pouvant être détectés.

  Si vous souhaitez utiliser cette option pour spécifier le fichier driver supplémentaire, vous devez contacter le support technique de Dr Solomon's. Vous devez spécifier le chemin d'accès complet au fichier driver supplémentaire.

Conseil 

Si le fichier driver supplémentaire est appelé EXTRA.DRV et qu'il se trouve dans le répertoire de Toolkit, il n'est pas nécessaire de le spécifier, car le système l'utilise automatiquement.

Conseil 

Pour vous aider à les identifier et à les classer, vous pouvez ajouter vos propres commentaires dans les fichiers driver supplémentaires. Utilisez un éditeur de texte, tel que Notepad pour ajouter et visualiser vos commentaires. Commencez chaque ligne de commentaire par un point-virgule (;).

- **Balayage des fichiers sur les lecteurs :** les lecteurs locaux sont les disques durs connectés à votre ordinateur, tels que le lecteur "C:" et d'autres lecteurs le cas échéant. Les lecteurs distants sont les lecteurs accessibles par l'intermédiaire d'un réseau.

Conseil 

Il est recommandé de choisir l'option **Tous** pour détecter les virus existants à mesure qu'ils s'installent sur votre (vos) disque(s) dur(s) et d'empêcher ainsi les virus d'infecter votre ordinateur à partir de sources externes.

Si vous sélectionnez l'option **Définis par utilisateur**, tapez les lettres correspondant aux lecteurs à balayer dans la zone de texte. Aucun

caractère d'espacement ni signe de ponctuation n'est nécessaire entre les lettres.

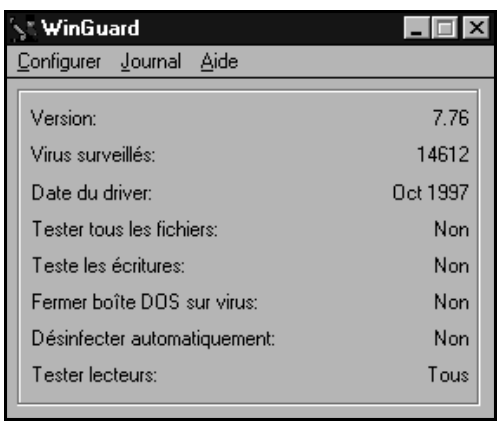
Modification des messages d'alerte

Pour changer les options de message de WinGuard :

1. Ouvrez WinGuard en cliquant deux fois sur l'icône WinGuard de votre bureau (Windows 3.x) ou en cliquant sur l'icône WinGuard de votre barre des tâches (Windows 95) :

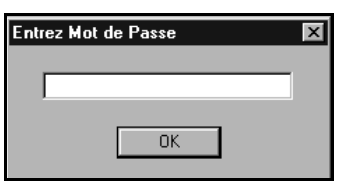
Si WinGuard a été désactivé, l'icône n'est pas affichée. Dans ce cas, vous devez d'abord activer WinGuard (voir la section "Modification de la configuration de balayage" à la page 89).

La boîte de dialogue représentée ci-dessous apparaît :



2. Sélectionnez **Alerte** dans le menu **Configurer**.

3. Entrez votre mot de passe à l'invite .



La boîte de dialogue suivante apparaît :

La boîte de dialogue illustre les messages d'alerte au virus. Un message différent s'affiche en fonction de l'emplacement auquel le virus est détecté : dans un fichier, un secteur de boot ou un secteur de partition. Un "message réseau" est transmis par le réseau en plus du message d'alerte local.

4. Modifiez le texte du message pour qu'il réponde à vos besoins. Vous pouvez modifier n'importe quel texte à l'exception de <ce type de texte>. Le texte apparaissant entre chevrons est remplacé par le nom du virus ou du fichier approprié lorsque le message s'affiche à l'écran.

5. Si vous souhaitez définir ou changer un mot de passe, saisissez-le dans la zone "Mot de passe". Confirmez-le en le tapant dans la zone "Vérif. mot de passe".

   Le mot de passe protège les deux options du menu **Configurer**.

Consignation des rapports

WinGuard peut conserver un enregistrement de ses activités dans un fichier journal. Seuls les balayages qui détectent un virus sont consignés sur fichier. Le journal est enregistré sous la forme d'un fichier texte. Par défaut, il est placé dans le répertoire du Toolkit.

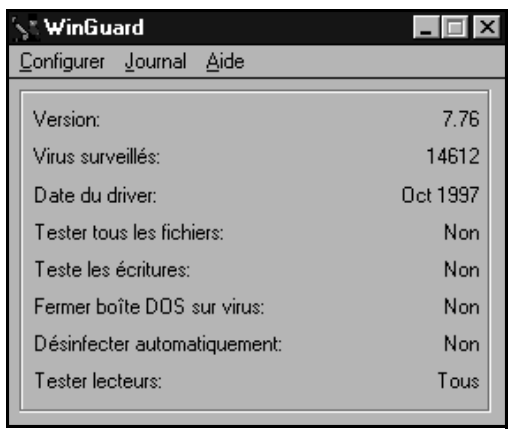
Activation

Pour activer la consignation des rapports :

1. Ouvrez WinGuard en cliquant deux fois sur l'icône WinGuard de votre bureau (pour Windows 3.x) ou en cliquant sur l'icône WinGuard de votre barre des tâches (pour Windows 95) :

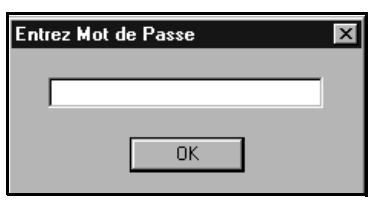
   Si WinGuard a été désactivé, l'icône n'est pas affichée. Dans ce cas, vous devez d'abord activer WinGuard (voir la section "Modification de la configuration de balayage" à la page 89).

2. La boîte de dialogue représentée ci-dessous apparaît :

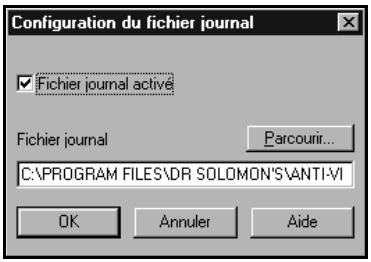


3. Sélectionnez **Options** dans le menu **Journal**.

4. Entrez votre mot de passe à l'invite.



La boîte de dialogue suivante apparaît :



5. Activez la case à cocher **Fichier journal activé**.

6. Si vous le souhaitez, vous pouvez remplacer le nom du fichier journal par défaut par un nom de votre choix. Vous pouvez spécifier un autre chemin d'accès en le tapant directement ou en utilisant le bouton **Parcourir** et en le sélectionnant à partir de l'interface utilisateur.

7. Cliquez sur **OK**.

Affichage

Le fichier journal étant en format texte standard, vous pouvez utiliser un éditeur de texte pour l'afficher.

Vous pouvez aussi utiliser le programme de configuration de WinGuard :

1. Ouvrez WinGuard en cliquant deux fois sur l'icône WinGuard de votre bureau (pour Windows 3.x) ou en cliquant sur l'icône WinGuard de votre barre des tâches (pour Windows 95) :

   Si WinGuard a été désactivé, l'icône n'est pas affichée. Dans ce cas, vous devez d'abord activer WinGuard (voir la section "Modification de la configuration de balayage" à la page 89).

2. Sélectionnez **Afficher** dans le menu **Journal**.

   Le journal s'affiche dans l'application Notepad de Windows.

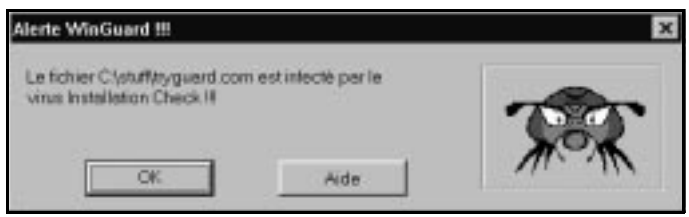
Si WinGuard détecte un virus

Les réactions de WinGuard à la détection d'un virus dépend de l'activation ou non de l'option **Désinfection automatique**.

Conseil L'option **Désinfection automatique** étant désactivée par défaut, vous devez l'activer manuellement (voir page 93).

Si WinGuard détecte un virus et que l'option **Désinfection automatique** n'est pas activée :

- Si le balayage ne s'effectue pas à l'écriture (voir **Balayer à l'écriture** à la page 93), l'action est interrompue.
- Un écran d'alerte apparaît par-dessus le programme exécuté.

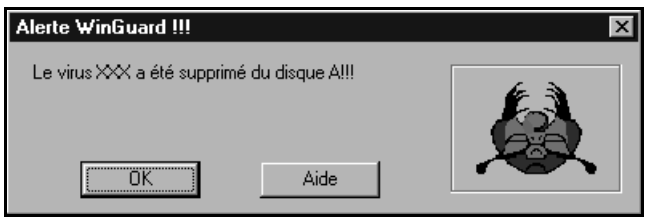


- Selon les paramètres définis (voir la section "Modification des messages d'alerte" à la page 95), vous pouvez enregistrer le rapport concernant le virus dans un fichier journal ou l'envoyer sous la forme d'un message réseau.
- Si le balayage ne s'effectue pas à l'écriture, votre application vous avertit également qu'elle ne peut pas accéder au fichier ou au disque spécifié.

Cliquez sur **OK** et désinfectez immédiatement les fichiers corrompus. Vous pouvez procéder à une désinfection :

- en activant l'option **Désinfection automatique** de WinGuard (vous devez redémarrez le système après la sélection de l'option **Désinfection automatique** afin que celle-ci entre en vigueur) et en répétant la procédure,
- en utilisant FindVirus, soit à partir de l'interface utilisateur, soit à partir de l'utilitaire Magic Bullet ("Utilisation de Magic Bullet" à la page 1).

Si WinGuard détecte un virus, avec l'option **Désinfection automatique** activée et que la désinfection réussit, un message d'alerte semblable à celui représenté ci-dessous apparaît :



Cliquez sur **OK** pour continuer.

Si la désinfection échoue, l'effet est le même que lorsque l'option **Désinfection automatique** est désactivée. Dans ce cas, contactez le support technique de Dr Solomon's pour quelques conseils.

Attention

Pour les utilisateurs de Windows 95 : si WinGuard ne parvient pas à désinfecter un fichier, vous devez supprimer ce fichier. Après avoir supprimé le fichier, vous devez vider la Corbeille de votre bureau pour vous assurer que le fichier infecté ne reste pas sur votre ordinateur.

4.5 Balayage avancé avec WinGuard pour Windows NT

Désinfecter constitue l'une des actions que vous pouvez exécuter sur les fichiers infectés à la lecture mais aussi (indépendamment) sur les fichiers infectés à l'écriture. L'action par défaut est **Ne rien faire**. Si vous souhaitez que WinGuard désinfecte les fichiers automatiquement, vous devez sélectionner l'option **Désinfecter**. Effectuez cette sélection à l'aide de l'onglet Action (voir page 108).

Si WinGuard détecte un virus - option Désinfecter non sélectionnée

L'option **Désinfecter** ne s'applique pas aux secteurs de boot et de partition du disque dur et, si WinGuard détecte un virus dans l'un de ces secteurs, l'effet est toujours semblable à la description de cette section.

Si WinGuard détecte un virus et que l'option **Désinfecter** n'est pas sélectionnée pour le type d'accès :

- L'action exécutée est interrompue.
- La boîte de dialogue Alerte (dans une de ses deux formes) apparaît à l'écran par-dessus le programme exécuté (voir les pages 104 et 105 pour des illustrations de cette boîte de dialogue).
- Selon les paramètres définis, les rapports sur le virus peuvent être envoyés sous la forme de messages et enregistrés dans le journal des événements (voir la section "Onglet Sortie" à la page 111).
- En fonction de l'action sélectionnée pour le type d'accès (voir la section "Onglet Action" à la page 108), WinGuard peut ne rien faire, supprimer le fichier ou déplacer le fichier vers un répertoire de quarantaine.
- Votre application vous avertit également qu'elle ne peut pas accéder au fichier / disque spécifié.
- Toutes les autres activités du système continuent normalement.

Suivez ces étapes :

1. Si vous utilisez le type de liste historique de la boîte de dialogue Alerte, vous pouvez utiliser le bouton **Exécuter FindVirus** pour désinfecter rapidement les fichiers infectés. Pour cela, vous devez activer **Désinfecter** dans l'onglet FindVirus. Il est également recommandé de suivre le reste des étapes ci-dessous.

2. Notez les détails concernant les fichiers infectés affichés dans la boîte de dialogue Alerte, puis fermez cette dernière.

3. Quittez l'application normalement et enregistrez les fichiers sur lesquels vous travaillez.

4. Essayez de contenir l'expansion du virus en fermant toutes les applications superflues sur votre ordinateur.

Attention Assurez-vous de ne pas fermer trop précipitamment des programmes qui sont essentiels au fonctionnement du réseau.

5. Vous devez vous débarrasser du virus aussi rapidement que possible à l'aide de FindVirus (voir la section "Désinfection des lecteurs" à la page 145). Vous pouvez également sélectionner l'option **Désinfecter** et répéter la procédure.

Si WinGuard détecte un virus - option Désinfecter sélectionnée

L'option **Désinfecter** ne s'applique pas aux secteurs de boot et de partition du disque dur et, si WinGuard détecte un virus dans l'un de ces secteurs, l'effet est semblable à la description figurant à la page 101.

Si WinGuard détecte un virus dans un fichier ou dans le secteur de boot d'une disquette et que l'option **Désinfecter** est sélectionnée pour le type d'accès, le système tente de supprimer le virus automatiquement.

Si le système parvient éliminer le virus, vous pouvez continuer à travailler normalement. Si l'option **Ne pas afficher de message d'alerte si la désinfection est réussie** n'est pas sélectionnée dans l'onglet Désinfecter (voir page 110), la boîte de dialogue Alerte s'affiche pour vous informer de la désinfection. Si l'option **Ne pas afficher de message d'alerte si la désinfection est réussie** est sélectionnée, la boîte de dialogue Alerte ne s'affiche pas.

Si le système tente de désinfecter le secteur de boot d'une disquette et qu'il n'y parvient pas, WinGuard réagit comme si l'option **Désinfecter** n'était pas sélectionnée, comme il est décrit à la page 101.

Si le système essaie de désinfecter un fichier et qu'il n'y parvient pas, l'effet produit dépend de l'action sélectionnée pour l'option "Si le fichier ne peut pas être désinfecté" de l'onglet Désinfecter (voir page 110).

- Si l'option sélectionnée est **Ne rien faire**, WinGuard affiche seulement la boîte de dialogue Alerte.
- Si l'option sélectionnée est **Supprimer**, WinGuard détruit le fichier et affiche la boîte de dialogue Alerte.
- Si l'option sélectionnée est **Déplacer vers le répertoire de quarantaine**, WinGuard déplace le fichier vers le répertoire de quarantaine, comme il est spécifié dans l'onglet Action et affiche la boîte de dialogue Alerte.

Reportez-vous à la page 101 pour une description de la procédure qui suit la détection d'un virus par WinGuard, lorsque l'action **Désinfecter** n'est pas sélectionnée pour le type d'accès effectué.

Boîte de dialogue Alerte - type liste historique

Vous pouvez configurer WinGuard de sorte à utiliser l'un des deux types de la boîte de dialogue Alerte. Cette section couvre le type "liste historique". Pour plus de détails sur le type "message personnalisé", consultez les pages suivantes.

L'illustration ci-dessous représente la boîte de dialogue Alerte de type liste historique :

La boîte de dialogue affiche la liste des rapports d'infections.

Si l'option "Ne pas afficher de message d'alerte si la désinfection est réussie" est désactivée dans l'onglet Désinfecter (voir page 110), la boîte de dialogue affiche aussi la liste des rapports des désinfections réussies.

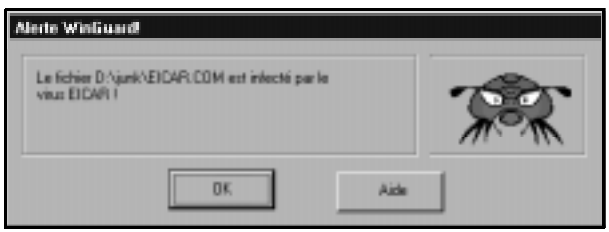
La boîte de dialogue vous donne le choix de démarrer FindVirus ou le Toolkit complet (si ces derniers sont installés sur votre système).

Les rapports incluent un horodateur et le nom du fichier infecté ou désinfecté. Les nouveaux rapports sont ajoutés à la fin de la liste et restent affichés jusqu'à ce que vous cliquiez sur **Effacer**.

Boîte de dialogue Alerte - type message personnalisé

Vous pouvez configurer WinGuard de sorte à utiliser un des deux types de la boîte de dialogue Alerte. Cette section couvre le type “message personnalisé”. Pour plus de détails sur le type “liste historique”, reportez-vous aux pages précédentes.

L’illustration ci-dessous représente la boîte de dialogue Alerte de type message personnalisé :



Cette boîte de dialogue affiche les rapports concernant les :

- infections,
- tentatives de désinfection infructueuses,
- désinfections réussies mais uniquement si l’option “Ne pas afficher de message d’alerte si la désinfection est réussie” est désactivée dans l’onglet Désinfecter (voir page 110).

A l’aide de l’onglet Message (voir page 112), vous pouvez écrire votre propre texte pour le message affiché en cas d’infection du secteur de boot et de partition et pour le message affiché en cas d’infection de fichier(s).

Modification des paramètres d'option

La configuration d'origine de WinGuard (paramètres à l'installation) convient à la plupart des situations mais vous pouvez la modifier si vous avez des exigences particulières.

Vous trouverez tous les détails relatifs aux paramètres d'option par défaut dans un tableau de référence sous la rubrique "Configuration" de l'aide de WinGuard.

Lancement de l'application de configuration

Pour modifier les paramètres d'option, lancez l'application de configuration qui se trouve dans le Panneau de configuration.

Conseil

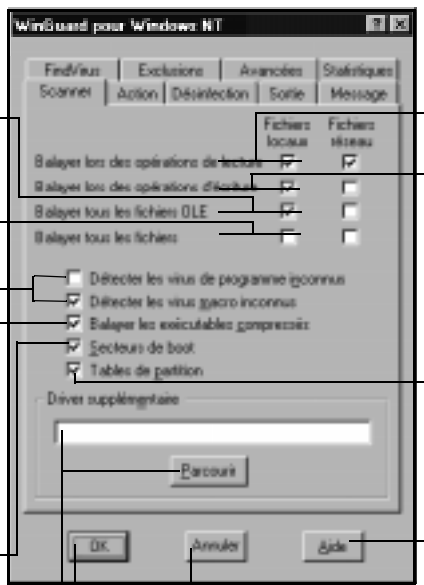
Vous ne pouvez modifier la configuration des paramètres d'option que si vous avez un statut d'administrateur.

Une boîte de dialogue à plusieurs onglets apparaît. Cliquez sur l'onglet que vous désirez activer.

Vous trouverez tous les détails relatifs à chacune des options des onglets dans les sections suivantes.

Onglet Scanner

Utilisez cet onglet pour définir ce que vous souhaitez balayer et, si les fichiers sont balayés, le moment où vous souhaitez les balayer. Vous pouvez également spécifier si un driver supplémentaire est utilisé.



