ALWIL SOFTWARE

avast32

Le programme anti-virus complet pour
Windows 95
Windows NT

Design: Jan Parizek, ALWIL Software
Editeur: Roman Svihalek, ALWIL Software
Traduction: Calyx Data Control
Cette documentation a été rédigée, illustrée et publiée en utilisant
Adobe PageMaker 6.5 CZ et Adobe Acrobat 3.0

ALWIL Software, Lipi 1244
193 00 Praha 9 - Horni Pocernice
République Tchèque
Tél. : (+420 2) 819 216 61, 819 216 62

Table des matières

1.Introduction

Cher client, Nous vous félicitons d'avoir acheté le programme anti-virus AVAST32, l'un des meilleurs dans sa catégorie. Nous espérons que vous serez satisfait de notre produit et que vous apprécierez le confort de travailler avec ce programme.

AVAST32 est un ensemble d'applications ayant pour but de protéger votre ordinateur contre des attaques virales. Si vous l'utilisez correctement et à des intervalles réguliers, conjointement avec d'autres applications comme, par exemple, les programmes de sauvegarde (Backup), vous pourrez réduire radicalement le risque d'une infection virale de votre ordinateur et ainsi éviter la perte de vos données.

Le but de cette documentation est de familiariser même des utilisateurs moins expérimentés avec les commandes du programme AVAST32 et de leur permettre de profiter pleinement de toutes ses fonctions et propriétés. Cependant, nous n'oublions pas non plus les utilisateurs « hautement expérimentés » qui trouveront également dans cette documentation les descriptions d'opérations d'applications individuelles.

Ce manuel a été élaboré de façon à familiariser continuellement le lecteur avec les propriétés et en particulier avec les fonctions de l'ensemble du programme, mais aussi avec ses modules individuels. Nous présupposons une bonne connaissance des termes et techniques de bases de l'environnement des systèmes d'exploitation Windows 95 ou NT, sans lesquelles quelques éléments de ce manuel pourraient vous paraître relativement incompréhensibles. Si vous ne savez rien des dossiers, des fichiers, des fenêtres, ou comment ouvrir une fenêtre ou appuyer sur un bouton, nous vous recommandons d'étudier le manuel d'utilisateur ou de consulter le programme d'aide du système d'exploitation.

Si vous rencontrez des problèmes ou des questions dans l'exécution de ce programme, n'hésitez pas à contacter votre revendeur ou la société ALWIL Trade. Leurs représentants seront à votre disposition pour vous aider.

Le personnel d'ALWIL Software vous souhaite du bon travail avec votre ordinateur, et sans tomber sur des virus.

1.1 Exigences techniques

Afin de réussir à installer AVAST32 sur votre ordinateur et de vous en servir ensuite sans problèmes, le système de votre ordinateur devrait remplir certaines conditions de base. Selon les standards actuellement appliqués, il s'agit de conditions vraiment minimes :

- au moins un processeur 80386 ou compatible,
- une mémoire vive de 8 Mo pour des opérations sous Windows 95 et de 16 Mo pour Windows NT,

- 10 Mo d'espace libre sur votre disque dur pour le programme + 2 Mo pour l'installation,
- Windows 95 ou Windows NT 3.51 ou plus,
- même si AVAST32 peut être utilisé avec un clavier, nous vous recommandons l'utilisation d'une souris ou d'un autre périphérique.

En général, plus votre ordinateur est performant, plus des applications particulières répondent rapidement.

L'exécution d'AVAST32 sur un ordinateur ayant une mémoire vive de moins de 8 Mo n'a pas été testée !

La durée d'exécution du système d'exploitation sur un tel ordinateur est si lente qu'une charge supplémentaire rend toute autre application pratiquement impossible.

Toutefois, il est probable que AVAST32 fonctionnera même sur ces ordinateurs, mais nous le recommandons uniquement à des utilisateurs vraiment très patients.

1.2 Installation

AVAST32 est fourni sur CD-ROM (ou sur plusieurs disquettes) en fichiers compressés et ne peut donc pas être utilisé immédiatement. Un programme d'installation créant toutes les applications a été conçu pour une installation facile.

Le programme d'installation d'AVAST32, copie les fichiers nécessaires sur votre disque dur, effectue toutes les modifications nécessaires dans votre système et configure le démarrage automatique de la protection active au redémarrage du système d'exploitation (La tâche « Résident: protection active » sera lancée automatiquement, voir chapitre 2.6).

1.2.1 Avant de commencer l'installation...

Manipulez le CD-ROM d'installation avec prudence et rangez le immédiatement après l'installation dans un endroit sûr. Si le support d'installation est endommagé, le programme ne pourra pas être installé.

Si vous avez la version sur disquettes, nous vous recommandons de faire, avant toute opération, une copie de sauvegarde des disquettes d'origine. Vous aurez besoin du même nombre de disquettes haute densité (marquées HD). Pour copier le contenu des disquettes, nous vous recommandons la commande DOS DISKCOPY. Pour toute utilisation ultérieure, utilisez uniquement ces nouvelles disquettes et garder les originaux dans un endroit sûr.

Avant de commencer, assurez-vous que vous travaillez vraiment sous le système d'exploitation Microsoft Windows 95 ou Microsoft Windows NT. Si vous utilisez par exemple Microsoft Windows 3.x avec Win32, vous ne pourrez utiliser ni AVAST32, ni son programme d'installation. Le résultat le plus probable lors d'un essai de démarrage sera une « erreur système » de votre ordinateur. Dans ce cas, essayez d'installer le programme AVAST!.

En outre, assurez-vous qu'aucune ancienne version d'AVAST32 n'est installée sur votre ordinateur. Si oui, essayez de la désinstaller. La description de la désinstallation d'une version d'AVAST32 se trouve dans le manuel d'utilisateur ou dans le programme d'aide. Si non, le programme

d'installation essaiera de désinstaller lui-même l'ancienne version. Nous ne recommandons pas cette procédure.

Afin de pouvoir installer AVAST32 sous l'environnement de Windows NT, vous aurez besoin d'avoir les droits d'accès d'un administrateur réseau. Dans la négative, le programme d'installation vous informera de ce fait et refusera d'installer le programme ! Dans ce cas, contactez l'administrateur réseau.

Si vous souhaitez vous servir de l'aide d'AVAST32, vous devez installer le programme **Acrobat Reader** avant de lancer AVAST32 (nous recommandons de l'installer avant AVAST32, sinon vous serez averti par le programme d'installation que Acrobat Reader n'est pas présent sur votre disque dur. Vous trouverez le programme d'installation d'Acrobat Reader AR32E30.EXE sur le CD dans le répertoire ACROWIN. L'installation d'Acrobat Reader est similaire à celle d'AVAST32 et s'effectue automatiquement, sauf pour la question dans quel répertoire vous souhaitez installer le programme.

Il est déconseillé d'installer Acrobat Reader dans le même répertoire qu'AVAST32. Une telle installation entraînerait des incompatibilités entre les programmes et la désinstallation ne fonctionnerait pas aussi bien non plus. Nous recommandons d'installer les programmes dans des répertoires par défaut. AVAST32 pourra trouver Acrobat Reader partout sur votre disque dur.

Si toutes les conditions sont remplies, vous pourrez installer le produit.

1.2.2 Menu de démarrage

Vous pourrez lancer l'installation d'AVAST32 de plusieurs façons. La méthode la plus simple est de se servir d'un outil spécialement créé à cet effet dans votre système d'exploitation. Premièrement, enlevez toutes vos disquettes et CD-ROM des lecteurs et insérez le CD d'installation d'AVAST32 (ou la première disquette si vous avez la version sur disquettes). Faites un clic avec le bouton gauche de la souris sur « Démarrer », « Paramètres » et « Panneau de configuration » (fig. 1).

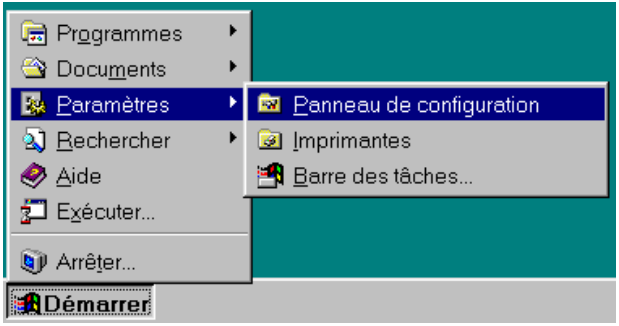

fig. 1

Après, une fenêtre avec plusieurs icônes apparaît. Faites un double clic avec le bouton gauche de la souris sur « Ajout/Suppression de Programmes » (fig. 2).

fig. 2

Dans l'écran suivant, cliquez sur « Installer... », ensuite sur « Suivant > ». L'ordinateur trouvera automatiquement le programme d'installation et la seule chose qui vous reste à faire est de cliquer sur « Fermer ». La procédure d'installation est décrite de façon plus détaillée au chapitre suivant.

Des utilisateurs plus expérimentés peuvent également exécuter directement le programme « Setup.exe » sur le CD-ROM d'installation ou sur la première disquette d'installation (si vous installez à partir de disquettes). L'exécution du programme est décrite en détail dans le manuel ou dans le programme d'aide du système d'exploitation. Pour les autres utilisateurs, nous vous recommandons la première méthode d'installation décrite ci-dessus.

Toutes les méthodes sont identiques et aboutiront au même résultat.

1.2.3 Installation

L'installation du programme AVAST32 s'effectue sous forme d'un dialogue entre l'utilisateur et le programme d'installation.

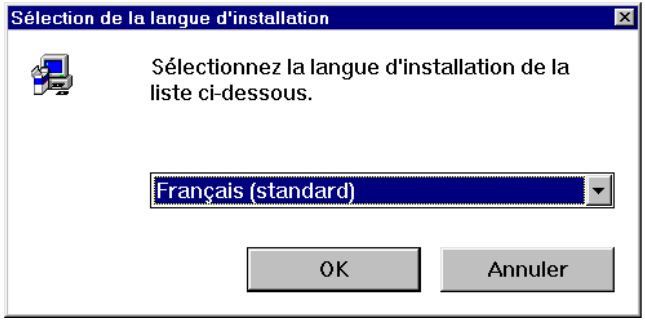

fig. 3

Nous allons décrire ci-après en détail les différents écrans qui s'afficheront au cours de l'installation.

Au démarrage d'AVAST32, vous avez la possibilité de choisir la langue dans laquelle vous souhaitez communiquer avec le programme (Fig. 3). La sélection s'effectue dans une liste qui apparaît en cliquant sur la flèche à droite de la langue actuelle.

On vous demandera de patienter pendant que l'installation prépare le choix de la langue.

fig. 4

Une fois l'installation terminée, vous verrez programme d'installation s'afficher (Fig. 4). La fenêtre de l'Assistant d'installation se trouve au centre et vous guidera sur tout le processus d'installation. La partie inférieure affiche trois boutons de communication avec l'Assistant.

Le bouton « < Précédent » vous ramène à l'écran précédent de l'Assistant. S'il ne peut être utilisé, c'est-à-dire si vous êtes à la première étape telle qu'affichée à la fig. 4, le bouton sera grisé. Le bouton « Suivant > » vous amène à l'étape suivante de l'Assistant. Avant de cliquer dessus, nous vous recommandons cependant de lire soigneusement le contenu affiché sur écran. Vous pourrez interrompre le processus d'installation à tout moment avec le bouton « Annuler ».

Le premier écran affiche les droits d'utilisation et met en garde l'utilisateur contre l'utilisation illicite de certaines parties du programme. Après lecture, vous pourrez ouvrir l'écran suivant en cliquant sur « Suivant > ».

La fenêtre d'installation suivante vous présente l'accord de Licence entre vous et ALWIL Software (fig. 5). Cet accord contient les conditions et les droits d'utilisateur que vous devez reconnaître en tant qu'utilisateur d'AVAST32. Si vous êtes d'accord avec tout, activer le bouton « Oui ». L'Assistant d'installation vous amènera à l'étape suivante. Si, les conditions ne vous convenant pas, vous activez « Non », vous annulez le programme d'installation et AVAST32 ne sera pas installé.

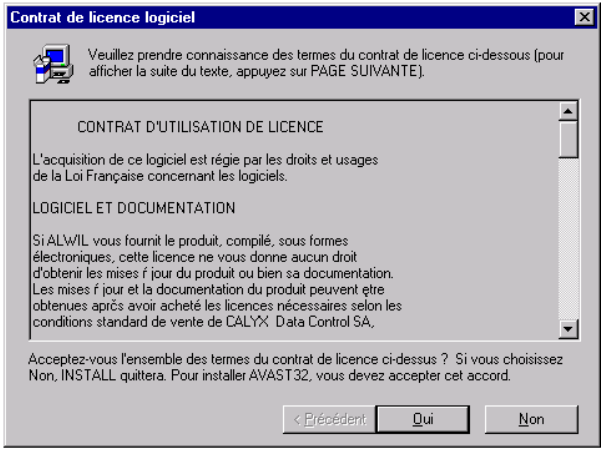

fig. 5

L'accord de licence étant plus long que la place disponible dans la fenêtre, il ne pourra pas être affiché dans sa totalité. Vous trouverez sur la droite de la fenêtre la barre fléchée afin de faire défiler le texte. L'indicateur vous montre en même temps la position exacte. Vous pourrez également vous servir des touches fléchées à droite de votre clavier signifiant page suivante ou page précédente pour afficher les autres pages de l'accord.

L'écran suivant affiche le fichier « LISEZMOI.TXT ». Ce fichier contient d'importantes informations que nous n'avons pas eu le temps d'inclure dans ce manuel. Ces renseignements pourront concerner le programme mais aussi l'installation, par exemple, ainsi que des instructions sur la façon de résoudre d'éventuels problèmes. Dans tous les cas, vous devrez lire soigneusement le fichier « LISEZMOI.TXT » pour éviter d'éventuels problèmes à l'avenir.

Il est possible de faire défiler ce texte de la même façon que l'accord de licence. Les commandes de la fenêtre sont les mêmes. Si vous avez lu le fichier « LISEZMOI.TXT » et activé « Oui », vous arriverez au bouton suivant. Le bouton « précédent » vous ramènera à la fenêtre précédente avec l'accord de licence et en activant « Non », vous annulerez l'installation d'AVAST32.

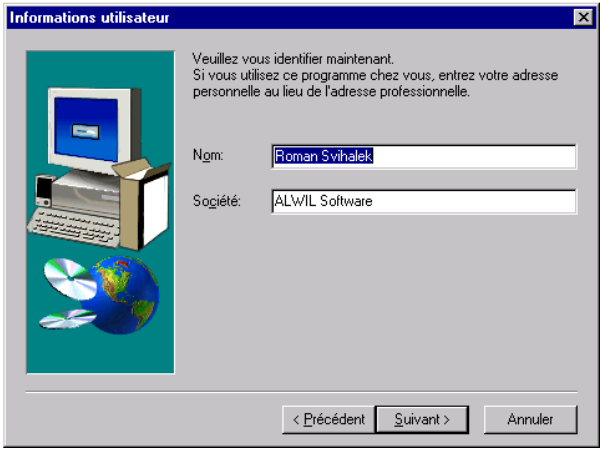

fig. 6

Dans l'écran suivant (fig. 6), l'Assistant d'installation vous demande de saisir votre nom et celui de votre entreprise (éventuellement aussi votre adresse personnelle, si l'installation se fait chez vous). L'Assistant d'Installation essaiera de trouver tout seul le renseignement demandé afin que la plupart des utilisateurs puissent confirmer des données déjà affichées. Si les données ne correspondent pas à la réalité, il est naturellement possible de les corriger. Si vous cliquez avec le bouton gauche de votre souris dans la ligne de texte avec les données en question, vous pourrez modifier celles-ci. Le curseur apparaîtra là où vous avez cliqué avec la souris et vous pourrez entrer les données correctes à l'aide du clavier.

Si les données correspondent à votre situation, veuillez confirmer en cliquant sur « SUIVANT » ce qui vous amène à la fenêtre suivante. Le bouton « PRECEDENT » vous ramène vers le fichier « Lisez-moi » et le bouton « ANNULER » arrêtera l'installation.

Figure 7 affiche la fenêtre dans laquelle vous devez saisir le numéro de série de votre programme. Ce numéro se présente sous la forme suivante : AABBB.CDDDDDD-EEEEEE. La première partie du numéro (AABBB) est déjà affichée par l'Assistant d'Installation et les autres chiffres doivent être complétés. La partie CDDDDDD devrait être saisie dans la case centrée et la partie EEEEEE à droite. Vous pourrez saisir ou modifier des données dans les cases en faisant un clic avec le bouton gauche de votre souris. Vous pourrez également passer dans la case suivante à l'aide de la touche de tabulation.

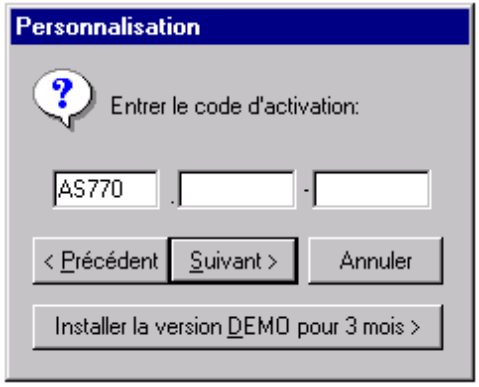

fig. 7

Faites attention en saisissant le code d'activation. Le programme ne peut pas être installé sans un code valable! Si vous ne connaissez pas le code, vous pourrez installer la version d'évaluation en cliquant sur « Installer la version DEMO pour 3 mois > ».

Confirmez le code d'activation à l'aide de la touche « Suivant > ». Si vous avez correctement saisi le bon code, l'assistant d'installation vous laissera continuer. Dans le cas contraire, un message d'erreur s'affichera et vous devrez vérifier le code d'activation. Avec la touche « < Précédent » vous pourrez retourner dans la fenêtre d'enregistrement pour changer le nom ou le nom de l'entreprise. Avec la touche « Annuler » vous quittez le programme d'installation.

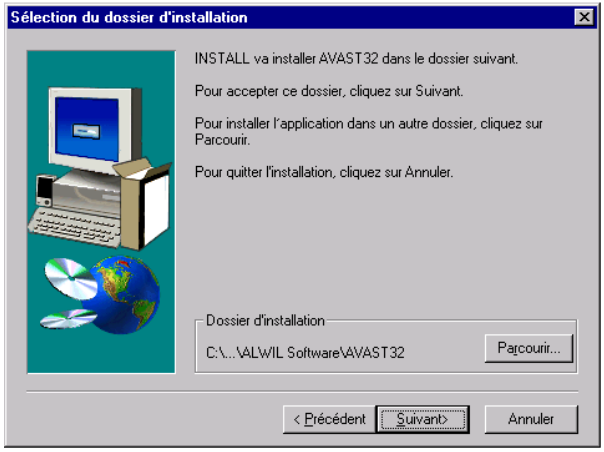

fig. 8

Si le code est correctement saisi, une fenêtre proposant le changement du répertoire cible pour installer AVAST32 s'affichera (Figure 8). Le répertoire figure dans le cadre « Dossier d'installation ». « ALWIL Software\AVAST32 » est le répertoire par défaut qui se crée dans le répertoire « Program files » sur votre disque dur. Nous recommandons cette procédure pour la plupart des utilisateurs. D'autres pourraient choisir le répertoire cible en cliquant sur la touche « Parcourir... » (Figure 9). Nous conseillons vraiment l'installation dans le répertoire par défaut aux utilisateurs moins avancés. Ils éviteront ainsi d'éventuels problèmes.

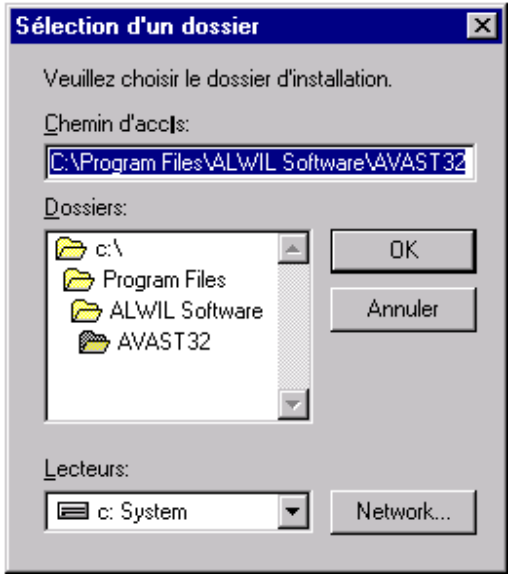

fig. 9

La fenêtre représentée sous Fig. 10 suit la fenêtre de la sélection du répertoire cible. La liste des modules se trouve en haut de la fenêtre. Vous pourrez choisir les modules que vous souhaitez installer ensemble avec AVAST32, par exemple le support en langue allemande. Ceci vous permettra de choisir la langue en utilisant AVAST32.

Vous pourrez changer le répertoire cible dans cette fenêtre en cliquant sur « Parcourir... » (Fig. 9). L'utilisateur pourra également observer s'il lui reste de l'espace libre

sur les disques durs. Vous confirmerez les éléments et le répertoire cible sélectionnés en cliquant sur « Suivant > ».

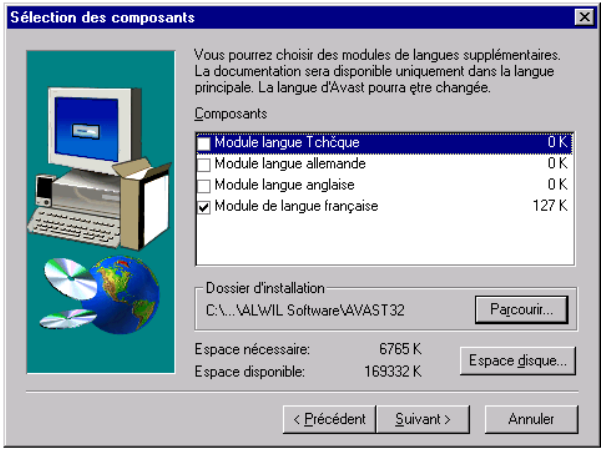

fig. 10

L'écran suivant affiche les informations précisées durant l'installation ou disponibles sur la machine : Nom d'utilisateur, Nom Société, adresse, Numéro de série et Répertoire d'installation d'Avast32. Vérifiez que ces informations soient correctes. Si elles le sont, cliquez sur « Suivant > » pour lancez l'installation. Sinon, cliquez sur le bouton « < Précédent » et apportez-y les corrections souhaitées. Le bouton « Annuler » vous permet d'interrompre l'installation.

La fenêtre centrale contient les informations sur le pourcentage des fichiers déjà installés sur votre disque dur. L'installation peut être interrompue à l'aide du bouton en bas à droite de l'écran ou avec la touche F3 de votre clavier. Une fois tous les fichiers installés, une nouvelle fenêtre sera ouverte automatiquement.

La dernière fenêtre de l'Assistant d'Installation est représentée à la fig. 11. Elle affiche les boutons à activer pour redémarrer l'ordinateur tout de suite ou plus tard. Nous vous recommandons d'activer le bouton affiché par défaut. A la fin de l'installation, vous terminerez le programme et suivant votre choix, l'ordinateur sera redémarré ou non.

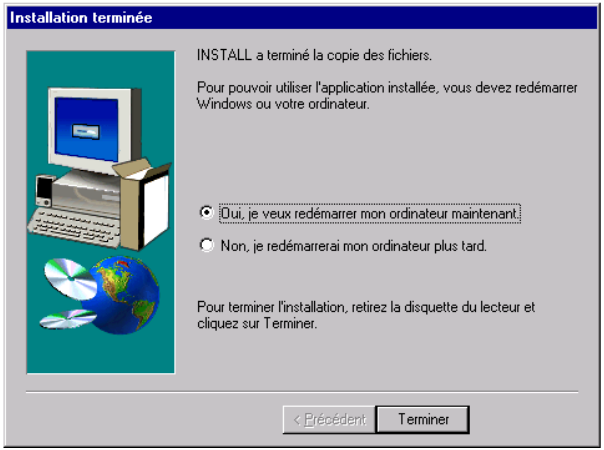

fig. 11

Après l'installation du programme AVAST32 et avant sa première exécution, il faut redémarrer l'ordinateur. Si vous ne l'avez pas fait à l'aide de l'Assistant d'Installation, vous devez le faire vous-même plus tard. Dans le menu de démarrage, choisissez la commande « Arrêter », ensuite activez « Redémarrer l'ordinateur ? » dans la fenêtre affichée et cliquez sur « Oui ».

1.2.4 Problèmes d'installation

Veuillez trouver ci-après une liste des problèmes les plus fréquents rencontrés lors de l'installation d'AVAST32:

- vous ne pouvez pas installer le programme à cause d'une erreur de numéro de série. Vous avez saisi un numéro de série incorrect. Le numéro de série a le format AABBB.CDDDDDD-EEEEEE (déjà décrit dans l'annexe D).
- Assurez-vous qu'il a vraiment été saisi correctement. Si vous en êtes sûr et si vous n'avez vraiment pas tapé la lettre O à la place du 0 (et l'inverse) et s'il n'y a pas d'espace ni de tiret (entre les cases de texte), contactez ALWIL Trade ltd. (à l'adresse fournie sur la boîte contenant le CD-ROM) et demandez une vérification de votre numéro de série.
- AVAST32 ne peut être installé par manque de mémoire sur votre disque dur. Le seul conseil dans ce cas-là est d'annuler l'installation, de faire de la place sur votre disque, c'est-à-dire de vider la corbeille, supprimer des programmes inutiles, de vieux fichiers etc. (nous vous recommandons de faire d'abord une copie de sauvegarde de tout ce qui doit être supprimé et de ne procéder qu'ensuite à la suppression). Pour une installation réussie du programme AVAST32, vous aurez besoin d'environ 10 + 2 Mo d'espace libre sur le disque dur sur lequel vous souhaitez installer le programme. Une fois fini, procédez à l'installation à nouveau et répétez la procédure d'installation.
- le programme ne peut pas être installé pour manque de droits suffisants (uniquement Windows NT). Vous avez besoin de droits d'administrateur système pour l'installation d'AVAST32 sous Windows NT. Déconnectez-vous et reconnectez-vous en tant qu'administrateur système ou contactez votre administrateur système.

Si d'autres erreurs d'installation se présentent, il faut être sûr qu'elles ne soient pas de votre fait ou ne proviennent pas de votre système. Si vous avez totalement éliminé tout problème venant de votre côté, n'hésitez pas à contacter l'assistance technique. Cependant, nous vous demandons de bien noter tous les messages d'erreur.

1.2.5 Installation à partir d'autres supports

Le programme AVAST32 peut également être installé à partir de tout autre support qu'un CD-ROM ou des disquettes. Cette procédure a l'avantage d'une plus grande rapidité d'installation (qui pourra se trouver réduite suivant le type de support utilisé) ou en cas d'une installation sur réseau. Dans ce cas précis, il est nécessaire de copier les répertoires DISK1, DISK2, etc. du CD-ROM d'installation sur le support effectuant l'installation (si vous utilisez des disquettes, vous devez d'abord créer des répertoires et copier ensuite les disquettes de distribution ou les copies dans

ces répertoires en tenant compte que la première disquette d'installation doit être copiée dans le répertoire DISK1 etc.) et de démarrer l'installation à partir de ce support à l'aide de la procédure décrite dans le chapitre 1.2.2.

1.2.6 Installation pour un administrateur réseau

Le programme d'installation d'AVAST32 permet dans une certaine mesure également l'installation pour administrateur réseau basée sur la préparation de l'installation du client dans le répertoire partagé sur le serveur. L'installation du client elle-même pourra se faire de façon totalement automatique sans l'intervention de l'utilisateur. Cette méthode d'installation représente un avantage, en particulier pour les administrateurs d'un grand parc d'ordinateurs.

Pendant l'installation pour administrateur, l'administrateur réseau fait des copies des disquettes d'installation dans les répertoires DISK1...DISKn sur le serveur des fichiers comme nous l'avons décrit pour l'installation à partir d'autres supports. Il modifie ensuite les valeurs dans le fichier ADMIN.INI du répertoire DISK1 créé et copie AVAST32.CNF avec les paramètres par défaut. Il faut comprendre qu'il ne convient pas de rajouter des chemins d'accès absolus aux fichiers (par exemple des fichiers WAV) dans les paramètres.

Si vous désirez En outre amples informations sur l'installation pour administrateur réseau, veuillez consulter le fichier texte **ADMIN.TXT** sur la première disquette d'installation qui contient En outre amples détails sur cette façon de procéder.

1.3 Désinstallation du programme

AVAST32 pourra être désinstallé du système à tout moment. Cette action supprime AVAST32 de façon irréversible de votre disque dur et remet le système dans son état initial (naturellement, à l'exception d'une installation renouvelée). La désinstallation résout également des problèmes tels que la désinstallation de librairies partagées et le renouvellement d'informations internes dans le registre du système d'exploitation.

Les étapes individuelles de la désinstallation sont décrites dans les chapitres suivants.

1.3.1 Préparation de la désinstallation

Avant de lancer la désinstallation d'Avast32, assurez-vous, qu'aucun de ses modules ne soit actif. En effet, dans ce cas, la désinstallation ne pourrait s'effectuer totalement, et les programmes actifs ne pourraient être supprimés du disque dur, ce qui pourrait poser certains problèmes lors de l'installation d'une version supérieure du produit.

Si certains modules sont visibles dans la barre des résidents actifs, cliquez sur leurs icônes avec le bouton droit de la souris, puis sur le bouton quitter pour les interrompre.

1.3.2 Lancement du programme de désinstallation

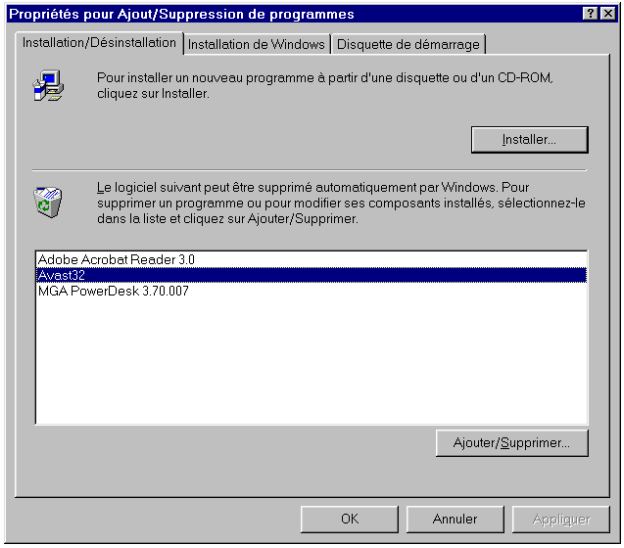

fig. 12

Pour la désinstallation, nous vous recommandons les outils standard du système d'exploitation. Vous les trouverez dans le « Panneau de configuration » dans un répertoire « Ajout/Suppression de Programmes » (nous avons décrit dans le chapitre 1.2.2 comment ouvrir et démarrer cette application).

La fenêtre de cette application présente dans sa partie inférieure la liste des programmes installés (fig. 11) qui permettent une désinstallation automatique (dont AVAST32, bien sûr). Si vous souhaitez désinstaller un programme, dans notre cas le programme AVAST32, faites un double clic avec le bouton gauche de la souris sur le nom du programme concerné. Vous procéderez ainsi à la désinstallation du programme AVAST32.

1.3.3 Avancement de la désinstallation

La procédure de désinstallation est totalement automatique, mise á part la première question si vous êtes sûr de vouloir désinstaller le programme. Si vous répondez "OUI", AVAST32 sera désinstallé et le système sera remis dans son état initial. Si le programme de désinstallation ne peut pas désinstaller toutes les parties du programme AVAST32, ceci sera affiché avant la fin de la procédure. Ceci arrive très fréquemment, AVAST32 créant des fichiers pendant son opération et écrivant sur les variables du système (connues sous le nom de registre).

1.4 Utilisez les programmes d'origine

Pour que la protection de virus soit efficace, il est impératif de respecter quelques principes. A l'exception d'une utilisation régulière du programme anti-virus, il et nécessaire d'utiliser les programmes de sauvegarde et de faire des copies d'au moins les données les plus importantes. Des

données sont souvent perdues sans que ce soit dû à des virus.

Un autre principe important est d'utiliser uniquement des programmes d'origine dont le risque d'infection virale est minime. Un pack de programmes piratés pourrait avoir contracté un certain nombre de virus au cours de son trajet entre le fabricant et votre ordinateur, et les coûts investis pour réparer les dommages causés pourraient dépasser le prix du programme d'origine. En outre, en utilisant un programme piraté, vous êtes en infraction et pourrez encourir des poursuites judiciaires.

Un paradis des virus se cache souvent dans des archives de programmes de démonstration, dont vous ne connaissez jamais l'origine. Si vous décidez d'utiliser de tels programmes malgré ce risque, vous devrez au moins les faire contrôler par un programme anti-virus.

1.4.1 Comment reconnaître des programmes d'origine

Il n'y a actuellement aucune règle générale concernant la façon de distinguer des programmes d'origine d'une copie piratée, c'est pourquoi nous ne pouvons vous donner que quelques conseils. N'achetez des logiciels qu'à des revendeurs fiables et gardez toujours la facture. La garantie d'un logiciel, c'est-à-dire l'accord de licence etc., est censée faire partie du pack.

Si vous avez reçu autre chose, veuillez contacter votre revendeur. Ceci est également valable pour les étiquettes des disquettes d'installation ou les emballages des CD-ROM.

Le programme AVAST32 est livré sur un CD-ROM de couleur argentée sur lequel est imprimé le logo AVAST32. Sur la face données vous trouverez un hologramme portant le titre ALWIL. En option, vous pourrez également acheter le programme AVAST32 sur plusieurs disquettes. Dans ce cas, les étiquettes portent le logo d'ALWIL Software, ainsi que le nom du programme. Si vous avez un doute quelconque sur l'authenticité de votre exemplaire, veuillez contacter directement et immédiatement **ALWIL Trade** Ltd..

1.5 Service AVS

Le développement des virus est actuellement le secteur le plus dynamique de l'informatique. Il est donc de première importance que vous utilisiez la mise à jour la plus récente de votre anti-virus. Ceci implique que les utilisateurs sont souvent obligés de s'occuper eux-mêmes de l'actualisation de leur programme anti-virus.

Afin de faciliter cette tâche pour nos clients, nous offrons depuis longtemps un service appelé AVS vous permettant de recevoir automatiquement pendant un an non seulement les bases de données de virus les plus récentes, mais aussi toutes les mises à jour du programme ainsi que l'assistance technique.

AVAST32 est mis à jour tous les mois par le service AVS, les modules internes une ou deux fois par an. Vous pourrez obtenir des renseignements supplémentaires auprès

d’ALWIL Trade Ltd. Des mises à jour du fichier VPS seront disponibles sur notre site Internet.

2.Commencer

2.1 Lancement du programme

Vous pouvez lancer AVAST32 immédiatement si l'installation a été effectuée correctement. Le programme d'installation a créé un raccourci pour AVAST32 dans le menu de démarrage. En cliquant dessus, vous lancez le programme. Le raccourci se trouve dans le menu de démarrage (après avoir cliqué avec le bouton gauche de votre souris sur « Démarrer ») dans le répertoire « Programmes ». La présentation du menu de démarrage dépend de la configuration par défaut de l'environnement de votre système d'exploitation ainsi que des programmes déjà installés. L'une des présentations possibles est affichée à la fig. 13.

Si vous travaillez sous Windows NT 3.51, le programme d'installation aura créé pour vous le groupe AVAST32 antivirus avec un raccourci vers AVAST32. Le lancement du programme à travers ce raccourci s'effectue de la même façon que toute autre procédure de lancement.

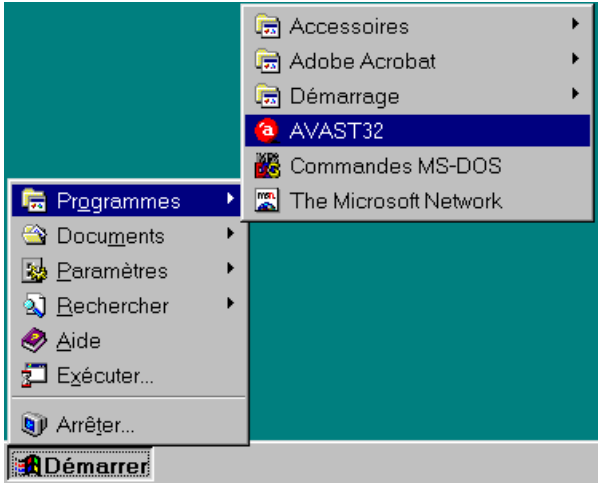

fig. 13

Nous vous recommandons de créer un raccourci AVAST32 sur votre bureau. Ainsi, vous n'aurez pas à passer constamment par la procédure complexe du menu « Démarrer » pour lancer AVAST32. Si vous désirez créer ce raccourci, ouvrez l'Explorateur, en cliquant par exemple avec le bouton gauche de la souris sur « Démarrer » et en activant « Explorer » dans le menu qui s'affiche (fig. 14).

fig. 14

Choisissez le répertoire dans lequel vous avez installé AVAST32 (fig. 15). Si vous n'avez pas modifié la configuration par défaut pendant la procédure d'installation, ce répertoire sera

« Programmes\ALWIL Software\AVAST32 » sur votre disque système. Cliquez avec le bouton gauche de votre souris sur le fichier AVAST32.exe et maintenez la touche enfoncée. Maintenant, faites glisser le curseur de la souris par dessus le bord, c'est-à-dire dans le secteur n'appartenant à aucune fenêtre, et relâchez le bouton.

