KASPERSKY LABS

Kaspersky Anti-Virus®
Personal / Personal Pro 4.5

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS®
PERSONAL / PERSONAL PRO 4.5

Manuel de l'utilisateur

Consultez notre site sur le Web: http://www.kaspersky.com/fr/

Date d'édition: Septembre 2003

Sommaire

CHAPITRE 1. KASPERSKY ANTI-VIRUS® PERSONAL

Attention ! Il apparaît chaque jour de nouveaux virus, c'est pourquoi il est indispensable d'actualiser régulièrement les bases anti-virus du produit au moins une fois par jour (pour plus de détails, voir ci-après). N'oubliez pas d'actualiser les bases de données anti-virus aussitôt après l'installation du produit sur votre ordinateur !

Le package Kaspersky Anti-Virus® Personal est un ensemble de programmes de protection de votre ordinateur équipé du système d'exploitation Windows. Il comprend les programmes suivants:

- **Kaspersky Anti-Virus® Scanner** un analyseur antiviral à la demande permettant de rechercher et de supprimer des virus. Le programme recherche et supprime les virus dans les fichiers, les secteurs de démarrage et la mémoire vive (RAM). Il est capable de détecter (mais pas de supprimer) les virus dans les fichiers d'archives et les boîtes aux lettres locales des systèmes de messagerie les plus courants. (Important: Kaspersky Anti-Virus® Scanner est uniquement capable de supprimer des virus dans les bases de données de MS Outlook Express version 5.0 (ou supérieur) !)
- **Kaspersky Anti-Virus® Monitor** est un moniteur anti-virus résident qui permet de vérifier la présence de virus dans tous les fichiers lancés et ouverts dans l'ordinateur.

  Remarquez que Kaspersky Anti-Virus® Monitor est en mesure de supprimer des virus uniquement depuis des fichiers ZIP !
- **Kaspersky Anti-Virus® Updater** est un programme de mise à jour des bases de données anti-virus. Les bases anti-virus sont utilisées lors de la recherche de virus par Kaspersky AV Scanner et Kaspersky AV Monitor. Le Laboratoire Kaspersky met quotidiennement à jour les bases anti-virus par le biais des informations sur les nouveaux virus et lance les mises à jour sur le réseau Internet via lequel le programme de mise à jour les reçoit.
- **Kaspersky Anti-Virus® Mail Checker** est un logiciel assurant la protection antivirale des utilisateurs de Microsoft Outlook 98/2000/XP .

- **Kaspersky Anti-Virus® Script Checker** est un programme de protection de l'ordinateur contre la pénétration des virus de script et des "vers" s'exécutant directement dans la mémoire de l'ordinateur.
- **Kaspersky Anti-Virus® Rescue Disk** est un programme permettant de préparer des disquettes de restauration destinées à remettre le système en état de fonctionnement à la suite d'une offensive virale.
- **Kaspersky Anti-Virus® Control Centre** est un programme permettant de superviser tous les autres logiciels du package. Kaspersky AV Control Centre a pour fonction de gérer l'installation et de mettre à jour les composants du package, de contrôler leur planning de lancement automatique, ainsi que les résultats consécutifs à leur exécution.
- **Kaspersky® Report Viewer** permet de consulter les rapports générés par les autres modules du package.

1.1. Nouveautés de la version 4.5

La version du logiciel Kaspersky Anti-Virus® Personal décrite dans ce document inclut les nouveautés suivantes:

- Amélioration de la vitesse de traitement du logiciel;
- Désinfection des fichiers d'archive ZIP.
- L'algorithme de vérification des messages joints dans les messages sortants et entrants a été renforcé dans l'utilitaire Kaspersky Anti-Virus® MailChecker afin de réduire les besoins en ressources de l'ordinateur lors de la vérification **Windows 95/98/Me.**

1.2. Configuration matérielle et logicielle requise

Pour que votre programme fonctionne au maximum de ses capacités, votre ordinateur doit être conforme aux normes système suivantes :

- Processeur Intel Pentium (ou compatible) **150 MHz** ou supérieur.
- Au moins **32 Mo** de RAM (**64 Mo** recommandés).

Windows NT Workstation 4.0 (SP6 ou supérieur):

- Processeur Intel Pentium (ou compatible) **150 MHz** ou supérieur.
- Au moins **48 Mo** de RAM (**64 Mo** recommandés).

Windows 2000 Professional:

- Processeur Intel Pentium (ou compatible) **150 MHz** ou supérieur.
- Au moins **64 Mo** de RAM (**96 Mo** recommandés).

Windows XP Home Edition/Professional:

- Processeur Intel Pentium (ou compatible) **300 MHz** ou supérieur.
- Au moins **128 Mo** de RAM.

Lors de l'utilisation de Kaspersky Anti-Virus® avec les systèmes d'exploitation Windows XP Home Edition ou Windows XP Professional, certaines restrictions limitent l'emploi de la fonctionnalité de basculement entre utilisateurs. Certaines options de paramétrage de Kaspersky Anti-Virus® ne sont alors pas accessibles et certaines boîtes de dialogue de confirmation n'apparaissent pas (demande de confirmation des actions sur les fichiers infectés).

Spécifications générales requises pour tous les systèmes d'exploitation:

- Au moins **72 Mo** d'espace disponible sur le disque pour l'installation, et **23 Mo** pour l'exploitation.
- Microsoft Internet Explorer version 5.5 ou supérieur avec SP2.
- Aucun autre logiciel antivirus installé dans l'ordinateur, y compris les produits Kaspersky Lab.

Si un programme antivirus est installés dans votre ordinateur, nous vous conseillons de le désinstaller avant d'installer Kaspersky Anti-Virus® Personal.

- La résolution du moniteur doit être définie à 800 x 600 au moins, avec petite taille de polices, et l'heure du système doit être définie correctement.

1.3. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus® Personal chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, www.kaspersky.com - lien **Buy online** / Achat en ligne).

Le pack logiciel contient:

- une enveloppe cachetée contenant le CD d'installation où les fichiers du produit de programme sont enregistrés
- le manuel de l'utilisateur

- Une clé de licence inscrite sur le CD d'installation ;
- le contrat de licence.

Avant de décacheter l'enveloppe contenant le CD (ou les disquettes), lisez attentivement le contrat de licence.

Si vous achetez Kaspersky Anti-Virus® Personal en-ligne, le fichier d'installation du produit est téléchargé du site Web de Kaspersky Labs. Ce fichier d'installation inclut ce guide de l'utilisateur et la clé de licence. La clé de licence peut être également envoyée par courriel après réception de votre paiement.

Le contrat de licence constitue l'accord juridique passé entre vous et Kaspersky Labs Ltd., stipulant les conditions d'utilisation du logiciel que vous avez acquis.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez retourner la boîte contenant Kaspersky AV au distributeur agréé qui vous l'a vendue et être intégralement remboursé. Dans ce cas, l'enveloppe contenant le CD (ou les disquettes) ne doit en aucun cas avoir été décachetée.

L'ouverture du package cacheté ou l'installation du logiciel implique que vous acceptez les termes du contrat de licence.

1.4. Services réservés aux utilisateurs inscrits

Kaspersky Labs Ltd. offre à ses utilisateurs légalement enregistrés une gamme élargie de prestations leur permettant d'augmenter l'efficacité d'utilisation du logiciel Kaspersky Anti-Virus®.

En vous enregistrant, vous devenez utilisateur agréé du programme et durant toute la période de validité de votre souscription, vous bénéficiez des prestations suivantes:

- nouvelles versions de ce logiciel antivirus, fournies gratuitement ;
- assistance téléphonique et par voie électronique sur l'installation, la configuration et l'utilisation de ce produit antivirus ;
- les avis de lancement des nouveaux logiciels de la société Kaspersky Labs et les informations sur l'apparition des nouveaux virus dans le

monde (ne bénéficient de ce dernier service que les utilisateurs ayant souscrit un abonnement au bulletin de **Kaspersky Labs.**).

Le service d'assistance technique ne donne pas de consultations sur les problèmes de fonctionnement et d'utilisation des systèmes d'exploitation ainsi que sur des questions sur le fonctionnement des différentes technologies.

1.5. Notations conventionnelles

Le texte de la documentation se distingue par divers éléments de mise en forme en fonction de son affectation sémantique.

Mise en forme	Fonction sémantique
Caractères gras	Nom du menu, des options du menu, des fenêtres, des éléments des boîtes de dialogue, etc.
 Remarque.	Information complémentaire.
 Nota Bene !	Information à laquelle il est recommandé d'accorder une attention particulière.
 *Pour exécuter une action,* 1. Etape 1. 2. …	Description de la succession des étapes accomplies par l'utilisateur.
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du produit.
 Solution	A solution of the problem formulated
[touche] — la fonction de la touche.	Touches de ligne de commande
`Texte des messages d'information et sur ligne de commandes`	Texte des fichiers de configuration, des messages d'information et de la ligne de commandes.

CHAPITRE 2. INSTALLATION ET DESINSTALLATION DU PROGRAMME

Avant d'installer le programme Kaspersky Anti-Virus® sur votre ordinateur, il est recommandé de quitter toutes les applications actives dans votre ordinateur.

Pour installer le logiciel, lancer le programme Setup.exe présent sur le CD. Le programme d'installation se compose d'une succession de boîtes de dialogue comportant différents boutons destinés à contrôler la procédure.

- **OK** – validation des actions
- **Annuler** – annulation des actions
- **Suivant** – passer à l'étape suivante
- **Précédent** – revenir à l'étape précédente.

Vous avez le choix entre deux variantes d'installation du produit : première installation et réinstallation. Les deux variantes sont décrites en détail

2.1. Première installation

Etape 1. Lecture du contrat de licence

La boîte de dialogue **Licence d'utilisation** (2) contient le texte du contrat de licence. Lisez le texte du contrat de licence et si vous en acceptez les conditions, cliquez sur le bouton **Oui**. Dans le cas contraire cliquez sur le bouton **Non**, ce qui a pour effet d'interrompre le processus d'installation.

Etape 2. Saisie des données concernant l'utilisateur

Dans la boîte de dialogue **Information Utilisateur** (3) entrez l'information concernant l'utilisateur. Dans le champ **Nom**, entrez le nom de l'utilisateur et dans le champ **Société**, celui de la société. Ces champs contiennent par défaut l'information préenregistrée dans la base de registre de Windows.

Etape 3. Choix du répertoire d'installation

Dans la boîte de dialogue **Choisissez un répertoire de destination**, sélectionnez les répertoires d'installation des composants de Kaspersky Anti-Virus®. Dans le groupe **Dossier final** est donné le répertoire pour les composants et dans le groupe **Dossier pour les fichiers communs** – le répertoire pour les fichiers communs à tous les composants. Le choix des répertoires est effectué au moyen du bouton **Parcourir**.

Etape 4. Choix du nom du groupe de programmes dans le menu "Démarrer\Programmes"

Dans la boîte de dialogue **Sélectionnez un répertoire programme** indiquez le nom du groupe de **Programmes**, dans lequel sera placée l'icône destinée au lancement des programmes du package de Kaspersky Anti-Virus®. Cliquez sur le bouton **Suivant**.

Etape 5. Choix du type d'installation

Dans la boîte de dialogue **Type d'installation** choisissez un des trois types d'installation suivants :

Personnalisée	Il vous sera proposé de choisir le jeu de composants que vous voulez installer dans la liste.
Minimum	Ne seront installés que les composants indispensables du package, tels que Kaspersky Anti-Virus® Scanner, Kaspersky Anti-Virus® Monitor, les bases anti-virus et le programme de mise à jour.
Complète	Tous les composants du package Anti-Virus Kaspersky® seront installés.

Etape 6. Choix des composants de Kaspersky Anti-Virus® à installer

Si vous avez choisi le type d'installation **Personnalisée**, vous devez indiquer les composants que vous voulez installer dans la boîte de dialogue **Sélectionnez les composants**.

Pour sélectionner un composant, activez le commutateur situé à gauche du nom du composant.

Etape 7. Copie des fichiers sur le disque

Dans la boîte de dialogue **Démarrage de la copie des fichiers**, vérifiez les informations concernant l'installation. Pour continuer l'installation, cliquez sur le bouton **Suivant**. Ceci a pour effet de lancer la procédure de copie vers le disque dur de l'ordinateur, les informations sur la procédure étant affichées dans la boîte de dialogue **Etat de l'installation**.

Etape 8. Choix du répertoire de stockage des rapports

Dans la boîte de dialogue **Paramètres de Report Viewer**, il est nécessaire d'indiquer le répertoire dans lequel les rapports générés par les composants du package Kaspersky Anti-Virus®.

Etape 9. Indication du chemin d'accès vers les fichiers-clés

Dans la boite de dialogue **Fichier-clé**, il est indispensable d'indiquer le nom du fichier-clé et son chemin d'accès.

Si ce fichier est placé dans le dossier depuis lequel l'installation est réalisée, il sera automatiquement affiché dans la liste **Liste des fichiers-clés**.

Si le fichier-clé est placé dans un autre dossier, cliquez sur le bouton **Ajouter** et dans la boîte de dialogue standard **Choix du fichier-clé** qui s'affiche à l'écran, indiquer le nom et le chemin d'accès. Le cas échéant, il est possible d'utiliser simultanément plusieurs fichiers-clés.

Le fichier-clé est votre **clé** personnelle dans laquelle se trouvent toutes les informations fonctionnelles indispensables au travail de Kaspersky Anti-Virus®, à savoir:

- les coordonnées du distributeur de votre version du produit (nom de la société, adresse, téléphone)
- les informations sur l'assistance technique (par qui est-elle assurée et comment l'obtenir)
- la date de lancement du produit
- le nom et le numéro de la licence
- le tableau de fonctionnalité des divers composants
- le délai de validité de la licence.

Etape 10. Fin de l'installation

Après la fin de l'installation du package Kaspersky Anti-Virus®, la fenêtre **Installation du programme achevée** s'affiche à l'écran. Choisissez l'une des options suivantes :

- **Oui, redémarrer l'ordinateur maintenant**
- **Non, redémarrer l'ordinateur plus tard**

Dans ce cas, pour terminer correctement l'installation du progiciel Kaspersky Anti-Virus® Personal et démarrer le travail, il est INDISPENSABLE de redémarrer votre ordinateur.

Cliquez sur le bouton **Terminer**.

Le redémarrage du système d'exploitation peut être retardé en raison du programme d'installation qui termine l'installation de Kaspersky Anti-Virus® Personal sur votre ordinateur. Ne vous inquiétez pas ! C'est à ce moment que le programme Kaspersky Anti-Virus® Personal est intégré dans votre système.

2.2. Réinstallation

Si vous procédez à une réinstallation du logiciel, après le lancement de l'installateur, la boîte de dialogue **Programme de maintenance** s'affichera à l'écran, dans laquelle il est possible de choisir un des modes suivants:

- **Modifier** — ajouter de nouveaux programmes du package aux programmes déjà installés.
- **Réparer** — restaurer tous les programmes du package installés antérieurement mais éventuellement endommagés.
- **Supprimer** — désinstaller le package de programmes de Kaspersky Anti-Virus® de l'ordinateur (voir p. 2.3).

Pour choisir une de ces actions, activez l'option correspondante et de cliquer sur le bouton **Suivant**.

Si vous choisissez l'option **Modifier**, la boîte de dialogue **Sélectionnez les composants** s'affiche à l'écran. Dans cette boîte il est possible de sélectionner les composants souhaités après avoir préalablement activé les commutateurs appropriés. Après avoir sélectionné les composants souhaités, cliquez sur le bouton **Suivant**, à la suite de quoi les boîtes de dialogue **Etat de l'installation** et **Installation du programme achevée** s'afficheront consécutivement à l'écran.

Si vous avez choisi l'option **Réparer**, les boîtes de dialogue **Etat de l'installation** et **Installation du programme achevée** s'afficheront

consécutivement à l'écran. Cette option peut être choisie, par exemple, si vous avez malencontreusement effacé de l'ordinateur un des fichiers faisant partie intégrante du package de Kaspersky Anti-Virus®.

Il est possible que la même version ou une version antérieure du programme Kaspersky AV Control Centre ait déjà été déjà installée sur votre ordinateur, par exemple depuis un autre package logiciel. Dans ce cas, au cours de la procédure d'installation la boîte de dialogue **Composant : Kaspersky Anti-Virus® Control Centre** s'affichera à l'écran et demandera quelles sont les actions à effectuer concernant l'installation du fichier standard de réglages.

Vous pouvez choisir un des types suivants d'installation du fichier de réglages:

- **Fusionner** — ajouter aux réglages au fichier de réglages existant
- **Ecraser** — remplacer le fichier de réglages existant par le fichier standard
- **Omettre** — laisser le fichier de réglages existant inchangé.

Si le programme Kaspersky AV Updater a déjà été installé sur votre ordinateur, une boîte de dialogue semblable à celle présentée dans apparaîtra à l'écran. Cependant, dans cette boîte l'option **Fusionner** sera inaccessible. Vous pourrez soit écraser le fichier standard de réglages, soit sauvegarder le fichier existant.

2.3. Supprimer un programme

Si, pour une raison quelconque, vous devez désinstaller le programme Kaspersky Anti-Virus®, choisissez dans la boîte de dialogue **Programme de maintenance** l'option **Supprimer** et cliquez sur le bouton **Suivant**.

La boîte de dialogue de confirmation de la suppression apparaîtra alors à l'écran. Pour lancer la procédure de désinstallation, cliquez sur le bouton **OK**. Ceci aura pour effet de débuter la procédure de suppression des fichiers du programme du disque dur de l'ordinateur. Il est possible de suivre la procédure dans la boîte de dialogue **Etat de l'installation**.

Si en cours de désinstallation, le programme détecte des fichiers susceptibles d'être utilisés par d'autres programmes, l'écran affiche une boîte de dialogue de confirmation de la suppression. Pour supprimer le fichier concerné, cliquez sur le bouton **Oui**. Il convient d'être prudent afin de ne pas priver d'autres programmes de fichiers qui leur sont indispensables.

CHAPITRE 3. KASPERSKY ANTI-VIRUS® SCANNER

Kaspersky Anti-Virus® Scanner (Kaspersky AV Scanner) est un programme lancé par l'utilisateur pour rechercher les virus et pour éliminer les virus éventuellement détectés.

Lors de sa mise en oeuvre, le scanner anti-virus exécute les opérations suivantes:

- Il détecte et élimine tous les types de virus présents dans les fichiers sur les disques vérifiés, dans les secteurs d'amorçage (boot) et dans la mémoire vive.
- Il détecte et élimine les virus présents dans les fichiers compressés (PKLITE, LZEXE, DIET, COM2EXE et autres utilitaires de compression).
- Il détecte (mais n'élimine pas) les virus présents dans les archives créées avec les utilitaires les plus répandus: Microsoft Outlook, Microsoft Exchange, Microsoft Internet Mail, Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, serveur JSMail SMTP/POP3.
- Il détecte (mais n'élimine pas) les virus dans les messageries locales de courrier électronique.
- Détecte et supprime les virus des bases de données de MS Outlook Express v. 5.0 (et supérieur).
- Il utilise un mécanisme heuristique sophistiqué de détection des virus inconnus (efficacité allant jusqu'à 92%).

3.1. Lancement du scanner anti-virus

Le scanner anti-virus peut être lancé par un des procédés suivants:

Option 1 : menu principal de **Windows:** cliquer sur le bouton **Démarrer** et à sélectionner **Programmes**, à passer ensuite dans le groupe **Kaspersky Anti-Virus®** et à sélectionner l'item **Kaspersky Anti-Virus® Scanner**. Vous faites ainsi apparaître la fenêtre principale du programme (voir 3.3.2). Dans la barre des tâches s'affiche l'icône  . En cliquant sur elle avec le bouton droit, vous pourrez dérouler le menu Système (voir p. 3.2.1).

Option 2 : AV Control Centre: lancer le programme à partir du module Control Centre, c'est-à-dire à créer une tâche spéciale qui lancera le scanner à un moment donné et avec des réglages prédéfinis. Il est également possible de démarrer cette tâche manuellement ou de programmer son démarrage automatique.

Option 3 : ligne de commande: cliquez sur le bouton **Démarrer** de Windows, sélectionnez la commande **Exécuter**, puis, dans la boîte de dialogue **Exécuter**, saisissez le chemin d'accès complet vers le module exécutable avp32.exe. Par exemple,

"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Personal\Avp32.exe".

Voici les paramètres disponibles lors du lancement à partir de la ligne de commande :

[/?] ou [/H] – montrer la liste de tous les paramètres de la ligne de commande

[/P**=nom_de fichier**] – lancer Kaspersky AV Scanner avec les réglages définis dans le fichier **nom de fichier**

[/S] – commencer la vérification antivirale aussitôt après le lancement de Kaspersky AV Scanner

[/W] – créer un fichier de rapport

[/N] – réduire la fenêtre principale de Kaspersky AV Scanner aussitôt après le lancement

[/Q] – fermer la fenêtre principale de Kaspersky AV Scanner aussitôt après la fin de la procédure d'analyse

[/D] – signifie que Kaspersky AV Scanner ne sera pas lancé si durant la journée en cours une analyse a déjà été exécutée et s'est achevée avec succès, c.-à-d. si elle n'a pas été interrompue et qu'aucun virus n'a été détecté.

[/@[!]=nom_de fichier] – analyser uniquement les fichiers et/ou les dossiers indiqués dans le fichier **nom_de fichier**. C'est un fichier texte ordinaire (ASCII) contenant la liste des noms de fichiers destinés à être analysés. Dans cette liste chaque ligne ne doit comporter qu'un nom de fichier ou de dossier (avec spécification du chemin d'accès complet). Si la clé comporte le signe **!** (c.-à-d. /@!=nom_de fichier), le fichier **nom_de fichier** sera supprimé après la fin de l'analyse. Si le symbole **!** n'est pas indiqué (c.-à-d. /@nom_de fichier), ce fichier ne sera pas supprimé.

[/redundant] – utiliser le mécanisme d'analyse redondante (pour plus de détails, voir p. A.2).Ce mode d'analyse est conseillé si aucun virus n'a pu être détecté lors de la recherche ordinaire et que dans le travail du système des "phénomènes bizarres" continuent de se produire ("rebootages" fréquents, ralentissement du travail de certains programmes, etc.). Dans les autres cas, l'utilisation de ce mode est déconseillée dans la mesure où la procédure d'analyse est fortement ralentie.

[/virlist=nom_de fichier] – créer un fichier **nom_de fichier** et sauvegarder dans ce fichier la liste et y inscrire le liste des noms de virus connus a ce moment que Kaspersky AV Scanner peut détecter.

Si un fichier ou un dossier contenant une liste de fichiers (/@=**liste_fichiers.lst**) est spécifié sur la ligne de commande, l'analyse démarre automatiquement sans le paramètre **/S**.

[/EL] –- exclure de l'analyse les objets spécifiés dans le fichier **nom_fichier** du paramètre **[/@[!]=nomfichier]**.

[/EF] –- exclure de l'analyse les fichiers et/ou les dossiers indiqués dans la ligne de commande. La clé **/EF** peut être appliquée non seulement dans la ligne de commande, mais aussi dans les lignes du fichier **nom_de fichier** avec le paramètre **/@=nom_de fichier**. La présence de la clé **/EF** dans la ligne signifie qu'il n'est pas nécessaire d'analyser le fichier (ou le dossier). Si le nom du fichier comporte des espaces, la clé doit être placée dans la ligne avant le nom du fichier ou, si la clé suit le nom du fichier de ce type, le nom du fichier doit être indiqué entre guillemets. Si le nom du fichier ne comporte pas d'espaces, la clé peut se trouver à n'importe quel endroit.

Grâce aux combinaisons de paramètres /EF, /EL, /@ et de la liste des fichiers et des dossiers, vous pouvez prédéfinir les différents secteurs d'analyse.

Voici quelques exemples d'utilisation des paramètres de la ligne de commande :

Exemple 1. Lancement du programme et analyse des fichiers se trouvant dans le dossier **Mes documents**.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" /S "C:\Mes documents"
```

Exemple 2. Lancement du scanner, constitution de la liste des virus dans le fichier E:\virlist.txt puis sortie du programme.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Per-
sonal\Avp32.exe" /virlist=E:\virlist.txt /q
```

Exemple 3. Lancement du scanner avec recherche immédiate de virus dans le cas où la dernière vérification a été effectuée les jours précédents ou le jour même, alors que la vérification a détecté des virus dans les fichiers. Après la vérification, quitter le programme.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus Per-
sonal\Avp32.exe" /s/d/q
```

Exemple 4. Lancement du programme et analyse de tous les fichiers du dossier **Mes documents**, excepté les fichiers dont la liste se trouve dans le fichier **exclude.txt**.