Balaye tous les fichiers comportant des objets OLE sur les lecteurs locaux et/ou de réseau. Cette option détecte les éventuels virus de macro dans tous les fichiers.

Balaye toutes les données et tous les fichiers exécutables sur les lecteurs locaux et/ou de réseau.

Recherche les virus non identifiés ou nouveaux (balayage heuristique). Ce mode accroît la sécurité mais aussi la durée du balayage.

Balaye les fichiers compressés à l'aide de programmes tels que PKLite ou LZExe.

Balaye les secteurs de boot du disque dur local (NTFS ou DOS FAT) au démarrage ou à chaque fois que WinGuard est relancé. Balaye également les secteurs de boot d'une disquette lorsqu'elle est lue pour la première fois.

Balaye les fichiers à la lecture sur les lecteurs locaux et/ou de réseau.

Balaye les fichiers immédiatement après leur écriture sur les lecteurs locaux et/ou de réseau.

Balaye les tables de partition du disque dur local au démarrage ou à chaque fois que WinGuard est relancé.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Annule toute modification.

Valide les modifications. Si vous ajoutez un driver supplémentaire, vous devez redémarrer Windows NT pour que les modifications entrent en vigueur.

Tapez le nom de fichier du driver supplémentaire dans cette zone ou cliquez sur **Parcourir** pour le sélectionner à partir de la boîte de dialogue Parcourir.

A utiliser sous instructions de Dr Solomon's, par exemple lorsque Dr Solomon's publie un driver supplémentaire pour répondre à une soudaine épidémie de virus.

Onglet Action

Utilisez cet onglet pour configurer les actions que WinGuard doit prendre dès qu'il détecte un virus, en plus d'afficher la boîte de dialogue Alerte et d'envoyer des messages réseau (si l'option est activée).

Pour les options **Balayer lors de la lecture** et **Balayer lors de l'écriture**, cliquez sur  et sélectionnez l'option désirée dans le menu déroulant.

Conseil

Remarquez qu'aucune des sélections que vous pouvez effectuer pour les options de cet onglet ne s'applique aux lecteurs réseau (accès en lecture ou en écriture). Pour ces lecteurs, l'option **Ne rien faire** reste toujours activée.

Détermine l'effet de la détection d'un fichier infecté à la lecture. Sélectionnez : **Désinfecter** pour supprimer le virus automatiquement, **Déplacer vers le répertoire de quarantaine** pour déplacer le fichier infecté vers le répertoire spécifié dans l'option "Répertoire de quarantaine", **Ne rien faire** pour ne lancer aucune autre action que l'affichage des résultats.

Détermine l'effet de la détection d'un fichier infecté à l'écriture sur le disque. Choisissez parmi les options **Désinfecter**, **Déplacer vers le répertoire de quarantaine**, **Ne rien faire** ou **Supprimer** pour supprimer le fichier infecté.

Crée le répertoire vers lequel les fichiers infectés sont déplacés si **Déplacer vers le répertoire de quarantaine** est sélectionné pour l'option **Balayer lors de la lecture** ou **Balayer lors de l'écriture**. Tapez le nom du répertoire et/ou le chemin d'accès mais ne spécifiez pas de lettre de lecteur.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Annule toute modification.

Valide les modifications.

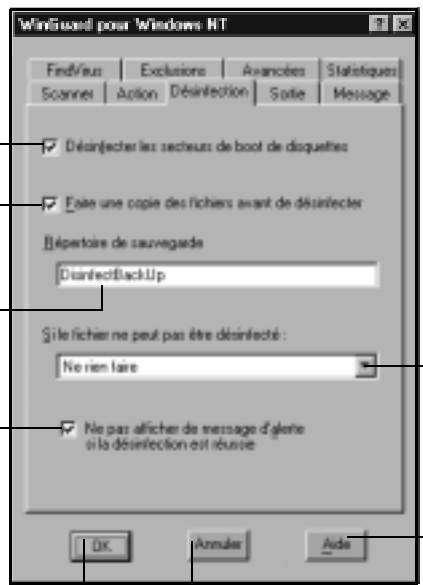
Remarquez que si un fichier est déplacé vers un répertoire de quarantaine qui contient déjà un fichier du même nom, son extension est changée. La nouvelle extension comprend “l’ancien” premier caractère, suivi d’un nombre. Par exemple, le nom de fichier AFILE.COM devient AFILE.C01, le fichier AFILE.COM suivant devient AFILE.C02, etc.

Attention

Si vous choisissez **Supprimer** pour l’option **Balayer lors de l’écriture**, vous risquez de perdre certains fichiers. Imaginons ce scénario : un ordinateur non protégé ouvre un fichier de document MS Word par partage réseau. La machine proposant le partage est protégée. Le fichier se trouve infecté par un virus de macro, puis il est enregistré. Si l’option **Balayer lors de l’écriture** est activée sur l’ordinateur protégé, le fichier est balayé immédiatement après l’enregistrement, est signalé comme infecté et est supprimé. Le document est perdu.

Onglet Désinfecter

Utilisez cet onglet pour configurer les actions que WinGuard doit prendre si vous avez sélectionné **Désinfecter** pour l'option **Balayer lors de la lecture** ou **Balayer lors de l'écriture** dans l'onglet Action (voir page 108). Vous pouvez également déterminer si les secteurs de boot des disquettes doivent être automatiquement désinfectés (les secteurs de boot du disque dur ne sont pas automatiquement désinfectés).



Supprime automatiquement les virus détectés des secteurs de boot de la disquette.

Copie les fichiers vers le répertoire de sauvegarde spécifié avant une désinfection automatique.

Tapez le nom du répertoire vers lequel les fichiers de sauvegarde sont copiés.

ctivez cette option pour u'aucun message d'alerte e s'affiche lorsque la ésinfection d'un fichier est éussie.

Spécifie l'action à prendre pour le fichier si la désinfection automatique échoue. Sélectionnez : **Ne rien faire** pour rapporter l'infection comme si **Désinfecter** n'était pas sélectionné, **Déplacer vers le répertoire de quarantaine** pour déplacer le fichier infecté vers le répertoire spécifié dans l'option "Répertoire de quarantaine" de l'onglet "Action", **Supprimer** pour supprimer le fichier infecté

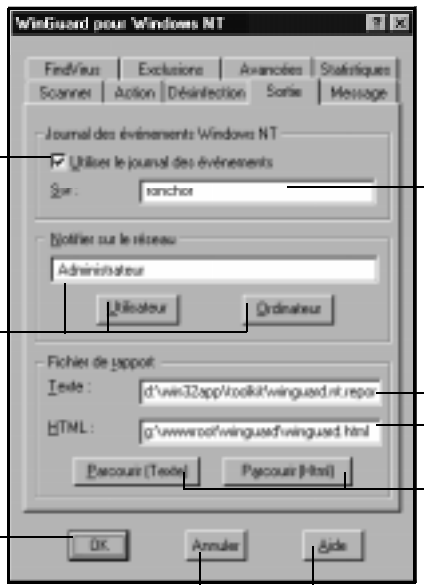
Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Annule toute modification.

Valide les modifications.

Onglet Sortie

Utilisez cet onglet pour définir les rapports que WinGuard doit établir lorsqu'il détecte un virus. WinGuard établit les rapports en plus d'afficher la boîte de dialogue Alerte .



Copie le nom du fichier et du virus infectieux dans le journal des événements de NT.

Tapez le nom d'un utilisateur ou d'une machine spécifique ou cliquez sur **Utilisateur** ou **Ordinateur** et choisissez dans la liste pour envoyer des rapports sur le réseau à l'aide des services de messagerie de Windows NT à l'utilisateur ou à la machine sélectionné(e).

Valide les modifications.

Annule toute modification.

Tapez le nom de l'ordinateur sur lequel se trouve le journal des évènements dans lequel vous voulez afficher le rapport. Remarque : vous devez disposer de droits d'accès suffisants pour cet ordinateur. Les droits d'accès peuvent être configurés manuellement (voir l'aide en ligne "Configuration de la consignation des évènements à distance").

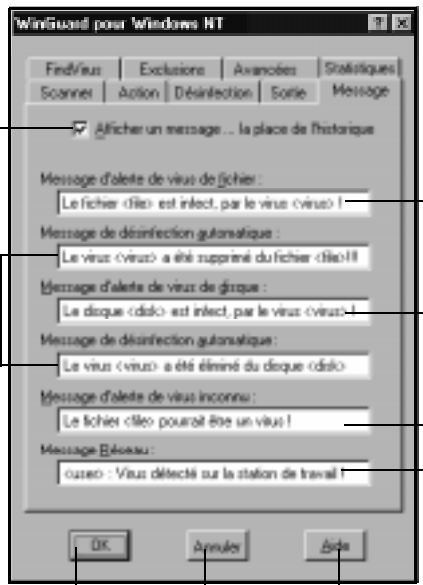
Pour créer un enregistrement permanent des infections par virus, tapez un nom de fichier dans la zone appropriée ou utilisez les boutons **Parcourir** pour sélectionner un fichier de rapport existant.

Cette option enregistre la date et l'heure de la détection de l'infection, le nom du fichier et le type de virus ainsi que le nom de l'utilisateur ayant tenté d'ouvrir le fichier. Les nouveaux rapports sont ajoutés à la fin du fichier existant.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Onglet Message

Utilisez cet onglet pour rédiger les messages qui seront affichés dans la boîte de dialogue Alerte de type message personnalisé (voir page 105).



Sélectionnez cette option pour que la boîte de dialogue Alerte affiche le message spécifié par les options de message d'alerte de cet onglet. Lorsque cette option est désactivée, la boîte de dialogue Alerte affiche une liste de toutes les infections par virus détectées depuis la dernière désinfection.

Tapez le texte du message d'alerte que vous souhaitez afficher lorsque la désinfection est réussie. Prenez soin d'inclure : <virus> pour afficher le nom du virus infectieux, <fichier> pour afficher le nom du fichier infecté, <disque> pour afficher la lettre du lecteur infecté.

Tapez le texte du message d'alerte que vous souhaitez afficher lorsqu'un virus est détecté. Prenez soin d'inclure : <virus> pour afficher le nom du virus infectieux, <fichier> pour afficher le nom du fichier infecté, <disque> pour afficher la lettre du lecteur infecté.

Tapez le texte du message que vous souhaitez envoyer à la destination spécifiée dans l'option "Notifier sur le réseau" de l'onglet "Sortie" lorsqu'un virus est détecté. Prenez soin d'inclure : <utilisateur> pour afficher le nom de l'utilisateur connecté, <virus> pour afficher le nom du virus infectieux, <fichier> pour afficher le nom du fichier infecté.

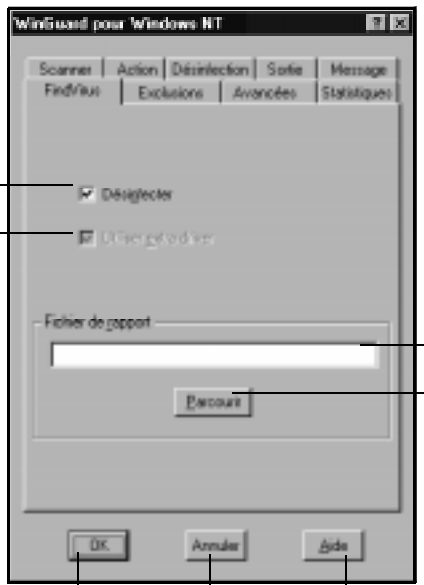
Valide les modifications.

Annule toute modification.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Onglet FindVirus

Si FindVirus est installé sur votre système, la boîte de dialogue Alerte de type liste historique vous offre la possibilité de lancer FindVirus. Utilisez cet onglet pour définir les paramètres utilisés par FindVirus.



Sélectionnez cette option pour que FindVirus désinfecte les fichiers automatiquement lors de son exécution.

Sélectionnez cette option pour que FindVirus utilise un driver supplémentaire (spécifié dans l'onglet Scanner) lorsqu'il est exécuté.
Les drivers supplémentaires sont publiés en tant que mesures temporaires entre les mises à jour prévues afin d'offrir une protection contre une épidémie de virus spécifique.
Cette fonction est indépendante et n'affecte pas les paramètres de FindVirus définis à partir du Toolkit principal.

Tapez un nom de fichier ou le chemin d'accès complet d'un fichier ou utilisez le bouton **Parcourir** pour sélectionner le fichier dans lequel vous voulez copier les rapports de balayage de FindVirus.
Cette fonction est indépendante et n'affecte pas les paramètres de FindVirus définis à partir du Toolkit principal.

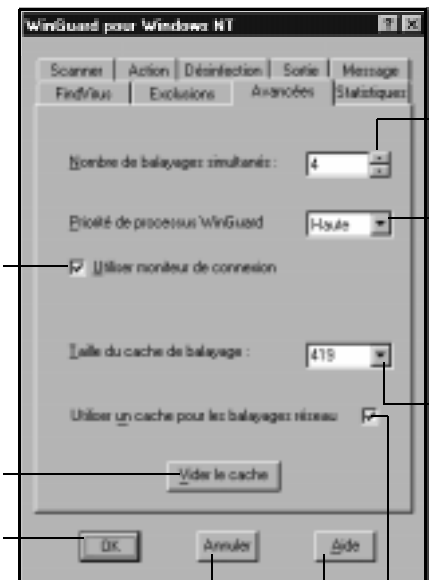
Valide les modifications.

Annule toute modification.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Onglet Avancé

Utilisez cet onglet pour affiner le fonctionnement interne de WinGuard. La configuration par défaut de cet onglet convient à la plupart des utilisateurs. Si vous pensez que vous avez besoin de modifier certains paramètres, procédez avec précaution et assurez-vous d'en connaître les conséquences.



Permet à WinGuard de s'intégrer au NetWare Toolkit fonctionnant sur un serveur.
Permet au poste de travail de passer la vérification effectuée par NetWare Toolkit afin de s'assurer que WinGuard fonctionne avant qu'une connexion au réseau puisse s'établir.

Supprime tous les enregistrements de fichiers de la mémoire cache de balayage.

Valide les modifications.

Annule toute modification.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Permet de définir le nombre (maximum 64) de fichiers pouvant être balayés en même temps à l'aide des fonctionnalités multiconnexions de Windows NT.

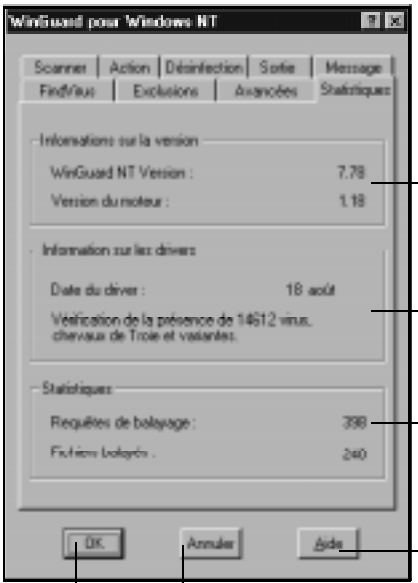
Permet de définir la priorité de processus WinGuard. **Haute** permet de s'assurer que WinGuard balaye les fichiers aussi rapidement que possible.
Cela n'affecte pas d'autre application car WinGuard utilise seulement le temps du processeur lors du balayage.

Permet de définir la taille de la mémoire cache de balayage. La mémoire cache de balayage garde un enregistrement des fichiers qui n'ont pas été modifiés en écriture depuis le dernier balayage.
Les fichiers ne pouvant être modifiés qu'en écriture, ces fichiers ne sont pas balayés à nouveau, réduisant ainsi la durée du balayage.

Permet d'inclure les fichiers lus à partir d'un ordinateur distant dans la mémoire cache de balayage. Cette option peut être utilisée en toute sécurité si tous les ordinateurs du réseau exécutent WinGuard NT. Sinon, utilisez-la avec précaution car les modifications en écriture apportées à un fichier depuis une machine distante ne suppriment pas l'entrée de ce fichier dans la mémoire cache de balayage.

Onglet A propos de

Cet onglet affiche les statistiques relatives à l'activité de balayage. Il ne s'agit pas vraiment d'un onglet configurable.



Affiche le numéro de version de WinGuard et le numéro de version du moteur de balayage (partagé avec FindVirus).

Affiche la date de publication du driver et le nombre de virus, troyens et variantes pour lesquels WinGuard recherche les "empreintes" caractéristiques. Cette zone est mise à jour à chaque nouvelle publication.

Affiche le nombre de fichiers ouverts et de balayages exécutés depuis l'exécution de WinGuard NT.

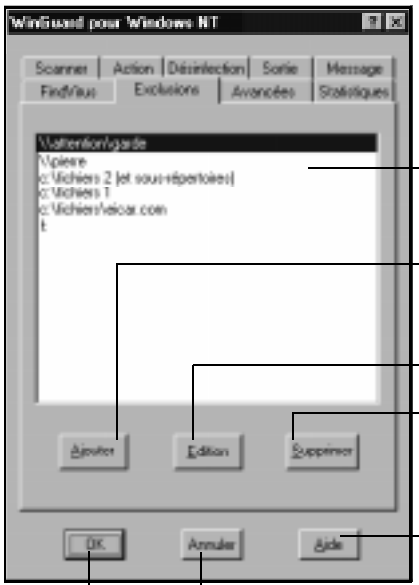
Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue.

Annule toute modification.

Valide les modifications.

Onglet Exclusions

Utilisez cet onglet pour spécifier les fichiers ou les répertoires que vous ne souhaitez pas balayer.



Affiche la liste des fichiers ou répertoires exemptés de balayage.

Permet d'ajouter un élément à la liste des exemptions. Vous pouvez utiliser la technique glisser-déplacer pour ajouter des fichiers et/ou répertoires à la zone de liste à partir du Gestionnaire de fichiers ou de l'Explorateur.

Permet de modifier un élément de la liste des exemptions.

Permet de supprimer un élément de la liste des exemptions.

Ouvre et affiche le fichier d'aide en ligne de cette boîte de dialogue..

Annule toute modification.

Valide les modifications.

5. Utilisation du Scheduler sous Windows 3.x, Windows 95 et Windows NT

L'Editeur de programmation sert à définir des événements qui doivent se déclencher à des moments prédéterminés. Ces événements peuvent consister en des balayages de recherche de virus, des vérifications de fichiers ou le lancement d'une application et peuvent se produire une fois ou à intervalles réguliers.

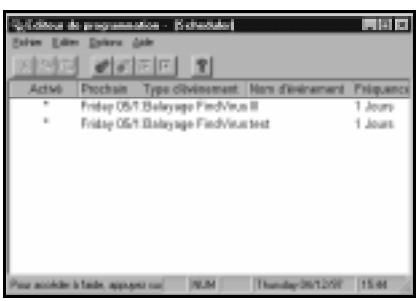
Une fois que vous avez défini les événements, le Scheduler qui est en mémoire fait en sorte qu'ils se produisent aux moments prévus.

Les résultats des événements peuvent être inscrits dans un fichier journal, pour que vous puissiez les passer en revue ultérieurement.

5.1 Editeur de programmation : aperçu et démarrage

Vous pouvez démarrer l'Editeur de programmation à l'aide de l'icône Editeur de programmation dans le groupe de programmes "Dr Solomon's Anti-Virus Toolkit".