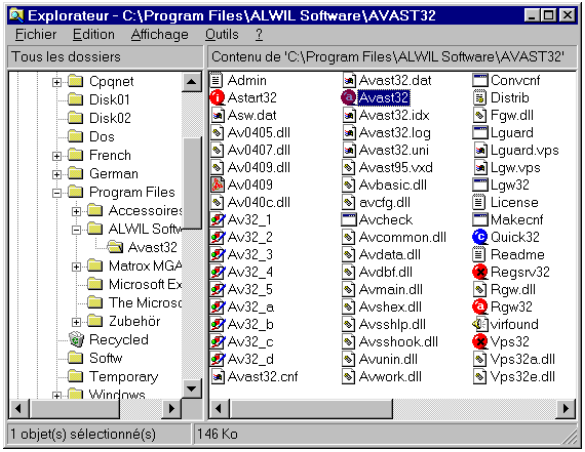

fig. 15

Le raccourci sera créé à l'endroit où vous avez relâché le bouton de la souris (fig. 16). Si vous double-cliquez avec le bouton gauche de la souris sur ce raccourci, le programme AVAST32 sera lancé.

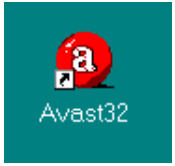

fig. 16

Le programme AVAST32 peut être lancé En outreieurs façons identiques. Il n'est pas important que vous ayez sélectionné l'icône AVAST32 dans le menu « Démarrer », double-cliqué sur le raccourci créé récemment sur votre bureau ou sur l'icône AVAST32 dans l'Explorer. Il y a d'autres façons de lancer le programme, mais elles ne vous concernent pas maintenant.

2.2 Démarrer le programme

Après le lancement d'AVAST32, vous verrez que la fenêtre principale (fig. 17) présente une liste d'éléments. Ces éléments représentent les tâches accessibles à ce moment. Après l'installation du programme AVAST32, nous vous recommandons de rechercher des virus sur le disque dur de votre ordinateur. Afin de s'apercevoir des modifications apportées à certains fichiers et de découvrir ainsi la présence d'un nouveau virus inconnu jusqu'alors, il faut créer une base de données des fichiers. Ces deux opérations seront effectuées par la tâche « Scan: tous les disques locaux ».

fig. 17

Cette tâche sera lancée en double-cliquant dessus avec le bouton gauche de la souris. Si la tâche est réellement lancée, vous constaterez que l'icône à côté du nom de la tâche a changé par rapport à l'icône représentée sous fig. 18. Si l'icône reste inchangée, vous n'avez probablement pas cliqué assez vite sur le bouton gauche de la souris.

fig. 18

La tâche « Scan+Check: tous les disques locaux » examine tous les répertories sur vos disques durs et vérifie tous les fichiers pour trouver la présence d'un virus. En même temps, le programme gardera en mémoire tous les fichiers rencontrés et garde l'état des fichiers sur le disque dur. La tâche ne manque pas non plus de contrôler la mémoire vive de votre ordinateur.

Si le programme trouve un virus dans un fichier ou dans la mémoire, il affichera le message d'alerte (fig. 19). Ce qu'il faut faire dans ce cas-là est décrit en annexe B. Dans tous les cas, ne paniquez pas, et si vous n'êtes pas sûr de vos compétences en matière informatique, il vaut mieux laisser la tâche d'enlever le virus à quelqu'un En outre expérimenté. Si aucun virus n'a été trouvé, aucun message ne sera affiché pendant l'opération.

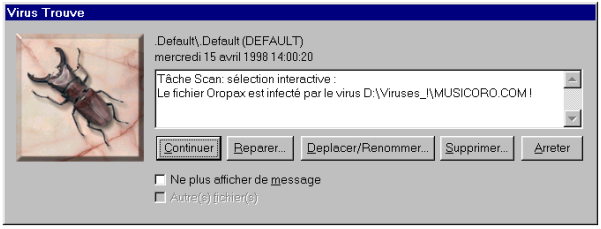

fig. 19

La durée de l'opération dépend du nombre et du type des fichiers sur vos disques durs et, bien sûr, de la capacité de votre ordinateur. Cela peut aller d'environ 12 secondes à quelques minutes. C'est une opération utile car, à la fin, vous saurez si votre ordinateur est infecté par un virus, et dans ce cas, vous aurez à votre disposition une base de données de fichiers qui vous aidera à restaurer les fichiers si un virus se trouve dans votre système.

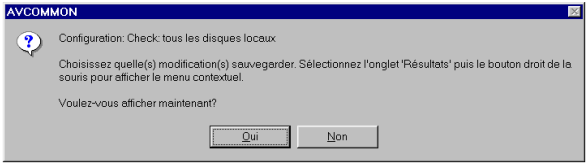

fig. 20

Une fois la tâche terminée, la boîte de dialogue de la Figure 20 s'affichera et l'icône aura l'apparence précédente (voir icônes à côté du nom de la tâche en Figure 17). Appuyez sur Oui dans la boîte de dialogue, et l'arborescence des fichiers de votre disque dur s'affichera. Maintenant, il faut créer la base de données des fichiers. Cliquez sur Bureau. Un menu raccourci s'affichera. Activer la commande « Accepter » dans le répertoire « Fichiers en cours » (Figure 21). Vous avez ainsi indiqué au programme qu'il doit enregistrer les informations sur tous les fichiers sur le disque dur dans la base des fichiers.

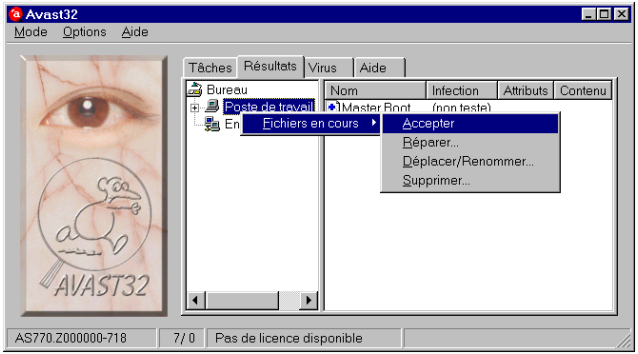

fig. 21

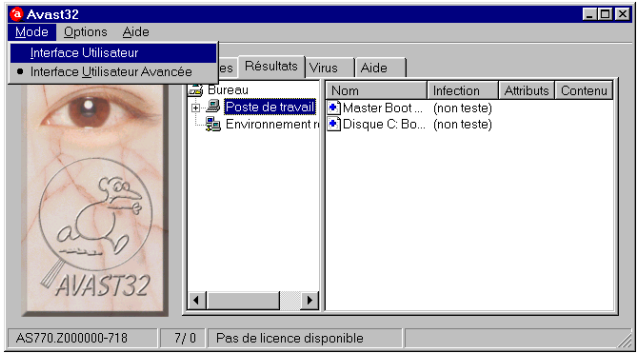

fig. 22

Si la fenêtre suivante est trop compliquée (cela veut dire que vous vous trouvez en mode étendu de l'interface, voir chapitres 3.3 et 5), vous pourrez passer en mode normal. Pour ce faire, sélectionnez « Interface Utilisateur » du menu « Mode » (figure 22). Vous repasserez ainsi en mode normal représenté dans la figure 17.

2.3 Y a-t-il des virus?

Si vous voulez uniquement savoir s'il y a des virus dans votre ordinateur, faites un double-clic avec le bouton gauche de la souris sur « Scan: tous les disques locaux ». Vous lancez la tâche qui teste tous les fichiers sur vos disques durs et dans la mémoire vive de votre ordinateur. Si la vérification est réellement en train de s'effectuer, cela se voit sur l'icône à côté du nom de la tâche qui se présentera tel que dans fig. 18.

Si AVAST32 trouve un virus dans un fichier, l'utilisateur en sera à chaque fois averti (fig. 19, une description plus détaillée est prévue dans le chapitre 5.4). Si aucun virus n'est détecté, la tâche se termine normalement et l'icône à côté du nom de la tâche ressemblera aux icônes des noms de tâches à la fig. 17.

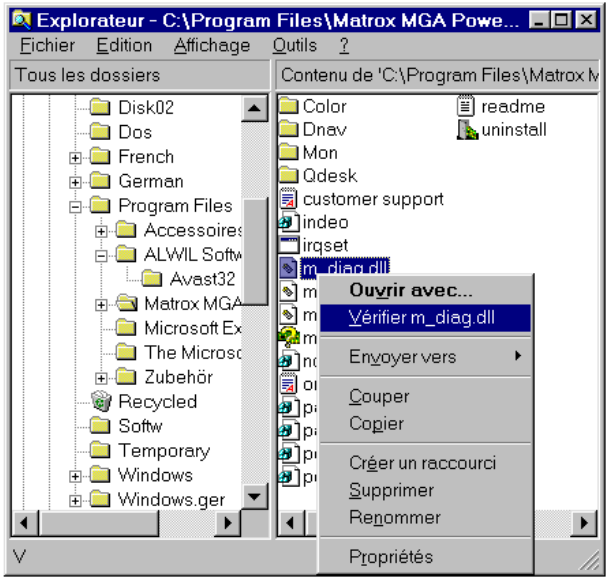

fig. 23

Si vous voulez savoir si un fichier est infecté, il n'est pas nécessaire de lancer tout le programme AVAST32. Il suffira de chercher le répertoire contenant le fichier concerné dans le programme « Explorer » (son lancement est décrit dans le chapitre 2.1), de faire un clic droit sur le fichier et de sélectionner « Vérifier <nom du programme>... » (fig. 23) dans le menu apparent. Le fichier choisi sera vérifié. S'il contient un virus, vous recevrez un message d'alerte représenté dans fig. 24 (Le message est décrit dans le chapitre 10).

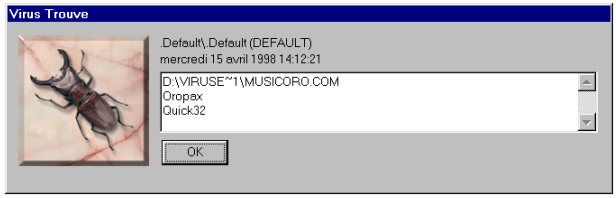

fig. 24

Il est possible de vérifier de la même manière tous les répertoires sans avoir à lancer l'ensemble du programme AVAST32. Sélectionnez avec le bouton droit de la souris le répertoire concerné et choisissez la commande « Vérifier <nom du répertoire> » dans le menu. Si le répertoire contrôlé contient des sous-répertoires, ils seront également testés.

2.4 Comment se protéger contre des virus macro?

Les « virus macro » constituent un problème sérieux que nous rencontrons depuis un moment. Ces virus se propagent sous la forme de macros dans des documents comme par exemple MS Word, MS Excel, etc. Avant même d'ouvrir le document qui était uniquement ouvert dans un ordinateur inconnu, il faut le vérifier afin de vérifier s'il contient des virus macro.

Si vous recevez un fichier document sur disquette, il convient de lancer la tâche « Scan: disquette A: » qui teste tous les documents et fichiers sur la disquette pour déceler la présence d'un virus.

Si un virus est trouvé dans un document ou un fichier, le programme affichera un message d'alerte (fig. 19). Ce qu'il faut faire dans ce cas-là est décrit dans l'annexe B.

Si vous souhaitez vérifier la présence d'un virus uniquement dans un document précis, servez-vous de la procédure décrite auparavant dans le chapitre 2.3.

Si vous devez télécharger des documents, par exemple, d'un site sur Internet, et vous n'êtes pas sûr que ces documents soient « propres » (vous ne pourrez jamais en être certain), il est nécessaire de tester également ces documents. Faite un double-clic avec le bouton gauche de la souris sur la tâche « Scan: sélection interactive ». Après le lancement de la tâche qui se manifeste par une modification de l'icône à côté du nom de tâche, vous aurez à spécifier dans une boîte de dialogue les fichiers à tester (voir chapitre 5.5). La boîte de dialogue ainsi que ses commandes sont similaires au dialogue système pour l'ouverture des fichiers.

2.5 Comment détecter un virus même inconnu?

Etant donné que la plus grande majorité des virus modifient d'une façon ou d'une autre les données sur le disque dur, il convient de vérifier de temps en temps les modifications intervenues sur vos disques. Donc, si vous voulez donc savoir si un fichier sur votre disque dur a été modifié (contrôle d'intégrité), lancez la tâche « Check: tous les disques locaux » (double-clic avec le bouton gauche de la souris sur le nom de la tâche). Après lancement, la tâche explorera tous les disques durs et gardera en mémoire tous les fichiers qu'elle rencontre avec l'état du fichier sur le disque dur.

Si un fichier a été changé, le programme affichera un message à la fin vous demandant si vous désirez afficher les résultats de la tâche (voir fig. 18). En activant le bouton « Oui », vous verrez la structure de votre ordinateur avec tous les fichiers qui ont été modifiés depuis la dernière vérification. Une description plus détaillée se trouvera dans le chapitre 5.3.2; l'interprétation des résultats sera traitée dans le chapitre 7.

Afin de déterminer quel fichier a été modifié, le programme doit créer une base de fichiers. Comment créer une base de fichier sera décrit dans le chapitre 2.2.

Des contrôles d'intégrité réguliers de vos données sur vos disques durs sont très importants, plus même que le scan pour des virus. Ils vous protégeront d'un certain nombre de problèmes et c'est pourquoi nous vous recommandons de les respecter.

2.6 Comment se protéger contre des virus système?

Afin de protéger votre ordinateur autant que possible, il convient de lancer le module « Résident: protection active » (double-clic avec le bouton gauche de la souris sur le nom

de la tâche) avant même de commencer le travail. La tâche surveillera presque toutes les activités à l'intérieur de votre ordinateur. En cas d'une tentative d'opération suspecte, ou si le programme détecte un virus dans le programme en cours ou dans la zone système de la disquette insérée, il affichera un message d'alerte (qui peut ressembler aux messages représentés à la fig. 25 et 26). La tâche empêchera le virus de s'introduire dans le système, s'il est en route (l'icône à la fig. 18 se trouve à côté de son nom). A la fin de l'opération, par contre, le système ne sera plus protégé.

fig. 25

La tâche: « Résident: protection active » après l'installation d'AVAST32 est automatiquement lancée à chaque démarrage système et vous n'avez pas à la lancer manuellement. Le chapitre 2.8 vous explique comment désactiver cette option (mais nous conseillons à la plupart des utilisateurs de garder cette fonction activée!!!).

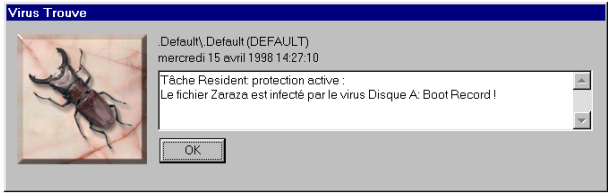

fig. 26

2.7 Avant de travailler avec une disquette inconnue

Pour que la protection de votre ordinateur soit efficace, il faut acquérir un certain nombre d'habitudes en travaillant avec votre ordinateur (à moins de lancer régulièrement un scanner, effectuer des mises à jour régulières de la base des fichiers et des sauvegardes régulières des données importantes). L'une de ces habitudes consiste à vérifier toute disquette que vous désirez copier dans votre ordinateur s'il y a un virus éventuel (ceci s'applique à toute disquette provenant d'un autre ordinateur).

L'opération décrite ci-dessus est effectuée par la tâche « Scan: disquette A: » qui sera lancée comme toute autre tâche en faisant un double-clic avec le bouton gauche de la souris sur le nom de la tâche. La commande « Scan: disquette A: » testera d'abord s'il y a un virus dans la zone système (secteur de démarrage) et ensuite dans tous les répertoires et fichiers documents. S'il y a un virus (virus macro ou virus programme), AVAST32 affichera un

message d'alerte (fig. 19); si non, l'opération se terminera normalement.

Un autre principe important est de ne jamais laisser une disquette dans le lecteur plus que nécessaire. Ainsi, vous éviterez de démarrer accidentellement le système avec une disquette infectée qui contaminera votre ordinateur. La plupart des ordinateurs prévoient aujourd'hui dans le SETUP une commande empêchant le système de démarrer avec une disquette. Si vous ne savez rien de votre SETUP, contactez l'administrateur système.

2.8 Comment travailler avec AVAST32

Ce chapitre contient des suggestions quant à l'utilisation d'Avast32 et de ses différents modules.

Créer un raccourci sur le bureau

Si vous exécutez périodiquement la même tâche, il est possible de créer un raccourci sur le bureau. En faisant un double-clic avec le bouton gauche de la souris sur le raccourci, AVAST32 sera lancé automatiquement avec la tâche appropriée. Cela veut dire qu'il ne sera pas nécessaire de lancer d'abord AVAST32 et ensuite la tâche en question. Vous pouvez créer ce raccourci en cliquant avec le bouton droit de la souris sur le nom de la tâche désirée et en sélectionnant « Créer un raccourci » dans le menu apparent (fig. 27).

fig. 27

Le raccourci portant le même nom que la tâche sera créé sur le bureau. On trouvera à la fig. 28 le raccourci vers la tâche « Scan+Check: tous les disques locaux ».

fig. 28

Grâce à la nouvelle structure d'AVAST32, vous n'aurez pas à attendre le lancement d'une nouvelle tâche pendant que la tâche exécutée se termine. Le programme est capable d'exécuter un certain nombre de tâches à la fois. La vitesse d'exécution de ces tâches dépend cependant de l'équipement de votre ordinateur.

Utilisation du module « ScreenSaver"

Bien que le scan soit gourmand en ressources, il est nécessaire de l'effectuer régulicrement. Avast32 fournit un module ScreenSaver qui permet de vérifier une machine lorsque l'écran de veille de Windows s'active. L'utilisateur est informé de la progression et du résultat de la vérification. La description détaillée du module « ScreenSaver » se trouve au chapitre 12.

Si vous désirez activer ce module, ouvrez le « Panneau de Configuration » via le menu « Démarrer », puis cliquez sur l'icône « Affichage » et enfin sur l'onglet « Ecran de veille » (Fig. 29).

Sous Windows 95, sélectionnez l'écran de veille « AvastSS » (Fig. 29). Sous Windows NT, sélectionnez « Anti-virus Avast32 ».

Définissez, dans la zone « Attente », le temps en minute à partir duquel l'écran de veille doit s'activer en cas d'inactivité clavier/souris.

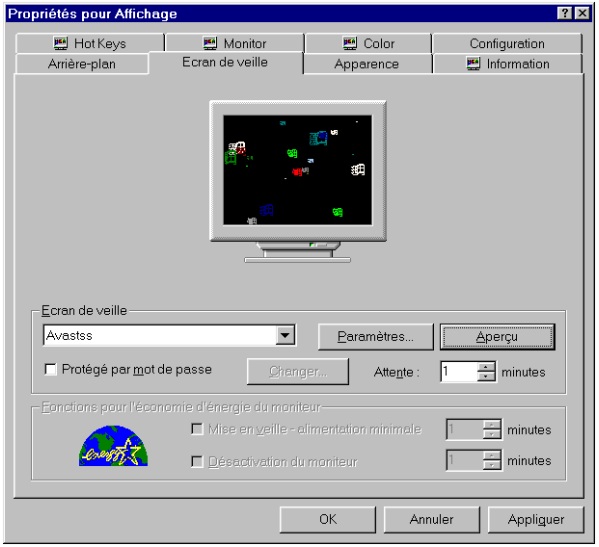

fig. 29

Le bouton « Paramètres » vous permet de définir l'écran de veille à utiliser ainsi que les paramètres de la tâche Avast32 (voir Chapitre 12.1). Si vous désirez avoir un aperçu du résultat, cliquez sur « Aperçu ».

Cliquez sur « OK » pour terminer. Lors de la prochaine mise en veille, Avast32 vérifiera, durant tout le temps de l'inactivité, les zones et fichiers que vous aurez spécifiés.

Lancer la tâche avec le système d'exploitation

Tout d'abord, assurez-vous que la tâche en question n'est ni en cours, ni interrompue. Si elle est interrompue (repérée par un indicateur rouge), réactivez-la – cliquez dessus avec le bouton droit et choisissez « Continuer » dans le menu. Si elle est active (repérée par un indicateur vert – Fig. 18), arrêtez-la – cliquez dessus avec le bouton droit et choisissez « Stop » dans le menu.

Si le programme affiche le message de la Fig. 20 alors que les étapes ci-dessus ont été accomplies, cliquez sur « Non ».

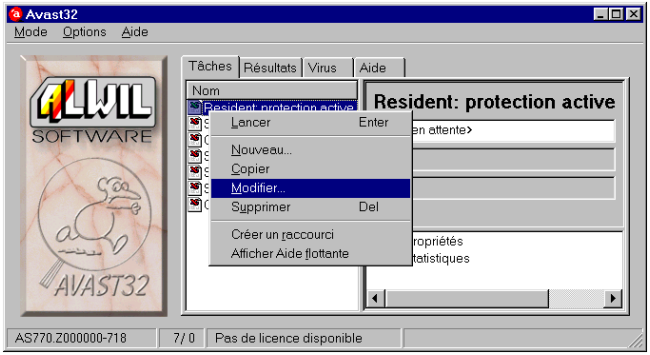

fig. 30

Vous pourrez faire en sorte que des tâches soient lancées immédiatement après la connexion avec le système d'exploitation (comme tâche: « Résident: protection » active dans chapitre 2.6). Choisissez l'interface en mode étendu dans le menu Affichage. Passer à l'onglet Tâches en cliquant sur le nom de la tâche.

Faites un clic droit sur le nom de la tâche que vous souhaitez lancer automatiquement avec le système d'exploitation et choisissez dans le menu raccourci « Modifier... » (Fig. 30). Un écran d'assistant s'affichera. En cliquant plusieurs fois sur le bouton « Suivant >> », vous ouvrirez la fenêtre « Sélectionnez ici les options communes à toutes les configurations » (Fig. 45). Activez la case « Lancer cette configuration au démarrage de Windows » et appuyez sur « OK » (voir chapitre 4.4.6 pour plus de détails). A la prochaine connexion, cette tâche sera lancée automatiquement.

Si vous souhaitez désactiver ce démarrage automatique, suivez les mêmes consignes mais désactivez la case.

Par contre, l'interface utilisateur est en mode étendu. Si vous voulez passer en mode normal, choisissez « Interface Utilisateur » dans le menu « Mode » (Figure 22).

3.Description générale du programme

AVAST32 offre une protection anti-virus totale pour les ordinateurs sous Windows 95 ou Windows NT. Le programme vous permet d'exécuter des contrôles qui englobent pratiquement tous les aspects de protection antivirale.

En plus du programme déjà classique recherchant des virus connus, AVAST32 contient également les outils vous permettant de détecter des virus macro ainsi que des virus polymorphes. Il peut même déceler la présence de virus jusqu'à présent inconnus.

Grâce aux contrôles résidents, il est possible de vérifier si le système a effectué des opérations éventuellement dues à l'activité d'un virus. AVAST32 permet également de surveiller toute opération active du système. En cas d'opération suspecte, il la bloquera et en avertira l'utilisateur. Il peut même scanner les fichiers exécutés et ainsi empêcher le système de s'infecter avec un virus.

L'interface utilisateur du programme AVAST32 est totalement compatible avec l'environnement des systèmes d'exploitation Windows 95 et NT et correspond tout à fait aux standards habituels. C'est pourquoi l'utilisateur qui travaille dans cet environnement n'aura pas de problèmes pour se familiariser avec ce programme.

Afin de permettre à l'utilisateur d'exécuter ce programme en tout confort, il contient une palette de tâches différentes et deux interfaces utilisateur. La description des interfaces est traitée dans les chapitres 3.3, 3.4, 3.5 et 5.

3.1 Propriétés et avantages d'AVAST32

AVAST32 est un anti-virus conçu pour les systèmes d'exploitation Microsoft Windows 95 et Microsoft Windows NT. Il y a très peu de différences sous ces deux systèmes qui sont dues uniquement à leurs structures différentes et l'utilisateur travaillant avec AVAST32 sous l'un des systèmes n'aura pas de problème quand il aura à l'utiliser sous l'autre.

Le principal avantage d'AVAST32 est le scanning rapide et, notamment, soigné de votre système et de tous ses modules. Les algorithmes utilisés sont si efficaces qu'un virus est reconnu dans presque 100 % des cas, comme l'ont confirmé des tests récents! Non seulement vous pouvez détecter la présence d'un virus, mais aussi les modifications qui auraient été apportées à votre ordinateur depuis le dernier test. C'est ainsi que vous pourrez détecter même un virus qui est toujours inconnu! Ce test s'appelle le contrôle d'intégrité.

Le module « Screen Saver » d'Avast32 permet la vérification d'une machine durant ses périodes d'inactivité. Il

peut être configuré aux besoins de chaque utilisateur sur le même principe que les tâches Avast32. Vous trouverez la description détaillée de ce module au chapitre 12.

Si un fichier est infecté ou endommagé, et si vous avez sauvegardé la base de ces fichiers, vous pourrez essayer de restaurer ce fichier avec AVAST32. Le taux de succès de la restauration d'un fichier est de 95 %, et AVAST32 est capable d'arriver à presque 100 % de restauration exacte du fichier!

AVAST32 peut aussi se servir des outils de communication d'un réseau. Si un virus a été détecté, tous les utilisateurs réseau en seront avertis à temps. Cette propriété vous permet de réduire de manière très efficace le risque d'une perte de données et d'empêcher ainsi la propagation d'une infection virale.

AVAST32 profite de tous les avantages d'un système d'exploitation moderne, comme par exemple les noms de fichiers longs (jusqu'à 256 caractères), de nouveaux contrôles ou de la possibilité d'exécuter plusieurs applications en même temps. L'utilisateur n'est plus bloqué et peut pleinement profiter du temps passé avec son ordinateur et de ses capacités.

L'interface peut être totalement adaptée aux besoins et capacités de son utilisateur. Des débutants apprécieront certainement la possibilité d'exécuter le programme sans avoir à apprendre des détails sur son fonctionnement alors que des utilisateurs plus expérimentés profiteront des possibilités des configurations détaillées des opérations du programme et de ses réactions face à certains problèmes.

Pour afficher l'aide, AVAST32 utilise le programme Acrobat Reader très performant et facile à utiliser. Cependant, Acrobat Reader paraît partie intégrante du programme AVAST32. Il vous permettra de traverser l'aide facilement et d'accéder rapidement à la partie qui vous intéresse plus spécifiquement.

3.2 Fonctions de base du programme

Un module classique de la plupart des anti-virus est la recherche de virus connus (appelé scanner). Ce programme doit contrôler si le fichier contient une présence d'une certaine séquence d'octets qui sera ensuite identifiée comme un virus particulier.

Ainsi, AVAST32 peut détecter un grand nombre de virus, mais de nouveaux virus arrivant rapidement et régulièrement, il est impératif de mettre à jour périodiquement la base des virus connus (voir chapitre 1.5). AVAST32 peut également reconnaître des virus appelés "virus polymorphes" qui sont capables de changer leur structure pendant l'activité et qui sont donc difficiles à reconnaître. Notre produit est également en mesure de reconnaître des virus macro qui se propagent sous forme de macros dans les documents OLE (c'est-à-dire sous MS Word ou Excel).

Une méthode moins connue de détecter des virus est le contrôle d'intégrité. Il est basé sur l'idée que le virus doit être stocké dans une mémoire résidente quand l'ordinateur est éteint. Actuellement, le disque dur de l'ordinateur est la mémoire la plus utilisée. Ceci implique que nous pourrons découvrir même un virus encore inconnu avec la même

réussite que les virus très connus, à condition de surveiller les modifications des fichiers.

Si, par exemple, un fichier texte (avec l'extension .TXT) a été modifié, on peut dire à 99% que ce n'est pas un virus. Par contre, si un programme ou même un fichier système a été changé, il y a une forte probabilité d'infection virale.

Afin de permettre l'exploration de certains fichiers, il faut garder des renseignements sur leur statut pendant un certain moment. En comparant le statut actuel avec ceux sauvegardés dans la base de données, il est possible de décider de façon fiable si le ficher a été modifié ou non.

Si vous faites dorénavant un contrôle d'intégrité, par exemple, toutes les semaines, vous serez averti de tout changement intervenu dans vos fichiers dans la semaine avant le test.

Les renseignements sauvegardés dans la base pourront être utilisés par AVAST32, mis à part le contrôle d'intégrité, pour restaurer le statut original des fichiers. Si vous mettez cette base régulièrement à jour, vous pourrez essayer de restaurer vos fichiers en cas d'attaque virale. A l'aide de la base des fichiers, il est possible de déterminer avec une totale précision si un fichier a été restauré avec succès ou non.

AVAST32 offre également la possibilité de détecter toute opération suspecte effectuée sur des fichiers et des zones système des disques durs et d'en informer l'utilisateur avant. L'utilisateur aura deux options: ou il autorise l'opération, ou il l'annule. Cette protection résidente s'appelle « Behaviour Blocker » et se base sur le fait que la très grande majorité des virus effectuent certaines opérations sur des fichiers pendant leur phase d'activité, indépendamment du fait qu'ils les infectent ou les endommagent ou non.

Il peut même arriver qu'un virus soit présent dans l'ordinateur, mais celui-ci n'est pas infecté.

Pou qu'un virus devienne actif, il faut l'exécuter. Ceci présuppose que la plupart des virus attaquent les exécutables, c'est-à-dire les programmes. AVAST32 vous offre un module résident appelé « Résident Scanner » qui effectue un test de tous vos programmes. Si vous souhaitez lancer un programme, AVAST32 va d'abord le contrôler pour vérifier s'il contient un virus ou non. Si tout va bien, le programme sera exécuté normalement. Si, par contre, un virus a été trouvé dans le programme, vous aurez un message d'alerte et le programme ne sera pas lancé sans votre autorisation.

Un autre groupe relativement fréquent de virus est celui des virus se propageant dans les zones systèmes de disques, c'est-à-dire en général dans le secteur de démarrage de disquettes. Un ordinateur ne peut pas être infecté par simple insertion d'une disquette contaminée dans le lecteur, mais il peut arriver qu'un système soit démarré par accident avec une disquette oubliée dans le lecteur et l'ordinateur peut s'infecter de cette manière. AVAST32 contient un module résident appelé « Protecteur des zones systeme » qui, au premier accès de la disquette, vérifie d'abord si son secteur de démarrage contient aucun virus. Si un virus est détecté, le programme informe l'utilisateur par le biais d'un

message d'alerte. Si aucun virus n'a été trouvé, il est possible de travailler normalement avec la disquette.

3.3 Interface utilisateur en mode normal et en mode étendu

Le programme AVAST32 peut être exécuté en deux modes diffèrant essentiellement par la quantité et la complexité de leurs commandes. Ceci s'adresse à deux groupes d'utilisateurs pour lesquels les deux modes d'interface ont été conçus.

La première forme d'interface utilisateur AVAST32 est représenté à la fig. 31. Ce mode d'interface est appelé mode normal parce qu'il ne contient que les contrôles les plus importants du programme et protège ainsi les utilisateurs d'un grand nombre de contrôles avec lesquels ils ne travaillent pas d'habitude.

Il est possible d'effectuer seulement les travaux et tâches les plus élémentaires dans l'interface utilisateur normal.

fig. 31

L'interface utilisateur AVAST32 peut également prendre la forme affichée à la fig. 32. Appelé mode étendu, il englobe toutes les commandes du programme. Ainsi, l'utilisateur peut accéder à toutes les fonctions et paramètres offerts par le programme AVAST32.

En ce qui concerne le contenu, le mode étendu est divisé en plusieurs onglets regroupant leurs propres fonctions et paramètres. Il est possible de passer d'un onglet à l'autre en cliquant avec le bouton gauche de la souris sur le nom de l'onglet concerné.

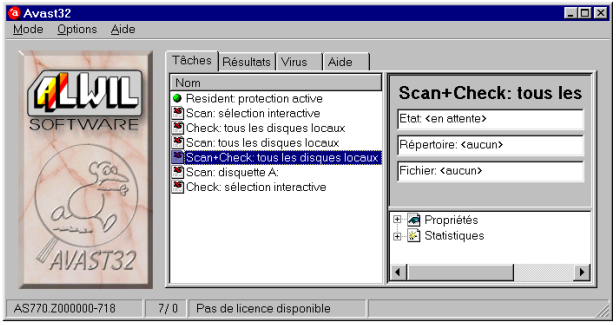

fig. 32

L'interface utilisée dépend de la configuration du moment, le mode normal de l'interface étant paramétré par défaut. Une description détaillée des deux modes du programme AVAST32 et comment passer de l'un à l'autre sont prévus dans le chapitre 5.

3.4 Quel mode d'interface ?

La division de l'interface utilisateur en deux modes s'inspire du fait que les utilisateurs peuvent être classés en deux groupes selon les opérations qu'ils effectuent avec l'ordinateur. D'un côté, il y a les experts (comme par exemple les administrateurs réseau responsables de la configuration et du fonctionnement corrects d'un réseau d'ordinateurs) et de l'autre côté, il y a les utilisateurs normaux.

Un utilisateur normal typique n'a en général pas besoin d'un grand nombre de paramètres - son besoin principal est souvent l'interface le plus simple possible sans avoir à apprendre comment configurer et contrôler un autre programme. Pour ce type d'utilisateur, nous vous recommandons le mode normal de l'interface, sa conception étant totalement adaptée à ces besoins.

Par contre, des administrateurs réseau et des utilisateurs plus expérimentés devront configurer exactement le fonctionnement et le comportement du programme. L'interface en mode étendu du programme AVAST32 a été conçue pour eux, rendant toute fonction et toute commande accessibles et permettant ainsi d'adapter le programme à leurs propres besoins.

Chaque utilisateur peut choisir l'interface qui lui convient le mieux et travailler avec lui. L'interface utilisée sera gardée en mémoire par le programme pour chaque utilisateur séparément.

3.5 Possibilités d' interfaces spécifiques

Tout ce qui peut être fait sous les interfaces spécifiques dépend de leurs champs d'activité. L'interface en mode normal a été conçue pour un utilisateur normal qui doit effectuer une tâche (c'est-à-dire tester une partie de son système) sans s'occuper des détails de l'opération ni des paramètres du programme. Ceci est respecté, et le mode normal permet d'effectuer facilement des opérations de base avec ces tâches.

L'interface en mode normal permet de démarrer une tâche ou, alternativement, de l'interrompre ou de l'arrêter.

Si une tâche détecte un virus, l'utilisateur en est averti. Par contre, l'interface en mode normal ne peut pas afficher des détails des résultats des tâches effectuées. Elle ne met pas non plus l'utilisateur en mesure de savoir quel fichier a été infecté ou modifié.

En outre, l'interface en mode normal offre les fonctions de base telles que fermer le programme, ouvrir l'aide du programme ou créer un raccourci bureau. L'interface en mode normal vous permet également de passer en mode étendu.

L'interface en mode étendu permet d'accéder à toutes les fonctions d'AVAST32. Outre les opérations de base avec les tâches déjà mentionnées pour l'interface en mode normal , l'utilisateur peut changer les paramètres de tâches générales ou même de les supprimer. Bien évidemment, vous pourrez créer de nouvelles tâches.

Les utilisateurs pourront consulter les résultats complets de toutes les tâches effectuées jusqu'à présent et avoir également accès aux outils qui lui permettront d'agir en fonction de ces résultats ou d'essayer de corriger les fichiers modifiés. Il est également possible de supprimer les fichiers suspects ou infectés ou de simplement les renommer et déplacer dans d'autres répertoires appropriés.

L'interface en mode étendu permet aussi le paramétrage de l'environnement des parties générales du programme aussi bien que du programme dans son ensemble. Sont à disposition de l'utilisateur des commandes permettant d'adapter les propriétés du programme à ses propres besoins. La configuration de l'environnement programme prévoit également la commande de passer en mode normal.

Quelques caractéristiques de virus font aussi partie du fichier VPS ainsi que des informations sur sa date de publication ainsi que celle de la version du programme et sur le détenteur de la licence. Cette information est importante, en particulier au moment de devoir faire appel au service technique.

3.6 Les tâches de base

L'élément de base du fonctionnement du programme AVAST32 est la "tâche". Son nom est une description détaillée de tous les tests à effectuer à partir du lancement de cette tâche. En cas de contrôle individuel, il est possible de configurer après une séquence de paramètres définissant le comportement de la tâche avec une plus grande précision.

Chaque tâche doit avoir son nom et être composée de quelques tests. Le test peut être par exemple le scan de fichiers sur le disque dur afin de déceler une présence virale, ou la surveillance du système effectuée de temps en temps. Une tâche peut même effectuer plusieurs tests à la fois; c'est-à-dire rechercher des virus et faire un contrôle d'intégrité.

