ThunderBYTE Anti-Virus for Windows

Sommaire de l'Aide

Tapez F1 si vous désirez apprendre à utiliser cette Aide

Félicitations ! L'achat des utilitaires ThunderBYTE Anti-Virus (TBAV) est la première étape de l'édification d'un puissant système de sécurité anti-viral qui va protéger votre ordinateur. L'utilisation de TBAV pour définir une défense appropriée est de votre ressort. Pour cela, nous vous recommendons de lire ce manuel en entier, afin de prendre connaissance de toutes les mesures de sécurité qui vous sont proposées.

NOTE : Si vous n'avez pas encore enregistré TBAV Windows, vous n'êtes autorisé à tester le programme durant une période de trois semaines. Passées ces trois semaines, certaines fonctionnalités de TBAV Windows seront désactivées. De ce fait, certaines informations contenues dans ce fichier d'aide deviendront caduques après la-dite période d'essai.

Ce fichie d'aide contient les chapitres suivants :

Introduction à TBAV Windows

Cette partie contient les informations de base sur TBAV Windows, ainsi que la stratégie anti-virus suivie par TBAV Windows. Vous trouverez également les termes de la licence TBAV.

Si vous désirez contacter les commerciaux ou techniciens ThunderBYTE, vous trouverez leurs adresses dans cette section.

Installer TBAV Windows

Cette partie du fichier d'aide traite de l'installation et la configuration de TBAV Windows.
Il est fortement recommendé de devenir famillier avec le contenu de cette section.

Lancement de TBAV Windows

Il est conseillée de lire ce chapitre afin de devenir famillier avec le lancement et l'utilisation de TBAV Windows.

Utiliser TBAV Windows

L'interface utilisateur de TBAV Windows est entièrement décrite dans ce chapitre. La lecture de cette section est indispensable pour tirer le maximum de TBAV Windows.

Utiliser le module TbScan

Le fonctionnement de TbScan, le module de contrôle de TBAV Windows est décrit dans ce chapitre. Toutes les options et paramètrages y sont expliqués, ainsi que des informations sur les méthodes utilisées de détection des virus.

Utiliser le module TbSetup

TbSetup est un outil indispensable si vous désirez optimiser le fonctionnemment de TBAV Windows. Le module TbSetup calcule les empreintes de chaque fichier exécutable de votre ordinateur.

Utiliser le module de recherche en tâche de fond

Vous pouvez configurer TBAV Windows pour fonctionner en tâche de fond. Cela permet de lancer périodiquement des détections de virus sur votre disque dur.

Utiliser le module de surveillance des Entrées/Sorties de fichiers

Ce module effectue une recherche de virus sur chaque fichier copié, désarchivé, téléchargé, etc.

Utiliser le module de Suivi des Applications Exécutées

Un virus ne s'active que lorsqu'une application infectée est exécutée.
TBAV Windows peut être configuré de façon à analyser toute application lancée sous Windows avant son lancement effectif.

Informations Diverses

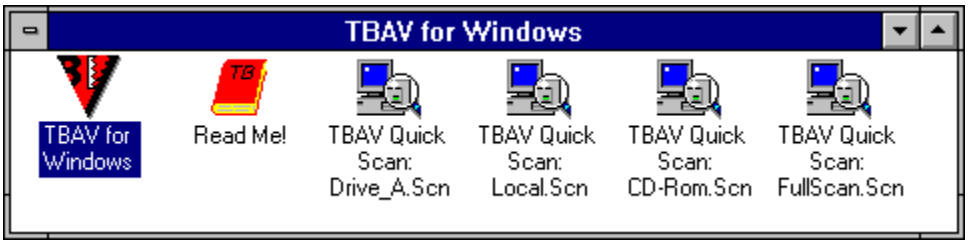
Cette section comprend diverses informatiuons complémentaires sur TBAV pour Windows
Cela inclut des renseignements sur la base de données de virus, la configuration générale de TBAV, l'interfaçage réseau et l'option de mise à jour automatique.

Prise en main de TBAV Windows

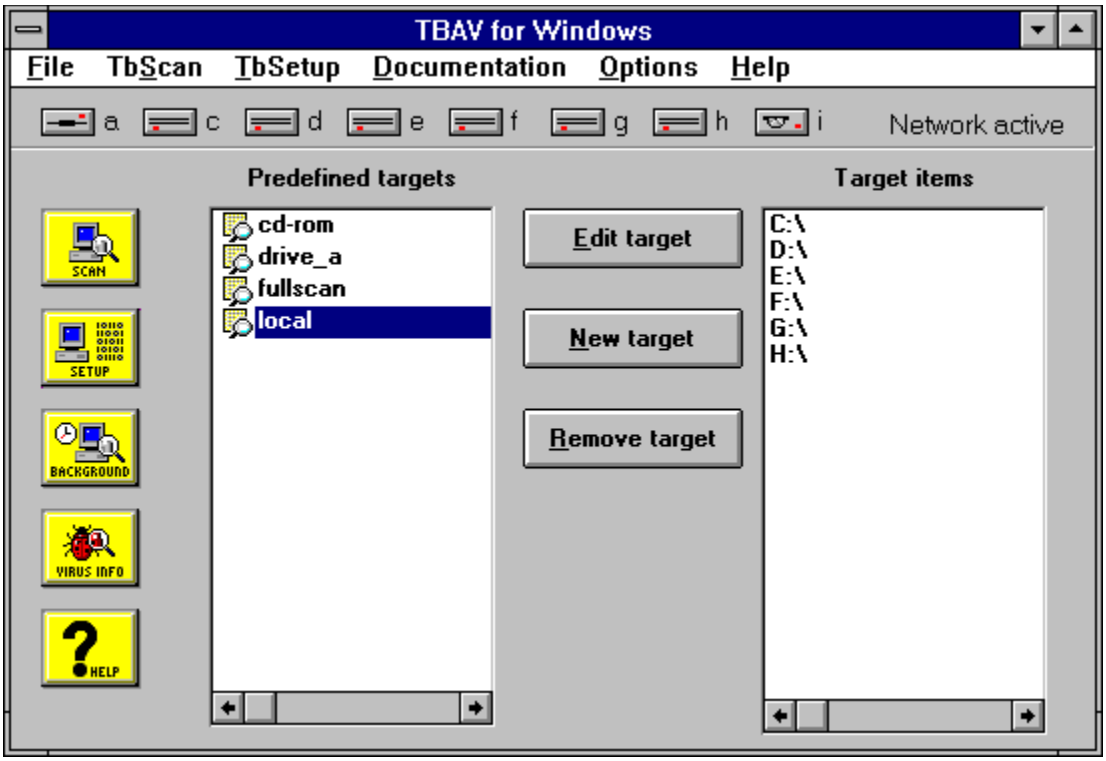
Ce section présente les principales caractéristiques de TBAV et vous indique comment maîtriser TBAV Windows en un minimum de temps. Pour toute information sur l'installation de TBAV Windows, veuillez choisir la rubrique : **Installer TBAV Windows**

Lancement de TBAV Windows

Durant l'installation, un nouveau groupe de programmes similaire à celui affiché ci-dessous, sera créé :



Comme toute application Windows, le lancement de TBAV Windows s'effectue en double-cliquant sur son icone dans le groupe de programmes du Gestionnaire de Programmes. Après quelques secondes, la fenêtre d'initialisation apparaît.
Lors de son lancement, TBAV Windows, analyse la mémoire de votre ordinateur afin de détecter un virus actif en mémoire. Durant ce test, la jauge en bas de la fenêtre progresse de 0 % à 100 %.
Lorsque TBAV a terminé l'analyse de la mémoire, la fenêtre principale de TBAV Windows, similaire à celle ci-dessous s'affiche (votre écran peut être légérement différent en fonction de la configuration de votre système et de votre version) :



Cette fenêtre est divisée en quatre parties :

1. La barre de menu, en haut de la fenêtre (contenant les menus Fichier, TbScan, TbSetup, Documentation, Options et Aide).
2. La barre des disques, affichant tous les disques disponibles sur votre ordinateur (dans notre exemple, A: et C: jusqu'à H:).
3. Cinq icones d'accès rapide, permettant d'accèder rapidement aux modules TbScan, TbSetup, à la configuration de la surveillance en tâche de fond, à la base d'information des virus, et à l'aide hypertexte.
4. Deux fenêtres Unités prédéfinies et Unités à contrôler avec trois boutons au milieu affichant les scenarii de détection.

Travailler avec TBAV Windows

La partie suivante de ce manuel, Utiliser TBAV Windows, détaille l'utilisation de TBAV Windows, mais cette petite section vous donnera un aperçu rapide des possibilités de TBAV Windows.

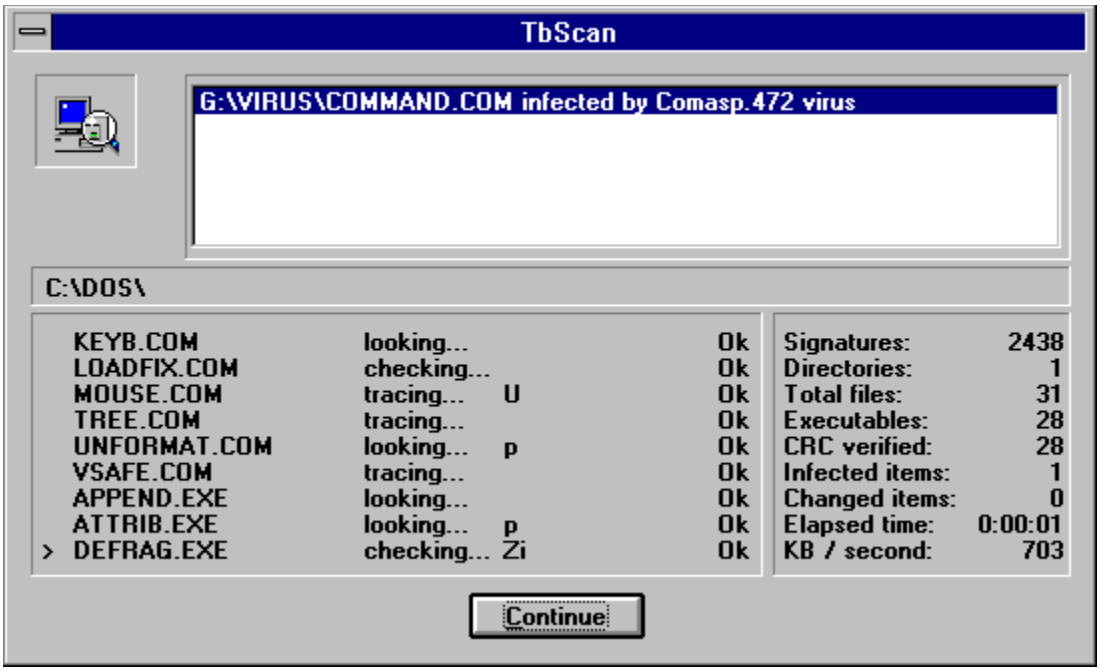
Effectuer une Recherche de virus

Pour effectuer une recherche de virus sur un disque ou un répertoire donné, vous pouvez :

- soit sélectionner un objet dans la fenêtre Unités prédéfinies (par exemple local) et cliquer sur l'icone scan à gauche de l'écran,
- soit douvle-cliquer avec la souris sur un objet de la fenêtre Unités prédéfinies.

NOTE: Reportez-vous à la section sur les unités à contrôler du chapitre Utiliser TBAV pour plus de détails sur la création, la modification et la suppression des unités à contrôler.

La fenêtre de dialogue de TbScan apparaît et affiche la progression de l'analyse des fichiers de l'unité sélectionnée (cf ci-dessous) :



Si TBAV ne détecte pas de virus, une boite de dialogue vous en informant apparaît à la fin de l'analyse. Tapez sur la bouton OK pour terminer la détection.
Dans le cas où TbScan détecerait un virus, reportez-vous à **Detection d'un Virus**.

Trouver de l'Aide

Il y a plusieurs moyens d'obtenir de l'aide quand vous travaillez avec TBAV Windows :

1. Sélectionnez le bouton “Aide”. Il affiche la boîte de dialogue d'aide de Windows que vous connaissez bien. Si vous sélectionnez le bouton “Rechercher”, par exemple, la boîte de dialogue “Rechercher” apparaît et vous permet de localiser rapidement la rubrique sur laquelle vous souhaitez être aidé.
2. Sélectionnez le menu Aide, puis sélectionnez Index de l'aide. Cela affiche également la boîte de dialogue “Aide de Windows”.
3. Sélectionnez le menu Documentation, puis sélectionnez “Manuel TBAV” qui affiche la version sur disque de ce manuel.
   CONSEIL : A la place de l'afficheur interne, vous pouvez utiliser un autre outil de consultation pour voir le manuel ou d'autres fichiers. Pour définir votre propre outil de consultation, par exemple Windows Write, sélectionnez le menu Options, puis sélectionnez Configuration de TBAVWIN. Désactivez l'option “Utilise l'afficheur interne”, tapez le nom complet de l'outil que vous voulez utiliser, y compris le chemin d'accès et l'extension (par exemple, C:\WINDOWS\WRITE.EXE), puis sélectionnez le bouton “OK”. Si vous utilisez Write, choisissez “Pas de conversion”.

Quitter TBAV Windows

TBAV Windows se quitte comme n'importe quelle application Windows, mais il affiche une boîte de dialogue vous informant que la surveillance des flux de fichiers, des programmes exécutés et la recherche en tâche de fond seront désactivées. Ce sont des fonctions puissantes que vous ne voulez peut-être pas abandonner.