```
"C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus
Personal\Avp32.exe" "C:\Mes documents" /EL
/@=C:\exclude.txt
```

3.2. Interface du programme

3.2.1. Menu Système

Après le lancement du programme, l'écran affiche la fenêtre principale du programme (voir 3.2.2) et dans la barre des tâches apparaît le symbole . En cliquant avec le bouton droit de la souris sur l'icône, vous pouvez ouvrir le menu Système (Illustration 1). Le menu système comporte les options suivantes:

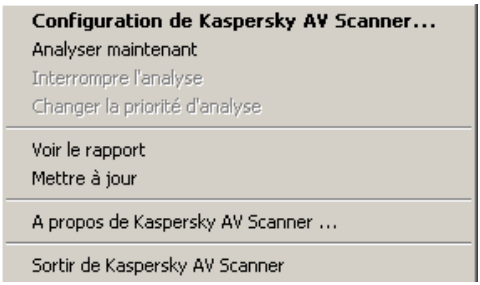


Illustration 1. Menu Système

- **Configuration de Kaspersky Anti-Virus® Scanner…** – ouvrir la fenêtre principale du programme.
- **Analyser maintenant / Stopper l'analyse** – lancer le scanner / arrêter le scanner.
- **Interrompre l'analyse / Reprendre l'analyse** – interrompre le scanner / relancer le scanner.
- **Changer la priorité d'analyse** – modifier la priorité de la procédure de l'analyse.
- **Voir le rapport** – afficher la fenêtre contenant les résultats de la tâche exécutée par le programme.

- **Mettre à jour les bases anti-virus** – lancer le programme de mise à jour des bases anti-virus de Kaspersky AV Updater.
- **A propos du programme** – afficher la fenêtre de renseignements comportant les principales informations sur le programme.
- **Sortir de Kaspersky Anti-Virus® Scanner** – Effacer le programme de la mémoire.

3.2.2. Fenêtre principale

La fenêtre principale du programme Kaspersky AV Scanner permet de modifier les paramètres de l'analyse, de lancer/stopper l'analyse et d'afficher les résultats. Vous pouvez fermer la fenêtre principale sans vider le programme de la mémoire.

Dans la fenêtre principale du programme Kaspersky AV Scanner sont disposés: le menu; la barre d'outils; la zone d'intervention; la barre d'état. Ces éléments sont décrits en détail dans la suite.

3.2.3. Menus

Dans la partie supérieure de la fenêtre principale se trouve la barre de menus . Certaines commandes des menus sont doublées par des combinaisons de raccourcis clavier ou par des boutons de la barre d'outils (voir paragraphe 3.2.4). Les combinaisons de raccourcis clavier sont indiquées dans les menus à côté des commandes appropriées. La correspondance raccourcis clavier et boutons de la barre d'outils est indiquée dans le paragraphe 3.2.4.

Commande du menu	**Fonction**
Fichier → Charger le profil	Charger le jeu de paramètres depuis le fichier de réglage (voir p. 3.3.4).
Fichier → Sauvegarder le profil	Sauvegarder le jeu de paramètres dans le fichier de réglage (voir p. 3.3.4).
Fichier → Enregistrer le profil sous	Enregistrer le jeu de paramètres dans le fichier de réglage sous un autre profil (voir p. 3.3.4).
Fichier → Sauvegarder le profil par défaut	Assigner un jeu de paramètres aux paramètres chargés par défaut (voir p. 3.3.4).
Fichier →	Vider le programme Kaspersky AV Scanner de

Effacer de Kaspersky Anti-Virus® Scanner la mémoire	la mémoire.
Fichier → Fermer la fenêtre	Fermer la fenêtre principale du programme.
Analyse → Analyser / Stopper	Lancer / stopper la procédure d'analyse (voir paragraphe 3.4.1).
Analyse → Interrompre / Reprendre	Interrompre / reprendre la procédure d'analyse (voir paragraphe 3.4.1).
Analyse→ Changer la priorité d'analyse	Modifier la priorité attribuée à l'analyse. Cette commande n'est disponible que si la procédure d'analyse a été lancée.
Analyse → Voir les options d'analyse	Montrer les paramètres sous forme de texte détaillé (voir paragraphe 3.3.5).
Outils → Mettre à jour	Mettre à jour les bases de données anti-virus (voir paragraphe 3.5).
Outils → Voir le rapport	Afficher la fenêtre contenant le rapport (voir paragraphe 3.4.3).
Outils → Créer la liste des virus	Générer la liste de tous les virus connus à l'heure actuelle (voir paragraphe 3.6).
Aide → Sommaire	Appeler le système d'aide.
Aide → Kaspersky AV sur le Web	Se connecter sur le site Web de Kaspersky Labs.
Aide → A propos de Kaspersky AV Scanner	Afficher quelques informations sur le programme.

3.2.4. Barre d'outils

La *barre d'outils* regroupe les boutons sur lesquels vous pouvez cliquer pour déclencher des actions.

Bouton	Menu	Fonction
	Fichier → Charger un profil	Charger les paramètres depuis le profil demandé.
	Fichier → Sauvegarder le profil	Sauvegarder les paramètres dans un profil.
	Fichier → Sauvegarder comme profil par défaut	Sauvegarder les paramètres dans un fichier de réglages et les affecter en tant que paramètres par défaut.
	Analyse → Démarrer l'analyse	Démarrer l'analyse.
	Analyse→ Interrompre l'analyse / Poursuivre l'analyse	Interrompre /reprendre l'analyse.
	Analyse → Stopper l'analyse	Stopper l'analyse.
	Analyse → Consulter les paramètres de l'analyse	Montrer les paramètres sous forme de texte cohérent.
	Outils → Montrer le rapport	Montrer la fenêtre de rapport.
	Outils → Mettre à jour les bases anti-virus	Lancer le programme de mise à jour des bases anti-virus.
	Fichier → Vider Kaspersky AV Scanner	Vider le programme de la mémoire.

3.2.5. Zone d'intervention

3.2.5.1. Catégories Objets, Options, Personnaliser, Statistiques

La zone d'intervention de la fenêtre principale se compose de deux parties. Dans la partie gauche se trouve la liste des catégories et les icônes qui leur

correspondent. Dans la partie droite est affichée le contenu des catégories. Les catégories sont au nombre de quatre: **Objets, Options, Personnaliser et Statistiques**.

La catégorie **Objets** permet de définir les secteurs d'analyse (liste des disques et des dossiers à vérifier), les objets devant être analysés (par exemple les secteurs, les fichiers, les bases de données e-mail), et les règles de traitement des objets infectés (voir p. 3.3.1). Tous ces réglages sont organisés sous la forme d'une arborescence hiérarchisée.

La catégorie **Options** offre la possibilité de définir les réglages généraux et la catégorie **Personnaliser** permet d'effectuer les réglages spéciaux du programme. Ces deux catégories font appel à une *arborescence* pour les réglages (voir paragraphes 3.3.2 et 3.3.3).

La catégorie **Statistiques** permet d'afficher les résultats du travail effectué par le programme dans un tableau (voir paragraphe 3.4.4).

3.2.5.2. Menu contextuel

Certains éléments de l'arborescence des réglages ont un *menu contextuel* dont l'utilisation permet d'exécuter certaines opérations qui leur sont propres. Pour appeler le menu contextuel d'un élément de l'arborescence des réglages:

1. Amenez le pointeur de la souris sur l'objet concerné.
2. Cliquez avec le bouton droit. Cette opération déclenche l'apparition du menu contextuel de l'élément (Illustration 2).

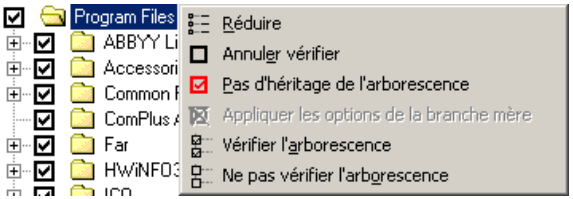


Illustration 2. Menu contextuel de l'arborescence des réglages

3.2.6. Barre d'état

Dans la partie inférieure de la fenêtre principale se trouve la *barre d'état.* Celle-ci affiche les informations suivantes:

- Aide contextuelle / nom de l'objet analysé
- Indicateur d'exécution de la procédure d'analyse

3.3. Réglage des paramètres de l'analyse

Ce sous-chapitre décrit la personnalisation de tous les paramètres de l'analyseur utilisés par Kaspersky AV Scanner.

3.3.1. Paramètres de l'analyse - Catégorie Objets

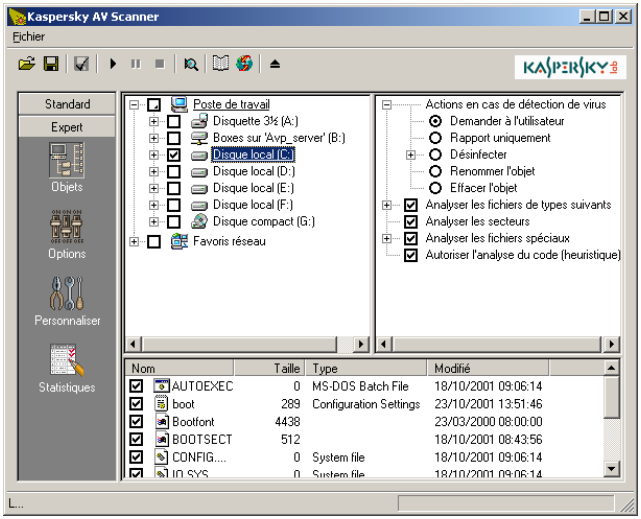


Illustration 3. Catégorie Objets

La catégorie **Objets** (Illustration 3) de la zone d'intervention est utilisée pour sélectionner la zone d'analyse et les objets devant être vérifiés par le scanner. La sélection de la zone et des objets est opérée grâce à l'arborescence des réglages des objets. L'arborescence des réglages peut être visualisée en mode habituel ou en mode expert. Le passage du mode habituel au mode expert est effectué au moyen des boutons **Standard** et **Expert** de la fenêtre principale.

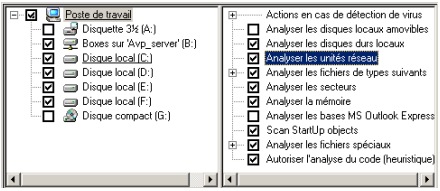


Illustration 4. Mode standard de visualization

En mode habituel, l'arborescence des réglages se présente sous la forme de deux panneaux: panneau de gauche: liste des disques reliés à l'ordinateur panneau de droite: réglages de l'objet sélectionné dans la liste de gauche (Illustration 4).

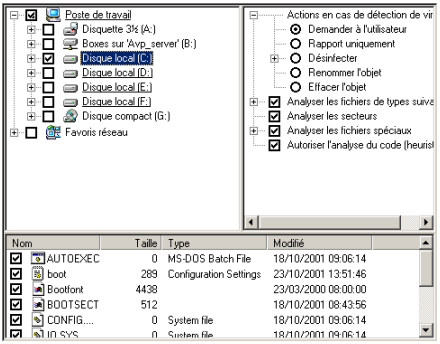


Illustration 5. Mode expert de visualisation

En mode expert, l'arborescence des réglages comprend trois panneaux: panneau de gauche: hiérarchie du système de fichiers de l'ordinateurpanneau de droite: arborescence des réglages le l'objet sélectionné dans la hiérarchie de l'objet panneau inférieur: liste des fichiers disposés à la racine de l'objet sélectionné dans la hiérarchie (Illustration 5).

La zone de vérification est disposée dans la partie gauche du panneau qui contient la hiérarchie du système de fichiers de l'ordinateur avec les indicateurs de vérification de chaque branche du système de fichiers. L'indicateur de vérification peut être activé ☑, ce qui impose la vérification de la branche sélectionnée, ou désactivé ☐, ce qui correspond à l'omission de la branche sélectionnée.

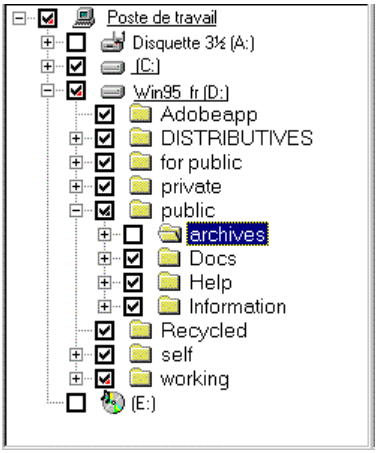
Pour que le programme effectue une analyse de la branche, activez l'indicateur de vérification disposé à gauche de son nom.

Pour sélectionner un groupe de disques en vue de leur analyse, choisissez dans le panneau contenant la hiérarchie du système de fichiers la ligne **Poste de travail** et activez les commutateurs appropriés dans le panneau droit contenant l'arborescence des réglages:

- ☑ **Analyse les disques locaux amovibles** – analyser tous les disques amovibles. Le commutateur n'est accessible que depuis l'arborescence de réglage de l'objet **Poste de travail**. Son activation revient à cocher les indicateurs de vérification de tous les disques amovibles.
- ☑ **Analyse les disques durs locaux** – analyser tous les disques durs locaux. Le commutateur n'est accessible que depuis l'arborescence de réglage de

l'objet **Poste de travail**. Son activation revient à cocher les indicateurs de vérification de tous les disques durs locaux figurant .

En cochant l'indicateur d'une branche quelconque du système de fichiers, vous activez automatiquement les indicateurs de tous les rameaux contenus à l'intérieur de la branche sélectionnée. Cependant, vous avez la possibilité d'exclure de la procédure d'analyse un dossier ou un fichier en passant en mode expert.



Par exemple, vous avez choisi d'analyser les disques C: et D:, mais vous ne voulez pas que le dossier D:\public\archives soit vérifié parce que vous êtes certain qu'il est exempt de virus. Dans ce cas, vous pouvez cocher les indicateurs situés à gauche du nom des disques C: et D:. Ensuite, en faisant apparaître la hiérarchie des fichiers du disque D:, décochez la case située en face du nom du dossier D:\public\archives.

Si vous avez exclu un dossier de l'analyse, dans toutes les zones **parentes** ou **ascendantes** du système de fichiers, la coche ☑ se change en une coche terminée par un triangle pointé vers le bas à droite ☑. Le programme indique de cette manière qu'il vérifie un des rameaux du système de fichiers contenu à l'intérieur de la zone sélectionnée d'une manière différente de l'ensemble de la branche. Vous pouvez effacer les différences de règles de vérification s'appliquant à l'intérieur d'une branche ou, au contraire, les établir pour une période durable. Pour plus de détails, consulter le chapitre 8.3.

Vous pouvez affecter vos paramètres d'analyses à chaque zone du système de fichiers. Dans chaque zone d'analyse choisie vous devez prédéfinir les objets à analyser à l'aide de l'arborescence des réglages du panneau de droite.

3.3.1.1. Objets à analyser - mémoire, secteurs et fichiers

Les branches situées aux différents niveaux de la hiérarchie du système de fichiers de l'ordinateur possèdent un jeu différent de réglages. La zone **Poste de travail** possède une arborescence dotée d'une quantité maximale de réglages. Dans la

liste des réglages sont inclus les paramètres d'analyse de la mémoire vive, des secteurs d'amorçage (boot), d'analyse des groupes de disques et des bases de données MS Outlook Express (v. 5.0 et supérieur). Les paramètres de la branche du disque ne permettent d'analyser que les secteurs d'amorçage (boot) de ce disque, ainsi que d'inclure ou d'exclure la vérification du système de fichiers du disque. Les paramètres de la branche d'un dossier ne permettent pas d'exclure la vérification du système de fichiers. Mais le choix des actions ciblant les objets infectés et suspects, le choix du type des fichiers analysés, et l'activation de modes complémentaires d'analyse font partie des paramètres.

☑ **Analyser les fichiers de types suivants** – analyser les fichiers contenus dans la branche (y compris les fichiers comprenant des attributs tels que Système, Caché et Lecture seule). Le commutateur n'est accessible que depuis l'arborescence de réglage des objets **Poste de travail** et disques. Il est impossible de désactiver le commutateur pour des objets du type **dossier** ou **fichier**. Vous pouvez limiter la vérification à certains types de fichiers, à savoir:

- ⊙ **Tous les fichiers infectables** – analyser tous les fichiers pouvant contenir un virus.
- ⊙ **Tous** – analyser tous les fichiers.
- ⊙ **Par type** – analyser les fichiers avec des masques, présélectionnés dans les champs de saisie disposés plus bas. La quantité de masques que vous pouvez saisir est illimitée, mais chaque champ de saisie ne doit contenir qu'une seule valeur.
- ☑ **Exclure les types** – exclure de l'analyse les fichiers avec des masques présélectionnés dans les champs de saisie disposés plus bas. La quantité de masques que vous pouvez saisir est illimitée, mais chaque champ de saisie ne doit contenir qu'une seule valeur.
- ☑ **Analyser les secteurs** – analyser les secteurs (secteur principal d'amorçage [master boot], secteurs d'amorçage [boot]). Le commutateur n'est accessible que depuis l'arborescence de réglage des objets **Poste de travail** et disques.
- ☑ **Analyser la mémoire** – analyser la mémoire vive. Le commutateur n'est accessible que depuis l'arborescence de réglage de l'objet **Poste de travail**.
- ☑ **Analyser les bases MS Outlook Express** – analyser les bases de données MS Outlook Express (v 5.0 et suivantes). Le commutateur n'est accessible que depuis l'arborescence de réglage de l'objet **Poste de travail**. Pour de plus amples détails sur l'analyse de bases de données en formats différents, consultez le sous-chapitre 3.3.1.3.3.

Kaspersky Anti-Virus® Scanner analyse uniquement les fichier *.dbx stockés dans le répertoire de travail de MS Outlook Express et qui sont ouverts chaque fois que vous démarrez MS Outlook Express. Les fichiers *.dbx des autres répertoires sont considérés par le logiciel comme des bases de données de courrier électronique standard. Le logiciel est capable de détecter, mais pas de supprimer, des virus dans ces bases de données.

☑ **Analyser les objets exécutables au démarrage du système** – analyser les objets exécutés automatiquement par le système d'exploitation aussitôt après l'amorçage. Le commutateur n'est accessible que depuis l'arborescence des réglages de l'objet **Poste de travail**.

3.3.1.2. Actions sur les objets infectés et suspects

Actions en cas de détection de virus – en cas de détection d'objets infectés ou suspects, le programme exécute une des actions suivantes.

⊙ **Demander à l'utilisateur** – en cas de détection de virus, Kaspersky AV Scanner ouvrira une boîte de dialogue (Illustration 6). Cette boîte contient le nom du fichier infecté, le nom du virus détecté et la liste des actions pouvant être exécutées sur l'objet infecté, excepté ⊙ Demander à l'utilisateur. En outre, la boîte de dialogue contient le commutateur **Appliquer à tous les objets infectés.** ,En activant ce commutateur vous pouvez étendre l'action sélectionnée dans la boîte à tous les autres objets infectés découverts par la suite, pour lesquels en tant qu'actions l'ouverture de la boîte de dialogue a été prédéfinie. Dans ce cas, lors de la détection d'un nouvel objet infecté, la boîte de dialogue n'apparaîtra plus. Dans la partie inférieure de la boîte sont disposés trois boutons **OK** (valider les actions sélectionnées), **Annuler** (fermer la fenêtre et continuer la procédure d'analyse) et **Stop** (arrêter la procédure d'analyse).

⊙ **Rapport uniquement** – en cas de détection d'objets infectés ou suspects, le programme ne fera que vous informer. Le rapport de vérification peut être visualisé en lançant le programme de consultation des rapports Kaspersky® Report Viewer (voir chap. Chapitre 7).

⊙ **Désinfecter** – tenter de réparer tous les objets infectés sans demande préalable. A la suite de la réparation de l'objet infecté, les virus seront supprimés et l'objet lui-même restauré et remis en état de travailler.

☑ **Faire une sauvegarde du fichier avant désinfection** – avant le début de la réparation, créer une copie de l'objet infecté. Le répertoire dans lequel sera créée la copie est indiqué dans

l'arborescence des réglages de la catégorie **Paramètres** (voir p. 3.3.2.2). Après la réparation la copie n'est pas supprimée.

- **Si la désinfection est impossible** –les objets infectés ne peuvent pas tous être réparés car certains virus endommagent irréversiblement les informations stockées dans l'ordinateur. Dans ce cas, le programme Kaspersky AV Scanner peut agir en utilisant un des trois procédés suivants: ⊙ **Rapport uniquement** – informer de la tentative infructueuse de réparation, ⊙ **Renommer l'objet** – renommer le fichier qui n'a pu être réparé, ⊙ **Effacer l'objet** – supprimer le fichier endommagé.

- ⊙ **Renommer l'objet** – renommer tous les objets infectés. Les règles de renomination sont définies dans l'arborescence des réglages de la catégorie **Options** (voir p. 3.3.2.2).
- ⊙ **Effacer l'objet** – supprimer tous les objets infectés sans avis préventif.

Pour identifier les archives infectées, les règles **Effacer l'objet** et **Renommer l'objet** ne fonctionneront que si l'option **Autoriser l'effacement ou le changement de nom des archives infectées** de l'onglet **Options** a été cochée. Dans le cas contraire, l'action sélectionnée – Effacer ou Renommer – ne sera pas exécutée.

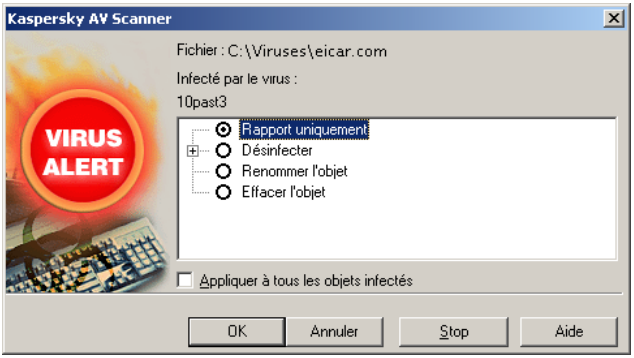


Illustration 6. de demande d'actions en cas d'infection

3.3.1.3. Modes complémentaires d'analyse

3.3.1.3.1. Analyse de fichiers spéciaux

Vous pouvez activer les modes complémentaires – d'analyse des archives, des fichiers compressés, des bases de messagerie e-mail et des fichiers aux formats

e-mail, des pièces jointes. Tous ces modes sont rassemblés dans un seul groupe:

- ☑ **Analyser les fichiers spéciaux** – traiter les objets complexes comme des dossiers contenant un jeu d'objets.

Il peut arriver que le logiciel détecte un virus dans un fichier complexe (archive, base de données de messagerie ou message) mais ne soit pas en mesure de le supprimer. Par conséquent, lorsque vous exécutez le logiciel avec les options **Supprimer les objets** ou **Renommer l'objet** sélectionnées, il est également conseillé de cocher la case ☑ **Analyser les objets complexes de types suivants** et de décocher la case ☑ **Autoriser l'effacement ou le changement de nom des fichiers complexes infectés** de l'onglet **Options**. Dans ce cas, en cas de détection d'un fichier complexe infecté, le logiciel enregistre cet événement, sans supprimer ou renommer le fichier. Par la suite, lorsque vous serez en mesure d'extraire l'objet, utilisez le logiciel anti-virus pour analyser et supprimer le virus des fichiers extraits.

Si vous cochez la case ☑ **Autoriser l'effacement ou le changement de nom des fichiers complexes infectés**, vous risquez de perdre des informations qu'il serait possible de récupérer.

3.3.1.3.2. Analyse des archives et des fichiers auto-extractibles

La détection de virus dans les archives est une tâche très importante, dans la mesure où un virus peut rester stocké dans un fichier archivé pendant plusieurs mois, voire plusieurs années, sans causer de dommages pour ensuite se propager rapidement et provoquer une masse de désagréments.

- ☑ **Archives** – rechercher les virus dans les fichiers d'archives créés par les archiveurs ZIP, ARJ, LHA, RAR, CAB et autres.

Kaspersky Anti-Virus® ne supprime pas les virus des archives mais ne fait que les détecter. En outre, Kaspersky Anti-Virus® ne décompresse pas les archives protégées par un mot de passe.

Dans le travail avec les archives il est donc conseillé de cocher la case ☑ **Archives** et de désactiver la case ☑ **Autoriser l'effacement ou le changement de nom des archives infectées** dans l'onglet **Options**, si en qualité d'action sur les objets infectés vous avez choisi de les supprimer ou de les renommer. Dans ce cas, si dans une archive un fichier infecté est découvert, une inscription appropriée sera insérée dans le rapport, mais l'archive ne sera ni supprimée ni renommée. Vous pourrez la décompresser, lancer ensuite la procédure d'analyse et supprimer les virus des fichiers extraits.

Si la case ☑ **Autoriser l'effacement ou le changement de nom des archives infectées** est cochée, vous risquez de perdre des informations qu'il serait possible de récupérer.

☑ **Archives auto-extractibles** – rechercher les virus dans les archives auto-extractibles, c'est-à-dire dans des fichiers exécutables, qui lors de leur lancement, se décompressent automatiquement. Certaines archives auto-extractibles sont conçues pour lancer aussitôt l'exécution d'un des fichiers décompressées.

Le mécanisme de décompression fonctionne correctement avec les fichiers comprimés plusieurs fois. Il fonctionne également avec certaines versions d'immuniseurs de fichiers, c.-à-d. de programmes protégeant les fichiers exécutables contre les infections via l'adjonction à ces derniers de blocs de contrôle (CPAV et F-XLOCK), ainsi que des programmes de cryptage (CryptCOM).

3.3.1.3.3. Analyse des bases de données de messageries e-mail et des fichiers aux formats e-mail

Le programme peut vérifier les bases de données des messageries e-mail et les fichiers aux formats e-mail.

☑ **Bases de courrier** – analyser les bases de données des messageries e-mail. Sont vérifiées les bases de données des messageries e-mail aux formats suivants:

- Microsoft Outlook, Microsoft Exchange (fichiers *.pst et *.pab, type d'archive MS Mail)
- Microsoft Internet Mail (fichiers *.mbx, type d'archive MS Internet Mail)
- Eudora Pro & Lite
- Pegasus Mail
- Netscape Navigator Mail
- JSMail SMTP/POP3 server (base de données définie par les utilisateurs).

En mode de vérification des bases de données de messageries e-mail, le programme vérifiera chaque inscription dans les bases de la messagerie électronique ainsi que les fichiers joints. Les formats supportés sont: UUEncode ; XXEncode ; btoa (jusqu'à 5.0); btoa 5.*; BinHex 4.0; ship; NETRUN 3.10 ; NETSEND 1.0 (non compressé) ; NETSEND 1.0C (compressé) ; MIME base64.

☑ **Tous formats de courrier** – analyser les fichiers e-mail aux formats Eudora Pro & Lite, Pegasus Mail, Netscape Navigator Mail, JSMail, la base définie par les utilisateurs du serveur SMTP/POP3.

En mode d'analyse des fichiers aux formats texte e-mail, l'Anti-Virus Kaspersky® vérifie dans chaque fichier la présence de préambule de courrier électronique et, en cas de détection de préambule, recherche les données associées (UUEncode, XXEncode, etc.) et les soumet à une vérification anti-virus.

Lors de l'activation du mode d'analyse des bases de données e-mail et, surtout, du mode d'analyse des fichiers aux formats texte e-mail, la vitesse de travail de Kaspersky AV Scanner peut diminuer. C'est pourquoi nous vous conseillons d'utiliser ces modes lors des vérifications habituelles de tous les fichiers de vos ordinateurs.

Kaspersky AV Scanner ne supprime pas les virus des bases de données e-mail et des fichiers aux formats texte e-mail, mais ne fait que les détecter. Cependant, en mode spécial d'analyse ☑ Analyser les bases MS Outlook Express, le programme détecte et supprime les virus des bases de données des versions MS Outlook Express 5.0 et supérieures.

3.3.1.3.4. Analyse des pièces jointes

Le programme permet d'analyser non seulement les fichiers mais également les pièces jointes à ces derniers selon la technologie OLE. Cochez la case ☑ **Objets OLE2 inclus** – pour analyser les objets OLE joints aux fichiers vérifiés.

3.3.1.3.5. Analyseur heuristique

Vous pouvez activer le mode d'analyse heuristique des fichiers pour détecter les virus encore inconnus dans le programme (non recensés dans les bases Anti-Virus). Cochez la case ☑ **Autoriser l'analyse du code (heuristique)** – pour activer la vérification par l'analyseur heuristique.

3.3.2. Paramètres généraux - Catégorie Options

La catégorie **Options** (Illustration 7) contient les paramètres s'appliquant à l'enregistrement des résultats de l'analyse dans le fichier, les réglages de modification du nom des fichiers infectés et le niveau de priorité de l'analyse.

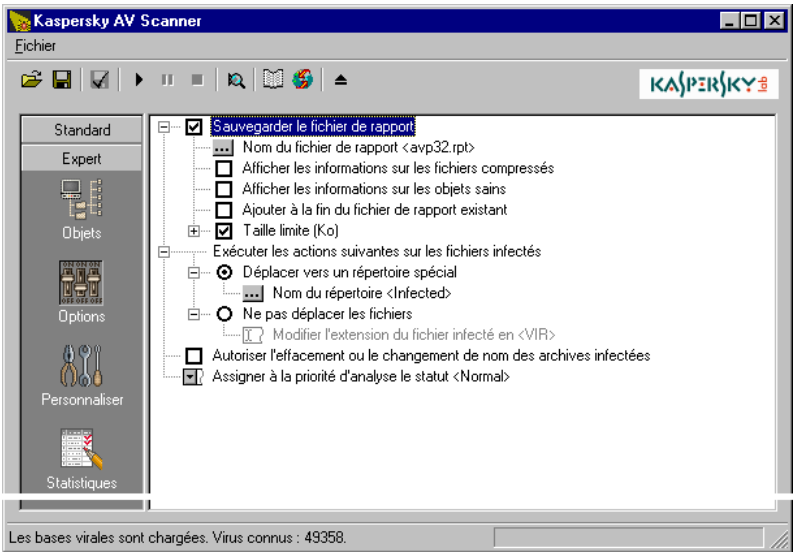


Illustration 7. Catégorie Options

3.3.2.1. Paramètres de tenue du rapport

☑ **Sauvegarder le fichier de rapport** – sauvegarder le rapport dans un fichier. En activant ce commutateur, vous pourrez suivre l'évolution du travail du programme Kaspersky AV Scanner à l'aide du programme Kaspersky® Report Viewer (voir chapitre Chapitre 7). Lors de l'affichage des résultats, ce programme utilisera tous les réglages de la ramification **Sauvegarder le fichier de rapport**.

… **Nom du fichier de rapport** – préciser le nom du fichier contenant le rapport.

Le rapport est créé par défaut dans le répertoire qui est présélectionné lors de l'installation du programme. Si le programme fonctionne sans liaison avec Kaspersky AV Control Centre, vous pouvez changer de répertoire en indiquant le chemin d'accès complet du fichier de rapport. Il est impossible autrement de modifier le chemin d'accès utilisé par défaut.

☑ **Afficher les informations sur les fichiers compressés** – faire apparaître dans le rapport les informations sur les fichiers compressés. Les informations apparaîtront dans le tableau Kaspersky® Report Viewer sous la forme suivante:

- dans la colonne **Objet** – le nom de l'objet,
- dans la colonne **Résultat** – l'inscription **Compressé** ou **Archive**,

• dans la colonne **Description** – le programme de compression / d'archivage.

☑ **Afficher les informations sur les objets sains** – faire apparaître dans le rapport l'information sur les objets non infectés. Les informations apparaîtront dans le tableau Kaspersky® Report Viewer sous la forme suivante:

- dans la colonne **Objet** – le nom de l'objet,
- dans la colonne **Résultat** – l'inscription **OK**.

☑ **Ajouter à la fin du fichier de rapport existant** – ajouter les résultats de la vérification au fichier de rapport déjà existant. Ainsi, vous pourrez sauvegarder tous les résultats des vérifications antérieures. Si vous désactivez ce commutateur, à chaque lancement du scanner, un nouveau fichier de rapport sera créé.

☑ **Taille limite (Ko)** – limiter la taille du fichier à la valeur indiquée dans la zone d'édition. Par défaut, la valeur utilisée sera 2048 Ko.

3.3.2.2. Paramètres de changement de nom, de copie et de suppression des objets

Exécuter les actions suivantes sur les fichiers infectés – le groupe de boutons de choix qui indique le traitement appliqué aux objets infectés.
Le programme applique ce procédé lors du traitement des objets auxquels on a assigné l'action **Renommer l'objet** dans l'arborescence des réglages de la catégorie **Objets** (voir sous-chapitre. 3.3.2.2).

⊙ **Déplacer vers un répertoire spécial** – transférer les objets infectés dans le répertoire spécial indiqué dans le champ disposé sous le bouton de choix. Avec ce procédé, les fichiers infectés sont transférés dans un répertoire spécial sans changement de nom ni d'extension.

⊙ **Ne pas déplacer les objets** – laisser les objets infectés dans les anciens répertoires mais changer leur extension dans le champ indiqué **Modifier l'extension du fichier infecté en**.

☑ **Autoriser l'effacement ou le changement de nom des fichiers complexes infectés** – si pour les fichiers infectés dans l'onglet **Objets** la règle **Supprimer l'objet** ou **Renommer l'objet** a été fixée, pour les archives infectées cette règle n'agira que si le mode approprié a été activé. Il est déconseillé de cocher cette case si vous ne disposez pas d'un quelconque système de copies de sauvegarde permettant de récupérer les données.

3.3.2.3. Priorité de la procédure d'analyse

Assigner à la priorité de la procédure d'analyse le statut – vous pouvez sélectionner dans la liste une des trois valeurs suivantes:

- **Elevé** – priorité élevée: le système d'exploitation privilégie le Kaspersky AV Scanner en lui donnant le contrôle plus souvent et pour une durée plus longue qu'aux autres applications lancées,
- **Normal** – priorité normale: le processeur attribue au contrôle du Kaspersky AV Scanner une priorité équivalente à celle accordée aux autres applications lancées,
- **Faible** – priorité faible: n'importe quelle application lancée prend le pas sur le Kaspersky AV Scanner.

3.3.3. Réglages complémentaires - Catégorie Personnaliser

La catégorie **Personnaliser** (Illustration 8) contient les paramètres complémentaires régissant le fonctionnement du programme.

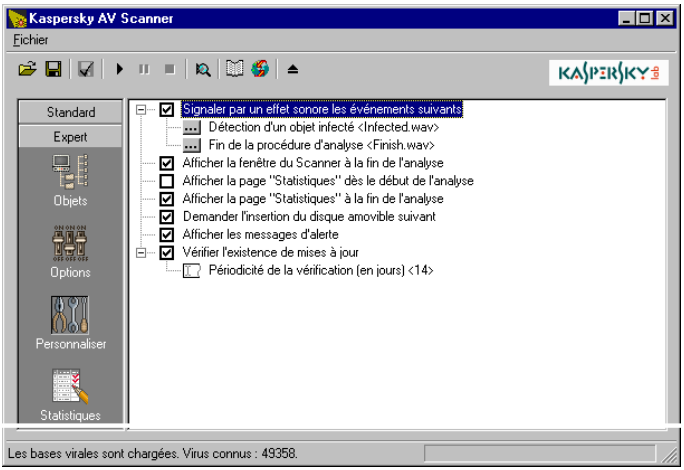


Illustration 8 Catégorie Personnaliser

Signaler par un effet sonore les événements suivants – accompagner certains événements d'une alarme diffusée sous la forme d'un fichier son.

- **Détection d'un objet infecté** – nom du fichier son diffusé lors de la détection d'un objet infecté. Dans la fenêtre contenant la liste des fichiers, vous pouvez écouter le signal sonore en cliquant sur le bouton **Test**.
- **Fin de la procédure d'analyse** – nom du fichier son diffusé à la fin de l'analyse. Dans la fenêtre contenant la liste des fichiers, vous pouvez écouter le signal sonore en cliquant sur le bouton **Test**.

☑ **Afficher la fenêtre du Scanner à la fin de l'analyse** – consulter les résultats dès que le programme a terminé son travail. Si la fenêtre principale du Kaspersky AV Scanner était fermée et que vous avez lancé l'analyse depuis le menu système, à la fin de l'analyse, la fenêtre principale sera fermée.

☑ **Afficher la page "Statistiques" dès le début de l'analyse** – après le lancement de l'analyse, basculer automatiquement vers la catégorie **Statistiques** pour surveiller l'activité du programme.

☑ **Afficher la page "Statistiques" à la fin de l'analyse** – à la fin de l'analyse, basculer automatiquement vers la catégorie **Statistiques** pour consulter les résultats.

☑ **Demander l'insertion du disque amovible suivant** – afficher la boîte de dialogue demandant l'insertion du disque amovible suivant, afin de le vérifier. Si habituellement, vous ne vérifiez qu'un seul disque, il est alors plus pratique de désactiver cette option.

☑ **Afficher les messages d'alerte** – afficher les autres messages d'alerte.

☑ **Vérifier l'existence de mises à jour** – lancer automatiquement le programme de mise à jour des bases de données anti-virus par le biais du nombre de jours indiqués dans la fenêtre d'édition **Périodicité de la vérification** (en jours) (la fenêtre d'édition devient active lorsque l'on coche cette case).

Si vous consultez les propriétés du programme à partir de Kaspersky AV Control Centre, certains réglages de la catégorie **Personnaliser**, qui n'ont pas de sens lorsque le programme travaille conjointement avec le Control Centre, sont absents de l'arborescence des réglages.

3.3.4. Fichier de réglages: sauvegarde/chargement des paramètres

Les jeux de paramètres de Kaspersky AV Scanner peuvent être stockés sur le disque dur dans les fichiers de réglages pour pouvoir consécutivement les charger en vue de l'exécution par le programme de certaines actions. Ceux-ci peuvent être rechargés par la suite pour piloter l'exécution de certaines actions

par le scanner. Ainsi, vous pouvez enregistrer un jeu sous le nom **Vérification des disques amovibles** et l'utiliser pour la vérification de plusieurs disquettes, enregistrer un autre jeu sous le nom **Vérification complète de tous les disques** et l'utiliser pour déclencher la vérification heuristique de tous les fichiers, en cas de suspicion de pénétration de virus dans votre ordinateur, etc.

Vous pouvez affecter un des fichiers de réglages aux paramètres chargés par défaut. Dans ce cas, à chaque lancement du Kaspersky AV Scanner, les réglages seront amorcés à partir du fichier de réglage.

	Menu principal	**Barre d'outils**	**Clavier**
Chargement des paramètres	Fichier → Charger un profil		<Ctrl>+<O>
Sauvegarde des paramètres	Fichier → Sauvegarder le profil Fichier → Sauvegarder le profil sous		<Ctrl>+<S>
Attribution des paramètres actuels aux valeurs par défaut	Fichier → Sauvegarder comme profil par défaut		

Par défaut, les fichiers de réglages ont une extension **.klr**.

Si, lors du lancement, aucun des fichiers de réglages n'est affecté comme fichier par défaut, le scanner utilise les réglages inclus dans le code du programme.

3.3.5. Consultation préalable des paramètres avant le début de l'analyse

Les paramètres de l'analyse peuvent être consultés sous la forme d'un texte exposant les règles de traitement s'appliquant à tous les objets du système de fichiers: du **Poste de travail** jusqu'à chaque fichier en particulier. Par exemple, si dans le fichier **autoexec.bat** les règles ne sont pas les mêmes que celles de l'objet ascendant **Disque Système (C:)**, la liste des règles relatives au fichier sera affichée séparément.

Pour consulter les différents paramètres de l'analyse sous la forme de texte, sélectionnez dans le menu **Fichier** la commande **Consulter les paramètres de l'analyse** ou cliquez sur bouton  de la barre d'outils.

Vous voyez alors apparaître la fenêtre **Options d'analyse** (Illustration 9), contenant les valeurs choisies pour les paramètres des catégories **Objets** et **Options**. Vous pouvez consulter et copier les valeurs des paramètres. Pour terminer le travail avec ces valeurs, cliquez sur le bouton **OK**.

Les paramètres d'analyse présentés sous forme de texte cohérent s'inscrivent aussi au début du fichier de rapport.

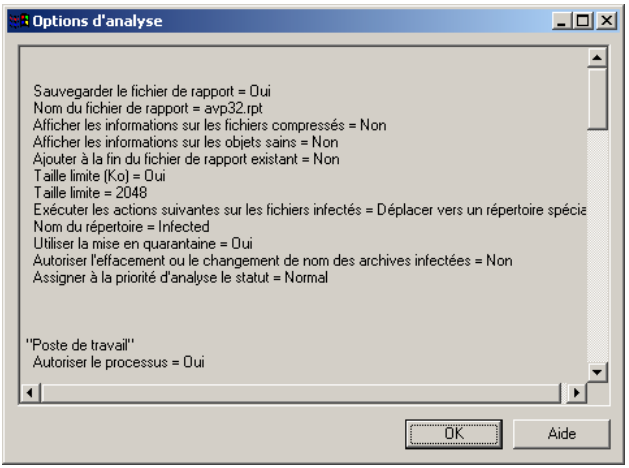


Illustration 9. Fenêtre Options d'analyse

3.4. Détection et éradication des virus

3.4.1. Lancement et arrêt de l'analyse

L'analyse peut être lancée et arrêtée soit en mode automatique, soit en mode manuel par le biais du programme Kaspersky AV Control Centre, soit en mode manuel Kaspersky AV Control Centre, soit encore à la main depuis la fenêtre principale de Kaspersky AV Scanner.

Après le début de l'analyse, vous pouvez interrompre ou reprendre la procédure d'analyse, modifier sa priorité ou stopper l'analyse.

	Menu principal	**Menu contextuel**	**Barre d'outils**
Lancement	Analyse → Démarrer l'analyse	Démarrer l'analyse	
Stopper	Analyse → Stopper l'analyse	Stopper l'analyse	
Interrompre	Analyse → Interrompre l'analyse	Interrompre l'analyse	
Reprendre	Analyse → Reprendre l'analyse	Reprendre l'analyse	

Examinons les actions les actions initiales que le scanner anti-virus exécute dès son lancement. Il charge les bases de données anti-virus et s'auto-analyse. Si le chargement s'est effectué avec succès, un message s'affiche dans la ligne inférieure de la fenêtre du programme:

```
Les bases virales sont chargées. Virus connus: XXXX
```

XXXX indique le nombre de virus connus, et en cas d'infection du programme lui-même, une tentative de réparation est effectuée. Si celle-ci est effectuée avec succès, le programme sera relancé et l'écran affichera un message d'information indiquant que les virus ont été éradiqués. Si la réparation s'avère impossible, le programme ne sera pas lancé et une fenêtre d'information appropriée s'ouvrira.

Si vous disposez d'une version enregistrée de Kaspersky Anti-Virus®, supprimez la copie infectée et réinstallez le programme.

Après l'analyse, le scanner anti-virus affiche des codes que vous pouvez utiliser lors de la création de procédures de traitement automatisé. Le scanner peut retourner une des valeurs suivantes:

- **0** – aucun virus détecté
- **1** – analyse non terminée
- **2** – objets détectés contenant un virus modifié ou endommagé
- **3** – objets détectés susceptibles d'être infectés par un virus
- **4** – virus connu détecté
- **5** – tous les virus détectés ont été éradiqués

- **7** – le programme Kaspersky AV Scanner est endommagé
- **10** – erreur interne du programme Kaspersky AV Scanner

3.4.2. Modification de la priorité de l'analyse

Vous pouvez modifier la priorité de la procédure d'analyse sans l'arrêter. Pour ce faire

1. Sélectionnez dans le menu **Analyse** la commande **Définir la priorité d'analyse**.
2. Dans la boîte de dialogue qui apparaît (Illustration 10), sélectionnez dans la liste déroulante une des trois valeurs de priorité: **Elevé**, **Normal** ou **Faible** (pour plus de détails, voir paragraphe 3.3.2.3)

Illustration 10. de sélection de la priorité d'analyse

Vous ne pouvez pas modifier les autres paramètres en cours d'analyse! Pour modifier les paramètres, arrêtez d'abord la procédure d'analyse puis changez les réglages. Après cela, vous pourrez relancer la procédure d'analyse.

3.4.3. Suivi du rapport

Si vous avez activé les paramètres de tenue du rapport (voir paragraphe 3.3.2.1), vous avez la possibilité de suivre le travail du Kaspersky AV

Scanner à l'aide du module Kaspersky® Report Viewer. Pour lancer ce programme, sélectionnez dans le menu **Outils** la commande **Voir le rapport** ou cliquez sur le bouton  de la barre d'outils. Vous faites ainsi apparaître la fenêtre principale du programme Kaspersky® Report Viewer, où vous pouvez consulter les messages sur l'analyse (voir chapitre Chapitre 7).

3.4.4. Consultation des statistiques - Catégorie Statistiques

Si vous n'avez pas activé les paramètres de tenue du rapport, vous pourrez suivre le changement intervenant dans les statistiques dans le tableau de la catégorie **Statistiques** (Illustration 11).

Le tableau est divisé en deux parties: **Analysés** et **Détectés**. La partie supérieure **Analysés** contient le nombre de secteurs ciblés, fichiers, répertoires, archives et fichiers compressés ayant été vérifiés.

La partie inférieure **Détectés** contient le nombre de:

- virus connus
- occurrences de virus (nombre de fichiers infectés par tel ou tel virus connu)
- objets désinfectés (objets d'où les virus ont été correctement éradiqués)
- objets effacés
- objets renommés
- objets mis en quarantaine
- messages d'alerte (messages sur le nombre d'objets contenant un code ressemblant à une variante de virus connu)
- suspects (messages de l'analyseur du code)
- objets endommagés
- problèmes d'entrée/sortie.

Dans sa partie inférieure, le tableau affiche la vitesse de travail (en Ko/s) et la durée globale de vérification de tous les objets.

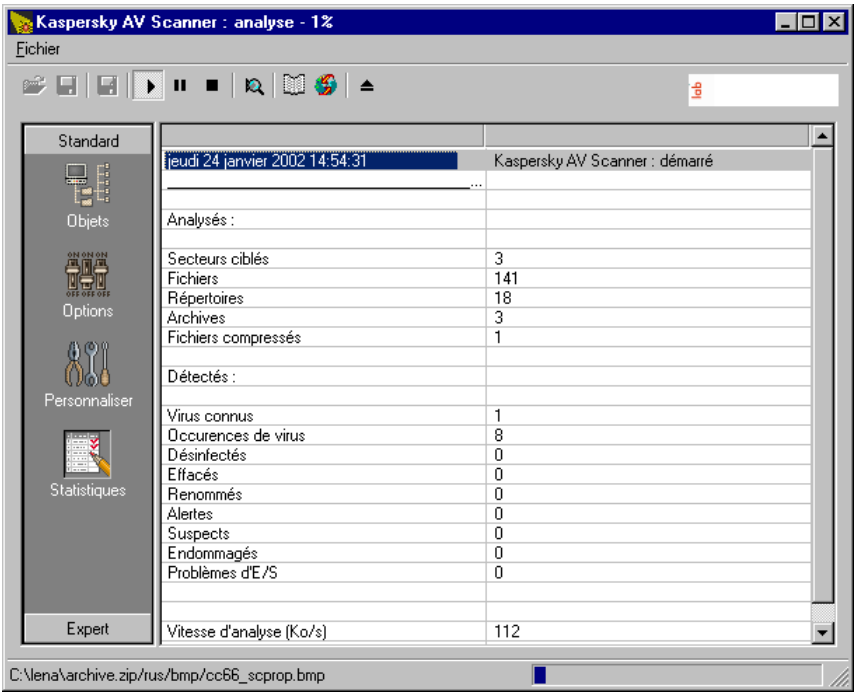


Illustration 11. Catégorie Statistiques

3.5. Lancement de la mise à jour des bases

Vous pouvez lancer le programme de mise à jour des bases anti-virus depuis la fenêtre principale du programme Kaspersky AV Scanner. Pour ce faire, sélectionnez dans le menu **Outils** la commande **Mettre à jour** ou cliquez sur le bouton  de la barre d'outils.

3.6. Création de la liste des virus connus

Vous pouvez consulter la liste de tous les virus connus du programme à l'heure actuelle. A cette fin

1. Sélectionnez dans le menu **Outils** la commande **Créer la liste des virus**. Après quoi le programme **Kaspersky® Virus List Generator** sera lancé.
2. Dans la boîte de dialogue **Kaspersky® Virus List Generator** (Illustration 12) qui vient de s'ouvrir spécifiez le nom du fichier dans lequel sera enregistrée la liste des virus. A cette fin, cliquez sur le bouton **Parcourir** et indiquez le nom du fichier.
3. Cliquez sur le bouton **Créer**.

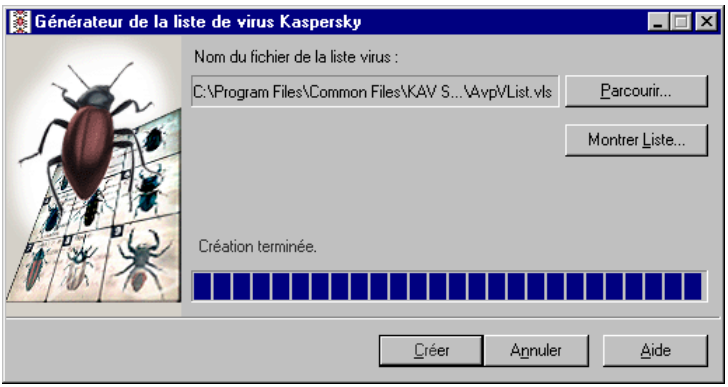


Illustration 12. Générateur de la liste de virus Kaspersky®

Pour consulter la liste, cliquez sur le bouton **Montrer Liste**.Le programme Report Viewer, à l'aide duquel vous pourrez consulter la liste créée, est lancé.

Pour fermer la boîte de dialogue **Générateur de la liste de virus Kaspersky®**, cliquez sur le bouton **Annuler**.

Vous pouvez lancer le programme **Générateur de la liste de virus Kaspersky®** en mode autonome. Pour cela, cliquez sur le bouton **Démarrer** de Windows, puis passez dans le sous-menu **Programmes**, et ensuite dans le groupe **Kaspersky Anti-Virus®** lancez la commande **Générateur de la liste de virus Kaspersky®**.

CHAPITRE 4. KASPERSKY ANTI-VIRUS® MONITOR

Le moteur d'analyse en temps réel Kaspersky Anti-Virus® Monitor (Kaspersky AV Monitor) est un programme chargé en permanence dans la mémoire vive de l'ordinateur et contrôlant les appels des fichiers et des secteurs (secteur principal d'amorçage [master boot] et secteurs d'amorçage [boot]). Avant d'autoriser l'accès à l'objet, Kaspersky AV Monitor vérifie que l'objet est exempt de virus. S'il en détecte un, il propose soit de désinfecter l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction de vos paramètres). Ainsi, Kaspersky AV Monitor permet de détecter et d'éradiquer les virus avant que le système soit réellement infecté.

Remarque: d'autres programmes analogues à ce module peuvent porter d'autres noms, comme par exemple: scanner résident, filtre anti-virus, scanner on access, etc.

4.1. Lancement et arrêt de Kaspersky AV Monitor

Il existe plusieurs procédés de lancement de Kaspersky AV Monitor:

Option 1 : Menu **Démarrer** de Windows. La méthode la plus rapide consiste à cliquer sur le bouton **Démarrer** et à sélectionner **Programmes**, à passer ensuite dans le groupe **Kaspersky Anti-Virus®** et à sélectionner l'item **Kaspersky Anti-Virus® Monitor**. Dans la barre des tâches s'affiche l'icône . En cliquant sur elle avec le bouton droit, vous pourrez dérouler le menu Système.

Option 2 : Groupe de **Démarrage.** Si, lors de l'installation de **Kaspersky Anti-Virus®** sur votre ordinateur, vous avez choisi d'ajouter Kaspersky Anti-Virus® Monitor dans le groupe de **Démarrage**, le programme sera lancé automatiquement aussitôt après l'initialisation de Windows.

Option 3 : Kaspersky AV Control Centre. Si vous avez installé le module Kaspersky AV Control Centre et défini dans les réglages le lancement automatique de Kaspersky Anti-Virus® Monitor, celui-ci sera lancé automatiquement aussitôt après le démarrage du module Kaspersky AV Control Centre. Mais dans ce cas, l'icône de Kaspersky AV Monitor ne s'affichera pas dans la barre des tâches.

Option 4 : Ligne de commande. Enfin, il est possible de lancer Kaspersky AV Monitor depuis la ligne de commande. Pour ce faire, vous devez ouvrir le dossier

dans lequel Kaspersky Anti-Virus® est installé et lancer ensuite le programme **avpm.exe**.

Les signes indiquant l'activation de Kaspersky AV Monitor sont les suivants:

- l'icône  .est affichée dans la barre des tâches
- en pointant avec la souris sur l'icône  , on fait surgir une bulle d'aide indiquant: **Kaspersky AV Monitor activé**
- le menu de la barre des tâches contient la commande Désactiver.
- Les signes indiquant que Kaspersky AV Monitor est désactivé sont les suivants:
- dans la barre des tâches s'affiche l'icône  .
- en pointant avec la souris sur l'icône  , on fait surgir une bulle d'aide indiquant: **Kaspersky AV Monitor désactivé**
- le menu de la barre des tâches contient la commande Activer.

Il est déconseillé d'utiliser sur le même ordinateur deux moniteurs antivirus distincts conçus par des sociétés différentes en raison des risques de conflits entre les deux modules et de fausses alertes.

Lors du lancement du moniteur depuis le module Kaspersky AV Control Centre, toutes ses options deviennent inaccessibles. Dans ce cas, il est indispensable de paramétrer Kaspersky Anti-Virus® Monitor par l'intermédiaire du module Kaspersky AV Control Centre !

4.2. Interface du programme

Cette section décrit l'interface Kaspersky AV Monitor interface, c'est à dire le menu système, la fenêtre principale, la zone de travail, etc.

Une fois activé, Kaspersky Anti-Virus® Monitor peut vous transmettre des messages en fonction de certains événements, par exemple, la détection d'un objet infecté. Il sera parfois nécessaire de répondre à ces messages. Si vous souhaitez terminer votre session sur l'ordinateur, refermez tous les messages avant de quitter la session.

4.2.1. Menu Système

Après le lancement du programme, l'écran affiche la fenêtre principale du programme (voir. sous-chapitre 3.2.2) et dans la barre des tâches apparaît l'icône  . En cliquant avec le bouton droit de la souris sur cette icône, vous pouvez ouvrir le menu contextuel (Illustration 13). Il comporte les options suivantes:

- **Configuration** – ouvrir la fenêtre principale du programme.
- **Désactiver le monitorage / Activer le monitorage** – activer/désactiver la fonction de monitorage.
- **Montrer le rapport** – afficher la fenêtre contenant le rapport sur les résultats de l'action du programme
- **Mettre à jour** – lancer le module Kaspersky AV Updater.
- **A propos de Kaspersky AV Monitor** – afficher la fenêtre contenant les principaux renseignements sur le programme.
- **Fermer** – décharger le programme de la mémoire.

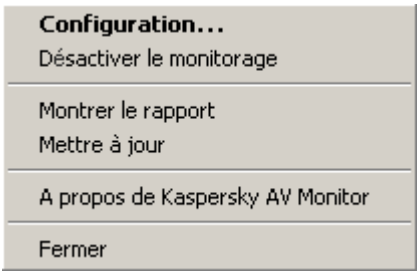


Illustration 13. Menu contextuel

4.2.2. Fenêtre principale

La fenêtre principale du programme Kaspersky AV Monitor sert à modifier les réglages du monitorage, à interrompre ou reprendre le monitorage et à consulter les résultats (Illustration 14). Vous pouvez fermer la fenêtre principale sans décharger le programme de la mémoire.

Dans la fenêtre principale du programme Kaspersky AV Monitor se trouvent:

- le menu
- la barre d'outils

- la zone de travail
- les boutons **OK, Annuler, Appliquer, Aide**.

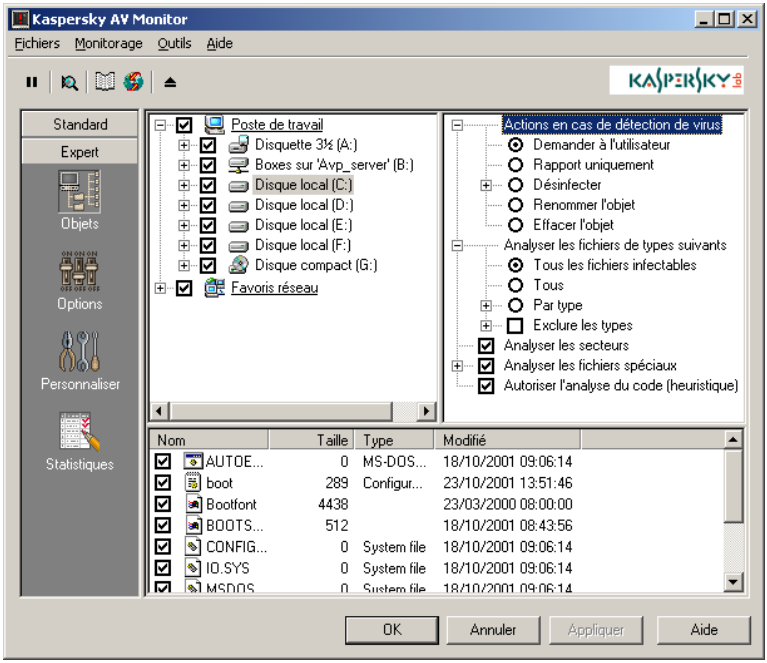


Illustration 14. Fenêtre principale du programme Kaspersky AV Monitor

4.2.3. Menus

Dans la partie supérieure de la fenêtre principale sont disposés les *menus*. Certaines commandes des menus sont accessibles par des raccourcis clavier ou par des boutons situés dans la barre d'outils. Les raccourcis clavier sont indiqués dans les menus à côté des options correspondantes. Un tableau regroupant toutes ces correspondances se trouve au sous-chapitre 4.2.4.

Commande du menu	**Fonction**
Fichier → Décharger Kaspersky Anti-Virus® Monitor	Eliminer le programme Kaspersky AV Monitor de la mémoire.
Fichier → Fermer la	Fermer la fenêtre principale du programme.

Commande du menu	Fonction
fenêtre	
Moniteur → Désactiver le monitorage / Activer le monitorage	Lancer / arrêter la procédure de monitorage (voir paragraphe 4.4).
Moniteur → Consulter les paramètres de monitorage	Montrer les paramètres sous la forme d'un texte (similaire au paragraphe 3.3.5).
Outils → Mettre à jour	Mettre à jour les bases de données anti-virus (voir paragraphe 3.5).
Outils → Montrer le rapport	Afficher la fenêtre contenant le rapport (voir paragraphe 3.4.3).
Outils → Créer la liste des virus	Générer la liste de tous les virus connus à la date actuelle (voir paragraphe 3.6).
Aide → Sommaire	Appeler le sommaire du fichier d'aide.
Aide → Site Web de Kaspersky AV	Ouvrir le navigateur Web et afficher la page d'accueil du site de la société Kaspersky Labs.
Aide → A propos du programme	Afficher des informations sur le programme.

4.2.4. Barre d'outils

Dans la *barre d'outils sont rassemblés les boutons* qui permettent, en cliquant sur ces derniers, d'initialiser telles ou telles actions.

Bouton	Menu	Fonction
	Monitorage → Désactiver / Activer le monitorage	Lancer / arrêter la procédure de monitorage
	Monitorage → Voir les options de monitorage	Montrer les paramètres sous la forme d'un texte.
	Outils → Mettre à jour les bases anti-virus	Lancer le programme de mise à jour des bases anti-virus.
	Outils → Montrer le rapport	Montrer la fenêtre de rapport.
	Fichier → Décharger Kaspersky Anti-Virus® Monitor	Eliminer le programme de la mémoire.

4.2.5. Zone d'intervention

La zone d'intervention de la fenêtre principale se compose de deux parties. Dans la partie gauche se trouve la liste des catégories et des icônes leur correspondant. Dans la partie droite est affiché le contenu des catégories. Il existe quatre catégories: **Objets, Options, Personnaliser et Statistiques**.

La catégorie **Objets** permet de définir la zone de monitorage, les objets devant être supervisés et les règles s'appliquant aux objets infectés. Tous ces réglages sont organisés au sein d'une arborescence hiérarchisée.

La catégorie **Options** offre la possibilité de définir les réglages généraux et la catégorie **Personnaliser** permet d'effectuer les réglages spéciaux du programme. Ces deux catégories font appel à une *arborescence* pour les réglages (voir paragraphes 3.3.2 et 3.3.3).

La catégorie **Statistiques** permet d'afficher les résultats du travail effectué par le programme dans un tableau (voir paragraphe 3.4.4).

Les éléments de l'arborescence des réglages sont dotés d'un *menu contextuel,* dont l'utilisation permet d'exécuter certaines opérations qui leur sont propres.

Pour appeler le menu contextuel d'un élément de l'arborescence des réglages,

1. Pointez avec la souris sur l'élément souhaité.

2. Cliquez avec le bouton droit de la souris. Cette opération déclenche l'apparition du menu contextuel de l'élément.

4.3. Réglage des paramètres du monitorage

Les paramètres de monitorage reprennent pratiquement en totalité les paramètres d'analyse (voir p. 3.3).

Les paramètres suivants constituent des exclusions: la catégorie **Objets** ne comporte pas les paramètres **Analyser les bases MS Outlook Express** et **Analyser les objets au démarrage du système**, et, par conséquent, il est impossible de monitorer les objets indiqués dans ces deux paramètres. Ceci veut dire qu'en mode de monitorage on ne peut pas réparer les bases de données e-mail. Cependant, le programme peut détecter dans ces bases de données un virus si les cases **Bases de courrier** et **Formats de courrier standard** sont cochées.

La catégorie **Options** ne comporte pas le paramètre **Définir la priorité de la procédure d'analyse**, car Kaspersky AV Monitor utilise des principes de travail distincts de ceux de Kaspersky AV Scanner. Le paramètre **Taille limite des fichiers spéciaux** analysés a été ajouté. Ce paramètre a été introduit afin de permettre, le cas échéant, l'accélérer le monitorage des archives trop volumineuses, etc. La **Taille limite** est entrée dans le champ numérique après l'activation du commutateur **Taille limite des fichiers spéciaux** (Ko).

Remarquez que dans cette version de Kaspersky Anti-Virus® Personal, Kaspersky AV Monitor analyse et désinfecte les archives au format ZIP.

La catégorie Personnaliser ne comporte pas les paramètres Montrer la fenêtre du Scanner après la fin de la procédure d'analyse, Ouvrir la page **Statistiques** après le début de la procédure d'analyse, Ouvrir la page **Statistiques** après la fin de la procédure d'analyse, Demander l'insertion du disque amovible suivant.

Si vous cochez les cases **Analyser les secteurs** et **Analyser la mémoire**, les secteurs et la mémoire seront vérifiés à une seule reprise, lors du lancement de la procédure de monitorage. En outre, le fait de cocher l'option **Analyser la mémoire** entraîne l'activation du mode de vérification de la mémoire des programmes lancés. Kaspersky AV Monitor exécute cette vérification aussitôt après le chargement et après chaque mise à jour des bases anti-virus dans l'ordinateur. Si la réparation de la mémoire infectée du programme est impossible, le programme concerné sera obligatoirement arrêté.

4.4. Monitorage

4.4.1. Lancement et arrêt du monitorage

Le monitorage peut être lancé et stoppé soit en mode automatique, à l'aide du programme Kaspersky AV Control Centre, soit en mode manuel, depuis ce même module Kaspersky AV Control Centre, soit, toujours en mode manuel, depuis la fenêtre principale de Kaspersky AV Monitor.

Après le début de l'analyse, vous pouvez interrompre et reprendre le monitorage.

	Menu principal	**Menu contextuel**	**Barre d'outils**
Arrêt	Monitorage → Désactiver le monitorage	Désactiver le monitorage	
Reprise	Monitorage → Activer le monitorage	Activer le monitorage	

4.4.2. Consultation des statistiques

Vous pouvez suivre l'évolution des statistiques dans le tableau de la catégorie **Statistiques** (Illustration 15).

Le tableau est divisé en deux parties: **Analysés** et **Détectés**. La partie supérieure **Analysés** contient le nombre de secteurs ciblés, fichiers, répertoires, archives et fichiers compressés ayant été vérifiés. La partie inférieure **Détectés** contient le nombre de:

- virus connus
- occurrences de virus (nombre de fichiers infectés par tel ou tel virus connu)
- objets désinfectés (objets d'où les virus ont été correctement éradiqués)
- objets effacés
- objets renommés
- objets mis en quarantaine

- messages d'alerte (messages sur le nombre d'objets contenant un code ressemblant à une variante de virus connu)
- suspects (messages de l'analyseur du code)
- objets endommagés
- problèmes d'entrée/sortie.

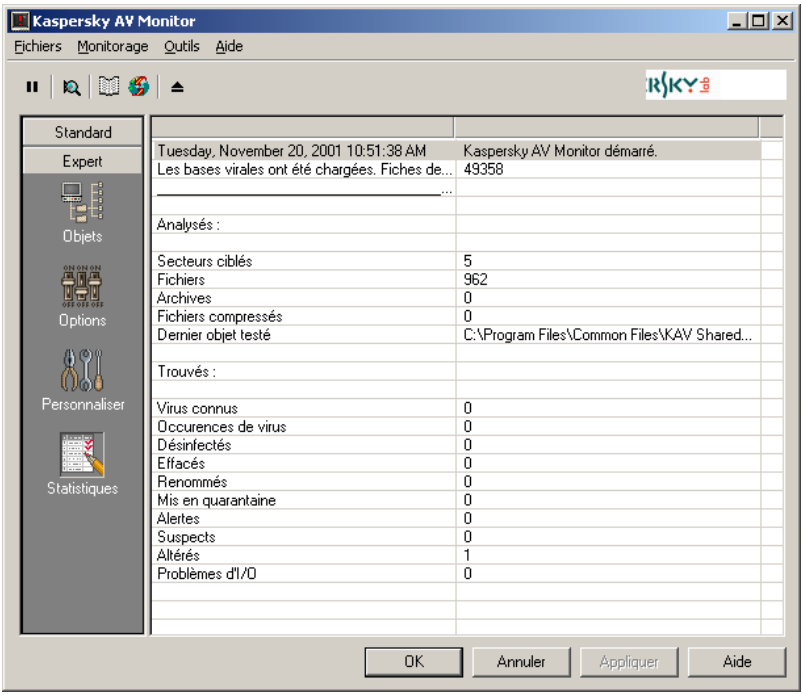


Illustration 15. Catégorie Statistiques

4.5. Lancement de la mise à jour des bases anti-virus

Vous pouvez lancer le programme de mise à jour des bases anti-virus depuis la fenêtre principale du programme Kaspersky AV Monitor. Pour ce faire, sélectionnez dans le menu **Outils** la commande **Mettre à jour les bases anti-virus** ou cliquez sur le bouton  de la barre d'outils.

CHAPITRE 5. KASPERSKY ANTI-VIRUS® UPDATER

Le programme Kaspersky Anti-Virus® Updater (Kaspersky AV Updater) fait partie du package Kaspersky Anti-Virus®. **Il se charge de** la mise à jour automatisée des bases de données anti-virus contenant la description des virus, des méthodes d'éradication de ces derniers ainsi que de composants du logiciel.

Kaspersky AV Updater effectue une copie des bases de données anti-virus et des exécutables soit par Internet (à partir d'un réseau ou d'une connexion distante), un dossier local ou un serveur antivirus géré par Kaspersky® Administration Kit.

5.1. Lancement du programme Kaspersky AV Updater

Il existe plusieurs procédés de lancement du programme de mise à jour, à savoir:

Option 1 : **menu Démarrer** de Windows. Pour lancer le programme Kaspersky AV Updater, cliquez sur le bouton **Démarrer** et sélectionnez **Programmes**, passez ensuite dans le groupe **Kaspersky Anti-Virus®** et sélectionnez l'item **Kaspersky Anti-Virus® Updater**.

Option 2 : **Kaspersky AV Control Centre.** Si vous avez installé le module Kaspersky AV Control Centre, il est possible de créer une tâche déclenchant le lancement automatique du programme Kaspersky AV Updater (pour plus de détails sur le module Kaspersky AV Control Centre, voir le chapitre).

Option 3 : ligne de commande. Il est également possible de lancer le programme depuis la ligne de commande. Pour ce faire, localisez le dossier commun de Kaspersky Anti-Virus® **(généralement KAV Shared Files)**, ouvrez ensuite le fichier avpupd.exe. Le dossier commun peut, par exemple, être accessible par le chemin: **C:\Program Files\Fichiers communs\KAV Shared Files**.

5.2. Description de l'interface du programme Kaspersky AV Updater

L'interface du programme Kaspersky AV Updater se présente sous la forme d'un assistant composé d'une succession de fenêtres (étapes) entre lesquelles on bascule en cliquant sur les boutons Préc. et Suivant. Pour terminer la mise à jour, on clique sur le bouton Terminer. Pour arrêter le travail du programme à n'importe quel stade, on utilise le bouton Annuler.

Dans la partie centrale de chaque fenêtre se trouve l'élément Tree-Chart (pour plus de détails sur la façon de l'utiliser, voir le chapitre Chapitre 8). Cet élément de contrôle permet de définir les paramètres en utilisant une arborescence hiérarchique.

5.2.1. Etape 1: Fenêtre 1 de l'assistant de Kaspersky AV Updater

Aussitôt après le lancement du programme Kaspersky AV Updater s'ouvre la première fenêtre de l'assistant: **Bienvenue dans l'assistant de Kaspersky AV Updater** (Illustration 16). Dans le cas contraire, les étapes suivantes seront omises

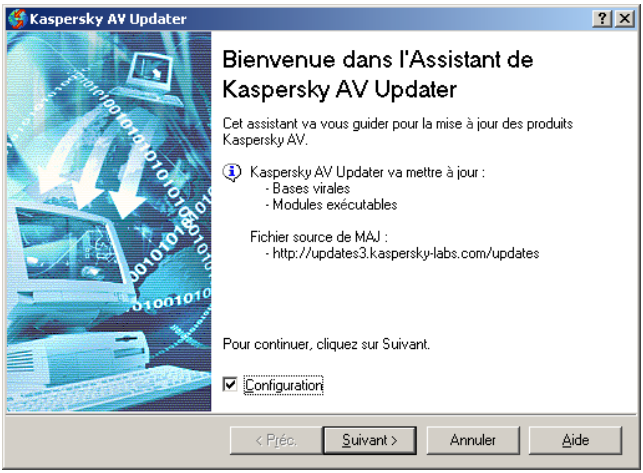


Illustration 16. Fenêtre de Bienvenue de l'Assistant de Kaspersky AV Updater

5.2.2. Etape 2: Fenêtre Connexion

S'il s'avère nécessaire de modifier les réglages prédéfinis par défaut, vous pouvez le faire dans la fenêtre Connexion (Illustration 17).

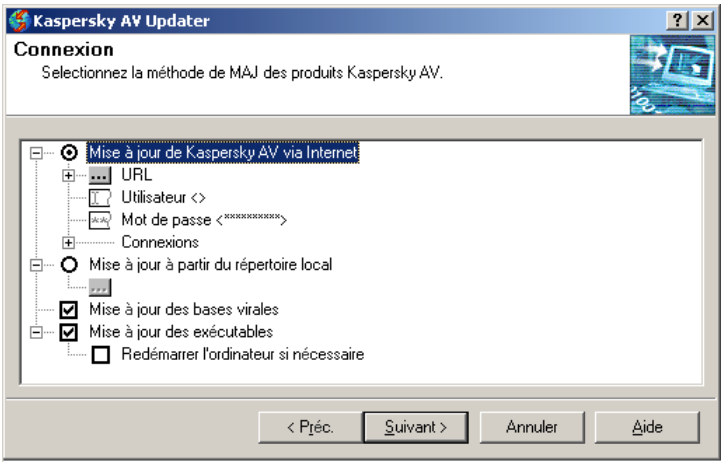


Illustration 17. Fenêtre Connexion

La fenêtre **Connexion** permet de définir le procédé et l'objet de la mise à jour.

Examinons le rôle de chaque commande au premier niveau de l'arborescence dans l'élément de contrôle **tree-chart** (Illustration 18):

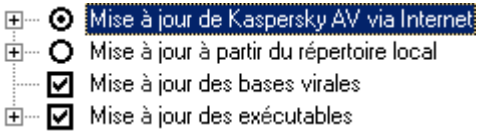


Illustration 18. Premier niveau de l'arborescence des réglages.

- **Mise à jour de Kaspersky AV via Internet** – procéder à la mise à jour via **Internet**.
- **Mise à jour depuis le répertoire local** – procéder à la mise à jour depuis un dossier local.
- **Mise à jour des bases virales** – procéder à la mise à jour des bases de données anti-virus.
- **Mise à jour des exécutables** – procéder à la mise à jour des modules exécutables du package Kaspersky Anti-Virus®.

☑ **Redémarrer l'ordinateur si nécessaire** – redémarrer l'ordinateur si nécessaire après la mise à jour des modules exécutables du logiciel.

Après le réglage des paramètres dans cette fenêtre, cliquez sur le bouton **Suivant**.

5.2.2.1. Paramétrage de la mise à jour via Internet

S vous avez choisi la mise à jour via Internet, il est indispensable de procéder au réglage de ce mode (

Illustration 19). Examinons les différents options de réglages dans cette partie de l'arborescence:

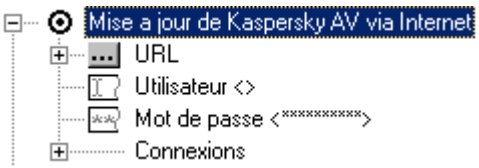


Illustration 19. Mise à jour via Internet

URL – Réglage de la source de mise à jour (protocole, nom du serveur, etc.)

Connexions – Réglage des paramètres de connexion avec un serveur à distance.

Mot de passé – mot de passe pour l'accès au serveur de mises à jour.

Nom de l'utilisateur – nom de l'utilisateur pour l'accès au serveur de mises à jour.

Si Microsoft Internet Explorer fonctionne en mode déconnecté, le logiciel ne pourra pas être mis à jour par Internet, même si les paramètres de connexion ont été définis manuellement.

5.2.2.1.1. Réglage de l'adresse

Les mises à jours peuvent être effectuées depuis un des serveurs de mises à jour figurant dans la liste appropriée. Pour consulter cette liste, déployez la ramification des **URL** de l'arborescence des réglages (Illustration 20).

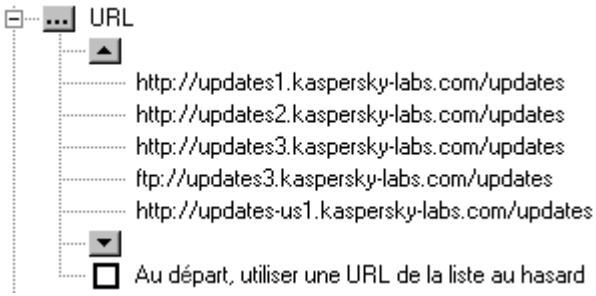


Illustration 20. Réglage de l'adresse du serveur de mises à jour

Lors de la mise à jour par défaut, on utilise l'adresse du premier serveur de mises à jour de la liste. En cas d'échec, on utilise le deuxième, etc. Le message d'erreur d'accès au serveur ne s'affiche à l'écran que si la connexion n'a pu être établie avec aucun serveur. Si vous activez l'option ☑ **Au départ, utiliser une URL de la liste au hasard**, un serveur choisi au hasard dans la liste sera utilisé comme premier serveur.

La liste des serveurs peut être éditée. A cette fin il convient de cliquer sur le bouton … **URL**, après quoi la fenêtre **Edition de la liste des URL** (Illustration 21) s'affichera à l'écran.

Pour travailler avec la liste des **URL,** on utilise les boutons suivants de la boîte de dialogue ou les commandes appropriées du menu contextuel:

– ajouter une nouvelle adresse à la liste

– éditer la liste courante des adresses

– supprimer la liste courante des adresses

– déplacer la liste courante des adresses d'une ligne vers le haut

– déplacer la liste courante des adresses d'une ligne vers le bas

OK – fermer la boîte de dialogue après avoir sauvegardé les modifications effectuées

Annuler – fermer la boîte de dialogue sans sauvegarder les modifications

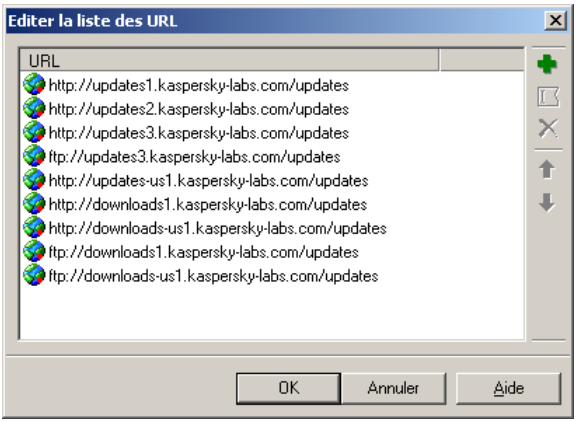


Illustration 21. Editer la liste des URL

5.2.2.1.2. Réglage des paramètres de connexion

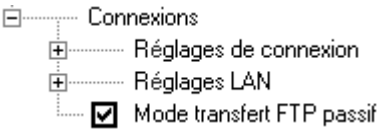


Illustration 22. Réglage de la connexion Internet

En fonction de la manière dont vous envisagez de réaliser la connexion avec le serveur de mise à jour, il est indispensable de régler les paramètres de connexion avec le fournisseur d'accès à Internet (Illustration 22), à savoir:

Réglages de connexion – régler la connexion à distance avec le fournisseur d'accès à Internet.

Réglage LAN – régler la connexion avec le fournisseur d'accès à Internet en utilisant le réseau local.

Mode transfert FTP passif – utiliser le mode passif pour le travail avec un serveur FTP (ceci vaut particulièrement pour les utilisateurs qui se connectent à un fournisseur d'accès à Internet via un serveur proxy ou un Firewall).

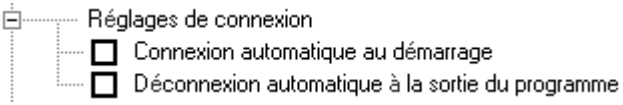


Illustration 23. Paramètres de l'accès à distance

Lors du réglage de la connexion à distance, on peut activer les cases suivantes (Illustration 23):

☑ **Connexion automatique au démarrage** – connexion automatique avec le fournisseur d'accès à Internet aussitôt après le lancement de la procédure de mise à jour

☑ **Déconnexion automatique à la sortie du programme** – raccrocher à la fin de la procédure de mise à jour.

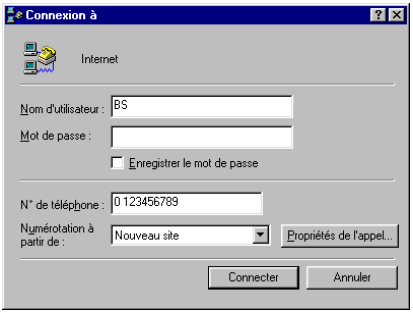


Illustration 24. **Connexion à**

Si vous avez choisi le mode de connexion à distance **avec le** fournisseur d'accès à Internet, avec appel automatique, après le lancement de la procédure de mise à jour, le programme appellera l'utilitaire standard d'accès à distance (si vous n'en avez pas installé d'autre).

Pour établir la connexion avec le fournisseur d'accès à Internet, remplissez la fenêtre Connexion à (Illustration 24) et cliquez sur le bouton Connecter. Après quoi, le serveur à distance sera appelé et la connexion établie.

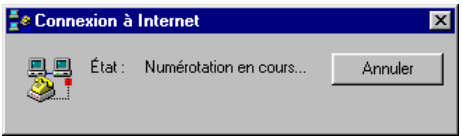


Illustration 25. **Connexion – Numérotation**

Lors de la procédure de connexion, la fenêtre Etablissement de la connexion avec le message Composition du numéro (Illustration 25) s'affiche à l'écran. Après l'établissement de la connexion, le nom et le mot de passe de l'utilisateur sont vérifiés.

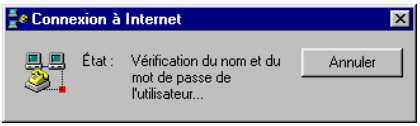


Illustration 26. **Connexion - Vérification**

Dans la ligne **Etat** s'affichera l'inscription **Vérification du nom et du mot de passe** de l'utilisateur… (Illustration 26).