Les tâches peuvent être "Privée", "Partagée" ou en lecture seule. Les tâches "partagées" sont accessibles à l'ensemble des utilisateurs d'une même machine, au contraire des tâches "privées" qui ne le sont qu'à leur auteur. L'op-

tion lecture seule permet de protéger les tâches « partagées » de toutes modifications par un utilisateur.

Toutes les tâches accessibles se trouvent dans la liste des tâches sous l'interface en mode normal ou en mode étendu.

La façon de créer une tâche est décrite dans le chapitre 4.

3.7 Tâches prédéfinies

Plusieurs tâches déjà créées permettant à l'utilisateur d'exécuter le programme immédiatement après son installation font partie de l'installation du programme AVAST32. Des tâches spécifiques sont décrites dans les paragraphes suivants.

Toutes les tâches fournies par défaut avec AVAST32, sont en lecture seule par défaut.

« Scan: tous les disques locaux »

La tâche testera tous les exécutables et documents OLE sur tous les disques locaux de l'ordinateur en question. En cas de découverte d'un virus par AVAST32, il affichera un message d'alerte et une alarme (si l'ordinateur est équipé d'une carte son). La tâche affiche tous les virus trouvés. Les fichiers compressés et la mémoire vive seront également testés ainsi que la zone système de tous les disques.

« Scan: sélection interactive »

La tâche effectuera exactement le même test que ci-dessus, mais l'utilisateur pourra choisir avant les zones à tester. Bien sûr, vous pourrez sélectionner plusieurs zones en même temps (voir chapitre 5.5). Au moment de choisir les répertoires, il est possible de préciser si vous souhaitez tester aussi les sous-répertoires.

« Scan: disquette A: »

Cette tâche effectue le même test que les deux précédentes, mais sur la disquette dans le lecteur A:. Nous vous recommandons d'effectuer ce test pour toute disquette éventuellement infectée. Ceci concerne en particulier les disquettes utilisées dans d'autres ordinateurs ou par d'autres utilisateurs. La zone système, c'est-à-dire le secteur de démarrage, sera également testé sur la disquette.

Si vous vous habituez à tester toutes les disquettes qui ne vous appartiennent pas, vous réduirez sensiblement le risque d'infecter votre ordinateur.

« Check: tous les disques locaux »

La tâche vérifiera si des fichiers exécutables et documents OLE sur tous les disques locaux ont été modifiés depuis le dernier contrôle. Le contenu des fichiers ne sera contrôlé que si un paramètre a été modifié depuis le dernier contrôle, comme par exemple des attributs, la taille du fichier etc. Les résultats seront sauvegardés dans une arborescence bien classée (voir chapitre 5.3.2). La tâche vérifiera également si une modification de la zone système est intervenue depuis le dernier test.

Conformément au texte précité, les modifications ne peuvent être contrôlées qu'entre deux contrôles d'intégrité. Le résultat de la première exécution de la tâche sera le

message que tous les fichiers du contrôle du disque ont été rajoutés. C'est pourquoi il est nécessaire de sauvegarder le statut de ces fichiers dans une base de données interne afin de pouvoir comparer, lors d'un contrôle d'intégrité suivant, le statut actuel de ces fichiers avec le précédent. La façon de créer la base de données est décrit dans le chapitre 2.2.

« Check: sélection interactive »

Cette tâche effectuera le même test que la précédente, mais demandera à l'utilisateur de préciser les zones à tester. Les zones à tester sont sélectionnées à l'aide du dialogue décrit dans le chapitre 5.5. Pour cette tâche, il convient également de sauvegarder d'abord les fichiers dans la base pour pouvoir exploiter les résultats.

« Resident: protection active »

La protection assurée par cette tâche est basée sur deux éléments. Si un virus est en train d'infecter l'ordinateur, il doit d'abord être exécuté (c'est-à-dire il doit prendre le contrôle), c'est pourquoi il est préférable de scanner tous les exécutables et les secteurs de démarrage des disquettes insérées. L'autre élément est que le virus exécute une activité dans l'ordinateur: il écrit dans un fichier à exécuter, sur le secteur de démarrage de disquettes, ou même essaie de reformater certaines parties du disque dur.

Toutes les opérations précitées sont contrôlées par cette tâche et dans le cas d'une tentative d'opération dangereuse, elle demande d'abord à l'utilisateur si cette opération peut être exécutée. Sans son autorisation, il ne sera pas possible de le faire.

Nous vous recommandons de toujours lancer cette tâche après le démarrage du système d'exploitation ou, de préférence, de configurer son lancement automatique avec le démarrage du système d'exploitation ou de créer un raccourci dans le répertoire « Programme\Démarrage ». Si cette tâche et ses protections doivent être actives, vous devez la lancer!

La tâche « Résident: protection active » est partagée.

« Scan+Check: tous les disques locaux »

Cette tâche est une combinaison des tâches « Scan: tous les disques locaux » et « Check: tous les disques locaux ». Si vous avez besoin d'exécuter les deux tâches, il est plus rapide (d'un point de vue opérationnel) de lancer la tâche « Scan+Check: tous les disques locaux ». Ce qui a été dit sur les deux tâches auparavant s'applique également à celle-ci.

Tâches Speciales

Il existe deux tâches spéciales dans Avast32 : « Quick32 » (voir Chapitre 10.1) et « Ecran de veille » (voir chapitre 12.1).

Toutes les tâches spéciales sont des tâches « Privées » et ne sont accessibles qu'à travers le panneau de configuration.

3.8 Description générale des commandes du programme

L'interface utilisateur AVAST32 a été conçue conformément aux standards les plus utilisés dans ce domaine en général. C'est pourquoi seules les commandes standard du système sont utilisées.

En principe, le programme peut être contrôlé de deux façons: à l'aide d'un clavier ou d'une souris. Afin de travailler plus rapidement, nous vous recommandons l'utilisation d'une souris et le clavier uniquement pour entrer du texte. Une description détaillée de l'utilisation de la souris et du clavier est prévue dans le manuel d'utilisation ou dans le programme d'aide du système d'exploitation.

Dans le paragraphe suivant, le terme "élément activé" sera utilisé pour identifier l'élément en surbrillance. Dans la fig. 31, par exemple, le bouton "Lancer" est activé pendant que dans la fig. 32, la tâche "Scan+Check: tous les disques locaux" est activée. La couleur de la surbrillance d'un élément dépend de la configuration de l'environnement de votre système d'exploitation (répertoire "Panneau de configuration", et "Affichage").

Le programme est commandé par les éléments de contrôle. Un des éléments le plus important est l'onglet "Propriétés" représenté dans la fig. 33. Elle contient toujours plusieurs onglets à plusieurs contenus et fonctions même si un seul onglet est visible. Chaque onglet peut être affiché en cliquant avec le bouton gauche de la souris sur l'onglet en question.

fig. 33

A l'aide du clavier, vous pouvez passer d'un onglet général à l'autre en activant le menu "Propriétés" utilisant les touches fléchées. C'est ainsi que vous sélectionnez l'onglet droit ou gauche.

L'arborescence est un autre élément de contrôle très important. C'est une structure hiérarchique dont le contenu peut varier. Il peut s'agir par exemple d'une arborescence des répertoires d'un disque (le programme explorateur l'utilise aussi) ou de l'information sur le statut actuel (fig. 32).

Le contrôle par arborescence contient divers éléments. Si vous voulez décompresser un élément, cliquez avec le bouton gauche de la souris sur l'icône affichée devant le nom de l'élément en question. Si vous vous servez du clavier, vous devez d'abord activer l'élément et ensuite utiliser la touche fléchée vers la gauche (pour compresser l'élément) et la touche fléchée vers la droite (pour décompresser).

AVAST32 présente aussi un autre module, à savoir une liste. La fig. 31 montre la liste des tâches disponibles, mais il est clair que cette liste est aussi utilisée ailleurs. Elle peut contenir plusieurs colonnes dont la fonction est toujours décrite dans la première ligne. La largeur des colonnes gé-

nérales de la liste peut être adaptée en fonction des besoins en cliquant avec le bouton gauche de la souris sur le coin droit du nom de colonne. Gardez le bouton enfoncé et agrandissez la colonne à la largeur requise, ensuite relâchez le bouton.

Un élément de la liste est en surbrillance. Nous l'appelons activé. Si vous voulez activer un élément, il faut cliquer dessus avec le bouton gauche de la souris ou le mettre en surbrillance avec les touches fléchées du clavier (flèches vers le haut ou vers le bas). Si la liste contient trop d'éléments, on peut faire défiler les pages à l'aide des touches "page suivante" et "page précédente".

Sous le système d'exploitation Microsoft Windows, vous pouvez ouvrir un menu avec le bouton droit de la souris (fig. 34). Il en va de même avec AVAST32. Les commandes du menu se réfèrent toujours à un élément sur lequel vous avez cliqué avec le bouton droit de la souris (fig. 34 tâche "Scan: disquette A:") et il contient des fonctions pouvant être exécutées avec l'élément. La commande que vous souhaitez exécuter sera sélectionnée en cliquant dessus avec le bouton gauche de la souris. Le menu peut contenir non seulement les commandes, mais aussi leurs répertoires dans lesquels les commandes ou autre sous-répertoires etc. peuvent être sauvegardés. Le menu est souvent utilisé pour commander AVAST32 et c'est pourquoi nous vous recommandons aux débutants de s'habituer à travailler avec le bouton droit de la souris, certaines parties du programme ne pouvant être dirigées qu'au moyen de ce menu ou d'un clavier.

fig. 34

4.Création de nouvelles tâches

AVAST32 comprend dans son installation plusieurs tâches prédéfinies (chapitre 3.7) qui vous permettent d'utiliser le programme immédiatement après son installation et de vous servir de la plupart de ses fonctions. Après quelque temps, la plupart des utilisateurs souhaitent créer leurs propres tâches correspondant plus à leurs besoins.

fig. 35

Une nouvelle tâche ne peut être créée que dans le mode étendu de l'interface ou dans le Panneau de configuration (voir chapitre 6.7). Si vous êtes en mode normal, choisissez le mode étendu dans le menu "Mode". Passez à l'onglet "Tâches" et faites un clic droit sur la liste des tâches. Choisissez "Nouveau..." dans le menu optionnel (Figure 35).

Pour changer ou créer une nouvelle tâche sans être dans le programme AVAST32, il faut sélectionner le Panneau de configuration. Pour plus de détails, consultez chapitre 6.7.

On ne trouvera une description détaillée de la procédure de création de tâches que dans ce chapitre. Nous énumérons non seulement les contrôles de base, mais nous vous donnerons en même temps des recommandations à respecter en particulier par des utilisateurs moins expérimentés.

4.1 Tâche personnalisée ou partagée?

Avant de créer sa propre tâche, l'utilisateur devrait réfléchir à la fonction et aux utilisateurs potentiels. Quelques tâches devraient être disponibles à tous les utilisateurs d'un système normal, comme par exemple tester une disquette dans le lecteur A: ou tester tout le système. Mais quelques tâches peuvent être accessibles uniquement à un seul utilisateur. Il est par exemple possible de faire tester des documents et des applications privés.

Une telle séparation est très pratique puisqu'elle évite de recréer des tâches identiques pour chaque utilisateur

individuellement et, en même temps, l'utilisateur peut créer des tâches adaptées à ses besoins.

Les tâches accessibles à l'ensemble des utilisateurs d'une machine sont des tâches "Partagées". Elles apparaissent dans la liste des tâches et peuvent être utilisées ou modifiées, si elles ne sont pas protégées, par l'ensemble des utilisateurs. Dans la liste des tâches, elles sont précédées de l'icône de la Fig 36.

Fig. 36

Un l'utilisateur devrait créer des tâches partagées si plusieurs personnes se partagent un ordinateur. Dans la plupart des cas, c'est l'administrateur système qui s'en charge. Une protection par mot de passe est possible. Les utilisateurs sans mot de passe valable peuvent simplement lancer, arrêter ou copier une telle tâche. Pour des modifications, il leur faut connaître le mot de passe (voir chapitre 6.1.2).

Nous appelons tâches personnalisées les tâches qui ne sont accessibles que pour l'utilisateur qui les a créées. De telles tâches ne figurent pas non plus dans la liste d'autres utilisateurs et ils ne pourront pas effectuer des opérations avec ces tâches. Les tâches personnalisées sont signalées par leurs propres icônes à côté de leur nom dans la liste (voir fig. 37).

Fig. 37

a la création d'une tâche, l'utilisateur détermine si elle doit être personnalisée ou partagée (voir chapitre 4.4.1). Il est possible de modifier ces tâches à tout moment (bien évidement, en cas de tâche partagée, il faut connaître le mot de passe).

4.2 L'Assistant de création de tâche

L'interface AVAST32 a été conçue en fonction de tous les utilisateurs qui travailleront avec le programme. Comme nous l'avons déjà signalé, il est possible d'utiliser l'interface en mode normal ou en mode étendu. La raison principale est d'aider des utilisateurs moins expérimentés avec les fonctions du programme et de ne pas les perturber avec des détails complexes, mais, en même temps, de rendre accessible, pour les expérimentes, le contrôle total et les tâches.

Il en va de même avec la création d'une nouvelle tâche quand il est possible d'utiliser l'Assistant de création ou l'onglet "Propriétés". La différence principale entre les deux systèmes est basée sur les approches différentes des utilisateurs. En cas d'utilisation de l'Assistant, le programme travaille comme un assistant et la liste des signets ext uniquement on outil de création d'ne nouvelle tâche. Cependant, les fonctions sont identiques dans les deux systèmes.

Lors de la création d'une tâche, l'assistant sera utilisé, si l'option « Utiliser l'assistant de création de tâche », de l'onglet « Basic » du « Menu Général » a été activée (voir Chapter 6.1.1).

Avec l'assistant (fig. 38), l'utilisateur est aidé par le programme. Il traverse progressivement toute la procédure de création de tâche, fenêtre par fenêtre, et configure les fonctions dans les onglets généraux. L'utilisateur peut passer à tout moment à la fenêtre suivante ou retourner à la précédente à l'aide des touches « Suivant >> » et « << Précédent ». Il est également possible d'annuler la création à tout moment à l'aide de la touche « Annuler » ou « Echap » sur le clavier. La tâche peut être créée aussi uniquement sur la base de paramètres par défaut en cliquant sur « OK ». Dans ce cas, les valeurs par défaut seront utilisées pour les paramètres non définis.

Nous vous recommandons notamment l'utilisation de l'Assistant pour des utilisateurs qui apprennent à se servir d'AVAST32. Son utilisation est facile et il exclut pratiquement toute erreur due à un paramètre important. L'utilisateur peut ainsi apprendre des options spécifiques de paramétrage, ainsi que leur affichage par onglets individuels.

Si l'utilisation de l'Assistant est fermée, tous les onglets disponibles seront visibles dans la fenêtre « Propriétés » (fig. 38) dont l'utilisation est décrite dans le chapitre 2.5. Ceci permet à l'utilisateur de passer directement à l'écran contenant les commandes nécessaires sans avoir à visualiser tous les écrans précédents. Il est possible d'annuler la création d'une tâche en utilisant le bouton « Annuler » ou, alternativement, demander la création d'une tâche avec les valeurs par défaut en appuyant sur « OK » au moment de spécifier les paramètres.

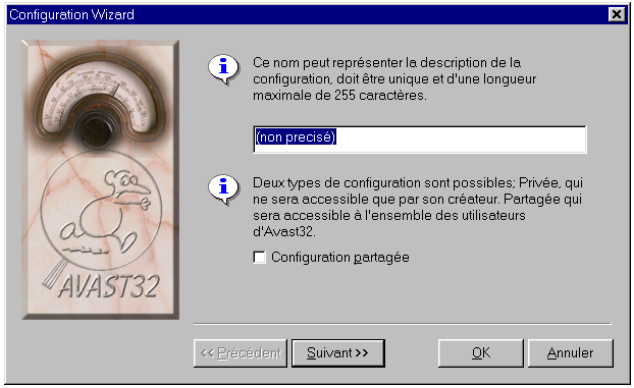

fig. 38

L'onglet « Propriétés » sera mieux utilisé par des utilisateurs plus expérimentés en raison de son exécution plus rapide. L'utilisateur ne configure que ce dont il a besoin et peut passer ensuite directement à la création d'une nouvelle tâche (cette façon de travailler, par contre, n'est pas recommandée pour des utilisateurs moins expérimentés). L'onglet « Propriétés » s'avère pratique en particulier pour modifier les paramètres d'une tâche déjà existante.

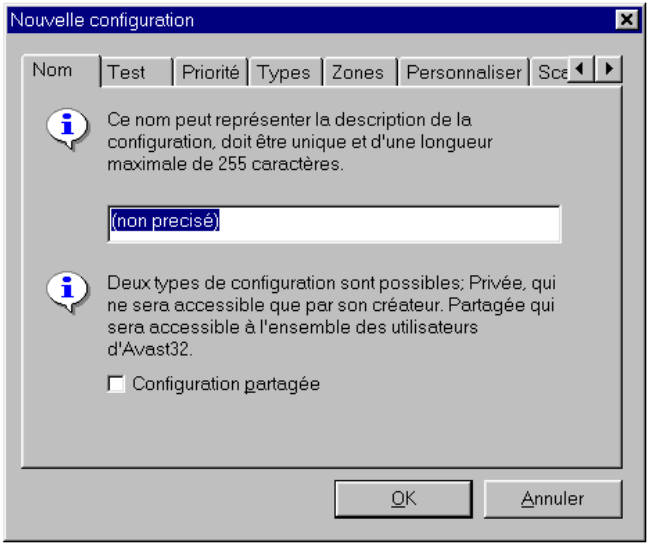

fig. 39

L'utilisation de l'assistant pour la création ou la modification des tâches est prévue par défaut.

La modification des paramètres de tâches existantes se fait dans le même environnement que la création de nouvelles tâches. Tout ce qui a été dit sur la création de nouvelles tâches s'applique donc également à leurs modifications. La seule différence est que si vous appuyez sur « Annuler » lors d'une modification des paramètres, les valeurs de tous les paramètres seront inchangées et, bien sûr, la tâche continue d'exister aussi.

L'assistant pour la modification d'une tâche peut être activé par la case « Utiliser assistant d'édition de configuration » sur l'onglet principal dans les « Options » du « Menu Général... » (voir chapitre 6.1.1).

4.3 Contenu de la tâche

Une tâche est l'élément de travail de base du programme AVAST32. Chaque tâche a un nom et contient une description détaillée de ses tests et propriétés à exécuter lors du lancement. Elle contient également des renseignements sur la priorité.

En général, trois tests peuvent être exécutés par une tâche: recherche de virus (scanner), contrôle d'identité et divers tests résidents). Les tests de base énumérés ci-dessus peuvent être divisés en sous-groupes mais, en principe, ce n'est pas nécessaire. Chaque test peut être configuré exactement pour les besoins de l'utilisateur.

En outre, il est possible de combiner ces tests presque arbitrairement, ce qui peut accélérer les procédures dans l'ensemble. Si vous programmez, par exemple, le scanner et en même temps le contrôle d'intégrité, ces tests seront exécutés sur des fichiers particuliers en même temps et il ne sera pas nécessaire d'appeler le fichier plus que nécessaire, etc.

Une partie de la tâche est l'information sur l'heure de lancement. Il est possible de configurer un démarrage automatique de la tâche en même temps que le système d'exploitation, ce qui protège votre ordinateur pratiquement pendant tout le temps de sa mise en route. C'est très prati-

que en cas de tests résidents quand l'ordinateur doit être "sous contrôle" le plus longtemps possible. Vous pouvez également programmer le lancement de la tâche avec le démarrage d'AVAST32 ou confier le lancement des tâches exclusivement aux utilisateurs. La tâche referme également la manière de présenter le message d'alerte en cas de virus. AVAST32 vous permet de saisir le texte d'un message d'alerte et vous pouvez choisir le type d'alarme qui l'accompagne.

4.4 Description des onglets des tâches

Ce paragraphe décrit les onglets individuels avec les fonctions. Vous trouverez la description de toutes les commandes des onglets et des paramètres par défaut. Les figures qui accompagnent l'utilisation des onglets individuels sont les mêmes que si vous utilisez l'Assistant. La fenêtre "propriétés" se présente d'une autre façon, les commandes et fonctions sont pourtant les mêmes (voir la différence entre fig. 38 et fig. 39).

Il convient de signaler que le nombre d'onglets disponibles dépend des activités sélectionnées de la tâche et peut souvent changer au moment de sa création. Aucun onglet avec les paramètres par défaut de la tâche ne sera affiché pour un contrôle qui ne fera pas partie de la tâche en question. Cette règle évite à l'utilisateur de passer par des onglets n'ayant rien à voir avec la fonction de la tâche.

4.4.1 Onglet « Nom »

Dans l'onglet "Nom", le programme demande de saisir le nom de la tâche à créer (fig. 38 et 39) Il doit être le plus approprié que possible et, afin d'éviter toute confusion, ne pas être identique à un autre nom de tâche existante, même si le programme est capable de travailler aussi avec des tâches portant le même nom. Si vous oubliez de saisir un nom, aucune tâche nouvelle sera créée. La ligne de texte marque par défaut: "non spécifié".

En cochant la case "Tâche partagée", il est possible de paramétrer s'il s'agit d'une tâche partagée ou personnalisée. Les tâches partagées peuvent être utilisées par tous les utilisateurs de l'ordinateur, contrairement aux tâches personnalisées qui ne pourront être exécutées que par leur créateur. Si vous ne cochez pas cette case, la tâche créée sera personnalisée, ce qui sera également configuré par défaut.

L'onglet "Nom" se trouve dans toute version de la tâche créée.

4.4.2 Onglet « Test »

L'onglet "Test" contient les commandes définissant le test à effectuer par la tâche (fig. 40). Il est possible de prévoir que la tâche effectue encore plus de tests en même temps. La configuration des commandes sur cet onglet relève de l'importance par rapport au nombre de Onglets disponibles. Si vous n'avez pas choisi un seul test, vous ne pourrez pas créer d'autres tâches.

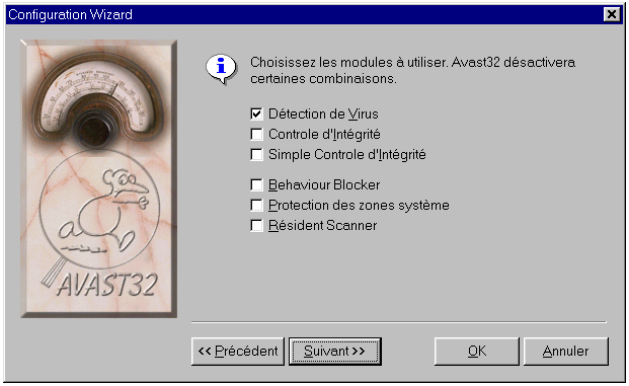

Fig. 40

La case "Détection de Virus" active la recherche des virus connus. Tous les virus connus seront recherchés dans chaque fichier sélectionné et leur présence sera annoncée à l'utilisateur. La recherche de virus est active par défaut.

La case "Contrôle d'Intégrité" est utilisée pour activer les test d'intégrité des données. Le test recherchera de toute façon dans tous les fichiers sélectionnés s'il y a eu des modifications ou non, et, dans l'affirmative, essaiera de déterminer comment ces changes ont été faits. La case est désactivée par défaut.

Avec "Simple Contrôle d'Intégrité", comme pour la case précédente, le test d'intégrité des données est activé. Mais contrairement au test ci-dessus, seuls les "checksum" simplifiés des contenus des fichiers seront calculés, aucun attribut des fichiers ne sera testé. De ce fait, le contrôle des modifications intervenues dans les fichiers sera plus rapide. Le contrôle d'intégrité simple n'est pas activé par défaut.

Les tests décrits ci-dessus sont appelés des tests non-résidents. Les tests suivants font partie de tests résidents. Suivant le type de test utilisé, nous parlons de tâches résidentes ou non-résidentes. Si un test non-résident est autorisé, la tâche sera non-résidente et tous les paramètres résidents seront ignorés. Si aucun test non-résident n'est coché, la tâche sera résidente.

La case "Contrôle d'Intégrité" ne peut être activée en même temps que "Simple Contrôle d'Intégrité" (ce qui n'aurait pas de sens non plus). Si vous cochez les deux cases, AVAST32 n'activera que la case cochée en dernier lieu. En d'autres termes, AVAST32 change l'activation pour qu'elle soit acceptable.

En cochant "Behaviour Blocker", l'utilisateur activera le blocage résident d'opérations suspectes de la tâche en question. Elle est basée sur une surveillance du système et un blocage successif des opérations potentiellement dangereuses. Ceci concerne quelques opérations des fichiers et le formatage des disques. Si le "Behaviour blocker" est permis, l'utilisateur est averti de chaque action de ce genre et il lui est demandé si l'opération doit vraiment être exécutée. Cette case est cochée par défaut.

La case "Protecteur des zone systeme" permet d'inclure dans les tâches le scanning du secteur de démarrage de la disquette avec laquelle le système d'exploitation est démarré. Il s'appelle le secteur de démarrage. Cette case est activée par défaut.

Le "Résident Scanner" active le contrôle des programmes et documents à exécuter pour la tâche en question. Chaque programme à exécuter sera d'abord contrôlé afin de vérifier s'il ne contient pas un des virus connus. En cas de détection d'un virus, le programme ne sera pas lancé et l'utilisateur en sera averti par un message d'alerte. Si non, le programme est lancé normalement. La surveillance du programme est activée par défaut.

L'onglet "Test" est disponible pour chaque version de tâche créée.

4.4.3 Onglet « Priorité »

Chaque tâche non-résidente permet de configurer sa priorité d'exécution. L'utilisateur annonce au système d'exploitation quelle importance la tâche revêt pour lui. Plus la tâche est prioritaire, plus le processeur lui donne de temps et plus vite elle tournera. il faut comprendre que la vitesse d'une tâche dépend non seulement de sa priorité mais aussi du statut actuel du système d'exploitation et des priorités de tous les autres programmes qui tournent en ce moment. La valeur par défaut de la priorité d'une tâche est plus petite que celle du programme AVAST32.

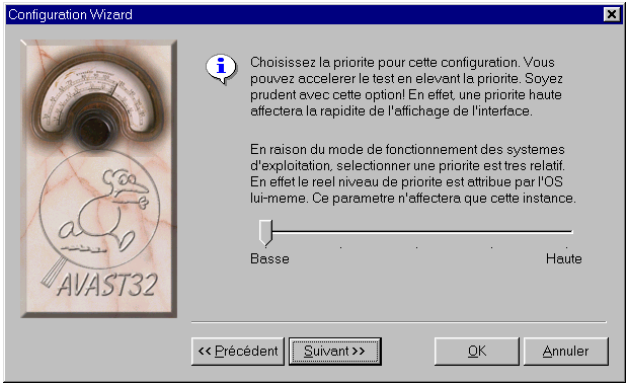

Fig. 41

Seul cet onglet permet de paramétrer la priorité d'une tâche (fig. 41). Il contient uniquement un curseur avec lequel on peut modifier la priorité de la tâche. Plus le curseur est à gauche, moins la priorité est importante et vice versa. Etant donné que vous intervenez directement dans le planning des tâches du système d'exploitation, nous vous recommandons de ne modifier le curseur que si vous savez ce que vous êtes en train de faire. La priorité par défaut sera suffisante pour la plupart des utilisateurs normaux. Si la priorité prédéfinie d'une tâche est trop haute, cela peut provoquer un ralentissement dans la restauration de l'environnement. Ceci n'est pas un défaut de programme, mais uniquement la conséquence d'une tâche qui a une priorité plus haute que l'interface AVAST32.

L'onglet "Priorité" n'est disponible que si vous avez activé virus scanning ou le contrôle d'intégrité normal ou simplifié, c'est-à-dire si la tâche contient des tests non-résidents.

4.4.4 Onglet « Types »

L'onglet "Types" détermine quels fichiers doivent être testés dans les zones sélectionnées (fig. 42). Dans la plupart des cas, il ne faut pas tester tous les fichiers, les virus n'en attaquent que quelques-uns. Par exemple, il est inutile de tester les fichiers texte (avec l'extension .TXT) car même s'il y avait un virus, le système d'exploitation ne permettrait pas de les ouvrir et le virus ne deviendrait jamais actif. En réduisant le nombre de fichiers à vérifier, vous augmenterez la vitesse d'exécution de la tâche.

Tous les fichiers à tester peuvent être consultés sur cette liste. Elle contient une description rapide du type de fichier et éventuellement de son extension. L'extension peut aussi comporter des signes tels que "*" (astérisque) et "?" (point d'interrogation), qui auront la signification habituelle dans le système d'exploitation.

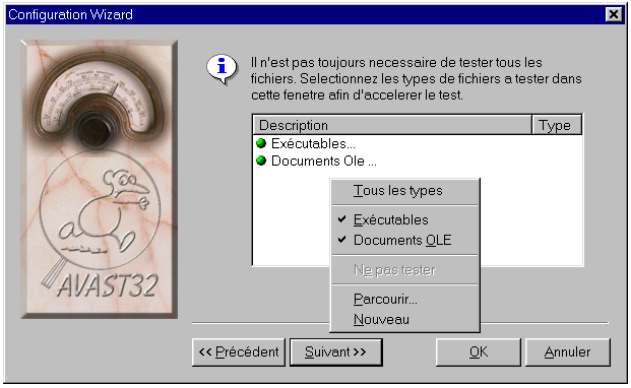

fig. 42

L'ajout d'un autre type dans la liste est possible à travers le menu contextuel (fig. 42) que vous ouvrez avec le bouton droit de la souris. Les trois premiers types dans ce menu sont les types par défaut que vous pourrez inclure dans la liste en les activant. Il y a "Tous les types" - le test de tous les types de fichiers sera activé, "Exécutables" - seuls les fichiers exécutables seront testés (librairies incluses) ainsi que "Documents OLE" qui entraînera un test des documents créés par la technologie OLE. Si leur sélection a été désactivée, ils seront automatiquement retirés de la liste.

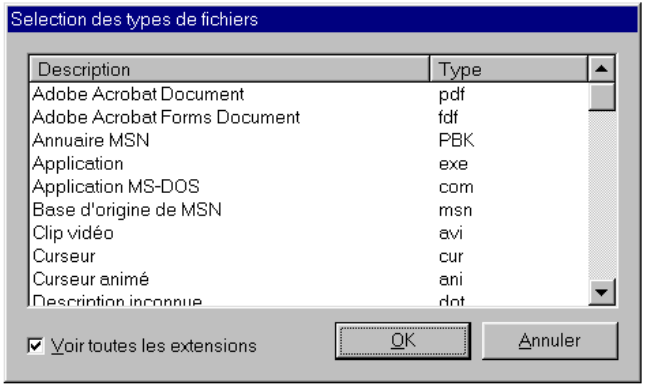

Fig. 43

Il est également possible d'ajouter des types à la liste venant de la base de données en utilisant la commande "Parcourir..." dans le menu contextuel. Si vous le sélectionnez, la boîte de dialogue de la base des types connus s'affichera (fig. 43). Elle peut contenir les types les plus importants ou, en cochant la case "Voir toutes les extensions", tous les types de fichiers. Si vous souhaitez inclure un type dans la liste des types activés, sélectionnez- le et cliquez sur OK. La fenêtre sera fermée en appuyant sur "Annuler" et la liste restera inchangée.

La commande "Nouveau" sert à entrer le type de fichiers directement sélectionnés. Après sélection, l'utilisateur peut écrire l'extension, appuyer sur Entrée et le nouveau type est ajouté à la liste.

Le symbole qui montre la façon de travailler avec ce type se trouve à côté du nom du type coché:

- des fichiers de ce type seront testés. Tous les types ajoutés en plus des types déjà activés sont marqués par défaut,
- ces fichiers ne seront pas testés. Ainsi, vous pourrez indiquer au programme de tester, par exemple, "Tous les fichiers" sauf les fichiers de l'extension TXT, etc. Pour marquer le type, il faut sélectionner la commande "Ne pas tester" du menu contextuel. Cependant, il n'est pas possible d'exclure les types par défaut.

Si certains types sont conçus pour ne pas être activés dans la liste, un léger ralentissement de la tâche peut se produire. Le programme doit vérifier non seulement si un type de fichier est à tester, mais aussi s'il faut l'exclure du test. Par contre, en excluant un type du test, vous pourrez considérablement accélérer l'exécution de la tâche. Chaque situation particulière dépend du modèle de fichier à tester. En résumé : si un test a été exécuté sur un fichier inutilement, cela ne vaut pas la peine d'exclure ce type de la liste. Un type peut être exclu de la liste en l'activant et en appuyant sur la touche "Suppr" ou, en cas de type par défaut (voir ci-dessus), il est possible d'annuler sa sélection dans le menu contextuel.

D'abord, le type du fichier sélectionné sera testé au cours de la tâche. Si le fichier se trouve sur la liste marqué d'un point vert, toutes les opérations seront effectuées. Sinon, il sera passé de côté. Les fichiers de programmes

(exécutables) ainsi que les documents OLE sont testés par défaut

Si la tâche doit exécuter le "Behaviour Blocker", seuls les tests avec les types prévus sur cet onglet seront effectués. Les commandes "Tous les fichiers“, "Documents OLE“ et les types à exclure (p. ex. marqués d’un point rouge) seront ignorés, leur présence dans la liste n’a pas d’influence sur Behaviour Blocker.

L’onglet "Types“ est disponible uniquement quand la configuration comporte au moins une des activités ci-après: virus scanning, contrôle d’intégrité (normal ou simplifié) ou Behaviour Blocker.

4.4.5 Onglet « Zones »

L’onglet "Zones" permet à l’utilisateur de programmer les disques ou répertoires devant être contrôlés par la tâche qui vient d’être créée (fig. 44). C’est ainsi que l’on peut déterminer uniquement les zones à tester et accélérer l’exécution de la tâche en écartant des zones dont le contrôle serait inutile.

Toutes les zones à tester s’affichent dans la liste sur cet onglet. Il est possible d’ajouter une zone avec le menu contextuel. Il prévoit les zones par défaut "Tous les lecteurs", "Disquette A:", "Disques Externes", "Disques durs locaux", "Disques durs Réseau" et "Choix à l'exécution". Le dernier élément signifie qu’avant le démarrage de la tâche, il sera demandé à l’utilisateur s’il y a d’autres zones à tester que celles spécifiées dans la liste. En activant la zone dans le menu contextuel, elle apparaîtra également dans la liste des zones à tester.

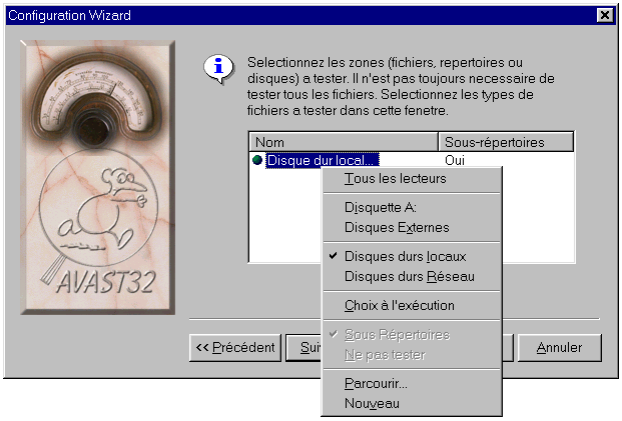

fig. 44

Avec la commande "Sous Répertoires" dans le menu contextuel, vous pourrez préciser si, dans une zone sélectionnée, tous les sous-répertoires doivent être testés. Si le répertoire n’est pas sélectionné, seuls les fichiers du répertoire ou du disque sélectionné seront testés - les répertoires éventuellement placés dedans ne seront pas testés. Cette commande peut être activé par défaut pour chaque zone testée séparément. Le test des sous-répertoires est actif par défaut.

Le symbole indiquant comment procéder se trouve à côté du nom de la zone à tester:

- cette zone sera testée. Toutes les zones ajoutées en plus des zones prédéfinies seront marquées par défaut,
- ces zones ne seront pas testées. C'est ainsi que vous pourrez indiquer au programme de tester par exemple "Disques durs locaux", sauf ceux du répertoire "C:\virus connus", etc. Le type pourra être marqué en choisissant "Ne pas tester" du menu contextuel. Cependant, il n'est pas possible d'exclure les zones prédéfinies.

La commande "Parcourir..." du menu contextuel vous permet de sélectionner directement les zones à tester. Après, vous verrez la boîte de dialogue standard pour choisir un nombre plus important de zones en même temps. Les zones choisies dans cette boîte de dialogue seront ajoutées à la liste.

La commande "Nouveau" sert à saisir une zone directement avec le clavier. Après saisie, la commande "Saisissez le nom de l'objet dans cette boite..." sera ajouté à la liste des zones testées, et il pourra être éditer. Une fois la zone saisie, appuyer sur "Entrée". Vous pourrez également vous servir des signes "*" (astérisque) et "?" (point d'interrogation) et préciser ainsi plusieurs répertoires à la fois.

Si vous souhaitez enlever une zone de la liste, sélectionnez-la d'abord avec le bouton gauche de la souris et appuyez sur "Suppr". Des zones programmées par défaut peuvent également être supprimées en les désactivant dans le menu contextuel.