Sauf si vous quittez Windows complètement, vous pouvez réduire en icône TBAV Windows, pour qu'il reste actif en tâche de fond. Sélectionnez le bouton “OK” si vous voulez fermer TBAV Windows ou le bouton “Annuler” si vous voulez qu'il continue à fonctionner.

Double-cliquez sur cette icone pour lancer TBAV Windows.

Double-cliquez sur cette icone pour connaître les notes de dernière minute de TBAV Windows.

Double-cliquez sur cette icone pour utiliser les analyses rapides de TBAV Windows.

Ceci est la barre de menu de TBAV Windows. Utilisez les sous-menus pour configurer TBAV Windows.

Ceci est la barre des unités disponibles de TBAV Windows. Vous pouvez l'utiliser pour modifier ou créer des 'unités prédifinies'.

Ce message d'état ne s'affiche que lorsque TBAV Windows coopére avec TBAV Networks.

Ce bouton permet de lancer une procédure de contrôle.

Ce bouton permet de lancer la prise d'empreintes (checksums) des fichiers exécutables.

Ce bouton permet de configurer le Module de Recherche et de Surveillance en Tâche de Fond.

L'accès à la base d'information sur les virus se fait en pressant sur ce bouton.

Vous pouvez obtenir de l'aide en pressant ce bouton.

Cette fenêtre contient les éléments des différentes unités prédéfinies, ou (lors de l'édition d'une unité) la liste des répertoires et fichiers.

Les "unités prédéfinies" affichent la liste des éléments contenus ou sélectionnés.

Pressez sur l'un de ces boutons pour modifier les unités affichées dans la fenêtre la plus à gauche.

Cette partie de la fenêtre vous donne des informations sur votre enregistrement de TBAV Windows.

Cette petite fenêtre contient quelques informations commerciales. Si un virus est détecté, cette fenêtre contiendra la liste des infections virales.

Zone contenant les fichiers du répertoire traité.

Liste déroulante des fichiers analysés. Le mode de défilement peut être modifié via le menu TbScan|Options.

Cette partie de la fenêtre indique le type d'algorithme d'analyse utilisé pour chaque fichier.

Zone d'affichage des heuristiques des fichiers analysés. Les heuristiques indiquent les caractéristiques spéciales de chaque fichier exécutable.

Etat des fichiers analysés, soit sain (Ok) soit infecté (X).

L'extrême droite de la fenêtre de TbScan contient des informations générales sur le processus d'analyse.

Cette partie de la fenêtre "Virus Trouvé!" contient l'élément infecté (eg., chemin d'accès et nom), le ttype d'infection et le nom du virus.

La liste des marqueurs heuristiquesdes fichiers infectés se trouve ici. Les marqueurs heuristiques fournit de nombreux renseignements sur le fonctionnement d'un virus.

Choisissez ce bouton si vous désirez effacer un fichier infecté.

Choisissez ce bouton si vous désirez détruire un fichier infecté. "Détruire" signifie effacer un fichier en interdisant sa restauration.

Choisissez ce bouton si vous désirez renommer un fichier infecté. La première lettre de l'extension du fichier deviendra un 'V'. Par exemple, "COMMAND.COM" deviendra "COMMAND.VOM".

L'option 'Valider' peut être utilisée afin d'indiquer à TbScan n'est pas infecté. Utilisez cette option avec précaution!

Choisissez le bouton "Quitter" pour interrompre TbScan lorsqu'un virus est détecté.

La sélection de ce bouton permet à TbScan jusqu'à ce que TbScan ait terminé d'analyser toutes les unités. La fenêtre "Virus Trouvé" ne sera plus affiché.

Afin de continuer le processus de détection, choisissez ce bouton.

Perform the action selected in the left-most window.

Ce bouton permet d'obtenir des informations sur le virus détecté.

Pour obtenir de l'aide en ligne sur la fenêtre "Virus Trouvé", pressez le bouton "Aide".

Utiliser TBAV Windows

Cette section, ainsi que les suivantes, décrivent en détail la façon dutiliser TBAV Windows. Cette section explique comment utiliser les “Unités cibles”, une fonctionnalité de TBAV Windows extrêmement importante.

Comprendre les “Unités cibles”

Définissons dabord une “Unité cible.” Cest la liste des noms dunités, de répertoires ou de fichiers que le Module de configuration, le Module de détection ou Module de détection en tâche de fond devront traiter. Initialement, TBAV Windows affiche les unités disponibles dans la fenêtre de gauche. Lexemple décran que nous avons donné plus haut contient quatre unités prédéfinies : CD_ROM, LECT_A, SCANTOUT et LOCAL.

Pendant linstallation de TBAV Windows, certaines unités prédéfinies sont générées suivant la configuration de votre système. En plus des unités prédéfinies, vous pouvez définir vos propres unités. par exemple, vous pouvez créer une unité que vous appellerez `DOWNLOAD` contenant le répertoire dans lequel vous téléchargez les programmes. Si vous téléchargez quelques fichiers et voulez savoir sil contiennent des virus, il vous suffira de sélectionner lunité `DOWNLOAD` et de lancer le Module de détection de TBAV Windows.

Unités prédéfinies

Pendant quil examine votre système, le programme dinstallation de TBAV Windows génère quelques unités prédéfinies et les affiche la première fois que vous exécutez TBAV Windows. Selon votre configuration, le programme dinstallation de TBAV Windows va créer les unités suivantes (si elles existent) :

`LECT_A`	Le premier lecteur de disquettes
`LECT_B`	Le second lecteur de disquettes
`LOCAL`	Tous les disques durs locaux
`CD_ROM`	Le(s) lecteur(s) de CD-ROM
`RESEAU`	Toutes les unités du réseau
`SCANTOUT`	Tous les disques durs, toutes les unités de réseau et tous les lecteurs de CD-ROM

La fenêtre de droite “Unités à contrôler” affiche toujours les unités sélectionnées dans la fenêtre de gauche. Ainsi, puisque dans lexemple `SCANTOUT` est sélectionné, la fenêtre de droite affiche C:\, D:\, E:\, F:\, G:\ et H:\.. Si lunité `CD_ROM` avait été sélectionnée, la fenêtre de droite contiendrait H:\, qui référence le lecteur de CD-ROM.

Mémoriser les unités cibles

Les unités cibles sont essentielles pour TBAV Windows, mais peuvent également être utilisée avec TBAV pour DOS. Pour cela, vous devez mémoriser les unités dans un simple fichier ASCII, portant lextension SCN. Le fichier des unités SCANTOUT.SCN, par exemple, contient les lignes suivantes :

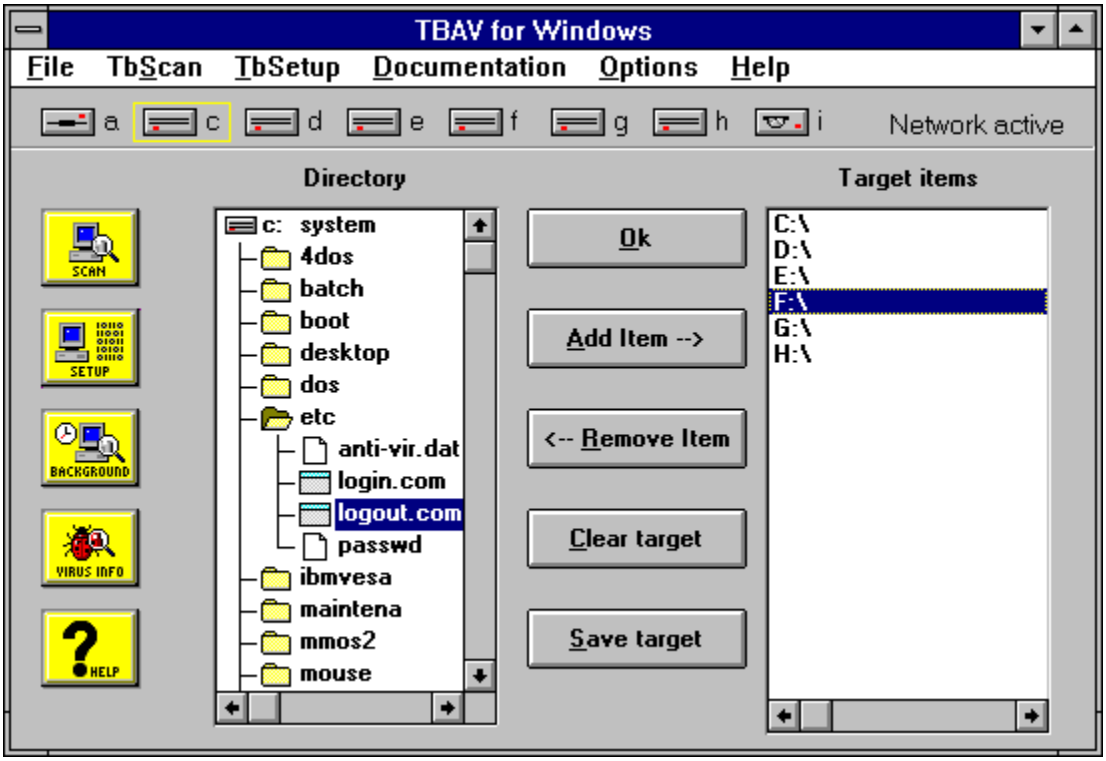
```
C:\
D:\
E:\
F:\
G:\
H:\
```

REMARQUE : Vous devez placer le fichier des unités dans le répertoire de ThunderBYTE Anti-Virus (C:\TBAV, par exemple).

Modifier les unités cibles

Vous pouvez facilement modifier une unité existante, à laide des instructions suivantes :

1. Sélectionnez lunité à modifier, puis sélectionnez le bouton “Modifier unité”. Remarquez que la fenêtre de gauche, “Unités prédéfinies” sappelle maintenant “Répertoire” et représente graphiquement la structure des répertoires de lunité par défaut. Les boutons sont également modifiés, comme illustré dans la figure suivante :



Dans cet exemple, la structure des répertoires de lunité par défaut, C:, saffiche dans la fenêtre de gauche. La première ligne contient le nom de lunité et son nom de volume (ici, “C:” et “systeme”). La fenêtre affiche tous les sous-répertoires et tous les fichiers de cette unité. TBAV Windows distingue les fichiers et les exécutables en plaçant une icône différente à côté de leur nom :

- Licône dossier [ ] indique un répertoire, comme AIDE.
- Licône fenêtre [ ] indique un fichier exécutable (comme SDKPAINT.EXE).
- Licône fichier [ ] indique un fichier ordinaire (ici, le fichier SDKPAINT.DAT).

2. Cliquez deux fois sur licône dossier ou sur le nom dun répertoire pour ouvrir le dossier et afficher le contenu de ce répertoire. Dans notre exemple, le répertoire ASHE est ouvert (notez licône de dossier ouvert [ ]). Cliquer deux fois sur un dossier ouvert “ferme” le répertoire (licône redevient un dossier normal et le contenu du répertoire disparaît).

3. Pour inclure un répertoire ou un fichier dans les “Unités prédéfinies,” sélectionnez-le tout simplement. Vous pouvez sélectionner plusieurs éléments en cliquant, avec le bouton gauche de la souris, sur chacun deux. Les éléments sélectionnés saffichent en inversion vidéo. Dans notre exemple, SDKPAINT.EXE est sélectionné.

CONSEIL : Si vous voulez désactiver la sélection courante dans la fenêtre Répertoire, cliquez deux fois sur la première ligne de cette fenêtre (la ligne où apparaît licône grise représentant un lecteur). Remarquez les barres de défilement horizontal et vertical placées dans la fenêtre Répertoire. Elles vous permettent de faire défiler les données.

4. Lorsque les répertoires et/ou les fichiers sont sélectionnés dans la fenêtre Répertoire, cliquez sur une autre icône dunité, dans le coin supérieur gauche, pour modifier une autre unité, puis sélectionnez dautres répertoires et fichiers. Les unités prédéfinies sont souvent composées de plusieurs lecteurs ou de plusieurs répertoires situés sur différents lecteurs.

5. Lorsque vous avez sélectionné un ou plusieurs éléments, sélectionnez le bouton “Ajouter” pour les copier de la fenêtre “Répertoire” vers la fenêtre “Unités à contrôler”. Voici quelques instructions :

   - Vous ne pouvez pas ajouter délément existant déjà dans la fenêtre “Unités à contrôler”. Si vous essayez de le faire, TBAV Windows lignorera.
   - Si vous activez loption “Sous-répertoires aussi” soit dans le Module de détection (TbScan, Options), soit dans le Module de configuration (TbSetup, Options) elle est activée par défaut dans les deux , TBAV Windows inclura tous les sous-répertoires dun chemin donné dans le traitement de Scan ou de Setup chaque fois que ce chemin sera analysé ou configuré. Si vous activez cette option, vous ne devez pas ajouter les sous-répertoires dune unité dans la fenêtre “Unités à contrôler”. Par exemple, si lunité à contrôler est C:\, lajout du répertoire AIDE serait redondant.
   - Vous ne pouvez pas ajouter un dossier ouvert dans la fenêtre “Unités à contrôler”. Vous devez le fermer (en cliquant deux fois sur lui) avant de le sélectionner et de lajouter dans la fenêtre.

6. Pour supprimer un élément de la fenêtre “Unités à contrôler”, cest-à-dire lexclure, sélectionnez cet élément, puis sélectionnez le bouton “Enlever”. Pour les enlever *tous* de la fenêtre “Unités à contrôler”, sélectionnez le bouton “Détruire unité” (il nest pas nécessaire de sélectionner dabord les éléments).