Après avoir lancé l'Editeur de programmation, un écran au format suivant apparaît :



Cet écran récapitule tous les événements que vous avez déjà définis et en affiche un par ligne.

Vous pouvez redimensionner les colonnes en sélectionnant les bords des boîtes contenant les en-têtes dans la barre des titres et en les faisant glisser.

Pour intervenir sur un événement existant, cliquez dessus pour le sélectionner.

Vous pouvez afficher une barre d'outils (voir page 144) contenant des icônes de raccourci pour accéder aux éléments du menu Edition. Vous pouvez afficher des conseils concernant ces icônes (voir page 144) en positionnant le curseur sur l'une d'entre elles.

Définition d'un nouvel événement

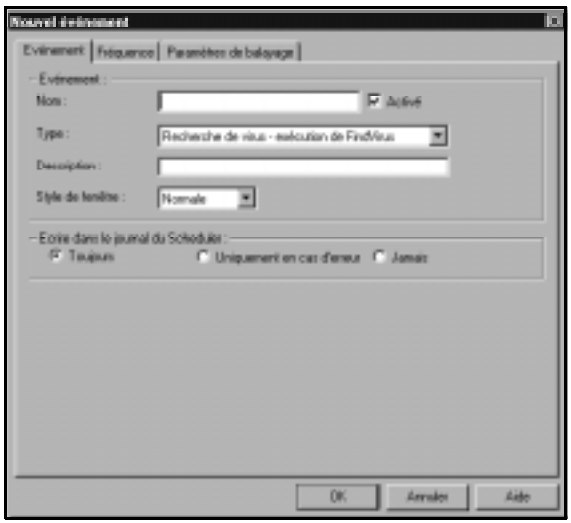
Conseil

Une fois que vous avez défini un nouvel événement comme décrit dans cette section, il faut vous assurer que le Scheduler est actif avant que l'événement puisse avoir lieu. Voir "Exécution du Scheduler" à la page 134.

Onglet Evénement

Pour créer un nouvel événement :

1. Cliquez sur l'icône "Nouvel événement" ou sélectionnez la commande **Ajouter événement** dans le menu **Evénement**. La boîte de dialogue "Nouvel événement" apparaît :



2. Dans la zone "Nom", tapez un nom unique pour l'événement.

3. Pour la boîte de dialogue "Type", sélectionnez un type d'événement à partir du menu déroulant. Les types d'événement disponibles sont :

- **Contrôle anti-virus -exécuter FindVirus.** Si vous sélectionnez ce type d'événement, l'onglet "Paramètres balayage" est disponible dans la boîte de dialogue.

- **Recherche de modifications -exécution de ViVerify.** Si vous sélectionnez ce type d'événement, un onglet "Vérification de la configuration" apparaît dans la boîte de dialogue.

- **Lancer une application.** Dans Windows NT, cette option n'est disponible que pour l'administrateur. Si vous sélectionnez ce type d'événement, un nouveau jeu d'options "Programme" apparaît en bas de la boîte de dialogue.

- **Envoi d'un message (disponible pour Windows 3.x et Windows NT uniquement)**. Si vous sélectionnez ce type d'événement, un nouveau jeu d'options "Message" apparaît en bas de la boîte de dialogue.

4. Sélectionnez un type de fenêtre à partir du menu déroulant pour déterminer l'aspect de la fenêtre de l'événement après son activation.

5. Pour "Ecrire dans le journal du Scheduler", cliquez sur l'une des cases d'option afin d'effectuer votre sélection. Le fichier journal du Scheduler enregistre les détails de tout événement déclenché. Il comprend la date et l'heure prévues pour l'événement ainsi que les détails de son exécution. Vous pouvez décider si le fichier journal doit être écrit :

- **Toujours,**

- **Uniquement en cas d'erreur** (une "erreur" indique que l'événement n'a pas pu être déclenché, par exemple si un fichier exécutable d'une application est introuvable),

- **Jamais.**

6. Accédez à l'onglet "Fréquence" et définissez vos paramètres comme indiqué dansla section "Onglet Fréquence" à la page 122.

7. Si vous avez sélectionné **Contrôle anti-virus -exécuter FindVirus** comme type d'événement,accédez à l'onglet "Paramètres de recherche" et définissez vos paramètres comme indiqué dans "Onglet Paramètres de balayage" à la page 123.

8. Si vous avez sélectionné **Recherche de modifications -exécution de ViVerify** comme type d'événement, accédez à l'onglet "Vérification de la configuration" et définissez vos paramètres comme indiqué dans la section "Onglet Vérification de la configuration" à la page 130.

9. Si vous avez sélectionné **Lancer une application**, définissez les éléments de la zone “Programme”, qui apparaissent en bas de la boîte de dialogue de la manière suivante :

- Vous pouvez taper une entrée directement dans la zone “Description”. Vous avez également la possibilité de cliquer sur la flèche descendante qui se trouve à côté de la boîte d’entrée pour afficher une liste déroulante. Cette liste contient la description de programmes qui ont été configurés dans l’onglet “Listes” de la boîte de dialogue “Paramètres par défaut du Dr Solomon’s Scheduler” (voir l’étape 11 à la page 143). Cliquez sur l’une d’entre elles pour sélectionner un programme.

- Dans la boîte “Ligne de commande”, tapez directement la ligne de commande ou utilisez le bouton **Parcourir** pour trouver le fichier exécutable du programme. Cette option est activée automatiquement si vous sélectionnez la description du programme à partir de la liste déroulante de la zone “Description”.

- Dans la boîte de dialogue “Répertoire de démarrage”, tapez le répertoire de démarrage du programme.

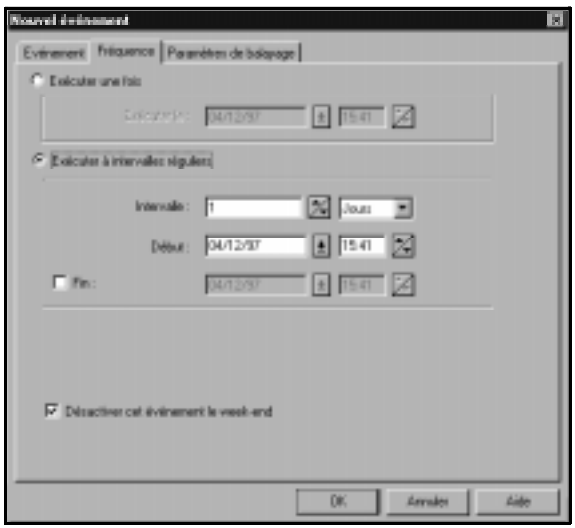
- Cliquez sur **OK**.

10. **Pour les utilisateurs de Windows 3.x et de Windows NT uniquement :** si vous avez sélectionné **Envoi d’un message**, tapez le texte du message dans la zone “Message” et le code de connexion de l’utilisateur destinataire dans la boîte “Envoyer à”. Cliquez sur **OK**. Vous pouvez définir des messages dans la boîte de dialogue des paramètres par défaut (voir page 140).

11. Une fois la définition de l’événement que vous souhaitez voir lancé par le Scheduler terminée, cliquez sur **OK**. La boîte de dialogue “Options d’enregistrement” apparaît. Sélectionnez l’option appropriée et cliquez sur **OK**.

Onglet Fréquence

Vous accédez à cet onglet à l'étape numéro 6 de la procédure de la section "Définition d'un nouvel événement" (voir page 120). Après avoir défini les paramètres, retournez à l'étape numéro 7 de la procédure.



Les points suivants fournissent des informations concernant les éléments de l'onglet Fréquence.

- Les formats d'heure et de date utilisés sont identiques à ceux configurés pour Windows.
- Vous ne pouvez pas sélectionner une heure au-delà de 23 h 59 et une date ultérieure au 31 décembre 2038.
- Vous ne pouvez pas sélectionner une heure ou une date passée.
- Pour l'option **Désactiver cet événement le week-end** : les week-ends commencent le vendredi à minuit et finissent le dimanche à minuit.
- Si vous sélectionnez une fréquence mensuelle et une date de départ se trouvant en fin de mois, une invite apparaît vous demandant si vous souhaitez que l'événement se produise le dernier jour de chaque mois ou uniquement le jour spécifié.

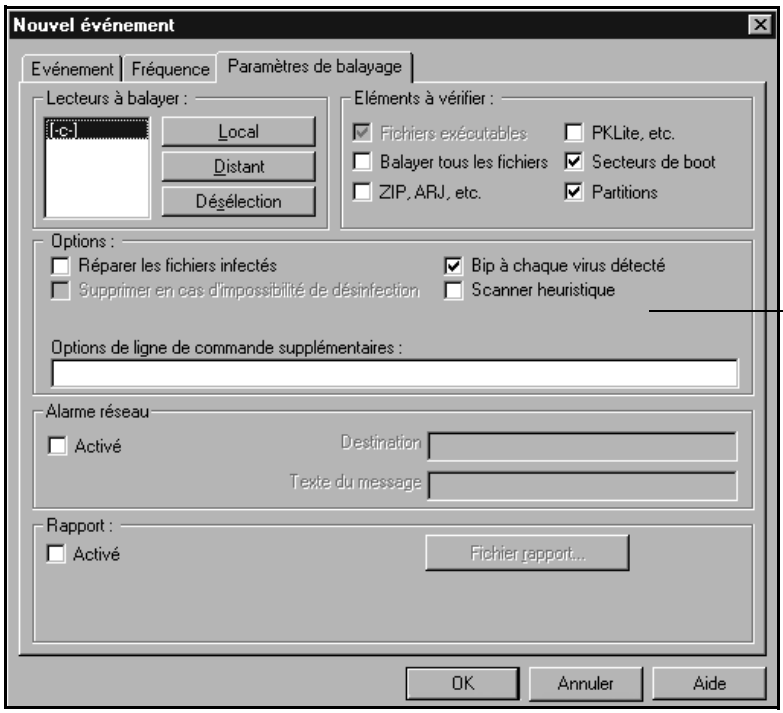
- Vous pouvez taper des dates et des heures directement ou utiliser les boutons servant à incrémenter et décrémenter les entrées.
- Pour entrer des dates, vous pouvez cliquer sur le bouton servant à décrémenter qui se trouve à côté de la boîte d'entrée, puis sélectionner une date à partir du calendrier.
- Les paramètres de fréquence initiaux dans la section "Exécuter à intervalles réguliers" sont définis de la même manière que dans l'onglet "Général" de la boîte de dialogue "Paramètres par défaut du Dr Solomon's Scheduler" (voir étapes 4 à 7 à la page 142). Vous pouvez vouloir utiliser cette possibilité si vous êtes souvent amené à utiliser souvent les mêmes paramètres.

Onglet Paramètres de balayage

Vous accédez à cet onglet à l'étape 7 de la procédure dans "Définition d'un nouvel événement" (voir page 120). Après avoir défini les paramètres, cliquez sur **OK**. La définition de l'événement est terminée.

Conseil

Les paramètres initiaux de cet onglet sont conformes à la définition qui en est faite dans l'onglet "Paramètres de balayage" de la boîte de dialogue "Paramètres par défaut du Dr Solomon's Scheduler" (voir l'étape 9, à la page 143). Cette fonction est utile si vous utilisez souvent les mêmes paramètres.



Windows NT comprend une option supplémentaire, **Inscrire dans le journal d'événement NT**. Activez cette option pour ajouter un enregistrement au journal d'événement NT à chaque fois qu'un événement prévu se produit.

Les paramètres et les options pour FindVirus sont les suivants :

Fonction	Description
Lecteurs à balayer :	Cliquez sur un lecteur désélectionné pour le sélectionner. Cliquez sur un lecteur sélectionné pour le désélectionner. Cliquez sur le bouton Locaux pour sélectionner tous les lecteurs locaux, en plus des lecteurs déjà sélectionnés. Cliquez sur le bouton “Réseau” pour ajouter tous les lecteurs se trouvant sur le réseau aux lecteurs déjà sélectionnés. Les noms de chemins d’accès UNC sont reconnus.
Eléments à vérifier :	
Fichiers exécutables	Cette fonction apparaît en grisé car les fichiers exécutables sont toujours balayés. FindVirus utilise l’extension du nom d’un fichier pour pouvoir l’identifier comme fichier exécutable et, par conséquent, le balayer. Si vous pensez que certains fichiers exécutables ne portent pas l’extension standard, sélectionnez la fonction “Tous les fichiers”.
Balayer tous les fichiers	Activez cette fonction si vous souhaitez que tous les fichiers soient balayés et non seulement les fichiers que leur extension rend exécutables. Cela vous apporte plus de sécurité, mais ralentit le balayage. Utilisez cette fonction sur les machines footbath, lors du nettoyage après une infection ou si vous pensez avoir des fichiers exécutables possédant une extension non standard.

Fonction	Description
ZIP, ARJ, etc.	Activez ces fonctions pour décompresser temporairement des fichiers compressés afin que les fichiers qu'ils contiennent puissent être balayés. Cette fonction opère sur les fichiers compressés aux formats suivants : ARC, PKZip, PKLite, LZExe, ARJ, ICE, LZH, Diet (Version 1.0) et CryptCom.
Si l'option "Tous les fichiers" est activée, les fichiers "shell" eux-mêmes (le fichier archive ".ZIP", par exemple) sont balayés.	
PKLite, etc.	Activez cette fonction pour décompresser temporairement des fichiers compressés afin que les fichiers qu'ils contiennent puissent être balayés. Cette fonction opère sur les fichiers compressés aux formats suivants : PKLite, LZExe, ICE, Diet (Version 1.0) et CryptCom. Si l'option "Tous les fichiers" est activée, les fichiers "shell" contenant les fichiers compressés sont également balayés.
Secteurs de Boot	Désactivez cette fonction uniquement si elle vous pose un problème particulier. Si vous balayez un lecteur sur réseau qui ne dispose pas d'un secteur de boot, par exemple.
Partitions	Désactivez cette fonction uniquement si elle vous pose un problème particulier.

Fonction	Description
Options:	
Réparer les fichiers infectés	Activez cette option pour supprimer les virus des fichiers infectés. Sauf spécification contraire à l'aide d' "Options de ligne de commande supplémentaires", les fichiers infectés qui n'auront pas pu être réparés sont renommés. La première lettre de leur extension devient "V".
Suppression en cas d'impossibilitéd e désinfection	Si vous sélectionnez cette option et que FindVirus ne parvient pas à désinfecter un fichier, ce dernier est effacé.
Bip sur virus	Emet un signal sonore à chaque détection de virus.
Scanner heuristique	L'analyse heuristique est une technique permettant d'identifier de nouveaux codes de virus potentiels (même les macros). L'activation de cette option vous permet d'obtenir une sécurité accrue, mais elle ralentit le balayage.
Options de ligne de commande supplémentaires	Vous pouvez encore modifier le balayage en assignant à FindVirus des commutateurs spécifiques dans la présente zone. Pour plus de détails, voir la rubrique "FindVirus" dans l'aide en ligne du Toolkit. Il n'est pas nécessaire de spécifier la plupart des commutateurs disponibles, car des options sont similaires dans l'onglet. Vous pouvez également les utiliser. Toutefois, certains commutateurs ne comprennent pas d'option leur correspondant. Dans ce cas, si vous avez besoin d'eux, il vous faudra spécifier duquel / desquels il s'agit.

Fonction	Description
Alerte réseau :	
Activé	Activez cette option pour l'envoi d'un message d'alerte sur le réseau.
Destination	Spécifiez le code de connexion au réseau de l'utilisateur destinataire.
Texte du message	Spécifiez le texte du message à transférer sur le réseau.
Rapport :	
Activé	Activez cette option si vous souhaitez que les résultats du balayage, de même que l'écran, soient copiés dans un fichier de type ASCII. Le fichier rapport doit être spécifié à l'aide du bouton "Fichier rapport".
Fichier rapport	Cette fonction fait apparaître une interface vous permettant de sélectionner un fichier existant ou d'entrer un nouveau fichier. Les fichiers existants sont écrasés et les nouveaux fichiers sont créés. La fonction "Rapport : Activé" doit être activée.

Aide

Si vous souhaitez définir un élément apparaissant dans l'une des boîtes de dialogue Trouver virus ou Trouver virus - Options avancées mais qui n'apparaît pas dans cet onglet, vous pouvez spécifier le commutateur qui lui correspond dans la zone "Options de ligne de commande supplémentaires". Pour plus d'informations, voir la rubrique "FindVirus" dans l'aide en ligne du Toolkit.

Attention

Bien que les balayages programmés de FindVirus détectent les virus se trouvant dans le secteur de boot et le secteur de partition du disque dur, FindVirus ne peut pas désinfecter ces secteurs automatiquement. Si un virus est détecté sur le secteur de boot ou le secteur de partition du disque dur lors d'un balayage programmé de FindVirus, il vous faut utiliser la disquette Magic Bullet pour procéder à une désinfection manuelle. Pour plus d'informations sur l'utilisation de la disquette Magic Bullet, voir la section "Utilisation de Magic Bullet" à la page 1.

Si un virus est détecté dans le secteur de boot ou le secteur de partition du disque dur lors d'un balayage de FindVirus sous Windows NT, contactez le support technique de Dr Solomon's. Pour plus d'informations sur la procédure à suivre pour contacter le support technique de Dr Solomon's, voir la section "Si vous avez besoin d'aide" à la page xiv.

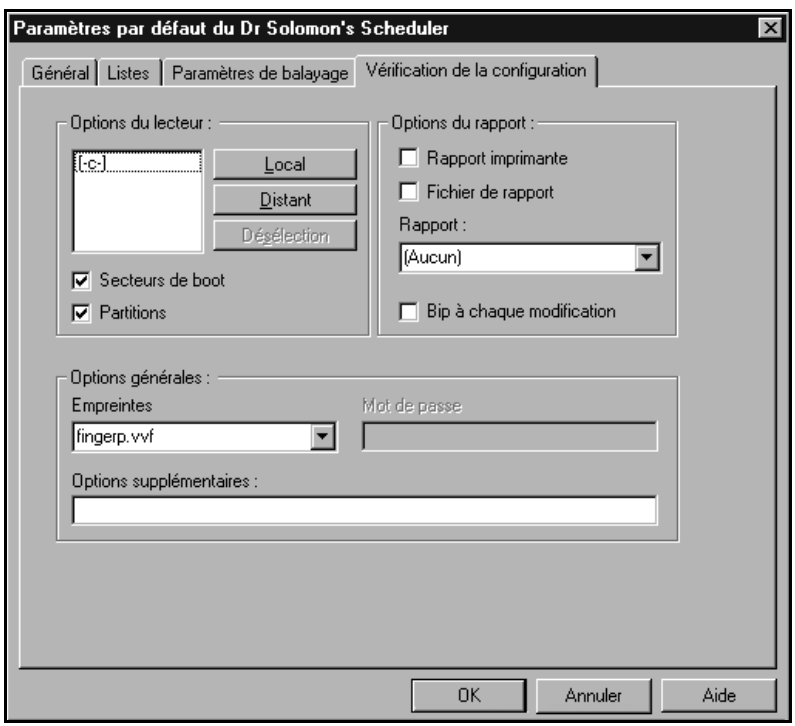
Onglet Vérification de la configuration

Vous accédez à cet onglet à l'étape 8 de la procédure décrite dans la section "Définition d'un nouvel événement" (voir page 120). Après avoir défini les paramètres, cliquez sur **OK**. La définition de l'événement est terminée.