L'onglet "Types" n'est disponible que si le virus scanning ou le contrôle d'intégrité, normal ou simplifié, sont autorisés.

4.4.6 Onglet « Personnaliser »

L'onglet "Personnaliser" présente les commandes des paramètres ne pouvant être regroupés sur un autre onglet à cause de leur nature (fig. 45).

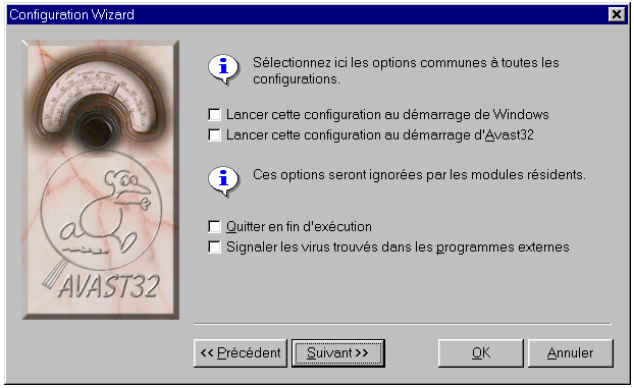

fig. 45

En activant la case "Lancer cette configuration au démarrage de Windows", l'utilisateur indique au programme que la tâche créée doit être lancée immédiatement après connexion de l'utilisateur. Cette case n'est pas cochée par défaut. S'il s'agit d'une tâche partagée et la case est acti-

vée, cette tâche sera lancée pour chaque utilisateur de l'ordinateur immédiatement après connexion.

La case "Lancer cette configuration au démarrage d'Avast32" démarre la tâche automatiquement après le lancement du programme AVAST32. S'il s'agit d'une tâche partagée, elle sera lancée automatiquement pour tous les utilisateurs ; dans le cas contraire, elle ne sera lancée que pour le créateur de la tâche. Le lancement avec AVAST32 est désactivé par défaut.

Les deux cases suivantes ne concerneront que les tâches non-résidentes, c'est-à-dire celles qui contiennent le virus scanning ou le contrôle d'intégrité. Leur programmation par défaut sera ignorée par les tâches résidentes.

La case "Quitter en fin d'exécution" active la fermeture automatique d'AVAST32 après la fin de la dernière tâche en cours. Cette option peut servir notamment en cas de tâches lancées d'une façon autre que directement par AVAST32, c'est-à-dire à l'aide d'un raccourci poste de travail. La case n'est pas activée par défaut.

La case "Signaler les virus trouvés dans les programmes externes" vous donne la possibilité de configurer que les programmes externes (c'est-à-dire des programmes ne faisant pas partie d'AVAST32) ne doivent être informés que du premier virus trouvé pendant la tâche en cours (case désactivée) ou de tous les virus trouvés (case activée). La case n'est pas activée par défaut. Vous trouverez En outre amples détails sur l'information des programmes externes dans l'annexe F.1.

L'onglet "Personnaliser" est disponible pour chaque variante de la tâche créée.

4.4.7 Onglet « Scanner »

Un des tests principaux du programme AVAST32 est le scanner. L'onglet "Scanner" (fig. 46) est utilisé pour configurer la partie du programme qui est uniquement responsable de la recherche des virus.

fig. 46

En activant la case "Tester la mémoire", l'utilisateur peut préciser si la mémoire vive doit être vérifiée au moment de la recherche des virus. On peut ainsi détecter un virus qui a déjà infecté l'ordinateur. Ce test sera effectué par défaut.

Pour le système d'exploitation Windows NT, vu sa structure, le test de la mémoire vive n'a aucun sens et si vous

travaillez avec ce système, ce test ne sera donc pas proposé. L'onglet "Scanner" sous Windows NT ne présente pas la case "tester la mémoire vive".

La case "Rechercher tous les virus" active la recherche de tous les virus de la base. Si la case n'est pas activée, les fichiers seront contrôlés pour déceler un virus attaquant le type de fichier en question. S'il s'agit d'un fichier COM, il ne sera pas testé pour un virus n'attaquant que des fichiers EXE, etc. La désactivation de cette case, vous permettra que les fichiers sont testés pour déceler la présence de tous les virus, sans tenir compte du type infecté. Cette case est activée par défaut.

La case "Test complet des fichiers" détermine si les fichiers doivent être balayés dans leur intégralié. Si la case n'est pas activée, AVAST32 testera uniquement quelques-unes des zones du fichier. C'est pratique du point de vue de la tâche. Le programme est conçu en partant du fait que la plus grande majorité des virus infectent des fichiers en se greffant à la fin du fichier ou en réécrivant le début et en général il est inutile de tester l'intégralité du fichier. Cette case est activée par défaut.

A l'aide de la case "Tester les fichiers compressés", vous pouvez activer le scanner des fichiers compressés. En effet, des fichiers compressés peuvent être attaqués de deux façons: avant la compression et après. Si le fichier n'est infecté qu'après compression, AVAST32 détectera le virus sans avoir à décompresser le fichier. Afin de pouvoir déceler un virus même s'il a infecté le fichier avant compression, il faut d'abord décompresser le fichier et scanner ensuite.

En cochant cette case, AVAST32 balayera d'abord les fichiers compressés, puis il décompressera les fichiers de façon interne (les fichiers resteront compressés sur le disque) et les fichiers ainsi obtenus seront balayés à nouveau.

A l'heure actuelle, AVAST32 supporte les programmes de compression Diet, Lzexe, Pklite et Ice. Le scanner des fichiers compressés est activé par défaut.

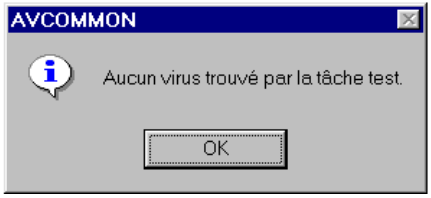

fig. 47

En activant "Prévenir si aucun virus trouvé", AVAST32 affichera un message après l'analyse, même si aucun virus n'a été trouvé (fig. 47). Cette commande est désactivée par défaut.

Vous pouvez aussi décider si vous voulez être averti des virus trouvés. Le choix se fait avec les boutons options:

- "Signaler tous les virus" indique à AVAST32 d'afficher un message d'alerte (voir chapitre 5.4) à chaque virus trouvé et d'attendre une réponse de l'utilisateur,
- "Notifier seulement le 1er virus trouvé" déclenchera un message d'alerte similaire mais uniquement pour le premier vi-

rus trouvé. Si l'utilisateur veut uniquement savoir si son ordinateur est infecté, il choisira cette option. S'il faut détecter tous les fichiers infectés après ce test, il suffit de cliquer sur l'onglet "Résultats" du mode étendu de l'interface,

- Avec "Ne pas signaler les virus trouvés" aucun message d'alerte sera affiché. Dans cette option, l'utilisateur ne sera pas informé de la découverte d'aucun virus. Comme on risque de passer à côté d'un virus découvert dans le système, nous conseillons de choisir cette option uniquement si vous avez opté pour le message de détection de virus à la connexion (chapitre 6.5.1, case "Afficher les messages d'alertes virales au démarrage").

La configuration par défaut est de signaler tous les virus trouvés.

L'onglet "Scanner" n'est disponible que si la tâche en question prévoit le scanner. Ce test sera sélectionné dans l'onglet "Test" (voir chapitre 4.4.2).

4.4.8 Onglet « Checker »

L'onglet "Checker" (voir fig. 48) sert à configurer le contrôle d'intégrité sur vos disques. On entend par contrôle d'intégrité le monitoring des changements effectués dans des fichiers individuels depuis le dernier contrôle. L'utilisateur peut ainsi détecter une activité de virus comprenant même des virus non-répertoriés.

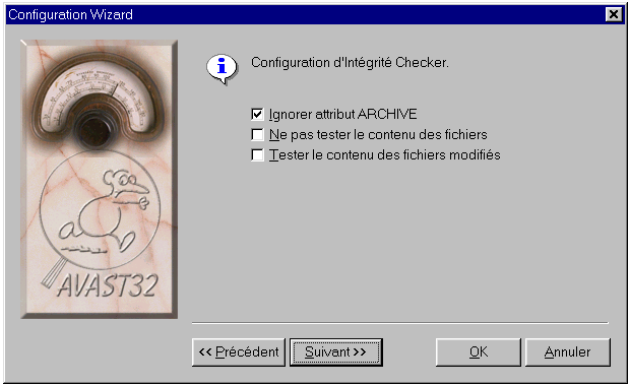

Fig. 48

En cochant la case "Ignorer attribut ARCHIVE", vous indiquerez au programme qu'il faut ignorer le changement dans l'attribut ARCHIVE des fichiers sélectionnés. Cet attribut est utilisé en particulier par les programmes de sauvegarde afin de reconnaître les fichiers à archiver. Le système d'exploitation prévoit cet attribut pour chaque enregistrement d'un fichier.

Si la case est activée, le contrôle d'intégrité ne signalera pas de modification de cet attribut, ce qui signifie que le fichier dont seul l'attribut ARCHIVE aura été changé depuis le dernier contrôle, ne sera pas mis sur la liste des fichiers modifiés. Cette case n'est pas activée par défaut.

Avec l'option "Ne pas tester les contenus des fichiers" vous pouvez désactiver le test de modification du contenu d'un fichier. Les fichiers ne seront contrôlés qu'en fonc-

tion de leurs paramètres de date de dernière modification, de la taille, des attributs, etc. mais aucun checksum de leur contenu ne sera créé. En activant cette case, vous accélérez l'exécution de la tâche, mais pour une plus grande sécurité de votre système, nous vous conseillons de maintenir le test des contenus des fichiers activé. Les contenus seront testés par défaut.

Avec l'option "Tester le contenu des fichiers modifiés", l'utilisateur à la possibilité de préciser que seul le contenu des fichiers doit être testé si une modification des propriétés de base est intervenue (attributs, date de dernière modification, etc.). Cette option est basée sur le fait que si le contenu du fichier a été changé, les paramètres ont aussi changé. En activant cette case, l'exécution de la tâche sera accélérée. Cette case n'est pas activée par défaut.

L'onglet "Checker" n'est disponible que si l'un des tests à faire est aussi prévu dans le contrôle d'intégrité normal ou simplifié (voir chapitre 4.4.2).

4.4.9 Onglet « Continuer »

L'utilisateur peut choisir ici une tâche à démarrer lorsque la tâche actuelle aura fini en cliquant sur "Continuer" (Figure 49).

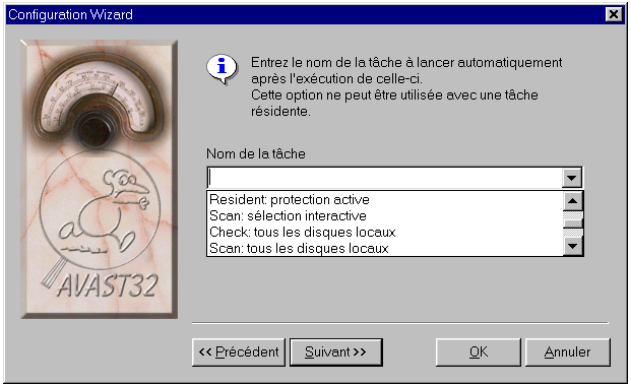

fig. 49

Vous pouvez saisir le nom d'une telle tâche dans la zone de texte prévue ou choisir une tâche dans la liste. Si vous cliquez sur la flèche à côté de la zone de texte, la liste s'affichera. La zone de texte est vide par défaut.

L'onglet "Continuer" est accessible uniquement pour les tâches non-résidentes, c'est-à-dire au moins un test non-résident doit être sélectionné dans l'onglet "Test".

4.4.10 Onglet « Rapport »

Au cours de l'exécution d'une tâche, AVAST32 peut créer un fichier contenant un message détaillé sur l'activité et les résultats. L'autorisation de créer un tel rapport et la définition de son nom fait l'objet de l'onglet "Rapport" (fig. 50). Le message sur l'opération de la tâche est stocké sous forme d'un fichier ASCII du fichier sélectionné (voir

ci-dessous). Il contient l'information sur les fichiers testés, les virus trouvés et d'autres informations importantes, plus des statistiques des tests.

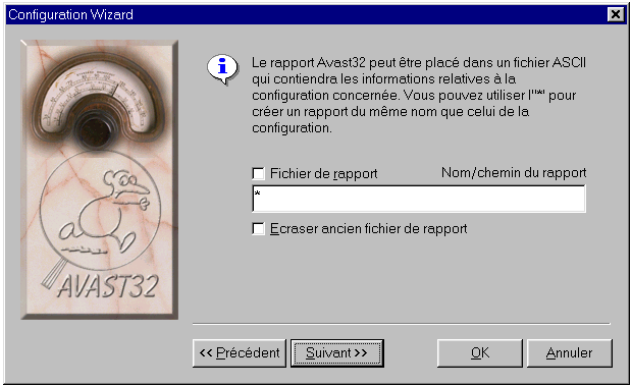

fig. 50

La case "Fichier de rapport" permet la création d'un fichier contenant un rapport sur l'activité de la tâche. Le fichier rapport sera créé par défaut.

La zone texte dans laquelle vous pouvez saisir le répertoire et le nom du fichier devant recevoir le rapport se trouve sous l'élément de contrôle précédent. Si l'utilisateur saisit l'astérisque "*" à la place du nom, le fichier rapport aura le même nom que la tâche, sauf avec l'extension RPT. Si aucune extension n'est précisée à la saisie du nom, l'extension RPT se met automatiquement. La zone texte présente "*" par défaut.

La case "Ecraser ancien fichier de rapport" informe le programme que, s'il y a déjà un fichier rapport de ce nom, il peut être remplacé. Si cette option n'est pas désactivée et si un fichier rapport existe déjà, le rapport sur la tâche sera ajouté au fichier déjà existant. Cette case n'est pas activée par défaut.

L'onglet "Rapport" n'est valable que si la tâche contient au moins une activité non-résidente, c'est-à-dire au moins un scanner ou un contrôle d'intégrité.

4.4.11 Onglet « Alarme réseau »

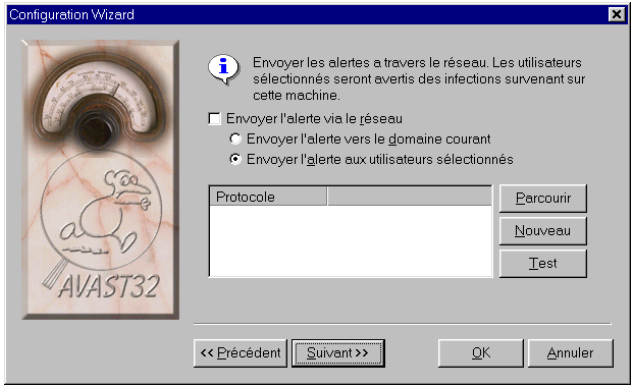

fig. 51

L'onglet « Alarme réseau » (fig. 51) prévoit les commandes pour paramétrer des messages d'alerte au réseau. En cas de découverte d'un virus, AVAST32 a prévu d'envoyer

des messages d'alerte sur le danger potentiel pour les ordinateurs reliés par réseau et empêcher ainsi une propagation.

La commande « Envoyer l'alerte via le réseau » déclenchera la diffusion d'un message d'alerte au réseau. Un tel envoi n'est pas autorisé par défaut.

Si vous avez activé l'envoi d'un tel message par réseau, vous devez également décider à quels postes de travail le message annonçant une éventuelle infection doit être diffusé. Vous avez deux options:

- « Envoyer l'alerte vers le domaine courant » prévoit l'envoi d'un message d'alerte de virus à tous les ordinateurs qui sont connectés à ce moment précis.
- « Envoyer l'alerte aux utilisateurs sélectionnés » enverra le message aux postes de travail précisés dans la liste de cet onglet.

L'envoi d'un message uniquement aux postes sélectionnés est activé par défaut.

Si l'envoi de message par réseau est autorisé et si l'envoi aux utilisateurs sélectionnés a été choisi, il faut déterminer les postes de travail. La liste des ordinateurs sélectionnés se trouve sous les commandes précitées.

Dans la liste des ordinateurs sélectionnés, vous pouvez entrer le nom de l'utilisateur à qui le message d'alerte virale doit être diffusé. Cliquez sur la touche « Nouveau » pour les protocoles des menus raccourcis.

- l'option « Internet » détermine que l'ordinateur destinataire du message d'avertissement est spécifié par une adresse URL standard. Le protocole SMTP (Internet Mail) sera utilisé,
- En choisissant l'option « Microsoft », vous indiquez au programme que l'ordinateur est accessible via Microsoft Mail,
- L'élément « RAW » autorise l'utilisateur à saisir toute adresse comportant le nom du protocole utilisé. Par exemple, l'adresse « SMTP:novak@aaa.cz » de ce protocole revient au même que l'adresse Internet « novak@aaa.cz » et réciproquement.
- « Interne » indique que l'ordinateur pour la diffusion du message d'alerte virale sera accessible par le réseau local.

Après avoir choisi un protocole approprié, la commande « Nouveau » s'ajoute à la liste. Faites un clic droit sur la commande pour éditer, ensuite, appuyez sur « Entrée ».

En cliquant sur « Parcourir... », un menu raccourci avec des protocoles s'affichera (dans cette version, il n'y a que la commande « Interne »). Vous pourrez choisir un ordinateur accessible via le réseau local dans une boîte de dialogue représentée dans la figure 52. Cliquez sur l'ordinateur concerné et sur « OK » pour le rajouter à la liste, sinon appuyez sur « Annuler » pour maintenir l'ancienne configuration.

fig. 52

Si vous voulez supprimer l'ordinateur de la liste, sélectionnez-le et appuyez sur « Suppr ».

Vous pourrez maintenant changer les paramètres des ordinateurs listés. Cliquez sur la colonne « Protocole » pour les modifier. Choisissez un nouveau protocole dans le menu raccourci. Vous pourrez également modifier le nom et l'adresse de la même façon. En cliquant sur le nom, vous pourrez éditer.

Si vous n'êtes pas sûr si un message a été diffusé, vous pourrez tester la « connexion » à l'aide du bouton « Test ». Un message test sera envoyé à chaque poste de travail sélectionné.

Si vous utilisez un autre protocole que « Interne », vous devez saisir le nom du profil souhaité ainsi que son mot de passe éventuel. Si vous laissez la zone « Profil » vide (ou si vous entrez un nom invalide), le profil déclaré pour l'utilisation de toutes les tâches sera utilisé (voir Chapitre 6.1.4). Si là encore, aucun nom de profil n'a été déclaré et si vous n'en utilisez aucun (par exemple si vous n'utilisez pas Microsoft Outlook), le nom du profil correct vous sera demandé.

Si vous saisissez un profil à ce niveau et saisissez un profil pour toutes les tâches, celui que vous aurez saisi à cette page sera utilisé.

Pour envoyer ou lire des messages réseau sous Windows NT, « Avertisseur » et « Messager » doivent être activés (« Panneau de configuration » / « Service »). Si vous n'avez pas le droit d'accès nécessaire, contactez votre administrateur système. Vous devez activer « WinPopup » pour la messagerie sous Windows 95.

Un message d'alerte peut arriver plusieurs fois sur un poste sélectionné. Ce n'est pas une erreur du programme mais relève du système. Le nombre de messages copiés envoyés dépend du nombre de protocoles réseau installés.

L'onglet « Alarme réseau » est disponible pour chaque variante de la tâche créée.

4.4.12 Onglet « Message »

Cet onglet sert à éditer le texte du message qui sera affiché à la découverte d'un virus (voir fig. 53). Si l'envoi de message par le réseau est activé, ce message sera diffusé à tous les postes sélectionnés (voir chapitre 4.4.11).

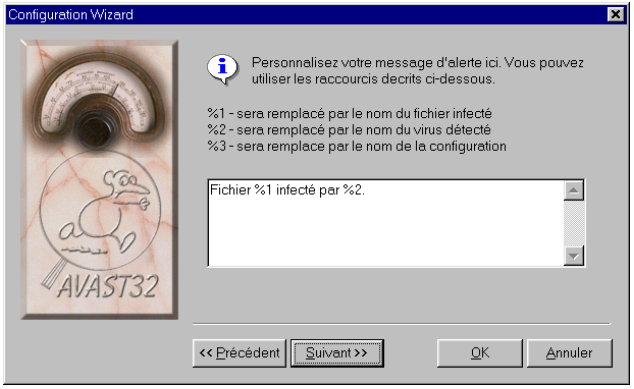

Fig. 53

Il y a une zone de texte permettant à l'utilisateur de saisir son propre rapport. A l'aide des signes de formatage, vous pouvez entrer même des variables comme le nom de fichier, le nom de la tâche, etc. Le signe de formatage sera alors remplacé par un nom normal.

Les signes sont les suivants:

%1 - fichier infecté,

%2 - nom du virus qui a infecté le fichier,

%3 - nom de la tâche où le virus est apparu.

Si, par exemple, la tâche "Personnelle" a détecté le virus "OneHalf" dans le fichier "D:\PRG.EXE", et le texte à saisir se présente ainsi: "Alerte! Virus %2 trouvé dans fichier%1. Tâche utilisée %3.", le message sera "Alerte! Virus OneHalf trouvé dans fichier D:\PRG.EXE. Tâche utilisée Personnelle.".

Par défaut, la zone de texte contient le message sous la forme:

Fichier %1 infecté par %2.

L'onglet "Message" est disponible si au moins une des activités est choisies: Scanner des virus, protecteur du secteur de démarrage et des fichiers exécutables ainsi que protecteur des documents OLE.

4.4.13 Onglet « Son »

A la découverte d'un virus, AVAST32 peut également diffuser un message sonore (fig. 54). Si vous désirez utiliser cette option, cliquez sur la touche "Setup" dans l'onglet "Son" et choisissez le fichier son dans cette boîte de dialogue (voir en bas pour plus de détails).

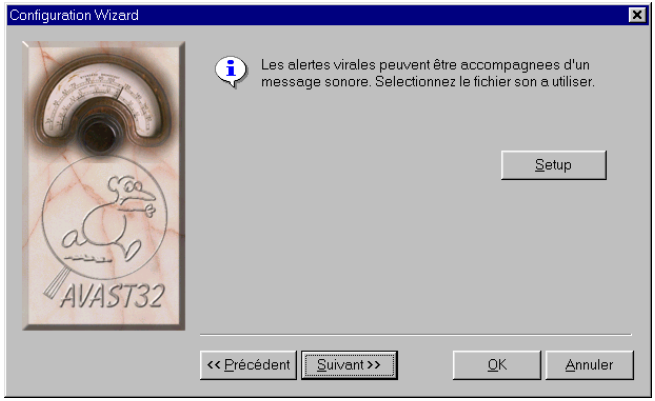

fig. 54

AVAST32 utilise pour le setup du message d'alerte virale un panneau de configuration du système "Sons" (Figure 55).

Trouvez d'abord le symbole "Avast32" et ensuite "Virus Trouvé" dans la liste des événements.

Vous pourrez saisir le répertoire et le nom du fichier son dans la zone de texte ou parcourir à l'aide de la boîte de dialogue pour ouvrir le fichier. Cette zone de texte sera disponible en cliquant sur "Parcourir...". Vous trouverez de plus amples détails sur cette boîte de dialogue dans l'aide ou dans le manuel du système d'exploitation.

Un fichier son approprié pourra également être choisi dans une liste en cliquant sur la flèche à côté de la zone de texte "Nom:".

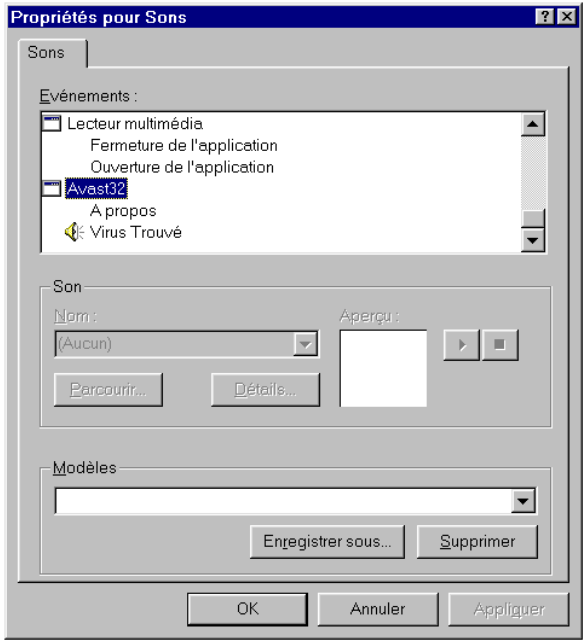

fig. 55

Les événements dans l'onglet sons du panneau de configuration pour AVAST32 peuvent même être choisis si AVAST32 n'est pas en cours - voir chapitre 6.7.3.

Votre ordinateur doit être équipé d'une carte son et des pilotes pour les fichiers son, le tout correctement installé et configuré. Si votre système d'exploitation émet des sons

(par exemple au démarrage du système, AVAST32 en émettra également.

L'onglet "Son" est disponible si au moins un des tests suivants est sélectionné: scanner des virus, protecteur du système de démarrage, behaviour blocker.

4.4.14 Onglet « Resident Scanner »

fig. 56

L'onglet "Resident Scanner" contient les commandes nécessaire à une plus grande précision des fichiers à scanner avant démarrage (fig. 56). Un type plus récent de virus n'attaque ni les exécutables, ni les secteur de démarrage des disques, mais les nouveaux fichiers de données: les documents OLE. Ces virus s'appellent les virus macro. AVAST32 prévoit également de contrôler de temps en temps les documents OLE à ouvrir. En réduisant le nombre de fichiers à tester, on peut accélérer le lancement des programmes et l'ouverture des documents OLE.

A chaque tentative de lancer un programme ou d'ouvrir un document, AVAST32 les testera d'abord par le scanner s'il sont infectés par un virus connu. Si non, le fichier sera ouvert. Dans le cas contraire, l'utilisateur sera averti. Cependant, les fichiers avec les documents OLE ne seront scannés que s'ils sont ouverts à l'aide de fonctions OLE. En cas d'opérations standard comme par exemple copier des fichiers, etc., le document ne sera pas scanné.

Les fichiers exécutables sont testés au moment où leur exécution ou ouverture nécessite les fonctions OLE. Ceci implique un léger ralentissement au démarrage d'une application testée ou lors de l'ouverture d'un document OLE, mais pas pendant le travail effectif avec l'application ou le document.

On peut tester les documents OLE, les applications 16-bits pour Windows 3.1x, les applications MS-DOS et, bien sûr, les programmes 32-bits. Vous déciderez de scanner le type de fichier en activant la case appropriée. Les applications 32-bits (c'est-à-dire désignées pour Windows 95 et NT) seront également scannées. On peut marquer une combinaison arbitraire des programmes surveillés. Tous les éléments sont activés par défaut.

En outre, l'utilisateur peut indiquer si au démarrage d'un programme, tous les fichiers doivent être scannés ou non, c'est-à-dire toutes les librairies, ou tous les fichiers sauf les librairies. La sélection sera activée avec les boutons op-

tionnels. La configuration par défaut aura une grande influence sur la vitesse de démarrage des applications, en particulier quand les mêmes librairies sont toujours utilisées. Si vous balayez périodiquement votre système, il convient, du point de vue vitesse, de désactiver au moins les contrôles des librairies. Au contraire, si vous avez l'intention d'installer un programme d'origine inconnue, nous conseillons d'activer le contrôle de tous les exécutables, librairies incluses.

Tous les fichiers exécutables ainsi que les fichiers DLL, sauf ceux du système, seront testés par défaut.

L'onglet "Resident Scanner" n'est disponible que si le protecteur des exécutables et des documents OLE fait partie des tests effectués par la tâche (voir chapitre 4.4.2).

4.4.15 Onglet « Behaviour Blocker »

L'onglet "Behaviour Blocker" présente les commandes pour la configuration d'un autre activité de la tâche, à savoir le blocage d'actions potentiellement dangereuses (fig. 57). A chaque tentative d'effectuer une telle opération, l'utilisateur sera averti et l'opération ne se fera qu'avec son accord.

De cette façon, par contre, l'utilisateur peut souvent être dérangé par des demandes inutiles. C'est pourquoi AVAST32 offre la possibilité de choisir uniquement les opérations qui doivent être surveillées.

fig. 57

En cochant la case "Surveiller les cessions DOS", AVAST32 surveillera des opérations potentiellement dangereuses provenant d'applications sous MS-DOS. Cette case est activée par défaut.

La case "Surveiller les applications Windows" activera le contrôle d'opérations potentiellement dangereuses avec les fichiers, entamées par des applications sous Windows. Cette case est activée par défaut.

Sous Windows 95, l'onglet contient également l'option "Surveiller le formatage de pistes". Nous conseillons de garder cette case cochée, parce que les virus se servant de ce service système sont particulièrement dangereux. Dans un cas moins grave, vous pourrez perdre une partie de votre disque dur, dans le pire des cas, tout son contenu. Cette case est activée par défaut.

Dans l'environnement du système d'exploitation Windows NT, l'onglet ne présente que "Surveiller les cessions DOS" et "Surveiller les applications Windows". L'onglet "Fermeture résidents" n'est disponible que si un des test est aussi "Behaviour Blocker" (voir chapitre 4.4.2).

4.4.16 Onglet « Ignorer »

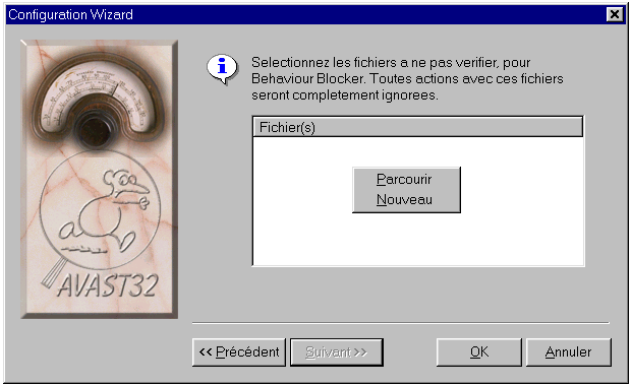

fig. 58

Cet onglet va permettre à l'utilisateur de préciser les fichiers pour lesquels toute opération (MS-DOS ou Windows) sera complètement ignorée par AVAST32 par le Behaviour Blocker activé (voir fig. 58). Cette possibilité a été incluse dans le programme, en particulier parce qu'il existe un grand nombre de programmes dont on sait qu'ils stockent des informations variées pendant leur exécution. Le signalement de ces opérations pourrait se révéler gênant et prendre du temps.

Cet onglet présente la liste des fichiers pour lesquels aucune opération ne sera effectuée. Si la tâche contient également d'autres tests que Behaviour Blocker, ils seront aussi exécutés sur ces fichiers de la liste. La liste de fichiers est vide par défaut. Si vous souhaitez ajouter un fichier, servez-vous du menu contextuel:

- La commande "Nouveau" mettra sur la liste un élément portant le nom "Nouveau..." et permettra à l'utilisateur de l'éditer. Après avoir saisi le nom du fichier, appuyez sur "Entrée".
- La commande "Parcourir..." ouvrira la boîte de dialogue standard pour l'ouverture de fichiers (fig. 89) et permettra à l'utilisateur de sélectionner le fichier recherché. Ce fichier sera ensuite transféré dans la liste.

Le nom de fichier ne comportera ni astérisques ni points d'interrogations. Le fichier pourra être supprimé de la liste comme d'habitude, c'est-à-dire en utilisant la touche "Suppr".

L'onglet "Ignorer" n'est disponible que quand Behaviour Blocker fait aussi partie de la tâche (chapitre 4.4.2).

4.5 Contrôler les données entrées

A la création d'une nouvelle tâche, AVAST32 demande de configurer certaines données et vérifie ensuite leur exhaustivité et leur authenticitié. Si les données sont incorrectes, l'utilisateur en sera averti. Si l'utilisation de l'Assistant pour cette opération est activée, l'utilisateur n'aura

même pas le droit de passer à l'écran suivant sans saisir les données correctes.

Le nom de tâche devrait être aussi proche de son action que possible et, pour des raisons de compréhension facile, ne pas s'appliquer à d'autres tâches. Cependant, le programme ne vous empêchera pas de créer d'autres tâches du même nom. Si le nom de configuration n'a pas été saisi, AVAST32 ne permet pas sa création.

Chaque nouvelle tâche doit effectuer une activité pour que sa création ait un sens. Des tests réguliers à effectuer par la tâche doivent être programmés sur l'onglet "Test" (chapitre 4.4.2). Si vous avez oublié de saisir l'activité de la tâche, sa création ne sera pas autorisée.

AVAST32 ne vous permet pas non plus de créer une nouvelle tâche si l'activité comporte le scanner et le contrôle d'intégrité, mais aucun type de fichier à tester n'a été spécifié (chapitre 4.4.4) ou aucune zone à tester n'a été définie (chapitre 4.4.5), c'est-à-dire les listes sur les onglets "Types" et "Zones" sont vides.

AVAST32 ne contrôle cependant pas si les fichiers saisis (fichiers son ou fichiers à ignorer) existent vraiment. L'utilisateur ne sera averti de leur non-existence qu'en cas de besoin. L'accessibilité des ordinateurs prévue sur l'onglet "Alerte réseau" (chapitre 4.4.11) n'est pas non plus vérifiée - vous pourrez le faire uniquement en utilisant le bouton "Test" sur cet onglet.

5.L'interface utilisateur

AVAST32 peut être commandé en deux modes. Le premier mode d'interface est le mode normal qui, de par sa nature, s'adresse aux utilisateurs devant exécuter des fonctions générales sans avoir à connaître des détails du programme et de ses fonctions.

L'autre mode "étendu" comporte l'extension de toutes les fonctions et possibilités offertes par AVAST32. Il sera plus utilisé par des utilisateurs plus expérimentés permettant d'adapter le programme à leurs besoins en profitant de toutes ses fonctions et avantages.

Un élément commun aux deux modes d'interface, à part le logo d'ALWIL Software company est le menu Fenêtres (voir chapitre suivant). La première colonne donne le numéro de la version du programme AVAST32 plus le numéro de compilation. Si vous contactez notre personnel pour un problème, vous aurez besoin de ces numéros.

La seconde colonne affiche le nombre de tâches disponibles et le nombre de tâches actuellement en cours. Dans la troisième colonne, vous trouverez le nombre de licences utilisé ainsi que celui des licences achetées. La dernière colonne n'est pas utilisée pour l'instant.

Au premier démarrage du programme, l'interface se présente en mode normal.

5.1 Menu principal Fenêtres

Le menu fenêtre est l'autre élément en commun du mode normal et mode étendu de l'interface (Figure 59). Il est installé dans la barre d'outils de la fenêtre principale et disponible quand le programme est en cours.

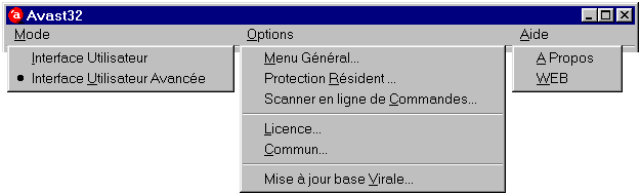

fig. 59

Menu "Mode"

Vous pourrez passer de l'interface en "Interface Utilisateur" au "Interface Utilisateur Avancée" et l'inverse. Le mode actuel est signalé par un point (Figure 59 montre l'utilisation du mode étendu de l'interface).

Menu "Options"

Utilisez ce menu pour personnaliser le programme AVAST32 et le comportement de ses modules. Il contient

par exemple l'option d'un assistant pour créer ou modifier une tâche. La commande "Options" prévoit également la mise à jour du fichier de base des virus (mise à jour fichier VPS). Compte tenu de la complexité et de l'importance de ces éléments, un chapitre entier leur est consacré. Vous trouverez donc toutes les informations sur la configuration du programme dans le chapitre 6.

Menu "Aide"

En cliquant sur "WEB" un logiciel pour parcourir Internet apparaîtra (s'il est installé) et si vous êtes connecté à Internet, la page de garde d'ALWIL Software s'affichera.

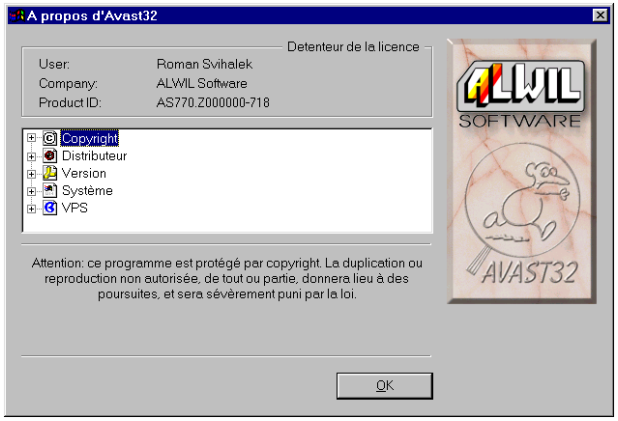

fig. 60

Le symbole "A Propos" dans ce menu vous donnera des renseignements sur le programme (Figure 60).

Vous devriez y jeter un oeil puisque vous pourriez en avoir besoin quand vous devez faire appel à notre technicien pour un renseignement technique.