7. Après avoir modifié une unité prédéfinie ou en avoir créée une, vous allez probablement lenregistrer pour lutiliser plus tard. Sélectionner le bouton “Sauver unité” pour afficher une boîte de dialogue contenant la liste des fichiers dunités existants.
   Quand vous modifiez une unité prédéfinie, elle porte par défaut le même nom que lunité initiale. Si vous en créez une, noubliez pas de taper un autre nom. Quand vous sélectionnez une unité existante, TBAV Windows affiche une boîte de dialogue pour vous avertir que lunité existante sera remplacée par la nouvelle. Faites-le uniquement si vous êtes sûr de le vouloir.

8. Sélectionner le bouton “OK” restaure la fenêtre de gauche “Unités prédéfinies”. Notez que le contenu de la fenêtre “Unités à contrôler” ne change pas, sauf si vous sélectionnez une autre unité dans la liste des unités prédéfinies.
   ATTENTION : Le contenu dune unité non sauvée sera perdu quand vous sélectionnerez une autre unité de la fenêtre “Unités prédéfinies”.

Créer de nouvelles unités

La création dune unité est sensiblement identique à la modification dune unité existante. Il y a une seule différence : lorsque vous sélectionnez le bouton “Nouvelle unité”, la fenêtre “Unités à contrôler” est complètement vide. Il suffit de définir et de sauver la nouvelle unité comme vous le feriez pour modifier une unité existante.

Supprimer des unités prédéfinies

TBAV Windows vous permet de créer de nouvelles unités et de modifier des unités existantes, mais vous pouvez également supprimer des unités. Vous le ferez lorsque, par exemple, la disposition de vos disques durs ou larborescence des répertoires auront changé.

Pour supprimer une unité, sélectionnez-la, puis sélectionnez le bouton “Enlever unité”. TBAV Windows affiche un message vous invitant à confirmer la suppression. Sélectionnez le bouton “Oui” pour effectuer la suppression ou le bouton “Non” pour lannuler.

Ces boutons peuvent être utilisés pour ajouter ou enlever des éléments dans les unités prédéfinies. Vous pouvez également effacer et sauver une unité prédéfinie. La mise à jour de la liste des unités prédéfinies est effectuée en pressant sur le bouton "OK".

Cette fenêtre affiche l'arborescence (répertoires & fichiers) du lecteur sélectionné. Choisissez les fichiers et répertoires à ajouter dans l'unité prédéfinie en cours de modification ou création.

Utiliser le module TbScan

Cette section décrit le Module de détection, qui est le module le plus important et probablement le plus fréquemment utilisé de TBAV Windows. Le Module de détection décèle à la fois les virus connus et les virus inconnus, quils soient situés dans les fichiers ou dans certaines zones des disques. Vous pouvez configurer le Module de détection grâce à plusieurs options, accessibles à partir du menu TbScan.

Activer le Module de détection

Le Module de détection utilise en entrée une unité cible, décrite dans la section précédente. Vous devez donc sélectionner ou créer une unité avant dactiver le Module de détection.

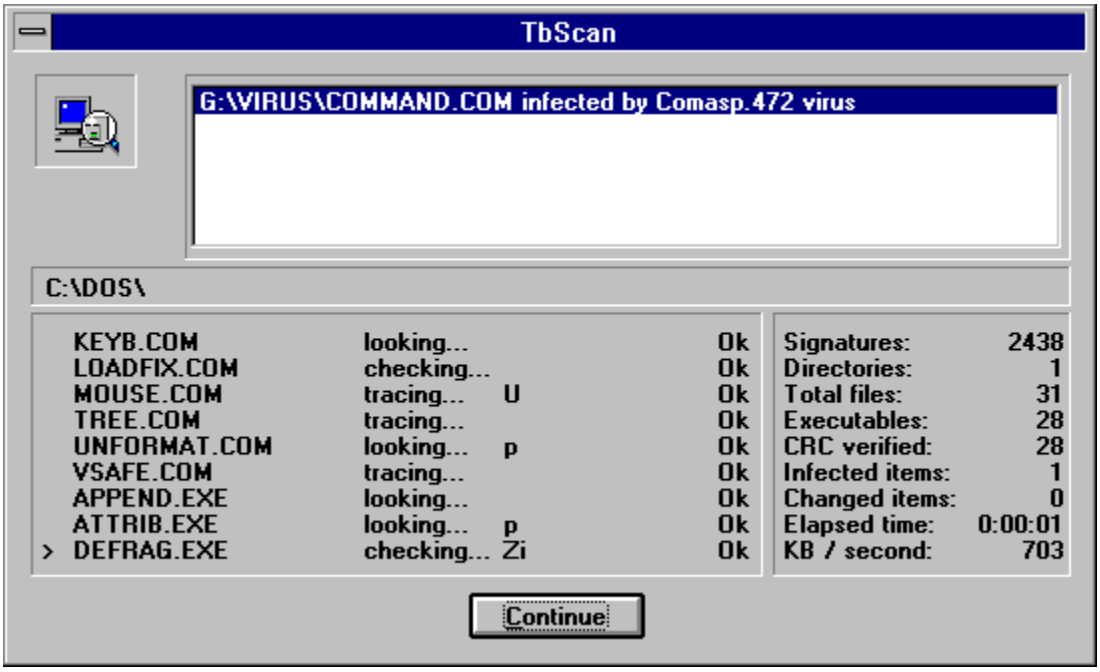
Vous pouvez activer le Module de détection de deux façons :

1. Sélectionnez une unité dans la fenêtre “Unités prédéfinies”, puis sélectionnez le bouton “scan”.
2. Cliquez deux fois sur une unité dans la fenêtre “Unités prédéfinies”.

Le Module de détection commence immédiatement le traitement des éléments affichés dans la fenêtre “Unités à contrôler”.

Utiliser le Module de détection

Activer le Module de détection affiche la boîte de dialogue suivante :



Cette boîte de dialogue, semblable à celle du Module de configuration, est composée de quatre parties :

1. La fenêtre des messages, en haut de la boîte de dialogue, affiche des informations sur les fichiers infectés ou modifiés. Dans cet exemple, la fenêtre des messages contient la référence à un virus. Par défaut, cette fenêtre affiche les coordonnées du distributeur.
2. La fenêtre du répertoire, en dessous de la fenêtre des messages, affiche le nom du répertoire en cours de traitement.

3. La fenêtre des fichiers, dans le coin inférieur gauche de la boîte de dialogue, affiche les fichiers qui ont déjà été examinés, suivis dinformations sur létat de ces fichiers : la méthode danalyse utilisée, les marqueurs heuristiques décrivant le contenu du fichier (et son comportement si le fichier est un fichier exécutable) et lindication que le fichier est ou nest pas infecté par un virus.
4. La fenêtre des statistiques, à droite de la fenêtre des fichiers, affiche des informations concernant le processus danalyse.

Le bouton “Stopper” ou “Continuer”, en bas de la boîte de dialogue, permet darrêter lanalyse ou de continuer lopération. Si TBAV Windows examine un ou plusieurs fichiers, “Stopper” arrête lexamen. Il arrive également que TBAV Windows attende lintervention de lutilisateur (par exemple, quand vous avez activé loption “Affichage par pages”). Dans ce cas, sélectionnez le bouton “Continuer” pour poursuivre lanalyse.

Recherche de virus

Selon les options que vous avez spécifiées, le Module de détection traite un certain nombre de fichiers chaque fois que vous lactivez. Il recherche, dans chaque fichier séparément, à la fois les virus connus et les virus inconnus. Au cours de cette analyse, il affiche les résultats de chaque fichier dans la fenêtre des fichiers. Par exemple, la fenêtre des fichiers peut contenir la ligne suivante :

```
NLSFUNC.EXE checking...      FU       Ok
```

Le premier champ de cette ligne indique le nom du fichier qui vient dêtre examiné (NLSFUNC.EXE).

Le deuxième champ décrit la méthode danalyse utilisée sur le fichier. Le Module de détection de TBAV Windows distingue cinq méthodes danalyse : *looking*, *checking*, *tracing*, *scanning* et *skipping*.
Le troisième champ, ici les lettres majuscules F et U, contient un ou plusieurs caractères davertissement, appelés aussi “marqueurs heuristiques,” concernant le fichier examiné. Pendant la recherche de virus, le Module de détection contrôle le comportement du fichier quil examine. TbScan résume le résultat de ce contrôle à laide de plusieurs lettres majuscules, chacune décrivant une caractéristique spéciale. Ce contrôle détectant le comportement courant des virus, un marqueur en majuscules *peut* indiquer la présence dun virus. Cependant, il est très probable que votre système contienne un petit nombre de fichiers qui, bien que nétant pas infectés, déclenchent quand même un ou deux marqueurs heuristiques. Ne vous en inquiétez pas.

ATTENTION : Vous ne devez ignorer les marqueurs heuristiques que sils concernent un tout petit nombre de fichiers. Si votre système se comporte de façon “bizarre” et si de nombreux fichiers provoquent les mêmes marqueurs heuristiques sérieux, alors il est tout à fait possible que ces fichiers soient infectés par un virus encore inconnu.

TbScan utilise aussi les caractères davertissement pour signaler des formats de fichiers incorrects, des fichiers spéciaux, etc. Mais ces caractères sont affichés en minuscules, indiquant des irrégularités sans gravité.

Configurer le Module de détection

Vous pouvez configurer le Module de détection à laide de la commande TbScan. Sélectionner TbScan affiche le menu suivant :

Options

Options Avancées

Si un virus est trouvé

Options du fichier d'Audit

Voir Fichier Audit

Loption “Options”

Sélectionner “Options” affiche la boîte de dialogue Options de configuration de TbScan pour Windows. Elle offre plusieurs options :

- “Affichage par pages.” Si vous activez cette option, le Module de détection attend lintervention de lutilisateur avant de remplir à nouveau la fenêtre des fichiers. Cela vous permet dexaminer les résultats de lanalyse sans avoir besoin de consulter par la suite le fichier historique. Cette option est désactivée par défaut.

- “Affichage rapide.” Habituellement, le Module de détection examine chaque fichier pour y rechercher des virus. Si vous activez cette option, le Module de détection ne contrôlera que les informations associées à ces fichiers (fichiers ANTIVIR.DAT générés par le Module de configuration). Toutefois, il examine les fichiers si ces informations ne concordent pas avec le contenu réel des fichiers ou si elles nexistent pas. Cette option est désactivée par défaut.
- “Non-exécutables aussi.” Si vous activez cette option, le Module de détection recherche des virus dans tous les fichiers. Normalement, il nexamine que les fichiers exécutables. Nous vous conseillons de laisser cette option désactivée. En effet, un virus doit être exécuté pour effectuer ce pourquoi il a été programmé. Or, pour exécuter un virus, il faut dabord lancer un programme exécutable. Les ordinateurs ne pouvant exécuter de fichiers non exécutables, les virus ninfectent pas ce type de fichiers. Lorsque certains virus le font, cest le résultat dune programmation “incorrecte”. De toutes façons, même si ces fichiers contiennent des données endommagées, il ne peuvent pas contaminer dautres programmes ou fichiers de données.
- “Répéter scan.” Cette option est particulièrement utile pour analyser plusieurs disquettes. Si vous lactivez, Lorsque le Module de détection aura fini dexaminer une disquette, une fenêtre de dialogue vous demandera si vous voulez répéter lexamen. Si vous désactivez cette option, le Module de détection sarrêtera simplement.
- “Bootsector aussi.” Les disquettes ou les disques durs contiennent une zone de petite taille, appelée secteur de démarrage, qui est utilisée pour initialiser lordinateur. Certains virus infectent cette zone particulière et sont activés chaque fois que vous démarrez à partir du disque infecté. Si vous activez cette option, le Module de détection recherchera des virus dans cette zone. Cette option est activée par défaut.
- “Scan dun fichier.” Si loption Scan dun fichier est activée, le Module de détection recherchera des virus dans vos fichiers. Par défaut, cette option est activée. Mais si, victime dun virus de secteur de démarrage, vous voulez analyser uniquement le secteur de démarrage de toutes vos disquettes et pas les fichiers, vous pouvez désactiver cette option.
- “Sous-répertoires aussi.” Par défaut, le Module de détection examine automatiquement les fichiers se trouvant dans tous les sous-répertoires de lunité spécifiée, sauf vous indiquez au Module de détection de nexaminer quun seul fichier. Désactivez cette option si vous ne voulez pas que le Module de détection examine les sous-répertoires.
- “Défilement affichage rapide.” Par défaut, le Module de détection utilise un algorithme de défilement spécial pour afficher les fichiers traités. Cet algorithme a été conçu pour ralentir le moins possible le processus danalyse. Cependant, cette méthode de défilement est inhabituelle. Si vous désactivez cette option, TbScan utilisera le défilement conventionnel.

Loption “Options avancées”

Nous recommandons aux utilisateurs débutants de ne pas toucher à ces options. Mais, au fur et à mesure que votre expérience grandira, vous serez amené à les modifier. Les voici :

- “Haute sensibilité heuristique.” Lorsque TbScan effectue une analyse heuristique des fichiers, il signale quun fichier a été infecté uniquement si linfection est très probable. Si vous activez cette option, TbScan sera plus sensible. Dans ce mode, il détecte 90 % des virus inconnus sans en connaître la signature. Mais faites attention, vous aurez quelques fausses alertes.