Conseil

Les paramètres initiaux de cet onglet sont conformes à la définition qui en est faite dans l'onglet "Vérification de la configuration" de la boîte de dialogue "Paramètres par défaut du Dr Solomon's Scheduler" (voir l'étape 10 à la page 143). Cette fonction peut vous être utile s'il vous arrive d'utiliser souvent les mêmes paramètres.

Le balayage vérifie les éventuelles modifications par rapport aux fichiers d'empreintes qui ont déjà été générés manuellement.



Les paramètres et les options pour ViVerify sont les suivants :

Fonction	Description
Options du lecteur	Cliquez sur un lecteur désélectionné pour le sélectionner. Cliquez sur un lecteur sélectionné pour le désélectionner. Cliquez sur le bouton **Locaux** pour ajouter tous les lecteurs locaux aux lecteurs déjà sélectionnés. Cliquez sur le bouton “Distant” pour ajouter tous les lecteurs se trouvant sur le réseau aux lecteurs déjà sélectionnés. Cliquez sur le bouton **Désélectionner** pour effacer toutes les sélections. Les noms de chemin UNC sont reconnus.
Secteurs de boot	Vérifie les secteurs de boot.
Partitions	Vérifie les secteurs de partition.
Options du rapport :	
Rapport imprimante	Activez cette option si vous souhaitez que les résultats du balayage soient copiés sur l’imprimante par défaut et apparaissent également à l’écran.
Fichier rapport	Activez cette option si vous souhaitez que les résultats du balayage soient copiés dans un fichier de type ASCII et apparaissent également à l’écran. Le fichier rapport par défaut est “VIVERIFY.REP” et se trouve dans le répertoire du Toolkit. Vous pouvez modifier cela à l’aide de l’élément “Rapport”.
Rapport :	Vous pouvez utiliser cette option pour spécifier un fichier rapport différent en saisissant un nouveau chemin d’accès et / ou un nom de fichier ou en sélectionnant un fichier à partir de la liste déroulante (qui contient les entrées les plus récentes).

Fonction	Description
Bip à chaque modification	Emet un signal sonore à chaque fois qu'un fichier modifié est découvert.
Options générales :	
Empreintes	Utilisez cette option pour spécifier le fichier d'empreintes en tapant un nouveau chemin d'accès et/ou un nouveau nom de fichier ou en sélectionnant un fichier à partir de la liste déroulante (qui contient les entrées les plus récentes). Une vérification concernant les modifications ne peut être effectuée que sur les fichiers possédant une entrée dans le fichier d'empreintes. Tout fichier que ViVerify tente de vérifier et qui ne possède pas une telle entrée est considéré comme un "nouveau" fichier. Vous pouvez éviter cela si, lorsque vous vérifiez les modifications après avoir sélectionné des lecteurs spécifiques, vous choisissez le fichier d'empreintes qui avait été créé avec les mêmes lecteurs.
Mot de passe	Afin qu'ils soient protégés d'éventuelles interférences avec des virus, les fichiers d'empreintes sont codés à l'aide d'un "Mot de passe" que vous entrez. Tapez le mot de passe utilisé lors du traitement du fichier d'empreintes.

Fonction	Description
Options supplémentaires	Vous pouvez encore modifier le balayage en assignant des commutateurs à ViVerify dans cette zone. Pour plus de détails, voir la rubrique “Viverify” dans l’aide en ligne du Toolkit. Il n’est pas nécessaire de spécifier la plupart des commutateurs disponibles, car des options leur correspondent dans un onglet que vous pouvez utiliser à leur place. Toutefois, certains commutateurs ne possèdent pas d’option leur correspondant. Dans ce cas, s’ils vous sont nécessaires, il vous faut spécifier duquel / desquels il s’agit.

Conseil

La plupart de ces éléments apparaît également, soit dans la boîte de dialogue ”Test pour modifications” (voir page 117), soit dans la boîte de dialogue “Test pour modifications - Options avancées” (voir page 120) de l’interface utilisateur du Toolkit. Si vous souhaitez définir un élément qui apparaît dans l’une de ces boîtes de dialogue mais qui n’apparaît pas dans cet onglet, vous pouvez spécifier le commutateur lui correspondant dans la boîte de dialogue “Options supplémentaires”.

5.2 Exécution du Scheduler

Une fois que vous avez défini les événements à occurrence périodique, assurez-vous que le Scheduler est actif. Si tel est le cas, son icône apparaît.

Si, lors de l'installation, vous avez choisi de ne pas activer le Scheduler, il vous est toujours possible de l'activer ultérieurement.

Pour les utilisateurs de Windows 3.x :

1. Dans le groupe de programmes "Dr Solomon's Anti-Virus Toolkit", cliquez sans relâcher sur l'icône du Scheduler.
2. Faites glisser l'icône du Scheduler vers le groupe de programmes Démarrage.
3. Relancez Windows. Le Scheduler est désormais actif et son icône apparaît en bas de l'écran.

Pour les utilisateurs de Windows 95 :

S'il n'est pas actif, démarrez le Scheduler à partir du groupe Dr Solomon dans le menu Démarrage.

Pour les utilisateurs de Windows NT :

1. Cliquez sur **Démarrer** et sélectionnez l'option **Paramètres**, puis **Panneau de configuration**.
2. Cliquez deux fois sur l'icône **Services** dans le groupe Panneau de configuration.
3. Dans la boîte de dialogue qui apparaît, faites défiler la liste des services et sélectionnez **Dr Solomon's Scheduler**. Cliquez sur **Démarrer**.

Configuration du Scheduler sous Windows NT

Vous pouvez changer le compte sur lequel le Scheduler se connecte habituellement (il utilise, par défaut, le compte “Système”).

Conseil Vous pouvez créer un compte réservé au Scheduler.

Vous pouvez programmer des balayages de FindVirus s’appliquant à des portions distantes du réseau ou permettant de copier des rapports. Dans ce cas, il faut vous assurer que le Scheduler se connecte avec un compte disposant des droits d’accès appropriés à ces différentes portions du réseau.

Pour que les balayages programmés FindVirus puissent balayer des portions distantes du réseau, le Scheduler doit être connecté via un compte disposant de l’accès en lecture aux portions concernées.

Pour que les balayages programmés FindVirus puissent copier des rapports dans des portions distantes du réseau, le Scheduler doit être connecté via un compte disposant de l’accès en écriture aux portions concernées.

5.3 Administration des événements

Modification d’un événement

Pour modifier un événement existant :

1. Démarrez l’Editeur de programmation.
2. Sélectionnez l’événement que vous souhaitez éditer, puis **Modification d’un événement** à partir du menu **Edition**. Vous pouvez également cliquer deux fois sur l’événement.

   La boîte de dialogue “Modification d’un événement” apparaît. Cette dernière est identique à la boîte de dialogue “Nouvel événement”, sauf qu’elle apparaît au départ sous le même aspect que lors de sa dernière sauvegarde pour l’événement en question plutôt que d’apparaître sous la forme déterminée par la boîte de dialogue des paramètres par défaut.

3. Répétez la procédure détaillée dans “Définition d’un nouvel événement” à la page 118 tout en modifiant les paramètres si nécessaire. Cliquez sur **OK** lorsque vous avez terminé d’apporter vos modifications.

4. Sélectionnez l’option appropriée dans la boîte de dialogue ”Options d’enregistrement”.

5. Cliquez sur **OK**.

Suppression d’un événement

1. Démarrez l’Editeur de programmation.

2. Dans l’Editeur de programmation, mettez l’événement concerné en évidence.

3. Cliquez sur l’icône **Supprimer l’événement** (ou sélectionnez l’option **Supprimer l’événement** dans le menu **Edition**).

4. Cliquez sur **Oui**.

5. Sélectionnez l’option appropriée dans la boîte de dialogue “Options d’enregistrement”.

6. Cliquez sur **OK**.

Désactivation d’un événement

Par défaut, un événement est activé. Ceci est indiqué par un symbole dans la colonne “Activé”.

1. Démarrez l’Editeur de programmation.

2. Dans l’Editeur de programmation, mettez l’événement concerné en évidence.

3. Cliquez sur l’icône **Désactiver l’événement** (ou sélectionnez l’option **Désactiver l’événement** dans le menu **Edition**).

4. Sélectionnez l’option appropriée dans la boîte de dialogue “Options d’enregistrement”.

5. Cliquez sur **OK**.

Activer un événement

Un symbole dans la colonne “Activé” indique qu’un événement est activé.

1. Démarrez l’Editeur de programmation.
2. Dans l’Editeur de programmation, mettez l’événement concerné en évidence.
3. Cliquez sur l’icône “Activer l’événement” (ou sélectionnez l’option **Activer l’événement** dans le menu **Edition**).
4. Sélectionnez l’option appropriée dans la boîte de dialogue “Options d’enregistrement”.
5. Cliquez sur **OK**.

Couper et coller un événement

Lorsqu’il vous arrive de “Couper” un événement, l’original est supprimé de la boîte de dialogue “Editeur de programmation”, mais les paramètres peuvent encore être collés dans un nouvel événement.

1. Démarrez l’Editeur de programmation.
2. Dans l’Editeur de programmation, mettez l’événement concerné en évidence.
3. Cliquez sur l’icône “Couper” (ou sélectionnez l’option **Couper** dans le menu **Edition**).
4. Sélectionnez l’option appropriée dans la boîte de dialogue “Options d’enregistrement”.
5. Cliquez sur **OK**.
6. Cliquez sur l’icône “Coller”.

7. Saisissez les détails appropriés et cliquez sur **OK**.
8. Sélectionnez l'option appropriée dans la boîte de dialogue "Options d'enregistrement".
9. Cliquez sur **OK**.

Copier et coller un événement

Le fait de "Copier" un événement vous permet de laisser l'original intact tout en collant les paramètres dans un nouvel événement. Si un événement a été copié il doit être renommé.

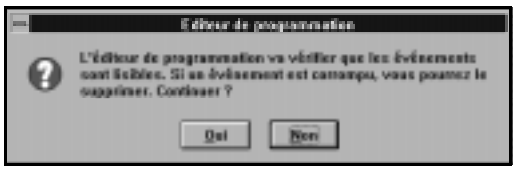
1. Démarrez l'Editeur de programmation.
2. Dans l'Editeur de programmation, mettez l'événement concerné en évidence.
3. Cliquez sur l'icône "Copier" (ou sélectionnez l'option **Copier** dans le menu **Edition**).
4. Cliquez sur l'icône "Coller"
   .

5. Tapez les détails appropriés et cliquez sur **OK**.
6. Sélectionnez l'option appropriée dans la boîte de dialogue "Options d'enregistrement".
7. Cliquez sur **OK**.

Validation d'événements (uniquement disponible sous Windows 3.x)

Vous pouvez vérifier la validité des événements. Ceux pour lesquels des données ont été corrompues sont supprimées.

1. Démarrez l'Editeur de programmation.
2. Dans le menu **Fichier**, sélectionnez l'option **Valider programme**.



3. Cliquez sur **Oui**. Si le programme n'a pas été corrompu, le message "Validation terminée" apparaît.

4. Cliquez sur **OK**.

Tous les événements corrompus sont supprimés.

5.4 Fichier journal du Scheduler

Le fichier journal de Scheduler peut enregistrer les détails d'une tentative de déclenchement d'un événement. Ces détails peuvent comprendre l'heure et la date prévues pour l'événement et si la tentative de déclenchement a réussi ou non.

Pour plus de détails sur la procédure à suivre pour définir les options nécessaires à l'élaboration du fichier journal de Scheduler, voir l'étape 5 à la page 120.

Consultation du fichier journal :

1. Démarrez l'Editeur de programmation.
2. Dans le menu **Fichier**, sélectionnez l'option **Fichier journal du Scheduler**.
3. Sélectionnez **Afficher**.

   Le fichier journal s'ouvre sous Bloc-notes.

Modification du nom de fichier journal

Par défaut, le fichier journal est enregistré sous le nom de TK_SCHED.LOG dans le dossier d'installation du Toolkit. Pour modifier ce nom :

1. Démarrez l'Editeur de programmation.
2. Dans le menu **Fichier**, sélectionnez l'option **Fichier journal du Scheduler** puis **Renommer**.

   La boîte de dialogue "Renommer le fichier journal du Scheduler" apparaît.
3. Utilisez la boîte de dialogue pour créer un nouveau fichier ou pour sélectionner un fichier existant que vous souhaitez écraser.

5.5 Paramètres par défaut de la boîte de dialogue Nouvel événement

Les paramètres initiaux pour les onglets "Fréquence", "Paramètres de balayage" et "Vérification de la configuration" de la boîte de dialogue "Nouvel événement" sont déterminés par les paramètres de la boîte de dialogue "Paramètres par défaut du Dr Solomon's Scheduler".

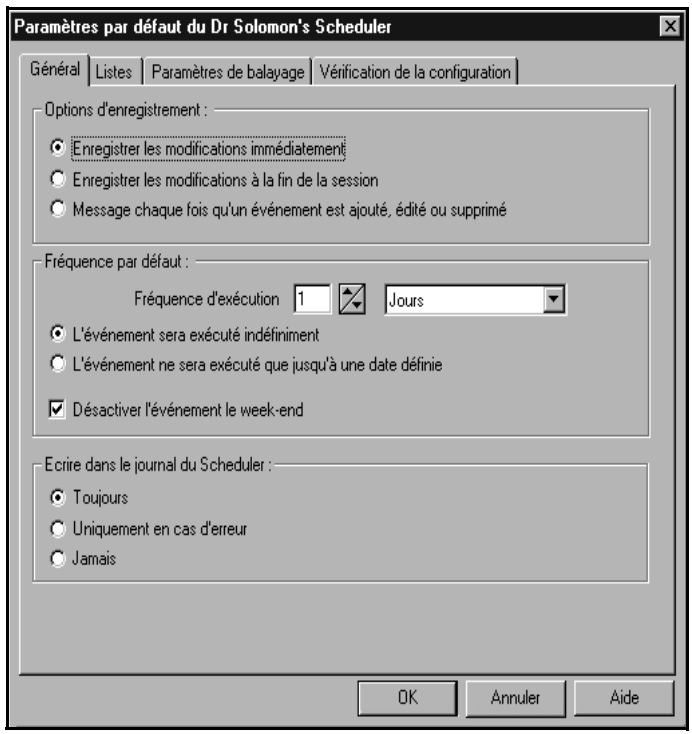
Cette boîte de dialogue vous permet également de définir des options d'enregistrement de données concernant les événements et de créer des options de sélection pour certains des menus déroulants de la boîte de dialogue "Nouvel événement".

Pour déterminer les paramètres dans la boîte de dialogue “Paramètres par défaut du Dr Solomon’s Scheduler” :

1. Démarrez l’Editeur de programmation.

2. Dans le menu **Options**, sélectionnez **Paramètres par défaut**.

   La boîte de dialogue “Paramètres par défaut du Dr Solomon’s Scheduler” apparaît. Elle contient plusieurs onglets, dont l’onglet “Général”, qui apparaît initialement.



Conseil

Vous pouvez cliquer à tout moment sur **OK** et ainsi mettre fin à la procédure, si vous jugez que d’autres modifications ne sont pas nécessaires.

3. Pour la section “Options d’enregistrement”, sélectionnez l’une des cases d’option. Les options sont :

- **Enregistrer les modifications immédiatement** : toutes les modifications que vous effectuez sont enregistrées sur le disque et prennent donc effet immédiatement. Par exemple, si vous programmez un événement pour qu’il se produise 5 minutes après, il se déclenchera, que l’Editeur de programmation soit encore actif ou non.

- **Enregistrer les modifications à la fin de la session** : les modifications que vous effectuez ne sont pas enregistrées sur le disque dur et ne deviennent effectives que si vous quittez l’Editeur de programmation.

- **Message chaque fois qu’un événement est ajouté, édité ou supprimé** : à chaque modification que vous effectuez, une boîte de dialogue vous invite à sélectionner **Enregistrer les modifications maintenant** (ce qui équivaut à “Enregistrer les modifications immédiatement”) ou **Ne pas enregistrer les modifications** (ce qui équivaut à ”Enregistrer les modifications à la fin de la session”). Cette boîte de dialogue vous propose également l’option **Enregistrer ce choix pour une utilisation ultérieure - ne plus afficher cette boîte de dialogue**.

4. Modifiez les éléments de “Fréquence d’exécution” afin d’obtenir la présentation que vous souhaitez avoir lorsque vous accédez à l’onglet “Fréquence” de la boîte de dialogue “Nouvel événement” (voir l’étape 6 à la page 120).

5. Sélectionnez la case d’option pour l’option **L’événement sera exécuté indéfiniment** si vous souhaitez que les éléments “Fin : ” soient désactivés, lorsque vous accédez à l’onglet “Fréquence” de la boîte de dialogue “Nouvel événement” pour la première fois.

6. Sélectionnez la case d’option correspondant à **L’événement ne sera exécuté que jusqu’à une date définie** si vous souhaitez que les éléments “Fin : ” soient activés, lorsque vous accédez à l’onglet “Fréquence” de la boîte de dialogue “Nouvel événement” pour la première fois.

7. Définissez l’état de **Désactiver cet événement le week-end** selon la présentation que vous souhaitez obtenir lors de l’ouverture de la boîte de dialogue “Nouvel événement”.

8. Sélectionnez la case d'option **Ecrire dans le journal du Scheduler** que vous souhaitez voir sélectionné lorsque vous ouvrez le boîte de dialogue "Nouvel événement".

9. Accédez à l'onglet "Paramètres de balayage". Modifiez cet onglet selon la présentation que vous souhaitez obtenir dans la boîte de dialogue "Nouvel événement", lorsque vous l'ouvrez pour la première fois (voir page 123).

10. Accédez à l'onglet "Vérification de la configuration". Modifiez cet onglet selon la présentation que vous souhaitez obtenir dans la boîte de dialogue "Nouvel événement", lorsque vous l'ouvrez pour la première fois (voir page 130).

11. Accédez à l'onglet "Listes".

12. L'onglet "Listes" vous permet de définir des programmes pouvant être utilisés avec la fonction "Lancer une application". Sous Windows 3.x et Windows NT, l'onglet "Listes" vous permet aussi de définir une liste de messages par défaut qui peut être utilisée avec la fonction "Envoi d'un message". Cet emplacement apparaît dans l'onglet Evénement des boîtes de dialogue "Nouvel événement" (voir l'étape 9 à la page 121) et "Modification d'un événement", mais uniquement lorsque vous sélectionnez **Lancer une application** ou **Envoi d'un message**.

    Dans "Liste des programmes", cliquez sur **Nouveau** ou sélectionnez une description et cliquez sur **Edition**. Vous voyez apparaître la boîte de dialogue "Infos programme". Celle-ci vous montre l'aspect de la zone "Programme" de la boîte de dialogue "Evénement" lorsque vous sélectionnez la description du programme à partir de la liste déroulante. Modifiez les éléments de cette boîte de dialogue à votre gré. Pour supprimer un programme, mettez-le en évidence et cliquez sur **Supprimer.**

Conseil

Pour les utilisateurs de Windows NT : remarquez que seul l'administrateur peut utiliser la "Liste des programmes".