Le personnel peut refuser de répondre à vos questions si vous ne fournissez pas ces renseignements!

Vous y trouverez les informations suivantes:

- copyright ,
- propriétaire de la licence et nombre de licences en cours dans le réseau,
- version d'AVAST32 et modules ainsi que le numéro de fabrication détaillé,
- système d'exploitation et mémoire physique disponible,
- version du fichier VPS et renseignements sur sa constitution.

La version d'AVAST32 et le numéro de fabrication pourront également être relevés dans la première colonne de la barre des titres dans la fenêtre principale du programme.

5.2 Interface en mode normal

Le mode normal de l'interface utilisateur est représenté dans la figure 61. Il contient la liste des tâches disponibles et plusieurs touches de commandes.

fig. 61

La liste des tâches contient les tâches disponibles. Elles sont précédées d'une icône vous renseignant sur leur statut. Suivant que la tâche soit "Privée" ou "Partagée" et en lecture seule ou non l'icône diffère comme le montre la Fig. 61. Si la tâche est en cours d'exécution, elle est précédée d'une boule verte (Fig. 61); Si elle est en pause, d'une boule rouge (Fig. 61).

Le bouton du milieu sert à lancer ou à arrêter l'exécution de la tâche. Son affichage change toujours en fonction de la tâche active, c'est-à-dire la tâche qui est en surbrillance dans la liste des tâches disponibles. Si la tâche active ne tourne pas, le bouton affiche "Lancer" et sert à lancer la tâche. Si, par contre, la tâche est en cours, le bouton affiche "Stopper" et sert à arrêter l'exécution de la tâche.

La tâche peut également être exécutée ou interrompue (mais pas arrêtée) en l'activant et en appuyant sur la touche "Entrée" ou en faisant un double-clic avec le bouton gauche de la suris sur son nom.

Avec le bouton "Quitter", vous terminerez le programme AVAST32. Toutes les tâches non-résidents seront arrêtées en même temps.

fig. 62

La figure 62 montre la fenêtre ouverte avec le bouton droit de la souris sur la tâche. Son contenu général dépend, par contre, de l'état actuel de la tâche. La fonction sélectionnée sera exécutée avec la tâche activée par la souris.

Le menu ouvert peut présenter les commandes suivantes:

- "Lancer" fait démarrer la tâche et n'est disponible que pour les tâches qui ne sont pas en cours à ce moment.
- "Stop" arrêtera la tâche et est uniquement disponible pour les tâches en cours ou interrompues.
- "Pause" va interrompre la tâche et n'est disponible que pour les tâches en cours à ce moment précis.

- "Créer un raccourci" va créer un raccourci pour la tâche sur le bureau. Un tel raccourci pourra ensuite être utilisé pour lancer la tâche directement sans passer d'abord par AVAST32. Cette commande est toujours disponible dans le menu contextuel.
- La commande "Afficher Aide flottante" fait accéder à l'aide du programme AVAST32. Vous pouvez également y accéder avec la touche F1 du clavier. Cette commande est toujours disponible par le menu contextuel.

5.3 Interface en mode étendu

L'interface en mode étendu présente l'interface facile à utiliser avec l'accès à toutes les fonctions et configurations d'AVAST32. Etant donné qu'un nombre élevé de fonctions et de paramètres ne tient pas sur une page, la structure du mode étendu se présente sur plusieurs onglets. Les chapitres suivants traitent les onglets individuels en détail.

5.3.1 Onglet « Tâches »

Cet onglet est divisé en deux parties (fig. 63). La partie gauche affiche la liste des tâches disponibles comme nous l'avons décrit pour le mode normal. Son utilisation et ses caractéristiques, à part le menu contextuel, sont identiques.

La partie droite de l'onglet contient les informations sur le statut d'une tâche active, ses caractéristiques et son avancement.

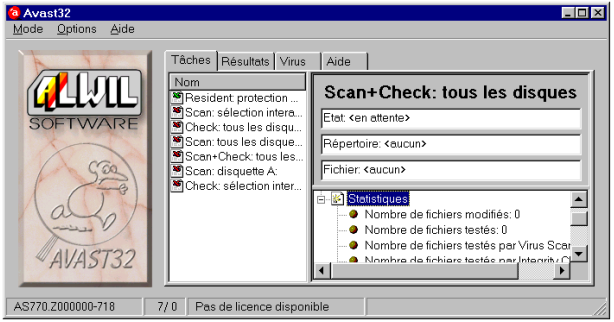

fig. 63

L'information sur le statut d'une tâche active se trouve dans la ligne de texte en haut. La première ligne "Etat:" indique le statut actuel de la tâche. Trois statuts sont possibles: la tâche n'a pas encore été lancée ("<en attente>"), la tâche a été lancée ("En cours") ou la tâche a été lancée mais est interrompue en ce moment ("<pause>"). Le chemin d'accès complet au répertoire contrôlé en ce moment est indiqué dans la deuxième ligne de texte "Répertoire" et la dernière affiche le nom du fichier contrôlé en ce moment. Si la tâche active est résidente (voir chapitre 4.4.2), seule l'information sur l'état de la tâche est affichée.

Les caractéristiques et données statistiques concernant l'avancement de la tâche sont classées dans l'arborescence qui se trouve sous les lignes de texte. Si vous décompresser l'élément concerné en faisant un double-clic avec le bouton gauche de la souris sur l'icône avant le nom de la tâche, vous aurez accès aux données de base.

Les informations sur le propriétaire de la tâche, les tests effectués pendant l'exécution, la date de création et la date de dernière utilisation se trouvent dans l'élément "Propriétés". Vous y trouverez aussi les informations sur le nombre total de lancements de la tâche depuis sa création.

Le dernier élément "Statistiques" (ouvert à la fig. 63) renseigne l'utilisateur sur le nombre de fichiers trouvés, testés, contrôlés en vue d'un virus, contrôles d'intégrité, non testés, infectés et le nombre de virus trouvés. Tous ces éléments concernent la tâche active. Si la tâche active vérifie l'intégrité de données, par exemple, l'élément concernant le nombre de virus trouvés sera toujours de 0!

Si la tâche active (c'est-à-dire la tâche sélectionnée sur la liste des tâches) est actuellement en cours, l'information est actualisée en temps réel et l'utilisateur est ainsi mis au courant de l'avancement.

Menu contextuel

Comme en mode normal, le mode étendu contient le menu contextuel qui sera ouvert en cliquant avec le bouton droit de la souris sur le nom de la tâche appropriée (fig. 64). Outre les commandes pour lancement, l'arrêt et l'annulation de la tâche, il affiche les commandes décrites ci-après:

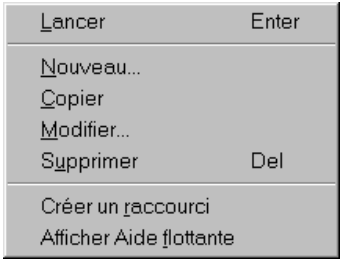

fig. 64

- "Nouveau..." est utilisé pour la création de nouvelles tâches. Son description détaillée se trouve dans le chapitre 4,
- Avec la commande "Copier", vous pouvez créer une copie exacte de la tâche en question. la nouvelle tâche contiendra la configuration de tous les paramètres exactement identique à celle de la tâche choisie. Cependant, le nom de la nouvelle tâche sera "Copie de <nom de la tâche>". Par contre, une copie ne peut être créée que d'une tâche disponible pour l'utilisateur, c'est-à-dire d'une tâche personnalisée. En cas de tâches non protégées par un mot de passe ou si l'utilisateur connaît le mot de passe, la copie pourra être faite d'une tâche partagée.
  Si l'utilisateur souhaite créer une copie de la tâche partagée et si les tâches partagées sont protégées par mot de passe que l'utilisateur ne connaît pas, la nouvelle tâche sera personnalisée. Toute configuration ultérieure restera inchangée.
- La commande "Modifier..." permet de changer les paramètres de la tâche. La modification se fait dans le même environnement que la création de la tâche. Tout ce qui a été dit

dans le chapitre 4 sur la création de nouvelles tâches s'applique également à la modification. Si vous appuyez sur le bouton "OK" dans la fenêtre de commandes des modifications et si les changements effectués remplissent les conditions prévues dans le chapitre 4.5, la modification sera prise en compte. Si, par contre, Vous appuyez sur "annuler", aucun changement sera effectué et les configurations restent les mêmes.

- Avec la commande "Supprimer", la tâche pourra être supprimée de la liste et du disque dur. Après l'avoir sélectionné, l'utilisateur sera demandé s'il veut vraiment supprimer la tâche (fig. 65). En appuyant sur "Oui", la tâche sera supprimée de manière irrévocable de la liste des tâches et du disque dur.

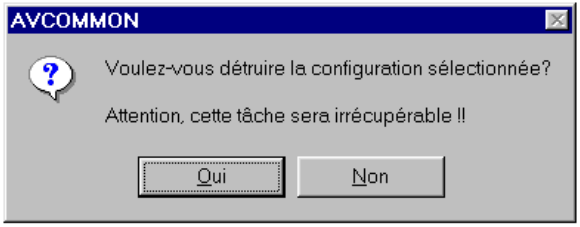

fig. 65

- La commande "Créer un raccourci" créera, comme en mode normal, un raccourci pour la tâche sur le bureau. Ce raccourci pourra être utilisé plus tard pour lancer directement la tâche sans passer par AVAST32.
- "Afficher Aide flottante" affichera le programme d'aide d'AVAST32. Vous pouvez y accéder également en utilisant la touche F1 du clavier.

5.3.2 Onglet « Résultats »

L'onglet "Résultats" affiche les résultats de toutes les tâches effectuant un scanner ou un contrôle d'intégrité (fig. 66). Les commandes de cet onglet sont très similaires aux commandes de l'Explorateur. Ce chapitre décrit uniquement les commandes et certains faits de l'onglet "Résultats". L'interprétation de ces faits sera traitée dans le chapitre 7.

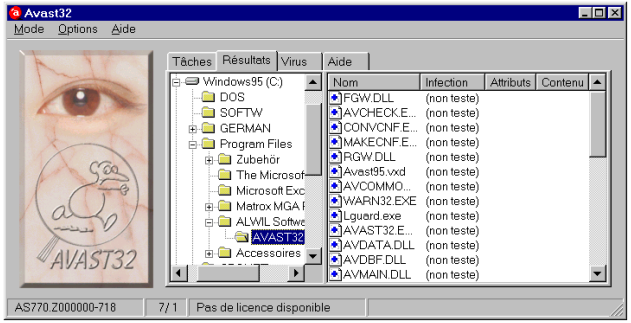

fig. 66

Les résultats des tâches sont résumés dans l'arbre du répertoire permettant à l'utilisateur à être bien informé des les résultats de toutes les tâches exécutées depuis le lancement du programme. Cependant, seuls les fichiers indiquant l'infection virale ou ayant été modifiés d'une façon ou d'une autre depuis le dernier contrôle, seront classés dans l'arbo-

rescence par AVAST32. En d'autres termes, c'est ici que vous trouverez tous les fichiers suspects.

Les nouveaux fichiers seront également classés dans cet arborescence, plus exactement ceux qui n'ont pas été trouvés par AVAST32 dans sa base de fichiers interne. Vous y trouverez également les fichiers qui ont été supprimés ou déplacés. Les secteurs de démarrage des disques et la mémoire sont traités de la même manière que les fichiers. En cas de changements, ceux-ci figureront aussi dans l'arborescence directement dans le répertoire "Poste de travail".

Les fichiers suspects seront classés sous l'arborescence selon leur chemins d'accès. Si l'arbre contient un répertoire, ce répertoire (ou un répertoire inséré) contient avec certitude le fichier suspect. Si vous souhaitez connaître les contenus de certains répertoires, sélectionnez-les et vous verrez dans la partie droite de l'onglet les fichiers suspects (s'il y en a). Le symbole représentant l'action effectuée avec ce fichier en question se trouvera devant le nom du fichier.

fig. 67

S'il s'agit d'une croix bleue (fig. 67), c'est un nouveau fichier, c'est-à-dire il a été créé depuis le dernier contrôle. Si vous avec lancé le contrôle d'intégrité pour la première fois, tous les fichiers trouvés seront marqués nouveaux parce que la base interne est toujours vide et doit d'abord être remplie.

fig. 68

Le signe moins en vert (fig. 68) signifie au contraire que le fichier portant un certain nom est manquant. Il est important pour vous de savoir ce qui a été fait avec votre ordinateur. Si, par exemple, vous avez vidé la corbeille depuis le dernier contrôle, il est évident que le programme signalera les fichiers du répertoire "corbeille" comme disparus. De la même manière, vous serez informé de la disparition de fichiers temporaires, etc.

fig. 69

Un autre signe à côté du nom de ficher est le point d'exclamation rouge (Figure 69). AVAST32 informe ainsi l'utilisateur que le fichier est infecté ou qu'une erreur s'est produite lors de l'analyse du fichier.

Si le fichier est infecté, le nom du virus s'affichera dans la colonne "Infection". S'il n'y a rien dans la colonne, une erreur a dû se produire lors du test. Ceci peut arriver pour

de nombreuses raisons, le plus souvent il s'agit d'une erreur de partage, c'est-à-dire que le fichier est utilisé par une autre application.

fig. 70

Si vous avez procédé à la restauration d'un document OLE (voir ci-dessous), un point d'interrogation jaune apparaîtra à côté du nom du fichier corrigé (fig. 70). AVAST32 indique ainsi que le statut du fichier est inconnu depuis la restauration ou depuis l'éradication d'un virus macro du fichier. Si vous devez savoir si le statut du fichier signalé varie de celui sauvegardé dans la base de données, veuillez revérifier l'intégrité du fichier.

L'indicateur vert peut apparaître à coté d'un fichier récupéré. Dans ce cas, il indique que le fichier en question n'est pas du type OLE et qu'il a été récupéré avec succès. Un fichier ainsi repéré se trouve dans l'état dans lequel il avait été stocké dans la base.

fig. 71

Si un icône tel que celui montré Fig. 71 apparaît à coté d'un fichier, cela indique un changement. Des informations sur la nature du changement sont données dans les colonnes à coté du nom du fichier. Pour plus de détails, voir ci-dessous.

- "Infection" indique le nom du virus avec lequel le fichier a probablement été infecté. Cette colonne est uniquement appropriée si le fichier en question a réellement été scanné en vue d'un virus. Dans l'affirmative, et si la colonne est vide, aucun virus connu n'a été découvert dans ce fichier. Si, par contre, la colonne affiche un nom de virus, le fichier a très probablement été infecté! Si le fichier n'a pas été testé, la colonne contient le texte "(non testé)",
- La colonne « Attribut » donne des informations sur les modifications d'attribut et la date de dernière modification du fichier. Sous Windows NT, elle contient également des données sur les modifications des sécurités du fichier. Si le contrôle d'intégrité a été effectué et que la colonne est vide, le fichier n'a subi aucune modification depuis le dernier contrôle. Dans le cas contraire, la colonne contiendra 3 points d'exclamation (!!!).
- La colonne « Contenu » donne des informations sur la nature (taille, contenu) de la modification. Si le contrôle d'intégrité a été effectué et que la colonne est vide, le fichier n'a subi aucune modification depuis le dernier contrôle. Dans le cas contraire, la colonne contiendra 3 points d'exclamation (!!!).

Nous attirons votre attention sur le fait que si la colonne "Infection" est vide, cela ne doit pas dire que le fichier n'est

pas infecté. Si le fichier en question a été contrôlé afin de déceler la présence d'un virus et que la colonne est vide, cela veut dire qu'au moment précis du programme, aucun virus connu n'a été détecté dans le fichier!

Menu contextuel

Le menu contextuel (fig. 72) se réfère toujours aux fichiers qui ont été marqués. Le même menu est aussi utilisé pour les répertoires à gauche de l'onglet. La fonction sélectionnée pour le répertoire en question sera exécutée pour tous les fichiers du répertoire ainsi que ceux dans les sous-répertoires.

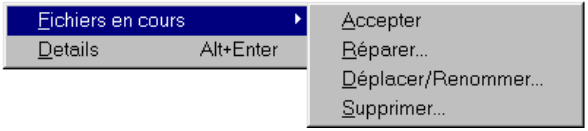

fig. 72

La commande "Détails" est utilisée pour afficher la boîte de dialogue avec une information plus exacte sur le type de fichier changé (fig. 73). Elle fournit des informations sur le statut, les attributs, la date de création et la dernière modification ainsi que la taille du fichier sélectionné et éventuellement aussi le nom du virus qui l'a infecté. Toutes ces informations s'affichent sur le statut original du fichier (sauvegardé dans la base de données) ainsi que sur le statut actuel sur le disque.

Vous pouvez afficher ce dialogue également avec la combinaison des touches Alt + Entrée.

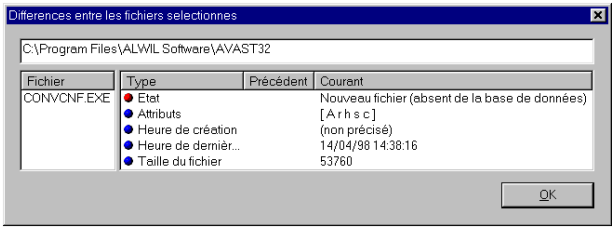

fig. 73

Le menu contextuel contient le répertoire "Fichiers en cours" qui affiche les commandes pour le travail avec des fichiers suspects:

Accepter des fichiers

La commande "Accepter" indiquera à AVAST32 que vous êtes au courant des modifications de vos fichiers et qu'il ne doit plus les signaler. Les fichiers ainsi traités disparaîtront de la liste des fichier suspects et si le répertoire dans lequel ils étaient stockés devait rester vide, il devrait disparaître à son tour. Cette commande sauvegardera le statut actuel des fichiers dans la base interne et au prochain contrôle ce statut sera le statut de départ.

Réparer des fichiers

La commande "Réparer..." essaiera de remettre les fichiers sélectionnés dans leur état d'origine. Si vous choi-

sissez cette commande, vous verrez un dialogue tel que celui de la fig. 74. Si le fichier à réparer est un document OLE, l'utilisateur a le droit de configurer des paramètres. Si non, la configuration n'a pas de sens et sera ignorée.

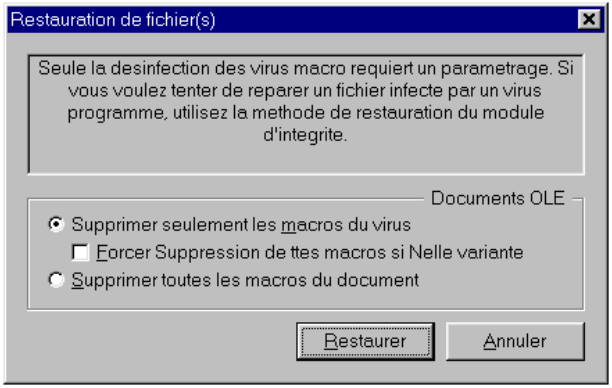

fig. 74

Avec le bouton d'option "Supprimer seulement les macros du virus", on peut demander que seuls les macros présentant un virus soient supprimés du document. Les autres macros resteront inchangés.

Le bouton d'option "Supprimer toutes les macros du document" aura pour effet de supprimer tous les macros du document OLE, même ceux qui ne contiennent pas de virus.

La configuration par défaut a pour effet de supprimer uniquement les macros qui contiennent un virus.

Si vous activez la case "Forcer Suppression de ttes macros si Nelle variante" (en cas de certains virus macro, la détection est très difficile), toutes les macros doivent être supprimées dans le document.

Si un fichier qui ne contient pas un document OLE doit être corrigé, AVAST32 essaiera de restaurer le fichier en utilisant la méthode basée sur le contrôle d'intégrité. En réalité, AVAST32 garde sa base de données dans laquelle il stocke d'importantes informations sur le statut de fichiers individuels et, à l'aide de la checksum, aussi sur leur contenu. AVAST32 essaiera de réparer le fichier sélectionné en utilisant ces informations. Il est possible de réparer jusqu'à 95 % de fichiers infectés. AVAST32 peut déterminer avec 100 % de précision si un fichier a été réparé ou non.

Il en résulte que si vous voulez réussir à réparer vos fichiers, vous aurez besoin d'une base de données régulièrement mise à jour sur les fichiers de vos disques durs. Cette base doit être actualisée, c'est-à-dire il faut effectuer des contrôles d'identité de temps en temps et d'enregistrer des changements autorisés dans la base interne de la commande "Accepter".

Les algorithmes utilisés pour la restauration de fichiers sous AVAST32 sont exclusivement destinés à réparer des fichiers infectés par un virus. Ils ne peuvent pas être utilisés pour le renouvellement de fichiers remplacés ou édités. La configuration des commandes du dialogue sera ignorée pour les fichiers ne contenant pas de documents OLE.

Si vous activez le bouton "Réparer", le processus de réparation de fichier sera lancé. Avec le bouton "Annuler"

vous fermerez la boîte de dialogue et les fichiers sélectionnés ne seront pas touchés.

Renommer et déplacer des fichiers

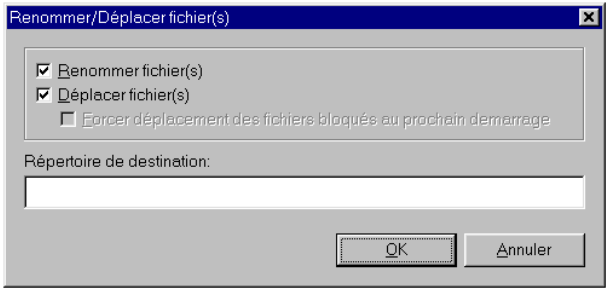

fig. 75

La commande "Déplacer/Renommer..." vous permet de déplacer des fichiers suspects dans un autre répertoire ou de les renommer. La commande affichera la boîte de dialogue représenté à la fig. 75. Ce dialogue contient trois commandes:

La case "Renommer fichier(s)" vous permet de changer l'extension des fichiers sélectionnés. les fichiers ainsi renommés seront distingués des autres et, en cas d'exécutables, vous les empêcherez d'être lancés accidentellement. Ceci provoquerait, en cas d'infection virale du fichier, la contamination de l'ordinateur (si ce n'est pas déjà arrivé). L'extension existante sera remplacée par celle prédéfinie (voir chapitre 6.1.3). Le nom propre du fichier restera inchangé.

Si le programme trouve un type inconnu de ce fichier pendant le processus de renomination, il va demander à l'utilisateur comment l'extension du fichier trouvé sera changée.

En activant la case "Déplacer fichier(s)", vous déplacerez les fichiers sélectionnés dans le répertoire choisi. Le nom du répertoire dans lequel les fichiers doivent être stockés ainsi que son chemin d'accès seront saisis dans la ligne de texte "Répertoire de destination:".

Si le déplacement des fichiers est activé, vous pouvez déterminer, en activant la case "Forcer déplacement des fichiers bloqués au prochain démarrage" que s'il n'est pas possible de toucher au fichier à ce moment précis (parce qu'il est utilisé par une autre application), on peut remettre le déplacement jusqu'au prochain démarrage du système. C'est ainsi que vous n'oublierez pas de déplacer le fichier - le programme s'en occupera lui-même.

L'action de renommer et de déplacer des fichiers plus la possibilité de remettre l'action au prochain démarrage sont activés par défaut.

Supprimer des fichiers

La dernière commande dans le répertoire "Fichiers en cours" est la commande "Supprimer...". En activant cette commande, vous verrez la boîte de dialogue pour choisir la manière de supprimer des fichiers. (fig. 76).

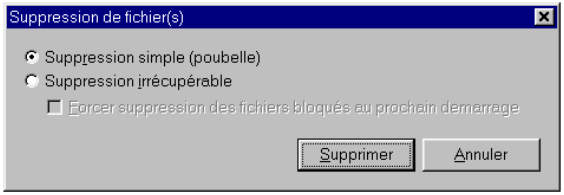

fig. 76

Si vous activez "Suppression simple (poubelle)", vous déterminez que les fichiers sélectionnés seront déplacés dans la corbeille et supprimés. C'est ainsi que vous pourrez restaurer à tout moment les fichiers supprimés et nous vous recommandons cette méthode aux l'utilisateurs moins expérimentés.

Si vous travaillez sous Windows NT, version 3.51, cette commande sera inaccessible et vous devrez suivra la procédure suivante.

Avec "Suppression irrécupérable", la suppression directe des fichiers du disque sera effectuée sans aucune possibilité de les restaurer.

En activant la case "Forcer suppression des fichiers bloqués au prochain démarrage" vous pouvez déterminer que s'il n'est pas possible de toucher au fichier à ce moment précis (parce qu'il est utilisé par une autre application), on peut remettre la suppression jusqu'au prochain démarrage du système. Cette case n'est pas active par défaut contrairement à la commande "Supp&ression simple (poubelle)".

En appuyant sur "Supprimer", tous les fichiers seront supprimés par la méthode choisie. Le bouton "Annuler" fermera la boîte de dialogue.

5.3.3 Onglet « Virus »

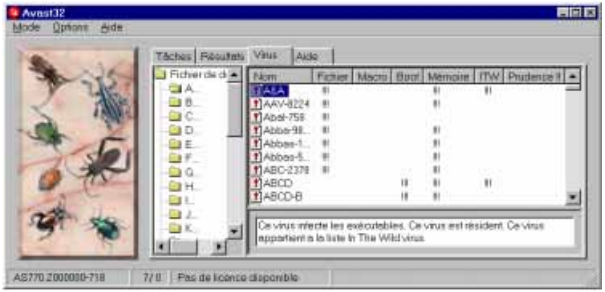

fig. 77

Si vous êtes intéressés à avoir plus de détails sur tous les virus qu'AVAST32 peut reconnaître, cliquez sur l'onglet "Virus". Cet onglet contient une liste complète par ordre alphabétique de tous les types de base de virus (fig. 77).

Comme tous les autres onglets, il est divisé en deux. A gauche, l'utilisateur a la possibilité de choisir la première lettre ou chiffre du nom du virus dont il voudrait savoir plus. Les virus commençant par cette lettre s'afficheront avec leur caractéristiques à droite de l'onglet.

Des virus peuvent se propager en général de la manière suivante: comme partie d'un fichier exécutable, en tant que macro d'un document spécifique ("virus macro"), ou en réécrivant le secteur de démarrage (qui est lu au démarrage du système d'un disque).

Les trois premiers colonnes ("Fichier", "Macro", "Boot") après le nom du virus correspondent aux méthodes précitées. Si une colonne à côté du virus en question contient "!!!" (trois points d'exclamation), ce virus infecte le système en utilisant la méthode décrite.

La colonne "Mémoire" indique si le virus peut être présent dans la mémoire vive de l'ordinateur infecté ou à long-terme (ceci s'appelle être résident). L'autre colonne indique si le virus figure sur la liste ITW des virus les plus fréquents. La dernière colonne marquée "Attention!!!" (trois points d'exclamation) vous met en garde contre la nature dangereuse du virus. Si vous rencontrez les trois points d'exclamation à côté d'un virus, il est plus prudent de ne pas y toucher. Les virus ainsi signalés sont très difficiles à enlever des ordinateurs ou peuvent très sérieusement endommager vos données. L'éradication de tels virus devrait être entamée par quelqu'un ayant vraiment de l'expérience!

Si vous marquez un virus sur la liste située à gauche de l'onglet "virus", un résumé de ses caractéristiques apparaîtra dans la zone texte de la partie inférieure. Ceci concerne en principe un listing compréhensible des contenus des colonnes décrites.

La partie gauche de l'onglet "Virus" montre, à part des signes alphanumériques et autres, deux éléments spéciaux. En utilisant "ITW", vous pouvez afficher à droite de l'onglet une liste de tous les virus du fichier actuel VPS, qui se trouvent sur la liste ITW. L'élément "Prudence !!" marche de la même façon affichant les virus les plus dangereux sur la liste à droite de l'onglet. Dans les deux cas, les virus sont triés par ordre alphanumérique.

Comme il faut explorer tout le fichier VPS afin de trouver les virus des deux éléments précités, ceci peut durer un certain temps. Il n'y a pas de description plus détaillée de tous les virus connus, de leurs activités et particularités. Vu leur grande quantité, il est d'abord impossible et ensuite inutile de tout savoir et de trouver chaque détail sur chaque virus. Les personnes intéressées par plus de détails sur un virus précis sont priées de contacter nos collaborateurs qui seront heureux de leur donner les renseignements demandés.

5.3.4 Onglet « Aide »

L'onglet "Aide" contient l'aide pour AVAST32. Les utilisateurs y trouveront toutes les informations utiles.

fig. 78

En cas d'un problème quel qu'il soit avec Avast32, le manuel d'Avast32 est accessible en permanence dans l'Onglet "Aide" de l'interface principale d'Avast32. Bien evidement, si votre problème n'y est pas référencé, contactez notre support technique.

Si le programme Acrobat Reader n'est pas installé sur votre ordinateur, il ne sera pas possible d'ouvrir l'Aide d'AVAST32. Dans ce cas, vous devez sortir d'AVAST32, installer Acrobat Reader (voir chapitre 1.2.1) et démarrez AVAST32 à nouveau.

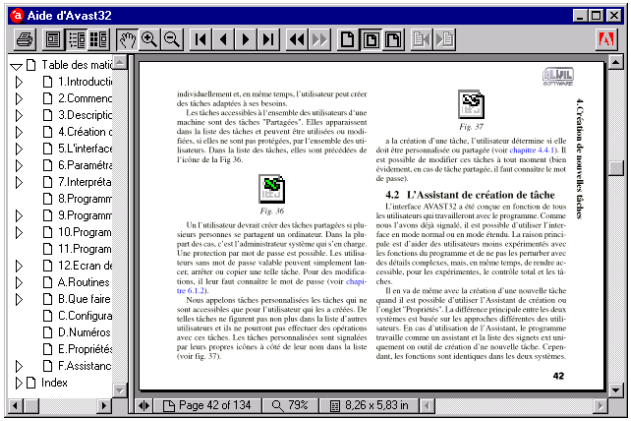

fig. 79

L'Aide AVAST32 peut constituer une partie de l'onglet "Aide" (voir fig. 78) ou être "flottante". L'Aide flottante désigne la fenêtre Aide que l'on peut déplacer librement sur le bureau (fig. 79). L'aide n'est donc pas limitée à l'onglet spécifique "Aide" mais peut être placée partout et est ainsi disponible à tout moment.

L'Aide flottante peut être appelée à tout moment de l'exécution du programme AVAST32, ou avec le menu contextuel ou par la méthode habituelle des systèmes d'exploitation Windows 95 et NT, c'est-à-dire avec la touche F1. Elle sera fermée en appuyant sur "Echap".

Si l'aide flottante est affichée, l'onglet "Aide n'affiche plus l'aide". Vous ne pouvez afficher qu'un seul menu d'aide à la fois. Qu'il soit sur l'onglet ou flottant, ses com-

mandes sont toujours les mêmes, le programme Acrobat Reader étant habitué à afficher l'Aide des deux façons. Cependant, il paraît faire partie intégrante d'AVAST32.

Les paragraphes suivants traitent les commandes d'aide.


fait imprimer l'aide ou une partie. En cliquant dessus, vous ouvrez la boîte de dialogue pour configurer les paramètres, la qualité et la longueur de l'impression.

Les trois icônes suivantes présentent les options du système d'aide:


La fenêtre n'affiche que l'aide normale. La partie amovible ne sera pas affichée.


La fenêtre Aide présente, à part l'aide, également la partie contenu (fig. 79). Si vous cliquez sur contenu, vous pouvez passer à la partie appropriée.


Affiche des onglets individuels à côté d'Aide. En cliquant dessus, vous passez sur l'onglet approprié.

Les trois boutons suivants déterminent la façon de travailler avec l'Aide (le pointeur de la souris prendra l'apparence de l'icône sélectionnée):


Déplace la page aide affichée dans une direction voulue et affiche la partie désirée.


La partie du menu aide sera agrandie en double.


Le document diminue de deux fois sa taille. Sa partie plus grande sera visible mais avec des détails plus petits.

Les quatre boutons suivants indiquent les déplacements dans le menu Aide (les autres paramètres, comme par exemple le zoom, resteront inchangées):


Première page du menu aide.


Page précédente.


Page suivante.


Dernière page.

Les deux boutons suivants vous permettent de passer par les étapes exécutées jusqu'à présent:


Annule la dernière commande, c'est-à-dire retourne à l'état précédant la commande. Ainsi on peut retourner à toutes les pages du menu Aide décrites jusqu'à présent.


Répète la même opération annulée auparavant.

Les trois boutons suivants agrandissent la page affichée:


Taille réelle, c'est-à-dire 100 %. La page peut être plus grande ou plus petite que la partie de la fenêtre réservée pour son affichage.


Le zoom sera configuré de façon à toujours afficher la page entière du menu Aide. Si la taille de la fenêtre est modifiée, la taille de la page le sera aussi.


La largeur de la page peut correspondre à la largeur de la fenêtre Aide, peu importe la hauteur de la page. Si la largeur de la fenêtre change, la largeur de l'affichage changera également.

5.4 Message d'alerte

Si un virus a été trouvé pendant l'exécution d'une tâche, AVAST32 affichera un message d'alerte (fig. 80). Le texte de ce message varie selon la configuration de la tâche qui a détecté le virus en question (voir chapitre 4.4.12).

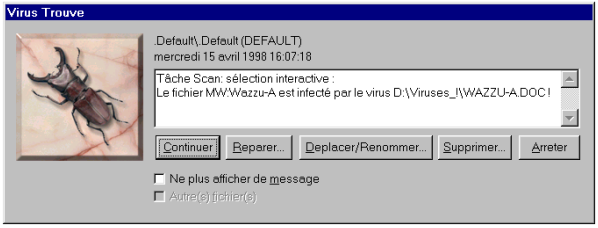

fig. 80

Avec le bouton "Continuer", vous indiquerez au programme qu'il devrait continuer avec la tâche. Le fichier infecté peut être traité plus tard à l'aide de l'onglet "Résultats" (chapitre 5.3.2).

Le bouton "Réparer..." sert à réparer immédiatement le fichier infecté. La même boîte de dialogue que celle de la commande "Réparer" du menu contextuel de l'onglet "Résultats" du mode étendu s'affichera. L'explication détaillée de cette boîte de dialogue est prévue au chapitre 5.3.2. Après réparation du fichier, vous pourrez continuer à exécuter la tâche.

Avec le bouton "Déplacer/Renommer...", l'utilisateur peut déplacer le fichier infecté dans un autre répertoire et/ou changer son extension. La description détaillée se trouve sous la commande du même nom du chapitre 5.3.2. Dès que le fichier aura été déplacé et/ou renommé, la tâche continuera son exécution.

Avec "Supprimer", vous enlevez le fichier infecté du disque. Une description détaillée de la boîte de dialogue apparente se trouve dans le chapitre 5.3.2 sous la commande "Supprimer...". Après fermeture de la fenêtre, la tâche continuera à s'exécuter.

A l'aide du bouton "Arrêter", vous arrêterez la tâche qui a détecté le virus.

Le message d'alerte contient deux contrôles supplémentaires.

Si vous activez "Ne plus afficher de message", vous indiquerez au programme qu'il ne dit plus afficher le message d'alerte à la prochaine détection de virus. Cette case n'est pas activée par défaut.

Si vous activez "Autre(s) fichier(s)", le programme procédera exactement de la même façon pour tout autre fichier infecté qu'il trouvera. Cette case n'est disponible que si "Ne plus afficher de message" est activée. Cette option n'est pas activée par défaut.

5.5 Sélectionner des zones à tester

AVAST32 demande à certains moments de spécifier les zones, c'est-à-dire fichiers, répertoires, ou disques entiers à tester. La fenêtre de dialogue (fig. 81) vous facilite cette précision. L'utilisateur pourra ainsi choisir plusieurs réper-

toires ou disques en même temps, ce qui rend le travail avec le programme beaucoup plus facile.

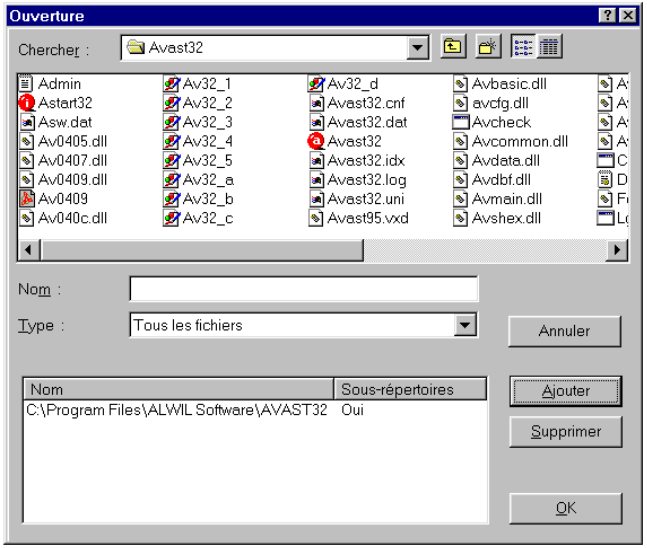

fig. 81

La partie supérieure de la fenêtre est pratiquement identique à celle de la fenêtre de dialogue standard pour l'ouverture des fichiers du système d'exploitation. D'habitude, l'utilisateur choisit le fichier, répertoire ou tout le disque qu'il veut sélectionner. Avec "Ajouter", il place l'élément sélectionné dans la liste dans la partie inférieure de la fenêtre. L'utilisateur procédera ainsi jusqu'à ce que la liste contienne toutes les zones à tester.