- “Ajustement automatique.” Par défaut, TbScan ajuste automatiquement le niveau de détection heuristique lorsquil découvre un virus. En dautres termes, quand TbScan trouve un virus, il se comporte comme si vous aviez sélectionné loption “Haute sensibilité heuristique.” Loption “Ajustement automatique” vous offre une capacité de détection maximale lorsque cest devenu nécessaire, tout en limitant au minimum le nombre de fausses alertes.
- “Basse sensibilité heuristique.” Dans ce mode, TbScan ne provoque pratiquement jamais de fausse alerte. Il détecte quand même environ 50 % de virus inconnus.
- “Configurer les extensions des exécutables.” Par défaut, TbScan nexamine que les fichiers dont lextension est celle des programmes. Tous les virus infectent du code exécutable. Sont considérés comme exécutables les fichiers dont lextension est EXE, COM, BIN, SYS, DLL, DOC, DOT et OV? (OV? représente les fichiers OVR ou OVL). Malgré tout, certains autres fichiers ont une structure interne qui les expose aux virus. Bien quil soit peu vraisemblable que vous soyez amené à les exécuter, vous pouvez quand même les analyser. Voici les extensions qui peuvent indiquer un format exécutable :.SCR (fichier économiseur décran MSWindows), .MOD (fichier MSWindows), .CPL (Panneau de configuration MSWindows), .00? et .APP. Comme linfection de ces fichiers est peu probable, examinez-les une fois de temps en temps. Si vous voulez que TbScan les examine par défaut, sélectionnez cette option en indiquant les extensions des fichiers que vous voulez analyser. Par exemple : .SCR.CPL (sans espace). Vous pouvez utiliser le point dinterrogation comme caractère générique.

AVERTISSEMENT : Faites attention aux extensions que vous indiquez. Lexamen dun fichier non exécutable peut entraîner des résultats imprévisibles et provoquer des fausses alertes.

- “Extraction de signatures.” Cette option nest disponible que pour les utilisateurs enregistrés. Reportez-vous à la section “TbGensig” du Chapitre 4, pour plus dinformations.

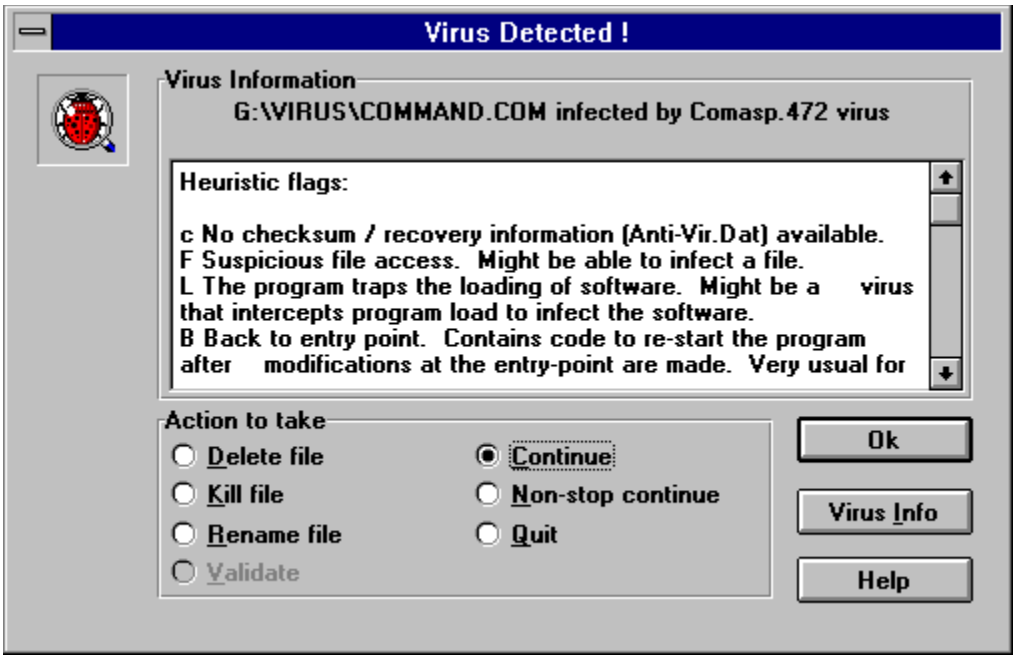
Détection d'un Virus

Quand le Module de détection détecte la présence dun virus, un message concernant le fichier infecté saffiche dans la fenêtre des messages. Le Module de détection distingue six types de messages :

1. **“[Nom du fichier] infecté par [nom du virus] virus.”** Le fichier est infecté par le virus indiqué.
2. **“[Nom du fichier] plaisanterie nommée [nom de la plaisanterie].”** Certains programmes simulent linfection du système par un virus, ce sont des “plaisanteries.” Une plaisanterie est totalement inoffensive, mais provoque une confusion et peut pousser certains utilisateurs à abandonner leur ordinateur. Cest pourquoi il vaut mieux la supprimer.
3. **“[Nom du fichier] cheval de Troie nommé [nom du Cheval de Troie].”** Ce fichier est un Cheval de Troie. Cest-à-dire un programme “transporteur” de virus. Il nest pas lui-même un virus, mais il introduit un virus dans votre système, lorsquil est exécuté. Nexécutez pas de tels programmes, supprimez-les.
4. **“[Nom du fichier] endommagé par [nom du virus].”** Un fichier endommagé est un fichier victime du virus, mais qui ne le contient pas.
5. **“[Nom du fichier] dropper de [nom du virus].”** Un “dropper” est un programme qui na pas lui-même été infecté, mais qui contient un virus de secteur de démarrage et qui peut lintroduire dans votre secteur de démarrage.
6. **“[Nom du fichier] garbage: (pas un virus) [nom du garbage].”** Un “garbage” (déchet), que certains considèrent comme un virus, est un programme qui ne fonctionne pas, soit parce quil a été gravement endommagé, soit pour une autre raison. Parce que certains concurrents lappellent virus ou parce quil figure dans diverses collections de virus, des utilisateurs continuent de nous signaler ce “nouveau virus” que nous “ne détectons pas.” Lappeler virus ne ferait quaggraver le problème, aussi nous préférons lappeler “garbage” pour faire savoir aux utilisateurs que nous nignorons pas ce type de fichier, mais que ce nest pas un virus.

Le Module de détection de TBAV Windows place parfois le préfixe “Probablement” ou “Peut-être” avant lun des messages précédents. Par exemple : “C:\UNFICH.COM probablement infecté par un virus inconnu”. Ces messages apparaissent en cas de virus encore inconnu, quand le Module de détection a effectué une analyse heuristique sur le fichier. Si le préfixe est “Probablement,” il est presque certain que le fichier est infecté par un virus inconnu. Si le préfixe est “Peut-être,” la probabilité dinfection est bien plus faible, mais existe quand même.

Par défaut, si TbScan détecte un virus, il affiche une boîte de dialogue semblable à celle-ci :



La première ligne de cette boîte de dialogue contient le nom du fichier infecté, suivi du type dinfection et du nom du virus. La liste des marqueurs heuristiques et leur description saffiche en dessous de cette ligne.

La boîte de dialogue affiche alors, dans sa partie inférieure, la liste des actions que vous pouvez effectuer :

- Laction par défaut est de continuer le processus de détection, sans rien faire de particulier.
- La deuxième action possible est laction “Plus dinterruptions”. Quand vous sélectionnez cette action, le Module de détection continu lanalyse sans sarrêter sil trouve dautres virus.
- Vous pouvez arrêter le processus danalyse en sélectionnant loption “Stopper contrôle”.
- Loption “Détruire fichier” supprime simplement le fichier infecté.
- Loption “Renommer fichier” renomme le fichier infecté, en remplaçant par “V” la première lettre de lextension du fichier. Par exemple, EXE devient VXE.
- Loption “Ecraser fichier” est semblable à loption “Détruire fichier”, mais vous ne pourrez pas restaurer ce fichier à laide dun utilitaire de récupération de fichiers (comme la commande UNDELETE du DOS).
- Loption “Valider fichier” nest accessible que si les informations concernant le fichier incriminé stockées dans ANTIVIR.DAT ne concordent plus avec le contenu actuel du fichier. Dans ce cas, le Module de détection vous informe que le fichier a été modifié. Si vous êtes absolument certain que ce fichier nest pas contaminé, vous pouvez sélectionner loption “Valider fichier”. Si vous le faites, le Module de détection ne vous avertira plus au cours dun examen ultérieur de ce fichier, si les informations enregistrées dans ANTIVIR.DAT et celles du fichier ne concordent pas. Mais, les infections par virus seront encore détectées, même si un programme a été validé !

Remarquez les deux boutons situés à droite de la boîte : “Information sur le virus” et “Que faire ?”. Ce dernier vous offre une aide en ligne sur la boîte de dialogue. Le premier affiche une autre boîte de dialogue contenant des informations sur le virus détecté. Ces informations concernent par exemple le type de fichier contaminé par le virus, la longueur du code viral, laction réellement entreprise par le virus et quelques renseignements sur la façon den débarrasser votre système.

Lorsque vous avez choisi une action, sélectionnez le bouton “OK”, à droite de la boîte de dialogue, pour lexécuter.

Options de TbScan

Sélectionner “Options” affiche la boîte de dialogue Options de configuration de TbScan pour Windows. Elle offre plusieurs options :

“Affichage par pages.”
Si vous activez cette option, le Module de détection attend l'intervention de l'utilisateur avant de remplir à nouveau la fenêtre des fichiers. Cela vous permet d'examiner les résultats de l'analyse sans avoir besoin de consulter par la suite le fichier historique. Cette option est désactivée par défaut.

“Affichage rapide.”
Habituellement, le Module de détection examine chaque fichier pour y rechercher des virus. Si vous activez cette option, le Module de détection ne contrôlera que les informations associées à ces fichiers (fichiers ANTIVIR.DAT générés par le Module de configuration). Toutefois, il examine les fichiers si ces informations ne concordent pas avec le contenu réel des fichiers ou si elles n'existent pas. Cette option est désactivée par défaut.

“Non-exécutables aussi.”
Si vous activez cette option, le Module de détection recherche des virus dans tous les fichiers. Normalement, il n'examine que les fichiers exécutables. Nous vous conseillons de laisser cette option désactivée. En effet, un virus doit être exécuté pour effectuer ce pourquoi il a été programmé. Or, pour exécuter un virus, il faut d'abord lancer un programme exécutable. Les ordinateurs ne pouvant exécuter de fichiers non exécutables, les virus n'infectent pas ce type de fichiers. Lorsque certains virus le font, c'est le résultat d'une programmation “incorrecte”. De toutes façons, même si ces fichiers contiennent des données endommagées, il ne peuvent pas contaminer d'autres programmes ou fichiers de données.

“Répéter scan.”
Cette option est particulièrement utile pour analyser plusieurs disquettes. Si vous l'activez, Lorsque le Module de détection aura fini d'examiner une disquette, une fenêtre de dialogue vous demandera si vous voulez répéter l'examen. Si vous désactivez cette option, le Module de détection s'arrêtera simplement.

“Bootsector aussi.”
Les disquettes ou les disques durs contiennent une zone de petite taille, appelée secteur de démarrage, qui est utilisée pour initialiser l'ordinateur. Certains virus infectent cette zone particulière et sont activés chaque fois que vous démarrez à partir du disque infecté. Si vous activez cette option, le Module de détection recherchera des virus dans cette zone. Cette option est activée par défaut.

“Scan d'un fichier.”
Si l'option Scan d'un fichier est activée, le Module de détection recherchera des virus dans vos fichiers. Par défaut, cette option est activée. Mais si, victime d'un virus de secteur de démarrage, vous voulez analyser uniquement le secteur de démarrage de toutes vos disquettes et pas les fichiers, vous pouvez désactiver cette option.

“Sous-répertoires aussi.”
Par défaut, le Module de détection examine automatiquement les fichiers se trouvant dans tous les sous-répertoires de l'unité spécifiée, sauf vous indiquez au Module de détection de n'examiner qu'un seul fichier. Désactivez cette option si vous ne voulez pas que le Module de détection examine les sous-répertoires.

“Défilement affichage rapide.”
Par défaut, le Module de détection utilise un algorithme de défilement spécial pour afficher les fichiers traités. Cet algorithme a été conçu pour ralentir le moins possible le processus d'analyse. Cependant, cette méthode de défilement est inhabituelle. Si vous désactivez cette option, TbScan utilisera le défilement conventionnel.

Options Avancées de TbScan

Nous recommandons aux utilisateurs débutants de ne pas toucher à ces options. Mais, au fur et à mesure que votre expérience grandira, vous serez amené à les modifier. Les voici :

“Haute sensibilité heuristique.”
Lorsque TbScan effectue une analyse heuristique des fichiers, il signale qu'un fichier a été infecté uniquement si l'infection est très probable. Si vous activez cette option, TbScan sera plus sensible. Dans ce mode, il détecte 90 % des virus inconnus sans en connaître la signature. Mais faites attention, vous aurez quelques fausses alertes.

“Ajustement automatique.”
Par défaut, TbScan ajuste automatiquement le niveau de détection heuristique lorsqu'il découvre un virus. En d'autres termes, quand TbScan trouve un virus, il se comporte comme si vous aviez sélectionné l'option “Haute sensibilité heuristique.” L'option “Ajustement automatique” vous offre une capacité de détection maximale lorsque c'est devenu nécessaire, tout en limitant au minimum le nombre de fausses alertes.

“Basse sensibilité heuristique.”
Dans ce mode, TbScan ne provoque pratiquement jamais de fausse alerte. Il détecte quand même environ 50 % de virus inconnus.