Pour les utilisateurs de Windows 3.x et de Windows NT : dans “Liste des messages”, cliquez sur **Nouveau** ou sélectionnez un message et cliquez sur **Edition**. Vous voyez apparaître la boîte de dialogue “Message”. Vous pouvez ainsi créer une liste de messages qui apparaîtront dans la liste déroulante. Modifiez les éléments de cette boîte de dialogue selon vos besoins. Pour supprimer un message, mettez-le en évidence et cliquez sur **Supprimer**.

5.6 Options d’environnement général

Les options suivantes vous permettent de modifier l’environnement de l’Editeur de programmation :

Elément du menu Options	Fonction
Police	Permet d’ouvrir une interface pour choisir la police d’affichage de l’Editeur de programmation.
Afficher barre d’outils	Permet d’afficher ou de masquer la barre d’outils (voir page 118).
Afficher barre d’état	Permet d’afficher ou de masquer la barre d’état.
Afficher conseils	Permet d’afficher ou de masquer les conseils (voir page 118).

6. Désinfection

6.1 Désinfection des lecteurs

Une manière rapide de désinfecter, à l'aide des paramètres d'options initiaux ou des derniers paramètres d'options définis via le menu **Désinfecter** (ou via le menu **Balayer**), est d'utiliser l'écran principal :

1. Sélectionnez le(s) lecteur(s) que vous souhaitez désinfecter dans la boîte de dialogue "Lecteurs".

2. Cliquez sur **Désinfecter**. **Pour les utilisateurs de OS/2 :** cliquez sur **Réparer**.

3. La boîte de dialogue qui apparaît vous indique d'abord l'évolution du processus de désinfection, puis les résultats de celle-ci. Vous pouvez annuler la désinfection à tout moment en cliquant sur **Sortie**. Dans ce cas, l'écran principal du Toolkit apparaît.

4. Une fois la désinfection terminée, notez les résultats et cliquez sur **Sortie** pour retourner à l'écran principal du Toolkit.

Attention

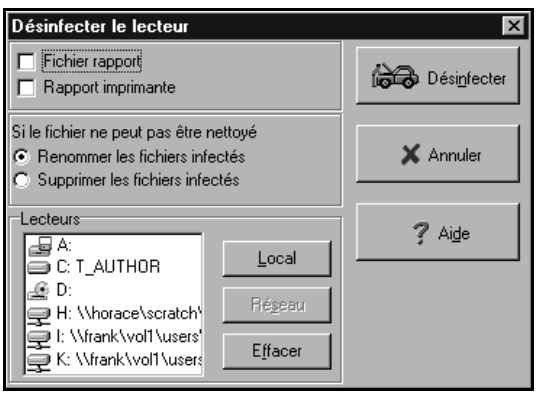
Pour les utilisateurs de Windows NT : si le nom d'utilisateur (avec lequel vous vous êtes connecté) ne fait pas partie du groupe "Administrateur", FindVirus ne peut pas accéder au secteur de partition et au secteur de boot du disque dur. Dans ce cas, les messages "Ne peut lire le secteur de partition" et "Ne peut lire le secteur de boot" apparaissent. Si vous devez désinfecter ces secteurs, reportez-vous alors à l'administrateur de votre système.

Vous pouvez supprimer les virus des fichiers, des secteurs de boot et de partition à l'aide du menu **Désinfecter**. Ce dernier vous propose, en effet, différentes options permettant de modifier le mode de balayage de désinfection.

Pour modifier les paramètres des options et désinfecter les lecteurs :

1. A partir du menu **Désinfecter**, sélectionnez **Désinfecter le lecteur**. La boîte de dialogue “Désinfecter le lecteur” apparaît alors.

Conseil **Pour les utilisateurs de OS/2 :** veuillez sélectionner la commande **Réparer lecteur** dans le menu **Réparer**. Vous voyez alors apparaître la boîte de dialogue “Réparer le lecteur”.



2. Sélectionnez le(s) lecteur(s) que vous souhaitez désinfecter dans la boîte de dialogue “Lecteurs”.

3. Vous pouvez désormais commencer la désinfection. Pour cela, rendez-vous directement à l’étape 8, à moins que vous ne souhaitiez définir encore d’autres options, auquel cas vous pouvez passer à l’étape suivante.

4. Sélectionnez l’option **Rapport vers fichier** si vous souhaitez que les résultats de la désinfection soient copiés sur un fichier ASCII en plus d’être affichés à l’écran. Ce fichier sera nommé “findviru.rep” et sera créé dans le répertoire du Toolkit.

5. Sélectionnez l’option **Rapport vers imprim.** si vous souhaitez que les résultats du balayage soient imprimés en plus d’être affichés à l’écran.

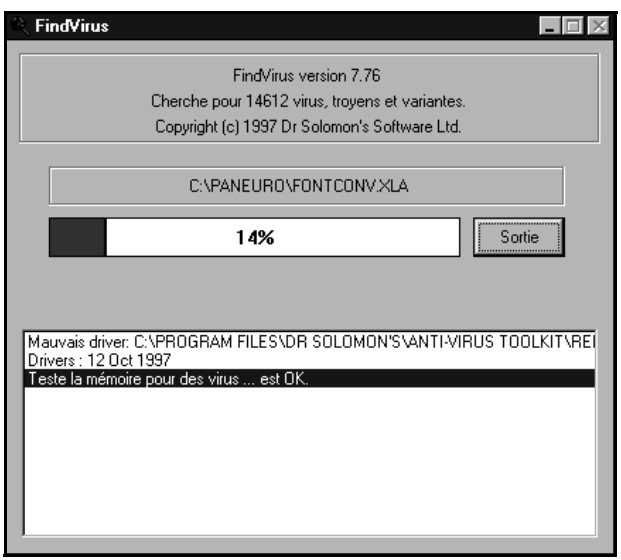
6. Sélectionnez **Renommer infectés** si vous souhaitez renommer des fichiers infectés qui n'ont pas pu être décontaminés plutôt que de les effacer. Si vous sélectionnez cette option, la première lettre de l'extension d'un fichier infecté sera alors "V". Par exemple, "FORMAT.COM" devient "FORMAT.VOM".

7. Sélectionnez **Effacer infectés** si vous souhaitez effacer des fichiers infectés qui n'ont pas pu être décontaminés plutôt que de les renommer.

8. Cliquez sur **Désinfecter**.

Conseil **Pour les utilisateurs de OS/2 :** cliquez sur **Réparer**.

La boîte de dialogue qui apparaît vous indique tout d'abord l'évolution du processus de désinfection, puis les résultats de celle-ci.



Vous pouvez annuler la désinfection à tout moment en cliquant sur **Sortie**. Dans ce cas, l'écran principal du Toolkit apparaît.

9. Une fois la désinfection terminée, notez les résultats et cliquez sur **Sortie** pour retourner à l'écran principal du Toolkit.

Attention

Pour les utilisateurs de Windows NT : si le nom d'utilisateur (avec lequel vous vous êtes connecté) ne fait pas partie du groupe "Administrateur", FindVirus ne peut pas accéder au secteur de partition et au secteur de boot du disque dur. Dans ce cas, les messages "Ne peut lire le secteur de partition" et "Ne peut lire le secteur de boot" apparaissent. Si vous devez désinfecter ces secteurs, reportez-vous alors à l'administrateur de votre système.

6.2 Remplacement des secteurs de boot

Conseil

Veuillez noter que cette option n'est pas disponible pour OS/2. Si vous travaillez sous OS/2 et que vous découvrez un virus dans le secteur de boot ou dans le secteur de partition, contactez le support technique de Dr Solomon's. Pour savoir comment contacter le support technique de Dr Solomon's, voir la section "Si vous avez besoin d'aide" à la page xiv.

Pour remplacer le secteur de boot d'une disquette :

Conseil

Les secteurs de boot des disques durs (par opposition aux secteurs de boot des disquettes), sur les systèmes fonctionnant sous Windows 3.x, Windows 95 ou DOS, doivent être désinfectés à l'aide de Magic Bullet. Pour plus d'informations sur l'utilisation de Magic Bullet, voir la section "Utilisation de Magic Bullet" à la page 1.

Si vous travaillez sous Windows NT et que vous découvrez un virus dans le secteur de boot ou dans le secteur de partition du disque dur, contactez le support technique de Dr Solomon's. Pour savoir comment contacter le support technique de Dr Solomon's, voir la section "Si vous avez besoin d'aide" à la page xiv.

1. Sélectionnez **Remplacement du secteur de boot** à partir du menu **Désinfecter**.

   La boîte de dialogue “Remplacer le secteur de boot” apparaît.

2. Sélectionnez la lettre représentant le lecteur souhaité.

3. Sélectionnez l’option **Détection automatique du disque** si vous souhaitez nettoyer un disque sans avoir à sélectionner son type. Le type du disque est sélectionné automatiquement avant la désinfection.

4. Cliquez sur **Remplacer**.

5. Vous voyez apparaître une boîte de dialogue vous indiquant que le disque a été nettoyé avec succès. Cliquez sur **OK**.

6. Si vous choisissez de ne pas sélectionner **Détection automatique du disque**, vous devez choisir un type de disque à partir de la liste proposée. Si le type de disque que vous avez choisi n’est pas le bon, la boîte de dialogue suivante apparaît :

Ne sélectionnez **Oui** que si vous êtes certain de vouloir remplacer le secteur de boot par le type de disque que vous avez choisi. Dans le cas contraire, cliquez sur **Non**. Si vous cliquez sur **Non**, vous revenez à la boîte de dialogue “Remplacement du secteur de boot”. A partir de cette dernière, sélectionnez **Détection automatique du disque** et cliquez sur **Remplacer**.

7. Si vous avez sélectionné **Oui** à l’étape précédente et, qu’après avoir remplacé le secteur de boot, vous ne pouvez plus accéder au disque :

Attention

Evitez d’écrire sur le disque. Si vous écrivez sur le disque et que le secteur de boot n’est pas le bon, des données peuvent être perdues.

Sélectionnez **Remplacer le secteur de boot** à partir du menu **Désinfecter**. Sélectionnez **Détection automatique du disque** à partir de la boîte de dialogue “Remplacement du secteur de boot” et cliquez sur **Remplacer**. Cette procédure vous permet d’écrire le secteur de boot approprié sur le disque. Vous pouvez désormais accéder normalement au disque.

Le message “Ne peut écrire le secteur de boot” peut signifier que le disque est protégé en écriture.

7. Documentation en ligne

Conseil

Veuillez noter que le présent chapitre ne concerne que les utilisateurs de Windows 3.x, Windows 95, Windows NT et OS/2 possédant l'anti-virus Dr Solomon's Toolkit pour Workstation sur CD-ROM.

Vous avez la possibilité de consulter le manuel d'utilisation de l'anti-virus Dr Solomon Toolkit pour Workstation sur le CD du Toolkit. Pour visualiser le manuel, vous avez besoin d'un lecteur PDF. Si vous ne disposez pas déjà d'un lecteur PDF, vous pouvez installer Adobe Acrobat Reader à partir du CD du Toolkit.

7.1 Windows 3.x

Conseil

Vous pouvez, si vous le souhaitez, installer Adobe Acrobat Reader et copier le manuel en même temps. Pour cela, voir les instructions à suivre dans “Installation de Adobe Acrobat Reader et reproduction du manuel en même temps” à la page 163.

Installation de Adobe Acrobat Reader

1. Démarrez votre ordinateur et chargez Windows 3.x. Lorsque le Bureau de Windows 3.x apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Sélectionnez le menu **Fichier,** puis la commande **Exécuter**.

3. Dans la boîte d’entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points. Tapez ensuite :

   ```
   \INSTALLATION
   ```

   et cliquez sur **OK**. Par exemple, tapez :

   ```
   D:\INSTALLATION
   ```

4. L’écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Manuel** et cliquez sur **Suivant**.

5. Dans la boîte de dialogue qui apparaît, sélectionnez **Installer Adobe Acrobat Reader**.

   Si vous souhaitez installer Adobe Acrobat Reader dans une autre langue, cliquez sur **Autre langue**. La boîte de dialogue suivante vous présente la liste des langues disponibles. Sélectionnez la langue dans laquelle vous voulez que soit installé Adobe Acrobat Reader, puis cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Installer Adobe Acrobat Reader** réapparaît. Cliquez sur **Suivant**.

6. La boîte de dialogue suivante confirme que vous avez choisi d'installer Adobe Acrobat Reader. Cliquez sur **Aller**.

7. Suivez les instructions qui apparaissent à l'écran.

Reproduction du manuel

1. Démarrez votre ordinateur et chargez Windows 3.x. Lorsque le Bureau de Windows 3.x apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Sélectionnez le menu **Fichier**, puis la commande **Exécuter**.

3. Dans la boîte d'entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points. Tapez ensuite :

   ```
   \INSTALLATION
   ```

   et cliquez **OK**. Par exemple, tapez :

   ```
   D:\INSTALLATION
   ```

4. Un écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Manuel** et cliquez sur **Suivant**.

5. Dans la boîte de dialogue qui apparaît, sélectionnez **Copier le manuel**. Sélectionnez le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel en spécifiant le chemin dans la boîte d'entrée en haut de cette boîte de dialogue. Vous pouvez spécifier le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel à l'aide de la fonction **Parcourir** ou en saisissant le chemin directement dans la boîte d'entrée.

6. Si vous souhaitez copier un manuel qui est écrit dans une langue étrangère, cliquez sur l'option **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle est écrit le manuel que vous souhaitez copier puis cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Copier le manuel** réapparaît. Cliquez sur **Suivant**.

7. La boîte de dialogue suivante confirme que vous avez choisi de copier le manuel. Cliquez sur **Aller**.

8. Suivez les instructions qui apparaissent à l'écran.

7.2 Windows 95

Conseil

Vous pouvez, si vous le souhaitez, installer Adobe Acrobat Reader et copier le manuel en même temps. Pour cela, voir les instructions à suivre dans “Installation de Adobe Acrobat Reader et reproduction du manuel en même temps” à la page 163.

Installation de Adobe Acrobat Reader

1. Démarrez votre ordinateur. Lorsque le Bureau de Windows 95 apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L’écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Manuel** et cliquez sur **Suivant**.

3. Dans la boîte de dialogue qui apparaît, sélectionnez **Installer Adobe Acrobat Reader**.

   Si vous souhaitez installer Adobe Acrobat Reader dans une langue étrangère, cliquez sur **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle vous souhaitez installer Adobe Acrobat Reader puis cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Installer Adobe Acrobat Reader** réapparaît. Cliquez sur **Suivant**.

4. La boîte de dialogue suivante confirme que vous avez choisi d’installer Adobe Acrobat Reader. Cliquez sur **Aller**.

5. Suivez les instructions qui apparaissent à l’écran.

Reproduction du manuel

1. Démarrez votre ordinateur. Lorsque le Bureau de Windows 95 apparaît, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L’écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Manuel** et cliquez sur **Suivant**.

3. Dans la boîte de dialogue qui apparaît, sélectionnez **Copier le manuel**. Sélectionnez le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel en spécifiant le chemin dans la boîte d'entrée en haut de cette boîte de dialogue. Vous pouvez spécifier le lecteur et / ou le répertoire dans lesquels vous souhaitez copier le manuel en utilisant la fonction **Parcourir** ou en saisissant le chemin directement dans la boîte d'entrée.

4. Si vous souhaitez copier un manuel qui est écrit dans une langue étrangère, cliquez sur **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle est écrit le manuel que vous souhaitez copier et cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Copier le manuel** réapparaît. Cliquez sur **Suivant**.

5. La boîte de dialogue suivante confirme que vous avez choisi de copier le manuel. Cliquez sur **Aller**.

6. Suivez les instructions qui apparaissent à l'écran.

7.3 Windows NT

Conseil

Vous pouvez, si vous le souhaitez, installer Adobe Acrobat Reader et copier le manuel en même temps. Pour cela, voir les instructions à suivre dans “Installation de Adobe Acrobat Reader et reproduction du manuel en même temps” à la page 163.

Installation de Adobe Acrobat Reader

1. Démarrez votre ordinateur et connectez-vous sur le Bureau de Windows NT avec un nom d’utilisateur qui soit dans le groupe administrateur. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L’écran de démarrage du CD du Toolkit apparaît si vous utilisez la version 4 de Windows NT.

Pour les utilisateurs de Windows NT version 3.51 :
Après avoir inséré le CD du Toolkit dans le lecteur de CD-ROM, sélectionnez le menu **Fichier** puis la commande **Exécuter**.

Dans la boîte d’entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points.Tapez ensuite :

```
\INSTALLATION
```

et cliquez sur **OK**. Par exemple, tapez :

```
D:\INSTALLATION
```

Vous allez voir apparaître l’écran de démarrage du CD du Toolkit.

3. Dans la boîte de dialogue qui apparaît, sélectionnez **Manuel** et cliquez sur **Suivant**.

4. Dans la boîte de dialogue qui apparaît, sélectionnez **Installer Adobe Acrobat Reader**.

   Si vous souhaitez installer Adobe Acrobat Reader dans une langue étrangère, cliquez sur **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle vous souhaitez installer Adobe Acrobat Reader puis cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Installer Adobe Acrobat Reader** réapparaît. Cliquez sur **Suivant**.

5. La boîte de dialogue suivante confirme que vous avez choisi d'installer Adobe Acrobat Reader. Cliquez sur **Aller**.

6. Suivez les instructions qui apparaissent à l'écran.

Reproduction du manuel

1. Démarrez votre ordinateur et connectez-vous au Bureau de Windows NT avec un nom d'utilisateur qui soit dans le groupe administrateur. Insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. L'écran de démarrage du CD du Toolkit apparaît si vous utilisez la version 4 de Windows NT.

Pour les utilisateurs de Windows NT version 3.51 :
Après avoir inséré le CD du Toolkit dans le lecteur de CD-ROM, sélectionnez le menu **Fichier** puis la commande **Exécuter**.

Dans la boîte d'entrée qui apparaît, tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points. Tapez ensuite :

```
\INSTALLATION
```

et cliquez sur **OK**. Par exemple, tapez :

```
D:\INSTALLATION
```

Vous allez voir apparaître l'écran de démarrage du CD du Toolkit.

3. Dans la boîte de dialogue qui apparaît, sélectionnez **Manuel** et cliquez sur **Suivant**.

4. Dans la boîte de dialogue qui apparaît, sélectionnez **Copier le manuel**. Sélectionnez le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel en spécifiant le chemin dans la boîte d'entrée en haut de cette boîte de dialogue. Vous pouvez spécifier le lecteur et / ou le répertoire dans lesquels vous souhaitez copier le manuel à l'aide de la fonction **Parcourir** ou en saisissant le chemin directement dans la boîte d'entrée.

5. Si vous souhaitez copier un manuel écrit dans une langue étrangère, cliquez sur **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle est écrit le manuel que vous souhaitez copier puis cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Copier le manuel** réapparaît. Cliquez sur **Suivant**.

6. La boîte de dialogue suivante confirme que vous avez choisi de copier le manuel. Cliquez sur **Aller**.

7. Suivez les instructions qui apparaissent à l'écran.

7.4 OS/2

Installation de Adobe Acrobat Reader

1. Démarrez votre ordinateur. Une fois que le Bureau du Gestionnaire d'amorçage est apparu, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Ouvrez une session de commandes OS/2.

   Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `D:` <Entrée>

   Tapez ensuite :

   `CD <`*`LANGUE`*`>\MANUALS\OS2` <Entrée>

   Par exemple, si vous installiez la version anglaise de Adobe Acrobat Reader, il vous faudrait taper :

   `CD ENGLISH\MANUALS\OS2` <Entrée>

   Veuillez noter que le nom de la langue doit apparaître dans la langue elle-même. Par exemple, si vous travaillez en Anglais mais que vous souhaitez installer la version française de Adobe Acrobat Reader, le nom du répertoire auquel vous avez besoin d'accéder est FRANÇAIS, et non pas FRENCH.

   Lorsque l'invite revient, tapez :

   `DIR` <Entrée>

Cette commande vous fournit la liste des fichiers contenus dans le répertoire. L'un des fichiers de cette liste est le fichier exécutable Adobe ; il possède l'extension .EXE. Pour démarrer le programme d'installation de Adobe, tapez :

`<NOM DU FICHIER>` <Entrée>

où *<NOM DU FICHIER>* est le nom du fichier exécutable Adobe possédant l'extension .EXE. Par exemple, si vous installiez la version anglaise de Adobe Acrobat Reader, le nom du fichier serait ARO2E30.

3. Suivez les instructions qui apparaissent à l'écran.

Reproduction du manuel

1. Démarrez votre ordinateur. Une fois que le Bureau du Gestionnaire d'amorçage est apparu, insérez le CD du Toolkit dans le lecteur de CD-ROM.

2. Ouvrez une session de commandes OS/2.

   Tapez la lettre représentant votre lecteur de CD-ROM suivie de deux points, puis appuyez sur la touche Entrée. Par exemple, tapez :

   `D:` <Entrée>

   Tapez ensuite :

   `CD <LANGUE>\MANUALS` <Entrée>

   Par exemple, si vous souhaitiez copier la version anglaise du manuel, vous taperiez :

   `CD ENGLISH\MANUALS` <Entrée>

   Veuillez noter que le nom de la langue doit apparaître dans la langue elle-même. Par exemple, si vous travaillez en Anglais mais que vous souhaitez copier un manuel écrit en Français, le nom du répertoire auquel vous avez besoin d'accéder est FRANÇAIS, et non pas FRENCH.

Lorsque l'invite revient, tapez :

`DIR` <Entrée>

Cette commande vous fournira le nom du fichier contenant le manuel. Il n'y aura qu'un seul fichier dans le répertoire.

3. Pour copier le manuel, tapez :

   `copy <NOM DU MANUEL>.PDF [<LETTRE CORRESPONDANT AU LECTEUR>:\<NOM DU REPERTOIRE>]` <Entrée>

   où *<NOM DU MANUEL>* est le nom du fichier contenant le manuel et où *[<LETTRE CORRESPONDANT AU LECTEUR>:\<NOM DU REPERTOIRE>]* sont le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel.

7.5 Installation de Adobe Acrobat Reader et reproduction du manuel en même temps

Conseil  Veuillez noter que cette option est disponible uniquement pour les utilisateurs de Windows 3.x, Windows 95 et de Windows NT.

1. Suivez les instructions spécifiques à la plate-forme que vous utilisez pour lancer le programme d'installation du CD du Toolkit.

2. L'écran de démarrage du CD du Toolkit apparaît. Dans la boîte de dialogue suivante, sélectionnez **Manuel** et cliquez sur **Suivant**.

3. Dans la boîte de dialogue qui apparaît, sélectionnez **Copier le manuel** et **Installer Adobe Acrobat Reader**.

4. Sélectionnez le lecteur et le répertoire dans lesquels vous souhaitez copier le manuel en spécifiant le chemin dans la boîte d'entrée en haut de cette boîte de dialogue. Vous pouvez spécifier le lecteur et / ou le répertoire dans lesquels vous souhaitez copier le manuel à l'aide de la fonction **Parcourir** ou en saisissant le chemin directement dans la boîte d'entrée.

5. Si vous souhaitez copier le manuel et installer Adobe Acrobat Reader dans une langue étrangère, cliquez sur **Autre langue**. La boîte de dialogue suivante présente la liste des langues disponibles. Sélectionnez la langue dans laquelle est écrit le manuel que vous souhaitez copier et dans laquelle vous souhaitez également installer Adobe Acrobat Reader et cliquez sur **OK**. La boîte de dialogue dans laquelle vous aviez sélectionné **Copier le manuel** et **Installer Adobe Acrobat Reader** réapparaît. Cliquez sur **Suivant**.

6. La boîte de dialogue suivante confirme que vous avez choisi de copier le manuel et d'installer Adobe Acrobat Reader. Cliquez sur **Aller**.

7. Suivez les instructions qui apparaissent à l'écran.

8. A propos des virus informatiques

Ce chapitre fournit des informations sur les virus, évoque les problèmes dont l'origine est parfois attribuée à tort aux virus et propose des mesures à prendre à l'encontre des virus.

Nombreux sont ceux qui paniquent lorsqu'ils entendent le mot *virus*. Sachez cependant que les infections de virus informatiques peuvent être évitées et qu'une infection rapidement découverte n'est pas particulièrement dommageable. Il est indispensable de prendre des mesures préventives, mais il est également nécessaire de savoir faire face à l'apparition d'un virus.

Dr. Solomon's Anti-Virus Toolkit détecte les virus et traite les infections de virus. Il détecte et supprime tout virus connu par la version actuelle du fichier driver. Il existe également une option de Toolkit qui recherche les nouveaux virus, qui n'ont pas encore été découverts.

8.1 Qu'est-ce qu'un virus ?

Les virus informatiques sont ainsi appelés car ils se reproduisent. Un virus est généralement conçu pour se reproduire à votre insu. Par exemple, il peut se rattacher au programme FORMAT et s'exécuter chaque fois que vous formatez une disquette. Il se peut que vous rencontriez des problèmes qui ne sont pas dûs à des virus. Certains de ces problèmes sont évoqués dans la rubrique "Autres problèmes potentiels."

La plupart des virus ont des effets secondaires délibérés ou intentionnels. Certains effets semblent inoffensifs. Le virus affiche simplement un message, fait tomber les lettres de l'écran ou joue un air. D'autres virus sont spécifiquement conçus pour détruire, écraser des données ou effacer des fichiers dans le disque dur. De plus, certains virus n'agissent pas comme leurs créateurs le prévoient à cause des bogues dans le logiciel. Les effets secondaires de ces virus sont alors imprévisibles. La plupart des virus restent dans la mémoire de votre ordinateur et peuvent perturber d'autres logiciels.

Aucun virus n'est inoffensif. Les virus vous font perdre votre temps, ils perturbent la mémoire de l'ordinateur et l'espace disque. Dr Solomon's Anti-Virus Toolkit peut vous aider à faire en sorte qu'aucun virus informatique n'infecte votre ordinateur.

Il existe différents types de virus tels que :

- les virus de fichiers
- les virus de macros
- les virus de secteurs de boot et de partition
- les virus multipartites

AIDE

Pour plus d'informations sur les virus et leurs caractéristiques, voir la rubrique "A propos des Virus" dans Toolkit Help.

8.2 Comment les virus se propagent-ils ?

Un virus se propage généralement par l'intermédiaire d'une disquette infectée ou lorsque des documents sont attachés au courrier électronique. A l'heure actuelle, les types de virus les plus courants sont les virus de macros et les virus de secteur de boot.

Les virus de macros peuvent se propager lors du transfert de fichiers infectés rattachés au courrier électronique ou par disquette ou encore lors du chargement d'un fichier internet infecté.

Les virus de secteurs de boot peuvent seulement se propager par l'intermédiaire d'une disquette. Les personnes qui utilisent des disquettes sur plusieurs ordinateurs augmentent ainsi les risques d'infection et de propagation du virus.

Certaines personnes pensent à tort que le shareware, les disquettes gratuites et les jeux sont la seule source de virus. Bien que les virus se propagent parfois par l'intermédiaire de ces types de logiciel (car souvent copiés), des virus ont également été détectés dans des logiciels emballés sous film

plastique, distribués par les plus grands éditeurs de logiciels et sur des disquettes livrées avec le matériel. C'est pourquoi il est indispensable de toujours procéder à un balayage de vos disquettes avant de les utiliser.

Les virus de fichiers peuvent également se propager lors du chargement de programmes infectés à partir des BBs et via Internet, ou lors du transfert de documents infectés attachés au courrier électronique. Vérifiez soigneusement tout logiciel transféré par réseau ou par liaison de communication avant de l'utiliser.

Une station de travail sur réseau peut être infectée de la même façon qu'un ordinateur autonome et un virus peut se propager très rapidement sur un réseau. Puisque les effets d'une infection informatique peuvent être particulièrement graves si un serveur de fichiers est infecté, vous devez veiller à protéger soigneusement les réseaux contre toute infection.

8.3 Autres problèmes potentiels

Lorsqu'un ordinateur est défaillant, on pense généralement qu'il s'agit d'un virus. Cependant, il existe plusieurs problèmes différents qui peuvent perturber votre travail et détruire des données. Certains de ces problèmes sont décrits ci-dessous.

Bogues

Un bogue est une anomalie involontaire contenue dans un programme. En fait, tout logiciel complexe contient des bogues. Des bogues de moindre importance ne provoquent que peu d'inconvénients. En revanche, des bogues principaux peuvent entraîner des pertes de données irréparables. Il n'existe aucun moyen de détecter les bogues. Par conséquent, l'unique protection efficace consiste à effectuer régulièrement une copie de sauvegarde de vos données.

Conflits entre logiciels de niveau inférieur

Les programmes de niveau inférieur fonctionnent directement sur disquette. Ils sont appelés ainsi car ils fonctionnent sous le niveau du système d'exploitation qui habituellement contrôle l'accès aux disquettes et applique certaines règles. Les programmes de niveau inférieur comprennent :

- des éditeurs de secteurs de disquettes.
- des programmes de mise en antémémoire des disquettes.
- des logiciels de compression de disquettes.
- des défragmenteurs.

Ces outils ne présentent aucun danger d'utilisation si vous n'en exécutez qu'un seul à la fois, mais des problèmes peuvent se produire si vous exécutez simultanément plusieurs outils de niveau inférieur. Lorsque plusieurs outils tentent d'accéder à un disque, des conflits aux conséquences graves peuvent en résulter. Ces outils devenant de plus en plus courants, ce type de problème est de plus en plus susceptible de se produire.

Afin éviter tout problème avec des outils de niveau inférieur :

- Effectuez toujours une copie avant d'utiliser tout utilitaire de disquettes.
- N'exécutez jamais plus d'un utilitaire à la fois.
- Evitez d'utiliser ces outils simultanément lorsque vous utilisez un logiciel résident en mémoire.
- Lisez toujours les manuels et tout fichier README fourni avec le produit. Si le fabricant a inclu des avertissements spécifiques, c'est généralement pour une bonne raison !

Troyens

Les troyens sont des programmes qui fonctionnent de façon inattendue et provoquent généralement des dommages. Ils sont moins répandus que les virus car ils ne se reproduisent pas, mais ils peuvent représenter une menace lorsqu'ils sont copiés. Beaucoup de personnes confondent les troyens et les virus : la disquette d'information sur le SIDA, souvent citée dans les médias comme exemple de virus est en réalité un troyen. Les virus contiennent parfois des troyens.

Il est peu vraisemblable que vous rencontriez un troyen si vous acquérez un logiciel de source fiable. Néanmoins, la meilleure défense contre les dommages que peuvent créer de tels programmes consiste à effectuer une copie de sauvegarde de votre système.

Le Toolkit cherche et identifie certains troyens connus et les traite de la même manière que les virus.

Bombes de temps et bombes logiques

Ce sont des types particuliers de troyens. Une bombe de temps est réglée pour se déclencher à une date précise alors qu'une bombe logique est déclenchée par un ensemble particulier de conditions telles le nombre de fichiers sur la disquette ou une séquence de caractères saisis particulière. Ces deux types de bombes sont généralement destructrices.

Virus farceurs

Certains programmes semblent agir de façon destructive sur votre ordinateur mais ne sont en réalité que des virus farceurs inoffensifs. Par exemple, un message peut s'afficher vous informant que le disque dur est sur le point d'être reformaté. Malheureusement, il est facile de réagir de manière excessive et de provoquer plus de dégâts en essayant de supprimer ce qui n'est pas, en réalité, un virus.

Erreur humaine

Lorsqu'un ordinateur est défaillant ou lorsque des données sont perdues, la cause d'erreur la plus probable n'est ni un virus ni un problème informatique mais une erreur humaine. Tout le monde commet des erreurs, comme d'appuyer sur la mauvaise touche ou entrer SUPPR *.* dans le mauvais répertoire, provoquant ainsi des conséquences irréparables.

Conseils

Les données stockées sur le disque dur de votre ordinateur sont bien plus importantes que le PC lui-même ou que les logiciels installés. Ces derniers peuvent, en effet, être réinstallés tandis que vous ne pouvez remplacer vos données que si vous en avez effectué une copie de sauvegarde.

8.4 Ce qu'il convient de faire

Bien que les virus constituent un réel problème, il faut relativiser leur importance. La cause la plus commune de perte de données vient en premier lieu d'une erreur humaine, puis d'une défaillance de matériel et ensuite de problèmes logiciels et des bogues. Les virus n'arrivent qu'en quatrième position.

Cependant, la mise en place d'une politique anti-virus directe vous aidera à protéger vos données contre toutes sortes de pertes y compris celles provoquées par un virus. Considérez attentivement les trois éléments de protection suivants :

- Prévention - pour limiter la propagation de virus.
- Détection - pour vous assurer qu'en cas de virus dans votre système, il soit découvert le plus vite possible.
- Récupération - pour vous assurer qu'en cas de perte de fichiers ou de dommages, ils puissent être récupérés le plus vite possible.

Copies de sauvegarde

Attention

La meilleure précaution à prendre contre toute perte de données consiste à effectuer régulièrement une copie de sauvegarde de vos données.

Il est risqué de ne pas effectuer régulièrement une copie de sauvegarde de vos données.

Pensez à vérifier régulièrement vos copies de sauvegarde et à vous assurer de pouvoir récupérer vos données à partir de ces copies de sauvegarde.

Assurez-vous que vous possédez des copies saines de tous vos fichiers exécutables sur disquette. Toutes vos disquettes de copies de sauvegarde ainsi que vos disquettes d'initialisation doivent être protégées en écriture.

Sources logicielles

Assurez-vous que tous vos logiciels proviennent de source fiable. Vérifiez que les logiciels se trouvent dans leur emballage d'origine.

N'utilisez jamais de logiciels pirate. Même si vous avez le sentiment d'être autorisé à utiliser temporairement une autre copie (par exemple, si vous avez laissé la copie dont vous possédez la licence autre part) n'oubliez pas que la copie peut vous exposer à l'infection d'un virus.

Des logiciels peuvent être installés sur votre ordinateur par l'intermédiaire de ports de communication et de portables. Veillez à transférer avec précaution des logiciels depuis ou vers un ordinateur portable et via des réseaux ainsi que lorsque vous chargez des fichiers à partir de BBs et d'Internet.

Disquettes et autres supports

Le risque de contamination informatique via disquette est particulièrement élevé, cependant de simples précautions peuvent diminuer ce risque.

- Ayez toujours des disquettes protégées en écriture, afin d'éviter la copie de virus.
- Ne laissez pas de disquette dans le lecteur lors de la mise hors tension de l'ordinateur. Cette mesure évite le lancement du système à partir d'une disquette susceptible d'être infectée par un virus de secteur de boot.
- En cas de lancement accidentel du système à partir d'une disquette non initialisable, éteignez l'ordinateur puis redémarrez-le au lieu de démarrer depuis le lecteur C:.
- Changez le paramètre CMOS de votre ordinateur afin qu'il démarre à partir du lecteur C: et non du lecteur A: (ceci n'est pas toujours possible avec des lecteurs SCSI).
- N'oubliez pas que des fichiers sur bande ont pu être infectés lors de la copie de sauvegarde.

Eviter le codage et la protection par mot de passe

Le codage et la protection par mot de passe permettent de protéger des fichiers en interdisant l'accès aux utilisateurs non autorisés.

Malheureusement, les programmes de balayage ne peuvent pas toujours accéder à des fichiers protégés de cette façon et certains virus peuvent être oubliés.

Lorsque un document n'est pas protégé par un mot de passe, il peut être analysé et vous pouvez y trouver les virus éventuels.

Cooperation de la part du personnel

Les employeurs ont besoin de la coopération volontaire de leurs employés lors de toute politique anti-virus. Si des membres du personnel pensent qu'ils seront réprimandés s'ils découvrent un virus, il est peu vraisemblable qu'ils signalent le problème.

Certaines sociétés ont essayé d'interdire les logiciels de jeux. Il est préférable de s'assurer que les jeux proviennent d'une source sûre et qu'ils soient vérifiés avant d'être utilisés. Il peut être utile de donner à une personne ou à une petite équipe la responsabilité de vérifier et de distribuer les logiciels de jeux.

Utilisation du Toolkit Anti-Virus

Les utilisations du Dr Solomon's Anti Virus Toolkit permettent d'effectuer une vérification rapide et facile de virus sur des ordinateurs individuels, et de répondre aux besoins d'anti-virus de grandes sociétés possédant des réseaux très étendus.

Le Toolkit Anti-Virus fournit un ensemble d'outils destinés à la détection ainsi qu'à la désinfection de virus. Il existe deux types de logiciels anti-virus.

- Un *scanner* est un programme de recherche de virus. Les scanners sont régulièrement mis à jour car de nouveaux virus apparaissent continuellement.
- Un *checksummer* détecte les modifications dans les fichiers. Il calcule une empreinte numérique unique, appelée checksum, pour chaque fichier à protéger. Le checksummer peut ensuite recalculer l'empreinte d'un fichier afin de contrôler les différences. Les fichiers exécutables ne changent généralement pas. Par conséquent, en cas de différence entre l'empreinte originale et celle recalculée, cela signifie qu'un virus peut être présent.

Dr Solomon's Anti Virus Toolkit contient :

WinGuard
WinGuard démarre automatiquement lors du démarrage de Windows et fonctionne en arrière plan. WinGuard balaie automatiquement les fichiers, les secteurs de boot et de partition lorsque ceux-ci sont accessibles. Si WinGuard détecte un virus, la tentative d'accès est infructueuse et vous êtes averti par un message d'alerte.

VirusGuard
VirusGuard est un scanner qui effectue des contrôles continus de virus en arrière-plan lorsque vous travaillez en mode DOS. VirusGuard balaie automatiquement les fichiers, les secteurs de boot et de partition lorsque ceux-ci sont accessibles.

FindVirus
FindVirus est un scanner que vous pouvez utiliser régulièrement pour balayer les disques durs ou toute nouvelle disquette. Il détecte et vous avertit de la découverte d'un virus connu par la version actuelle du fichier driver. Il contient également une option d'analyse heuristique qui recherche les codes dans les fichiers, ce qui peut indiquer la présence d'un virus auparavant inconnu.

FindVirus détecte et supprime les virus dans les fichiers, les secteurs de boot et de partition. Vous pouvez utiliser FindVirus pour balayer de nouvelles disquettes et des fichiers sur une machine "footbath", utilisée à cet effet. Le scanner FindVirus fonctionne très rapidement et peut être utilisé pour le balayage quotidien des disques durs.