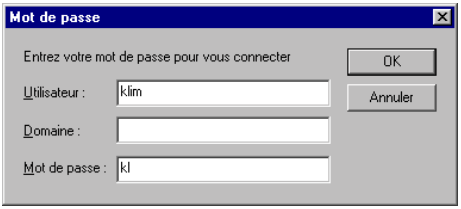


Illustration 27. **Mot de passe**

S'il est impossible d'identifier l'utilisateur en fonction des paramètres définis, l'écran affichera la boîte de dialogue **Mot de passe** (Illustration 27), dans les champs desquels il faut indiquer les différents paramètres: **Utilisateur, Domaine et Mot de passe**.

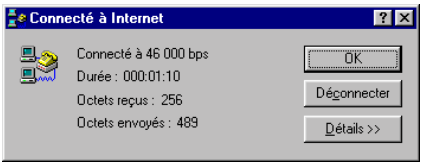


Illustration 28.
Paramètres de connexion

En cours de connexion, une icône spéciale apparaît dans la barre des tâches. Pour consulter les paramètres de connexion, double-cliquez sur cette icône spéciale (Illustration 28).

Si vous utilisez le réseau local pour vous connecter au fournisseur d'accès à Internet, vous pouvez soit utiliser les paramètres à partir du **Panneau de Configuration**, soit régler la connexion en mode manuel (Illustration 29).

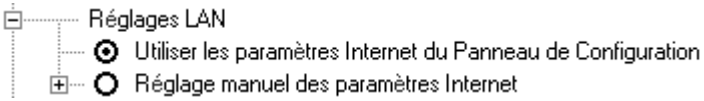
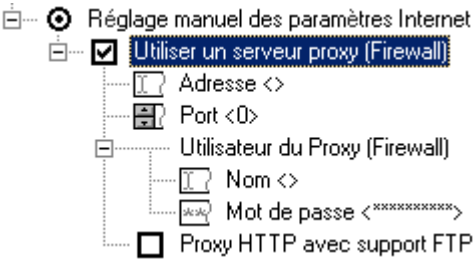


Illustration 29. Paramètres de connexion au réseau local

- **Utiliser les paramètres Internet du Panneau de configuration** – recevoir les paramètres de connexion depuis le panneau de configuration.
- **Réglage manuel des paramètres Internet** – régler les paramètres de connexion à la main.



Si le mode de réglage manuel a été choisi, il est indispensable d'effectuer le réglage des paramètres suivants de connexion (Illustration 30):

Illustration 30. Réglage manuel des paramètres Internet

- **Utiliser un serveur proxy (Firewall)** – utiliser un serveur proxy ou un Firewall pour établir la connexion avec le fournisseur d'accès à Internet
  - **Adresse** – adresse du serveur proxy (ou Firewall), via lequel la connexion sera établie. L'adresse peut être entrée au moyen d'une inscription décimale (par exemple, 125.5.29.1), en spécifiant une adresse (par exemple, test.russia.ru) ou une brève incription (par exemple, test)
  - **Port** – port pour la connexion avec un serveur proxy (ou Firewall)
- **Utilisateur du Proxy (Firewall)** – réglage des paramètres individuels de l'utilisateur
  - **Nom** – nom de l'utilisateur du proxy (ou du Firewall)
  - **Mot de passe** – mot de passe d'accès au serveur proxy (ou Firewall)
- **Proxy HTTP avec support FTP** – accès au serveur proxy FTP via le serveur proxy HTTP (proxy CERN-)

Pour des informations plus détaillées sur les réglages de connexion sus-mentionnés, adressez-vous à l'administrateur système de votre réseau.

5.2.2.2. Mise à jour depuis un dossier local

Si un dossier local a été sélectionné comme source de mise à jour, il est nécessaire d'en connaître le chemin d'accès complet.

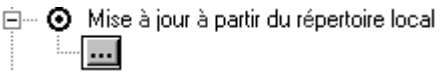


Illustration 31. Choix de la mise à jour via un répertoire local

Pour ce faire, cliquez sur le bouton gris (Illustration 31),

Ce choix entraîne l'ouverture de la boîte de dialogue **Rechercher un dossier** (Illustration 32) grâce à laquelle vous pouvez localiser et indiquer le répertoire contenant les fichiers de mise à jour.

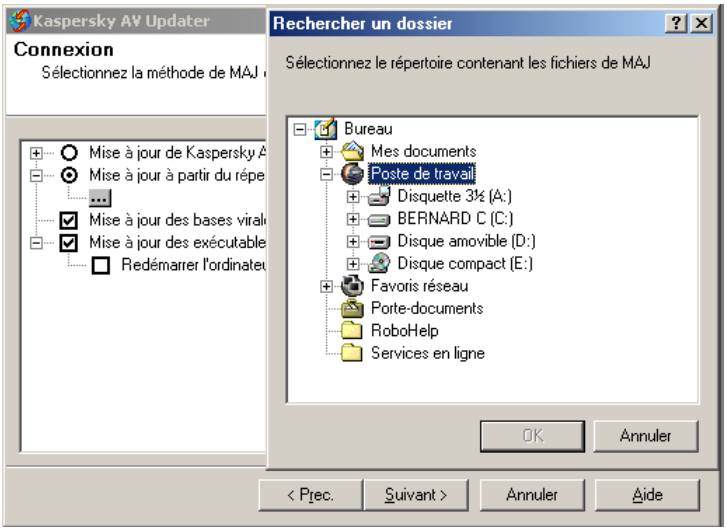


Illustration 32. Sélectionnez le répertoire contenant les fichiers de mise à jour.

5.2.2.3. Choix des objets à mettre à jour

Dans la partie inférieure de l'arborescence de réglages sont disposées deux options (Illustration 33), à savoir:

Illustration 33. Choix de l'objet de la mise à jour

☑ **Mise à jour des bases virales** – copier et installer depuis le serveur de mises à jour les bases de données anti-virus.

☑ **Mise à jour des exécutables** – copier et installer depuis le serveur de mises à jour les modules exécutables.

  ☑ **Redémarrer l'ordinateur si nécessaire** – rebooter automatiquement (le cas échéant) l'ordinateur après la mise à jour d'un logiciel.

5.2.3. Etape 3: Fenêtre Options

Dans la fenêtre **Options** on peut ajuster d'autres paramètres affectant le fonctionnement du programme de mise à jour des bases anti-virus (Illustration 34).

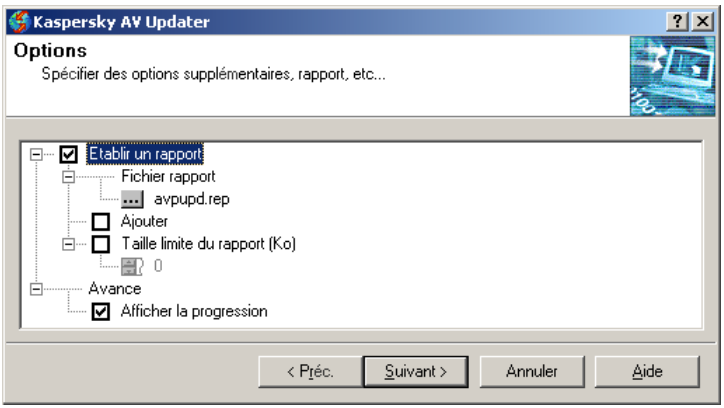


Illustration 34. Fenêtre Options

☑ **Etablir un rapport** – tenir un rapport sur la procédure de mise à jour.

  ⊟ **Fichier rapport** – saisie des informations sur le nom et l'emplacement du fichier de rapport.

  ☑ **Ajouter** – ajouter des informations aux fichier de rapport ou créer chaque fois un nouveau fichier de rapport.

  ☑ **Taille limite du rapport (Ko)** – taille maximum du fichier de rapport. Lorsque la taille prédéfinie du fichier de rapport est atteinte, celui-ci est réenregistré.

⊟ **Avancé** – réglage de l'interface utilisateur

  ☑ **Afficher la progression** – afficher la fenêtre Réception des mises à jour

Cliquez sur le bouton **Suivant** pour continuer la procédure de mise à jour.

5.2.4. Etape 4: Fenêtre Recherche des mises à jour

La fenêtre **Recherche des mises à jour** (Illustration 35) n'apparaît que si, dans la fenêtre Options, **dans** l'élément Avancé, vous avez coché la case Afficher la progression.

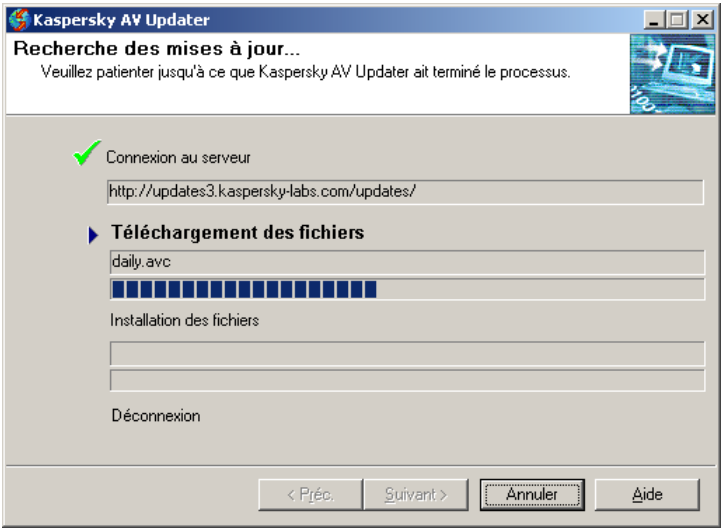


Illustration 35. Fenêtre Recherche des mises à jour

La fenêtre se compose de quatre parties montrant les différents stades d'exécution de la procédure de mise à jour des bases anti-virus:

- **Connexion au serveur** – connexion avec le serveur depuis lequel les fichiers seront copiés.
- **Téléchargement des fichiers** – copie des fichiers depuis le serveur vers l'ordinateur (en haut est affiché le nom du fichier copié, et en bas, le pourcentage d'exécution de la procédure de mise à jour).
- **Installation des fichiers…** - installation des fichiers sur l'ordinateur (dans la partie supérieure s'affiche le nom du fichier installé, et dans la partie inférieure – l'état d'avancement de l'opération).
- **Déconnexion** – fin de la connexion.

A gauche de l'intitulé des différents stades se trouve une zone indiquant le degré d'avancement (l'absence de coche indique que cette étape n'est pas terminée).

La marque ✔ indique que ce stade de la procédure a été exécuté correctement, et le signe ▶ indique que le programme de mise à jour est en train d'exécuter ce stade de la procédure.

5.2.5. Etape 5: Sortie de l'assistant de mise à jour

La fenêtre **Sortie de l'assistant Kaspersky AV Updater** (Illustration 36) apparaît en dernier. Dans cette fenêtre on peut consulter le rapport sur la procédure de mise à jour (pour ce faire, il faut cliquer sur le bouton Rapport), et aussi activer ou désactiver la case **Page d'accueil du site** Web de Kaspersky Labs.

Pour terminer la session de travail avec le programme, cliquez sur le bouton **Terminer**. Si vous avez activé la case **Page d'accueil du site** Web de Kaspersky Labs, votre navigateur Internet apparaît automatiquement, affichant la page d'accueil du site de Kaspersky Lab.

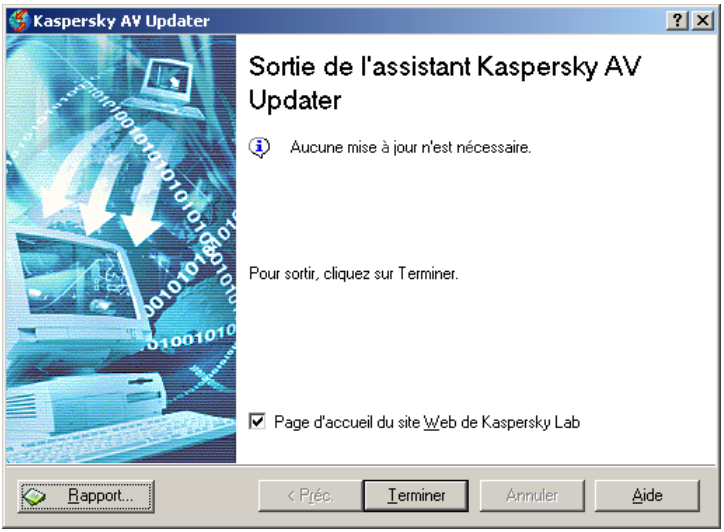


Illustration 36. Fenêtre Sortie de l'assistant Kaspersky AV Updater

CHAPITRE 6. KASPERSKY ANTI-VIRUS® CONTROL CENTRE

Le module Kaspersky Anti-Virus® Control Centre (Kaspersky AV Control Centre) fait partie intégrante du package anti-virus. Il est chargé d'organiser l'installation et la mise à jour des composants du package Kaspersky Anti-Virus® Personal, le lancement automatique des tâches, ainsi que le contrôle des résultats.

La possibilité de visualiser des informations sur les composants installés et sur leur version facilite les relations entre l'utilisateur et le service d'assistance technique de **Kaspersky Labs** et permet de déclencher en temps opportun la mise à jour des bases anti-virus.

Avec le module Kaspersky AV Control Centre, vous pouvez planifier le lancement des programmes anti-virus faisant partie intégrante du package. Ainsi, vous maintiendrez un haut niveau d'intégrité du système contre les virus et, dans le même temps, vous augmenterez l'efficacité de votre travail.

La possibilité de lancer automatiquement des programmes externes permet d'utiliser module Kaspersky AV Control Centre comme un planificateur de tâches. De ce fait, dans la plupart des cas, il devient inutile d'utiliser les autres outils de lancement automatique, ce qui permet d'économiser les ressources de l'ordinateur. De plus, le programme synchronise avec précision les procédures liées à la protection antivirale du système et aux autres tâches, ce qui permet d'éviter les conflits entre elles.

6.1. Lancement du module Kaspersky AV Control Centre

Il existe deux possibilités pour lancer Kaspersky AV Control Centre:

Option 1 : menu démarrer de Windows. Pour lancer le programme Kaspersky AV Control Centre, cliquez sur le bouton Démarrer et sélectionnez Programmes, passez ensuite dans le groupe Kaspersky Anti-Virus® et sélectionnez l'item Kaspersky Anti-Virus® Control Centre.

Option 2 : mode automatique aussitôt après le démarrage de Windows et avant l'ouverture de session, si le module Kaspersky AV Control Centre est installé .

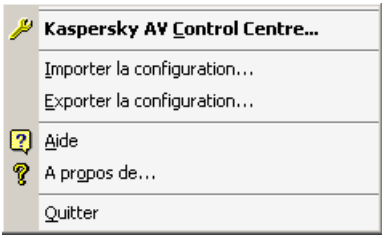


Illustration 37. Menu de Kaspersky AV Control Centre dans la barre des tâches

Après le lancement de Kaspersky AV Control Centre, l'icône apparaît dans la partie droite de la barre des tâches. En pointant sur cette icône avec la souris et en cliquant avec le bouton droit, vous faites apparaître un menu contextuel (Illustration 37), comportant les commandes suivantes:

- **Kaspersky AV Control Centre…** – ouverture de la fenêtre principale du programme
- **Importer la configuration…** – chargement des réglages du programme préalablement sauvegardés dans un fichier
- **Exporter la configuration…** – sauvegarde des réglages du programme dans un fichier spécial avec l'extension et la date. Les réglages peuvent être importés par la suite.
- **Aide** – affichage de la fenêtre d'aide
- **A propos de…** – affichage de la fenêtre avec les informations sur la version du produit, le nom de la licence, la date d'expiration de la licence, etc. (voir par exemple Illustration 38)
- **Quitter** – quitter le programme.

Les commandes **Exporter la configuration** et **Importer la configuration** sont destinées à transférer les réglages de Kaspersky AV Control Centre d'un ordinateur vers un autre ordinateur, c'est-à-dire que vous pouvez paramétrer un programme sur un ordinateur, sauvegarder les réglages dans un fichier dans un dossier commun sur le serveur, puis les charger sur un autre ordinateur.

Dans la partie supérieure du menu utilisateur, au-dessus de la barre, se trouve la liste des tâches accompagnées de leurs paramètres de lancement automatique. Pour lancer ces tâches, on peut choisir dans le menu la commande appropriée sans ouvrir la fenêtre principale de Kaspersky AV Control Centre.

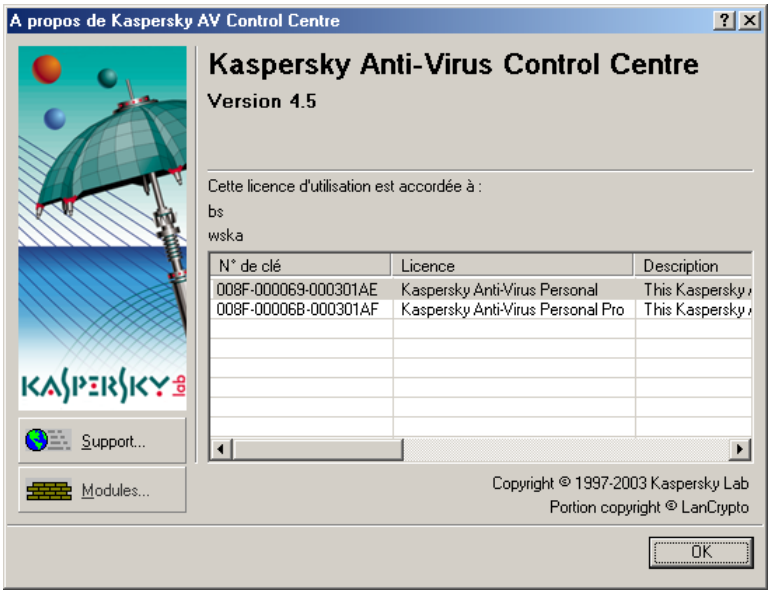


Illustration 38. **A propos de Kaspersky AV Control Centre**

Pour quitter Kaspersky AV Control Centre, choisissez la commande **Quitter** dans le menu de la barre des tâches.

Il convient ici de fournir quelques explications sur les particularités du programme. Le module Kaspersky AV Control Centre se compose de deux parties : la partie service qui est lancée comme un service système et démarre avant la procédure d'entrée du mot de passe, et la partie interface qui offre une interface graphique et assure l'interaction avec l'utilisateur. Si on ne décharge que la partie interface, les tâches définies dans les réglages de Kaspersky AV Control Centre seront exécutées comme auparavant, mais l'utilisateur sera privé de la possibilité d'éditer les paramètres et de créer de nouvelles tâches. Si, de plus, on décharge également la partie service, le module Kaspersky AV Control Centre cessera d'exécuter les tâches prescrites.

Option 3 : Depuis la ligne de commande. Pour démarrer Kaspersky AV Control Centre depuis la ligne de commande, ouvrez le dossier **KAV Shared Files** et exécutez *avpcc.exe*. Le fichier commun se trouve sur le chemin suivant : **C:\Program Files\Common Files\KAV Shared Files**.

6.2. Interface du module Kaspersky AV Control Centre

La fenêtre principale contient trois onglets: **Tâches**, **Composants**, **Configuration** et **Quarantaine** (voir leur description plus bas).

Pour exécuter une action, on utilise le menu contextuel et le panneau de configuration.

Dans la partie inférieure de la fenêtre sont disposés les boutons **OK**, **Annuler**, **Appliquer** et  . Si l'on clique sur le bouton **OK**, on sauvegarde toutes les modifications apportées dans la procédure de paramétrage, ce qui n'est pas le cas si l'on clique sur le bouton **Annuler**. Dans l'un et l'autre cas, la fenêtre principale se ferme. Un clic sur le bouton **Appliquer** entraîne la sauvegarde des modifications, la fenêtre principale restant ouverte, et vous pouvez continuer le paramétrage. Pour les tâches résidentes qui sont en fonctionnement, les réglages seront chargés aussitôt dans le module exécutable. Un clic sur le bouton  entraîne l'ouverture de l'aide.

6.2.1. Feuillet Tâches

L'onglet **Tâches** (Illustration 39) est destiné à la gestion des tâches. On entend par tâche, comme cela a déjà été mentionné plus haut, l'exécution d'un programme spécifique lancé à un moment donné, soit lors de la survenue d'un événement déterminé, soit sur indication directe de l'utilisateur avec sélection de paramètres et de réglages définis.

L'onglet se compose de trois parties:

- dans la partie gauche se trouve la liste des tâches avec indication de leur état
- dans la partie droite sont affichées les statistiques[1]
- dans la partie inférieure se trouve la liste des événements (erreurs, alertes, messages d'information).

1 Statistiques – forme abrégée de rapport sur l'activité du programme.

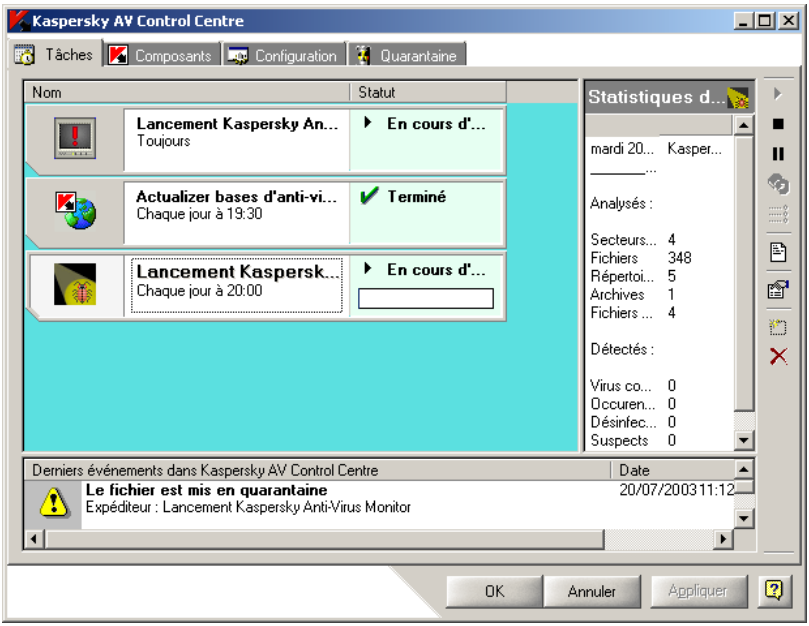


Illustration 39. Feuillet **Tâches**

Examinons chaque partie de l'onglet. La liste des tâches comporte deux colonnes: **Nom** et **Statuts**. Dans la colonne **Nom** se trouve la liste des tâches et dans la colonne **Statuts** – le statut d'exécution de la tâche correspondante. Voici les différents statuts:

- **En cours d'exécution** – tâche en cours d'exécution
- **Terminé** – tâche correctement exécutée
- **Echec** – panne lors de l'exécution de la tâche
- **Interrompu par l'utilisateur** – exécution de la tâche stoppée par l'utilisateur
- **Pause** – exécution interrompue
- **Démarrage** – lancement de la tâche à exécuter
- **Arrêt** – arrêt de la tâche
- **Erreur de lancement** – erreur de lancement de la tâche
- **Relancé** – la tâche est relancée

Dans la partie droite de la fenêtre se trouve la fenêtre des statistiques. Son contenu dépend du type de la tâche.

Par exemple, pour la tâche de mise à jour automatique, les statistiques se composent des champs suivants: Date**,** Heure**,** Action, Statut et Objet, qui reflètent respectivement la date et l'heure de lancement de la tâche, les actions exécutées et leur résultat, ainsi que l'objet concerné par l'action.

Dans la partie inférieure de la fenêtre est disposée la liste des événements avec indication de la date et de l'heure de survenue, ainsi que le composant se trouvant à leur origine. Les événements aboutissent au Kaspersky AV Control Centre depuis tous les composants du package qui sont en fonctionnement. Cette liste comporte tous les événements critiques. de réception, tant par ordre de croissance que de suppression. Dans cette liste ne sont affichés que les événements critiques (vous pouvez les trier par nom ou par date) et le dernier événement est indiqué dans la partie supérieure de la liste. Lors du choix d'un événement dans la liste, la tâche à l'origine de l'événement est indiquée en surbrillance.

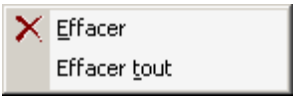


Illustration 40. Menu contextuel de la liste des événements

Cette liste est pourvue d'un menu contextuel (Illustration 40) dont les options sont les suivantes:

- **Supprimer** – supprimer l'événement désigné (avec confirmation de la suppression)
- **Supprimer tout** – supprimer tous les événements de la liste (avec confirmation de la suppression).

La gestion des tâches, (par exemple, création, paramétrage, suppression, lancement et arrêt) s'effectue à l'aide du menu contextuel et des boutons situés dans la barre d'outils (Illustration 41).

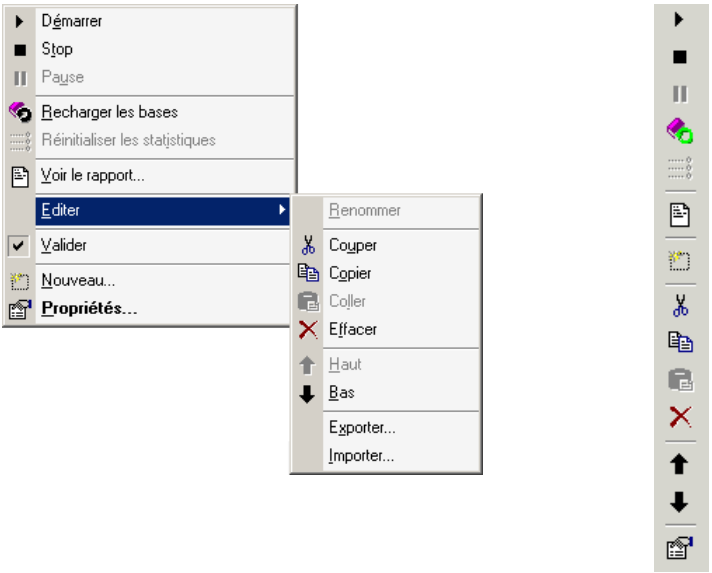


Illustration 41. Menu contextuel de la liste des tâches et panneau de contrôle sur l'onglet Tâches

Le menu contextuel est appelé par un clic avec le bouton droit de la souris dans la partie gauche de la fenêtre, c'est-à-dire dans la partie de la fenêtre contenant la liste des tâches et leur statut.

- **Démarrer** – lancer la tâche
- **Stop** – arrêter l'exécution et décharger la tâche de la mémoire
- **Pause** – interrompre l'exécution de la tâche. A cette occasion, la tâche n'est pas déchargée de la mémoire, seule son exécution est interrompue
- **Recharger les bases** – réinitialiser les bases de données anti-virus. Cette commande n'est destinée qu'aux tâches résidentes dans lesquelles il est nécessaire d'initialiser de nouvelles bases anti-virus sans relancer la tâche
- **Réinitialiser les statistiques** – remettre à zéro les statistiques relatives à la tâche (uniquement pour les tâches résidentes)
- **Voir le rapport** – montrer dans la fenêtre du programme Kaspersky® Report Viewer (voir chap.**Chapitre 7**) le rapport relatif à la tâche
- **Editer** – éditer la tâche (cette commande comporte un sous-menu avec les commandes suivantes

- **Renommer** – renommer la tâche
- **Couper** – **couper** la tâche de la liste et la sauvegarder dans le tampon d'échange interne de Kaspersky AV Control Centre (le nom de la tâche, ses paramètres et les réglages de sa programmation seront sauvegardés)
- **Copier** – copier la tâche dans le tampon d'échange interne
- **Coller**– insérer la tâche du tampon d'échange dans la liste des tâches du programme
- **Effacer** – supprimer la tâche de la liste
- **Haut** – déplacer le nom de la tâche d'un cran vers le haut de la liste
- **Bas** – déplacer le nom de la tâche d'un cran vers le bas de la liste
- **Exporter** – sauvegarder la tâche avec tous ses paramètres dans un fichier. Une boîte de dialogue apparaît et propose l'enregistrement dans un fichier ayant une extension **tsk**
- **Importer –** charger la tâche depuis un fichier

- **Valider** – activer ou désactiver la tâche dans le planning. Si la tâche est activée, celle-ci continuera de Illustrationr dans la liste des tâches mais le planificateur ne la lancera pas
- **Nouveau** – créer une nouvelle tâche. La sélection de cette commande a pour effet d'initialiser l'assistant de création d'une nouvelle tâche (voir. 6.2.3.4)
- **Propriétés** – afficher les réglages de la tâche.

Les commande Exporter et Importer sont destinées à l'échange de tâches entre ordinateurs : vous pouvez créer une tâche sur un ordinateur, la sauvegarder dans un fichier dans un dossier commun ou sur le serveur, et ensuite la charger sur un autre ordinateur.

Certaines commandes peuvent être réservées à certains types de tâches.

La position des tâches dans la liste indique leur ordre de chargement.

La gestion des tâches, comme cela a déjà été mentionné plus haut, est également effectuée au moyen des boutons de la barre d'outils.

Voici les correspondances entre les boutons et les commandes du menu contextuel :

Bouton	Commande du menu contextuel
	Lancer
	Stop
	Pause
	Recharger les bases
	Réinitialiser les statistiques
	Voir le rapport
	Nouvelle tâche
	Propriétés
	Supprimer

En pointant avec la souris sur un bouton, on fait apparaître à côté du bouton une bulle d'aide indiquant la fonction du bouton.

Les fonctions suivantes sont destinées à la manipulation des tâches :

- *Appuyer sur une touche* – vous pouvez basculer entre les éléments de liste en utilisant la touche correspondant à la première lettre du nom choisi.
- *Utiliser des raccourcis clavier spéciaux:*
    - **<INSERT>** – créer une nouvelle tâche. Le fait d'appuyer sur cette touche entraîne l'ouverture de la boîte de dialogue **Nouvelle tâche** (pour plus de détails, voir le paragraphe 6.2.3.4).
    - **<DELETE>** – supprimer la tâche de la liste (avec confirmation de la suppression).
    - **<SPACE>** – montrer les propriétés de la tâche mise en évidence. Le fait d'appuyer sur cette touche entraîne l'ouverture de la boîte de dialogue **Propriétés** (pour plus de détails voir le sous-chapitre 6.2.1.1).

6.2.1.1. Fenêtre Propriétés

Cette fenêtre est appelée par un clic sur le bouton  ou par le choix de l'option **Propriétés** dans le menu contextuel. L'aspect de la fenêtre dépend du type de tâche qu'elle caractérise.

Cette version du produit comporte les variantes suivantes de fenêtres:

- fenêtre des propriétés de la tâche Kaspersky AV Scanner
- fenêtre des propriétés de la tâche de Kaspersky AV Monitor
- fenêtre des propriétés de la tâche Kaspersky AV Updater

6.2.1.1.1. Fenêtre des propriétés de la tâche Kaspersky AV Scanner

La fenêtre des propriétés de la tâche de Kaspersky AV Scanner (Illustration 42) montre les réglages de la tâche exécutée sur la base du composant Kaspersky AV Scanner.

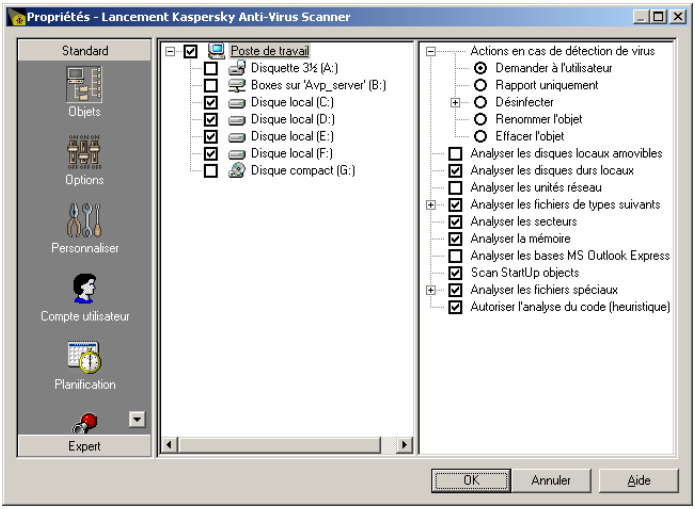


Illustration 42. Fenêtre des propriétés de la tâche de Kaspersky AV Scanner

La fenêtre se compose des catégories suivantes.

Catégorie	Description
Objets	Voir paragraphe 3.3.1
Options	Voir paragraphe 3.3.2
Personnaliser	Voir paragraphe 3.3.3
Compte utilisateur	Voir paragraphe 6.3.5
Planification	Voir paragraphe 6.3.3
Alertes	Voir paragraphe 6.3.4

6.2.1.1.2. Fenêtre des propriétés de la tâche Kaspersky AV Monitor

Dans la fenêtre des propriétés de la tâche Kaspersky AV Monitor (Illustration 43) sont affichés les réglages de la tâche créée sur la base du composant Kaspersky AV Monitor. Cette fenêtre comporte différentes sections contenant les réglages de la tâche. Certaines sections sont identiques à celles du composant correspondant, d'autres sont spécifiques à Kaspersky AV Control Centre.

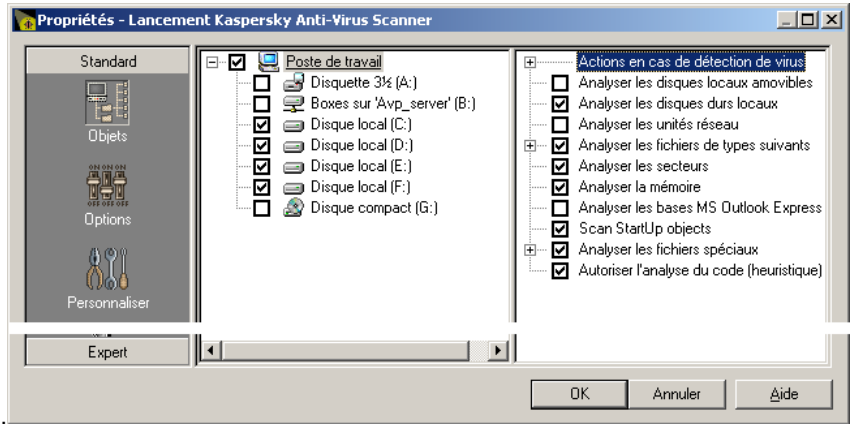


Illustration 43. Fenêtre des propriétés de la tâche de Kaspersky AV Monitor

Catégorie	Description
Objets, Options, Personnaliser	Voir paragraphe 3.3.1, 3.3.2, 3.3.3
Planification	Voir paragraphe 6.3.2
Alertes	Voir paragraphe 6.3.4

6.2.1.1.3. Fenêtre des propriétés de la tâche Kaspersky AV Updater (mise à jour)

La fenêtre des propriétés de la tâche de Kaspersky AV Updater se compose d'une série d'onglets permettant d'effectuer les réglages (Illustration 44).

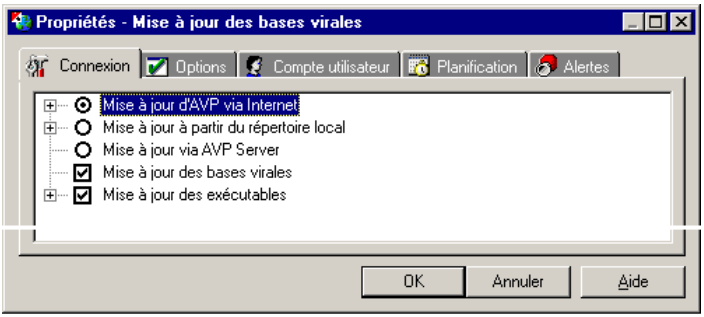


Illustration 44. Fenêtre des propriétés de la tâche de Kaspersky AV Updater

Feuillet	Description
Connexion	Voir p. 5.2.2
Options	Voir p. 5.2.3
Compte utilisateur	Voir p. 6.3.5
Planification	Voir p.6.3.3
Alertes	Voir p. 6.3.4

L'onglet Connexion **de** la fenêtre des propriétés contient une option supplémentaire permettant de mettre à jour les bases anti-virus et les modules exécutables dans des dossiers sur le serveur Kaspersky AV Server. Il s'agit de l'option **Mise à jour** via le serveur Kaspersky AV Server.

6.2.2. Feuillet Composants

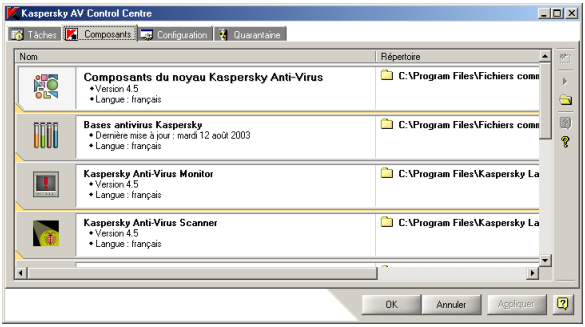


Illustration 45. Feuillet **Composants**

L'onglet **Composants** (Illustration 45) contient la liste des composants2 du package Anti-Virus Kaspersky. Dans la partie droite de l'onglet se trouve la barre d'outils ; un clic avec le bouton droit de la souris fait apparaître le menu contextuel (Illustration 46).

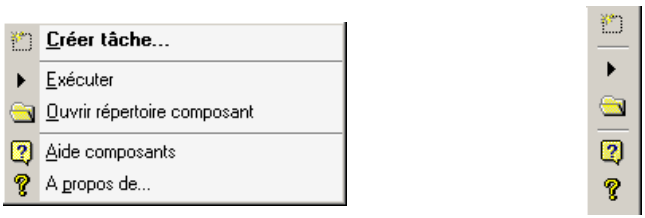


Illustration 46. Menu contextuel et barre d'outils dans l'onglet **Composants**

Les boutons de la barre d'outils correspondent exactement aux options du menu contextuel (voir plus bas).

Bouton	Commande du menu contextuel	Description
	Nouvelle tâche	Création d'une nouvelle tâche sur la base du composant sélectionné. Un clic sur ce bouton ou la sélection de l'option du menu a pour

2 Un composant est un programme, un outil, une bibliotèque ou une base de données faisant partie de Kaspersky Anti-Virus ou responsable d'un nombre strictement défini des tâches.

Bouton	Commande du menu contextuel	Description
		effet d'ouvrir la fenêtre Nouvelle tâche (pour plus de détails voir le paragraphe 6.2.3.4)
	Exécuter…	Lancer l'exécution d'une tâche.
	Ouvrir un répertoire de composant	Vue du répertoire de composant dans la fenêtre standard de MS Windows.
	Aide composants…	Lancement du système d'information sur le composant spécifié
	A propos du programme	Affichage des informations sur la version du produit, la date de la dernière mise à jour des bases anti-virus, etc. Un clic sur ce bouton ou la sélection de l'option du menu ont pour effet d'ouvrir la fenêtre **A propos du programme**.

6.2.3. Feuillet Configuration

L'onglet **Configuration** (Illustration 47) est destiné à l'entrée des réglages du Control Centre. Les réglages sont répartis en quatre catégories. Chaque catégorie de réglages regroupe des paramètres avec une fonctionnalité strictement définie.

La liste des catégories de réglages est située dans la partie gauche de la fenêtre. Lors du choix de telle ou telle catégorie, à droite de la fenêtre s'affiche l'arborescence des réglages. L'arborescence des réglages est élaborée sur la base de l'élément de l'arborescence (pour plus de détails sur la manière de travailler avec lui, voir le Chapitre 8).

Si toutes les catégories ne tiennent pas dans la fenêtre, les boutons  et  qui apparaissent dans ce cas permettent de faire défiler la liste entière.

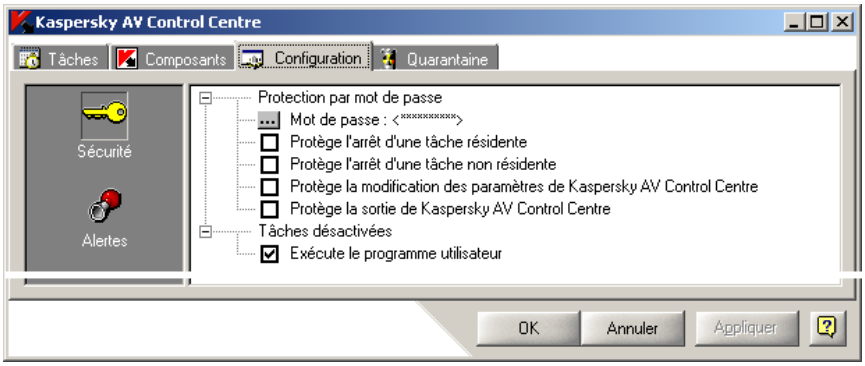


Illustration 47. Fragment de l'onglet Configuration

Catégorie	Rôle
Sécurité	contient les paramètres de sécurité du système et de restriction de l'accès aux réglages et aux composants du Control Centre
Alertes	contient les paramètres de traitement des messages d'information relatifs aux événements critiques dans l'exécution des tâches du Control Centre
Quarantaine	contient les paramètres d'emplacement des fichiers mis en quarantaine sur cet ordinateur ou serveur (uniquement si Kaspersky® Administration Kit est installé) (voir la suite pour plus d'information sur la Quarantaine).
Personnaliser	contient les paramètres de réglage de l'interface utilisateur du Control Centre.

6.2.3.1. La catégorie Sécurité

Illustration 48. Feuillet **Configuration**. Catégorie **Sécurité**

Cette catégorie (Illustration 48) est destinée au réglage des fonctions de sécurité du système. Elle permet de régler les mots de passe et d'interdire certains types de tâches.

La protection de certaines actions par un mot de passe s'effectue dans la section **Protection par mot de passe**, et l'interdiction d'exécuter certains types de tâches s'effectue dans la section **Actions interdites** (pour plus de détails sur ces fonctions, voir plus bas).

6.2.3.1.1. La section Protection par mot de passe

Le Control Centre offre la possibilité de protéger par un mot de passe une partie des actions exécutées. Ceci permet à l'utilisateur de limiter l'accès à certaines commandes d'exécution.

Illustration 49. Section des réglages Protection par mot de passe

Ces fonctions, comme nous l'avons vu plus haut, sont régulées dans la section de l'arborescence **Protection par mot de passe** (Illustration 49).

Cette section contient les paramètres suivants:

- Mot de passe – saisie du mot de passe pour la gestion de l'Anti-Virus Kaspersky® à l'aide de Kaspersky Anti-Virus® Control Centre, ainsi que pour la restriction de l'accès à certaines fonctions du programme (liste des fonctions disposée en bas de l'arborescence). Un clic sur le bouton ... a pour effet d'ouvrir la boîte de dialogue **Changer le mot de passe**.