“Configurer les extensions des exécutables.”
Par défaut, TbScan n'examine que les fichiers dont l'extension est celle des programmes. Tous les virus infectent du code exécutable. Sont considérés comme exécutables les fichiers dont l'extension est EXE, COM, BIN, SYS et OV? (OV? représente les fichiers OVR ou OVL). Malgré tout, certains autres fichiers ont une structure interne qui les expose aux virus. Bien qu'il soit peu vraisemblable que vous soyez amené à les exécuter, vous pouvez quand même les analyser. Voici les extensions qui peuvent indiquer un format exécutable : .DLL (bibliothèques de liens dynamiques MSWindows), .SCR (fichier économiseur d'écran MSWindows), .MOD (fichier MSWindows), .CPL (Panneau de configuration MSWindows), .00? et .APP. Comme l'infection de ces fichiers est peu probable, examinez-les une fois de temps en temps. Si vous voulez que TbScan les examine par défaut, sélectionnez cette option en indiquant les extensions des fichiers que vous voulez analyser. Par exemple : .DLL.SCR.CPL (sans espace). Vous pouvez utiliser le point d'interrogation comme caractère générique.
ATTENTION : Faites attention aux extensions que vous indiquez. L'examen d'un fichier non exécutable peut entraîner des résultats imprévisibles et provoquer des fausses alertes.

“Extraction de signatures.” Cette option n'est disponible que pour les utilisateurs enregistrés. Reportez-vous à la section “TbGensig” du Chapitre 4, pour plus d'informations.

Si un Virus est Trouvé ?

L'option “Si un virus est trouvé” vous permet de choisir l'action qu'effectuera le Module de détection lorsqu'il détectera un virus :

“Présenter le menu d'actions.”
Cette option (activée par défaut) demande à TbScan d'afficher un menu proposant trois actions possibles lorsqu'un virus est détecté : “continuer”, “détruire” ou “renommer” le fichier infecté.

“Continuer (logger alarme).”
Par défaut, quand TbScan détecte un fichier infecté, il vous invite à supprimer ou à renommer ce fichier, ou bien à poursuivre l'examen sans effectuer d'action. Cependant, si vous sélectionnez cette option, TbScan continuera toujours son analyse. Dans ce cas, nous vous recommandons vivement d'utiliser un fichier historique pour connaître les messages envoyés, sinon l'examen ne serait d'aucune utilité (voir plus loin “Options du fichier Log”, pour plus d'informations).

“Détruire fichier infecté.”
Par défaut, quand TbScan détecte un fichier infecté, il vous invite à supprimer ou à renommer ce fichier, ou bien à poursuivre l'examen sans effectuer d'action. Cependant, si vous sélectionnez cette option, TbScan supprimera automatiquement le fichier infecté, sans vous demander confirmation. Utilisez cette option si vous savez que votre ordinateur est infecté par un virus et souhaitez effacer tous les fichiers contaminés. Soyez certain de posséder une sauvegarde saine et de vouloir vous débarrasser immédiatement de tous les fichiers infectés.

“Ecraser fichier infecté.”
Cette option est proche de l'option “Détruire fichier infecté”, avec une différence majeure. La commande DOS UNDELETE vous permet habituellement de récupérer un fichier supprimé, mais si le fichier infecté a été supprimé par cette option, cette récupération n'est plus possible.

“Renommer fichier infecté.”
Par défaut, quand TbScan détecte un fichier infecté, il vous invite à supprimer ou à renommer ce fichier, ou bien à poursuivre l'examen sans effectuer d'action. Cependant, si vous sélectionnez cette option, TbScan renommera automatiquement le fichier infecté, sans vous demander confirmation. Par défaut, TbScan remplace par “V” le premier caractère de l'extension du fichier. Par exemple il renomme .VXE un fichier .EXE et .VOM un fichier .COM. Cela empêche l'exécution des programmes infectés et, par conséquent, la propagation du virus. Cela permet également de conserver les fichiers pour les examiner et les réparer plus tard.

Options du fichier Audit de TbScan

Le Module de détection de TBAV Windows peut créer un fichier historique au cours de l'analyse, contenant les noms de fichiers complets, les noms des virus et les marqueurs heuristiques. Pour réduire la taille de ce fichier, vous pouvez limiter son contenu :

“Fichiers infectés seulement.”
Seuls les fichiers infectés, par un virus connu ou inconnu, apparaîtront dans le fichier historique..

“Ajouter un résumé.”
Semblable à l'option précédente, mais un cours résumé du processus d'analyse sera ajouté.

“Ajouter les fichiers suspects.”
Utilisez cette option si vous voulez garder aussi la trace des fichiers suspects, c'est-à-dire ceux qui déclenchent un avertissement heuristique avec le niveau de détection par défaut.

“Ajouter toutes les alarmes.”
Cette option mentionne dans le fichier historique tous les fichiers qui déclenchent un ou plusieurs avertissements heuristiques.

“Ajouter les fichiers non infectés.”
Tous les fichiers traités figureront dans le fichier historique.

“Sortie dans un fichier.”
Cette option demande au Module de détection de créer un fichier historique. Vous devez l'activer avant de définir le contenu du fichier à l'aide des options précédentes.

“Ajouter à la fin du fichier Audit existant.”
Dans certains cas, vous voudrez conserver le contenu actuel du fichier historique et ajouter les nouvelles entrées à la fin de ce fichier. Cette option vous le permettra.
REMARQUE : Vous devez quand même activer l'option “Sortie dans un fichier” pour écrire les résultats de l'analyse dans le fichier historique.

“Pas de description heuristique.”
Par défaut, le Module de détection indique les marqueurs heuristiques dans le fichier historique, sous la forme d'un caractère d'avertissement et d'une brève description. Par exemple, si un fichier déclenche le marqueur “#”, la description “Routine ou instructions de décryptage trouvées. Ceci est classique des virus mais aussi de certains logiciels protégés” est insérée dans le fichier historique. Mais, le fichier historique peut devenir volumineux. Si vous sélectionnez cette option, TbScan n'inscrira pas ces descriptions dans le fichier historique.

Le bouton “LogFile”.
Ce bouton vous permet de choisir le nom du fichier historique. Vous pouvez choisir un nom existant ou entrer le nom d'un nouveau fichier. Dans ce dernier cas, nous vous conseillons d'utiliser l'extension .LOG, qui correspond aux conventions d'appellation standard. Le Module de détection utilisera le nom spécifié pour toutes les opérations d'analyse suivantes, jusqu'à ce que vous changiez ce nom. Par défaut, le nom du fichier historique est TBSCAN.LOG et il se trouve dans le répertoire de TBAV Windows.

Visualiser le fichier Audit

Cette option permet d'afficher le fichier historique créé par le Module de détection. C'est l'afficheur interne du Module de détection qui permet de le visualiser (voir l'illustration suivante). Si le fichier historique n'existe pas, un avertissement vous le signale. Vous pouvez aussi imprimer le contenu du fichier historique, en sélectionnant le menu File, puis l'option Print, de l'afficheur.
CONSEIL : Vous pouvez choisir votre propre outil de consultation de fichiers à la place de l'afficheur interne de TBAV Windows, en utilisant l'option “Configuration de TBAVWIN” du menu “Options”.

Utiliser le module TbSetup

Le Module de configuration de TBAV Windows collecte des informations sur tous les fichiers exécutables de votre système. Le Module de détection utilise ces informations, qu'il stocke dans des fichiers spéciaux, ANTIVIR.DAT (un par répertoire), pour vérifier si les fichiers ont été modifiés (ce qui peut indiquer la présence d'un virus). L'utilitaire de nettoyage (qui fait partie de TBAV pour DOS) utilise ensuite ces informations pour restaurer le contenu initial des fichiers infectés.
ATTENTION : Nous vous recommandons d'utiliser le Module de configuration uniquement lors de la première installation et pour les nouvelles applications. Si vous exécutiez le Module de configuration après une infection, il validerait les programmes infectés ! Analysez d'abord l'unité sur laquelle vous voulez appliquer le Module de configuration, afin d'éviter de valider accidentellement des fichiers infectés.
Le Module de configuration de TBAV Windows utilise un fichier de données à part pour reconnaître certains fichiers programmes. De tels fichiers exigent une attention particulière. Quand le Module de détection traite ces fichiers, il les mentionne dans le fichier TBSETUP.DAT. Ce fichier est livré avec TBAV.

REMARQUE : Le fichier TBSETUP.DAT contient également une importante documentation et la liste des programmes spéciaux. Ce fichier de données est en format texte et vous pouvez le consulter en le chargeant dans votre éditeur ASCII. TBAV Windows vous offre également le moyen de le visualiser (reportez-vous à la section “Configurer le Module TbSetup”.

Les utilitaires ThunderBYTE Anti-Virus suivants utilisent les informations générées par le Module de configuration :

TBAV DOS
- TbScan. Il utilise ces informations pour un contrôle de validité.
- TbClean. TbClean utilise ces informations pour restaurer le contenu initial d'un fichier infecté.
- TbScanX, TbCheck, TbFile, TbMem. Tous ces programmes utilisent ces informations pour mémoriser les permissions.

TBAV Windows
- Le Module de détection. Il utilise ces informations pour un contrôle de validité.
- Le Module de détection en tâche de fond et le Module de suivi des applications exécutées. Ces modules utilisent ces informations pour mémoriser les permissions.

Activer le Module TbSetup

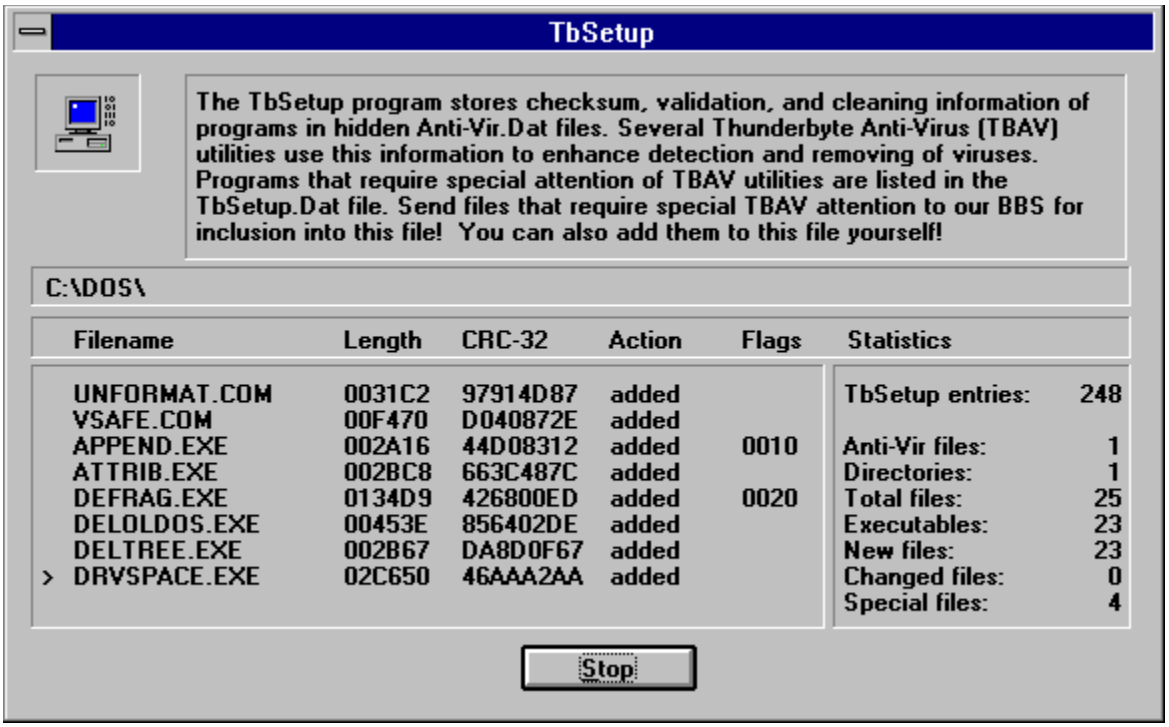
Le Module TbSetup utilise en entrée une unité cible (décrite plus haut).Vous devez donc sélectionner une unité avant d'activer le Module de configuration. Le Module de configuration utilise toujours comme cible le contenu courant de la fenêtre “Unités à contrôler”.

Vous activez le Module TbSetup en sélectionnant le deuxième bouton d'accès rapide, à gauche, de la fenêtre principale de TBAV Windows :

Le Module TbSetup commence immédiatement à traiter les éléments de la fenêtre “Unités à contrôler”.

Utiliser le Module TbSetup

Quand vous lancez le Module de configuration, il affiche la boîte de dialogue suivante :



Cette boîte de dialogue, très semblable à celle du Module de détection, est composée de quatre parties :

1. La fenêtre des messages. Située en haut de la boîte de dialogue, elle contient des informations concernant le Module de configuration. Le contenu de cette fenêtre ne change pas au cours du processus de configuration.
2. La fenêtre du répertoire. Située en dessous de la fenêtre des messages, elle affiche le nom du répertoire en cours de traitement.
3. La fenêtre des fichiers. Dans la partie inférieure gauche de la boîte de dialogue, elle affiche les fichiers pour lesquels les informations ont été ou sont sur le point d'être collectées, suivis d'informations sur l'état de ces fichiers : longueur du fichier, somme de contrôle, action appliquée au fichier et certains marqueurs indiquant des fichiers spéciaux.
4. La fenêtre des statistiques. Située à droite, elle affiche des informations sur le processus de configuration.

Le bouton “Stopper” ou “Continuer”. Si le Module de configuration est en train de traiter un ou plusieurs fichiers, ce bouton indique “Stopper”, et vous permet d'arrêter l'opération de configuration. Si TbSetup attend la réponse d'un utilisateur (par exemple si vous avez choisi l'option “Affichage par pages”), le bouton indique “Continuer”, qui vous permet de poursuivre le traitement.