ViVerify
ViVerify est un checksummer qui détecte les modifications des fichiers exécutables qui ont pu être provoquées par une infection de virus. Vous pouvez utiliser ViVerify au début afin de calculer une empreinte ou un checksum pour chaque fichier. Vous pouvez ensuite exécuter ViVerify régulièrement afin de recalculer cette empreinte et contrôler les modifications. Bien qu'une modification de fichier exécutable ne signifie pas nécessairement que ce fichier est infecté, le code exécutable ne change généralement pas. ViVerify vous informe de la possibilité d'un virus, même s'il s'agit d'un virus inconnu.

Magic Bullet

Magic Bullet est une disquette à partir de laquelle vous pouvez lancer le système et exécuter une version DOS de Find Virus.

Scheduler

Scheduler est un outil permettant d'exécuter des événements (recherche de virus, etc.) à des moments prédéterminés.

L'encyclopédie des Virus

L'encyclopedie des virus en ligne contient des informations sur les virus les plus courants détectés par Toolkit.

9. Dépannage et options avancées

Ce chapitre couvre les problèmes potentiels et les fonctions les plus techniques du Toolkit.

9.1 Dépannage

Cette section met en évidence certains problèmes rencontrés et offre une solution.

Message “Fichier messages.drv incorrect”

Lorsque vous tentez de démarrer le Toolkit, il se peut que le message “Fichier messages.drv incorrect” apparaisse.

Ceci s’explique par la présence de plusieurs fichiers “messages.drv” sur votre système. Vous avez, par exemple, installé certains composants du Toolkit sur un système comprenant déjà une version complète du Toolkit.

Il est recommandé de retirer du système tout fichier “messages.drv” n’appartenant pas au répertoire Toolkit. Vous pouvez trouver de tels fichiers dans un répertoire “s&stemp” ou dans la poubelle, par exemple.

Si le problème persiste, il est recommandé de désinstaller toutes les versions antérieures du Toolkit puis d’installer à nouveau la version actuelle.

Désinstallation sans un utilitaire de désinstallation

Vous devez désinstaller les Toolkits pour OS/2 et DOS à la main ; voir page 50 (OS/2) ou page 57 (DOS).

Si votre Toolkit pour Windows comprend un utilitaire de désinstallation, utilisez-le ; voir page 17 (Windows 3.x) ou page 35 (Windows 95).

Pour désinstaller une ancienne version du Toolkit pour Windows ne comprenant pas un utilitaire de désinstallation :

1. Si WinGuard est activé, désactivez-le.
2. Relancez le PC.
3. Effacez le répertoire Toolkit et ses fichiers.

L'installation du Toolkit arrête l'exécution de Windows 95

Après l'installation du Toolkit pour Windows 95, il se peut que Windows 95 démarre uniquement en mode Sécurité.

Cela vient peut-être de WinGuard. Essayez de désactiver WinGuard puis redémarrez votre PC.

Si Windows 95 continue à démarrer en mode sécurité, désinstallez le Toolkit comme indiqué à la page 35 puis contactez le support technique de Dr Solomon's. Pour plus d'informations sur la procédure à suivre pour contacter le support technique de Dr Solomon's, voir la section "Si vous avez besoin d'aide" à la page xiv.

Message "Insérez la disquette comportant \COMMAND.COM"

Lorsque vous travaillez dans DOS, il se peut que le message "Insérez la disquette comportant \COMMAND.COM dans le lecteur A" apparaisse.

Insérez une disquette système (d'initialisation). Appuyez ensuite sur n'importe quelle touche.

9.2 Options avancées d'installation

Dans l'écran d'accueil de l'installateur de CD, vous pouvez sélectionner "Options avancées d'installation". Vous trouverez plus de détails dans l'aide de l'installateur de CD. En résumé, vous pouvez :

- installer une version du Toolkit. Ceci implique une nouvelle installation, à l'inverse de l'option "Installation rapide" de l'écran d'accueil, qui met à jour la version antérieure du Toolkit (le cas échéant).
- installer des composants individuels du Toolkit.
- copier les fichiers d'installation du Toolkit entier ou des composants sélectionnés sur votre système. A partir de ces fichiers, vous pouvez installer le Toolkit ultérieurement. Cette option est utile si vous souhaitez par exemple, installer le Toolkit sur des postes de travail à partir d'un répertoire de réseau.
- copier les fichiers de mise à jour sur votre système. Vous pouvez utiliser ces fichiers pour mettre à jour des versions du Toolkit à partir de l'interface utilisateur du Toolkit.
- créer des ensembles de disquettes d'installation. Vous pouvez utiliser ces disquettes pour une installation ultérieure. Si vous possédez une licence sur site, vous pouvez utilisez ces disquettes pour installer le logiciel de Dr Solomon's sur des ordinateurs autonomes.

9.3 Utilitaires supplémentaires

Cette section comprend plus de détails sur les utilitaires DOS fournis avec le Toolkit.

CleanBoot

Sous Windows, vous pouvez utiliser l'option de menu "Remplacer le secteur de boot". Si vous travaillez sous DOS, vous devez employer l'utilitaire "CleanBoot".

1. Insérez la disquette suspecte.
2. Entrez la commande :

   `CLEANBOO [`*`drive`*`] [/`*`type`*`] [/`*`silent`*`]`

   où :

   `lecteur` est le lecteur contenant la disquette à nettoyer.

   `type` est à choisir dans le tableau suivant :

Type	Taille de la disquette	Capacité
1	5¼"	360 Ko
2	5¼"	1,2 Mo
3	3½"	720 Ko
4	3½"	1,44 Mo
5	3½"	2,88 Mo
A	Toute taille	Autodetect

   `silent` Supprime l'affichage à l'écran.

   En conjonction avec cette commande, il est recommandé d'utiliser le commutateur "`/oneonly`", car le programme risque d'attendre en vain une autre disquette à traiter, étant donné qu'il n'y aura aucune invite.

   Exemple de commande :

   ```
   CLEANBOO B: /4
   ```

   Celle-ci crée un secteur de boot nettoyé sur une disquette de 1,44 Mo (3½") située dans le lecteur B:.

3. Spécifiez le lecteur de disquette si on vous le demande (on ne vous le demandera pas si vous l'avez déjà spécifié dans la commande).

4. Spécifiez le type de disquette si on vous le demande (on ne vous le demandera pas si vous l'avez déjà spécifié dans la commande).

Conseil  Il est recommandé d'utiliser "Autodetect", car cette méthode de détection fait rarement des erreurs.

5. Si vous avez spécifié "Autodetect", confirmez la sélection automatique de disquette.

6. Répondez à l'invite "..ne correspond pas.....?" (s'affiche uniquement si le type spécifié ne correspond pas au type détecté).

7. Lorsque le processus est terminé, appuyez sur O pour nettoyer une autre disquette ou N pour sortir.

8. Tapez "dir" pour voir le contenu des disquettes puis vérifier les fichiers. Si les fichiers sont introuvables ou que les répertoires sont corrompus, il se peut que vous ayez copié le mauvais secteur de boot sur la disquette. Dans ce cas, essayez d'utiliser CleanBoot pour écrire un secteur de boot différent sur la disquette. Si vous avez ignoré à l'origine la détection automatique, essayez de l'accepter (elle peut souvent détecter l'identité normale du secteur de boot même si elle ne correspond pas à l'identité du secteur de boot figurant sur la disquette). Si ce n'est pas le cas, essayez de spécifier manuellement le type de disquette. Les fichiers ne sont pas perdus sauf si vous écrivez sur la disquette tout en ayant le mauvais secteur de boot.

Disquettes mal formatées

Une disquette mal formatée est une disquette formatée pour une capacité différente de celle pour laquelle elle a été conçue.

Par exemple, si une disquette de 360 Ko est formatée pour 1,2 Mo, lorsque vous exécutez CHKDSK, un message s'affiche indiquant 800-900 Ko d'espace utilisable et 300-400 Ko dans de mauvais secteurs. Si cette disquette est utilisée pour du stockage, les données risquent de devenir inaccessibles.

Le même problème peut survenir si une disquette de 720 Ko est formatée pour 1.44 Mo.

Ces problèmes proviennent des PC qui ne peuvent pas faire la différence entre les deux types de disquettes parce qu'ils ne détectent pas le second trou qui caractérise les disquettes de haute densité.

Si vous avez une disquette mal formatée, il est recommandé de transférer les données sur une autre disquette puis de reformater la première le plus vite possible.

CleanPart

Les utilitaires CleanPart et FindVirus suppriment tous deux les virus des secteurs de partition et de boot. Vous pouvez utiliser CleanPart si FindVirus a échoué.

Attention

CleanPart, utilisé de manière incorrecte peut endommager vos disquettes. Vous ne devez l'utiliser que sous la supervision du support technique de Dr Solomon's ; voir page xiv.

TKUTIL

Conseil

TKUTIL n'est pas fourni avec le Toolkit pour Windows NT. Les utilisateurs de Windows NT peuvent ignorer cette section.

Les utilitaires TKUTIL sont répertoriés dans le tableau ci-dessous et expliqués dans les sections suivantes :

Utilitaire	Objet
ADD	Ajoute du texte à un endroit spécifié dans un fichier texte.
ADUPDATE	Remplace un vieux fichier par un fichier plus récent portant le même nom.

Utilitaire	Objet
ADD WINGUARD	Ajoute des lignes aux fichiers .ini de Windows permettant de lancer WinGuard automatiquement lors du démarrage de Windows.
ALARM	Génère une alarme visible.
CPU	Indique le type de processeur principal.
DELETE	Supprime une ligne d'un fichier texte.
DISKSPACE	Indique l'espace libre sur le lecteur.
DRIVETYPE	Indique le type de lecteur en cours d'utilisation.
FORMFEED	Envoie une demande de saut de page à l'imprimante.
FROM	Supprime de vos fichiers système les références aux autres produits anti-virus.
GUARDCHECK	Indique si VirusGuard est installé ou non.
INIUPDATE	Synchronise les fichiers .ini.
LASTRUN	Indique la dernière utilisation en date du programme.
LOCK	Impose un démarrage à froid au PC.
MEMTYPE	Indique le type de mémoire installé.
MKDIR	Crée un nouveau répertoire.
MONTHDAY	Indique le jour du mois.
REGUARD	Réinitialise VirusGuard après le démarrage du réseau.
REMOVE WINGUARD	Supprime les lignes des fichiers .ini de Windows qui lancent WinGuard à la mise en route de Windows.
RETKEY	Indique les frappes ASCII en majuscule.

Utilitaire	Objet
RETSR	Réinitialise tous les programmes résidents (TSR) du Toolkit après démarrage du réseau.
RFCHECK	Indique si RingFence est installé.
SEARCH	Recherche une phrase donnée dans un fichier ASCII.
TECHFILE	Génére un fichier comprenant des informations sur le système.
TSRMAP	Renvoie la liste des programmes en mémoire.
TUNE	Active un indicatif sonore.
UPDATE	Remplace un vieux fichier par une version plus récente du même nom.
WEEKDAY	Renvoie le jour de la semaine.

Présentation du lecteur de disque

La commande DRIVETYPE renvoie le type du lecteur de disque en cours. Elle respecte la syntaxe suivante :

```
TKUTIL DRIVETYPE
```

Le niveau d'erreur renvoyé indique le type de lecteur :

Niveau d'erreur	Lecteur
1	Lecteur de disquette.
2	Lecteur de disque dur local.
3	Lecteur de réseau.

Présentation de l'espace disque disponible

La commande DISKSPACE renvoie un niveau d'erreur indiquant l'espace restant sur le lecteur, arrondi au nombre entier inférieur et exprimé en méga-octets.

Elle affiche aussi à l'écran l'espace disponible sur le lecteur en octet.

Présentation du processeur

La commande CPU renvoie le type de processeur. Elle respecte la syntaxe suivante :

```
TKUTIL CPU
```

Le niveau d'erreur renvoyé indique le type de processeur installé sur le PC :

Niveau d'erreur	Type de processeur
0	8086
2	80286
3	80386
4	80486
5	Pentium

Présentation du type de mémoire

La commande MEMTYPE renvoie le type de mémoire installée. Elle respecte la syntaxe suivante :

```
TKUTIL MEMTYPE
```

Le niveau d'erreur renvoyé indique le type de mémoire installée sur le PC, de la manière suivante :

Niveau d'erreur	Type de mémoire
0	Conventionnelle
1	EMS
2	XMS
3	EMS et XMS

Présentation des programmes résidents du Toolkit

La commande TSRMAP répertorie tous les programmes résidents en mémoire. Elle respecte la syntaxe suivante :

```
TKUTIL TSRMAP
```

Si vous utilisez DOS 5.0 ou une version ultérieure, vous pouvez utiliser la commande `MEM /C` qui a la même fonction.

Présentation de la toute dernière touche

La commande RETKEY renvoie le code ASCII en majuscule de la touche en cours. Vous pouvez utiliser celle-ci pour vérifier si l'utilisateur a répondu O ou N à une invite. La commande respecte la syntaxe suivante :

```
TKUTIL RETKEY
```

La touche est renvoyée en tant que niveau d'erreur.

Présentation de l'exécution d'un fichier séquentiel

La commande TKUTIL LASTRUN renvoie le nombre de jours écoulés depuis sa dernière exécution. Vous pouvez l'utiliser dans un fichier séquentiel pour savoir quand ce fichier a été utilisé pour la dernière fois. Utilisez-le, par exemple dans AUTOEXEC.BAT pour vous assurer d'effectuer un balayage uniquement au premier lancement de la journée (n'effectuez pas de balayage si `TKUTIL LASTRUN=0`).

Vous pouvez utiliser cette commande en conjonction avec TKUTIL WEEKDAY pour écrire un fichier séquentiel qui lance un balayage si vous l'exécutez un certain jour de la semaine et s'il n'y a pas eu de balayage effectué ce jour-là.

La syntaxe est :

```
TKUTIL LASTRUN <fichier>
```

où :

<fichier> est utilisé pour stocker les informations concernant la date. Si aucun nom de fichier n'est proposé, le fichier est appellé TKUTIL.DAT.

La commande renvoie le nombre de jours écoulés depuis la dernière utilisation du programme. Elle renvoie le niveau d'erreur 254 dans les cas suivants :

- Si le nombre de jours écoulés depuis la dernière utilisation du programme est supérieur à 254.
- Si le programme séquentiel n'a jamais été exécuté.
- Si elle ne trouve pas le fichier de données spécifié.

Création d'un nouveau répertoire

Vous pouvez utiliser la commande MKDIR pour créer un nouveau répertoire. La commande respecte la syntaxe suivante :

`TKUTIL MKDIR <répertoire>`

Les niveaux d'erreur renvoyés sont les suivants :

Niveau d'erreur	Signification
0	Répertoire créé.
1	Répertoire déjà existant.
2	Impossible de créer le répertoire.

Mise à jour des fichiers

Vous pouvez utiliser les commandes UPDATE ou ADUPDATE pour remplacer des fichiers existants par de nouvelles versions. Ces commandes respectent la syntaxe suivante :

`TKUTIL UPDATE <source> <destination> [/A] [/N]`

`TKUTIL ADUPDATE <destination> <source> [/A] [/N]`

où <*source*> et <*destination*> sont les noms d'accès de répertoires. Les fichiers du répertoire de destination sont remplacés par des fichiers du répertoire source plus récents et portant le même nom.

Vous avez le choix entre deux commutateurs :

/A	Met à jour les fichiers et ajoute les nouveaux fichiers du répertoire source au répertoire de destination.
/N	Copie uniquement les nouveaux fichiers du répertoire source dans le répertoire de destination.

Les options UPDATE et ADUPDATE renvoient les niveaux d'erreur suivants :

Niveau d'erreur	Signification
0	Rien de fait.
1	Fichiers mis à jour mais non copiés.
2	Fichiers copiés mais non mis à jour.
3	Fichiers copiés et mis à jour.
5	Répertoire source non valide.
6	Répertoire destination non valide.
11	Mémoire insuffisante.
12	Répertoires source et destination identiques.
14	Erreur lors de la copie.
17	Répertoire source vide (ADUPDATE uniquement).
18	Répertoire destination vide (UPDATE uniquement).
255	Echec du total de contrôle / version DOS.

Synchronisation des fichiers .ini

La commande INIUPDATE synchronise les fichiers .ini de Windows. Elle copie chaque section du fichier source .ini vers le fichier de destination .ini, en écrasant toute section du fichier de destination qui existe déjà.

Elle respecte la syntaxe suivante :

TKUTIL INIUPDATE *<nom_fichier1> <nom_fichier2>*

pour laquelle :

<filename1> est le nom du fichier source.

<filename2> est le nom du fichier de destination.

Ajout de texte dans un fichier

Vous pouvez utiliser la commande ADD pour ajouter du texte dans un fichier. Elle permet d' ajouter des entrées dans les fichiers AUTOEXEC.BAT ou CONFIG.SYS. Elle respecte la syntaxe suivante :

TKUTIL ADD *<fichier>* '*<texte>*' [/START][/END]
[/AFTER '*<phrase>*']

où :

<fichier> est le fichier dans lequel vous souhaitez ajouter du texte.

<texte> est le texte à ajouter.

Vous devez préciser l'un des commutateurs facultatifs, /START, /END ou /AFTER pour spécifier l'emplacement du texte.

Si vous précisez /AFTER et que <*texte*> se trouve déjà dans le fichier et après <*phrase*>, alors <*texte*> ne sera pas inséré. Si vous spécifiez /AFTER et que <*texte*> est déjà dans le fichier mais avant <*phrase*>, alors <*texte*> est inséré après <*phrase*> (par conséquent, le texte figurera deux fois).

La commande ADD renvoie les niveaux d'errreur suivants :

Niveau d'erreur	Signification
1	Paramètres incorrects.
2	Fichier introuvable.
3	Erreur lors de la lecture du fichier.
4	Erreur lors de l'écriture de fichier.
5	Le commutateur /AFTER a été inclus mais le texte est introuvable.

Exemples d'utilisation de la commande ADD :

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /COPY=FLOPPY' /START
```

ajoute GUARD /COPY=FLOPPY au début du fichier AUTOEXEC.BAT.