Si vous vous êtes trompé pendant la sélection ou si vous ne voulez pas tester des zones sélectionnées, supprimez les de la liste en les activant et en appuyant sur "Supprimer". L'opération ne sera pas effectuée sur une zone que a été enlevée de la liste.

A côté du nom de la zone il est indiqué si les sous-répertoires doivent également être testés. Si vous souhaitez modifier ce paramètre, cliquez sur le nom de la zone avec le bouton gauche de la souris. Le test des sous-répertoires est activé par défaut dans les zones rajoutées.

Si vous avez sélectionné toutes les zones demandées, vous pouvez démarrer l'opération en cliquant sur OK. Si vous activez "Annuler" (ou si vous fermez la boîte de dialogue d'une autre façon), la tâche sélectionnée sera annulée et les fichiers sélectionnés seront ignorés.

6.Paramétrage du programme

Utilisez le menu « Options » (Figure 82) pour adapter les fonctions d'AVAST32.

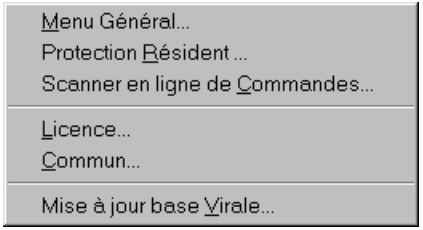

fig. 82

A chaque sélection d'un symbole, une boîte de dialogue s'ouvrira dans laquelle vous pourrez configurer les éléments appropriés. Toutes les fenêtres de dialogues sont divisées en plusieurs onglets identiques à la fenêtre principale d'AVAST32 et vous pourrez passer d'un onglet à l'autre.

Les pages sont marquées de points de couleurs différentes. S'il s'agit d'un point bleu, les commandes de l'onglet sont disponibles pour tous les utilisateurs – leurs paramètres n'affectent pas les fonctions du programme. Si le point est rouge, les commandes de l'onglet pourront être modifiées par des utilisateurs plus avancés qui connaissent les résultats de telles modifications. Les onglets marqués de point rouge sont donc uniquement accessibles aux utilisateurs ayant des droits d'administrateur système – ils ne s'afficheront pas aux autres utilisateurs.

Vous trouverez ci-après des détails sur des éléments particuliers du menu de la fenêtre principale « Options ».

6.1 « Menu Général... »

En cliquant sur cette option, une boîte de dialogue divisée en plusieurs onglets avec les configuration d'AVAST32 s'affichera.

6.1.1 Onglet « Général »

Cet onglet permet à l'utilisateur de personnaliser les fonctions du programme (Figure 83). Toutes les commandes sont sauvegardées séparément pour chaque utilisateur afin qu'AVAST32 maintienne un accès individuel pour chaque utilisateur. Ces modifications ne seront prises en compte qu'au prochain démarrage du programme.

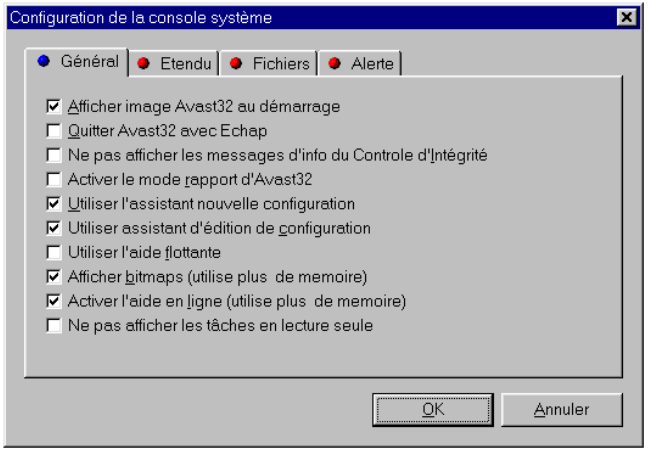

fig. 83

En activant la case « Afficher image Avast32 au démarrage », vous indiquez au programme d'afficher une fenêtre d'ouverture au démarrage d'AVAST32. Si cette fenêtre vous dérange ou si vous souhaitez accélérer le démarrage du programme, n'activez pas cette case. Cette case est activée par défaut.

« Quitter Avast32 avec Echap » définit s'il est possible de quitter AVAST32 avec la touche « Echap ». C'est intéressant pour des utilisateurs expérimentés préférant des touches de raccourci. Ne pas activer cette case peut empêcher des utilisateurs moins avancés de quitter le programme involontairement. Ce n'est pas coché par défaut.

En sélectionnant « Ne pas afficher les messages d'info du Controle d'Intégrité », vous indiquez au programme d'afficher le message de contrôle d'intégrité (Figure 92). Ceci s'applique pareillement au contrôle d'intégrité normal ou simple.

Le message n'apparaîtra pas jusqu'à ce qu'au moins un fichier testé ait été modifié. Il contient également un invite pour diffuser les résultats de la tâche. En appuyant sur « Oui », l'onglet « Résultats » de l'interface en mode avancé est activé. L'affichage de ce message est autorisé par défaut.

« Activer le mode rapport d'Avast32 » permet sous Windows 95 que toutes les opérations effectuées avec AVAST32 seront sauvegardées dans le fichier journal « AVAST32.log » qui sera créé dans le répertoire AVAST32. Les informations sur des virus trouvées ainsi que sur les utilisateurs travaillant avec ce programme seront également enregistrées.

La taille de ce fichier journal est donnée par la valeur saisie dans la zone de texte « Taille fichier journal » dans l'onglet « Fichiers » (Chapitre 6.1.3). Cet enregistrement (login) sera désactivé par défaut.

Sous Windows NT, le programme tentera d'enregistrer les informations dans le fichier journal du système. Vous pourrez visualiser ce fichier dans « Affichage événements » que vous choisirez dans le répertoire « Programmes/Outils système ». Si le programme ne peut pas écrire dans ce fichier, il enregistrera les informations de la même façon que sous Windows 95.

L'utilisation de l'enregistrement dans un fichier journal (login) s'applique particulièrement dans l'environnement réseau où vous pourrez contrôler l'activité des utilisateurs individuels.

« &Utiliser l'assistant nouvelle configuration » ouvrira la fenêtre de l'assistant qui vous guidera à travers la création d'une nouvelle tâche (voir chapitre 4). Nous recommandons ce procédé en particulier aux utilisateurs débutants. Cette case est activée par défaut.

« Utiliser assistant d'édition de configuration » ouvrira la fenêtre de l'assistant, mais cette fois-ci pour modifier une tâche existante (voir chapitre 4). L'utilisation de l'assistant est prévue par défaut.

Avec « Utiliser l'assistant nouvelle configuration » vous pouvez configurer une position arbitraire du programme d'aide sur l'écran sans être lié à l'onglet « Aide » (Chapitre 5.3.4). Cette case n'est pas activée par défaut.

« Afficher bitmaps (utilise plus de memoire) » activera l'affichage des images dans la fenêtre principale d'AVAST32. Les images illustrent les opérations effectuées et rendent le travail plus agréable. Cependant, leur affichage demande plus de mémoire vive et si vous n'en avez pas ou si vous n'êtes pas intéressé par les images, ne cochez pas cette case. L'autochargement des images est prévu par défaut.

La case n'aura d'influence que sur le programme AVAST32 - les images dans les fenêtres de dialogue de WARN32 et QUICK32 ne seront pas enlevées.

« Activer l'aide en ligne (utilise plus de memoire) » permet le lancement automatique du fichier aide d'AVAST32 après le démarrage. Il ne sera donc pas nécessaire de le charger du disque à chaque appel. Si cette option n'est pas activée, le fichier ne sera chargé qu'à la demande de l'utilisateur, c'est-à-dire après la sélection du symbole approprié du menu ou à l'aide de la touche F1. Cette case n'est pas activée par défaut.

Si vous disposez d'une mémoire vive suffisante et si vous consultez souvent l'aide, nous conseillons d'activer la case ce qui accéléra l'affichage du programme d'aide.

L'option « Ne pas afficher les tâches en lecture seule » permet de cacher ses tâches aux utilisateurs, quel que soit le mode d'interface choisit. Cette option n'est pas active par défaut.

6.1.2 Onglet « Etendu »

Les commandes du mode étendu sont visibles dans la figure 84. Leur modification aura une influence sur tous les utilisateurs travaillant avec le programme, la configuration de ces commandes est sauvegardée dans l'ensemble du programme AVAST32. Le changement prendra effet au redémarrage du programme.

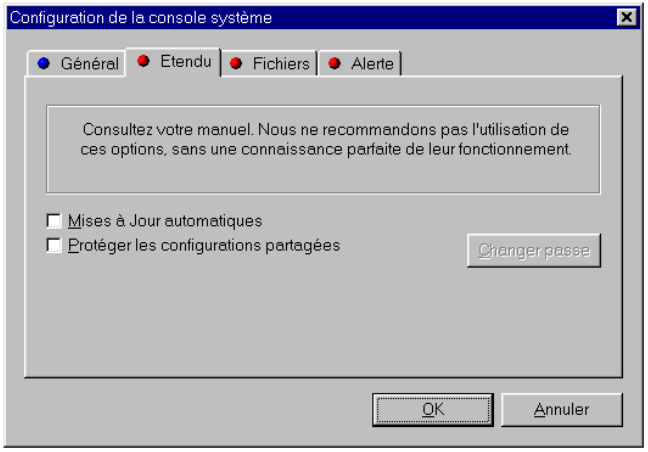

fig. 84

« Mises à Jour automatiques » sert à programmer la mise à jour automatique du fichier VPS contenant la base de données des virus connus. Si la case est activée, le programme AVAST32 cherchera automatiquement le répertoire prévu (Chapitre 6.6, zone de texte « Chemin d'acces au fichier de signatures ») au démarrage. Si le programme découvre un fichier plus récent, le fichier VPS existant sera automatiquement remplacé, sinon, rien ne se passera.

La mise à jour automatique du fichier VPS n'est pas activée par défaut.

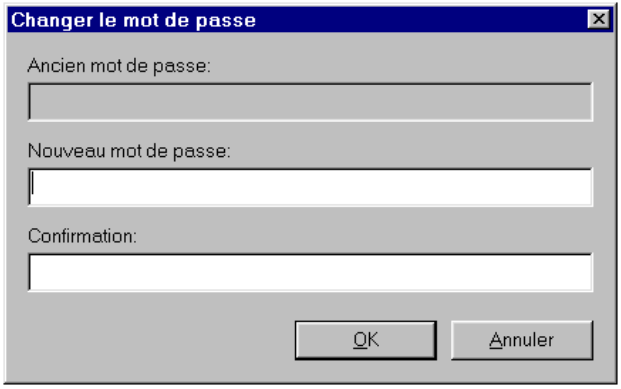

fig. 85

« Protéger les configurations partagées » vous permet de protéger par mot de passe les tâches partagées d'un changement. En activant cette option, la boîte de dialogue s'affichera pour entrer le mot de passe (Figure 85). Il doit être saisi deux fois, d'abord dans la zone de texte « Entrer nouveau mot de passe" et pour des raisons de contrôle également dans la zone de texte « Répéter nouveau mot de passe ». Si le mot de passe a été saisi de façon identique dans les deux zones de texte, il sera utilisé, sinon vous en serez averti et aurez une possibilité de le saisir à nouveau. Cette case peut être désactivée uniquement si vous connaissez le mot de passe valable actuellement.

Si des tâches partagées sont protégées par un mot de passe, les utilisateurs ne le connaissant pas peuvent uniquement lancer, arrêter, faire une copie personnalisée de

cette tâche ou créer un raccourci bureau, toute action ultérieure sera interdite.

fig. 86

Vous verrez la boîte de dialogue pour entrer le mot de passe dans la figure 86. Si le mot de passe est correcte, l'utilisateur pourra effectuer l'opération voulue. Il sera demandé de saisir le mot de passe une fois seulement - le programme se rappelle le mot de passe correcte et une nouvelle saisie ne sera demandée qu'au prochain démarrage du programme AVAST32, ou après la modification du mot de passe.

Pour modifier le mot de passe existant, utiliser la touche « Changer passe ». En appuyant sur cette touche, la même boîte de dialogue que celle pour la protection des tâches partagées s'ouvrira. Avant de mettre un nouveau mot de passe, il faut saisir le mot existant dans la zone de texte « Ancien mot de passe », même si l'utilisateur l'a déj saisi une fois au cours du programme. Si vous ne l'avez pas correctement saisi, une modification ne sera pas possible!

6.1.3 Onglet « Fichiers »

L'onglet « Fichiers » permet à l'utilisateur de spécifier les fichiers avec lesquels AVAST32 travaillera (Fig. 87). Les commandes de cet onglet sont maintenues pour l'ensemble du programme et leur changement affectera tous les utilisateurs. Les modifications seront prises en compte au redémarrage du programme.

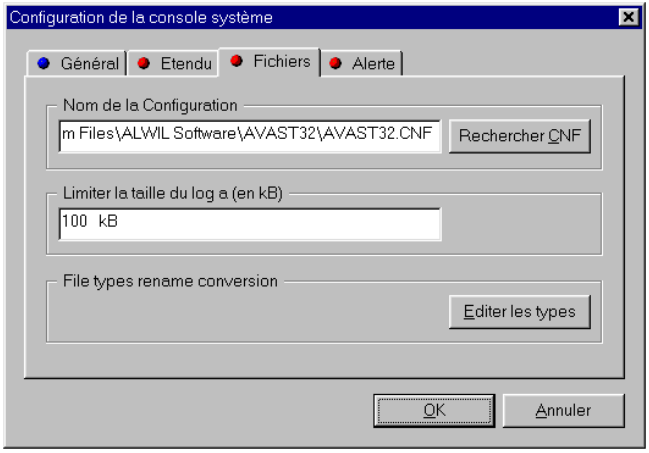

fig. 87

Dans la zone de texte « Nom de la Configuration », l'utilisateur peut entrer le nom ainsi que son chemin d'accès du ficher tâche (*.CNF) du programme AVAST32. Le fi-

chier tâche ainsi décrit sera utilisé à la place des fichiers existants.

En cliquant sur « Rechercher CNF », vous pourrez choisir le fichier tâche dans la boîte de dialogue standard du système pour l'ouverture de fichiers (Figure 88). Le nom du fichier sélectionné s'insère automatiquement dans la zone de texte. Le fichier CNF fichier dans le répertoire AVAST32 et utilisé par défaut.

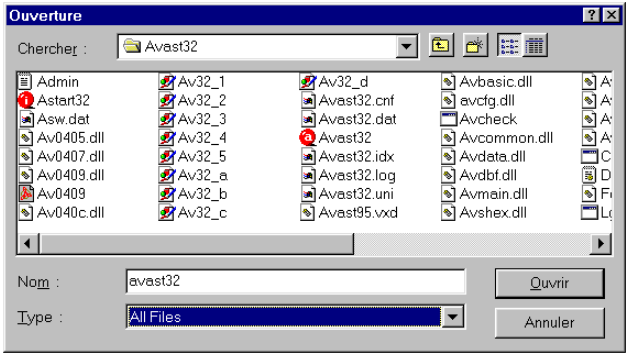

fig. 88

Dans la zone de texte « Limiter la taille du log a (en kB) », on peut donne une taille maximum du fichier d'enregistrement (log-in). La taille est indiquée en Ko (kilo octets). Si le fichier atteint à peu près la taille spécifiée, le premier tiers de ce fichier sera supprimé. Ainsi, les données les plus anciennes seront supprimées et la place sera faite pour recevoir de nouvelles données. La taille par défaut est de 64 Ko. La valeur dans la zone de texte n'a qu'un sens sous Windows 95 et si l'enregistrement est activé (pour plus de détails voir chapitre 6.1.1 « Activer le mode rapport d'Avast32 »).

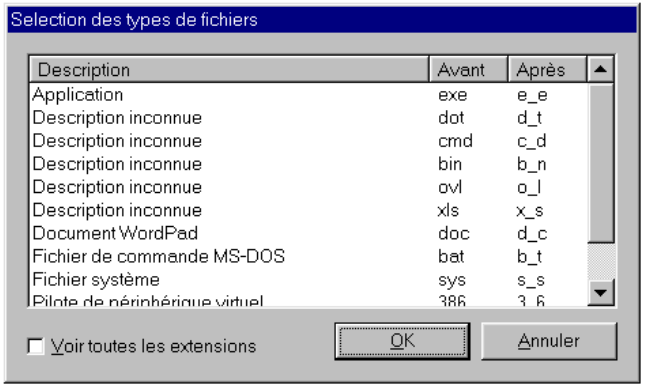

fig. 89

La touche « Editer les types » permet d'ouvrir une boîte de dialogue dans laquelle vous pouvez attribuer une nouvelle extension à un type donné de fichiers (Figure 89).

La boîte de dialogue contient une liste des types de fichiers connus et leurs extensions (colonne « Avant »). Dans la colonne « Après », les nouvelles extension remplaceront les anciennes en renommant le type donné de fichiers. Vous pourrez choisir entre deux options, les extensions les plus connues ou toutes les extensions connues en activant la case « Voir toutes les extensions ».

Les extensions dans la liste seront appliquées en renommant le fichier dans l'onglet « Résultats » (Chapitre 5.3.2). Les fichiers prévus dans l'arborescence dans cet onglet ont été modifiés d'une certaine façon ou le programme a trouvé un virus dans quelques-uns.

Si tel est le cas, il est recommandé (en particulier pour les exécutables) de les renommer pour éviter leur lancement, même accidentel.

Pour changer l'extension d'un type de fichiers, sélectionnez-le et cliquez dessus avec le bouton gauche de la souris. Ainsi vous pourrez l'éditer. La nouvelle extension sera confirmée avec la touche Entrée.

Si les modifications des extensions des fichiers vous conviennent, cliquez sur « OK ». Si vous préférez de garder les extensions utilisées jusqu'à présent, appuyez sur « Annuler ».

6.1.4 Onglet « Alerte »

L'onglet « Alerte » sert à choisir les postes auxquels le message d'alerte sera diffusé en cas de découverte d'un virus (Figure 90). Les utilisateurs de ces postes seront informés ensemble avec ceux dont les postes ont été sélectionnés pendant la création de la tâche qui a trouvé le virus (Chapitre 4.4.11).

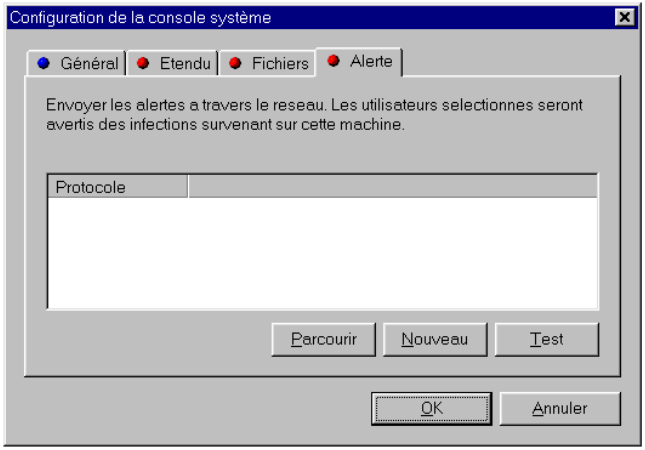

fig. 90

La liste des ordinateurs sélectionnés est sauvegardée pour l'ensemble d'AVAST32 ce qui veut dire que toute modification affectera tous les utilisateurs. Les modifications seront prises en compte au redémarrage du programme.

Le poste auquel le message d'alerte doit être diffusé sera défini en mettant son nom sur la liste des postes sélectionnés. En appuyant sur « Nouveau », un menu raccourci avec des protocoles s'affichera:

- L'option « Internet » détermine que l'ordinateur destinataire du message d'avertissement est spécifié par une adresse URL standard. Le protocole SMTP (Internet Mail) sera utilisé,

- En choisissant l'option « Microsoft », vous indiquez au programme que l'ordinateur est accessible via Microsoft Mail.,
- L'élément « RAW » autorise l'utilisateur à saisir toute adresse comportant le nom du protocole utilisé. Par exemple, l'adresse « SMTP:novak@aaa.cz » de ce protocole revient au même que l'adresse Internet « novak@aaa.cz » et réciproquement.
- « Interne » - le poste sera accessible par le réseau local.

En choisissant le protocole approprié, l'option "Nouveau" sera ajouté à la liste. Faites un clic droit sur l'option et appuyez sur « Entrée ».

Avec la touche « Parcourir », un menu optionnel avec des protocoles réapparaîtra (dans cette version, seul l'option « Interne » s'affichera). Vous pourrez choisir un ordinateur disponible par le réseau local dans une boîte de dialogue présentée dans la figure 52.

Pour supprimer l'ordinateur de la liste, cliquez dessus et appuyez sur « Suppr ».

Si vous utilisez un autre protocole que « Interne », vous devez saisir le nom du profil souhaité ainsi que son mot de passe éventuel. Si vous laissez la zone « Profil » vide (ou si vous entrez un nom invalide) et que le programme tente de vous envoyer un message, le nom du profil correct vous sera demandé.

Vous pourrez changer des paramètres des ordinateurs dans la liste en cliquant sur la colonne « Protocole » pour un changement de protocole. Choisissez nouveau protocole dans le menu optionnel. Vous pourrez changer de la même façon le nom et l'adresse. En cliquant dessus, vous pourrez éditer.

Si vous n'êtes pas sure de l'envoi du message, testez la connexion avec la touche « Test ». Un message sera envoyé à tous les postes sélectionnés. La liste des ordinateurs sélectionnés pour recevoir le message d'alerte est vide par défaut.

6.2 « Protection Résidente… »

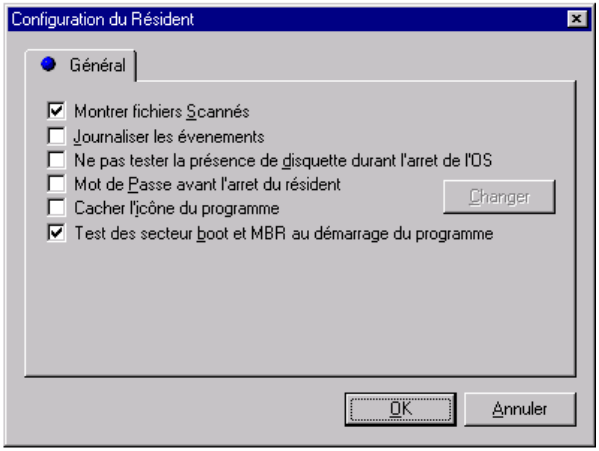

fig. 91

Une boîte de dialogue représentée dans la figure 91 s'affichera. Elle contient des commandes pour la configura-

tion de la protection résidente (il s'agit du programme RGW32, voir chapitre 9)

Les changements seront prises en compte au prochain démarrage du programme.

« Montrer fichiers Scannés » détermine si l'utilisateur souhaite être informé sur les activités résidentes en cours. Si cette option est activée, une brève information sur les activités résidentes en cours s'affiche en bas à droite du bureau. Si la case n'est pas activée (par défaut), aucune information ne s'affichera.

En activant « Journaliser les évènements », l'utilisateur pourra activer l'enregistrement des activités résidentes dans le fichier journal (pour de plus amples détails voir chapitre 6.1.1, « Activer enregistrement Avast32 »).

Si le résident d'AVAST32 est actif, vous pouvez désactiver le test de disquette pendant l'arrêt du système en validant l'option « Ne pas tester les disquettes pendant l'arrêt du système ».

Si une disquette infectée est présente dans le lecteur, votre ordinateur peut être infecté au démarrage suivant (si le boot depuis une disquette est autorisé dans les paramètres du BIOS). Si une disquette est détectée alors que l'option n'a pas été validée, un message d'erreur sera affiché (voir chapitre 9.3). Par défaut, cette option n'est pas validée.

« Mot de passe requis pour désactiver le résident ». Cette option, quand elle est validée, interdit l'arrêt du résident sans saisie d'un mot de passe correct (voir Fig. 86). Cette mesure protège les utilisateurs les moins expérimentés contre les attaques virales.

La boîte de dialogue (Fig. 85) sera affichée après validation de l'option. Celle-ci ne pourra être invalidée sans saisie d'un mot de passe correct.

Le bouton « Change » permet de modifier le mot de passe de RGW32 – si vous connaissez le mot de passe en cours. Le changement s'effectue par l'intermédiaire de la boîte de dialogue Fig. 85.

En cochant la case « Cacher l'icône », il se peut que l'icône de RGW32 ne s'affiche pas dans la barre de tâches même s'il est activé (Fig 103).Cette option n'est pas recommandée aux utilisateurs inexpérimentés. Par défaut, cette case n'est pas cochée.

La case « Tester les secteurs boot et MBR au démarrage » active le test des zones systèmes des disques locaux au démarrage. Cochée par défaut.

Sous Windows 95, présence de l'option « Test de la mémoire au démarrage ».

6.3 « Scanner en ligne de Commandes… »

En cliquant sur « Scanner en ligne de Commandes… » une boîte de dialogue telle que représentée dans la figure 92 s'affichera. Elle contient des commandes pour la configuration de base du scanner ligne de commandes – programme pour détecter des virus – démarré à partir de la ligne de commandes (il s'agit du programme LGW32, voir chapitre 8).

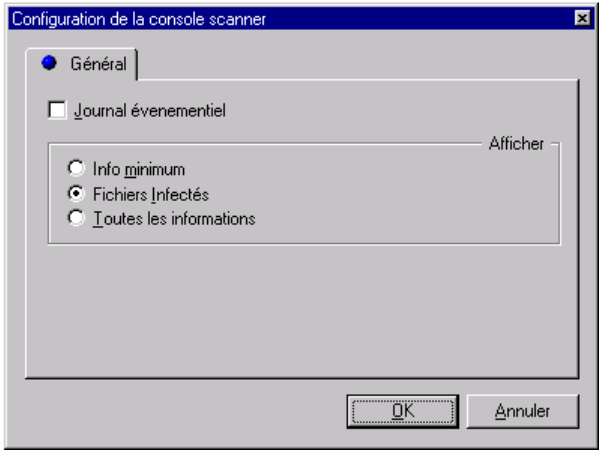

fig. 92

La boîte de dialogue contient également des options pour le nombre d'informations affichées à la sortie standard (en général une fenêtre de la ligne de commandes):

- le bouton optionnel « Info minimum » fait en sorte que le scanner ligne de commandes n'écrive que son en-tête,
- le bouton optionnel « Fichiers &Infectés » permet d'afficher des informations sur l'en-tête du scanner ligne de commandes, les fichiers infectés et les noms des virus. Le tableau avec le test complet s'affichera également,
- En activant « Toutes les informations », toutes les informations sur les activités du scanner ainsi que les résultats seront affichées.

Le nombre d'informations affichées sur le scanner ligne de commandes peut également être configuré par le biais des paramètres de la ligne de commandes (voir chapitre 8, /V paramètre). Dans ce cas, les configurations de cet onglet ne seront pas respectées.

6.4 « Licence… »

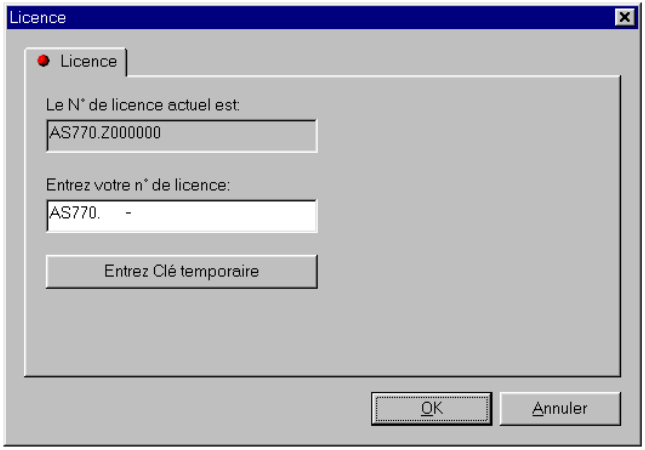

fig. 93

Dans la boîte de dialogue « Licence », l'utilisateur pourra modifier le numéro de série du programme (Figure 93). Entre autres, elle contient également des informations sur le nombre de licences achetées et si vous décidez d'en acheter d'autres, vous n'aurez pas à répéter

l'installation d'AVAST32. Vous ne changerez que le numéro de série dans cet onglet et tout sera prêt.

La page contient le code d'activation actuel. Vous pourrez saisir un nouveau code dans la zone de texte située en dessous. En cliquant sur « OK », le change s'effectue tout seul. Si le code n'est pas valable, un message d'erreur s'affichera et le code ne sera pas modifié.

Si vous cliquez sur « Entrez Clé temporaire », vous pourrez saisir le no. de code de cette version. Le programme fonctionnera totalement pendant trois mois avec ce code d'activation à moins que vous ne saisissez le code d'activation valable).

La signification des parties individuelles du numéro de série est expliquée dans l'annexe D.

6.5 « Commun… »

La boîte de dialogue propose les onglets avec des commandes communes pour tous les modules du programme AVAST32.

6.5.1 Onglet « Général »

Cet onglet contient des commandes pour la configuration de base de tous les modules d'AVAST32 (Figure 94). Les configurations des commandes dans cet onglet sont sauvegardées pour l'ensemble du programme et des modifications affecteront tous les utilisateurs.

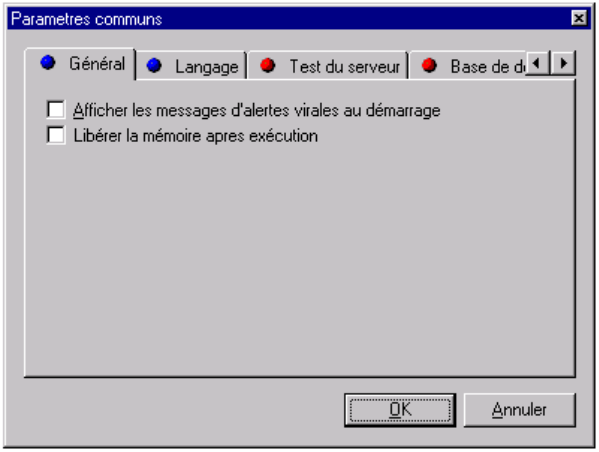

fig. 94

Les modifications seront prises en compte au prochain démarrage du programme.

« Afficher les messages d'alertes virales au démarrage » permet l'affichage du message d'alerte après la connexion de l'utilisateur. Le message d'alerte ne sera affiché que si un virus a été détecté au dernier démarrage de l'ordinateur. L'utilisateur est ainsi mis en garde qu'il travaille avec un ordinateur infecté. Cette case n'est pas activée par défaut.

Le programme WARN32 sert à afficher le message d'alerte. Vous trouverez des détails sur son fonctionnement dans le Chapitre 11.

« Libérer la mémoire apres exécution » détermine les conditions selon lesquelles le serveur de test (fichier

« VPS32.DLL », voir annexe A) sera présent en mémoire.

Si la case n'est pas cochée, le serveur sera présent en mémoire dès la première utilisation et ne sera pas enlevé, même à la fin de la dernière activité.

Si la case est activée, le serveur de test sera enlevé de la mémoire vive dès qu'il ne sera plus utilisé, c'est-à-dire à la fin de la dernière tâche. Au lancement de la prochaine tâche, il sera chargé à nouveau du disque.

Si vous disposez d'une mémoire vive suffisante, nous conseillons ne pas cocher la case. Ainsi vous pouvez accélérer AVAST32. Si vous avez un manque de mémoire vive, il vaut mieux activer la case mais s'attendre à des réponses plus lentes du programme. Cette case n'est pas activée par défaut.

6.5.2 Onglet « Langage »

L'écran « Langage » permet de basculer entre les différentes langues supportées par AVAST32 (Fig. 95). Les langues disponibles sont indiquées dans la première colonne. La langue en cours est repérée par un indicateur vert, les autres par un indicateur bleu.

La deuxième colonne renseigne l'utilisateur sur la disponibilité des documentations dans les langues considérées, c'est à dire si elles sont installées ou non.

Pour changer une langue dans le programme AVAST32, cliquez sur la langue concernée avec le bouton gauche de la souris. Cette modification sera prise en compte au prochain démarrage du programme. AVAST32 sauvegarde ce paramétrage pour chaque utilisateur séparément et cette modification n'affectera pas les autres utilisateurs.

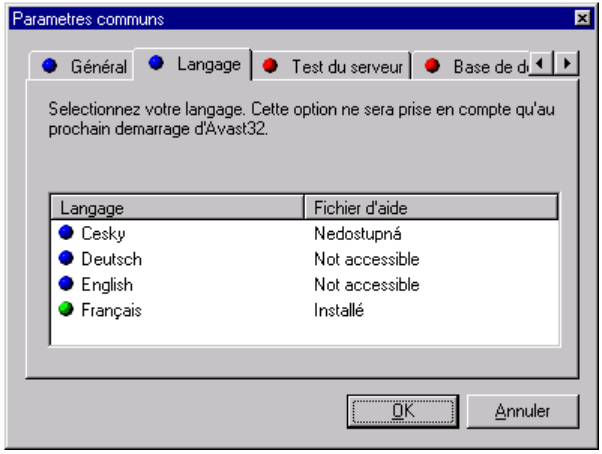

fig. 95

La langue choisie pendant l'installation est la langue par défaut (Figure 3).

6.5.3 Onglet « Test du serveur »

« Test du serveur » permet à l'utilisateur de paramétrer le serveur des tests (Figure 96). Il sera utilisé par tous les modules du programme AVAST32 et les modifications auront une influence sur tous les utilisateurs de ce poste (voir détails annexe A).

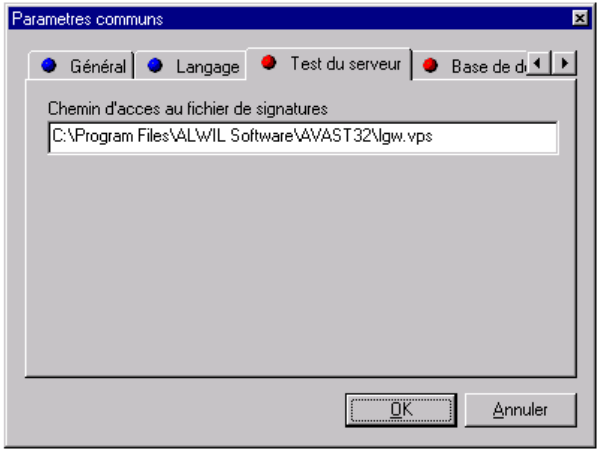

fig. 96

« Chemin d'acces au fichier de signatures » contient le nom du fichier VPS, c'est-à-dire du fichier qui contient la base de données des virus connus. Comme il s'agit d'un fichier très important, les utilisateurs devraient réaliser qu'en cas d'un mauvais paramétrage du fichier VPS, ils risquent de ne pas reconnaître des virus ou, par contre, de courir le danger de recevoir des fausses alertes. La valeur par défaut est le nom du fichier « lgw.vps » du répertoire d'AVAST32.

6.5.4 Onglet « Base de données »

Vous pourrez configurer dans la zone de texte « Repertoire de destination: » (Figure 97) le répertoire dans lequel AVAST32 gardera ces fichiers de bases. Les fichiers dans la base sauvegardés sur votre disque durs seront principalement utilisés dans le test d'intégrité des données.

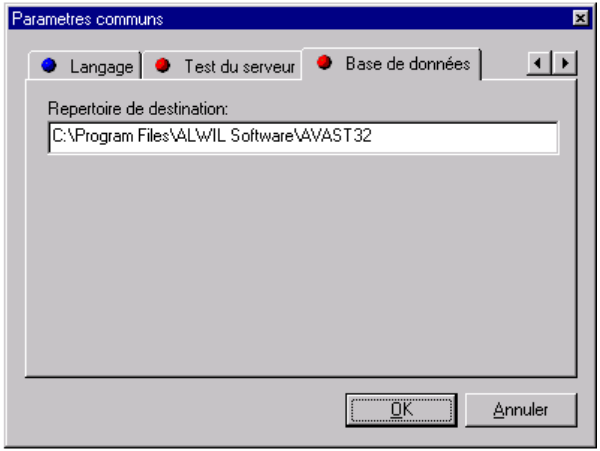

fig. 97

6.6 « Mise à jour base Virale… »

AVAST32 prévoit une mise à jour facile du fichier de données des virus. Il faut juste remplacer le fichier LGW.VPS actuel par le nouveau et vous n'aurez pas à réinstaller tout le programme.

Vous pourrez copier le fichier LGW.VPS manuellement (pas recommandé) ou utiliser cette option. En sélection-

nant cette option, la boîte de dialogue de la figure 98 s'affichera.

fig. 98

« Nom du fichier: » indique le chemin d'accès au répertoire dans lequel un nouveau fichier VPS sera cherché. La mise à jour du fichier VPS peut également se faire automatiquement (Chapitre 6.1.2, « Mises à Jour automatiques »). Si vous avez installé AVAST32 du CD-ROM, la zone de texte contiendra le chemin d'accès par défaut « <cd>:\AVS\LGW.VPS » où se trouve l'identification de votre CD-ROM au lieu de <cd>. En cas d'installation par disquettes, le chemin d'accès sera « A:\LGW.VPS ».