Selon les options sélectionnés, le Module de configuration traite un certain nombre de fichiers chaque fois que vous le lancez. Au cours du traitement, il affiche les résultats de chaque fichier dans la fenêtre des fichiers. Par exemple, cette fenêtre peut contenir la ligne suivante :

NLSFUNC.EXE 003D86 9BAE1A00 ajout * 0010

REMARQUE : Ne vous inquiétez pas si les informations défilent trop vite pour les lire ou si vous ne les comprenez pas. Vous n'aurez probablement jamais besoin de tous ces détails.

Le premier champ de la ligne indique le nom du fichier en cours de traitement, ici NLSFUNC.EXE.

Le deuxième champ contient la longueur du fichier en hexadécimal.

Le troisième champ est une somme de contrôle 32 bits. TbSetup utilise un algorithme qui calcule cette somme en

tenant compte du contenu du fichier

Le quatrième champ indique l'une des trois actions possibles qu'effectue TbSetup :

“Ajouté.”
Indique que ANTIVIR.DAT ne contenait pas de référence au fichier traité. TbSetup a ajouté une nouvelle entrée pour ce fichier dans le fichier ANTIVIR.DAT.

“Changé.”
Indique que ANTIVIR.DAT contenait une entrée pour le fichier dont les informations ne concordaient plus avec le contenu réel du fichier. TbSetup a mis à jour l'enregistrement.
ATTENTION : N'oubliez pas que la modification d'un fichier peut indique la présence d'un virus.

“Mis à jour.”
Indique que ANTIVIR.DAT contenait une entrée pour le fichier, mais que le Module de configuration a modifié les marqueurs de permission. Les informations associées au fichier concordaient avec le contenu du fichier.

Le cinquième champ spécifie les marqueurs de permission du fichier. TbSetup obtient ces marqueurs soit du fichier TBSETUP.DAT (le fichier contenant la liste des fichiers spéciaux), soit d'une définition ou d'une réinitialisation effectuée par l'utilisateur.
REMARQUE : La compréhension du sens exact des marqueurs de permission n'est pas nécessaire à un utilisateur débutant. Si vous voulez en savoir plus, consultez le fichier TBSETUP.DAT, qui contient une brève description de chaque marqueur.

Configurer le Module de configuration

Vous pouvez configurer le Module TbSetup au moyen de la barre de menus de TBAV Windows. Cliquer sur “TbSetup” affiche un menu avec les options suivantes :

Options de TbSetup

Flags de réglage

Nom du fichier de données

Visualiser le fichier de données

Options de TbSetup

Le Module TbSetup de TBAV Windows offre plusieures options :

“Affichage par pages.”
Quand vous spécifiez cette option, TbSetup s'interrompt après avoir traité le contenu de chaque fenêtre. Cela vous permet d'examiner les résultats.

“Nouveaux fichiers uniquement.”
Utilisez cette option si vous voulez ajouter de nouveaux fichiers à la base de données ANTIVIR.DAT mais empêcher la mise à jour des informations des fichiers modifiées. Mettre à jour les informations des fichiers modifiés serait dangereux, car si ces fichiers sont infectés les informations qui permettent de détecter et de supprimer le virus seraient remplacées. Cette option empêche le remplacement des informations existantes, mais permet l'ajout des informations sur les nouveaux fichiers.

“Retire les fichiers Anti-Vir.Dat.”
Si vous voulez plus vous servir des utilitaires ThunderBYTE, vous n'êtes pas obligé de supprimer vous-même les fichiers ANTIVIR.DAT. Grâce à cette option, TbSetup enlève scrupuleusement tous les fichiers ANTIVIR.DAT de votre système.

“Test (pas de changements).”
Utilisez cette option si vous voulez connaître les conséquences d'une option sans prendre le risque de provoquer quelque chose que vous regretteriez. Cette option demande au programme de se comporter comme il devrait le faire, mais de n'effectuer ni modification ni mise à jour sur votre disque dur.

“Cache les fichiers Anti-Vir.Dat.”
Normalement, les fichiers ANTIVIR.DAT n'apparaissent pas dans l'affichage de la liste des fichiers. Désactivez cette option si vous voulez qu'ils soient visibles, comme des fichiers normaux.
REMARQUE : Cette option ne s'appliquera qu'aux nouveaux fichiers ANTIVIR.DAT.

“Protéger les EXE/COM (read-only).”
Comme TbFile surveille en permanence l'attribut lecture-seule, nous vous recommandons vivement de rendre tous les fichiers exécutables accessibles seulement en lecture, pour éviter qu'ils soient modifiés. Si vous activez cette option, TbSetup le fera automatiquement pour vous. TbSetup sait reconnaître les fichiers qui ne doivent pas être accessibles seulement en lecture.

“Effacer attribut lecture seulement.”
Utilisez cette option pour annuler l'opération “Protéger les EXE/COM (read-only)”. Si vous activez cette option, TBAV enlève l'attribut lecture-seule de tous les fichiers exécutables.

“Inclure les sous-répertoires.”
Par défaut, TbSetup recherche les fichiers exécutables dans les sous-répertoires, sauf si vous précisez un nom de fichier (les caractères génériques sont autorisés). Si vous désactivez cette option, TbSetup ne traitera pas les sous-répertoires.

Flags de réglage de TbSetup

Le Module TbSetup contient des options réservées aux utilisateurs expérimentés. Elles permettent de changer manuellement les marqueurs de permission des fichiers. Cliquez sur l'option “Flags de réglage” du menu “TbSetup” pour afficher une boîte de dialogue dans laquelle vous pouvez définir ou réinitialiser manuellement les marqueurs, ou utiliser les marqueurs normaux.

Vous spécifiez les marqueurs à définir ou à réinitialiser en sélectionnant un ou plusieurs éléments de la fenêtre inférieure de la boîte de dialogue.

“Util. normale flags.”
C'est l'option par défaut, que vous utiliserez tant que vous n'aurez pas acquis davantage d'expérience.

“Posit. manuel flags.”
Cette option est réservée aux utilisateurs expérimentés. En l'utilisant, vous pouvez définir manuellement certains marqueurs de permission dans l'enregistrement ANTIVIR.DAT. Cette option nécessite l'utilisation d'un masque de bits hexadécimal (consultez le fichier TBSETUP.DAT, pour en savoir plus sur les masques de bits). La boîte “Choix des flags à modifier” contient la liste des marqueurs que vous pouvez modifier.

“Réinit. manuelle flags.”
Cette option est réservée aux utilisateurs expérimentés. En l'utilisant, vous pouvez restaurer manuellement certains marqueurs de permission ou empêcher que certains marqueurs soient définis dans l'enregistrement ANTIVIR.DAT. Cette option nécessite l'utilisation d'un masque de bits hexadécimal (consultez le fichier TBSETUP.DAT, pour en savoir plus sur les masques de bits). La boîte “Choix des flags à modifier” contient la liste des marqueurs que vous pouvez modifier.

Nom du fichier de données

Cette option vous permet de choisir le nom et l'emplacement du fichier TBSETUP.DAT. Par défaut, ce fichier se nomme TBSETUP.DAT et se trouve dans le répertoire de TBAV Windows.

REMARQUE : Le fichier que vous indiquez doit exister.

Vous pouvez visualiser le fichier de donénes avec l'option **Visualiser le fichier de données** du menu de TbSetup.

Visualiser le fichier de données

Sélectionner cette option affiche le fichier de données dans une nouvelle fenêtre. Vous pouvez imprimer le contenu de TBSETUP.DAT en sélectionnant File, Print.

REMARQUE : Vous pouvez utiliser votre propre outil de consultation de fichiers à la place de l'afficheur interne de TBAV Windows, en sélectionnant la commande Options, Configuration de TBAV Windows.

This is where TbSetup shows the special flags of a file to indicate certain characteristics of that file.

The TbSetup statistics are collected in this window.

The CRC (the result of a special mathematical algorithm) of files processed by TbSetup, is written here.

The action performed by TbSetup (e.g., "added" or "changed") is displayed in this area.

The length of the file being processed in displayed here, in hexadecimal notation.

This area of the TbSetup window holds the name of the current directory.

This part of the TbSetup window always contains some information about TbSetup.

The names of the files being processed by TbSetup are displayed here.

Utiliser le module de surveillance des Entrées/Sorties de fichiers

Le Module de surveillance des flux de fichiers lance une recherche de virus sur chaque fichier que vous créez, copiez, décompressez, téléchargez, etc. Ce sont là les opérations les plus courantes que les utilisateurs effectuent sur les fichiers. De plus, la plupart des utilisateurs introduisent régulièrement des disquettes dans le lecteur de leur ordinateur. Comme c'est surtout à ce moment-là que les virus deviennent actifs, vous devez absolument surveiller tous les fichiers qui sont ainsi manipulés

Le Module de surveillance des flux de fichiers analyse automatiquement tous les fichiers créés ou modifiés de votre disque dur ainsi que les disquettes insérées dans un lecteur.

Activer le Module de surveillance des flux de fichiers

Par défaut, le Module de surveillance des flux de fichiers est actif quel que soit le mode de TBAV Windows. Vous pouvez le désactiver en utilisant la boîte de dialogue de configuration du Module de détection en tâche de fond. Pour accéder à la boîte de dialogue de configuration utilisez la commande Options, Programmateur, ou sélectionnez le troisième bouton d'accès rapide :

Reportez-vous à la section “Configurer le Module de surveillance des flux de fichiers”, plus loin dans ce chapitre, pour savoir comment configurer, activer et désactiver le Module de surveillance des flux de fichiers.

Utiliser le Module de surveillance des flux de fichiers

Si vous utilisez TBAV Windows en mode normal (c'est-à-dire lorsqu'il n'est ni minimisé ni réduit en icône), le Module de surveillance des flux de fichiers utilise la barre de titre pour indiquer ce qu'il fait. Chaque fois qu'il examine un fichier ou une disquette, la barre de titre affiche “Scanning...”

La fenêtre d'état, qui apparaît dès que vous minimisez TBAV Windows, affiche également l'activité du surveillant. La première ligne indique l'état du surveillant des flux de fichiers. La deuxième ligne de la fenêtre d'état indique ici ce dernier nom de fichier, qui est le fichier surveillé.

REMARQUE : Reportez-vous à la section **Utiliser le Module de détection en tâche de fond**, plus haut dans ce chapitre, pour plus d'informations sur la fenêtre d'état.

Configurer le Module de surveillance des flux de fichiers

Vous pouvez désactiver le Module de surveillance des flux de fichiers en utilisant la boîte de dialogue de configuration du Module de détection en tâche de fond. Pour accéder à la boîte de dialogue de configuration, utilisez la commande Options, Programmateur, ou sélectionnez le troisième bouton d'accès rapide. Cochez la case correspondante pour activer la surveillance des flux de fichiers, enlevez la coche pour la mettre hors fonction.

ATTENTION : Si l'option “Active la surveillance des fichiers” est “grisée”, ce qui signifie que vous ne pouvez y accéder, c'est que le pilote de TBAV Windows (qui notifie les modifications à TBAV Windows via le système interne de gestion des fichiers DOS/Windows) n'est pas correctement installé. Réinstallez TBAV Windows en choisissant “Première installation”.

Utiliser le Module de Recherche en Tâche de Fond

Le Module de détection en tâche de fond est particulièrement intéressant. Grâce à lui, vous pourrez analyser régulièrement les disques, les répertoires ou les fichiers.

L'avantage d'un système d'exploitation comme Windows ou OS/2 est la possibilité d'exécuter des applications en arrière plan. En d'autres termes, ces systèmes permettent d'effectuer simultanément plusieurs tâches. La tâche qui nécessite l'intervention de l'utilisateur est la tâche “de premier plan”, alors que les tâches qui se déroulent sans lui sont dites “tâches de fond”. Vous pouvez configurer TBAV Windows en tâche de fond. Il examinera périodiquement les disques, les répertoires ou les fichiers pour y rechercher des virus. C'est à vous de choisir la fréquence de ces analyses

L'analyse en tâche de fond présente deux gros avantages :

1. Les virus sont recherchés pendant que vous effectuez votre travail normalement. En d'autres termes, l'analyse de votre ordinateur ne vous prend pas de temps !
2. De plus, vous n'oublierez plus jamais de rechercher les virus dans votre système, puisque TBAV Windows le fait automatiquement.

Le Module de détection en tâche de fond n'utilise que les temps morts. Par exemple, quand vous tapez du texte, il y a un temps mort, très court, entre deux frappes de touches. Le Module de détection en tâche de fond exploite ce temps mort. Grâce à ce système, vous ne subirez jamais de baisse de performance, ou alors très peu.

Activer le Module de détection en tâche de fond

Avant d'activer le Module de détection en tâche de fond, vous devez vous assurer qu'il est correctement configuré. Pour accéder à la boîte de dialogue de configuration, utilisez la commande Options, Programmateur, ou sélectionnez le troisième bouton d'accès rapide.

Pour plus d'informations, reportez-vous à la section “Configurer le Module de détection en tâche de fond”, plus loin.

Pour activer le Module de détection en tâche de fond, réduisez TBAV Windows en icône.

CONSEIL : Pour réduire en icône une application Windows, Cliquez sur la flèche descendante qui se trouve dans le coin supérieur gauche de la fenêtre. Pour l'agrandir, cliquez sur la flèche ascendante.

Quand vous réduisez TBAV Windows en icône, sa fenêtre principale disparaît, et une petite fenêtre contenant des informations d'état s'affiche en bas de l'écran.

Si vous ne voulez pas voir cette fenêtre d'état, vous pouvez également la réduire en icône. Si vous l'agrandissez par la suite, la fenêtre “normale” de TBAV Windows réapparaît.

Utiliser le Module de détection en tâche de fond

Lorsque vous activez le Module de détection en tâche de fond, la fenêtre d'état apparaît.