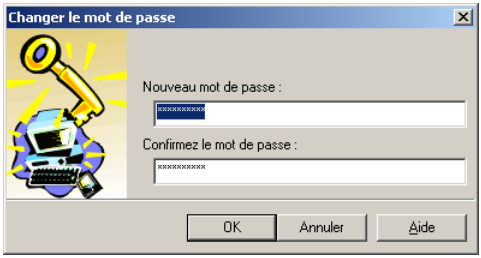


Illustration 50. Changer le mot de passe

Cette boîte de dialogue (Illustration 50) sert à entrer et à modifier le mot de passe. Saisissez dans le champ **Nouveau mot de passe** votre mot de passe et répétez l'opération dans le champ **Confirmer le mot de passe**.

- **Protection de l'arrêt des tâches residents** – création d'un mot de passe pour l'arrêt des tâches résidentes. Si, par exemple, le moniteur anti-virus a été lancé sur votre ordinateur et que cette option a été activée, le mot de passe sera nécessaire pour arrêter le moniteur..
- **Protection de l'arrêt des tâches non-résidentes** – création d'un mot de passe pour l'arrêt des tâches non-résidentes. Lors de l'activation de cette option, pour arrêter l'exécution de tâches non-résidentes, telles que le lancement de Kaspersky AV Scanner ou de Kaspersky AV Updater, l'utilisateur doit entrer un mot de passe.
- **Protection de la modification des paramètres de Kaspersky AV Centre** – création d'un mot de passe pour l'ouverture de la fenêtre des réglages de Kaspersky AV Control Centre.
- **Protection de la sortie de Kaspersky AV Control Centre** – création d'un mot de passe pour le déchargement de Kaspersky AV Control Centre de la mémoire.

Lors du choix d'actions protégées, n'oubliez pas d'entrer le mot de passe approprié dans le champ Mot de passe !

En outre, dans cet onglet il est possible d'interdire l'exécution de certains types de tâches présentant un risque lors de l'administration à distance, en cas d'accès non-autorisé (entrée par effraction dans le système).

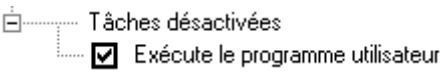


Illustration 51. Section des réglages Tâches désactivées

Exécution dans la section **Tâches désactivées** (voir Illustration 51).

Dans la version actuelle du produit il n'existe qu'un seul type de réglage de ce genre, à savoir:

☑ **Lancement du programme de l'utilisateur** – l'activation de cette option interdit le lancement des programmes de l'utilisateur comme des tâches de Kaspersky AV Control Centre.

6.2.3.2. La catégorie Alertes

La catégorie **Alertes** (voir Illustration 52) est destinée à la gestion du traitement des avis générés par les tâches.

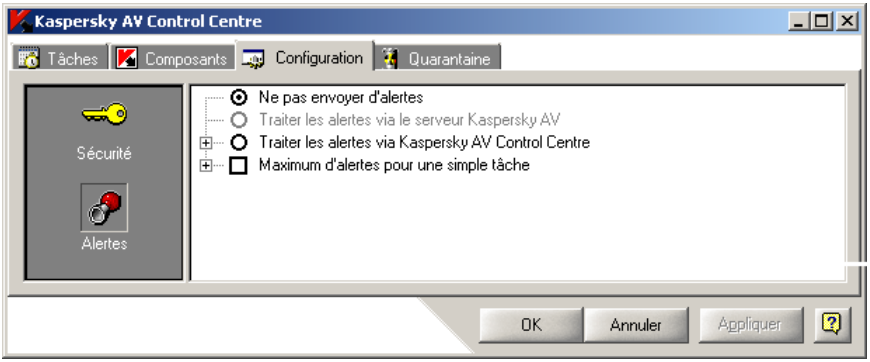


Illustration 52. Feuillet Configuration. Catégorie Alertes

Les différentes options de traitement des messages d'information sont les suivantes:

- **Ne pas envoyer d'alertes** – interdire l'envoi de messages d'alertes
- **Traiter les alertes via le Serveur Kaspersky AV** – envoyer les messages d'information à l'aide du Serveur Kaspersky AV – il s'agit du composant serveur du système de gestion à distance du package Anti-Virus Kaspersky.
- **Traiter les alertes via Kaspersky AV Control Centre** – envoyer les messages d'alertes à l'aide de Kaspersky AV Control Centre

Pour restreindre le nombre des messages d'information émis par une tâche, activez l'option **Maximum d'alertes pour une simple tâche**, puis entrez le nombre maximum.

Par exemple, sur l'Illustration 53 nous voyons que le nombre maximum de messages d'information émis par une tâche a été limité. Supposons que cette limite soit 10. Ceci signifie que lorsque le onzième message d'alerte parviendra à Kaspersky AV Control Centre, la liste des messages d'alertes reçues sera automatiquement nettoyée.

Si vous avez sélectionné l'option **Traiter les alertes via Kaspersky AV Control Centre**, il est nécessaire de régler les paramètres d'envoi des messages d'information. Pour l'activation des envois par l'intermédiaire d'un e-mail, activez l'option **Envoyer un e-mail**. Réglez ensuite les paramètres suivants:

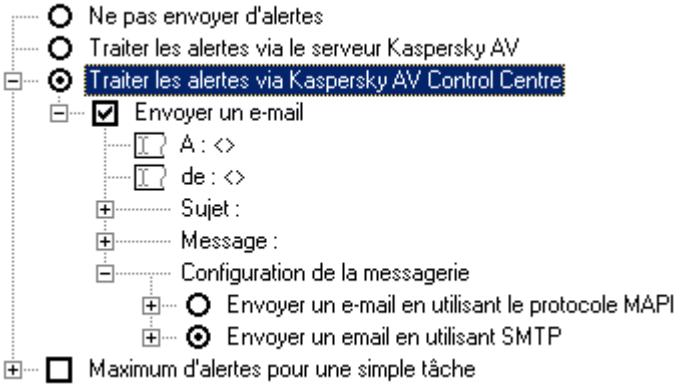


Illustration 53. Option de traitement par Kaspersky AV Control Centre

A: dans ce champ entrez l'adresse électronique du destinataire des messages

de: entrez ici ce qui s'affichera dans le champ **de** du courrier électronique. La valeur de cette option peut être n'importe quelle ligne. Ce paramètre est obligatoire lors du travail avec certains serveurs SMTP et est utilisé pour identifier l'utilisateur

Objet: nom de l'objet du message dans le courrier électronique

Message: texte du message qui sera contenu dans le courrier électronique expédié

Configuration de la messagerie dans cette section il est indispensable de prédéfinir les paramètres du système de messagerie servant pour l'expédition des messages d'information. Il existe deux procédés d'envoi:

- par SMTP
- par MAPI

Vous pouvez demander des informations plus détaillées sur SMTP et MAPI à l'administrateur système de votre réseau.

6.2.3.2.1. Le réglage de l'envoi des messages d'information par SMTP

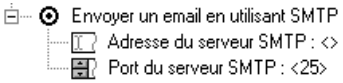


Illustration 54.
Paramètres de réglage SMTP

pour l'envoi des messages d'information par SMTP, il est nécessaire de sélectionner l'option **Envoyer un e-mail en utilisant le protocole SMTP** (Illustration 54) et ensuite d'activer les paramètres suivants:

Adresse du serveur SMTP — contient l'adresse du serveur SMTP, en outre, il est possible d'entrer l'adresse en utilisant une inscription DNS (par exemple, 125.5.29.1), soit une inscription de domaine complète (par exemple, test.mail.ru), soit une inscription brève (par exemple, test)

Port du serveur SMTP — contient l'adresse du port du serveur SMTP. La valeur par défaut est égale à 25.

Examinons un exemple de paramètres de l'onglet **Alertes**. Admettons qu'il soit nécessaire de paramétrer l'envoi des messages SMS sur les événements critiques sur le réseau vers le téléphone portable de l'administrateur système en utilisant e-mail-gate.

Données d'entrée:

- **numéro de téléphone portable de l'administrateur** – 1234567 (numéro direct)
- **opérateur du réseau téléphonique** – Beeline GSM (c'est-à-dire code d'accès pour les numéros directs – 7 901)
- **adresse du serveur SMTP** – mysmtp.home.ru
- **port du serveur SMTP** – 25

en outre, il est nécessaire que:

- le message soit expédié de la part de **Control Centre**,
- porte le titre **Alert**,
- dans le corps du courrier se trouve le texte suivant: **Attention ! Un événement critique s'est produit !**.

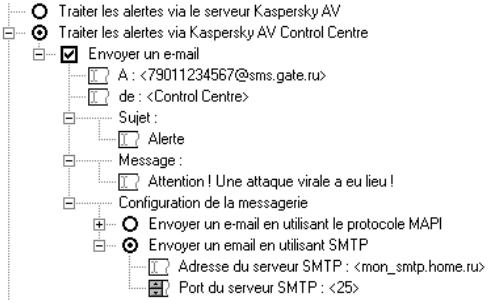


Illustration 55. Réglages pour l'envoi des messages SMS sur les événements critiques

Pour cela, il est nécessaire d'entrer les réglages suivants (Illustration 55).

L'adresse e-mail-gate, ainsi que le code d'accès à l'opérateur de communication mobile peuvent différer selon les régions.

6.2.3.2.2. Le réglage de l'envoi des messages d'information avec utilisation du protocole MAPI

Si votre ordinateur est équipé du système d'exploitation Windows 95/OSR2/98 , le programme Kaspersky AV Control Centre permet de paramétrer l'envoi des messages d'information en utilisant le protocole MAPI.

Illustration 56. Paramètres de réglage MAPI

Pour régler les paramètres du protocole MAPI, sélectionnez l'option **Envoyer un e-mail en utilisant le protocole MAPI** (Illustration 56), entrez ensuite les valeurs des paramètres suivants:

Configuration	nom du profil (du fichier de réglages) du client MAPI
Mot de passe pour la configuration	mot de passe pour l'accès au profil
Client MAPI	nom du client MAP qui sera utilisé pour l'envoi des messages d'information.

Tous les clients MAPI n'utilisent pas de profils parce que pour certains d'entre eux les champs Configuration et Mot de passe de configuration doivent rester vides.

6.2.3.3. La catégorie Personnaliser

Illustration 57. Feuillet Paramètres. Catégorie Personnaliser

La catégorie **Personnaliser** (Illustration 57) contient les paramètres de l'interface du programme. Dans cette catégorie, on peut régler la sonorisation de l'exécution de certaines actions, ainsi que l'apparence du programme.

La catégorie **Personnaliser** contient deux sections: **Activer le son sur un événement** et **Apparence**. Elles ont la valeur suivante:

Activer le son sur un événement — réglage des effets sonores résultant de l'exécution (ou de la fin d'exécution) de certaines opérations (pour plus de détails voir le chapitre **Réglage de la sonorisation du programme**)

Apparence — réglage de l'apparence du programme (pour plus de détails, voir le chapitre **Réglage de l'apparence**)

6.2.3.3.1. Réglage de la sonorisation du programme

Le programme Kaspersky AV Control Centre permet d'associer un son à certains événements, ajoutant au programme des possibilités étendues.

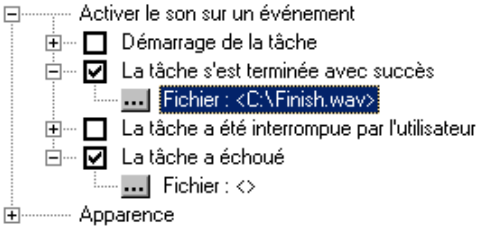


Illustration 58. Réglage de la sonorisation

Le réglage des effets sonores, comme cela a été noté plus haut, est effectué dans la section **Sonorisation** (Illustration 58).

Pour activer un effet sonore, il faut le cocher dans la liste et ensuite cliquer sur le bouton ... pour appeler la boîte de dialogue permettant de choisir le fichier son. Le fichier son doit être enregistré au format WAV. Examinons le rôle de chaque effet sonore:

Démarrage de la tâche	diffusion du son aussitôt après le démarrage de la tâche (quel que soit le type de tâche)
La tâche s'est terminée avec succès	diffusion du son en cas d'exécution correcte de la tâche, c'est-à-dire si la tâche n'a pas été interrompue par l'utilisateur et a été exécutée sans erreur
La tâche a été interrompue par l'utilisateur	diffusion du son en cas d'arrêt d'exécution de la tâche par l'utilisateur
La tâche a échoué	diffusion du son en cas d'échec dans l'exécution de la tâche

6.2.3.3.2. Réglage de l'apparence

Le programme Kaspersky AV Control Centre permet de modifier les couleurs de l'interface.

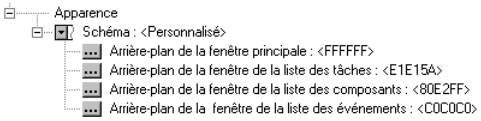


Illustration 59. Réglage de l'apparence

La modification des couleurs des éléments de l'interface, comme cela a été noté plus haut, s'effectue dans la section **Apparence** (voir Illustration 59).

Pour faciliter le réglage des couleurs, le programme offre à l'utilisateur un ensemble de couleurs standards. Le choix de cet ensemble s'opère dans la liste **Schéma**. Chaque schéma est caractérisé par les paramètres suivants:

Arrière-plan de la fenêtre principale	couleur de fond de la fenêtre principale du programme
Arrière-plan de la fenêtre de la liste des tâches	couleur de fond de la liste des tâches de l'onglet **Tâches**
Arrière-plan de la fenêtre de la liste des composants	couleur de fond de la liste des composants de l'onglet **Composants**
Arrière-plan de la fenêtre de la liste des événements	couleur de fond de la fenêtre des événements de l'onglet **Tâches**

Ci-dessous, l'Illustration 60 montre l'exemple du schéma de couleurs **Lilas** avec indication de ses paramètres.

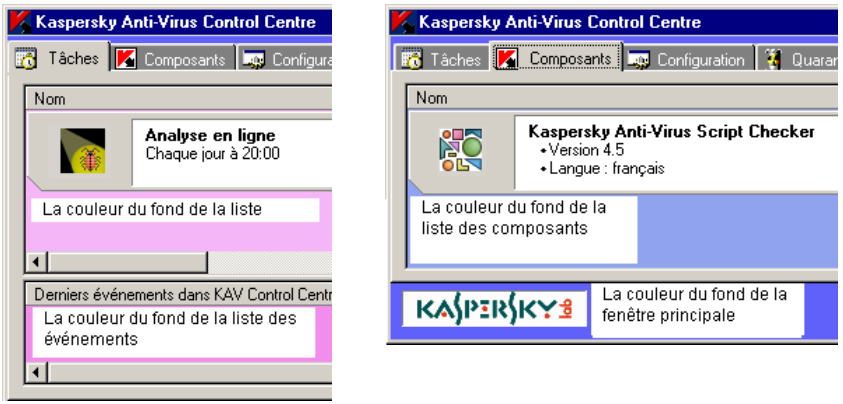


Illustration 60. Exemple d'apparence

6.2.3.4. La catégorie Quarantaine

La catégorie **Quarantaine** contient le réglage de la mise en quarantaine anti-virus – sorte d'entrepôt où Kaspersky Anti-Virus® Scanner et Kaspersky Anti-Virus® Monitor mettent les fichiers infectés et suspects (Illustration 61).

Pour que Kaspersky Anti-Virus® Scanner et Kaspersky Anti-Virus® Monitor puissent stocker un fichier dans cet entrepôt spécial, il est indispensable, dans l'onglet **Paramètres** de la boîte de dialogue des propriétés, de cocher la case **Utiliser la quarantaine**. Dans ce régime de travail le programme copie les fichiers infectés et les met en quarantaine, sans les supprimer du dossier où ils se trouvaient initialement. La suppression des fichiers infectés de l'ordinateur est effectuée par le programme si, comme actions sur les fichiers infectés, vous avez sélectionné la commande **Supprimer** dans les réglages de Kaspersky Anti-Virus® Scanner et Kaspersky Anti-Virus® Monitor.

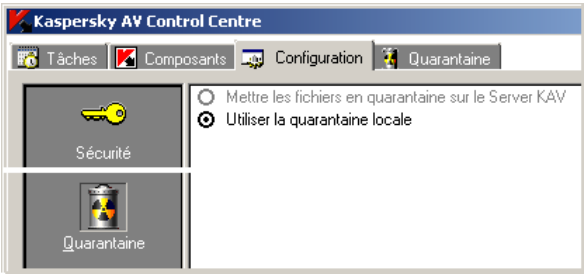


Illustration 61. Catégorie Quarantaine

Les fichiers mis en quarantaine sont stockés sous une forme codée, ce qui garantit:

- l'absence de risque d'infection (le code exécutable ne peut être lancé sans décryptage)
- un gain de temps au niveau du travail des programmes anti-virus (les fichiers au format de quarantaine ne sont pas considérés comme des fichiers infectés).

Ultérieurement, les fichiers mis en quarantaine peuvent être analysés et soit restaurés sous leur forme d'origine, soit supprimés.

Pour mettre des fichiers en quarantaine dans votre ordinateur, (quarantaine *locale*), sélectionnez dans le groupe de boutons de choix la variante **Utiliser la quarantaine locale**. Le travail sur les fichiers mis en quarantaine locale est décrit dans le chapitre suivant.

6.2.4. Feuillet Quarantaine

Dans l'onglet **Quarantaine** (Illustration 62) est affiché le contenu de la quarantaine locale (sur la quarantaine locale, voir chap. 6.2.3.4).

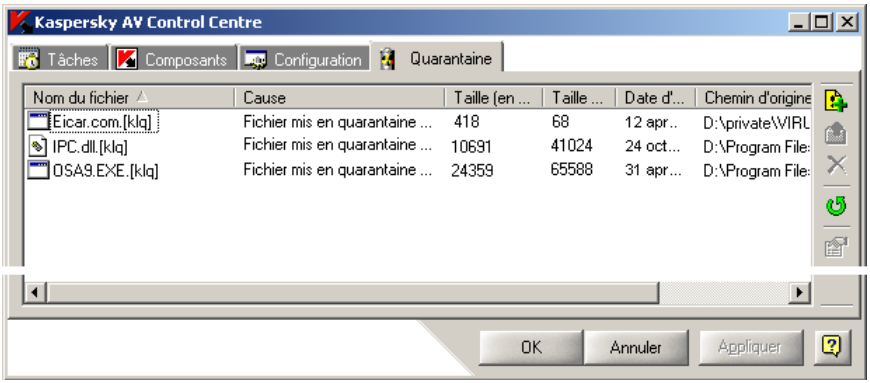


Illustration 62. Feuillet Quarantaine

Vous pouvez paramétrer le mode de présentation des fichiers dans cet onglet et exécuter différentes opérations sur les fichiers. Le menu dynamique de l'onglet est prévu à cet effet (Illustration 63).

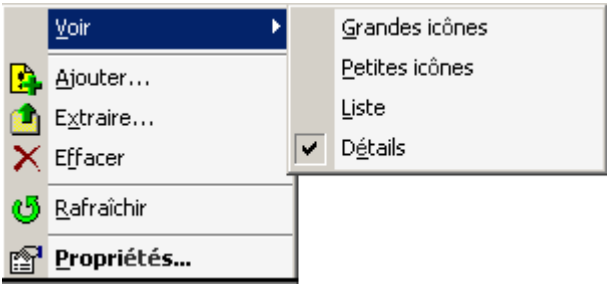


Illustration 63. Menu dynamique de l'onglet **Quarantaine**

Toutes les commandes de ce menu, excepté la commande **Voir**, sont doublées par les boutons de la barre d'outils de la partie droite de l'onglet.

A l'aide des commandes du sous-menu **Voir** vous pouvez régler le type d'icônes et le procédé de présentation de la liste (tableau ou noms des fichiers uniquement).

Pour voir les propriétés du fichier:

1. Choisissez son nom et cliquez sur le bouton .
2. La fenêtre d'informations sur le fichier apparaît (les informations sont les mêmes que celles qui sont affichées dans le tableau, cependant les informations sont disposées de façon plus lisible (Illustration 64).

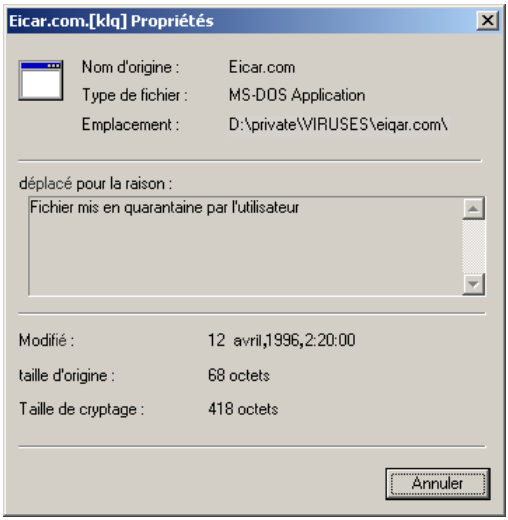


Illustration 64. Informations sur le fichier en quarantaine

Pour mettre à jour la liste des fichiers mis en quarantaine, choisissez dans le menu dynamique la commande **Rafraîchir** ou cliquez sur le bouton .

Pour extraire un fichier mis en quarantaine:

1. Choisissez son nom dans la fenêtre et cliquez sur le bouton dans la partie droite de la fenêtre ou choisissez la commande Extraire dans le menu dynamique de la liste.

2. Dans la fenêtre de l'assistant d'extraction des fichiers mis en quarantaine (Illustration 65) choisissez le répertoire dans lequel le fichier extrait sera placé. Pour ce faire, cliquez sur le bouton .

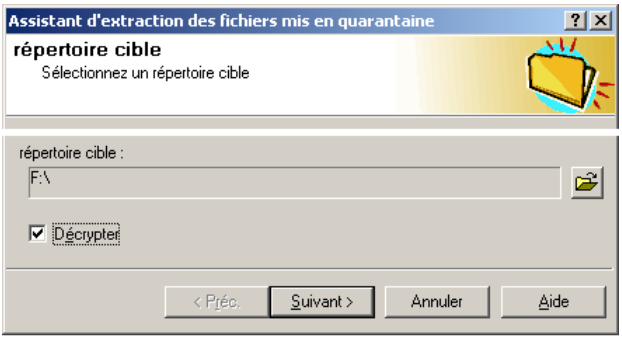


Illustration 65. Assistant d'extraction des fichiers mis en quarantaine

3. Cochez le champ **Décrypter**.
4. Cliquez sur le bouton **Suivant>**.
5. Une fenêtre d'informations apparaît dans laquelle s'affiche le déroulement de l'opération. A la fin de l'opération, cliquez sur le bouton **Terminer**.

Pour supprimer un fichier mis en quarantaine,

6. Choisissez son nom et cliquez sur le bouton ou sélectionnez la commande **Supprimer** dans le menu dynamique du fichier.
7. Une fenêtre de demande de confirmation de l'opération s'ouvre. Cliquez sur le bouton **Oui**.

Le programme ne supprimera le fichier que de la quarantaine, pas du dossier où il se trouvait initialement. Le programme ne supprimera définitivement un fichier infecté de l'ordinateur que si vous avez choisi **Supprimer** comme action à effectuer sur les fichiers infectés.

Pour mettre manuellement un fichier en quarantaine:

1. Choisissez, dans le menu dynamique, la commande **Mettre le fichier en quarantaine** ou cliquez sur le bouton . Ceci aura pour effet d'activer l'assistant de placement de fichier en quarantaine (Illustration 66).

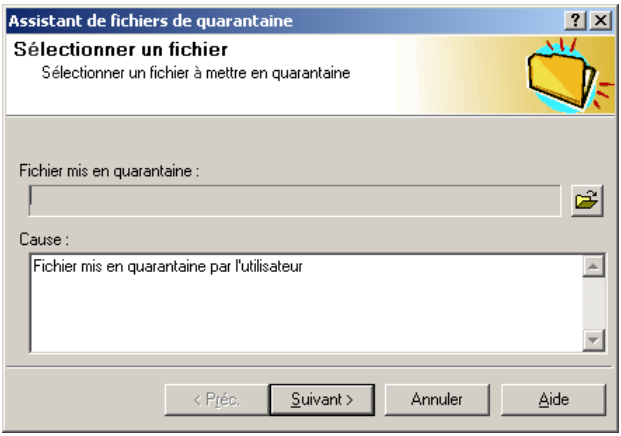


Illustration 66. Assistant de placement de fichier en quarantaine

2. Cliquez sur le bouton  et dans la boîte standard de dialogue Windows qui apparaît, sélectionnez le nom du fichier.
3. Le cas échéant, éditez le texte explicitant les motifs de mise en quarantaine du fichier dans le champ **Cause** et cliquez sur le bouton **Suivant**.
4. Une fenêtre d'informations apparaît dans laquelle s'affiche le déroulement de l'opération. A la fin de l'opération, cliquez sur le bouton **Terminer**.

6.3. Assistant de création d'une nouvelle tâche

L'exécution planifiée d'un programme déterminé, avec la liste prédéfinie des paramètres et des réglages, peut être sauvegardée sous la forme d'une tâche.

L'assistant de création d'une nouvelle tâche s'ouvre à la suite, soit de la sélection de la commande du menu contextuel **Nouvelle tâche**, soit après un clic sur le bouton  de la barre d'outils de l'onglet **Tâches** ou **Composants**.

La création d'une nouvelle tâche dans Kaspersky AV Control Centre est réalisée sous la forme de l'assistant pour Windows qui prend la forme d'une succession de fenêtres (étapes) permettant d'exécuter des actions définies.

Le passage d'une fenêtre à l'autre s'effectue en cliquant sur le bouton **Suivant** (pour avancer) et **Préc**. (pour revenir en arrière). Une fois la procédure de création de tâche terminée, cliquer sur le bouton **Terminer**. Pour annuler les actions de création de tâche, cliquer sur le bouton **Annuler**. Pour recevoir une aide opérationnelle sur une étape donnée, cliquer sur le bouton **Aide**.

6.3.1. Fenêtre Tâche

En fonction des tâches en cours d'exécution, des programmes lancés et des particularités de leurs réglages, il est possible de diviser les tâches en deux groupes:

- les tâches dont l'exécution suppose le lancement des programmes faisant partie intégrante du package Kaspersky Anti-Virus®
- les autres tâches.

La fenêtre **Tâche** (Illustration 67) est destinée à entrer le nom de la tâche et son type.

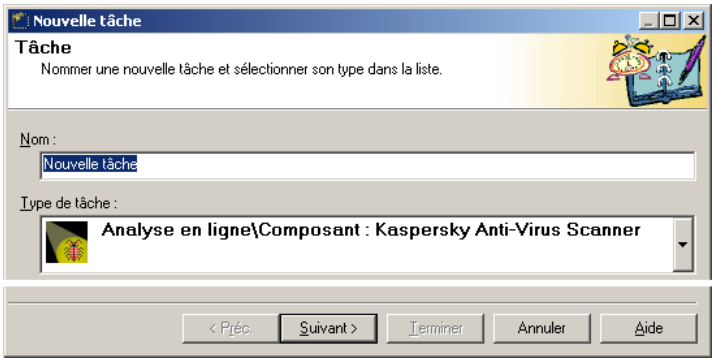


Illustration 67. Fenêtre Tâche

Par exemple, il existe les types de tâches suivants:

- **analyse de la mémoire et des disques** – lancement du Kaspersky AV Scanner avec possibilité de réglage individuel des différents paramètres d'analyse pour chacune des tâches. Les tâches peuvent être lancées automatiquement, en cas d'événement déterminé ou sur indication directe de l'utilisateur
- **analyse en temps réel** – lancement du moniteur anti-virus et/ou modification provisoire de ses paramètres de travail sans relance. Les périodes d'action de tels ou tels réglages peuvent être, soit définies rigoureusement, conformément au planning, soit dépendre de

l'intervention de certains événements dans le système, mais aussi être définies par l'utilisateur lors du changement de caractère de l'action (par exemple, pour la durée d'installation d'un nouveau logiciel, de copie de programmes et de documents provenant de l'extérieur, lors de la réception de courrier électronique, etc.)

- **mise à jour des bases anti-virus** – mise à jour automatique des bases de données d'informations relatives aux nouveaux virus. La mise à jour peut être effectuée aussi bien via Internet que par le biais du réseau local, ce qui diminue le coût de la connexion, accélère la procédure de mise à jour et facilite la gestion du package
- **lancement du programme de l'utilisateur** – tous programmes pouvant être lancés depuis Kaspersky AV Control Centre
- **installation de nouveaux programmes** – lancement de l'assistant d'installation des applications Windows.

6.3.2. Fenêtre Planification pour la tâche de Kaspersky AV Monitor

Illustration 68. Fenêtre **Planification** pour la tâche du Kaspersky AV Monitor.

Dans la fenêtre **Planification**, lors de la création d'une tâche pour Kaspersky AV Monitor (Illustration 68), il est nécessaire de définir les intervalles de lancement et d'arrêt. Pour le lancement de la tâche, aussitôt après le démarrage de Kaspersky AV Control Centre, il est nécessaire de cocher l'option **Toujours**. Pour définir l'intervalle de travail, cochez l'option **Intervalle**, régler ensuite le planning de lancement et d'arrêt du programme. Pour régler le lancement du programme, cliquez sur le bouton **Départ**, cette manipulation ayant pour effet d'ouvrir une fenêtre analogue à la fenêtre **Planification** pour la tâche de Kaspersky AV Scanner (voir plus loin la description).

Un clic sur le bouton **Stop** permet de paramétrer l'arrêt de l'exécution de la tâche.

6.3.3. Fenêtre Planification pour la tâche de Kaspersky AV Scanner et Updater

Dans la fenêtre **Planification**, lors de la création d'une tâche pour Kaspersky AV Scanner , il est indispensable de définir les conditions et la périodicité du lancement. (Illustration 69).

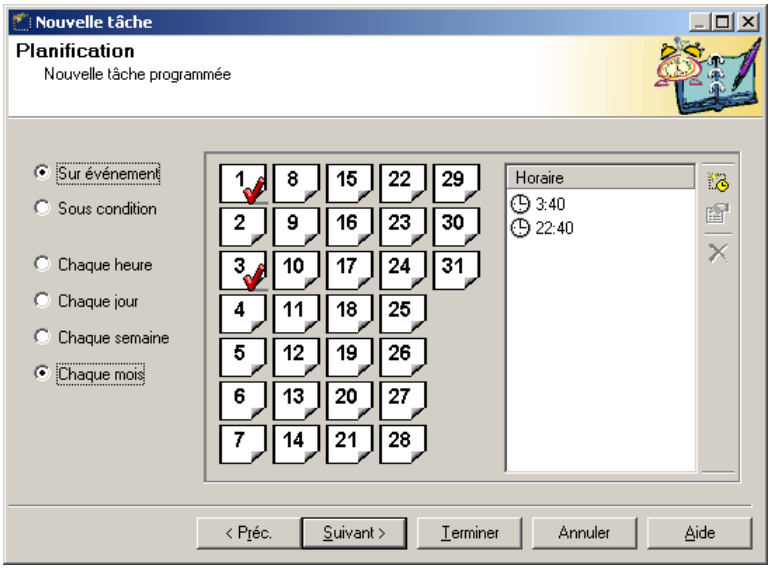


Illustration 69. Fenêtre Planification pour la tâche du Scanner et la Mise à jour automatique.

Variantes possibles de lancement:

Sur événement — lancement de la tâche lors d'un événement ou à la demande de l'utilisateur (voir "Lancement événementiel de la tâche")

Sous condition — lancement de la tâche lors de l'apparition d'une condition liée à l'achèvement d'un certain type de tâche ("Lancement conditionnel de la tâche")

Chaque heure — lancement de la tâche à un moment déterminé avec un intervalle d'une heure (voir "Lancement de la tâche

toutes les heures")

Chaque jour — lancement de la tâche chaque jour à un moment déterminé de la journée (voir "Lancement quotidien de la tâche")

Chaque semaine — lancement hebdomadaire de la tâche un jour déterminé de la semaine à un moment déterminé de la journée (voir "Lancement hebdomadaire de la tâche")

Chaque mois — lancement de la tâche un jour déterminé du mois à un moment déterminé de la journée (voir "Lancement mensuel de la tâche").

Sélectionnez la variante désirée de lancement dans la partie gauche de la fenêtre, procédez ensuite au réglage du planning conformément aux instructions fournies dans les chapitres suivants.

6.3.3.1. Lancement événementiel de la tâche

Kaspersky AV Control Centre permet d'initialiser le lancement d'une tâche en cas d'événement au niveau du système, et de régler le lancement de la tâche à la demande de l'utilisateur.

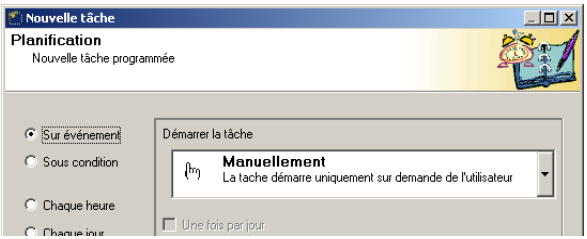


Illustration 70. Réglage du lancement événementiel

Pour choisir ce type de lancement, il est indispensable de cocher la case **Sur événement**, après quoi dans la partie droite de la fenêtre **Planification** s'affichera la liste des conditions (Illustration 70).

Sélectionnez dans la liste une des conditions de lancement. Les variantes suivantes sont possibles:

Mode manuel — la tâche est lancée depuis Kaspersky AV Control Centre à la demande de l'utilisateur

Au démarrage de Kaspersky AV Control Centre	la tâche est lancée au démarrage de Kaspersky AV Control Centre, c'est-à-dire, de fait, au moment de l'entrée de l'utilisateur dans le système
Lors du lancement de l'économiseur d'écran	la tâche est lancée lors du lancement du programme économiseur d'écran
Au démarrage du service système de Kaspersky AV Control Centre	la tâche est lancée au démarrage du service système de Kaspersky AV Control Centre, c'est-à-dire, de fait, pendant le chargement du système.

Pour tous les types de tâches on peut décider de lancer la tâche une fois par jour ou à l'occasion d'un événement donné.

6.3.3.2. Lancement conditionnel de la tâche

Kaspersky AV Control Centre permet de définir le lancement de la tâche lors de conditions déterminées liées aux résultats du travail de certains composants du package.

Dans cette version du produit, ce type de lancement est conçu de la manière suivante: l'utilisateur peut créer une tâche qui sera lancée à la condition qu'un certain composant de l'Anti-Virus Kaspersky ait achevé son travail avec un code de retour déterminé.

Pour sélectionner cette variante de lancement, mettez le commutateur situé dans la partie gauche de la fenêtre **Planification** dans l'état **Sous condition** (Illustration 71).

Ensuite, sélectionnez dans la liste **Si la tâche…** l'état de la tâche sur laquelle porte la condition, et dans la liste **s'est terminée avec le code sortie**, choisissez la valeur avec laquelle la tâche doit se terminer.

Différents types de tâches principales:

- **Lancement de Kaspersky AV Monitor**
- **Mise à jour des bases anti-virus**
- **Lancement de Kaspersky AV Scanner.**

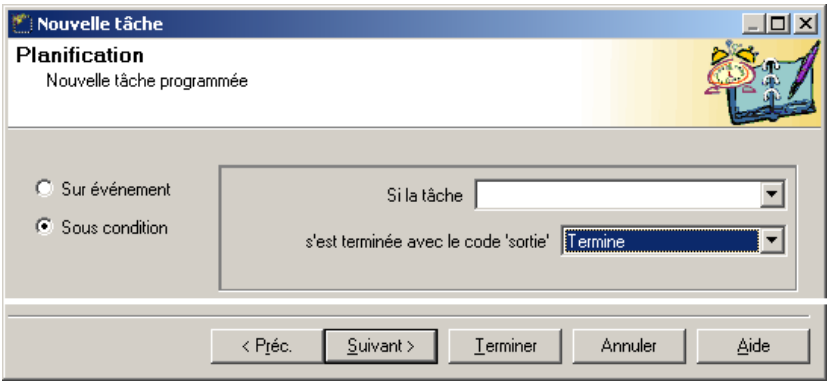


Illustration 71. Réglage du lancement conditionnel

Le programme traite les résultats suivants des tâches principales:

- **Indifférent** – la tâche créée sera exécutée aussitôt après l'exécution de la tâche principale, indépendamment du résultat obtenu
- **Terminer** – la tâche créée ne sera exécutée que si la tâche principale a été exécutée avec succès
- **Panne** – la tâche créée ne sera exécutée que si l'exécution de la tâche principale a échoué
- **Interrompu** – la tâche créée sera exécutée si la tâche principale a été interrompue par l'utilisateur.

Il arrive que les virus informatiques infectent Kaspersky AV Monitor. Dans ce cas il faut éradiquer les virus par d'autres procédés.

En utilisant cette option, il est possible, par exemple, de créer une tâche qui lancera Kaspersky AV Scanner dans le cas où Kaspersky AV Monitor a détecté une erreur lors de son lancement.

6.3.3.3. Lancement de la tâche toutes les heures

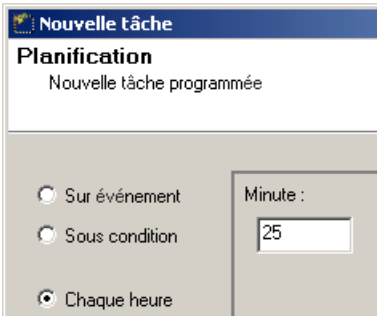


Illustration 72. Réglage du lancement de la tâche toutes les heures

Pour le lancement de la tâche créée toutes les heures, il faut choisir l'option **Chaque heure** dans la partie gauche de la fenêtre **Planification** (voir illustr. Illustration 72), après quoi entrer l'heure de lancement dans la partie droite.

L'Illustration 72 fournit un exemple de réglage du lancement de la tâche toutes les heures + 25 minutes. Ainsi, en admettant qu'il soit maintenant 12:00, la tâche sera lancée à 12:25, 13:25, 14:25, etc.

6.3.3.4. Lancement quotidien de la tâche

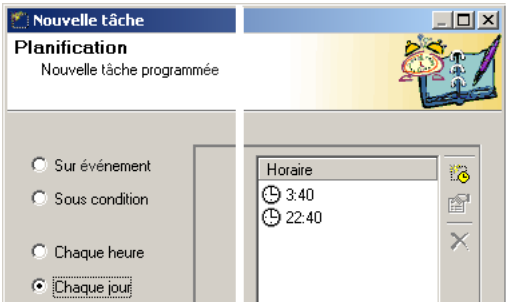


Illustration 73. Réglage du lancement quotidien de la tâche

Pour le lancement quotidien de la tâche créée à un moment déterminé, il faut choisir dans la fenêtre **Planification** l'option **Chaque jour** (Illustration 73), puis régler l'heure du lancement.

Le réglage de l'heure de lancement s'effectue dans la liste **Horaire**. A cet effet on utilise le panneau de configuration et le menu contextuel. Examinons leur rôle.

Bouton de la barre d'outils	Option du menu contextuel	Rôle
	**Ajouter…**	Ajouter un nouvel horaire de lancement. Le choix de cette option a pour effet d'ouvrir la boîte de dialogue **Ajouter un horaire**, dans laquelle il faut entrer l'heure de lancement de la tâche. Il est également possible d'appeler cette fenêtre en double-cliquant avec la souris à n'importe quel endroit libre de la liste **Heure**, ou en appuyant sur la touche **<INS>**.
	**Modifier…**	Modifier la valeur de l'heure de lancement de la tâche. Le choix de cette option a pour effet d'ouvrir la boîte de dialogue **Ajouter un horaire**, dans laquelle il est nécessaire de modifier la valeur de l'heure. Vous pouvez également double-cliquer avec la souris sur la ligne que vous voulez modifier ou bien appuyer sur la touche **<ESPACE>**.
	**Effacer…**	Effacer la notation de l'heure de lancement de la liste. Vous pouvez également appuyer sur la touche **<DEL>** de la ligne à supprimer.

6.3.3.5. Lancement hebdomadaire de la tâche

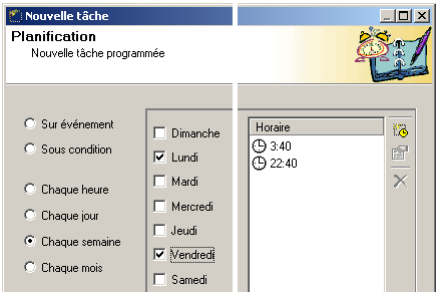