Vous pourrez également spécifier le répertoire approprié par le biais de la boîte de dialogue standard pour l'ouverture des fichiers qui s'affichera en appuyant sur « Parcourir ».

« Dernière Mise à Jour : » contient la date et l'heure de la dernière mise à jour du fichier VPS (si applicable).

En cliquant sur « Mise à jour » vous lancez la mise à jour du fichier LGW.VPS. La mise à jour ne s'effectuera que si le fichier LGW.VPS spécifié est plus récent que le fichier actuel.

6.7 Configuration du programme par le biais du « Panneau de configuration »

Vous pouvez configurer tous les modules d'AVAST32 sans exécuter le programme principal en ouvrant le menu « Démarrer », « Paramètres », « Panneau de configuration » (Figure 99).

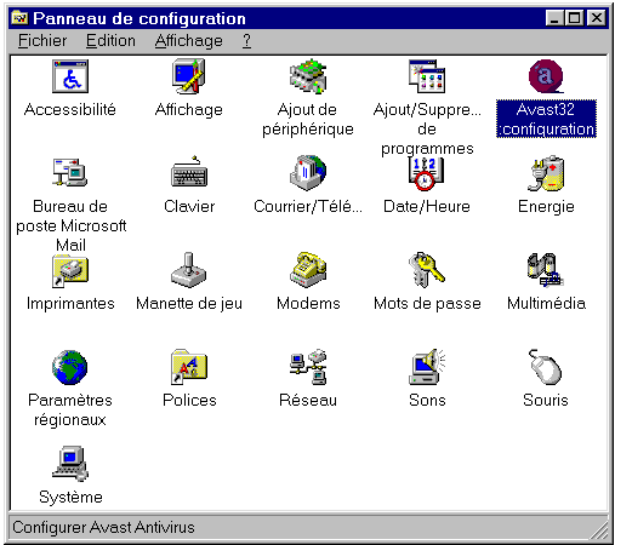

fig. 99

Cliquez sur « Configuration d'Avast32 » dans la fenêtre. Une autre fenêtre avec plusieurs onglets s'affichera. La description de ces onglets suivra.

6.7.1 Onglet « Programmes »

Permet de sélectionner la partie du programme que vous désirez paramétrée (Fig. 100). Après cette sélection, une boite de dialogue sera affichée dans laquelle vous pourrez intervenir sur le paramétrage du module sélectionné.

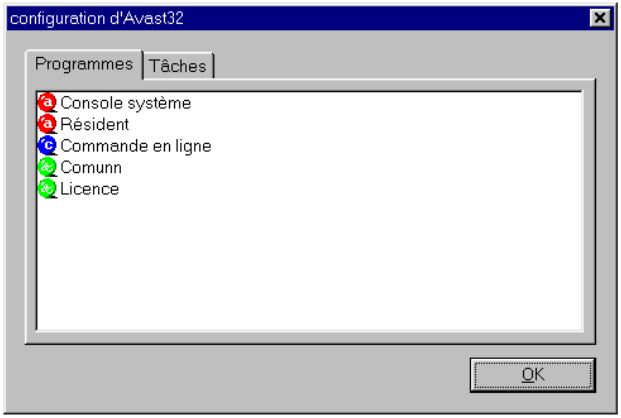

fig. 100

Ce Menu contient les options suivantes :

- « Général » permet le paramétrage d'Avast32. Cette boîte de dialogue est décrite au Chapitre 6.1,
- « Protection Résidente » permet le paramétrage des modules résidents d'AVAST32 (RGW32, voir Chapitre 9). Cette boîte de dialogue est décrite au Chapitre 6.2,
- « Ligne de Commandes » permet le paramétrage du module de recherche en ligne de commandes (LGW32, voir Chapitre 8). Cette boîte de dialogue est décrite au chapitre 6.3,
- Vous pouvez définir un certain nombre de paramètres communs à tous les modules d'AVAST32 dans l'option « Communs ». Pour plus d'informations, voir chapitre 6.5,
- « Licence » permet de mettre à jour votre numéro de licence voir Chapitre 6.4.

6.7.2 Onglet « Tâches »

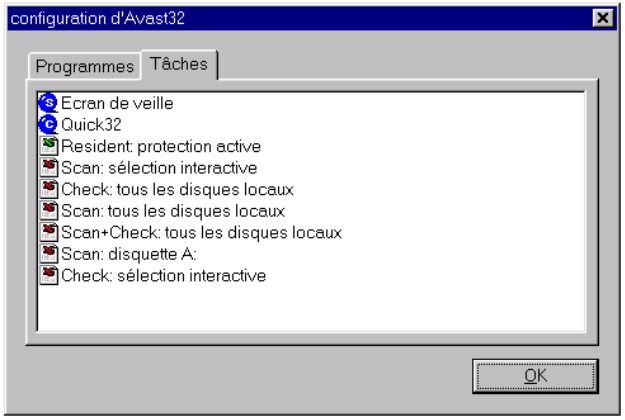

Fig.101

A partir de cette fenêtre, vous pouvez visualisez et/ou modifier les paramètres des tâches existantes. (Fig. 101). La listes des tâches est identique que vous soyez en mode Normal ou Avancé. Si vous double cliquez sur la tâche que vous désirez modifier, la boîte de dialogue qui apparaîtra est décrite au Chapitre 4.

Menu contextuel

Le menu apparaissant après un clic bouton droit est montré en Fig. 102.

fig. 102

- « Nouveau... » sert à la création d'une nouvelle tâche d'AVAST32 sans avoir à redémarrer le programme. (voir chapitre 4),
- En choisissant « Copier », l'utilisateur pourra créer une copie de la tâche. La nouvelle tâche aura les mêmes paramètres que la tâche originale. S'il s'agit d'une tâche partagée et l'utilisateur ne connaît pas le mot de passe valable, la copie sera créée en tant que tâche personnalisée,
- En choisissant « Modifier... » ou en cliquant sur le nom de la tâche, la boîte de dialogue s'ouvrira pour modifier les paramètres de la tâche (voir au-dessus),
- En activant « Supprimer », vous pourrez supprimer une tâche en question dans une liste de tâches. D'abord, il faut confirmer la suppression avec la touche « Oui » dans une boîte de dialogue qui s'affichera (Figure 65).

Si vous effectuez une modification d'une tâche par le biais du « Panneau de configuration » et AVAST32 est en cours, les modifications ne prennent effet qu'au prochain démarrage du programme AVAST32!

6.7.3 Configuration des sons

AVAST32 offre l'option de choisir un son pour les événements qui sera émis quand l'événement a lieu.

Les sons peuvent être choisis dans l'onglet "Sons" dans le Panneau de configuration représenté dans la Figure 55. Etant donné que la configuration des sons s'effectue à l'aide d'un outil système standard, il n'est pas nécessaire de lancer AVAST32.

Cherchez le symbole "Avast32" dans la liste des "Événements" et choisissez l'élément pour lequel vous aimeriez modifier le fichier son.

Vous trouverez une description de la configuration des sons pour certains événements dans le chapitre 4.4.13.

7.Interprétation des résultats

Nous vous recommandons de lire soigneusement ce chapitre et d'y réfléchir. Peut-être ne répétons-nous que des faits déjà connus, mais on ne peut pas faire suffisamment attention. En particulier, les utilisateurs moins expérimentés devraient faire attention à ce chapitre et ne pas l'ignorer.

Vous devez tenir compte du fait qu'il y a une relation directe entre le travail, les connaissances, l'expérience et la sécurité de votre ordinateur. Vous êtes peut-être surpris d'apprendre que peu importe la qualité d'un anti-virus, il ne vous aidera pas si vous ne faites pas continuellement attention à ce que vous faites, en particulier en cas d'une éventuelle infection virale. En même temps, si vous ne vous intéressez pas aux ordinateurs, puisque vous êtes médecin, économiste ou avocat, et que vous n'avez pas assez de temps pour vous occuper de "choses secondaires" telles que les ordinateurs et la sécurité de vos données, nous devons vous décevoir. Vous avez vraiment tort. Et si vous ne voulez même pas respecter notre conseil ni apprendre les principes de base, alors nous vous conseillons de rendre votre anti-virus à votre revendeur qui vous rembourse votre argent. Vous éviterez ainsi beaucoup d'ennuis pour vous et votre entreprise. Pour bien faire votre travail, vous devez connaître la grammaire et l'orthographe. Il en va de même pour le travail avec des ordinateurs. Pour ce travail, quelques notions de base sont aussi nécessaires, si non, vous n'y arriverez pas.

On peut écrire un traitement de texte, une base de données ou un tableur faciles à utiliser et qui ne demande pratiquement aucune connaissance particulière ou qui pourrait vous les apprendre. Les issues de sécurité et la protection antivirale sont tout autre chose.

Nous vous prions de leur consacrer le temps et l'attention nécessaires.

7.1 AVAST32 a trouvé des virus

Cette partie est très simple, même si ce n'est pas tout à fait banal. Si le programme AVAST32 signale qu'il a trouvé un virus, cela ne veut pas encore dire qu'il y a vraiment un virus. Et même s'il y en a un, cela ne veut pas encore dire que votre ordinateur est infecté par des virus. Ce manuel a été écrit sur un ordinateur qui contient un grand nombre de virus différents, mais l'auteur est tout à fait calme, parce que ces virus ne sont pas actifs.

Une description détaillée de ce qu'il faut faire avec un peu d'informations sur le virus trouvé est traité en annexe B dont nous vous conseillons l'étude soignée.

7.2 AVAST32 a détecté des changements dans des fichiers

Cette situation est un peu plus compliquée mais on peut la résoudre. Cependant, seule l'expérience d'un travail régulier avec le programme et des contrôles d'intégrité de vos données vous apporteront les résultats espérés.

L'interprétation des résultats n'est pas facile. Ce n'est pas parce que le programme fournit des informations ou codes compliqués, mais chacun de vous aura à chaque lancement d'un contrôle d'identité des informations différentes , et le traitement de ces informations sera différent pour chaque cas. C'est pourquoi il n'est pas possible de donner des recettes passe partout qui satisferont tous les utilisateurs. Nous ne pouvons que donner quelques conseils généraux, de suggestions et des procédures dont nous conseillons l'application. Les détails et particularités doivent être découverts par vous-même.

7.2.1 Des fichiers nouveaux

Si AVAST32 signale qu'il a trouvé de nouveaux fichiers, cela peut avoir plusieurs raisons. La plus simple est qu'il se réfère vraiment à un fichier nouveau provenant d'une source légale. La solution est toute simple: il faut l'accepter et il sera stocké dans la base de fichiers. Plus difficile sera la question de la source légale. Une vraie source légale est, par exemple, le médium d'installation d'un programme que vous avez ajouté récemment. Ce programme en question aurait pu être installé par un collègue ou par l'administrateur réseau. Si vous avez des bonnes relations de travail, vous pouvez être sûr d'avoir été informé auparavant et vous pouvez décider si ce fichier est en règle ou non.

Il peut aussi s'agir d'un fichier temporaire qui a été créé par un programme pour ses besoins et un tel programme l'utilise actuellement ou „a oublié" de le supprimer. C'est probablement aussi correct, mais un fichier de ce genre peut également créer un virus. La décision peut être très difficile et vous incombe entièrement.

L'utilisation de la corbeille pour supprimer des fichiers aura pour conséquence que les fichiers nouveaux dans le répertoire concerné seront détectés.

Ne soyez pas étonné de voir qu'un fichier nouveau émerge dans un répertoire bien connu comme, par exemple, dans le répertoire du système d'exploitation. Les auteurs de virus aussi connaissent ces répertoires et s'en servent avec succès.

7.2.2 Des fichiers modifiés

Il peut y avoir beaucoup d'explications pour un changement dans un fichier. Le système d'exploitation lui-même mène sa propre vie et se sert de façon intensive des fichiers. Chaque démarrage d'un programme ou édition d'un fichier se termine par une piste détectée et signalée par AVAST32. C'est à vous de décider laquelle des modifications est valable et laquelle ne l'est pas. Par exemple, un changement dans un fichier texte sera à 99 % de votre fait alors qu'une

modification du fichier COMMAND.COM aura été causée par un virus. Veuillez prendre note que rien n'est sûr à 100 % et c'est valable pour tout ce qui concerne les virus. Les autres types de fichiers se placent entre ces deux exemples extrêmes. Il est, par exemple, très difficile de dire d'un document MS WORD (*.doc) pourquoi il a changé. Cela peut avoir été vous, simplement en lisant le contenu, ou „le virus macro" qui a attaqué le document en question.

Cependant, en général, quand un programme exécutable (avec des extensions exe, sys, dll, bin, vxd, scr, ...) est infecté, la modification paraît beaucoup plus suspecte que quand un document ou un fichier de données ont été changés. Mais soyez prudent, il peut y avoir des exceptions.

7.2.3 Fichiers supprimés

Il n'y a pas grand chose pour vous aider. La réparation d'un tel fichier n'est possible qu'à l'aide d'outils spéciaux du système d'exploitation ou des copies de sauvegarde. A part cela, quand avez-vous fait des copies de sauvegarde de vos données? Comptez-vous vraiment sur votre chance?

7.2.4 Cas particuliers

Il existe beaucoup de situations particulières où vous n'arrivez pas à travailler avec un fichier. Dans un tel cas, AVAST32 signalera une erreur pendant le travail (chapitre 5.3.2).

Dans la majorité des cas, vous ne serez pas capable de vérifier le fichier qui est actuellement utilisé par un autre programme. Ce fichier est fermé et le système d'exploitation ne vous permettra pas de l'ouvrir. Ceci s'applique autant au système d'exploitation qui utilise les fichiers qu'aux programmes de travail. Ces derniers ne sont peut-être pas affichés à l'écran à chaque fois. Cependant, s'ils travaillent et utilisent les fichiers, AVAST32 ne sera pas capable de les tester.

Si vous travaillez avec un système d'exploitation qui accepte des aspects de sécurité au niveau des fichiers, et si vous utilisez le système de fichiers qui supporte également cette caractéristique (Windows NT avec NTFS), vous devez avoir suffisamment de droits pour tester des fichiers individuels. Si vos droits ne suffisent pas, le fichier restera non vérifié.

8.Programme LGW32

Ce programme est utilisé pour chercher des virus connus, dont des virus polymorphes et virus macro. Il est l'équivalent de la tâche avec laquelle on testerait uniquement la présence de virus connus dans le programme AVAST32, et il a donc des options de configurations similaires.

Comme AVAST32 et LGW 32 utilisent les services de VPS serveur test, leurs résultats sont entièrement identiques. La seule différence est que le programme LGW32 ne se sert que d'une ligne de commande, contrairement à l'environnement facile à utiliser du programme AVAST32.

La ligne de commande du programme LGW32 se présente ainsi:

```
LGW32 [@<nom de la tâche> | [+ | -]<nom de
zone> [-] [<paramčtre>, ...]]
```

Si vous voulez lancer une tâche créée par AVAST32, tapez "@" suivi du nom de la tâche. Si le nom contient des espaces, il doit être inséré entre guillemets. Sinon, le programme n'effectuera pas la tâche! S'il n'y a pas de nom de tâche, le programme LGW32 vérifiera les zones configurées. Vous pouvez spécifier la façon d'effectuer le contrôle à l'aide de paramètres comme pour les commandes du système d'exploitation.

On peut configurer plusieurs paramètres dans le programme LGW32 programme. Vous trouverez une description détaillée dans le chapitre 6.3.

Si dans la ligne de commande il y a un /, le paramètre suivra direvtement après.

[+ | -]

- ces signes devant un nom de zone signifient que les sous-répertoires doivent être testés aussi. Le signe + activera le test alors que le signe - le désactivera.

[-]

- le signe - après un nom de zone signifie que la zone ne fait pas partie du test. Il est ainsi possible d'informer le programme LGW32 que, par exemple, tout le disque D:, à l'exception du répertoire D:\virus, doit être balayé. C'est la même chose que le point rouge à côté du nom de la zone testée dans AVAST32 (voir chapitre 4.4.5). LGW32 accepte les paramètres suivants:

/?, /H, /HELP

- le programme affiche l'aide. Le menu aide comporte plusieurs pages et on peut passer de l'une à l'autre à l'aide des touches numériques qui signifient toujours le numéro de page à afficher. En appuyant sur une touche quelconque du clavier, vous retournerez dans la ligne de commande.

/A
- mettra en route le scanner des fichiers pour rechercher tous les virus, dont ceux qui n'attaquent pas le type de ce fichier. Par exemple, un fichier COM sera testé pour des virus n'attaquant que des fichiers EXE.

/C[+]
- Tester l'intégralité des fichiers (voir chapitre 4.4.7). Le programme passera tout seul dans ce mode après avoir trouvé un virus. Le signe "+" fera en sorte que les fichiers compressés soient balayés, internement décompressés et balayés ensuite.

/E[A|E|O|<types>]
- indique au programme les fichiers à tester (voir chapitre 4.4.4). La lettre "A" signifie le test de tous les fichiers, "E" des fichiers exécutables et "O" des document OLE. Vous pourrez également spécifier directement les types de fichiers à tester. Leur nombre n'est pas limité et ils doivent être séparés par des virgules. Si le paramètre n'est pas précisé, seuls les fichiers exécutables et les documents OLE seront testés.

/X[types]
- ces types spécifiés ne seront pas testés. On peut ainsi faire tester tous les fichiers sauf les fichiers txt. Ce paramètre est identique au point rouge à côté du nom de type sur la liste des types à tester dans AVAST32 (voir chapitre 4.4.4).

/L[-]
- l'opération activera l'enregistrement. Vous trouverez des informations détaillées dans le chapitre 6.1.1, dans la case "Activer le mode rapport d'Avast32".

/M
- Test mémoire vive, mais aucun autre.

/R[<nom>]
- En effectuant le test, un fichier rapport sera créé (voir chapitre 4.4.10). Si le nom du fichier n'est pas précisé, le compte-rendu sera écrit dans le fichier "LGW32.RPT" dans un répertoire courant valable.

/V[N|I|A]
- Précise sur quels fichiers l'information doit être affichée à l'écran. La lettre "N" désactive le listing, la lettre "I" uniquement le listing des fichiers infectés et "A" le listing de tous les fichiers trouvés.

/U<nom>[,<nom>]
- Le nom de l'ordinateur ou du domaine où le message d'alerte virale doit être envoyé. Au moins un nom doit être saisi après le paramètre.

/Z[+|V]
- enlève automatiquement les virus macro dans les documents OLE. Le signe + fera en sorte que tous les macros soient supprimés si le virus n'a pas été totalement identifié

dans un document. La lettre V assûre la suppression automatique de tous les macros du document infecté. Si aucun signe n'est prévu, seules la macro contenant un virus sera enlevée du document OLE.

Quand le programme LGW32 a fini, il renvoie un code au système d'exploitation. Ce code pourra être testé plus tard par le programme qui l'a lancé ou par la ligne de commande avec IF ERRORLEVEL. Le code retour du programme LGW32 ne peut comporter que les valeurs:

0	- programme a fini normalement, pas de virus trouvé,
1	- programme a trouvé un virus,
10	- la durée de la version de démonstration du programme a expiré,
11	- programme ne peut être exécuté, peut-être mauvaise installation,
255	- erreur sérieuse à l'exécution du programme.

9.Programme RGW32

Le programme s'occupe de tous les test résidents. Si, par exemple, vous lancez une tâche résidente d'AVAST32, uniquement RGW32 sera exécuté. Sa présence en mémoire sera indiquée par une icône à droite de la barre des tâches (fig. 103). La fenêtre s'affiche avec un double-clic avec le bouton gauche de la souris sur cette icône.

Il est possible de ne pas afficher l'icône de RWG32– voir Chapitre 6.2, "Cacher l'icône du programme". Pour la plupart des utilisateurs, nous recommandons de laisser l'icône visible.

fig. 103

Dans cette fenêtre (Fig. 104), vous pouvez sortir de RGW32 et mettre fin à la tâche en cours. Cette fenêtre contient une arborescence de contrôle et deux groupes principaux : « Resident Guard » et « Behavior Blocker ». En ouvrant un groupe, vous avez le détail des activités en cours.

Vous pourrez prévoir plusieurs paramètres dans le programme RGW32 programme. Des renseignements détaillés se trouvent dans le chapitre 6.2.

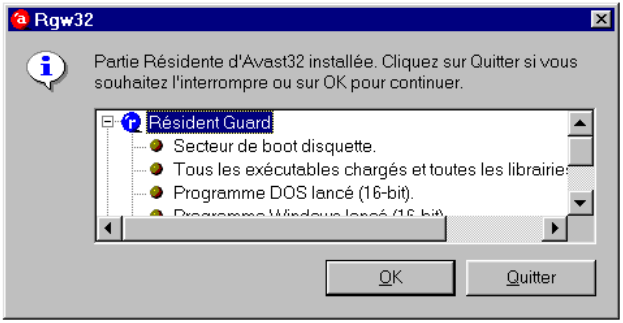

fig. 104

La ligne de commande du programme RGW32 est la suivante:

```
RGW32 <nom de tâche> | /E
```

Le paramètre <nom> spécifie la tâche résidente à exécuter. Si le paramètre n'est pas précisé, ou si aucune tâche de ce paramètre n'existe, le programme affichera un message d'erreur. Seule une tâche résidente pourra être exécutée sur le même poste. Si une autre tâche résidente est lancée, la première sera annulée.

Si la tâche contient également des activités non-résidentes, elles seront ignorées ainsi que leur configuration - seuls les test résidents seront effectués.

Si la ligne de commande contient le commutateur ”/E” à la place d’un nom de tâche, la tâche résidente sera interrompue. Ce commutateur est particulièrement utile pour arrêter RGW32 depuis un fichier batch.

RGW32 n’envoie pas de code retour.

RGW32 peut afficher plusieurs autres dialogues pendant son opération. Ces dialogues informent l’utilisateur d’une opération dangereuse à l’intérieur d’un fichier, de la découverte d’un virus dans le secteur de démarrage ou de la disquette insérée, ou d’un virus dans le programme en cours ou dans un document OLE ouvert avec une fonction OLE. La description se trouve dans les chapitres suivants.

9.1 Signaler des opérations dangereuses

Comme nous l’avons déjà dit, RGW32 s’occupe de tous les tests résidents pouvant être effectués par les tâches. Behaviour Blocker fait aussi partie de ces tests. Si une tâche avec Behaviour Blocker est lancée, toutes les opérations du système d’exploitation seront surveillées (chapitre 4.4.15).

A la première tentative d’une opération suspecte, RGW32 affichera un message d’alerte (fig. 105) et retardera l’opération en question jusqu’à ce que l’utilisateur signale la marche à suivre. Le message d’alerte contient une zone texte avec le nom du fichier avec lequel l’opération suspecte devait être effectuée. En outre, la fenêtre affiche trois boutons:

fig. 105

OK

L’opération avec le fichier sera exécutée. D’autres opérations suspectes seront également signalées.

OK & IGNORER

L’opération sera autorisée et RGW32 n’avertira pas l’utilisateur d’aucune opération jusqu’à l’arrêt et redémarrage.

ANNULER

Indiquera au programme de s’abstenir d’exécuter cette opération en question. En cliquant dessus, le programme n’autorise pas l’opération et informera l’utilisateur de la prochaine tentative d’opération dangereuse avec le fichier en question.

9.2 Détection de virus au lancement d'un programme ou à l'ouverture d'un document

RGW32 peut également balayer les programmes en cours, des documents OLE ouverts avec une fonction OLE, ainsi que les secteurs de démarrage des disquettes insérées. Les tests précités seront effectués par RGW32 si vous les avez activés dans l'onglet "Test" (chapitre 4.4.2).

fig. 106

Si vous insérez une disquette dans le lecteur, le programme testera si le secteur de démarrage contient un virus. Dans l'affirmative, un message d'alerte sera affiché (fig. 106). Vous pourrez continuer de travailler avec la disquette parce que, pour être actif, un virus doit d'abord avoir été exécuté. En cas de virus du secteur de démarrage, ceci n'arrive que lors du démarrage du système. Le message d'alerte doit vous mettre en garde contre un danger potentiel.

Le message d'alerte à la fig. 106 s'affichera aussi si un virus connu a été détecté dans un programme exécutable ou si l'utilisateur a essayé d'ouvrir un document OLE contenant un virus. Afin que RGW32 puisse afficher le message, une tâche contenant le test protecteur pour exécutables et documents OLE doit évidemment être lancée et le test des fichiers appropriés doit être sélectionné.

Si un virus macro est détecté, la fenêtre du message d'alerte contient un bouton "Réparer" (Fig. 106), qui permet d'afficher une boite de dialogue (Fig. 74) à partir de laquelle vous pouvez désinfecter le document.

En cliquant sur OK, vous pouvez poursuivre votre travail.

9.3 Avertissement sur la présence de disquette pendant l'arrêt du système.

Si RGW32 est actif, il vérifiera si une disquette n'a pas été oubliée avant l'arrêt du système. C'est en effet le principal vecteur d'infection des ordinateurs. Si la présence d'une disquette est détectée, un message d'erreur sera affiché et l'arrêt du système interrompu. Dans le cas contraire, l'arrêt s'effectuera normalement.

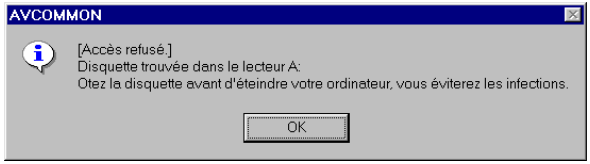

fig. 107

Le test de présence d'une disquette avant l'arrêt peut être désactivé – voir chapitre 6.2, bouton « Ne pas tester la présence de disquette avant l'arrêt ».

10.Programme QUICK32

Le programme QUICK32 est utilisé par Avast32, LGW32, et à travers l'explorateur, pour rechercher la présence d'un virus connu dans un fichier.

Il est utilisé lors des vérifications lancées via l'explorateur (Fig. 23). Dans le cadre d'une autre utilisation il est recommandé d'utiliser AVAST32 ou LGW32.

QUICK32, par défaut, effectue sa recherche virale dans tous les types de fichiers. Les fichiers compressés, sont d'abord vérifiés dans leur forme compressée, puis décompressés et vérifiés à nouveau.

La ligne de commande de QUICK32 est la suivante:

```
QUICK32 <nom>
```

Le paramètre <Nom> détermine le nom du répertoire ou du fichier à vérifier, chemin d'accès inclut. Si un répertoire est sélectionné, l'ensemble des sous-répertoires seront également vérifiés.

fig. 108

Le programme informe l'utilisateur de son avancement par le biais d'une petite icône à droite de la barre des tâches (fig. 108). Effectuez un double-clic dessus et vous ouvrez une fenêtre avec le nom du fichier testé à ce moment (fig. 109). Si vous souhaitez fermer le programme avant, cliquez sur "Quitter". La fenêtre sera fermée à l'aide du bouton OK.

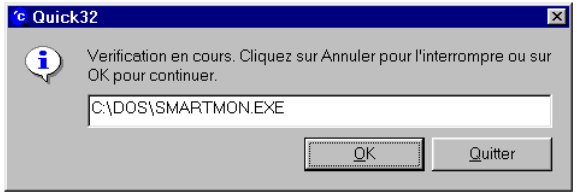

fig. 109

Si le programme QUICK32 a trouvé un virus, il en avertira l'utilisateur par le biais d'un message d'alerte (fig. 24). Cependant, le programme terminera après avoir trouvé et annoncé le premier virus, c'est pourquoi l'utilisateur ne sera averti que du premier virus, si jamais le répertoire testé contient d'autres fichiers infectés.

QUICK32 n'envoie pas de code retour.

10.1 Paramètrage du programme QUICK32

Il est possible de paramétrer QUICK32 à partir de l'icône Avast32 du panneau de configuration (Chapitre 6.7).

L'onglet "Tâches" contient une tâche "Quick32", que vous pouvez paraméter en cliquant 2 fois dessus ou via le choix "Modifier" après un clic sur le bouton droit.

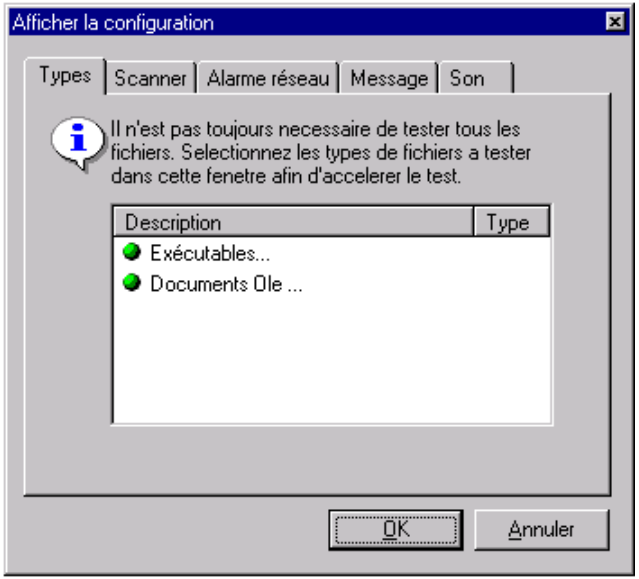

fig. 110

L'écran de paramètrage de QUICK32 contient les onglets suivants (fig. 110):

- "Types" permet de définir les types de fichiers à vérifier (voir Chapitre 4.4.4),
- "Scanner" contient les options de paramétrage de la tâche. Les choix, non disponibles avec Quick32 sont en grisés. Ces options sont décrites en détail dans le chapitre 4.4.7,
- "Message" contient le message à afficher en cas de détection de virus (voir Chapitre 4.4.12),
- "Sound" contient le fichier son à utiliser en cas de détection de virus (voir chapitre 4.4.13).

11.Programme WARN32

L'objectif de WARN32 est d'informer l'utilisateur du fait qu'un virus a été détecté sur son ordinateur. Il est automatiquement lancé après le démarrage du système d'exploitation si l'affichage du message d'alerte est activée (voir chapitre 6.5.1, case "Montrer message d'alerte après connexion").

La ligne de commande est la suivante:

```
WARN32
```

Comme vous le voyez, le programme n'a pas besoin de paramètres pour être lancé et vu la nature de son activité, il n'envoie pas non plus de code retour.

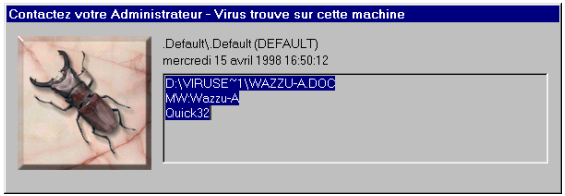

fig. 111

Au démarrage, le programme examine le registre du système d'exploitation, si un virus a été détecté sur ce poste (cette information pour WARN32 dans le registre est prévue par AVAST32, LGW32 et QUICK32). Si un virus a été trouvé, le programme affichera un message d'alerte (fig. 111) qui passera sur le poste de travail. Le message informera l'utilisateur du dernier fichier infecté trouvé, du nom du virus qui a infecté le fichier et du nom de la tâche qui l'a détectée.

Si aucun virus n'a été trouvé, le programme se termine sans envoyer aucun message. L'utilisateur peut ne pas se rendre compte qu'il avait commencé.

Si le programme a affiché un message d'alerte, il est difficile de l'arrêter. C'est pourquoi un utilisateur moins expérimenté ne devrait pas lancer WARN32 (il n'y a, d'ailleurs, aucune raison pour le faire).

Si un message d'alerte apparaît après la connexion, il faudrait en avertir immédiatement l'administrateur réseau ou toute autre responsable.

La suppression du message de WARN32 du poste de travail ne suffit pas, il faut aussi faire en sorte que le message ne soit pas rediffusé au prochain démarrage du système d'exploitation!

12.Ecran de veille

Le module "Screen Saver" d'Avast32 permet la vérification d'une machine durant ses périodes d'inactivité. Il peut être configuré aux besoins de chaque utilisateur sur le même principe que les tâches Avast32. L'utilisateur définira lui-même quel écran de veille il désire utiliser.

fig. 112

L'utilisateur est informé de la progression de la vérification grâce à une fenêtre affichée par dessus l'écran de veille (fig. 112). Dans le cas d'une détection de virus, le test est interrompu et un message d'alerte est affiché.

La fenêtre peut être de différentes couleurs. Si la palette définie est inférieure à 65536 couleurs, le fond de fen^tre est noir et le texte est blanc. Si la palette est supérieure à 65536, le fond de fenêtre est bleu ou rouge (en cas de détection de virus) et le texte est blanc.

Screen Saver s'interrompra automatiquement si le clavier ou la souris sont utilisés. Toutefois, si un virus a été découvert, un message d'alerte sera à nouveau affiché après l'interruption de l'écran de veille.

L'installation du module Screen Saver est décrite dans le chapitre Chapter 2.8.

12.1 Paramétrage de Screen saver

Il est possible de paramétrer Screen saver à partir de l'icône Avast32 du panneau de configuration (Chapitre 6.7).

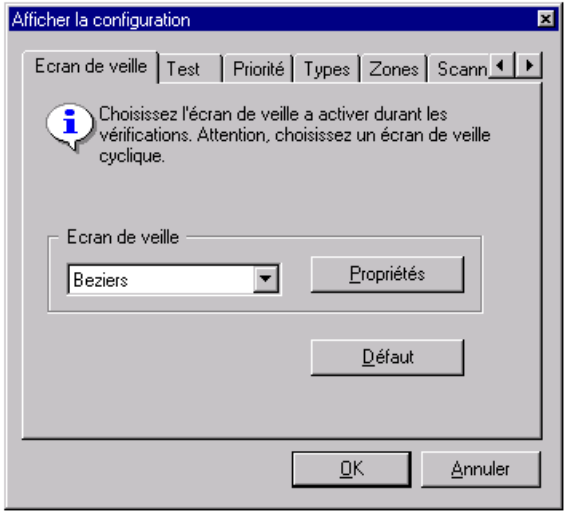

fig. 113

L'onglet "Tâches" contient une tâche "Screen Saver", que vous pouvez paraméter en cliquant 2 fois dessus ou via le choix "Modifier..." après un clic sur le bouton droit.

L'écran de paramètrage de screen saver (Fig. 113) contient les onglets suivantes :

- "Ecran de veille" contient le options de paramétrage de l'écran de veille – voir chapitre 12.1.1,
- "Test" permet de définir ce que doit faire Screen Saver (voir Chapitre 12.1.2).

Les onglets suivants sont visibles uniquement si le choix "Vérification antivirale" de l'onglet "Test" a été sélectionné (voir Chapitre 12.1.2).

- "Priorité" détermine la priorité pour cette instance (voir Chapitre 4.4.3). Une priorité Haute est recommandée pour Screen Saver.
- "Types" permet de définir les types de fichiers à vérifier (voir Chapitre 4.4.4),
- "Zones" permet de définir les zones à vérifier (voir chapitre 4.4.5)
- "Scanner" contient les options de paramétrage de la tâche. Les choix, non disponibles avec Screen Saver sont en grisés. Ces options sont décrites en détail dans le chapitre 4.4.7,
- "Alertes Réseau" permet de définir les destinataires des messages d'alertes virale (voir chapitre 4.4.11),
- "Son" contient le fichier son à utiliser en cas de détection de virus (voir chapitre 4.4.13).

12.1.1 Onglet « Ecran de veille »

Cet écran permet le paramètrage du module Screen Saver (Fig. 113).

L'onglet "Ecran de veille" permet de sélectionner l'écran de veille à utiliser. Il peut être sélectionné dans une liste qui apparaîtra après un clic sur la flèche située à sa droite. Si aucun écran n'est sélectionné ou s'il n'est pas disponible, le programme essaiera d'en sélectionner un automatiquement.

Le bouton "Propriétés" permet de paramétrer les options propres à l'écran de veille choisit.

Le bouton "Défaut" réinitialise les paramètres par défaut.

12.1.2 Onglet « Test »

"Test" permet de définir quel écran de veille sera utilisé et de le paramétrer (Fig. 114).

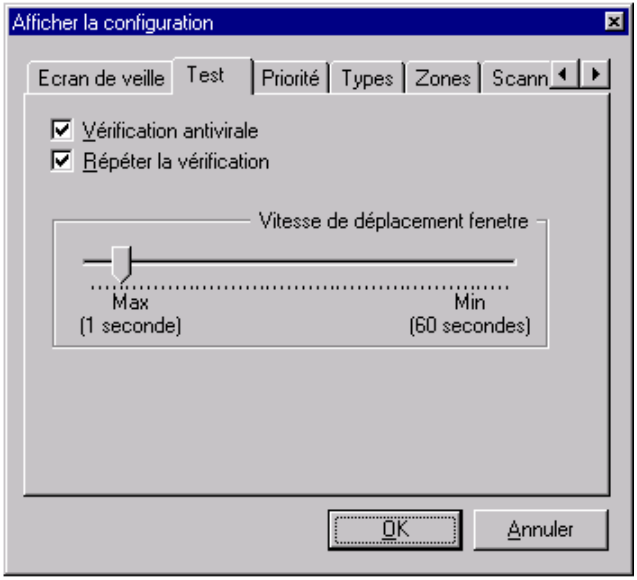

Fig. 114

L'option "Vérification antivirale" spécifie à Screen Saver d'effectuer une recherche virale à chaque mise en veille. Cette option est activée par défaut.