La première ligne indique l'état du Module de détection en tâche de fond. Dans cet exemple, l'analyse sera lancée après 154 minutes et 50 secondes. Si vous désactivez le Module de détection en tâche de fond, la première ligne affichera “Recherche en tâche de fond désactivée”.

La deuxième ligne de la fenêtre d'état indique l'unité à contrôler. Vous sélectionnez une unité dans la boîte de

dialogue **Contrôle en tâche de fond**. La dernière ligne affiche la date et l'heure du dernier examen du système (en tâche de fond ou normal).

Quand le Module de détection en tâche de fond commence l'examen de l'unité spécifiée, le contenu de la fenêtre d'état change.
La deuxième ligne affiche maintenant le nom complet du fichier en cours d'examen (ici, C:\JEUX\TOWERS.EXE).

Vous voulez certainement suivre les actions effectuées par le Module de détection en tâche de fond. Cependant, si une application s'exécute en plein écran, la fenêtre d'état sera cachée par cette application. Vous pouvez la configurer pour qu'elle reste toujours visible, c'est-à-dire pour qu'elle soit toujours au premier plan. Pour cela, activez le menu système en cliquant sur la case supérieure gauche de la fenêtre et cliquez sur “Toujours en premier plan”.

REMARQUE : Le menu système n'apparaît que si le Module de détection en tâche de fond n'est pas en train d'effectuer un contrôle. S'il l'est, vous pouvez utiliser la case du menu système pour arrêter le contrôle en tâche de fond. Si vous cliquez sur la case du menu système (ou sur la barre de titre) de la fenêtre d'état pendant que le Module de détection en tâche de fond examine l'unité spécifiée, une boîte de dialogue apparaît et vous demande si vous voulez stopper ou continuer le contrôle en tâche de fond.

Configurer le Module de Détection en Tâche de Fond

Configurer le Module de Détection en Tâche de Fond

Comme nous l'avons vu précédemment, vous pouvez accéder à la boîte de dialogue de configuration soit en utilisant la commande Options, Programmateur, soit en sélectionnant le troisième bouton d'accès rapide. Trois paramètres permettent de configurer le Module de détection en tâche de fond :

“Active la surveillance fichiers.”
Vous pouvez mettre le Module de surveillance des flux de fichiers hors fonction en désactivant cette case. Elle est cochée par défaut.

“Active la surveillance des applications exécutées.”
Vous pouvez mettre le Module de suivi des applications exécutées hors fonction en désactivant cette case. Elle est cochée par défaut.

“Active le Programmateur.”
Vous pouvez mettre le Module de détection en tâche de fond hors fonction en désactivant cette case. Elle est cochée par défaut.

Le Module de détection en tâche de fond comporte quelques options supplémentaires :

“Durée avant lancement du contrôle en tâche de fond.”
Spécifie la période après laquelle le Module de détection en tâche de fond doit commencer l'analyse. La période minimale est 1 minute, et la période maximale est 999 minutes. La période par défaut est 30 minutes. Le compte à rebours commence dès que TBAV Windows est minimisé ou réduit en icône.

“Unités, chemins & fichiers à contrôler.”
Spécifie l'unité qui sera examinée. Si vous sélectionnez le bouton “Unités”, une liste des unités accessibles apparaît pour vous permettre d'en choisir une. La fenêtre d'état affiche l'unité qui sera examinée. L'unité par défaut est LOCAL.SCN, c'est-à-dire l'ensemble de vos disques durs locaux.

“Niveau de priorité.”
Le niveau de priorité du Module de détection en tâche de fond peut être “Haut” ou “Bas”. Si vous choisissez “Haut”, le recherche de virus en arrière plan sera plus rapide, mais les autres applications subiront une perte de performance. Si vous choisissez “Bas”, les applications en cours ne seront pas ralenties, mais le processus de recherche sera plus long.

Vous pouvez changer le comportement de la case de réduction de TBAV Windows en utilisant les “Options de minimisation” :

“Afficher la fenêtre de status.”
Si cette case est cochée, TBAV Windows sera réduit en une petite fenêtre d'état dès que vous cliquerez sur sa case de réduction. La fenêtre d'état contient des informations sur l'état du Module de détection en tâche de fond. Si cette option est désactivée, TBAV Windows sera réduit en icône.

Utiliser le Module de Suivi des Applications Exécutées

Le Module de suivi des applications exécutées intercepte et examine chaque application avant qu'elle ne s'exécute. Les virus doivent d'abord devenir résidents (c'est-à-dire s'implanter dans une petite zone de mémoire) avant de commencer à se propager. Pour cela, presque tous les virus utilisent des fichiers exécutables (fichiers appartenant à des applications). En d'autres termes, un virus ne devient actif qu'au chargement d'une application. Pour minimiser ce risque, TBAV Windows intercepte les applications et les examine avant qu'elles ne soient exécutées.

Activer le Module de suivi des applications exécutées

Par défaut, le Module de suivi des applications exécutées est actif quel que soit le mode de TBAV Windows. Vous pouvez le désactiver en utilisant la boîte de dialogue de configuration du Module de détection en tâche de fond. Pour accéder à la boîte de dialogue de configuration, utilisez la commande Options, Programmateur, ou sélectionnez le troisième bouton d'accès rapide.

Reportez-vous à la section "Configurer le Module de suivi des applications exécutées", plus loin dans ce chapitre, pour savoir comment configurer, activer et désactiver le Module de suivi des applications exécutées.

Utiliser le Module de suivi des applications exécutées

Si vous utilisez TBAV Windows en mode normal (c'est-à-dire ni minimisé ni réduit en icône), le Module de suivi des applications exécutées utilise la barre de titre pour indiquer ce qu'il fait. Chaque fois qu'il examine un fichier ou une disquette, la barre de titre affiche “Scanning...”

La fenêtre d'état, qui apparaît dès que vous minimisez TBAV Windows, affiche également l'activité du Module de suivi des applications exécutées.

REMARQUE : Reportez-vous à la section **Utiliser le Module de détection en tâche de fond**, plus haut dans ce chapitre, pour plus d'informations sur la fenêtre d'état.

Configurer le Module de suivi des applications exécutées

Vous pouvez désactiver le Module de suivi des applications exécutées en utilisant la boîte de dialogue de configuration du Module de détection en tâche de fond. Pour accéder à la boîte de dialogue de configuration, utilisez la commande Options, Programmateur, ou sélectionnez le troisième bouton d'accès rapide. Cochez la case correspondante pour activer le suivi des applications exécutées, enlevez la coche pour le mettre hors fonction.

Informations diverses

Base de données d'informations sur les virus

TBAV Windows comprend une liste exhaustive des virus avec leur description. Cette base de données est particulièrement utile chaque fois que TBAV Windows détecte un virus dans votre système ; vous avez immédiatement accès aux informations concernant le comportement de ce virus et (plus important) à la façon de vous en débarrasser.

Vous pouvez accéder à la base de données d'informations sur les virus de deux façons :

1. Cliquez sur le bouton d'accès rapide “virus info”.

2. Sélectionnez l'option “Informations sur les virus” du menu Documentation.

Une petite boîte de dialogue apparaît, contenant les noms de tous les virus de la base. En voici un exemple :

Vous pouvez rapidement localiser les informations associées à un virus particulier, en tapant les premières lettres du nom du virus dans la zone de texte. La sélection affichée dans la zone de liste se met à jour en fonction du contenu de la zone de texte. Si vous cliquez deux fois sur le nom d'un virus dans la zone de liste, ou si vous cliquez sur le bouton “Voir infos”, à droite, une fenêtre contenant des informations sur le virus s'affiche.

Pour plus d'informations, reportez vous à la section **Base de données d'information sir les Virus**

Configuration générale

Comme vous le savez probablement, le menu Options contient la commande Configuration de TBAVWIN. Si vous la sélectionnez, une boîte de dialogue de configuration s'affiche, vous proposant trois options générales de TBAV Windows.
Pour plus d'informations, consultez **Configuration Générale de TBAV Windows**

Informations sur TBAV Networks

TBAV Windows est totalement compatible avec TBAV Networks. En fait, TBAV Networks nécessite l'exécution de TBAV Windows sur chaque station de travail Windows.

Pour l'instant, nous n'entrerons pas dans les détails concernant l'interaction entre TBAV Networks et TBAV Windows. Si vous voulez davantage d'informations, reportez-vous au Chapitre 6. Nous allons évoquer la visualisation de l'activité du réseau, ainsi que la configuration de l'interface réseau.

Normalement, TBAV Windows affiche l'activité du réseau dans la barre de titre. Si TBAV Windows est occupé à traiter une requête adressée par TBAV for Networks, la barre de titre affiche “Réponse demande réseau...” au lieu de “TBAV Windows.” Si vous minimisez TBAV Windows, c'est la fenêtre d'état qui affiche l'activité du réseau.

Si la partie réseau de TBAV Windows est active, le menu Options contient une option supplémentaire : **Configuration réseau**. Si vous la sélectionnez, une petite fenêtre apparaît, contenant des options de configuration.

Mise à jour automatique

Les produits ThunderBYTE sont régulièrement mis à jour, au moins six fois par an. Dans les entreprises importantes, mettre à jour toutes les stations de travail pourrait être terriblement fastidieux. C'est pourquoi, TBAV

Windows offre un dispositif de mise à jour automatique !

La Mise à jour automatique utilise un répertoire à part, appelé le “répertoire de mise à jour”. Si vous avez activé la Mise à jour automatique, à chaque chargement, TBAV Windows cherchera dans ce répertoire les fichiers modifiés ou nouveaux. S'il en trouve, il les copiera automatiquement dans le répertoire TBAV Windows.
CONSEIL : Si le répertoire de mise à jour est situé sur une unité du réseau, il vaut mieux rendre cette unité accessible aux utilisateurs normaux en lecture seulement. Sinon, ces derniers pourraient y ajouter leurs propres fichiers et TBAV Windows les copierait !

Supposez que vous êtes l'administrateur d'un réseau important utilisé par 800 personnes. Vous avez installé TBAV Windows sur le disque local de chaque station. Deux mois plus tard, vous recevez une mise à jour. Si TBAV Windows ne disposait pas d'une Mise à jour automatique, vous (l'opérateur système) devriez installer manuellement cette mise à jour, sur chacune des 800 stations ! Pour bénéficier de la Mise à jour automatique, il faut créer un répertoire serveur public lors de la première installation de TBAV Windows, activer la Mise à jour automatique et spécifier le répertoire serveur public comme répertoire de mise à jour de TBAV Windows. Ensuite, chaque fois que vous recevrez une nouvelle version de ThunderBYTE Anti-Virus, il vous suffira de copier les fichiers dans le répertoire serveur public pour que TBAV Windows mette automatiquement à jour toutes les stations de travail !

Activer la Mise à jour automatique

La “Mise à jour automatique” doit avoir été activée au cours de la première installation. De plus, vous devez avoir configuré TBAV Windows pour qu'il se charge automatiquement à chaque démarrage de Windows.

Pendant la phase d'installation de la Mise à jour automatique, vous serez invité à spécifier le nom du répertoire de mise à jour, ainsi que le type de mise à jour automatique. TBAV Windows propose deux niveaux de mise à jour automatique :

“Mise à jour des Nouveaux fichiers seulement.”
Si vous choisissez cette option, TBAV Windows conservera la date de la dernière mise à jour automatique. Si le répertoire de mise à jour contient des fichiers créés ou modifiés après cette date, ils seront copiés. Les autres fichiers seront ignorés.

“Mise à jour de tous les fichiers.”
Si vous choisissez cette option, TBAV Windows ne vérifiera pas la date des fichiers contenus dans le répertoire de mise à jour. Tous les fichiers de ce répertoire seront copiés dans le répertoire de TBAV Windows.

Vous pouvez changer de niveau de Mise à jour automatique dans TBAV Windows, en utilisant la commande **Configuration Mise à jour automatic** du menu Options.

REMARQUE : La Mise à jour automatique ne fonctionne que si MSWindows est lancé et si vous avez configuré TBAV Windows pour qu'il se charge au démarrage de MSWindows. La mise à jour automatique ne fonctionne pas si vous chargez TBAV Windows à partir du Gestionnaire de programmes.

Options de Sécurité de TBAV Windows

La configuration de TBAV Windows peut être protégée par les **Options de Sécurité**. Ces options peuvent être modifiées via le menu "Options|Options de Sécurité" de TBAV Windows.
Ces options de sécurité ne sont accessibles qu'aux utilisateurs enregistrés.

Configuration Générale de TBAV Windows

Ces options peuvent être modifiée via l'option 'Configuration de TBAV Windows' du menu 'Options'

“Attendre après toute exécution.”
Si vous activez cette option, TBAV Windows attendra lorsque le Module de configuration ou le Module de détection aura cessé son activité. Si vous la désactivez, TBAV Windows reviendra immédiatement à la fenêtre principale dès que ces modules auront cessé leur activité. Cette option est cochée par défaut.

“Utilitaire de visualisation.”
Comme nous l'avons indiqué précédemment, l'afficheur interne de TBAV Windows vous permet de voir et même d'imprimer le fichier de données de TbSetup ou le fichier historique créé par le Module de détection. Mais, si vous préférez utiliser votre propre éditeur, tapez son nom dans la zone de texte.
CONSEIL : Vous pouvez utiliser Microsoft Write pour visualiser les fichiers, en entrant C:\WINDOWS\WRITE.EXE. Lorsque Write est lancé, choisissez le bouton “Pas de conversion”. Vous pouvez également utiliser le Bloc-Notes, en entrant C:\WINDOWS\NOTEPAD.EXE.