Illustration 74. Réglage du lancement hebdomadaire de la tâche

Pour le lancement hebdomadaire de la tâche certains jours déterminés et à certaines heures, il faut sélectionner l'option **Chaque semaine** dans la fenêtre **Planification**, puis entrer les jours et les heures de lancement de la tâche dans la partie droite de la fenêtre.

Pour entrer les jours et les heures de lancement de la tâche, il faut cocher les jours de la semaine et ensuite entrer l'heure dans la liste **Horaire**. Pour plus de détails sur la façon d'entrer l'heure, voir le chapitre **Lancement quotidien de la tâche**.

L'Illustration 74 montre un exemple de réglage permettant de lancer la tâche le lundi (à 3:40 et à 22:40) et le vendredi (également à 3:40 et à 22:40).

6.3.3.6. Lancement mensuel de la tâche

Pour le lancement mensuel de la tâche certains jours déterminés et à certaines heures, il faut choisir l'option **Chaque mois** dans l'onglet **Planification** (Illustration 75).

Après quoi il est nécessaire de cocher avec la souris les dates auxquelles la tâche créée sera lancée, puis entrer l'heure de lancement dans la liste **Horaire** (pour plus de détails sur la façon d'entrer l'heure dans cette liste, voir le chapitre **Lancement quotidien de la tâche**).

Les jours de lancement de la tâche sont marqués de la coche . Par exemple Illustration 75. Réglage du lancement mensuel de la tâche donne un exemple de réglage quel la tâche créée sera lancée le 1er, le 2ème, le 13ème et le 30ème de chaque mois à 3:40 et à 22:40.

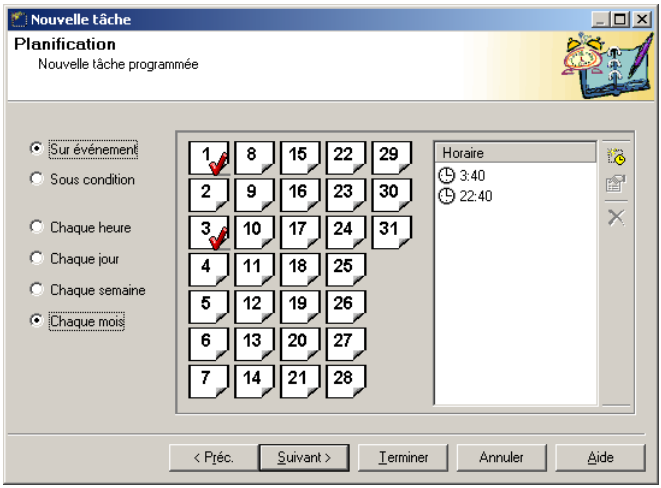


Illustration 75. Réglage du lancement mensuel de la tâche

6.3.4. Fenêtre Alertes

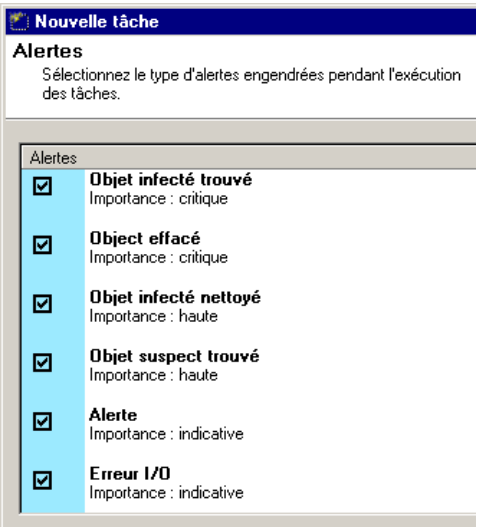


Illustration 76. Choix des types de messages

Dans la fenêtre **Alertes** (Illustration 76) il est nécessaire de cocher les types de messages d'alertes qui seront créés par la tâche.

Les messages d'alertes, comme cela a été indiqué plus haut, sont des messages générés par les tâches.

Pour sélectionner tels ou tels messages marquez-les d'une coche.

6.3.5. Fenêtre Compte utilisateur

Kaspersky AV Control Centre peut être lancé en tant que service système de Windows, c'est-à-dire avant le démarrage du système. Dans ce cas il est nécessaire d'indiquer l'inscription du compte utilisateur que la tâche utilisera.

L'inscription du compte utilisateur contient les données sur l'utilisateur (par exemple le nom complet, le mot de passe, etc.).

Le réglage du compte utilisateur peut être effectué dans la fenêtre **Compte utilisateur** (Illustration 77).

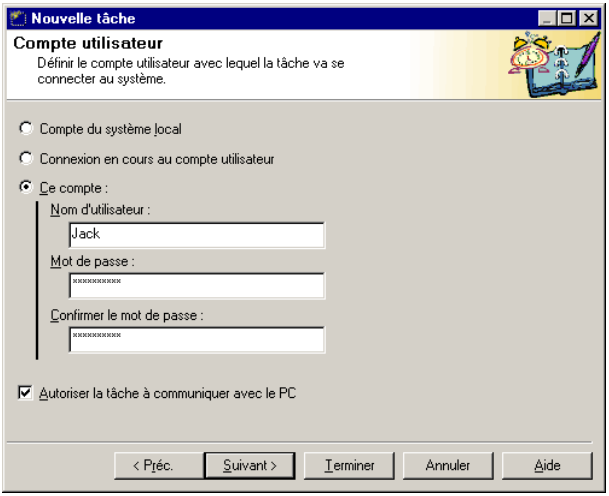


Illustration 77.Saisie du compte utilisateur pour le lancement de la tâche

Il est possible d'utiliser les inscriptions suivantes:

Compte du système local	inscription de contrôle Windows
Connexion en cours au compte utilisateur	inscription de contrôle de l'utilisateur
Autre inscription de contrôle	inscription de contrôle de l'utilisateur dont les paramètres sont indiqués plus bas dans les champs **Nom de l'utilisateur**, **Mot de passe** et **Confirmation du mot de passe**.

Pour autoriser l'accès à la tâche, cochez l'option **Autoriser la tâche à communiquer avec le PC**.

6.3.6. Réglage des options de la tâche

A cette étape de la création d'une tâche, il est indispensable d'effectuer le réglage des paramètres de la tâche qui sont caractéristiques de ce type de tâche. Comme il se doit, le contenu de ces réglages est adapté aux options choisies.

Examinons les types de tâches et les fenêtres qui apparaissent en commençant par cette étape:

Type de tâche	Succession des fenêtres	Description
Tâche de lancement de Kaspersky AV Scanner et Kaspersky AV Monitor	1. Objets	Voir paragraphe 3.3.1
	2. Options	Voir paragraphe 3.3.2
	3. Personnaliser	Voir paragraphe 3.3.3
Kaspersky AV Updater	1. Connexion	Voir paragraphe 5.2.2 ci-dessus. Cette fenêtre contient deux options supplémentaires permettant d'activer l'ajout de bases anti-virus et de modules dans le dossier spécial sur le Kaspersky AV Server.
	2. Options	Voir paragraphe 5.2.3

6.3.6.1. Fenêtre Options pour la tâche de Kaspersky AV Scanner et de Kaspersky AV Monitor

La fenêtre **Options** pour la tâche de Kaspersky AV Scanner et de Kaspersky AV Monitor est analogue, par son contenu, à la fenêtre **Options** des programmes correspondants (voir description de cette fenêtre au chapitre 3.3.2).

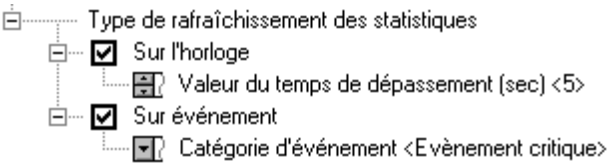


Illustration 78. Fenêtre **Options** pour la tâche de Kaspersky AV Scanner

La section **Type de rafraîchissement des statistiques** de l'arborescence des réglages (Illustration 78), dans laquelle sont définies les modalités de mise à jour des statistiques dans le composant **Kaspersky® Report Viewer**, constitue une exception.

Les Statistiques peuvent être mises à jour en utilisant le planificateur (pour ce faire, il faut cocher l'option **Sur l'horloge** et dans la fenêtre d'édition, entrer la durée de dépassement (en secondes.) Lors de la survenue d'un événement dans le système, il faut cocher l'option **Sur événement**, puis sélectionner la catégorie d'événement. Dans la version actuelle du produit, il est possible de mettre à jour les statistiques selon les événements critiques ou tout autre type d'événement.

CHAPITRE 7. KASPERSKY® REPORT VIEWER

Kaspersky® Report Viewer – est un programme de consultation et de gestion des rapports créés par les composants du package Kaspersky Anti-Virus®.

Kaspersky® Report Viewer apparaît lorsque vous sélectionnez la commande **Voir le rapport** dans la fenêtre de l'un des programmes Kaspersky AV Scanner, Kaspersky AV Monitor, Kaspersky® Inspector, ou après avoir cliqué sur le bouton **Rapport** dans la dernière fenêtre du programme de mise à jour Kaspersky AV Updater, ou dans la fenêtre principale du programme Kaspersky® Office Guard.

7.1. Description de l'interface de Kaspersky® Report Viewer

Dans la fenêtre principale du programme **Kaspersky® Report Viewer** (Illustration 79) sont disposés:

- le menu
- la barre d'outils
- la liste des sessions dans le fichier de rapport en cours (un seul fichier de rapport peut être ouvert à la fois !)
- le tableau de rapport
- la barre d'état.

Pour consulter un rapport de session, sélectionnez-le dans la partie gauche de la fenêtre, après quoi dans la partie droite s'affichera le rapport approprié.

Dans les colonnes du tableau de rapport se trouvent les informations suivantes:

- **Objet** – objet sur lequel l'action a été exécutée
- **Résultat** – résultat du travail
- **Description** – description de l'action exécutée.

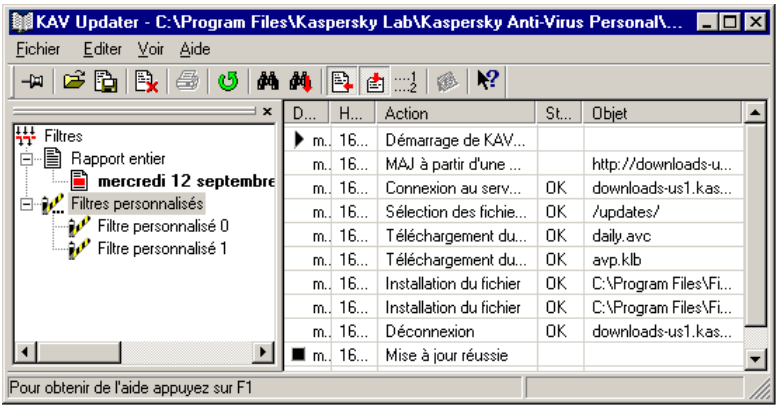


Illustration 79. Fenêtre affichant le rapport

Au-dessus du texte du rapport se trouve une barre d'outils contenant les boutons de commande correspondant aux opérations de base. Les boutons sont assortis de bulles d'aide apparaissant au passage de la souris et affichant une petite fenêtre contenant une information très brève.

Dans la partie supérieure se trouve le menu principal. Vous pouvez noter que les boutons de la barre d'outils et certaines commandes du menu ont la même fonction.

Dressons le tableau des correspondances boutons-commandes du menu et voyons leur rôle.

Barre d'outils	**Menu**	**Rôle**
	Affichage→ Toujours visible	Placer la fenêtre du programme au-dessus de toutes les fenêtres sur le bureau de Windows
	Fichier→Ouvrir	Ouvrir le rapport enregistré dans le fichier
	Fichier→ Enregistrer sous…	Sauvegarder le rapport avec un autre nom
	Fichier→ Purger	Effacer le contenu du rapport

Barre d'outils	Menu	Rôle
	Fichier→ Imprimer	Impression
	Affichage→ Actualiser	Nouveau chargement du rapport depuis le fichier
	Edition→ Rechercher	Recherche d'une ligne dans le rapport. Un clic sur ce bouton a pour effet d'ouvrir la fenêtre de recherche (voir plus bas)
	Edition→ Suivant	Recherche de la ligne suivante qui satisfait au critère de la recherche
	Affichage→ Suivi du rapport	Suivi du rapport (lors de l'activation de cette option, le rapport viendra automatiquement se positionner sur la première ligne, attendant l'arrivée de nouvelles données)
	Affichage→Voir la dernière session	Rappel du rapport correspondant à la dernière session.
	Affichage→ Uniquement les statistiques	Montrer uniquement les statistiques
	Affichage→ Commentaire	Montrer le commentaire
	Aide	Aide

Illustration 80. Fenêtre de recherche

La fenêtre de recherche (Illustration 80) apparaît dans la fenêtre de rapport après un clic sur le bouton de la barre d'outils, soit après le choix de la commande Rechercher dans la section du menu Edition. Pour rechercher une ligne (ou une portion de ligne), saisissez-la dans la fenêtre d'édition Chaîne à trouver, puis spécifiez les paramètres de recherche et cliquez sur le bouton OK

Voyons le rôle des paramètres de la recherche:

- **Correspondance avec le mot entier** – rechercher dans le rapport tous les mots coïncidant avec l'exemple qui a été entré
- **Respecter la casse** – tenir compte de la différence majuscules/minuscules lors de la recherche
- **Correspondance avec la chaîne complète** – rechercher les lignes du rapport coïncidant exactement avec la chaîne entrée.

Pour fermer la fenêtre cliquez sur le bouton **Annuler** et pour recevoir de l'aide, cliquez sur le bouton **Aide**.

Une fois que la première ligne (ou une portion de la ligne) correspondant aux critères de la recherche a été trouvée, il est possible de rechercher les autres lignes (ou sous-lignes). Pour cela il faut cliquer sur le bouton ou choisir la commande **Suivant** dans le menu **Edition**.

CHAPITRE 8. TREE-CHART™

L'interface de l'Anti-Virus Kaspersky® utilise la technologie **Tree-Chart™**.

Tree-Chart™ est une technologie universelle de présentation des données destinée aussi bien aux débutants qu'aux utilisateurs expérimentés et élaborée par les spécialistes de la société Kaspersky Labs. Avec cette technologie, toutes les données sont présentées sous la forme d'une arborescence dont les nodules constituent les éléments standards de gestion (boutons, listes, commutateurs, etc.).

Cette technologie permet de matérialiser l'interdépendance des différents réglages et facilite le paramétrage du programme.

Dans cette documentation, à côté du nom de chaque élément se trouve indiqué le type d'icône qui lui correspond.

8.1. Arborescence des réglages

Chaque nodule de l'arborescence des réglages peut avoir des branches. Si une branche est déployée, le signe du nodule correspondant aura l'aspect  , mais si la branche est repliée, le signe se changera en  .

Pour modifier un réglage, il est indispensable de déployer la branche appropriée.

Il est possible de déployer ou de replier une branche par un des procédés suivants:

Action à réaliser	**Comment faire**
Déployer la branche (nodule avec le signe )	Touche → du clavier. Commande  du menu contextuel. Touche **<+>** du pavé numérique (les deux branches du nodule se déploient).

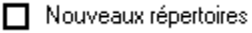
Action à réaliser	**Comment faire**
Replier la branche (nodule avec le signe )	Touche ← du clavier. Commande  du menu contextuel. Touche **<->** du pavé numérique (toutes les branches du nodule se replient).

8.2. Types d'éléments de gestion

Pour régler les différents paramètres de vérification dans le programme, on utilise plusieurs types d'éléments de gestion:

8.2.1. Commutateur

Le **Commutateur** peut se trouver dans deux états:

 — commutateur désactivé. La vérification n'est pas effectuée

 — commutateur activé. La vérification est effectuée

Comment modifier l'état des commutateurs:

Action à réaliser	**Comment faire**
Activation du commutateur	Touche <**ESPACE**> du clavier. Commande  du menu contextuel. Clic avec la souris.
Désactivation du commutateur	Touche **<ESPACE>** du clavier. Commande  du menu contextuel. Clic avec la souris.

8.2.2. Bouton d'option

Les **Boutons d'option** doivent obligatoirement être regroupés dans des groupes composés au minimum de deux boutons de choix, chaque bouton correspondant à l'une des variantes possibles que peut prendre le réglage. Chaque bouton peut se trouver dans deux états:

 — bouton d'option désactivé

 — bouton d'option activé

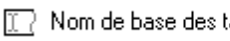
Un seul indicateur de chaque groupe peut être activé.

Comment modifier l'état des boutons d'option:

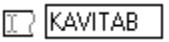
Action à réaliser	**Comment faire**
Activation du bouton d'option	Touche **ESPACE** du clavier. Commande  du menu contextuel. Clic avec la souris.
Désactivation du bouton d'option	Activation de l'autre bouton d'option.

8.2.3. Champ de saisie

Champ de saisie — La valeur de ce champ est saisie directement sur le clavier. La valeur actuelle de ce champ est indiquée entre mini-parenthèses après le nom du champ.

 — champ de saisie.

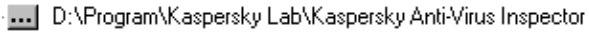
Comment modifier la valeur du champ de saisie:

Action à réaliser	**Comment faire**
Modification de la valeur du champ de saisie	Clic avec la souris sur l'icône de ce champ. Commande  du menu contextuel. Touche F2. Le champ prend l'aspect suivant:  .

A la fin de l'édition, cliquez sur la touche Entrée, ou cliquez avec la souris à l'extérieur du champ. Vous pouvez appuyer sur la touche Echap pour rappeler les anciennes valeurs du champ.

8.2.4. Champ de saisie d'un chemin d'accès

Champ de saisie d'un chemin d'accès — la valeur de ce champ est modifiée depuis la boîte de dialogue standard de Windows.

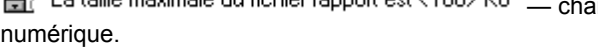
 — champ de saisie d'un chemin d'accès.

Comment modifier le chemin d'accès:

Action à réaliser	**Comment faire**
Modification de la valeur du champ de saisie d'un chemin d'accès	Clic de la souris sur l'icône de ce champ. Commande  du menu contextuel. Touche F2.

8.2.5. Champ de saisie d'une valeur numérique

Champ de saisie d'une valeur numérique — la valeur de ce champ est entrée directement depuis le clavier ou en cliquant sur les petits boutons fléchés. La valeur courante de ce champ est indiquée entre mini-parenthèses après le nom du champ.

 — champ de saisie de la valeur numérique.

Comment modifier la valeur du champ de saisie d'une valeur numérique:

Action à réaliser	Comment faire
Modification de la valeur du champ de saisie de la valeur numérique	Clic avec la souris sur l'icône de ce champ. commande  du menu contextuel. Touche F2.

Si le premier caractère du numéro est un zéro, le logiciel l'interprète comme une notation en octal, et le convertit en un nombre décimal.

8.2.6. Liste déroulante

La liste déroulante est destinée à la sélection de l'un des éléments (Illustration 81). Pour se déplacer dans la liste on peut utiliser les touches ↑ et ↓. Pour dérouler automatiquement la liste on utilise les touches **Ctrl+** ↑ et **Ctrl+** ↓.

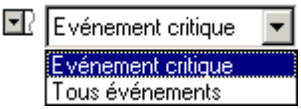


Illustration 81. Liste déroulante

8.3. Indicateurs de réglages

Lors du paramétrage des vérifications s'appliquant à l'arborescence des disques dans le programme, on utilise ce qu'on appelle les **règles d'héritage**, c'est-à-dire que si vous avez attribué des paramètres particuliers à l'élément Poste de Travail (Illustration 82), ces réglages s'appliquent à tous les disques de l'ordinateur.

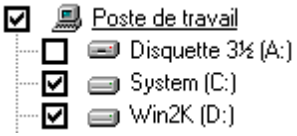


Illustration 82. Arborescence des disques

A chaque élément de la hiérarchie correspond un *indicateur de réglages* qui peut être activé ou désactivé, et des *règles* qui s'appliquent à cet élément.

L'indicateur de réglages montre si le régime de vérification de l'élément de la hiérarchie est activé ou désactivé et les règles établissent le procédé de vérification dudit élément.

Par défaut, tous les éléments *héritent de la règle du groupe de la hiérarchie* dans laquelle ils entrent. En cas de changement d'une règle du groupe, toutes les règles des éléments entrant dans ce groupe sont en même temps modifiées.

Vous pouvez assigner à certains éléments leurs propres règles ou modifier l'état de leurs indicateurs de contrôle. Ces éléments auront des *règles indépendantes*. En cas de modification d'une règle du groupe, ces éléments conserveront leurs règles. Cependant, en cas de changement de l'état de l'indicateur de contrôle de groupe, les éléments passent de nouveau en régime d'héritage.

Vous pouvez désactiver complètement le régime d'héritage des règles de l'élément en sélectionnant dans le menu dynamique la commande **Etablir Mode Strict**. Après quoi, l'indicateur de contrôle prendra l'aspect d'un carré rouge avec une coche noire à l'intérieur. Nous dirons que de tels éléments *ont des règles strictement indépendantes*. Ces éléments conserveront leurs règles, même en cas de modification des indicateurs de contrôle du groupe. Vous pourrez alors de nouveau assigner le régime d'héritage en sélectionnant dans le menu dynamique la commande **Annuler Mode Strict**.

L'indicateur de réglage peut avoir l'aspect suivant:

Aspect de l'indicateur	Description de l'indicateur	Valeur
	Le carré avec une coche à l'intérieur peut être rouge ou noir.	Mode de vérification activé. **Carré rouge** – mode d'héritage des règles désactivé. **Carré noir** – mode d'héritage des règles activé.
	Carré avec une coche à l'intérieur et un triangle dans l'angle inférieur droit. Le triangle peut être rouge ou noir..	Le mode d'héritage des règles est activé mais certains objets sont exclus du groupe ou ont leurs propres réglages. **Triangle rouge** – pour un ou plusieurs objets, le régime d'héritage des règles est désactivé. **Triangle noir** – pour un ou plusieurs objets la règle est modifiée.
	Carré sans coche avec un triangle dans le coin inférieur droit. Le triangle peut être rouge ou noir.	Mode de vérification désactivé. Pour un ou plusieurs objets, le mode de vérification est installé. **Triangle rouge** – pour un ou plusieurs objets, le mode d'héritage des règles est désactivé. **Triangle noir** – pour un ou plusieurs objets la règle est modifiée.

CHAPITRE 9. KASPERSKY ANTI-VIRUS® SCRIPT CHECKER

Kaspersky Anti-Virus® Script Checker est un programme anti-virus qui protège votre ordinateur contre les virus de script et les vers qui s'exécutent directement dans la mémoire de l'ordinateur.

9.1. Principe de fonctionnement

Les différents programmes utilisant Microsoft Windows Script Host (comme Microsoft Explorer, Microsoft Internet Explorer, Microsoft Outlook**, etc**.) transmettent dans le Script Hosting aux fins de traitement et d'exécution consécutive les scripts (tels que VB Script et Java Script). Avant l'exécution de ces fichiers script, Script Checker les envoie pour vérification au module Kaspersky AV Monitor (si ce dernier est installé et lancé), et si le moniteur n'a pas détecté de virus, il effectue une analyse heuristique3 du code du fichier script. En cas de suspicion de virus, Script Checker émet un message d'alerte approprié et interdit l'exécution de ce script.

Script Checker n'utilise pas les bases anti-virus. Les bases de données anti-virus sont utilisées par Kaspersky AV Scanner et Kaspersky AV Monitor. L'avantage de Script Checker sur les autres programmes anti-virus consiste dans le fait qu'il permet de prévenir l'utilisateur de la possibilité d'infection par un nouveau virus non encore décrit dans les bases de données anti-virus.

Les fichiers script dans le système d'exploitation Windows s'exécutent dans la mémoire de l'ordinateur sans appel préalable au disque, c'est pourquoi les moyens de protection comme le moniteur anti-virus ne peuvent pas vérifier les fichiers script avant leur exécution. Script Checker permet d'intercepter l'exécution des fichiers script et de les transmettre au moniteur pour vérification. Ainsi, Script Checker en combinaison avec le moniteur anti-virus offre à l'utilisateur une protection complète contre tous les types de virus.

Examinons l'exemple suivant de situation où Script Checker protège votre ordinateur contre un virus.

3 Analyse heuristique – analyse de la succession des commandes dans un objet en cours de vérification, s'appuyant sur un ensemble de statistiques pour déterminer une "possibilité d'infection" ou une "absence d'infection" (pour plus de détails voir sur www.viruslist.com).

Admettons que vous alliez sur un site WEB qui contient un virus de script ressemblant à LoveLetter[4]. Si votre navigateur Internet a un faible niveau de protection, l'exécution du virus de script sera lancée immédiatement. Script Checker est chargé d'empêcher l'exécution du script infecté et de protéger ainsi votre ordinateur contre une attaque virale. En outre, Script Checker émet un message d'alerte ci-dessous (Illustration 83).

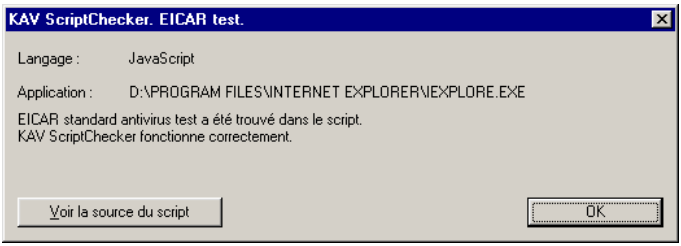


Illustration 83. Message d'alerte - possibilité de virus

4 LoveLetter – virus (ver) Internet dangereux ayant massivement infecté des ordinateurs en mai 2000. Le ver s'est répandu par l'intermédiaire des e-mails. Lors de son activation, il se diffusait en utilisant le carnet d'adresses Microsoft Outlook (pour plus de détails lire dans www.viruslist.com).

CHAPITRE 10. KASPERSKY ANTI-VIRUS® RESCUE DISK

Le package Anti-Virus Kaspersky® est équipé du programme spécial **Kaspersky Anti-Virus® Rescue Disk** permettant de créer un jeu de *disquettes de secours*.

Les disquettes de secours sont destinées à restaurer les capacités opérationnelles du système après une attaque virale. Ces disquettes comportent:

- les fichiers système du système d'exploitation Linux
- le scanner anti-virus
- les bases de données anti-virus.

Le principe de fonctionnement des disquettes de secours est le suivant. Supposons qu'après une offensive virale votre ordinateur ne puisse plus démarrer à partir du disque dur. Dans ce cas il est indispensable de faire appel à une disquette de démarrage. Celle-ci charge dans l'ordinateur le système d'exploitation Linux, puis lance le module Kaspersky Anti-virus® Scanner. Le cas échéant, elle demande également d'insérer les autres disquettes, celles qui contiennent les bases anti-virus. Si un virus est détecté, l'analyseur attendra des instructions de votre part sur la manière de procéder: supprimer le virus du fichier, supprimer le fichier infecté ou enregistrer l'événement dans le journal.

10.1. Préparation des disquettes de secours

Le programme de préparation des disquettes de secours **Kaspersky Anti-Virus® Rescue Disk** est lancé depuis le menu principal de Windows dans le groupe de programmes Kaspersky Anti-Virus®. Pour démarrer le programme, il est indispensable de choisir la commande **Kaspersky Anti-Virus® Rescue Disk**, ce qui a pour effet d'ouvrir la première boîte de dialogue Configuration de l'assistant de préparation des disquettes de secours (Illustration 84). Pour vous déplacer à la fenêtre suivante de l'assistant, cliquez sur **Suivant** dans la boîte de dialogue courante.

Illustration 84. Bienvenue dans la création des disquettes de secours Kaspersky®

Spécifiez dans la boîte de dialogue **Configuration** (Illustration 85) le type de disquettes que vous voulez créer.

- ☑ **Disquette bootable contenant les fichiers exécutables** – la disquette de démarrage contenant les fichiers du système d'exploitation Linux et les fichiers exécutables de Kaspersky Anti-Virus®.
- ☑ **Disquettes contenant les bases virales** – disquettes contenant les définitions de virus et les méthodes de suppression utilisées. Il est recommande de mettre régulièrement à jour les bases de données anti-virus de ces disquettes.

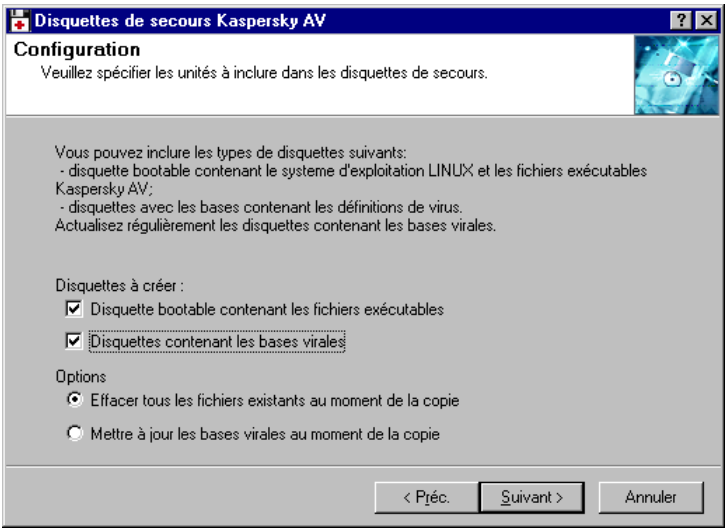


Illustration 85. Fenêtre **Configuration**

La disquette bootable (ou disquette de démarrage) contenant les fichiers du système d'exploitation Linux et les fichiers exécutables de l'Anti-Virus Kaspersky peut être créée une fois pour toutes. Quant à la disquette contenant les bases anti-virus, il est recommandé de la recréer lors de chaque mise à jour.

Le groupe **Options** vous permet de spécifier comment créer les disquettes de bases de données anti-virus:

- **Effacer tous les fichiers au moment de la copie** – supprime tous les fichiers du disque avant d'y copier les bases de données antivirales.
- **Mettre à jour les bases virales au moment de la copie** – copie uniquement les mises à jour de bases de données sur disquette. Avec cette cette option, le logiciel compare les bases de données du disque avec leurs mises à jour avant de copier ces dernières uniquement. Si les bases de données sont les mêmes, le logiciel ne copie aucun fichier vers la disquette.

Si vous sélectionnez **Mettre à jour les bases virales au moment de la copie**, vous devez insérer les disquettes de bases de données anti-virus dans l'ordre où elles ont été créées.

Dans la boîte de dialogue suivante Bases virales (Illustration 86), il est indispensable de spécifier le chemin d'accès au fichier AVP.SET. Ce fichier fait partie intégrante du package de l'Anti-Virus Kaspersky® et contient la liste des bases de données anti-virus accessibles.

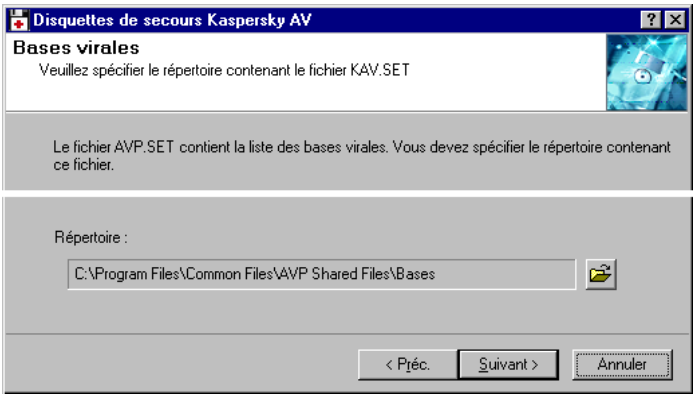


Illustration 86. Base virales

Dans la boîte de dialogue Destination (Illustration 87), sélectionnez l'unité logique vers laquelle les fichiers seront copiés.

Illustration 87. **Destination**

Ensuite le programme effectue une copie des fichiers vers l'unité logique sélectionnée (Illustration 88. Copie des fichiers en **cours**). Durant la procédure de copie, il est possible que le programme demande d'insérer des disquettes complémentaires.

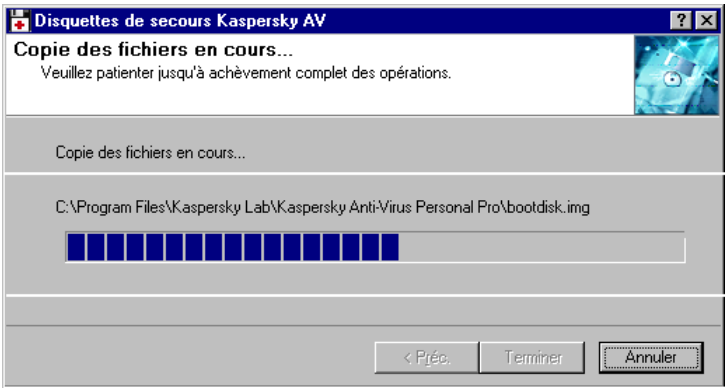


Illustration 88. **Copie des fichiers en cours**

A la fin de la procédure de copie des fichiers sur les disquettes, la boîte de dialogue du programme affiche la fenêtre **Terminer** (Illustration 89). Elle signifie que le programme de création des disquettes de secours a terminé son travail.

Les disquettes ainsi obtenues constituent le jeu de disquettes de secours.

Illustration 89. Terminer

10.2. Utiliser les disquettes de secours

Lors de l'utilisation des disquettes de secours, il est recommandé de respecter l'ordre suivant dans la succession des actions:

1. Insérez la disquette de boot (ou disquette de démarrage) dans le lecteur et redémarrez l'ordinateur. Après le redémarrage du système d'exploitation, le scanner anti-virus sera lancé. Il vérifiera les secteurs d'amorçage et le Master Boot Record de votre ordinateur. En cas de détection de virus, le programme supprimera automatiquement les virus découverts. Ensuite, le programme affichera sur l'écran une demande du type :

   ```
   Please select a device for swapping.
   N …
   1. /dev/ide/host0/bus0/target0/lun0/part 1
   2. /dev/ide/host0/bus0/target0/lun0/part 5
   0. No swap (Recommended)
   Please enter the preferred partition number and press ENTER.
   ```

   Vous devez sélectionner le disque sur le lequel le système enregistrera les données temporaires en indiquant son numéro. Les noms des disques sont affichés au format Linux. Après quoi, le programme demandera un disque sur lequel sera enregistré le fichier avec le rapport.

Observez les informations sur le noms de lecteurs au format du système d'exploitation Linux OS qui Illustrationnt au dessus de la demande de disquettes de données temporaires. Vous aurez besoin de ces noms par la suite, lorsque vous choisirez de démarrer vous-même le logiciel anti-virus. Le format de données est:

```
Remounting root filesystem in read-write mode.

/dev/ide/host0/bus0/target0/lun0/part1 (Vfat) has been mounted to /mnt/disk1
```

Il n'est pas conseillé d'utiliser les disquettes de secours avec un système de fichiers NTFS. Si le dispositif est du type **ntfs**, ne le sélectionnez pas, ou lancez votre analyseur anti-virus pour vérifier et supprimer les virus qui pourraient s'y trouver.

2. À la demande du logiciel, insérez la disquette appropriée du jeu de disquettes de secours. Après avoir copié les bases de données anti-virus depuis la disquette, remplacez-les en cliquant sur

<ENTREE> trois fois, afin de lancer l'opération. Le logiciel lance ensuite l'analyse pour rechercher des virus dans votre ordinateur.

3. Lorsqu'il détecte un virus, le logiciel présente un message de ce type:

File <nom_fichier> Infected by virus:<nom_virus>
Actions – Report only (Ok, disInfect/Delete/Cancel/Stop)

où <nom_fichier> est le nom du fichier infecté, et <nom_virus> celui du virus détecté. En tapant l'un des caractères suivants, vous pouvez indiquer de quelle manière le logiciel procédera avec le fichier infecté:
O ou pas de saisie – enregistre les détails du virus,
I – essaie de désinfecter le fichier,
D – supprime le fichier infecté,
C – ignore le fichier,
S – interrompt l'analyse.

Le logiciel vous demande ensuite si vous souhaitez appliquer la même action à tous les fichiers infectés qui seront détectés par la suite:

Apply to all infected objects? – Yes/No

Pour répondre, tapez l'un des caractères suivants:
Y – applique l'action sélectionnée à tous les fichiers infectés qui seront détectés par la suite;
N – affichera la même question chaque fois qu'un fichier infecté est détecté

4. Après l'analyse, un tableau statistique est présenté sur votre écran. Examinez ces statistiques puis appuyez sur la touche **<ENTREE>**.

- **Sector objects** – secteurs traités ;
- **Files** – fichiers traités ;
- **Folders** – dossiers traités ;
- **Archives** – archives traitées ;
- **Packed** – objets compressés exécutables ;
- **Known viruses** – virus connus détectés ;
- **Viruses bodies** – corps de virus détectés ;
- **Disinfected** – objets désinfectés ;
- **Deleted** – objets supprimés;
- **Warnings** – avertissements générés ;
- **Suspicious** – objets suspects détectés ;

- **Corrupted** – objets endommagés détectés ;
- **I/O errors** – erreurs d'entrée sortie apparues .
- **Speed (Kb/sec)** – vitesse moyenne de l'analyse, en Ko/sec .
- **Scan time** – durée totale de l'analyse .

5. Un menu d'actions s'affichera sur votre écran:

1: Run kavscanner
2: See config
3: See report
4: Exit
Your choice [1,2,3,4]>

- Tapez le numéro de votre choix:

- **1** – démarre à nouveau l'analyseur anti-virus. Si vous choisissez cette option, la question suivante est affichée sur votre écran:

- **Enter directories for scanning>**

- Spécifiez les répertoires à analyser dans le format du système d'exploitation Linux, en ayant soin de les séparer par des espaces. Par exemple, le répertoire du disque C: appelé **work** ressemblera a ce qui suit, dans la notation du système Linux: /mnt/disk1/work. Les noms de disquettes s'affichent sur votre écran après avoir inséré la première voir plus haut).

- Après avoir indiqué les répertoires, le logiciel demande les disquettes des bases anti-virus, puis lance l'analyse des emplacements sélectionnés.

- **2** – affiche la configuration de l'analyseur anti-virus.
- **3** – affiche les résultats de l'analyse précédente.
- **4** – quitte le logiciel.

6. Après l'analyse et la réparation, pressez sur les touches <Ctrl>+<Alt>+<Suppr> pour redémarrer l'ordinateur en prenant soin de retirer la disquette de secours du lecteur.

CHAPITRE 11. KASPERSKY ANTI-VIRUS® MAIL CHECKER

Le programme **Kaspersky Anti-Virus® Mail Checker** est destiné à garantir la protection antivirale des ordinateurs utilisant des messages électroniques transitant par un logiciel compatible avec Microsoft Exchange Client, notamment Microsoft Outlook 98/2000/XP .

Actuellement Kaspersky AV Mail Checker n'est pas compatible avec Outlook Express et TheBat!.

Le logiciel Kaspersky AV Mail Checker exécute les fonctions suivantes:

- Vérification de la présence de virus dans tous les messages entrants ou sortants. Le logiciel vérifie les messages juste au moment de leur réception ou de leur envoi, et y recherche des virus aussi bien dans le corps du message que dans les pièces jointes.

Kaspersky AV Mail Checker recherche également des virus à l'intérieur des archives incorporées, des fichiers exécutables compressés, les fichiers de texte et les bases de données de messages électroniques.

- Vérification de la présence de virus dans les messages stockés dans la boîte aux lettres locale avant que vous n'installiez le logiciel Kaspersky AV Mail Checker. Ces messages sont vérifiés lorsque l'utilisateur les ouvre.
- Permet à l'utilisateur de désinfecter les messages avec un virus.
- Kaspersky AV MailChecker supprime les objets infectés des messages et si tous les éléments du message sont infectés, il supprime le message entièrement.

Les paramètres anti-virus sont définis à partir du logiciel utilisé comme client de messagerie.

Tout en contrôlant les boîtes au lettres intégrées au client de messagerie, les fonctionnalités du logiciel restent limitées: il ne vérifie par les messages lorsqu'ils arrivent dans les boîtes aux lettres. Les messages sont vérifiés uniquement lorsque l'utilisateur les ouvre.

11.1. Configuration de Kaspersky AV Mail Checker

Les paramètres de protection du destinataire peuvent être affichés et modifiés sur l'onglet **Kaspersky Anti-Virus® MailChecker** de la fenêtre **Options** qu'il est possible d'ouvrir depuis le client de messagerie Microsoft Outlook 98/2000/XP.

Pour afficher la fenêtre Options dans Microsoft Outlook:

1. Démarrez Microsoft Outlook ;
2. Choisissez **Options** dans le menu **Outils** ;
3. Activez l'onglet **Kaspersky Anti-Virus® MailChecker**.

L'onglet **Kaspersky Anti-Virus® MailChecker** présente les paramètres de la boîte au lettres (Illustration 90):

- Activer ou désactiver la protection antivirus de vos courriers entrants ou sortants. Pour ce faire, cochez ou décochez la case ☑ **Activer la protection** ;
- Programmer l'affichage d'un message d'avertissement lorsque le client de messagerie tente d'envoyer un message infecté (case ☑ **Afficher un message d'alerte en cas de détection**).

Kaspersky Anti-Virus® MailChecker incorporé dans cette version de Kaspersky Anti-Virus® Personal/Personal Pro ne permet pas d'utiliser une approche unifiée de traitement des messages infectés.

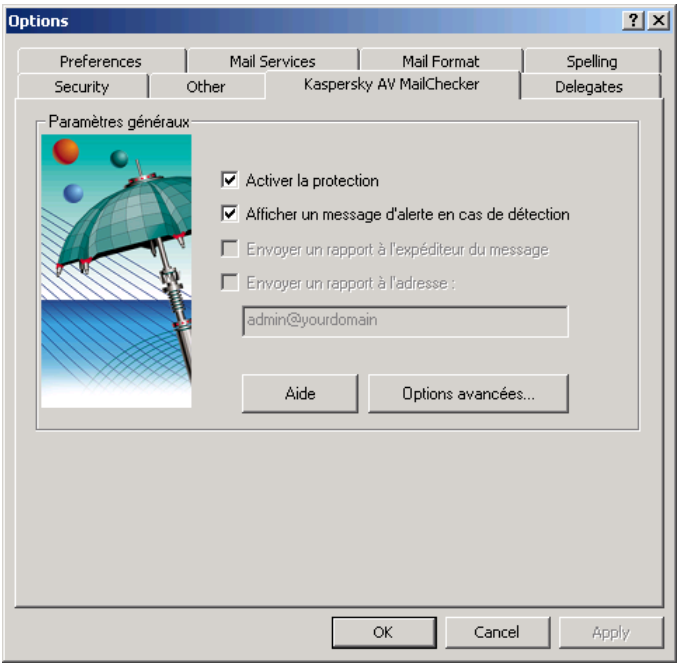


Illustration 90. La fenêtre **Options** affichant l'onglet **Kaspersky Anti-Virus® MailChecker**

11.2. Utilisation de Kaspersky® MailChecker

Juste après son installation, Kaspersky AV Mail Checker commencera a afficher des messages d'avertissement. Vous ne verrez ce messages, cependant, que si des virus sont détectés dans vos message sortants (et vous avez coché la case ☑ **Afficher un message d'alerte en cas de détection**).

Nous décrivons ci-après les différences dans le traitement par Kaspersky AV MailChecker du trafic entrant et sortant .

11.2.1. Messages entrants

Les messages entrants sont vérifiés automatiquement juste après leur arrivée dans la boîte aux lettres protégée. Si ces messages sont sains, vous les recevez tout de suite. Si Kaspersky Anti-Virus® détecte un objet infecté, il essaie de le

nettoyer. Si l'opération échoue, l'objet sera supprimé du message. Si la désinfection réussit, le message contenant l'objet infecté est remis immédiatement après le traitement.

Remarquez que l'application ne vous informe pas de la désinfection / suppression d'un objet dans le message.

Si tous les objets du message sont infectés, celui-ci vous parviendra si au moins un des objets a été désinfecté. Dans le cas contraire, le message est entièrement supprimé.

Remarquez que l'application ne vous informe pas de la suppression du message.

11.2.2. Messages sortants

La présence de virus est vérifiée dans les messages sortants dès que l'utilisateur appuie sur **Envoi**. En cas de message sortant infecté, le logiciel tente de le désinfecter (si l'option correspondant est active).

Si la case **Afficher un message d'alerte en cas de détection** n'est pas cochée, le traitement du message se fera en arrière-plan, sans intervention de votre part. Les message sains seront transmis aux correspondants et ceux infectés seront soumis au traitement approprié. Après le traitement, les messages seront :

- *envoyés*, si la désinfection réussit ;
- *envoyés sans pièces jointes* si le programme échoue dans la désinfection de celles-ci ;
- *supprimés* si la désinfection du message ou de TOUTES les pièces jointes échoue.

Si la case ☑ **Afficher un message d'alerte en cas de détection** est cochée, l'utilisateur devra répondre aux messages affichés par le logiciel :

1. Si le logiciel détecte une pièce jointe infectée sans parvenir à la désinfecter, un avertissement est affiché à l'écran (Illustration 91. Avertissement de).

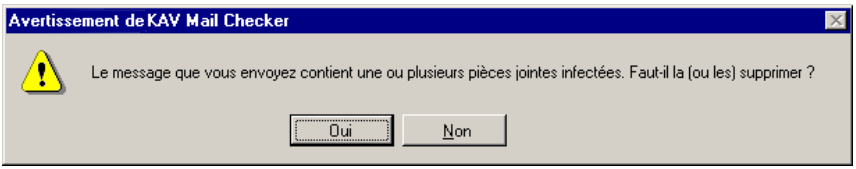


Illustration 91. Avertissement de pièces jointe infectée dans un message sortant

- Cliquez sur **Oui** pour supprimer la pièce jointe et envoyer ce message au destinataire.

- Cliquez sur **Non** , si vous ne souhaitez pas envoyer le message sans pièce jointe. Si le message est infecté, le logiciel affichera l'avertissement approprié (Illustration 92). Annulez l'envoi en cliquant sur **Non**.

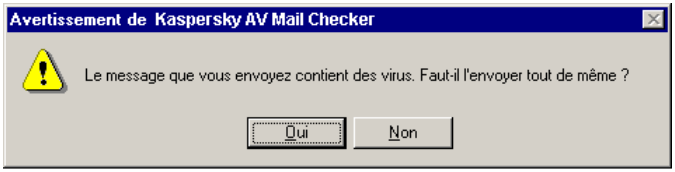


Illustration 92. Le message sortant est infecté !

11.2.3. Messages dans la boîte aux lettres

Kaspersky AV Mail Checker la présence de virus dans les messages stockés dans la boîte aux lettres avant que vous n'installiez le logiciel proprement dit. Ces messages sont vérifiés à leur ouverture. Dans ce cas, le logiciel contrôle ces messages comme s'ils étaient arrivés dans votre boîte aux lettres.

CHAPITRE 12. KASPERSKY ANTI-VIRUS® PERSONAL PRO

Le package Personal Pro a été spécialement conçu pour assurer une protection antivirale complète des PC fonctionnant avec les systèmes d'exploitation Windows 95 OSR2/98/ME, Windows 2000/NT, les applications de MS Office 2000, ainsi qu'avec les programmes de messagerie électronique Outlook, Outlook Express. Il ajoute deux composants supplémentaires à ceux de la version Personal (voir Chapitre 1):

- **Kaspersky® Office Guard** est un programme de protection des documents Office 2000, contre les virus de macro connus et inconnus. Kaspersky® Office Guard contrôle le fonctionnement des macros créées en Visual Basic pour Applications dans les applications de Microsoft Office 2000. Lors d'une tentative d'exécution d'une macro-commande suspecte, le programme Office Guard, en fonction du niveau de protection choisi par l'utilisateur, réalise une des quatre actions suivantes: interdire l'exécution de la commande, l'autoriser, stopper complètement la macro ou demander à l'utilisateur de sélectionner une des trois variantes ci-dessus.
- **Kaspersky® Inspector** est un programme d'inspection du disque géré par le système d'exploitation Microsoft Windows 95 OSR2/98/ME ou Microsoft Windows NT/2000. Kaspersky® Inspector teste les disques et recherche les modifications intervenues dans le contenu des fichiers et des répertoires. Ce programme peut être utilisé comme programme anti-virus auxiliaire ou comme programme de contrôle des changements intervenus sur le disque.

L'installation du package Anti-Virus Kaspersky® Personal Pro est identique à l'installation du package Anti-Virus Kaspersky® Personal.

CHAPITRE 13. KASPERSKY® OFFICE GUARD

Le programme Kaspersky® Office Guard est destiné à la protection des documents Microsoft Office 2000 contre les virus de macro aussi bien connus qu'inconnus. Si un virus de macro est présent dans un document, Kaspersky® Office Guard le détectera, quel qu'en soit le type, et exécutera les actions appropriées.

Le programme Kaspersky® Office Guard exécute les fonctions suivantes:

- Il contrôle le travail des macros écrites en langage Visual Basic pour Applications (VBA) dans les applications de Microsoft Office 2000. Dès qu'une macro est lancée, le programme intercepte chaque commande exécutée par cette macro et vérifie si elle Illustration dans la liste des *commandes de macro suspectes* – c'est-à-dire des commandes susceptibles d'avoir été exécutées par un code de virus.

La liste des macro-commandes suspectes, leur description et les informations sur la fréquence d'utilisation de ces commandes par des virus sont données au système d'aide

- Lorsqu'une macro tente d'exécuter une macro-commande suspecte, le programme Kaspersky® Office Guard peut, en fonction du niveau de protection antivirale assigné par vous (voir paragraphe 13.3.1), choisir une des quatre actions suivantes: interdire l'exécution de la commande, l'autoriser, arrêter complètement la macro ou demander à l'utilisateur de choisir une des trois variantes mentionnées ci-dessus.

Le programme Kaspersky® Office Guard détecte à coup sûr les actions de tout virus de macro contenu dans un document Microsoft Office 2000. Cependant il vous appartient personnellement de décider que l'action suspecte exécute précisément un virus de macro pour ensuite lancer le scanner anti-virus ou transmettre le document infecté à l'administrateur. Le système d'aide contient les informations qui vous aideront à prendre la bonne décision.

13.1. Kaspersky® Office Guard – protection contre les virus de macro inconnus

Pour automatiser l'exécution des actions qui se répètent dans des logiciels de traitement de texte, des tableurs, des gestionnaires de bases de données et des systèmes de conception sont intégrés des langages permettant de créer des macros. Ces langages peuvent avoir une structure complexe et un jeu étendu de commandes.

Le virus de macro est un programme écrit dans ce macro-langage qui exécute des actions destructrices et transfère son code depuis le fichier infecté (document ou tableau) vers d'autres fichiers.

A la fin de l'an 2000, on connaissait plusieurs systèmes dans lesquels des virus de macro avaient été détectés. Il s'agissait des principales applications de Microsoft Office, intégrant le macro-langage VBA (Visual Basic pour Applications):

- le traitement de texte Microsoft Word (Microsoft Word 6/7 intègre le langage WordBasic, alors que Microsoft Word 8, etc. intègre VBA)
- le tableur Microsoft Excel
- le gestionnaire de bases de données Microsoft Access
- l'outil de création de présentations Microsoft PowerPoint
- le gestionnaire de projets Microsoft Project
- l'outil de création de diagrammes Microsoft Visio.

Le logiciel de traitement de texte Ami Pro, dans lequel est intégré un langage de script spécial s'est lui aussi trouvé exposé à l'infection par les virus de macro.

Les virus de macro pour Microsoft Office (Word, Excel et PowerPoint) ont connu la plus grande diffusion. Les virus affectant les autres applications de Microsoft Office sont assez rares, et pour AmiPro, on ne connaît qu'un seul virus de macro.

Pour que des virus existent dans un système existant, la présence d'un macro-langage incorporé dans le système avec les possibilités suivantes est indispensable:

- les programmes en macro-langage sont **attachés** à des fichiers documents conservés à l'intérieur de ces derniers

- dans le macro-langage il existe des commandes de copie des programmes de macro d'un fichier vers un autre
- le programme de macro peut être géré sans l'intervention de l'utilisateur (macros automatiques ou standards).

Les systèmes mentionnés ci-dessus dans lesquels des virus de macro ont été détectés répondent à ces critères:

- les programmes de macro sont **attachés** à un fichier concret (AmiPro) ou se trouvent à l'intérieur d'un fichier (applications de Microsoft Office).
- le macro-langage permet de copier les fichiers (AmiPro) ou de déplacer les programmes de macro dans des fichiers de service du système et dans les fichiers édités (Microsoft Office).
- lors du travail avec fichier dans des conditions déterminées (ouverture, fermeture, etc.) des programmes de macro sont appelés (si ces derniers existent). Ils sont désignés d'une façon spéciale (AmiPro) ou ont des noms standard (Microsoft Office).

Les possibilités des macro-langages sont destinées au traitement automatique des données dans les grandes entreprises ou dans les réseaux globaux et permettent d'organiser la "circulation automatisée des documents". D'un autre côté, les possibilités des macro-langages de tels systèmes permettent au virus de transférer son code vers d'autres fichiers, ce qui a pour effet de les infecter.

13.1.1. Comment fonctionnent les virus de macro

Toutes les applications de Microsoft Office supportent les macros automatiques – macros appelées lors de la survenue d'un événement quelconque. Les macros automatiques sont **attachées** aux événements par leurs noms d'après lesquels l'application décide quelle macro appeler et à quelle occasion. Par exemple, dans Microsoft Word, lors de l'ouverture d'un fichier, la macro AutoOpen est exécutée automatiquement si cette macro existe dans ce document et, lors de l'impression du document, la macro FilePrint est exécutée.

Sont également exécutées automatiquement (c'est-à-dire sans intervention de l'utilisateur) les macros/fonctions associées à une touche quelconque, soit à un moment déterminé, soit à une date précise, c'est-à-dire que l'application appelle la macro/fonction lors de l'utilisation d'une touche spécifique (ou une combinaison de touches), soit à l'issue d'un certain laps de temps.

Les virus de macro infectant les documents Microsoft Office utilisent, bien sûr, une des propriétés énumérées ci-dessus. Le virus soit contient une macro automatique, soit la macro du virus est appelée par l'utilisation d'une touche spécifique ou d'une

combinaison de touches. Il existe également des semi-virus qui n'utilisent pas ces méthodes et ne se multiplient que lorsque l'utilisateur les lance de lui-même.

De cette manière, si un document est infecté, en appelant une macro automatique, l'application lance en fait le code du virus. Si le virus contient des macros avec des noms standards, elles sont gérées lors de l'appel de la commande appropriée du menu (**Fichier > Ouvrir**, **Fichier > Fermer**, **Fichier > Enregistrer sous**). Si la macro du virus est associée à une touche (ou une combinaison de touches), le virus n'est activé que si l'on utilise la touche appropriée.

La plupart des virus de macro contiennent toutes leurs fonctions sous la forme de macros standards de Microsoft Office 97. Cependant, il existe des virus qui utilisent des méthodes de dissimulation de leur code et qui le stockent sous une forme autre que celle d'une macro. On connaît trois méthodes de ce type, qui toutes utilisent la possibilité qu'offrent les macros de créer, d'éditer et d'exécuter d'autres macros. Comme il se doit, de tels virus ont une macro amorce de virus (parfois polymorphe) qui appelle l'outil incorporé d'écriture de macros, crée une nouvelle macro, lui donne le code principal du virus, l'exécute et, bien entendu, la détruit (pour masquer les traces de présence du virus). Le code principal de tels virus est présent soit dans la macro elle-même sous la forme de lignes de texte (parfois cryptées), soit est stocké dans la zone des données temporaires du document ou dans la zone Texte-auto.

Il convient de noter que toutes les applications de Microsoft Office permettent de crypter les macros présentes dans un document. De cette façon, certains virus sont présents dans des documents infectés, mais sous une forme cryptée.

Les virus pour Microsoft Office peuvent infecter toutes sortes d'ordinateurs, et pas seulement des PC. L'infection est transmissible si, sur l'ordinateur destinataire, une application entièrement compatible Microsoft Office a été installée (par exemple, Microsoft Word pour Macintosh).

13.1.2. Macro-commandes suspectes

Sont considérées comme *suspectes* les macro-commandes donnant au virus la possibilité de créer des copies ou d'exécuter des actions destructives. De telles commandes peuvent être exécutées par les macros en fonctionnement, mais le cas est rare. La liste de toutes les macro-commandes contrôlées par le programme est mentionnée ci-après (Illustration 93). Les macro-commandes sont regroupées par catégories: au dernier degré de la hiérarchie se trouvent les noms des macro-commandes suspectes rassemblées dans différents groupes.

Illustration 93. Liste des macro-commandes suspectes

Il est pratique de distinguer quatre groupes de macro-commandes:

Les opérations sur les macros. Les macros habituelles modifient rarement le code des autres macros et pratiquement jamais leur propre code. La modification du code est signe de forte probabilité de présence de virus. Parmi les opérations sur les macros on distingue deux groupes. Premièrement les macro-commandes de travail avec les modules de projet: création, ajout, copie, exportation et importation de modules, et, deuxièmement les macro-commandes de modification du code des macros: insertion de lignes dans la macro, copie de lignes, suppression de lignes, insertion de lignes depuis le fichier.

Les opérations sur les fichiers. Les commandes de travail avec les fichiers sont également hautement suspectes. Par exemple, la suppression du fichier sur le disque. Si un virus exécute cette commande, ceci peut avoir des conséquences fatales pour vos données.

Les autres commandes. Cette liste comporte des macro-commandes suspectes comme la modification de la protection antivirale d'un document, le lancement d'applications extérieures (appel de commandes Shell), travail avec les objets ActiveX, émulation de la pression des touches. De telles macro-commandes peuvent également être utilisées par les virus.

L'appel de fonctions API. L'appel de fonctions et de procédures du système d'exploitation et d'autres programmes avec utilisation de l'interface API permet aux virus d'exécuter des actions nuisibles sans utiliser les commandes standards du langage Visual Basic.

13.1.3. Interception des virus de macro. Règles pour les macro-commandes suspectes

Kaspersky® Office Guard contrôle totalement le travail des macros dans les applications de Microsoft Office 2000. Dès qu'une macro est lancée et que dans sa procédure de travail une tentative est faite pour appeler une macro-commande entrant dans la liste des macro-commandes suspectes, le programme s'active et intercepte la commande. En fonctions des réglages (voir paragraphe 13.3.1), le programme Kaspersky® Office Guard exécute une des quatre actions suivantes: autoriser l'exécution de la macro-commande suspecte, l'interdire, arrêter complètement la macro ou demander à l'utilisateur d'indiquer les actions ultérieures à entreprendre. Nous appellerons *règle pour la macro-commande* l'action du programme Kaspersky® Office Guard correspondant à la macro-commande. Par la suite, pour désigner les règles, nous utiliserons les signes suivants:

 (sonnette) – demander à l'utilisateur d'indiquer les actions ultérieures

 (arrêt) – arrêter l'action de la macro

 (fanion rouge) – interdire la macro-commande suspecte

 (fanion vert) – autoriser la macro-commande suspecte.

Par exemple, vous pouvez assigner les règles suivantes: arrêter automatiquement toutes les macros qui tentent d'exécuter les actions les plus dangereuses, demander l'autorisation pour la macro-commande de copier des feuilles Microsoft Excel, définir la macro-commande de création des procédures et ignorer toutes les autres macro-commandes suspectes. Sur l'illustration de cet exemple, dans la liste des macro-commandes suspectes, à gauche du nom de chaque commande, se trouve le signe indiquant la règle qui lui correspond (Illustration 94).

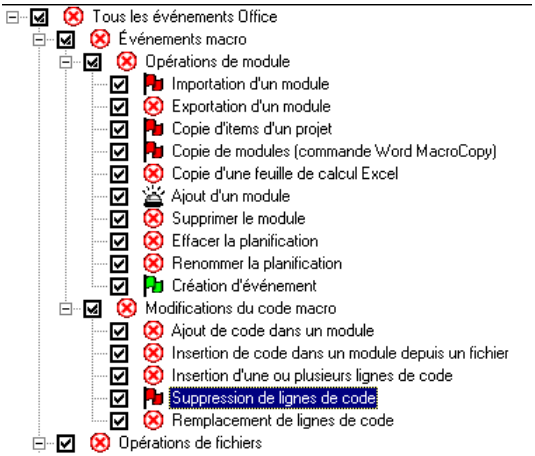


Illustration 94. Exemple. Règles pour les macro-commandes suspectes

13.2. Interface

13.2.1. Lancement du programme

A chaque chargement dans votre ordinateur de l'une des applications de Microsoft Office 2000, celui-ci lancera *le module Kaspersky® Office Guard* qui sert à l'exécution des fonctions de la protection anti-virus. C'est précisément cette partie qui agit lors de la tentative d'exécution d'une macro-commande suspecte. La deuxième partie ou *Interface Kaspersky® Office Guard* est lancée soit au moment de la détection par la partie service d'une commande suspecte, soit manuellement pour l'édition des réglages anti-virus.

Pour lancer manuellement la partie Interface Kaspersky® Office Guard*,*

1. Cliquez sur le bouton **Démarrer**.
2. Sélectionnez dans le menu l'option **Programmes**.
3. Dans le menu qui apparaît sélectionnez l'option **Kaspersky Anti-Virus®** et **Kaspersky® Office Guard**.

Après le lancement de la partie Interface de Kaspersky® Office Guard, dans la partie droite de la barre des tâches de Windows et à gauche de l'horloge apparaît le signe

Pour ouvrir la fenêtre principale de Kaspersky® Office Guard, sélectionnez dans le menu Système (voir p. 13.2.2) la commande ***Afficher les réglages*** *ou double-cliquez avec la souris sur l'icône dans la barre des tâches de Windows (Illustration 95).*

Illustration 95. Fenêtre principale de Kaspersky® Office Guard

13.2.2. Menu Système

Pour gérer le travail de la partie interface de Kaspersky® Office Guard, on utilise son *menu Système* (Illustration 96).

Pour appeler le menu Système de l'unité d'interface du programme Kaspersky® Office Guard, pointez avec la souris sur le signe dans la barre des tâches de Windows et cliquez avec le bouton droit.

Le menu Système contient les options énumérées ci-après:

- **Afficher les réglages** – ouvrir la fenêtre principale du programme.
- **Désactiver Anti-Virus Kaspersky® Office Guard / Activer Anti-Virus Kaspersky® Office Guard** – arrêter/relancer le travail du programme Kaspersky® Office Guard. Quand le travail est interrompu, le contrôle de l'action des macros n'est pas effectué.
- **Fermer automatiquement** – terminer le travail de la partie interface du programme lors de la fermeture de la dernière application de Microsoft Office 2000 utilisant VBA.
- **Aide** – appeler le système d'aide.

- **A propos** – ouvrir la fenêtre contenant les informations sur les fichiers clés.
- **Fermer** – terminer le travail de la partie interface du programme Kaspersky® Office Guard.

Après la sélection de la commande **Fermer,** la partie service du programme ne sera pas déchargée.

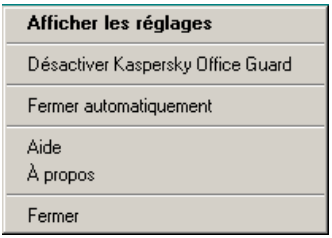


Illustration 96. Menu système

13.2.3. Fenêtre principale

La fenêtre principale de Kaspersky® Office Guard contient trois onglets : **Réglage de la sécurité**, **Personnalisé** et **Statistiques**. L'onglet **Réglage de la sécurité** est destiné à la sélection du niveau de sécurité anti-virus que doit garantir le programme, l'onglet **Statistiques** sert l'affichage des statistiques sur les résultats. Sur l'onglet **Personnalisé** il est possible de consulter le niveau de protection antivirale sélectionné par l'utilisateur, et lors du choix du niveau, il est également possible de modifier le réglage du niveau de protection souhaité.

Pour exécuter les différentes actions, on utilise des menus contextuels, c'est pourquoi les menus habituels sont absents de la fenêtre principale.

13.2.4. Fin du travail du programme

*Pour arrêter le travail de la partie interface de Kaspersky® Office Guard, sélectionnez la commande **Fermer** dans le menu Système.*

Après la fin du travail de la partie interface, la partie service continue de fonctionner.

13.2.5. Système d'aide

Pour bien comprendre comment utiliser Kaspersky® Office Guard, vous pouvez utiliser son *fichier d'aide*.

*Pour appeler le système d'aide, sélectionnez dans le menu Système la commande **Aide**.*

Pour demander une aide contextuelle à propos d'un élément de l'interface, cliquez sur cet élément avec le bouton droit de la souris.

13.3. Réglage des paramètres

13.3.1. Choix du niveau de protection antivirale

Pour choisir le niveau de protection antivirale,

1. Basculez sur l'onglet **Réglage de la sécurité** (Illustration 95).
2. Dans le groupe de boutons, indiquez le niveau de protection désiré:

   - **Maximum** – niveau maximum de protection antivirale (voir 13.3.2).
   - **Moyenne** – niveau moyen de protection antivirale (voir 13.3.3).
   - **Demander à chaque fois** – niveau de protection lors duquel Kaspersky® Office Guard demandera l'autorisation d'exécuter toute commande suspecte (voir 13.3.4).
   - **Faible** – faible niveau de protection antivirale (voir 13.3.5).
   - **Personnalisée** – niveau de réglage grâce auquel vous pouvez paramétrer les actions pour chaque commande contrôlée. Les réglages sont définis sur l'onglet **Personnalisé** (voir paragraphe 13.3.6).

Le bouton **Personnalisée** n'est accessible qu'avec la clé d'enregistrement.
Pour la majorité des utilisateurs, le niveau moyen de protection antivirale est suffisant. Il est déconseillé de choisir le niveau faible.

13.3.2. Niveau maximum de protection antivirale

Lorsque la protection antivirale est réglée au maximum, le programme stoppera automatiquement toutes les macros tentant d'exécuter une commande suspecte (Illustration 97).

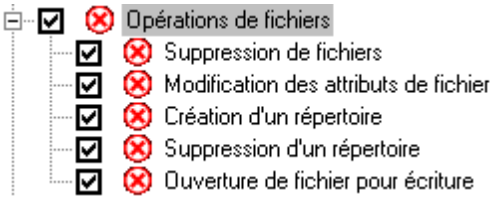


Illustration 97. Liste des règles pour le niveau maximum de protection antivirale (– arrêt de l'action de la macro)

13.3.3. Niveau moyen de protection antivirale

Au niveau moyen de protection antivirale, le programme interdit l'exécution de la majorité des macro-commandes suspectes et stoppe complètement les macros tentant de lancer une des macro-commandes les plus dangereuses, à savoir: **Importation de modules**, **Copie de modules**, **Commande MacroCopy**, **Copie de feuilles Excel**, **Suppression de fichiers**, **Désactivation de la demande de sauvegarde du modèle Normal**, **Désactivation de la protection antivirale** (Illustration 98).

Le niveau moyen de protection antivirale convient à la majorité des utilisateurs.

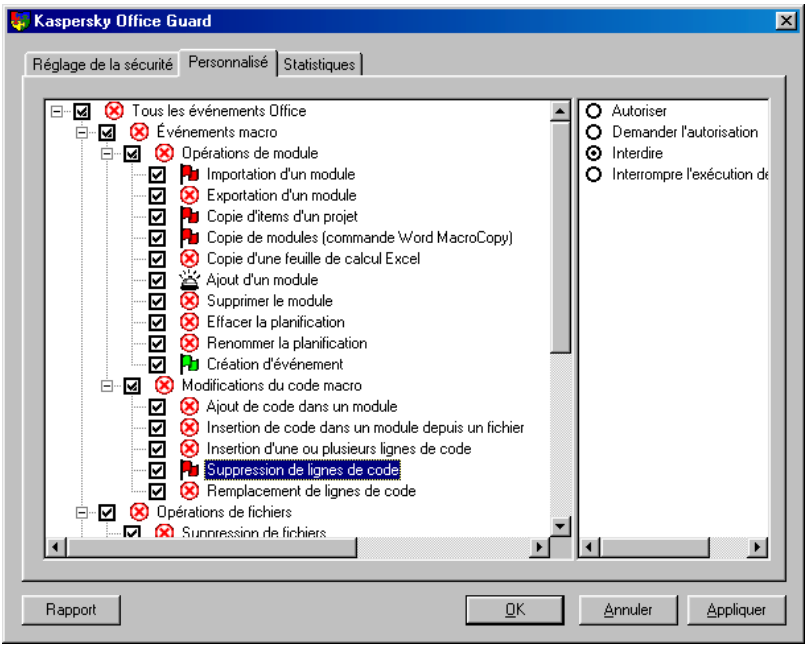


Illustration 98. Liste des règles pour le niveau moyen de protection antivirale

( – arrêt de l'action de la macro,  – interdiction de la macro-commande suspecte)

13.3.4. Niveau de protection avec demandes

Lors du travail avec demande prélable, Kaspersky® Office Guard demande l'autorisation d'exécuter chaque macro-commande suspecte (Illustration 99).

Illustration 99. Liste des règles pour le niveau **avec demandes**

( – demande auprès de l'utilisateur pour les actions ultérieures)

13.3.5. Niveau faible de protection antivirale

Au niveau faible de protection antivirale, le programme autorise automatiquement toutes les actions des macros, à l'exception des plus dangereuses pour lesquelles il demande à l'utilisateur l'autorisation d'exécuter les actions ultérieures (Illustration 100).

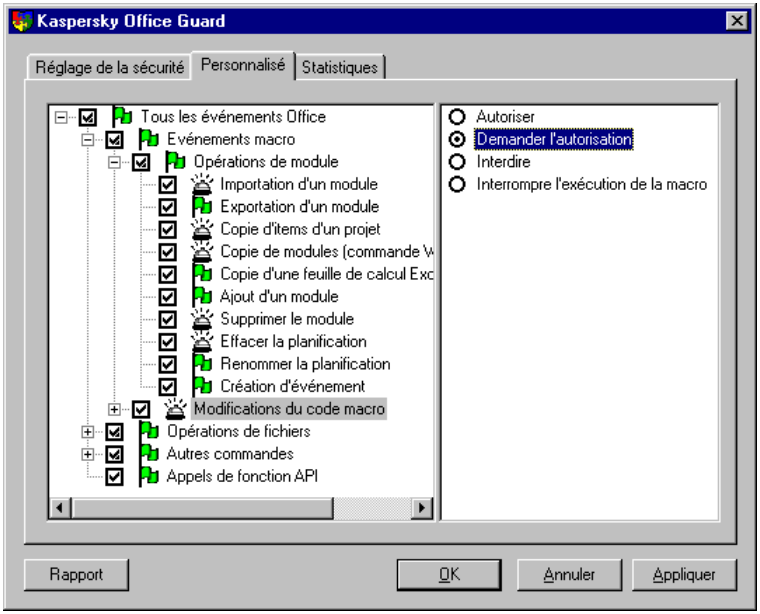


Illustration 100. Liste des règles pour le niveau faible de protection antivirale (– demande à l'utilisateur l'autorisation d'exécuter les actions ultérieures, – autorisation d'exécuter une macro-commande suspecte)

13.3.6. Niveau de protection défini par l'utilisateur

Parfois, il peut vous être demandé de paramétrer vous-même les règles pour les commandes suspectes.

Exemple: Dans votre travail quotidien, vous utilisez une macro qui appelle une des commandes suspectes. Le programme Kaspersky® Office

Guard vous demande régulièrement l'autorisation d'exécuter la commande suspecte. Pour que cela ne se produise plus, vous pouvez régler le régime utilisateur de sécurité de telle sorte que l'action suspecte utilisée par la macro soit autorisée par défaut.

Pour régler le niveau de protection antivirale dont vous avez besoin,

1. Dans le groupe de boutons accessibles sur l'onglet **Réglage de la sécurité,** cochez l'option **Personnalisée** (Illustration 101).
2. Basculez sur l'onglet **Personnalisé** et définissez les règles pour les commandes suspectes dans l'*arborescence des réglages* (voir ci-après pour plus de détails).

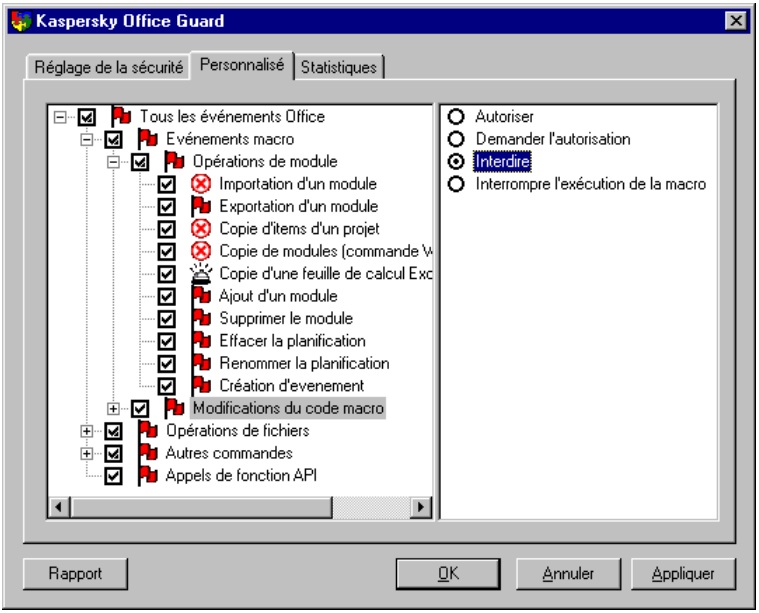


Illustration 101. Réglage des paramètres personnalisés de protection

Dans l'onglet **Personnalisé** se trouve l'arborescence des réglages. Dans la partie gauche de la fenêtre est affichée la liste de toutes les macro-commandes suspectes, les *indicateurs de contrôle* et les symboles des règles qui leur correspondent, et dans la partie droite se trouve le groupe de boutons de choix, dans lequel est indiqué le nom de la règle à appliquer.

Dans l'arborescence des réglages, vous pouvez modifier l'état de l'indicateur de contrôle ainsi que les règles des macro-commandes et des groupes.

En fonction des modifications que vous apportez, divers changements se produisent dans l'arborescence des réglages: les macro-commandes peuvent hériter de la règle du groupe, avoir des règles indépendantes et des règles strictement indépendantes, c'est-à-dire des règles non soumises à héritage.

Pour modifier l'état de l'indicateur de contrôle de la macro-commande sélectionnée ou du groupe:

1. Sélectionnez dans l'arborescence des réglages la ligne nécessaire.
2. Cliquez avec la souris sur l'indicateur de contrôle de la macro-commande, appuyez sur la touche d'espacement, ou sélectionnez dans le menu contextuel la commande **Activer (Désactiver)**.

L'indicateur de contrôle de la macro-commande peut avoir différents états (voir 8.3).

Pour définir une règle pour une macro-commande suspecte ou un groupe:

1. Sélectionnez dans l'arborescence des réglages la ligne désirée
2. Définissez dans le groupe de boutons disposé à droite la règle qui sera appliquée par le programme.

   - **Autoriser** – autoriser l'exécution d'une macro-commande suspecte (à gauche de la ligne dans l'arborescence apparaît le symbole)
   - **Demander l'autorisation** – demander à l'utilisateur l'autorisation d'exécuter une macro-commande suspecte (à gauche de la ligne dans l'arborescence des réglages apparaît le symbole)
   - **Interdire** – interdire l'exécution d'une macro-commande suspecte et transmettre la gestion à la commande qui suit (à gauche de la ligne dans l'arborescence des réglages apparaît le symbole)
   - **Interrompre l'exécution de la macro** – stopper l'exécution d'une macro (à gauche de la ligne dans l'arborescence des réglages apparaît le symbole).

En fonction des changements apportés (modification des réglages du groupe ou d'une commande particulière), l'arborescence des réglages change.

13.4. Interception des macro-commandes suspectes

Dès qu'une macro tente d'exécuter une macro-commande suspecte, le programme l'intercepte et, en fonction de la règle qui a été définie pour cette macro-commande (voir 13.3.1), il exécute une des quatre actions suivantes: interdire la macro-commande et passer à la commande suivante, autoriser l'exécution de la macro-commande, arrêter la macro ou interroger l'utilisateur à propos des actions ultérieures.