```
TKUTIL ADD C:\AUTOEXEC.BAT 'GUARD /REGUARD' /AFTER
'login'
```

ajoute GUARD /REGUARD au fichier AUTOEXEC.BAT après la ligne comprenant le texte "login".

Démarrage de WinGuard à l'initialisation

La commande ADD WINGUARD ajoute aux fichiers Win.ini et System.ini les lignes nécessaires pour démarrer WinGuard automatiquement à l'initialisation.

Elle ajoute "....(chemin)....\wgfe.exe"à la ligne "run" de Win.ini et ajoute "device=....(chemin)....\windguard.386" au début de la section "386Enh" de System.ini.

La commande respecte la syntaxe suivante :

`TKUTIL ADD WINGUARD <répertoire1> <répertoire2>`

où :

<répertoire1> est le répertoire dans lequel Toolkit a été installé ; il comprend le fichier “winguard.386”.

<répertoire2> est le répertoire Windows, qui comprend les fichiers “win.ini” et “system.ini”.

Suppression de texte d’un fichier

Vous pouvez utiliser la commande DELETE pour supprimer une ligne précise de texte d’un fichier. Elle respecte la syntaxe suivante.

`TKUTIL DELETE <fichier> '<texte>'`

où :

<fichier> est le fichier dans lequel du texte doit être supprimé.

<texte> est la ligne à supprimer.

La commande renvoie les niveaux d’erreur suivants :

Niveau d’erreur	Signification
255	Erreur de fichier ou erreur de ligne de commande.
1	Phrase introuvable.
0	Phrase trouvée.

Désactivation du démarrage de WinGuard à l'initialisation

La commande REMOVE WINGUARD supprime les lignes de "win.ini" et de "system.ini" qui lancent WinGuard à l'initialisation.

Elle respecte la syntaxe suivante :

`TKUTIL REMOVE WINGUARD <répertoire>`

où :

<répertoire> est le répertoire Windows, qui comprend "win.ini" et "system.ini".

Recherche de texte

Vous pouvez utiliser la commande SEARCH pour rechercher une ligne de texte précise dans un fichier. Elle respecte la syntaxe suivante :

`TKUTIL SEARCH <fichier> '<texte>'`

où :

<fichier> est le fichier à analyser.

<texte> est le texte à rechercher.

Les niveaux d'erreur renvoyés sont les suivants :

Errorlevel	Signification
255	Erreur de fichier ou erreur de ligne de commande.
1	Texte trouvé.
0	Texte introuvable.

Vérification de VirusGuard

Vous pouvez utiliser la commande GUARDCHECK pour vérifier si VirusGuard est installé. Elle respecte la syntaxe suivante :

```
TKUTIL GUARDCHECK
```

Les niveaux d'erreur renvoyés sont les suivants :

Niveau d'erreur	Signification
0	VirusGuard installé.
1	VirusGuard non installé.

Vérification de RingFence

Vous pouvez utiliser la commande RFCHECK pour vérifier si RingFence est installée. RingFence interdit l'utilisation de disquettes tant qu'elles n'ont pas fait l'objet d'un contrôle antivirus sur le PC réservé à ce contrôle. Cette autorisation permet d'interdire l'utilisation ou l'accés de tout logiciel infecté ou non. Pour plus d'informations sur RingFence, contactez Dr Solomon's.

La commande RFCHECK respecte la syntaxe suivante :

```
TKUTIL RFCHECK
```

Les niveaux d'erreur renvoyés sont les suivants :

Niveau d'erreur	Signification
0	RingFence installé.
1	RingFence non installé.

Détermination du jour de la semaine

Vous pouvez utiliser la commande WEEKDAY pour vérifier le jour de la semaine. Elle respecte la syntaxe suivante :

```
TKUTIL WEEKDAY
```

Elle renvoie un niveau d'erreur compris entre 1 et 7, comme suit :

Niveau d'erreur	Signification
1	Lundi
2	Mardi
3	Mercredi
4	Jeudi
5	Vendredi
6	Samedi
7	Dimanche

Détermination du jour du mois

Vous pouvez utiliser la commande MONTHDAY pour vérifier le jour du mois. Elle respecte la syntaxe suivante :

```
TKUTIL MONTHDAY
```

Elle renvoie un niveau d'erreur entre 1 et 31 indiquant le jour du mois.

Verrouillage du PC

Vous pouvez utiliser la commande LOCK pour imposer un démarrage à froid du PC si un problème survient. Elle désactive la combinaison Ctrl + Alt + Suppr et force l'utilisateur à tout éteindre. La commande LOCK respecte la syntaxe suivante :

```
TKUTIL LOCK
```

Activation d'une alarme

Vous pouvez utiliser la commande ALARM pour générer une alarme en cas de problème. Elle respecte la syntaxe suivante :

```
TKUTIL ALARM
```

Cette commande fait clignoter l'écran. L'horaire de l'alarme apparaît au centre de l'écran.

Indicatif sonore

Vous pouvez utiliser la commande TUNE pour activer un des quatre indicatifs sonores. Cette commande respecte la syntaxe suivante :

```
TKUTIL TUNE n
```

où *n* est un nombre compris entre 1 et 4.

Suppression d'autres kits antivirus

Si vous avez utilisé auparavant d'autres logiciels antivirus, vous pouvez supprimer toute référence à ces derniers à partir de vos fichiers système en utilisant la commande FROM. Cette commande respecte la syntaxe suivante (remarquez qu'il n'y a pas d'espace après "FROM') :

```
TKUTIL FROM[CPAV][NAV][MSAV] [<drive\directory>]
```

où :

`CPAV`	supprime toutes les références au kit antivirus de Central Point.
`NAV`	supprime toutes les références au kit antivirus de Norton.
`MSAV`	supprime toutes les références au kit antivirus de Microsoft.
<drive\directory>	est l'emplacement où le kit est installé. Si vous ne le précisez pas, une invite vous demande de le faire.

Les niveaux d'erreur renvoyés sont les suivants :

Niveau d'erreur	Signification
255	Erreur fichier.
0	Suppression des références réussie.

Envoi d'un saut de page à l'imprimante

La commande FORMFEED envoie un caractère de saut de page à l'imprimante. Elle respecte la syntaxe suivante :

```
TKUTIL FORMFEED
```

Les niveaux d'erreur renvoyés sont les suivants :

Niveau d'erreur	Signification
1	Aucune imprimante connectée.
0	Saut de page réussi.

Redémarrage de VirusGuard

Vous pouvez avoir besoin d'utiliser la commande REGUARD si vous exécutez VirusGuard sur un réseau. Si vous démarrez VirusGuard avant de vous connecter au réseau, il se peut que VirusGuard fonctionne mal. Veillez à ce qu'il soit activé à nouveau. La commande REGUARD active à nouveau VirusGuard. Elle respecte la syntaxe suivante :

```
TKUTIL REGUARD
```

Nous vous conseillons de placer cette commande à la fin de la séquence de commandes de connexion.

Redémarrage des programmes résidents (TSR)

Il se peut que vous ayez besoin d'utiliser la commande RETSR si vous exécutez VirusGuard sur un réseau. Elle active à nouveau les programmes résidents après la connexion au réseau en s'assurant qu'ils fonctionnent correctement. La commande respecte la syntaxe suivante :

```
TKUTIL RETSR
```

Nous vous conseillons de placer cette commande à la fin de la séquence type de connexion. Remarquez que si vous utilisez RETSR, vous n'avez pas besoin d'utiliser REGUARD en même temps.

Présentation des informations techniques

La commande TECHFILE génère un fichier d'informations sur le système comprenant notamment le contenu de vos fichiers AUTOEXEC.BAT et CONFIG.SYS. Il se peut que le personnel du support technique Dr Solomon's vous le demande si vous avez un problème.

La commande respecte la syntaxe suivante :

```
TKUTIL TECHFILE <fichier>
```

où <*fichier*> précise le fichier à créer. Si vous ne fournissez pas de nom de fichier, le fichier sera intitulé TECHDATA.S&S.

WTKUTIL

Conseil

L'utilitaire WTKUTIL n'est pas fourni avec le Toolkit pour Windows NT. Les utilisateurs de Windows NT peuvent ignorer cette section.

WTKUTIL est un utilitaire de gestion de votre installation WinGuard. Il comprend un certain nombre de commandes comportant chacune une fonction différente.

Ajout de WinGuard

Il existe une fonction de modification du registre qui permet à WinGuard de démarrer automatiquement en même temps que Windows 95. Vous pouvez utiliser cette fonction si vous n'avez pas choisi d'activer WinGuard lors de l'installation du Toolkit.

Cette commande respecte la syntaxe suivante :

```
WTKUTIL ADD WINGUARD <toolkitpath>
```

où *<toolkitpath>* est le chemin complet d'accès au répertoire Toolkit (comprenant l'exécutable WinGuard).

Suppression de WinGuard

Il existe une fonction qui équivaut à désactiver WinGuard en utilisant son programme de configuration. Le registre est modifié de manière à ce que WinGuard ne démarre plus automatiquement en même temps que Windows 95.

Utilisez la commande :

```
WTKUTIL REMOVE WINGUARD
```

Vérification de l'exécution de WinGuard

Il existe une fonction qui affiche un message indiquant si WinGuard est activé ou non. Elle renvoie le niveau d'erreur 0 si WinGuard est chargé et 1 dans le cas contraire.

Utilisez la commande :

```
WTKUTIL WINGUARDCHECK
```

Enregistrement des paramètres d'option

Il existe une fonction d'enregistrement des paramètres d'option WinGuard actuels dans un fichier, en format texte. Le niveau d'erreur renvoyé est 255 si la section du fichier ou du registre ne peut être ouverte et 0 si l'opération est réussie. Le fichier comprend le détail des options modifiées par rapport aux paramètres par défaut.

Utilisez la commande :

```
WTKUTIL SAVESETTINGS WINGUARD <nom_fichier>
```

Rétablissement des paramètres d'option

Il existe une fonction de remplacement des paramètres d'option en cours par les paramètres antérieurs enregistrés dans un fichier. Le niveau d'erreur renvoyé est 255 si vous ne pouvez pas ouvrir le fichier et 0 si l'opération est réussie.

Utilisez la commande :

```
WTKUTIL LOADSETTINGS WINGUARD <nom_fichier>
```

Comparaison des paramètres d'option

Il existe un fonction de comparaison des paramètres WinGuard en cours avec ceux stockés dans un fichier précis. Le niveau d'erreur renvoyé est 1 si les paramètres sont les mêmes, 2 s'ils sont différents et 255 si la section du fichier ou du registre ne peut être ouverte.

Utilisez la commande :

```
WTKUTIL CHECKSETTINGS WINGUARD <nom_fichier>
```

Obtention d'un récapitulatif des commandes

Vous pouvez obtenir un récapitulatif des commandes disponibles en utilisant la commande :

```
WTKUTIL /?
```

ou

```
WTKUTIL /HELP
```

9.4 Niveaux d’erreur FindVirus

FindVirus définit un niveau d’erreur à chaque utilisation. Vous pouvez utiliser le niveau d’erreur pour effectuer des branchements conditionnels dans les fichiers séquentiels.

Pour obtenir un niveau d’erreur correct, il vous faut utiliser la commande suivante dans le fichier séquentiel :

```
start /w wfindv32 [<path>[\<file>]] [/switch]
[/switch]...
```

En utilisant le commutateur “ /exterror” (voir page 200), vous pouvez choisir un ensemble varié de niveaux d’erreur.

L’ensemble standard de niveaux d’erreur est le suivant :

255 Exécution interrompue par l’utilisateur.

2 Virus trouvé

1 Un problème autre qu’un virus est survenu. Il peut s’agir, par exemple, d’un fichier en cours de codage ou d’utilisation par une application ou de l’incapacité de FindVirus à reconnaître un commutateur précis.

0 Aucun problème rencontré.

Niveaux d’erreur FindVirus étendus

Vous obtenez des niveaux d’erreur étendus en utilisant le commutateur “ /exterror” dans la commande du fichier séquentiel permettant de démarrer FindVirus (voir page 200).

Les niveaux d’erreur étendus sont les suivants :

255 Exécution interrompue par l’utilisateur.

48 Virus de fichier, dropper ou virus test trouvé.

47 Virus de secteur de partition trouvé.

46	Virus de secteur de boot trouvé.
45	Virus trouvé en mémoire.
44	Troyen trouvé.
22	Echec du total de contrôle par le driver.
21	Fichier driver introuvable.
20	Echec de la vérification de l'intégrité.
11	Programme farceur trouvé.
10	Fichiers compressés trouvés.
1	Problème autre que virus rencontré. Il peut s'agir, par exemple, d'un fichier en cours de codage ou d'utilisation par une autre application, ou de l'incapacité de FindVirus à reconnaître un bouton précis.
0	Aucun problème rencontré.

Glossaire

AUTOEXEC.BAT	Fichier exécuté lors de chaque démarrage de votre ordinateur (non applicable à Windows NT). Pour OS/2, le fichier AUTOEXEC.BAT est utilisé chaque fois que vous exécutez une session Win-OS/2 ou DOS.
BBS	Bulletin Board System. Système de messagerie électronique utilisé pour envoyer des messages et transférer des fichiers.
BIOS	Basic Input/Output System. Programmes permanents utilisés pour charger le système d'exploitation lors du démarrage.
bogue	Anomalie involontaire dans un programme.
bombe de temps	Type de *troyen* qui se déclenche à une date précise.
bombe logique	Type de *troyen* déclenché par un ensemble de circonstances précis.
boot	Démarrage de l'ordinateur.
CARO	Computer Anti-Virus Researchers Organization (Organisation rassemblant des chercheurs d'antivirus). Plusieurs employés de Dr Salomon's sont membres de cette organisation.
compresseur de disque	Programme qui stocke des fichiers sous une forme compressée afin de libérer de l'espace sur le disque dur.

CONFIG.SYS	Fichier exécuté lors de chaque démarrage d'un ordinateur (non applicable à Windows NT).
copie de sauvegarde	Copie de vos données conservée au cas où votre copie de travail serait perdue ou endommagée.
défragmenteur	Programme qui réorganise un disque dur de façon à ce que les différentes *unités d'allocation* de chaque fichier soient, dans la mesure du possible, stockées de manière contigüe. L'efficacité du disque s'en trouve améliorée.
détecteur de modifications	Programme qui recherche des virus en vérifiant les modifications effectuées dans des *fichiers executables*. ViVerify est un exemple de détecteur de modifications.
disquette d'initialisation	Disquette contenant des fichiers du système d'exploitation utilisables pour démarrer l'ordinateur.
dossier	Subdivision logique d'un disque permettant d'organiser les fichiers en les regroupant.
dossier racine	Dossier d'entrée au sommet d'un disque dans lequel tous les autres dossiers et fichiers sont stockés.

dropper	Programme qui n'est pas lui-même un virus et qui n'est pas non plus infecté par un virus mais qui, lors de son exécution, installe un virus en mémoire sur un disque ou dans un fichier. Les "droppers" sont souvent utilisés pour véhiculer un virus de manière efficace et parfois dans un but de sabotage.
EICAR	European Institute for Computer Anti-Virus Research (Institut européen de recherche sur les antivirus). Dr Solomon's est membre de cet institut.
empreinte	Identificateur numérique propre à chaque fichier, utilisé comme *détecteur de modifications* pour contrôler les modifications survenues dans les fichiers exécutables. Synonyme de somme de contrôle.
fausse alerte	Détection d'un virus alors qu'il n'y en a aucun.
fichier COM	*Fichier executable* dont l'extension est COM.
fichier contaminé	Fichier contenant un virus.
fichier de macro	Fichier contenant des instructions qui indiquent les actions devant être effectuées par le programme d'application.
fichier driver	Fichier utilisé par le Toolkit pour activer la détection et annoncer la présence de virus.
fichier EXE	*Fichier exécutable* dont l'extention est EXE.

fichier exécutable	Fichier contenant un programme qui peut être exécuté en saisissant son nom sur la ligne de commande DOS ou en cliquant sur son nom dans la liste des programmes affichée par l'Explorateur.
fichier SYS	Fichier, généralement un *pilote de périphérique*, dont l'extension est SYS.
formater	Méthode permettant de préparer un disque à l'aide de la commande FORMATER afin d'y enregistrer des fichiers.
furtivité	Caractéristique d'un virus qui essaie d'échapper à la détection. Les virus furtifs perturbent les *interruptions de programmes BIOS* et DOS afin de dissimuler leur présence.
GDE	Generic Decryption Engine. Elément de FindVirus qui permet d'identifier jusqu'aux virus polymorphes cryptés les plus complexes.
hexadécimal	Représentation en base 16.
infecteur rapide	Virus de fichier qui contamine les programmes à leur ouverture, lors de leur copie ou lors de leur exécution.
logiciel du domaine publique	Logiciel que vous pouvez copier et distribuer en toute légalité.
Master Boot Record	Secteur de partition d'un disque dur.
mise à jour	Nouvelle version du Toolkit qui a été révisée afin de détecter des virus récemment découverts. Les mises à jour sont disponibles trimestriellement ou mensuellement.

ordinateur de désinfection cobaye	Ordinateur utilisé pour vérifier si les fichiers et les disquettes entrants sont contaminés par un virus. Synonyme d'*Ordinateur footbath*.
ordinateur footbath	Ordinateur utilisé pour vérifier si les fichiers et les disquettes entrants sont contaminés par un virus. Synonyme d'*Ordinateur de désinfection cobaye*.
pilote de périphérique	Programme utilisé pour contrôler les composants d'un équipement relié à un ordinateur, tels que les lecteurs de disques et les imprimantes.
programme batch	Fichier comprenant un ensemble de commandes exécutées par la saisie d'une seule commande. Les fichiers séquentiels portent l'extension BAT.
programme de virus farceurs	Programme trompeur qui n'est pas à proprement parler un virus mais qui peut parfois en contenir un.
protection en écriture	Permet d'assurer que des fichiers ne pourront pas être écrits sur un disque. Il suffit d'apposer un autocollant sur l'encoche d'une disquette de 5"¼ pour la protéger en écriture. Sur une disquette de 3"½, il suffit de faire glisser le loquet coulissant afin d'évider un petit carré.
pseudonyme	Autre nom sous lequel est connu un *virus*.
répertoire	voir "Dossier".
résident en mémoire	Programme qui reste dans la mémoire de l'ordinateur lorqu'il a été exécuté. Synonyme de *TSR* ou *VxD*.

sain	Ne comprenant plus de virus.
scanner	Programme de détection de virus, tel que FindVirus, qui recherche la présence de virus.
scanner heuristique	Elément de FindVirus qui vérifie dans les fichiers les codes suspects pouvant indiquer la présence d'un nouveau virus.
secteur de boot	Partie de tout disque ou disquette lu(e) par l'ordinateur lors de son initialisation.
shareware	Logiciel contributif que vous pouvez copier en toute légalité, mais que vous devez payer si vous décidez de l'utiliser.
secteur de partition	Première partie d'un disque dur qui est lue. Elle comporte l'emplacement de chaque partition et le nombre de secteurs de chacune d'entre elles.
troyen	Programme dont l'action est inattendue. Les troyens ne sont pas des virus car ils ne se reproduisent pas, mais ils provoquent souvent des dégâts et sont détectés par le Toolkit.
TSR	Terminate and Stay Resident. Programme DOS qui reste en mémoire après son exécution. Reportez-vous à *résidents en mémoire*.
variante	Variante d'un virus, généralement due à l'extension du code d'un virus déjà existant.
virus	Programme qui se reproduit.

virus de fichier	Virus qui contamine les *fichiers exécutables*. Lors de l'exécution d'un programme, le virus se reproduit. La plupart des virus de fichier sont *résidents en mémoire*.
virus de secteur de boot	Virus transmis dans le *secteur de boot* d'une disquette. Les virus de secteur de boot contaminent des secteurs de boot des disques durs et souvent les *secteurs de partition* par la même occasion.
virus de secteur de partition	Virus qui remplace le *secteur de partition* normal d'un disque dur.
virus écrasant	Virus qui recouvre les données de chaque fichier contaminé.
virus multipartite	Virus qui utilise une combinaison de techniques pour contaminer, par exemple, à la fois les fichiers et les *secteurs de boot*.
virus polymorphe	Virus qui tente d'échapper à la détection des scanners en faisant en sorte de ne pas avoir une structure fixe d'octets. Le Toolkit sait détecter les virus polymorphes grâce au GDE (Generic Decription Engine).
VxD	Virtual device driver. Programme Windows qui reste en mémoire après son exécution. Voir *résident en mémoire*.

Index