“Fenêtre d'alerte virus.”
TBAV Windows peut émettre des sons sur le haut-parleur interne du PC ou sur une carte son lorsqu'il découvre un virus. En sélectionnant l'option "Alarmes sonores", vous pouvez indiquer quel son TBAV Windows doit émettre, et dans quelles conditions. Vous pouvez choisir un simple beep', ou un son au format WAV (option "Alarme : Fichier WAV").
Avec l'option "Toujours" TBAV Windows émet un son à chaque fois qu'il détecte un virus. "Une seule fois" indique que TBAV Windows n'émettra un son que lors de la première détection d'un virus (option par défaut). "Arrière-plan" indique que TBAV Windows n'émettra un son que lors de la détection en tâche de fond. Vous pouvez également désactiver les effets sonores en sélectionnant l'option "Jamais".
REMARQUE : Le compteur de virus est remis à zéro chaque fois que TBAV Windows démarre.

L'option "Fenêtre d'alarme flashante" peut être utilisée pour donner encore plus de relief à la détection d'un virus.

“Messages d'information”
Un message d'information est affiché lorsque le driver virtuel Windows (VxD) de TBAV Windows n'est pas chargé. Lorsque ce driver n'est pas actif, la surveillance des Entrées/Sorties et des Applications Exécutées est désactivée, un message averti donc l'utilisateur de ce fait. Vous pouvez désactiver l'affichage de ce message via l'option "messages d'information" dans la fenêtre de configuration générale de TBAV Windows.

Par défaut, un message d'avertissement est affiché lorsque TBAV Windows va être fermé, car la fermeture de TBAV Windows désactive toutes les fonctionnalités de détection des vireus 'au vol' de TBAV Windows. Il est possible de désactiver ce message via cette option.

Configuration Réseau

On peut accéder à la fenêtre de configuration Réseau en activant l'option "Configuration Réseau" du menu 'Options'. Les éléments suivants peuvent être modifiés :

“Asynchronous request timeout.”
Grâce à cette option, vous pouvez définir dans quel délai une station de travail doit répondre à une requête asynchrone. Les requêtes asynchrones sont lancées par des procédures de TBAV for Networks. La valeur entrée ici doit être supérieure à 5000 millisecondes.

“Message scan time.”
TBAV Windows utilise cette option pour définir après quel délai TBAV Windows doit vérifier s'il y a des messages en attente, envoyés par TBAV for Networks. Le temps indiqué doit être compris entre 100 et 9999 millisecondes.

“Blocking message scan time.”
Les messages bloquants sont des messages qui interrogent immédiatement le serveur. Utilisez cette option pour définir après quel délai TBAV Windows doit vérifier s'il y a des messages bloquants en attente. Le temps indiqué doit être compris entre 100 et 9999 millisecondes.

“Blocking request timeout.”
Cette option permet de spécifier dans quel délai une station de travail doit répondre à une requête bloquante. Ce délai d'attente doit être compris entre 5000 et 99999 millisecondes
Pour valider les modifications, sélectionnez le bouton “OK”.
ATTENTION : Les modifications ne seront prises en compte qu'au redémarrage de TBAV Windows.

Configuration de la Mise à jour Automatique

Pendant la phase d'installation de la Mise à jour automatique, vous serez invité à spécifier le nom du répertoire de mise à jour, ainsi que le type de mise à jour automatique. TBAV Windows propose deux niveaux de mise à jour automatique :

“Mise à jour des Nouveaux fichiers seulement.”
Si vous choisissez cette option, TBAV Windows conservera la date de la dernière mise à jour automatique. Si le répertoire de mise à jour contient des fichiers créés ou modifiés après cette date, ils seront copiés. Les autres fichiers seront ignorés.

“Mise à jour de tous les fichiers.”
Si vous choisissez cette option, TBAV Windows ne vérifiera pas la date des fichiers contenus dans le répertoire de mise à jour. Tous les fichiers de ce répertoire seront copiés dans le répertoire de TBAV Windows.

Vous pouvez changer de niveau de Mise à jour automatique dans TBAV Windows, en utilisant la commande **Mise à jour automatic** du menu Options.

REMARQUE : La Mise à jour automatique ne fonctionne que si MSWindows est lancé et si vous avez configuré TBAV Windows pour qu'il se charge au démarrage de MSWindows. La mise à jour automatique ne fonctionne pas si vous chargez TBAV Windows à partir du Gestionnaire de programmes.
ger.

Base de donnée d'Information Virus

Vous pouvez rapidement localiser les informations associées à un virus particulier, en tapant les premières lettres du nom du virus dans la zone de texte. La sélection affichée dans la zone de liste se met à jour en fonction du contenu de la zone de texte. Dans cet exemple, nous avons tapé “Smiley_” et Smiley_Boot est apparu dans la zone de liste. Si vous cliquez deux fois sur le nom d'un virus dans la zone de liste, ou si vous cliquez sur le bouton “Voir infos”, à droite, une fenêtre contenant des informations sur le virus s'affiche.

Pour plus d'informations sur la fenêtre d'information virus, reportez-vous à **Détecter un Virus**.

Les fichiers "What's New ?"

Lorsque vous activez l'opton "Quoi de Neuf ?", une petite fenêtre de dialogue apparaît contenant le nom des fichiers d'information sur les mises à jour du répertoire TBAV. Chaque fichier a une extension relative au numérode version de TBAV. Par exemple, le fichier "Quoi de Neuf ?" de la version 7.00 de TBAV Windows s'appelle TBAVWNEW.700, tandis que celui de la version 7.00 DOS Dos s'appelle WHATSNEW.700.

Comment contacter un agent ThunderBYTE

A propos de ThunderBYTE

Les utilitaires ThunderBYTE Anti-Virus (TBAV) représentent la nouvelle génération de logiciels de détection et d'éradication des virus informatiques connus et inconnus. Ces utilitaires comportent 5 niveaux de sécurité différents pour vous protéger des virus : une technologie de détection basée sur des signatures et sur une analyse heuristique, un décryptage générique basé sur un émulateur de code, un contrôle d'intégrité des fichiers et une surveillance active de la machine.

Créés en Europe pour combattre l'avancée des nouveaux virus toujours plus intelligents et sophistiqués, ThunderBYTE Anti-Virus est, depuis plusieures années, le meilleur logiciel anti-virus du marché et également le scanneur le plus rapide au monde. Combinant des techniques traditionnelles et d'avant-garde (comme l'analyse heuristique des fichiers) pour débusquer les virus les plus récents et les plus furtifs, les chevaux de Troie et le bombes logiques, ces utilitaires offrent une protection anti-virus maximale à une vitesse encore inégalée dans le monde PC.

Ventes, Support Technique et Mises à jour de ThunderBYTE Anti-Virus

Pour des utilisateurs expérimentés, pas de compromis; seul le meilleur prévaut. Sur le marché des anti-virus, un produit domine largement la compétition quand il s'agit de puissance et de rapidité : les utilitaires ThunderBYTE Anti-Virus. ThunderBYTE est à la fois le moteur de détection de virus le plus rapide et le plus avancé technologiquement au monde.

ThunderBYTE est commercialisé dans le monde entier par des agents officiels spécialement entrainés au support technique anti-virus.

En France, **Delta Logic Sarl** - importateur exclusif -, **ses Distributeurs Conseils et son réseau de revendeurs** sont à votre disposition pour tout renseignement commercial ou technique.
Un serveur de téléchargement ouvert 24 heures sur 24 (Thunder-BBS : +33 (1) 41.21.00.13 - 8N1 - 28 800 bps - ANSI) permet de télécharger les mises à jour ou des versions d'évaluation.

Les agents ThunderBYTE en France

La liste complète des revendeurs des produits ThunderBYTE est disponible dans le fichier **Agents.Doc** via l'option **Documentation|Liste des agents officiels'** de menu de TBAV Windows.

Pour avoir la liste à jour des partenaires (Distributeurs Conseils et Revendeurs) de **Delta Logic Sarl** ou pour tous renseignement technique, vous pouvez nous contacter aux coordonnées ci-dessous :

Importateur

DELTA LOGIC

11, avenue Marc Sangnier
92398 VILLENEUVE-LA-GARENNE Cedex
Tél : +33 (1) 41.21.90.55 - Fax : +33 (1) 41.21.90.56
BBS : +33 (1) 41.21.00.13 [8N1 - 28 800 bps - ANSI]
E-mail : 100641.3111@compuserve.com

Configurer le Module de Surveillance d'Exécution des Fichiers

Les différentes options du module de Surveillance des Applications Exécutées de TBAV Windows sont présentées dans cette section. Ces options peuvent être modifiées via le menu "Options|Configuration Surveillance Applications Exécutées".

Activer la Surveillance des Applications Exécutées
Vous pouvez activer ou désactiver le module de Surveillance des Applications Exécutées avec cette option. **ATTENTION :** La désactivation de la Surveillance des Applications Exécutées augmentera les chances d'aggression de votre ordinateur par les virus. La Surveillance des Applications Exécutées est active par défaut.

Mode Sécurisé (Pas d'exécution des fichiers non autorisés)
Si cette option est active, le module de Surveillance des Applications Exécutées interrompera toute l'exécution de toute application non autorisée par TBAV. Toute application non traitée par TbSetup (*i.e.* pas d'empreinte (checksum) des fichiers exécutables), ou dont l'empreinte a été modifiée (attaque possible par un virus), est considérée comme non autorisée. Si le "Mode Sécurisé" est désactivé, TBAV Windows vous demandera si vous désirez vraiment exécuter une application non autorisée.

Vérification d'absence d'enregistrement Anti-Vir.Dat
Les empreintes et informations complémentaires sont stockées dans des fichiers "Anti-Vir.Dat". Si un tel fichier est absent d'un répertoire, les applications situées dans ce répertoire sont qualifiées de "non autorisées".
Vous pouvez forcer TBAV Windows à ignorer ce type de fichiers non autorisés sur votre système en activant l'option "Ne jamais contrôler l'absence d'empreinte".
Si vous ne désirez ignorer l'absence de fichiers Anti-Vir.Dat que sur certains disques (disques en lecture-seule comme les CD-ROM par exemple), vous pouvez utiliser l'option "Ne pas contrôler sur des disques donnés".
Pour être absolument sûr qu'aucun virus n'entrera dans votre système, vous devez choisir l'option "Toujours contrôler l'absence d'empreintes".

Si différence d'empreinte (checksum)
Les exécutables dont l'empreinte de correspondent pas à celle stockée dans le fichier Anti-Vir.Dat sont répertoriés comme "fichiers non autorisés". Afin de préciser le type d'action à suivre lorsqu'un tel fichier est exécuté, vous pouvez choisir l'une des cinq options suivantes. La première présente un menu vous permettant de choisir le type action à effectuer lorsqu'un tel fichier est exécuté. La seconde permet de continuer si le "Mode Sécurisé" est désactivé; sinon l'exécution est interrompue. Autrement, vous pouvez effacer, détruire ou renommer le fichier exécutable.

Options de Sécurité

La configuration de TBAV Windows peut être protégée par les Options de Sécurité présentées ci-dessous. Ces options peuvent être modifiées via le menu "Option|Security Options" de TBAV Windows.

Modifier les options de TbScan
Si désactivé, l'utilisateur ne pourra modifier aucun paramètre de TbScan.

Modifier les options de TbSetup
Si désactivé, l'utilisateur ne pourra modifier aucun paramètres de TbSetup.

Modifier les options Recherche en Tâche de Fond
Si désactivé, l'utilisateur ne pourra modifier aucun paramètres de la recherche en tâche de fond.

Modifier la Surveillance des Entrées / Sorties de fichiers
Si désactivé, l'utilisateur ne pourra activé ou désactivé la Surveillance des Entrées / Sorties de fichiers de TBAV Windows.

Modifier la Surveillance des Applications Exécutées
Si cette option est désactivée, l'utilisateur ne pourra modifier la configuration de la Surveillance d'Exécution des Applications.

Modifier les options de TbLoad
Si cette option est désactivée, l'utilisateur ne pourra modifier la configuration de TbLoad (module de chargement / mise à jour de TBAVpour Windows).

Modifier les options de TBAV-for-Networks
Si cette option est désactivée, l'utilisateur ne pourra modifier la configuration de TBAV for Networks. Si ce produit n'est pas installé, cette option est inactive.

Sauver les unités prédéfinies
Si cette option est désactivée, l'utilisateur ne pourra pas enregistrer d'unités prédéfinies. En utilisant cette option, un administrateur peut créer des unités prédéfinies standards non modifiables.

Scanner les disques réseaux
Si cette option est désactivée, l'utilisateur ne pourra pas analyser les disques réseaux. Cette option peut être utile en environnement réseau où les utilisateurs ont tendance à scanner tous les disques, causant ainsi des surcharges du traffic.

Continuer si détection de fichier infecté ou modifié
Si cette option est désactivée, l'utilisateur ne sera pas autorisé à continuer lors de la détection d'un fichier infecté; sauf entrée du mot de passe système.

Exécuter TbSetup
Si cette option est désactivée, l'utilisateur ne pourra pas exécuter TbSetup. L'exécution de TbSetup ne se fait généralement qu'une seule fois, et l'exécution régulière de TbSetup peut compromettre la détection de certains type de virus par TbScan. La désactivation de cette option permet d'éviter que des utilisateurs novices n'exécutent accidentellement TbSetup.

Quitter TBAV Windows
Si désactivé, l'utilisateur ne pourra pas quitter TBAV Windows.

Mot de passe
L'administrateur système peut modifier le mot de passe en pressant ce bouton. Votre ancien mot de passe vous sera d'abord demandé, puis le nouveau et sa confirmation.