L'option "Répeter recherche" signifie à Screen Saver qu'après vérification des zones et fichiers spécifiés la tâche sera automatiquement redémarrée, jusqu'à interruption par l'utilisateur. Cette option est activée par défaut.

L'option "Vitesse de déplacement fenêtre" définit la fréquence de rotation, dans l'écran, de la fenêtre de vérification de Screen Saver. La valeur par défaut est de 5 secondes.

A.Routines des virus

Les renseignements dans cette annexe s'adressent en particulier aux utilisateurs souhaitant optimiser le travail avec le système utilisant AVAST32. Ce chapitre traite les principes de base des fonctions du programme, dont des descriptions résumées de certaines librairies. Des utilisateurs moins expérimentés n'auront probablement pas d'utilité pour les informations fournies ci-après.

A.1 Principes de base

Comme AVAST32 contient plusieurs modules recherchant des virus, le contrôle en soi est prévu dans une partie indépendante appelée à partir de ces modules. C'est ainsi qu'on évite de répéter le code et les données s'y rapportant, qui provoquerait une durée d'exécution plus longue et une plus grande occupation de mémoire sur le disque dur et de RAM. Tous les programmes devant savoir s'il y a un virus dans le système utilisent la même procédure et les mêmes librairies réduisant substantiellement les besoins en mémoire vive.

L'utilisation des données est également optimisée. Comme nous l'avons déjà souligné, tous les données nécessaires pour la recherche des virus se trouvent dans le fichier LGW.VPS. Ce fichier est déjà suffisamment grand, et la mauvaise nouvelle pour les utilisateurs serait qu'il est amené à s'alourdir en respect du nombre croissant de virus. Si vous pouviez l'observer, vous verriez que ses contenus ne signifient pas trop à première vue, mais sont indispensables pour le fonctionnement du programme. La plupart des informations dans ce fichier sont statiques. Elles peuvent être utilisées par beaucoup de programmes sans danger de réécrire des données.

A.2 Librairies utilisées

Plusieurs librairies servent directement à l'ouverture des fonctions antivirales. La première est AvMain.DLL qui est une librairie normale, dynamique, déjà bien connue depuis la version Windows 3.x. Mises à part d'autres applications, cette librairie est utilisée pour l'initialisation, „le nettoyage“ et la généralisation des ouvertures des services anti-virus par plusieurs types de programmes. En général, on peut dire qu'il s'agit d'une enveloppe de la propre mise en oeuvre.

La recherche des virus se passe dans la librairie Vps32s.DLL. Elle sert comme serveur „InProc“ travaillant d'après le modèle „Appartement“. Elle représente le serveur COM lié à l'espace adresse du programme qui l'initialise. Si l'information précitée vous paraît être du chinois, cela ne fait rien et vous pouvez tranquillement ignorer ce chapitre.

Pour son propre travail, cette librairie utilise toujours plusieurs librairies auxiliaires (Vps32a.DLL, Vps32e.DLL),

mais celles-ci effectuent des tâches particulières qui ne sont pas intéressantes pour le contenu de ce chapitre.

L'implémentation utilisée a une caractéristique qui peut vous paraître intéressante, et peut-être, aimeriez-vous en profiter davantage. Il est vrai que le serveur COM présente une interface lisible et compréhensible, d'un point de vue externe. A plusieurs reprises, des utilisateurs ont été tentés de s'en servir d'une autre façon que celle autorisée par le programme. Nous aimerions vous mettre en garde contre cette tentation, et ce pour deux raisons: d'abord, un tel comportement est contre la loi, et si nous en avons connaissance, nous sommes obligés d'en informer nos avocats. L'autre raison beaucoup plus importante est que ces fonctions ne sont pas officiellement documentées et leur usage peut vraiment causer des dommages. Si vous faites confiance à l'implémentation actuelle, vous pourrez être désagréablement surpris à l'avenir.

A.3 Optimisation

L'optimisation des routines des virus résulte directement de leur mise en oeuvre. Chaque programme utilisant ces fonctions doit avoir accès à toutes les données du fichier LGW.VPS. Ce fichier doit être contrôlé, lu et analysé avant chaque utilisation, ce qui dure un certain temps. C'est pourquoi les opérations précitées ne sont effectuées que quand le fichier LGW.VPS n'est plus utilisé.

Si un fichier de données est utilisé par d'autres programmes, le démarrage d'un autre programme du pack AVAST32 sera plus rapide. Pour cette raison, nous fournissons également le programme Vps32.EXE, dont la seule fonction est de garder en mémoire le fichier des virus et d'accélérer son utilisation. Vous apprécierez cette propriété en particulier en case de faire vérifier vos fichiers à l'aide du menu local de l'Assistant Explorateur quand l'initialisation du fichier VPS pour chaque fichier peut être frustrant.

L'autre aspect de cette accélération est moins de RAM, même quand LGW.VPS n'est pas appelée par aucune application.

B.Que faire en cas de virus

Si un module du pack AVAST32 annonce la présence d'un virus, cela ne veut pas toujours dire que le fichier est vraiment infecté. Ce qu'il faut faire dans ce cas là sera décrit dans les chapitres suivants. Cependant, les opérations décrites ci-après ne devraient être exécutées que par des utilisateurs ayant de l'expérience avec les systèmes d'exploitation Windows 95 et NT et connaissant les résultats des opérations individuelles.

B.1 Qu'est-ce qu'un « faux message positif »?

Avant de vous adonner à la panique et de supprimer les fichiers infectés, faites appel au service anti-virus ou demandez un congé de longue durée. Vous devez découvrir si le fichier est réellement infecté ou si le message positif est faux. De tels faux messages peuvent avoir un certain nombre de raisons et l'alerte peut avoir les causes suivantes :

- utilisation de deux scanners à la fois (chapitre B.1.1),
- immunisation des fichiers (chapitre B.1.2),
- programme malveillant (chapitre B.1.3),
- défaut technique, de l'équipement du programme ou causé par l'utilisateur (chapitre B.1.4),
- principes d'exploitation sous Windows (chapitre B.1.5).

AVAST32 a été conçu de façon à minimiser les faux messages d'alerte virale. Les tests réguliers incluent environ 4 Go (4096 Mo) de fichiers d'origine et de contenu divers. Cependant, malgré ces tests complexes, il peut arriver qu'un module du pack AVAST32 affiche un faux message d'alerte. Si tel est le cas, veuillez nous contacter. Vous nous aiderez à améliorer notre produit et vous vous sentirez plus en sécurité.

Si vous ne comprenez pas les explications dans ce chapitre, ne vous faites pas de soucis. On n'est pas né avec des connaissances en informatique. Nous vous demandons de contacter de vrais experts en cas d'attaque virale.

B.1.1 Alerte due à l'utilisation de deux scanners en même temps

Si vous lancez deux scanners en même temps ou immédiatement l'un après l'autre, il peut arriver qu'un des deux affichera la présence d'un virus en mémoire. Il y a une simple explication. Chaque scanner a besoin de stocker, au moins pendant un petit moment, les informations non codées sur les virus. Si, au même moment, cette mémoire est testée par un autre scanner, ou si cette mémoire est transférée dans la mémoire virtuelle, et utilisée plus tard sans être

vidée, il peut arriver que cette information provoque un faux message d'alerte.

La situation est plus claire quand ces scanners sont conçus de façon „impropre", c'est-à-dire qu'ils ne vident pas leur mémoire. Dans ce cas, il est fort probable que vous découvriez plusieurs (c'est-à-dire 5 ou plus) types différents de virus. Dans ce cas, la situation est claire, il s'agit d'un faux message d'alerte.

La situation est pire quand les scanners sont écrits de façon „propre" et qu'ils nettoient leur mémoire après. Il peut également arriver que vous détectez un virus en mémoire.

Comment savoir s'il s'agit d'un faux message d'alerte? C'est relativement facile, mais prend beaucoup de temps. Terminez votre travail avec toutes les applications, fermez le système d'exploitation et éteignez votre poste. Rallumez et démarrez le système d'exploitation. Lancez le scanner qui a annoncé la présence d'un virus en mémoire. S'il ne répète pas cette annonce, essayez de refaire le travail (exécution de programmes) que vous faisiez avant de démarrer les scanners et, après un moment, relancez le test antiviral. Si, dans ce cas, aucun virus n'est trouvé en mémoire, il ,agissait d'un faux message d'alerte.

AVAST32 nettoie soigneusement la mémoire utilisée et, en plus, ne garde les informations et échantillons des virus que sous forme codée. Il déchiffre l'information sur un virus uniquement au moment de tester et supprime ces informations après. Ceci veut dire qu'à aucun moment ne peut y avoir plus qu'un exemplaire décodé de virus en mémoire.

B.1.2 Alerte provoquée par l'immunisation des fichiers

Il y a des moyens anti-virus qui offrent et travaillent avec une fonction que nous appelons "l'immunisation de fichiers" ou avec une fonction prévoyant d'ajouter un checksum au fichier testé. Pendant le prochain test, les utilitaires précités vont simplement comparer l'information ajoutée aux conditions actuelles et peuvent déclarer, sur la base de ce résultat, la suspicion qu'un fichier est infecté par un virus. Ce processus est très rapide et très simple à mettre en oeuvre.

Mais ce processus relativement simple et rapide entraîne quelques problèmes graves. Imaginez-vous qu'il y a deux produits travaillant ainsi et qui sont utilisés pour tester un seul fichier. Leur exécution en alternance va provoquer des interférences entre eux et les deux produits annonceront que le fichier a été modifié.

Un autre problème constitue le fait que le seul test d'un fichier le changera physiquement. Sans parler des problèmes de copyright pour les fichiers originaux, nous nous trouvons face à la question si vous pouvez être sûr que le programme changé continuera de fonctionner de la même façon que son original. C'est fort probable, mais il y a d'autres programmes qui se vérifient eux-mêmes avant démarrage, et ces programmes ne fonctionneront pas en cas de modification. En outre, ce qui précède ne s'applique qu'aux exécutables. Le moindre changement dans les fi-

chiers de données entraînera un risque d'échec du programme utilisant ces fichiers.

Si vous êtes persuadé que des virus ne peuvent pas se propager dans des fichiers de données, vous aviez raison jusqu'à présent. Actuellement, nous sommes face à un groupe spécial de virus ("virus macro") qui se propagent exclusivement à l'aide des fichiers données.

AVAST32 ne modifie aucun fichier testé d'aucune façon. Pour des raisons de sécurité, il ne fait qu'ouvrir le fichier à tester en lecture seule pour ne pas l'endommager, même accidentellement. Si des modules d'AVAST32 sauvegardent des information sur des fichiers, ils les stockent dans un fichier indépendant.

Il n'y a qu'un seul cas, c'est-à-dire la suppression des virus trouvés, que le programme écrit dans les fichiers, mais même dans ce cas là, c'est fait avec une copie du fichier et uniquement après exécution avec succès, le fichier corrigé est écrit avec son nom d'origine.

B.1.3 Alerte due aux programmes malveillants

S'il vous arrive que votre ordinateur se comporte de façon bizarre, voire suspecte, il ne doit pas forcément s'agir d'un virus. Vous pouvez avoir affaire à un programme malveillant qui a été installé sur votre poste par votre collègue ou qui vous avait été présenté avec des fausses informations sur son but. Un exemple peut être l'installation d'images bleues au démarrage de l'ordinateur. Des gens de faible caractère ou des utilisateurs moins expérimentés pourront avoir des problèmes pour remettre l'ordinateur en état initial et pourront considérer que la simple "blague" est due à un virus particulièrement dangereux.

Cependant, cela peut ne pas être vrai. Et comment distinguer une blague d'un vrai virus? C'est difficile puisqu'il est impossible de préciser la limite exacte entre ces deux groupes. Il faudrait adapter son analyse à la situation particulière. Par exemple, des virus ne peuvent pas se permettre des présentations de telles images (en particulier, en couleur) qui seraient trop longues. La plus grande différence, mais qui n'est pas facile à reconnaître, est que contrairement aux blagues, des virus se reproduisent.

B.1.4 Alerte due à un défaut technique, de l'équipement du programme ou par l'utilisateur

Des problèmes techniques, de programmes installés ou avec d'autres équipements, peuvent être facilement pris pour une infection virale. Par exemple, des problèmes fréquents de ce genre sont des problèmes d'impression ou avec le disque dur. Pourtant, il y a peu de virus capables de causer de tels problèmes.

Par contre, pour qualifier le message d'erreur "Erreur de parité mémoire", il faudrait vraiment un expert, ce message pouvant être dû à une micropuce défectueuse dans la mémoire mais aussi à un virus qui l'affiche sur écran. Seule l'expérience peut vous aider dans un tel cas.

B.1.5 Alerte due aux fonctions de Windows

Windows gère la mémoire de façon à vous permettre d'utiliser plus de mémoire que vous n'ayez en réalité. Cependant, ceci peut provoquer de faux messages d'alerte parce que les signatures des virus présentes dans la mémoire "physique" peuvent aussi apparaître sur le disque dans la mémoire "virtuelle". Il peut donc arriver que vous trouvez un virus par exemple dans le fichier WIN386.SWP (sous Windows NT - PAGEFILE.SYS). Il peut arriver relativement souvent que l'on trouve le virus "normal" dans le ficher .DOC. Ce faux message d'alerte peut être évité en ouvrant le document sous WORD, en choisissant "sauvegarder sous..." avec le même nom. Attention! Il faut d'abord savoir qu'il ne s'agit pas d'un virus macro.

B.2 Qu'est-ce donc qu'un virus!!!

La première question qui vous passera probablement par la tête est "Pourquoi moi?!". Ce n'est pas quelque chose de bizarre, une grande majorité d'utilisateurs ont déjà rencontré un virus. le danger ne menace pas uniquement "les fanas d'informatique". Si vous avez au moins un peu de chance, l'infection ne doit pas causer un dommage sérieux. Par contre, la chance a tendance à aider plus les personnes mieux préparées!!

B.2.1 La première chose à faire

La chose la plus importante à faire est ne pas céder à la panique. Le dommage éventuellement causé par le virus n'est rien en comparaison à ce que vous pourriez faire par une action irréfléchie.

C'est la panique qui et votre ennemi! Si vous êtes le genre de personne à s'énerver facilement, quittez votre ordinateur en cas de virus et prenez un café. Ensuite, appelez votre administrateur réseau. Vous verrez que tout n'est pas si grave.

Si vous voulez faire quelque chose sans l'aide de personne, terminez tranquillement l'exécution de tous les programmes en cours et sauvegardez vos données. Il ne se passera rien, vous pourrez finir ce qui doit être fini. Vous avez le temps, seul un nombre restreint de virus sont dépendants du temps d'activité. Essayez d'éviter d'exécuter d'autres programmes (si possible). En aucun cas, éteignez votre poste. Les conséquences pour vos données sur le disque dur seraient catastrophiques.

L'arrêt de l'ordinateur sans avoir terminé le travail du système d'exploitation ("Arrêt") et une très mauvaise habitude qui aura certainement des conséquences déplorables pour vous.

Si vous avez réussi à finir le travail du système d'exploitation, vous pouvez éteindre l'ordinateur. Reposez-vous

puisque vous devez réfléchir à ce qu'il faut faire maintenant.

Il faut prendre son temps. Non seulement vous devez enlever le virus mais aussi vous devez découvrir la source exacte (ou, au moins, probable) de l'infection (probablement votre ami avec la dernière version d'un jeu très connu). Une question très importante est depuis combien de temps vous pouvez avoir ce virus dans votre ordinateur.

Soyez plutôt pessimiste, cela se paie. La sous-estimation de la durée d'infection est la première étape vers une infection à répétition!!!

Il est également très important de vous rappeler si vous avez passé ce virus à d'autres postes. Que vous utilisiez un ordinateur d'entreprise et que votre société a envoyé un millier de disquettes infectées ou que vous n'ayez donné qu'une dernière version d'un nouveau jeu à votre ami, dans les deux cas la meilleure chose à faire est d'informer ceux immédiatement concernés par une infection potentielle. Faites-le tout de suite!!

La honte due à la propagation d'une infection virale est plus facile à supporter que si vous avertissez vous-même du danger de l'infection. Dans le cas d'une entreprise, vous pourriez perdre totalement la confiance de vos clients s'ils découvraient qu'il y a un virus et que vous étiez au courant sans les avertir (peut-être pouvez vous vous le permettre).

Une des questions les plus importantes est si vous avez vraiment sauvegardé toutes les données importantes de votre ordinateur infecté.

Chaque éradication de virus entraîne le risque d'une perte totale de données sur vos disques durs, même au cas où le nettoyage est fait par un expert formé ayant beaucoup d'expérience.

Nous sommes certains que vous savez qu'il faut sauvegarder les données. Mais soyez sincère, quand est-ce que vous avez fait un Back-up pour la dernière fois? Et si vus le faites à intervalles réguliers, avez-vous déjà essayé de restaurer les données? Et si vous remplissez les deux conditions, gardez-vous une copie de sauvegarde de votre programme Back-up ailleurs que sur le poste infecte? Qu'est-ce que vous allez faire si l'ordinateur n'est plus accessible?

Donc, si vous n'avez pas de copie de sauvegarde actuelle, il est grand temps d'en faire une. Il n'y a rien d'autre à faire et vous devez vous rendre compte que les données ainsi sauvegardées peuvent contenir le virus et que chaque amorçage futur peut augmenter le niveau d'infection du système. Mais vous ne pouvez rien faire d'autre. Une copie de sauvegarde est vraiment nécessaire, aussi au cas où le prochain travail serait fait par quelqu'un d'autre (en particulier, quelqu'un qui n'est pas responsable de vos données).

Veuillez trouver ci-après un résumé de ce qu'il faut faire en cas d'une infection virale:

- terminer le travail sans se dépêcher démesurément, mais sans tarder,
- découvrir le plus d'informations possibles sur le virus,
- terminer l'exécution du système d'exploitation,
- éteindre l'ordinateur,

- réfléchir quant à la source et la durée probable d'infection,
- avertir tous ceux auxquels vous avez passé des données ou des disquettes infectées,
- si nécessaire, faire une copie de sauvegarde des données. Ne rien laisser au hasard!!

Si vous avez fait ces démarches, vous pourrez continuer à travailler. Maintenant, évaluez de façon critique vos compétences et vos expériences en matière d'informatique. Si vous ne connaissez pas suffisamment les ordinateurs, nous vous déconseillons d'enlever le virus par vous-même. Par contre, si vous comprenez les explications qui vont suivre, vous pourrez essayer sans une aide particulière. Comment? C'est ce que nous allons essayer d'expliquer. Soyez prudent et évitez les soi-disant experts. Si vous les entendez prononcer l'expression "format de bas niveau", sauvez-vous. Ils pourraient bel et bien causer des dommages à vous et à vos données.

Si vous travaillez dans une grande entreprise, contactez d'abord votre administrateur réseau ou le responsable du service informatique.

B.3 Quel type de virus a infecté mon ordinateur?

Il faut connaître le type de virus présent dans votre ordinateur. Les étapes suivantes sont directement liées à ce fait et, en même temps, certains aspects de la détermination du type de virus peuvent changer la façon comment l'enlever.

Si les explications qui suivent vont paraître un peu non-professionnelles à certains d'entre vous, c'est dû à notre effort de garder une certaine lisibilité de ce chapitre également pour des utilisateurs qui ne rencontrent pas souvent des virus.

Les types principaux de virus sont:

- virus multi-mode,
- virus résident en mémoire,
- virus de fichiers,
- virus de secteur de démarrage,
- virus macro.

Si vous rencontrez un virus rare qui change ou modifie des fichiers de données autres que les documents OLE, vous n'avez pas eu de chance, de telles données n'étant pas très fiables ou même utilisables. En même temps, il n'y a pas de moyens comment restaurer des fichiers de données détruits (sauf, peut-être, par la sauvegarde de statistiques).

Dans le chapitre suivant, nous présupposons que vous travaillez avec le système d'exploitation Microsoft Windows 95 ou Microsoft Windows NT. Le nettoyage de virus sous MS-DOS peut différer des procédures décrites ci-après.

B.3.1 Virus multi-mode

Des virus multi-mode sont tout simplement ceux qui attaquent en même temps certaines des combinaisons de fichiers, des zones système et de mémoire. Leur éradication est la combinaison de procédures de nettoyage de types simples dans un ordre exactement défini.

- il n'est pas possible d'enlever un virus du disque qui est présent en mémoire,
- pour enlever des virus du disque, il faut d'abord l'enlever des zones système,
- des virus dans des fichiers particuliers doivent être enlevés en dernier.

B.3.2 Des virus résidents en mémoire

Ces virus ne sont non seulement installées en mémoire mais très certainement quelque part sur le disque dur.

Si un soi-disant expert vous dit qu'un virus peut être présent en mémoire sans se trouver ailleurs (sur le disque dur, une disquette ou un autre media de ce genre), contactez quelqu'un d'autre. Vous aurez plus de sécurité pour vos données.

Un virus peut être présent en mémoire sans être actif en même temps. Imaginez que vous êtes en train de copier le fichier infecté d'une disquette sur une autre disquette. Pour ce faire, vous vous servez de la mémoire vive de l'ordinateur, et la source ainsi que la cible sont stockées dedans. Ce qui veut dire que le virus peut exister en mémoire même après avoir terminé l'opération de copiage, tout simplement parce qu'il n'y a pas de raison de nettoyer la mémoire ainsi utilisée. Cependant, cela ne veut pas dire que le virus peut causer un quelconque dommage sous cette forme.

En même temps, vous ne pourrez pas enlever un virus de votre ordinateur quand il est présent et actif dans la mémoire vive. L'explication est simple: le virus attaque immédiatement chaque programme ou zone système que vous essayez d'accéder.

Vous ne pourrez rien y faire. En général, vous ne pourrez pas éliminer un virus en mémoire quand il est présent. Il existe peut-être des exceptions mais vous ne pouvez pas vous y fier.

En même temps, nous devons souligner que des virus exclusivement conçus pour les systèmes d'exploitation Windows 95 et NT n'existent pratiquement pas de nos jours, et aucun des exemplaires très rares est capables de rester résident en mémoire. Si la situation devait changer, nous vous en avertirions.

Il en résulte que la mémoire ne peut contenir que des virus conçus pour MS-DOS qui était en contact avec lui au démarrage ou pendant le travail dans la fenêtre DOS. S'il s'agit en même temps d'un virus qui attaque les zones systèmes, vous pourrez passer directement au chapitre consacré aux virus de ce type. En ce qui concerne des virus de fichiers, ils sont faciles à enlever de la mémoire.

Faites démarrer le système avec une disquette de secours. Vous pourrez prendre une disquette système MS-DOS 5.0 ou plus. Cependant, nus recommandons d'utiliser une disquette système conforme à celui qui et installé sur votre poste.

La continuation de l'opération dépend du type de virus.

Sous Windows NT, il n'y a pratiquement pas de problèmes avec des virus en mémoire. Les seuls virus qui peuvent vous déranger sont les virus attaquant les zones systèmes.

B.3.3 Virus de fichiers

L'éradication des virus de fichiers est facile mais plutôt ennuyeux. Le problème principal est de décider comment procéder.

Un renouvellement à 100 % ne sera assuré que si vous restaurez les fichiers à l'aide de leurs copies de sauvegarde (si vous en avez, bien sûr, et si ces copies ne sont pas infecté par le même ou un autre type de virus). Il peut être simple et fiable de restaurer les fichiers avec les copies de sauvegarde. Si vous consacrez du temps, régulièrement, à la création de copies de sauvegarde, vous verrez pourquoi cela vaut la peine. C'est du travail rapide et confortable.

Si vous utilisez régulièrement le programme de contrôle d'intégrité et avez à votre disposition la version actuelle de la base, vous n'aurez pratiquement aucun souci. AVAST32 vous permet de restaurer les fichiers infectés pratiquement par tous les virus (environ 95 % de types différents de virus). La fiabilité est la même que celle des copies de sauvegarde, parce qu'AVAST32 vérifie s'il a réussi à restaurer le fichier jusqu'au bout. Si rien de ce dernier paragraphe ne peut vous servir, la situation commence à être plus compliquée. Mais vous ne devez pas perdre en seul de vos programmes. Cependant, vous aurez besoin des disquettes d'origine ou de leurs copies. Ceci demande plus de travail parce que vous devez désinstaller et réinstaller les programmes infectés ce qui entraîne des problèmes connus avec la sauvegarde de toutes les tâches et configurations que vous avez inventées avec autant d'efforts.

La désinstallation de programmes ne se limite pas à leur simple suppression du disque dur. Tous les programmes "sérieux" des systèmes d'exploitation Windows 95 et NT sont capables d'être désinstallés ce qui signifie bien plus que d'être tout simplement supprimés du disque.

Si vous ne pouvez pas non plus utiliser cette méthode, vous aurez un problème. Le problème sera vraiment grave puisque tout ce que nous pouvons vous conseiller est de supprimer les fichiers infectés. Honnêtement, il vous reste toujours une possibilité mais pouvant avoir des résultats assez tristes. Il s'agit d'enlever les virus des fichiers à l'aide d'un autre programme anti-virus. Cette solution a un grand avantage. Vous ne pouvez pas savoir si le fichier corrigé est dans le même état qu'avant l'infection. C'est la raison principale pourquoi AVAST32 ne contient pas une telle propriété.

B.3.4 Virus de secteur de démarrage

Il y a un grand nombre de virus capables d'attaquer les zones système des disques durs. Cependant, seuls quelques-uns sont aussi des virus multi-mode pouvant infecter de fichiers et se propager à l'aide de fichiers.

C'est pourquoi nous pouvons affirmer avec une petite objection que si vous avez trouvé un virus dans la zone système d'un disque (virus du secteur de démarrage), c'est arrivé au démarrage de l'ordinateur à l'aide d'une disquette. Ce n'est pas important si vous êtes arrivé ou non. S'il y avait un virus sur la disquette en question, il a infecté votre

ordinateur, indépendamment du système d'exploitation utilisé.

Il ne sert à rien de penser voire de persuader quelqu'un qu'un virus comme par exemple "J&M" ou "JiMi" et entré dans votre ordinateur uniquement en lisant des données de la disquette. Ceci n'est tout simplement pas vrai, peu importe qui vous le dira. Ce tout simplement un mauvais renseignement.

Une exception est peut-être le virus "OneHalf" qui peut se propager aussi à l'aide de fichiers ce qui signifie qu'en exécutant le fichier infecté, l'ordinateur sera contaminé. De virus similaires sont tout de même très, très rares.

Procédure de nettoyage: démarrez le système avec votre disquette système et exécutez le programme: fdisk/MBR du système d'exploitation. La disquette ne doit absolument pas être infectée par un virus. Après avoir exécuté ces commandes avec succès, le virus sera enlevé des zones systèmes du disque sous Windows 95 et NT.

Si vous arrivez à démarrer le système d'exploitation, vous aurez presque gagné. Vous pourrez vous servir des capacités de restauration intégrées dans le système d'exploitation qui s'occuperont du reste. Si, par contre, vous n'arrivez pas du tout à le faire démarrer, ce sera le désastre.

B.3.5 Virus macro

Ce sont des virus qui se propagent à travers des documents. Actuellement, il s'agit des virus les plus fréquents dans le monde. Le plus souvent, ils attaquent les documents Microsoft WORD mais récemment, ils sont arrivés aussi dans d'autres applications.

Le nettoyage peut être effectué directement à partir de l'environnement AVAST32 (chapitre 5.3.2). Cependant, nous conseillons de sauvegarder les documents infectés, d'enlever les virus des originaux et de tester la lisibilité dans vos programmes. Si les documents ainsi traités sont en bon état, il est possible de supprimer leurs copies de sauvegarde infectées. Si non, n'hésitez pas à contacter nos collaborateurs. Les algorithmes utilisés par AVAST32 pour détecter des virus macro et leur enlèvement des documents OLE font actuellement partie des produits haut de gamme sur plan mondial c qui signifie que vos documents seront bien soignés.

C.Configurations par défaut des tâches

Onglet "Nom"

La zone de texte pour entrer le nom de la tâche contient le texte "(non spécifié)". La nouvelle tâche est personnalisée par défaut.

Onglet "Test"

Seul « Virus Scanning » a été selectionné depuis le test non résident. « Test d'intégrité « et « Test Simple d'intégrité » n'ont pas été sélectionnés. Aucun test résident n'est vérifié.

Onglet "Priorité"

La priorité de la tâche est configurée à une valeur inférieure à la priorité de l'interface utilisateur du programme AVAST32.

Onglet "Types"

Le contrôle de tous les fichiers exécutables et documents OLE est prévu pour une nouvelle tâche.

Onglet "Zones"

Le contrôle de tous les disque durs locaux est prévu par défaut, c'est-à-dire tous les disques durs installés directement dans votre ordinateur. Les sous-répertoires seront testés également.

Onglet "Personnaliser"

Aucune des cases de cet onglet n'est activée, ce qui veut dire que la nouvelle tâche sera lancée directement par l'utilisateur. Le programme AVAST32 sera fermé en même temps que la dernière tâche et seul le premier virus trouvé par la tâche sera signalé aux programmes externes.

Onglet "Scanner"

Sont activés: "Test de mémoire" (disponible uniquement sous Windows 95), "Rechercher tous les virus" et "Tester les fichiers compressés".

La tâche testera la mémoire vive dans le système d'exploitation Windows 95. Elle ignorera les caractéristiques des virus. Elle testera tous les fichiers et les fichiers compressés seront balayés en mode compressé et décompressé.

Si aucun virus n'est trouvé, aucun message ne s'affichera.

La case "Signaler tous les virus" est activée par défaut.

Onglet "Checker"

Seule la case "Ignorer attribut ARCHIVE" est activée. Le contrôle d'intégrité ignorera l'attribut ARCHIVE des fichiers et testera toujours les contenus.

Onglet "Continuer"

La zone de texte "Nom de la tâche" est vide. Après la fin de cette tâche, aucune autre tâche ne sera lancée.

Onglet "Rapport"

La case "Fichier de rapport" n'est pas cochée. La case "Nom/chemin du rapport" contient "*" (l'astérisque) et la case "Remplacer fichier rapport existant" n'est pas activée. La nouvelle tâche ne créera donc pas de rapport de son activité.

Onglet "Alarme réseau"

La case "Envoyer l'alerte via le réseau" n'est pas activée, la diffusion des messages par le réseau n'est donc pas autorisée et la configuration des autres commandes de cet onglet est ignorée. La case "Envoyer message aux postes sélectionnés uniquement" est cochée.

La liste des ordinateurs dans cet onglet est vide par défaut.

Onglet "Message"

La zone de texte pour le rapport contient le texte suivant par défaut:

Fichier %1 infecté par %2.

Onglet "Son"

Cet onglet ne contient pas de commandes.

Onglet "Résident scanner"

Les "Documents OLE (virus Macro)", "Applications 16-bit Windows" et "Applications MS-DOS" sont contrôlés, c'est-à-dire toutes les applications en cours sur votre poste seront contrôlées.

La case "Tout vérifier excepté librairies système" est activée.

Onglet "Behaviour Blocker"

Les zones "Surveiller les cessions DOS" et "Surveiller les applications Windows" sont activées. La zone "Surveiller le formatage de pistes" n'est pas activée sous Windows 95. Cela veut dire que toutes les opérations seront analysées, à l'exception du formatage.

Onglet "Ignorer"

La liste des fichiers de cet onglet est vide par défaut. Des opérations suspectes effectuées sur tous les fichiers de votre ordinateur seront analysées.

D.Numéros de série et licences

Un numéro de série est la chaîne de caractères AABB.CDDDDDD-EEEEEE. La première partie est consacrée à l'identification du programme, la partie commençant par BBB définit le numéro de version et le C spécifie le nombre de licences disponibles. S'il y a la lettre A, une licence a été achetée, B signifie deux licences etc. DDDDDD remplace le numéro de série du programme et EEEEEE le code avec lequel l'authenticité du programme peut être vérifiée. AVAST32 surveille le nombre de copies en cours dans le réseau à tout moment. Si vous avez acheté moins que dix licences, le programme vous permettra de faire tourner autant de licences achetées plus une. Si vous avez acheté au moins dix licences, vous pourrez faire tourner autant de copies plus deux.

L'utilisateur sera averti par le biais d' un message d'alerte (fig. 114) du fait que plus de copies que le nombre de licences sont en cours d'utilisation.

Le message d'avertissement (Fig. 115) informe l'utilisateur qu'il utilise plus de licences qu'il n'en a acheté. En cliquant sur le bouton « Activer » dans la boîte de dialogue qui apparaît, il peut entrer une nouvelle clé d'activation (voir chapitre 6.4). Pour fermer la boîte de dialogue, cliquer sur « OK ».

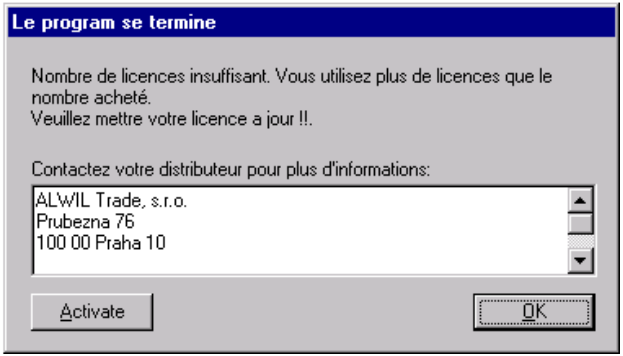

fig. 115

Si les utilisateurs essayent, malgré ce message, de faire tourner encore d'autres copies du programme AVAST32, toutes les licences en cours seront annulées.

Pour savoir sur quels ordinateurs de votre réseau, AVAST32 est utilisé avec votre clé d'activation, cliquez avec le bouton droit sur le troisième item de la barre d'état (cet item contient des informations sur le nombre de licences utilisées et disponibles).

E.Propriétés réseau et assistance

AVAST32 accepte bien évidemment le travail en réseau, l'équipement standard de beaucoup d'entreprises de nos jours.

A la découverte d'un virus, AVAST32 permet d'envoyer un message à chaque utilisateur connecté, le plus fréquemment à l'administrateur réseau ou tout autre responsable. Pour ce faire, AVAST32 se sert des fonctions prévues par le système d'exploitation Windows, donc aucune configuration supplémentaire n'est nécessaire.

Quand vous travaillez sur réseau, il est important de respecter l'accord de licence. AVAST32 surveille le nombre de copies du programme en cours qui ne doivent pas excéder le nombre de licences accordées. Vous trouverez des informations plus détaillées dans l'annexe D.

Il peut être parfois difficile de maintenir tous les programmes utilisés dans un état suffisamment actualisé. Ceci s'applique encore plus aux anti-virus. Afin de ne pas obliger l'administrateur réseau à mettre à jour les bases de virus dans chaque ordinateur séparément, l'autorégulation de cette activité a été incluse dans AVAST32. Tout ce qui reste à faire est de créer le répertoire accessible pour tous les utilisateurs réseau. Ce répertoire sera inclus dans AVAST32 pour la mise à jour automatique du fichier VPS (chapitre 6.6, zone de texte "chemin d'accès mise à jour fichier VPS") et il faut activer la mise à jour (chapitre 6.1.2, case "activer mise à jour automatique VPS").

Il suffit ensuite de copier chaque mise à jour du nouveau fichier VPS (appelée "petites mises à jour") dans le répertoire créé et la mise à jour se fera automatiquement sur tout le réseau. AVAST32 vérifiera après démarrage si le répertoire sélectionné ne contient pas de fichier VPS plus récent. Dans ce cas, il enlèvera l'ancien fichier et le remplacera par le plus récent.

F.Assistance technique pour programmeurs

AVAST32 s'adresse en grande partie aux utilisateurs mais contient quelques propriétés pouvant être exploitées en particulier par des programmeurs. La propriété la plus importante est décrite dans le chapitre suivant.

Si vous entrez le chemin d'accès quel que soit l'endroit dans AVAST32, le nom peut également comporter la variable système entre deux signes "%". Le répertoire racine du système peut donc être indiqué ainsi: "%RacineSystème%". Si la variable système du nom donné n'existe pas, cette partie du chemin d'accès sera ignorée.

F.1 Envoyer des messages sur les virus détectés

AVAST32 travaille avec les mécanismes qui permettent d'informer des programmes externes d'un virus. Pour cette raison, la boîte aux lettres nommée

\\.\boîte aux lettres\AVAST32\VIRUSTROUVE

a été créée. Cette boîte aux lettres contient toutes les informations sur le premier virus trouvé par un programme non-résident. On peut configurer que l'information sur tous les virus trouvés soit envoyée à la boîte aux lettres (chapitre 4.4.6).

Le message du virus trouvé contient les noms du domaine, de l'ordinateur, de l'utilisateur, du fichier infecté et du virus qui a infecté le fichier. Les données sont transmises à la boîte aux lettres sous forme d'une chaîne de caractères séparés entre eux par un 0.

Index

A

B

C

D

E

F

I

L

M

S

T

V

W