Si, pour une commande suspecte, il a été indiqué d'interroger l'utilisateur, la boîte de dialogue **Kaspersky® Office Guard – Autoriser cette action ?** s'affiche à l'écran (Illustration 102).

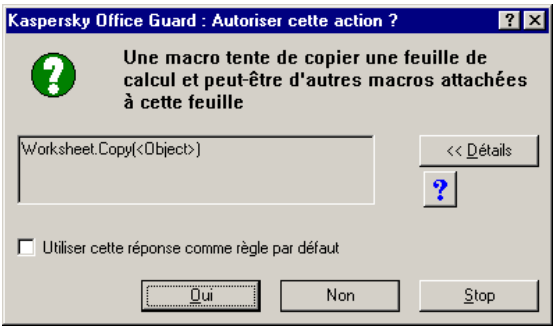


Illustration 102. Sollicitation de l'utilisateur à propos des actions

Dans la partie supérieure de la boîte de dialogue se trouvent les informations sur la macro-commande suspecte tentant d'exécuter une macro. En cliquant sur le bouton **Détails** on peut recevoir une information plus détaillée sur la commande, et en cliquant sur le bouton  des renseignements sur la dangerosité de la commande.

Dans la partie inférieure de la boîte de dialogue se trouvent trois boutons. Ces boutons servent à indiquer au programme quelle action exécuter:

- **Oui** – autoriser l'exécution de la commande suspecte
- **Non** – interdire l'exécution de la commande suspecte
- **Stop** – stopper l'exécution de la macro.

Pour que l'action que vous avez sélectionnée en cliquant sur un des boutons soit utilisée ultérieurement par le programme comme règle appliquée à cette commande suspecte, cochez la case ***Utiliser cette réponse comme règle par défaut****.*

La case d'option **Utiliser cette réponse comme règle par défaut** n'est accessible qu'au moyen de la clé.

Si vous cochez la case **Utiliser cette réponse comme règle par défaut**, la règle que vous avez sélectionnée pour la macro-commande suspecte sera reportée dans l'arborescence des réglages. Si l'arborescence des réglages est affichée sur l'écran, celle-ci reflétera les changements que vous avez effectués.

Si à la macro-commande est associée la règle **Demander l'autorisation** avec le statut **strictement indépendante**, la nouvelle règle aura simplement le statut **indépendante**.

Vous devez absolument décider vous-même si l'action suspecte est exécutée précisément par un virus, puis supprimer de la macro le code du virus, ou transmettre la macro infectée à l'administrateur. Le système d'aide contient des renseignements susceptibles de vous aider à prendre la bonne décision.

13.5. Rapport

Vous pouvez consulter le rapport contenant les résultats du travail du programme à l'aide du programme Kaspersky® Report Viewer. Pour ce faire, cliquez sur le bouton **Rapport** de la fenêtre principale.

Dans le rapport Illustrationnt:

- l'heure de la tentative d'exécution par la macro de la commande suspecte
- la commande suspecte
- l'action exécutée par le programme Kaspersky® Office Guard: **autorisée** – si l'action suspecte a été autorisée, **terminée** – si on a arrêté l'action suspecte, **désactivée** – si la macro a été arrêtée.

Les statistiques des résultats du travail du programme se trouvent sur l'onglet **Statistiques** de la fenêtre principale du programme (Illustration 103)

Illustration 103. Feuillet **Statistiques**

CHAPITRE 14. KASPERSKY® INSPECTOR

14.1. Rôle de Kaspersky® Inspector

14.1.1. Rôle et fonctions principales

Kaspersky® Inspector est un programme anti-virus d'inspection du disque géré par le système d'exploitation Microsoft Windows 95 OSR298/ME® ou NT/2000.

Kaspersky® Inspector vérifie sur les disques les éventuelles modifications intervenues dans le contenu des fichiers et des répertoires. Le programme peut aussi être utilisé comme programme anti-virus auxiliaire.

Le programme diminue sensiblement la durée de l'analyse des disques par le module Kaspersky Anti-Virus® Scanner, car après la vérification des changements sur les disques, il peut ne transmettre au scanner pour vérification que les fichiers neufs et modifiés.

Son travail est basé sur la sauvegarde des données de bases sur le disque dans la table contenant les images du Master-Boot et des secteurs d'amorçage, la liste des clusters défectueux, le schéma de l'arborescence des répertoires et les informations sur tous les fichiers contrôlés.

En plus de toutes ces vérifications, le programme explore le disque par secteurs directement par le biais du pilote IOS et n'utilise pas les méthodes standards (interruption INT 21h et INT 13h), ce qui permet de détecter avec succès les virus furtifs actifs se trouvant dans la mémoire et qui accaparent le traitement de ces interruptions d'une importance vitale (pour l'ordinateur).

En outre, Kaspersky® Inspector mémorise et, à chaque lancement, vérifie que le volume de mémoire vive DOS accessible n'a pas été modifié (ce qui se produit en cas d'infection par la majorité des virus d'amorce), ainsi que le nombre de disques durs installés.

Fonctionnalités essentielles de Kaspersky® Inspector:

- Appel des disques directement par le biais du pilote IOS (superviseur d'entrée-sortie) en contournant les résidents DOS (en particulier les virus d'amorce ayant intercepté l'interruption de 13h lors du chargement de l'ordinateur).
- Possibilité de restaurer les secteurs d'amorçage des disques.

- Possibilité de vérifier les disques compressés.
- Possibilité d'analyser les systèmes de fichiers (FAT12, FAT16, VFAT32, NTFS) sans utilisation des appels aux fonctions du système d'exploitation fonctionnant avec les fichiers.
- Analyse des fichiers modifiés avec recherche d'un changement analogue de longueur.
- Travail avec les documents OLE2 (documents Word, Excel et Access).
- Possibilité de restaurer les fichiers exécutables DOS, Windows 98/NT grâce au module de réparation KAVI Cure Module.
- Possibilité de détection des virus furtifs actifs.

14.1.2. Spécificités du travail du programme Kaspersky® Inspector avec Microsoft Windows NT

En raison des particularités architecturales de Microsoft Windows NT®, Kaspersky® Inspector n'effectue pas la vérification:

- des registres de mise au point (debug)
- de la taille de la mémoire DOS disponible.

Toutes les autres fonctions du programme sont réalisées sous Microsoft Windows en interne.

14.2. Principes de fonctionnement de Kaspersky® Inspector

Tous les inspecteurs anti-virus (qu'il s'agisse de scanners CRC ou de vérificateurs d'intégrité) ont le même algorithme de recherche des modifications. Ils exécutent les opérations suivantes:

1. Evaluation de valeurs numériques, plus connues sus le nom de sommes de contrôle (somme CRC – code de redondance cyclique) pour les secteurs des disques et pour les fichiers.
2. Sauvegarde des sommes CRC dans une base spéciale de données (table).

3. A chaque lancement, recalcul des valeurs et comparaison avec les sommes antérieures stockées dans la base de données.

Dans la base de données sont également stockées les informations complémentaires sur les fichiers — leur longueur, l'heure de leur création et de leur dernière modification, les attributs et les données indispensables à la restauration des fichiers modifiés (infectés). Dans la base de données sont également conservées les images complètes des secteurs d'amorçage du disque (Master-Boot et Boot), la liste des adresses des clusters défectueux, le schéma de l'arborescence des sous-répertoires et autres informations sur tous les objets contrôlés.

En outre, Kaspersky® Inspector mémorise et ensuite, à chaque lancement, vérifie les informations sur le système d'exploitation et le matériel installé: quantité de mémoire vive (contrôle de l'infection par un virus d'amorce) et nombre de disques durs installés.

Lors des vérifications, Kaspersky® Inspector appelle les secteurs du disque directement par le biais du pilote IOS et n'utilise pas les méthodes standards (interruptions INT 21h et INT 13h). Cette particularité lui permet de détecter et de supprimer avec succès les virus furtifs (Stealth) (voir paragraphe 14.2.3).

14.2.1. Vérifications effectuées par le programme Kaspersky® Inspector

Lors du premier lancement, Kaspersky® Inspector mémorise la quantité de mémoire vive en mode DOS, l'adresse du gestionnaire d'interruption INT 13h et enregistre ces données dans une base de données.

Lors des lancements ultérieurs, Kaspersky® Inspector exécute les opérations suivantes:

- Vérification de la quantité de mémoire vive DOS et de l'adresse du gestionnaire INT 13h.
- Vérification des secteurs d'amorçage (Master-Boot et Boot). Le secteur Master-Boot est vérifié lors de l'analyse de tous les disques logiques. Si une divergence entre la copie sauvegardée et les données obtenues est détectée, il est possible de restaurer le secteur. En outre, vous pouvez utiliser le visualiseur incorporé pour comparer les données contenues dans la base de données et celles obtenues lors de la vérification.
- Vérification du nombre de clusters défectueux. Il existe des virus qui marquent comme étant défectueux un cluster intact en vue d'y placer leur code et leurs données. En cas d'apparition d'un nouveau cluster défectueux, Kaspersky® Inspector vous en avertit.

- Vérification de l'arborescence des répertoires du disque. Le programme recherche des répertoires ayant été créés ou supprimés.
- Vérification de la structure des disques. Le programme recherche les fichiers créés, supprimés, renommés ou modifiés. Au cours de la vérification, il recherche toute modification de la taille, de la date et de l'heure de création du fichier, ainsi que du CRC (somme de contrôle).

Les modifications constatées au cours de la procédure de vérification sont analysées, et si elles ne correspondent pas à des manifestations virales (par exemple, modification de la taille du fichier accompagnée d'un changement de la date et de l'heure de sauvegarde), Kaspersky® Inspector affiche seulement toutes les statistiques sur les modifications. Si des ''modifications'' suspectes sont détectées, (faisant penser à des manifestations virales), Kaspersky® Inspector émet un message d'alerte sur la possibilité d'infection virale.

14.2.2. Analyse des modifications sur le disque

Toutes les modifications constatées par le programme lors de la vérification sont analysées et classées en deux catégories: **anodines** et **suspectes**. Sont classées dans la catégorie des modifications anodines, par exemple, la modification du contenu du fichier si, à cette occasion, la date et l'heure de création du fichier ont aussi été modifiées.

Dans tous les cas de Illustration, Kaspersky® Inspector fournit des informations détaillées sur toutes les modifications (ces statistiques peuvent êtres consultées dans une boîte de dialogue), et sauvegarde la liste des modifications sur le disque sous la forme d'un fichier texte. En cas de modifications suspectes, Kaspersky® Inspector émet un message d'alerte sur la possibilité d'infection virale.

Sont classées dans la catégorie **suspectes** les modifications suivantes:

- la modification du contenu d'un fichier sans modification de la date et de l'heure de la dernière modification (très évocateur de la présence d'un virus)
- des changements identiques au niveau de la taille de plusieurs fichiers
- date et heure de la dernière modification incorrectes: date supérieure à 31, nombre de mois supérieur à 12 ou chiffre de l'année supérieur à celui de l'année en cours, nombre de minutes supérieur à 59, nombre d'heures supérieur à 23 ou nombre de secondes supérieur à 59 (certains virus utilisent de telles méthodes pour marquer les fichiers infectés)

- modification d'un fichier dont le nom Illustration dans la liste des fichiers non modifiables
- modifications indiquant la présence de virus endommageant le noyau DOS (fichiers IO.SYS, IBMBIO.BIN, etc.)

N'ignorez jamais les messages de Kaspersky® Inspector concernant les modifications intervenues sur le disque (cette recommandation vaut surtout pour les modifications suspectes). Si la cause des modifications est inconnue, il faut s'en inquiéter et poursuivre les investigations.

Si les messages du programme contiennent des informations techniques difficilement compréhensibles pour vous, adressez-vous à un spécialiste qualifié ou au service d'assistance technique de Kaspersky Labs. NE NEGLIGEZ JAMAIS DE TELS MESSAGES!

La non-observance de ces recommandations peut avoir pour conséquence l'infection de votre ordinateur par un virus et l'augmentation de la probabilité de perte de données sur le disque.

14.2.3. Recherche des virus furtifs (stealth)

Le terme *furtif* (stealth — invisible) désigne les virus qui utilisent certaines méthodes pour masquer leur présence dans le système. Pour ce faire, ils interceptent les appels aux objets infectés et modifient les blocs de données correspondants de manière à ce que ces fichiers et ces secteurs paraissent intacts. Il existe des virus utilisant diverses méthodes pour se cacher dans le système, certaines étant extrêmement complexes. Il faut également noter qu'il existe des virus furtifs de tous types — les virus de fichier, d'amorce et même les virus de macro peuvent contenir des fonctions furtives. Pour plus de détails sur les virus furtifs, vous pouvez vous reporter au document *Virus Encyclopaedia*. consultable sur le site Web de la société Kaspersky®.

Certaines méthodes mises en œuvre par des virus pour se cacher les rendent indétectables par les procédés habituels. En effet, lorsque ces derniers ouvrent un fichier infecté par un virus furtif, ils n'y lisent que des données non infectées et le code du virus est indécelable. Pour détecter de tels virus, vous devez utiliser une technologie anti-furtivité (par exemple, la lecture directe des données sur le disque).

Kaspersky® Inspector utilise les méthodes les plus fiables, ce qui lui permet de détecter à coup sûr les virus furtifs, qu'ils soient identifiés ou inconnus.

Il faut noter que la capacité de se cacher s'est avérée être le point faible des virus furtifs. Nous avons élaboré une technique, certes relativement complexe, mais qui permet à Kaspersky® Inspector de détecter pratiquement n'importe quel virus furtif dans le système. Pour ce faire, le programme vérifie le contenu du

secteur d'amorçage ou du fichier suspect en utilisant deux procédés différents, puis il compare les résultats.

La première méthode de lecture est conventionnelle et permet de lire les données par l'intermédiaire du système d'exploitation.

Le deuxième procédé consiste à lire "directement" les données en contournant le système d'exploitation.

Si un virus furtif est présent dans le système, les résultats des deux vérifications (utilisant deux méthodes différentes) seront différents, dans la mesure où le virus furtif ne peut intercepter que l'appel conventionnel et ne peut pas intervenir sur la lecture en mode direct. La technique de comparaison s'appuyant cette méthode est implémentée dans Kaspersky® Inspector. (pour savoir comment activer le mode de vérification de la présence de virus furtifs, voir le paragraphe 14.5.3).

14.2.4. Suppression des virus avec KAVI Cure Module™

KAVI Cure Module™ (KAVIC) est un module programme (cure.dll) intégré qui permet de détecter et de se débarrasser des virus informatiques sans utiliser les bases de données.

Le concept de base du fonctionnement de KAVIC diffère de celui des scanners anti-virus. Le fait est que KAVIC connaît certaines informations sur le fichier protégé mais ne sait rien concernant le virus concret. Les tests effectués par la société Kaspersky® ont mis en évidence que KAVIC restaure complètement les fichiers dans 96% des cas (cette donnée statistique ne constituent pas un axiome car les résultats de la restauration dépendent d'une multitude de facteurs externes). Ainsi, KAVIC vous aidera à vous débarrasser de la majorité des virus, indépendamment du fait qu'ils soient connus ou inconnus.

Pendant l'exécution, Kaspersky® Inspector communique à KAVIC quels fichiers ont été modifiés, quels nouveaux fichiers sont apparus ou quels fichiers ont été supprimés depuis le dernier lancement. KAVIC collecte à son tour les informations indispensables à la restauration des fichiers.

La version actuelle de KAVIC permet de restaurer (réparer) les fichiers DOS et Windows (les fichiers avec une extension EXE, COM, SYS, PRG, DLL, SCR, OCX…).

14.2.5. Vérification des paramètres du système d'exploitation dans la procédure d'amorçage (pilote KAVIBOOT.VXD)

Le ***pilote KAVIBOOT.VXD*** est destiné à la vérification de certaines caractéristiques du système d'exploitation (Windows 95 OSR2/98), durant la procédure d'amorçage. Ce pilote vérifie:

- la quantité de mémoire DOS accessible
- le secteur de master boot (MBR)
- les adresses du gestionnaire INT 13h (lecture/enregistrement du disque).

De telles vérifications peuvent permettre de détecter l'infection de l'ordinateur par un virus d'amorce.

Toutes les opérations de lecture des secteurs sont exécutées en appelant directement le BIOS et en évitant le gestionnaire DOS. En outre, le pilote dispose d'un mécanisme de protection contre les tentatives d'interception des données à partir du disque.

Le système utilisé dans le pilote de protection contre les interceptions peut, dans certains cas très rares, entraîner un blocage du pilote pendant l'opération de lecture. Pour exclure de telles situations, lors du premier lancement du pilote, une vérification anti-blocage sera effectuée.

Si lors du premier lancement après l'installation du programme, votre ordinateur se bloque, il suffit de le rebooter. Dans ce cas, le pilote reconnaîtra que l'ordinateur a redémarré après une sortie incorrecte et ne réutilisera pas ces procédures.

14.3. Interface de Kaspersky® Inspector

14.3.1. Fenêtre principale

Si vous lancez le programme Kaspersky® Inspector sans utiliser une option accessible par l'intermédiaire de la ligne de commandes (voir sous-chapitre 14.4), la fenêtre principale du programme apparaît à l'écran (Illustration 104).

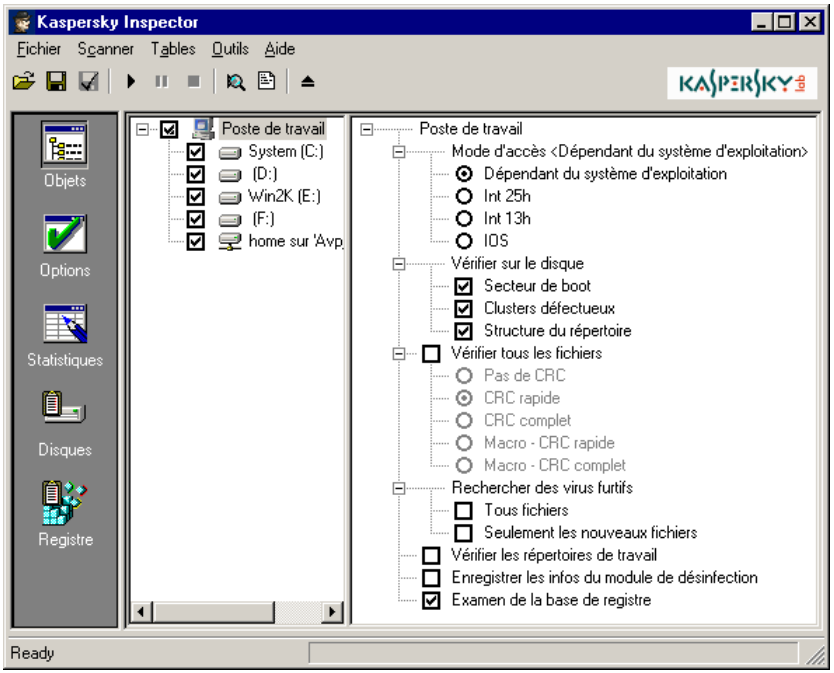


Illustration 104. Fenêtre principale du programme Kaspersky® Inspector

Dans la fenêtre principale sont disposés:

- la barre des menus (voir paragraphe 14.3.2)
- la barre de contrôle (voir paragraphe 14.3.3)
- la zone des catégories (voir paragraphe 0)
- la fenêtre active (voir paragraphe 14.3.5)
- la barre d'état (voir paragraphe 14.3.6).

14.3.2. Barre des menus

Juste sous le titre de la fenêtre principale se trouve la barre des menus (Illustration 105).

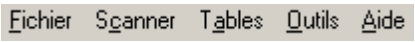


Illustration 105. Barre des menus

Toutes les actions réalisables par le programme correspondent à des commandes du menu. Elles sont décrites dans le Tableau 1.

Tableau 1. Commandes figurant dans les menus

Menu	Commande	Description
Fichier	**Enregistrer comme profil par défaut**	Définir le profil en cours comme profil par défaut
	Charger un profil	Charger un des profils sauvegardés antérieurement (voir 14.5.4)
	Enregistrer le profil	Sauvegarder les paramètres choisis comme profil (voir 14.5.4)
	Enregistrer le profil sous	Enregistrer le profil en cours sous un nouveau nom
	Quitter	Quitter le programme
Scanner	**Démarrer**	Lancer la procédure de vérification (voir 14.4.3)
	Arrêter	Arrêter la procédure de vérification
	Pause	Interrompre provisoirement la procédure de vérification
Tables	**Créer une table pour le registre**	Créer une nouvelle table pour le registre (voir 14.4.3.2)
	Créer des tables pour les disques	Créer de nouvelles tables pour les disques (voir 14.4.3.2)
Outils	**Afficher le rapport**	Consulter le rapport sur les résultats de la vérification précédente
Aide	**Sommaire**	Afficher les rubriques d'aide

Menu	Commande	Description
	A propos	Appeler la fenêtre contenant les informations sur les gestionnaires, le numéro de la version du programme et vos données d'enregistrement

14.3.3. Barre de contrôle

Sous la barre des menus se trouve la barre de contrôle (Illustration 106), sur laquelle sont disposés les boutons permettant d'exécuter les opérations les plus couramment utilisées.

Illustration 106. Barre de contrôle

La majorité des boutons de la barre de contrôle contiennent les mêmes commandes que les menus (voir 14.3.2). En pointant avec la souris sur un bouton, vous faites apparaître une bulle d'aide.

Les commandes sont décrites dans le Tableau 2.

Tableau 2. Boutons de la barre de contrôle

Bouton	Commande correspondante	Description
 **Charger un profil**	Commande **Charger un profil** du menu **Fichier**	Charger un des profils sauvegardés antérieurement (voir 14.5.4)
 **Sauvegarder le profil**	Commande **Enregistrer le profil** du menu **Fichier**	Sauvegarder comme profil les réglages de vérification choisis (voir 14.5.4)
 **Sauvegarder le profil par défaut**	Commande **Enregistrer** comme profil par défaut du menu **Fichier**	Sauvegarder le profil courant comme profil par défaut

Bouton	Commande correspondante	Description
 **Démarrer**	Commande **Démarrer** du menu **Scanner**	Lancer la procédure de vérification (voir 14.4.3)
 **Interrompre**	Commande **Pause** du menu **Scanner**	Interrompre provisoirement la procédure de vérification
 **Arrêter**	Commande **Arrêter** du menu **Scanner**	Arrêter la procédure de vérification
 **Aperçu des paramètres du Scan**		Consultation des paramètres en cours concernant la vérification des objets
 **Montrer le rapport**	Commande **Afficher le rapport** du menu **Outils**	Lancer le programme Kaspersky® Report Viewer faisant partie du pack de livraison
 **Quitter**	Commande **Quitter** du menu **Fichier**	Quitter le programme

14.3.4. Zone des catégories

Dans la partie gauche de la fenêtre principale se trouve la zone des catégories.

Cette zone comporte cinq icônes correspondant chacune à une catégorie de paramètres (voir Tableau 3). Pour accéder à la catégorie voulue, cliquez sur l'icône appropriée.

En cliquant avec le bouton droit de la souris en n'importe quel endroit de la zone des catégories, on peut appeler le menu contextuel de cette zone, offrant deux options:

- **Petites icônes** — afficher de petites icônes dans la zone des catégories
- **Grandes icônes** — afficher de grandes icônes dans la zone des catégories.

Tableau 3. Catégories

Catégorie	Description
	Permet de définir la zone d'analyse, les objets à analyser et les règles de traitement des objets infectés. Tous ces réglages sont organisés dans l'élément spécial de gestion, l'*arborescence des réglages de la hiérarchie des objets* (voir 14.5.2)
	Permet de définir les paramètres de vérification communs à tous les objets à vérifier, ainsi que les paramètres de travail conjoint du programme Kaspersky® Inspector et des autres modules entrant dans la composition du package Anti-Virus Kaspersky® Personal Pro (KAV Cure Module et KAV32). Ici on peut définir les paramètres de fonctionnement du rapport
	Permet de consulter les résultats généraux sous forme de tableau (voir 14.6.1)
	Affiche les renseignements complets sur les résultats de la vérification des objets et permet d'apporter les modifications nécessaires (voir 14.6.2–14.6.5)
	Affiche les résultats exhaustifs de la vérification du registre et permet d'apporter les modifications nécessaires (voir 14.6.6)

14.3.5. Fenêtre active

La fenêtre active occupe une grande partie de la fenêtre principale du programme. L'aspect de la fenêtre active dépend de la catégorie choisie.

14.3.6. Barre d'état

Dans la partie inférieure de la fenêtre principale se trouve la barre d'état.

Dans la barre d'état apparaît l'état actuel du programme, et durant la procédure de vérification, les noms des fichiers vérifiés sont affichés.

14.4. Lancement de Kaspersky® Inspector

14.4.1. Méthodes de lancement du programme

14.4.1.1. Lancement depuis le menu Démarrer de Windows

Il est possible de lancer Kaspersky® Inspector depuis le menu Démarrer dans le groupe **Kaspersky Anti-Virus®,** créé au moment de l'installation du programme. Pour ce faire, cliquez sur le bouton **Démarrer**, puis suivez l'arborescence suivante:

Démarrer→Programmes→Kaspersky Anti-Virus→Kaspersky Inspector.

14.4.1.2. Lancement de Kaspersky® Inspector depuis Kaspersky AV Control Centre

Kaspersky® Inspector, comme tous les programmes entrant dans la composition du package Anti-Virus Kaspersky® Personal Pro, peut être lancé depuis le module Control Centre (Centre de Contrôle). Dans ce programme, il est possible de paramétrer le lancement automatique de Kaspersky® Inspector à l'heure désirée, chaque jour, ou après un certain laps de temps.

14.4.2. Premier lancement du programme

Lors du tout premier lancement, Kaspersky® Inspector proposera, pour tous les objets vérifiés (voir paragraphe 14.5.2), de créer des tables (Illustration 107). Ces tables sont indispensables au travail de Kaspersky® Inspector. Si elles sont absentes, Kaspersky® Inspector ne peut pas vérifier les modifications affectant les disques.

Pour que Kaspersky® Inspector crée automatiquement des tables, cliquez sur le bouton **Oui**. Après quoi, lors des lancements ultérieurs, Kaspersky® Inspector sera complètement opérationnel.

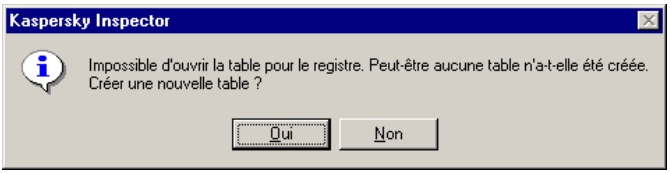


Illustration 107. Demande de création de tables

14.4.3. Lancement de la vérification des modifications affectant le disque

14.4.3.1. Vérification des modifications affectant le disque

Si, lors du lancement de Kaspersky® Inspector depuis le module Kaspersky AV Control Centre, il a été spécifié de lancer le programme une fois par jour, ou si le programme est lancé depuis la ligne de commande avec les paramètres appropriés (voir paragraphe 14.5.2), Kaspersky® Inspector sera lancé automatiquement et vérifiera les modifications affectant le disque (voir p. 14.2.1) au premier chargement du système d'exploitation de la journée.

S'il est nécessaire de vérifier les disques à n'importe quel autre moment, cliquez dans la barre d'outils de la fenêtre principale du programme sur le bouton  . A cette occasion, la procédure de vérification des objets spécifiés dans le réglage approprié sera lancée (voir paragraphe 14.5.2).

14.4.3.2. Création de nouvelles tables

Dans certains cas (par exemple, lors de l'ajout d'un nouveau disque dans l'ordinateur, ou si les tables existantes ont, pour une raison quelconque, été endommagées ou supprimées), il est nécessaire de créer de nouvelles tables.

Pour créer de nouvelles tables correspondant au(x) disque(s), il faut d'abord marquer ce(s) disque(s) en cliquant sur l'icône adéquate avec le bouton gauche de la souris (voir paragraphe 14.5.2), et ensuite sélectionner une des commandes suivantes du menu **Tables:**

- **Créer une table pour le registre** — elle permet de créer de nouvelles tables pour le registre. Un message s'affiche sur l'écran (Illustration 108). Pour confirmer la création de la nouvelle table, cliquez sur **Oui**. Après quoi, la création peut commencer.
- **Créer des tables pour les disques** — elle permet de créer de nouvelles tables pour les disques. Un message s'affiche sur l'écran (Illustration 109). Pour confirmer la création des nouvelles tables, cliquez sur **Oui**. Après quoi, la création peut commencer. Attention, elle peut prendre un certain temps.

Illustration 108. Confirmation de la création d'une nouvelle table de registre

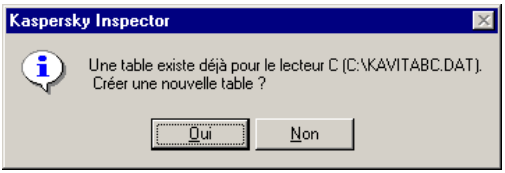


Illustration 109. Confirmation de la création d'une nouvelle table de disque

14.4.4. Lancement de la recherche des virus furtifs

Pour lancer la recherche des virus furtifs pour un ou plusieurs objets (voir paragraphe 14.5.2), il est nécessaire de cocher l'une des cases appropriées (voir

paragraphe 14.5.3) et de cliquer sur le bouton  dans la barre d'outils de la fenêtre principale du programme.

Lors de l'analyse du disque, Kaspersky® Inspector vérifie les secteurs d'amorçage (secteur Master-Boot et secteur Boot des disques logiques) et compare également les tailles des fichiers et les sommes de contrôle déterminées par les outils du système d'exploitation, avec leurs valeurs réelles qui sont calculées par lecture directe du disque. En cas de divergences entre les résultats, Kaspersky® Inspector stoppe immédiatement la procédure d'analyse du disque pour ne pas permettre à un virus d'infecter d'autres fichiers ou secteurs puis affiche une fenêtre avec un message d'alerte.

14.5. Personnalisation de Kaspersky® Inspector

14.5.1. La zone de travail Options: sélection des options générales

Pour afficher les paramètres généraux de Kaspersky® Inspector, cliquez sur l'icône 

dans la barre d'icônes de la fenêtre principale (reportez-vous au sous-chapitre 14.3.4). L'arborescence des options générales s'affiche alors dans la zone de travail de la fenêtre principale (Illustration 110).

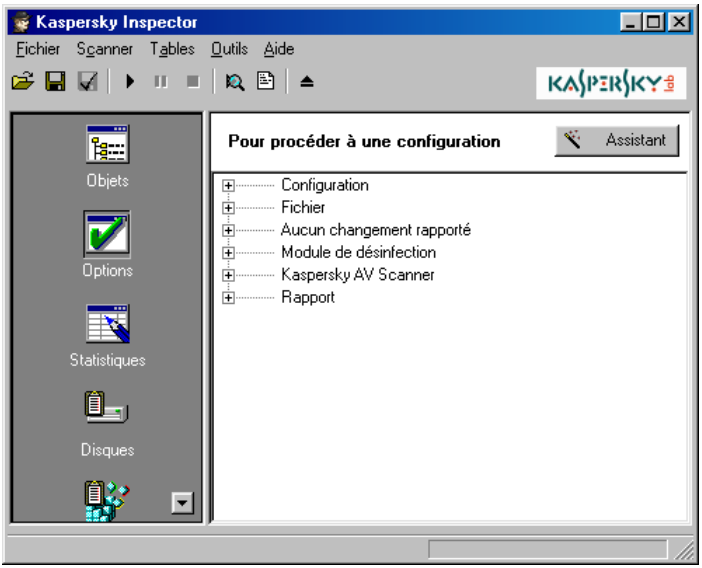


Illustration 110. Arborescence d'options générales du logiciel

Dans l'angle supérieur gauche de la zone de travail se trouve le bouton **Assistant**. Il s'agit d'un outil facile à utiliser permettant de définir les paramètres généraux du logiciel. L'assistant vous permet de définit et de modifier uniquement les principaux paramètres ; il est possible de modifier directement les autres paramètres dans la zone de travail **Options**

Pour conIllustrationr les paramètres du logiciel à l'aide de l'assistant, procédez comme suit:

1. Cliquez sur **Assistant**.
2. La fenêtre **Mode de vérification** de l'assistant (Illustration 111) s'affiche à l'écran. Dans cette fenêtre, sélectionnez l'un des modes de vérification proposés. Cliquez sur **Suivant** pour passer à la fenêtre suivante.

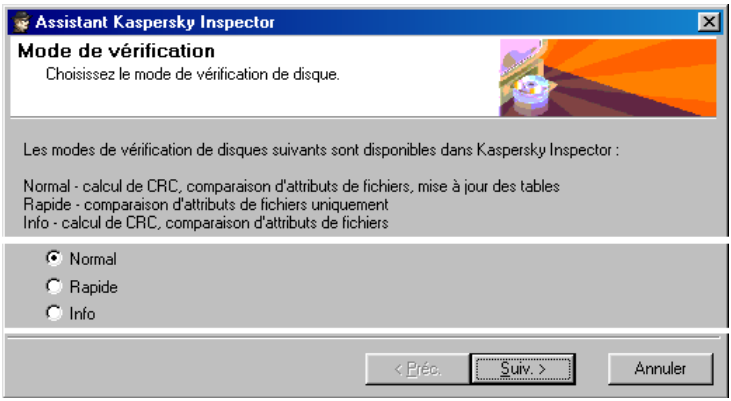


Illustration 111. La fenêtre **Mode de vérification** de l'assistant

3. La fenêtre **Types de fichiers** de l'assistant (Illustration 112) s'affiche à l'écran. La fenêtre présente la liste des extensions de fichier traitées par Kaspersky® Inspector. Vous pouvez également modifier cette liste:

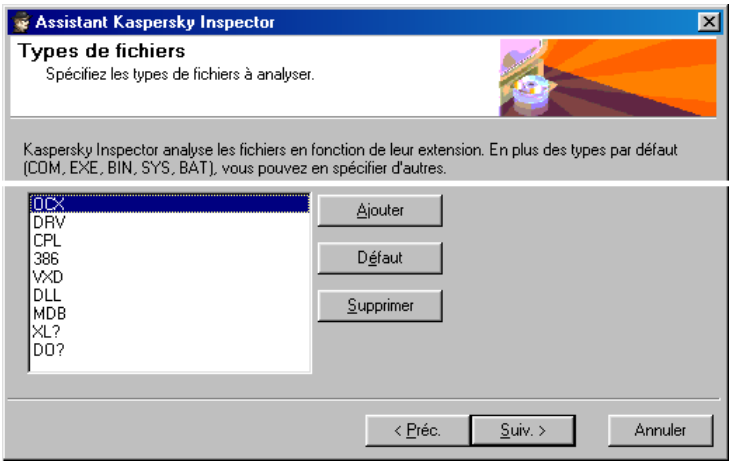


Illustration 112. Types de fichiers

- Pour ajouter la nouvelle extension à la liste, et appuyez sur le bouton **Ajouter**. La boîte de dialogue **Ajout d'extension** (Illustration 113) apparaît. Saisissez la nouvelle valeur dans le champ **Extension**, et, dans le champ **Type CRC**, choisissez l'algorithme de calcul des sommes de

contrôle dans la liste des options prédéfinies pour cette extension et appuyez sur le bouton **Ajouter**.

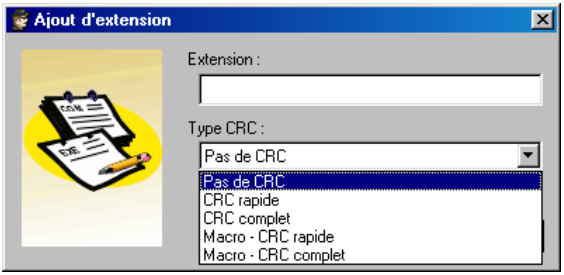


Illustration 113. La boîte de dialogue **Ajout d'extension**

Pour définir un jeu d'extensions dans la zone de texte Ajout d'extension, utilisez le signe d'interrogation, qui vaut pour n'importe quel caractère. Par exemple, la valeur OV dans la zone de texte correspond à tous les fichiers dont l'extension commence par OV (OVL, OVR, ...).

- Pour supprimer l'une des extensions entrées antérieurement, sélectionnez-la dans la liste avec la souris et cliquez sur le bouton Supprimer.

4. Cliquez sur **Suivant** pour passer à la fenêtre suivante. La fenêtre **Interaction avec Kaspersky AV Scanner** de l'assistant (Illustration 114) s'affiche à l'écran. Cette fenêtre vous permet de spécifier les informations indispensables pour que Kaspersky® Inspector puisse agir de concert avec l'analyseur anti-virus de votre ordinateur. La fenêtre vous présentera les deux zones de saisie suivantes:

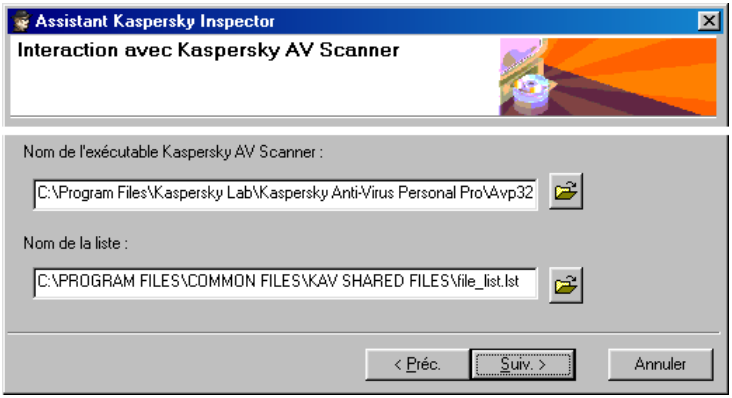


Illustration 114. La fenêtre **Interaction avec Kaspersky AV Scanner** de l'assistant

- **Nom de l'exécutable Kaspersky AV Scanner** — saissez le chemin d'accès au fichier exécutable KAV32. Pour ce faire, cliquez sur le bouton à droite du champ, ensuite dans la boîte de dialogue qui s'affiche, indiquez le chemin d'accès à ce fichier

- **Nom de la liste** — saissez le chemin d'accès au fichier dans lequel Kaspersky AV Inspector doit sauvegarder la liste des fichiers modifiés détectés. Pour ce faire, cliquez sur le bouton à droite du champ, ensuite dans la boîte de dialogue ouverte indiquez le chemin d'accès à ce fichier.

5. Cliquez sur le bouton **Suivant**. La boîte de dialogue **Rapport** (Illustration 115) apparaît. Dans le champ **Nom du rapport** saisissez le chemin d'accès au fichier dans lequel les rapports avec les résultats de l'analyse seront sauvegardés. Pour ce faire, cliquez sur le bouton à droite du champ, ensuite dans la boîte de dialogue qui s'affiche, indiquez le chemin d'accès à ce fichier.

6. Après la fin du réglage, cliquez sur le bouton **Terminer**.

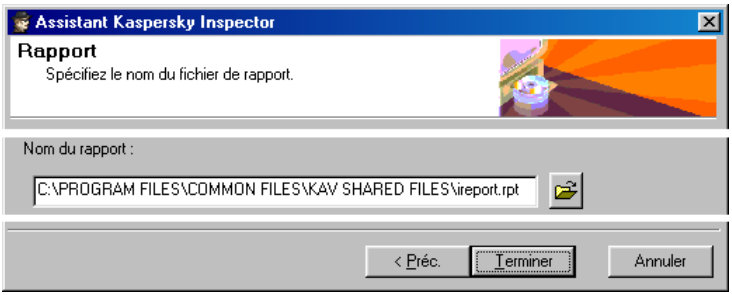


Illustration 115. **Rapport**

14.5.2. Réglage des paramètres de vérification des objets

14.5.2.1. Réglage des paramètres de vérification des disques durs et logiques

Pour passer au réglage des paramètres de vérification des disques, cliquez avec la souris dans la barre des catégories (voir paragraphe 14.3.4) sur l'icône 

. Après quoi, la fenêtre se divisera en deux parties (Illustration 116).

Dans la partie gauche de la fenêtre s'affiche la liste des disques de l'ordinateur accessibles pour la vérification, et dans la partie droite – l'arborescence des réglages.

Le fait de cocher la case ☑ correspondant à chaque disque signifie que le disque concerné va être vérifié par le programme Kaspersky® Inspector.

Il est possible de définir les paramètres de réglage pour chaque disque.

Cependant, le jeu de réglages accessibles dépend du type d'objet. Les objets se situant à des niveaux différents de la hiérarchie disposent d'un jeu de réglages différent.

L'objet **Poste de travail** a une arborescence de réglages avec un nombre maximum de réglages (voir paragraphes 14.5.2.2–14.5.3.1).

Pour les disques durs de l'ordinateur, presque tous les réglages existants sont accessibles, sauf le réglage des fichiers du registre (voir paragraphe 14.5.3.1).

Pour les disques logiques, il est impossible de choisir le type d'accès au disque de Kaspersky® Inspector (voir paragraphe 14.5.2.2), le réglage des éléments vérifiés du disque est inaccessible (on ne peut vérifier que les modifications affectant la structure des répertoires) (voir paragraphe 14.5.2.3).

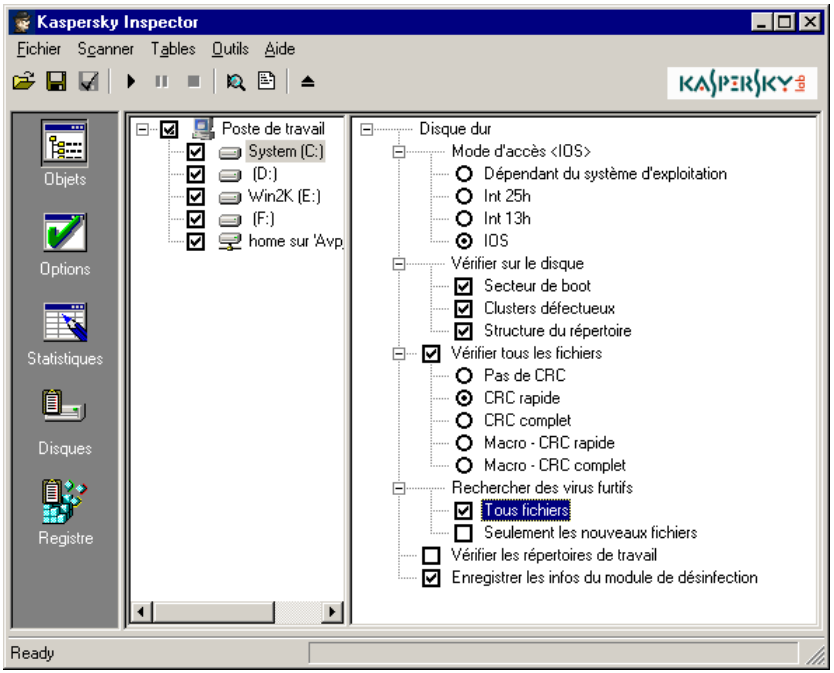


Illustration 116. Paramètres de vérification des disques

14.5.2.2. Type d'accès au disque

Accès au disque — type d'accès au disque:

- **Par les moyens du SE** — accès avec utilisation des outils du système d'exploitation. Si pour un disque, ce type d'accès a été défini, la vérification portant sur la recherche de virus furtifs devient impossible, de même que la vérification des secteurs d'amorçage et des clusters défectueux.
- **Int 25h** — accès avec les outils des pilotes de disques (INT 25h). Dans ce cas, la lecture et la recherche des fichiers sont effectuées par la lecture directe des secteurs du disque, directement, en contournant DOS, c'est-à-dire avec les outils de l'interruption 25h (lecture absolue du disque). Ce mode peut être utilisé pour la vérification des disques "compressés" (par exemple, par les programmes du type Stacker ver. 4.x, DriveSpace). Les programmes de compression des disques énumérés ci-dessus sont supportés par Kaspersky® Inspector, et de tels disques sont affichés avec une icône spéciale. Si vous utilisez d'autres programmes de compression

qui ne sont pas supportés par Kaspersky® Inspector, vous devrez établir vous-même le mode d'accès au disque "compressé" — INT 25h.

- **Int 13h** — accès avec les outils INT 13h. Dans ce cas, la lecture et la recherche des fichiers sont effectuées par la lecture des secteurs du disque, directement, via le BIOS (interruption 13h). Ce mode peut être utilisé **uniquement** pour la vérification des disques physiques, c'est-à-dire des secteurs du disque dur.
- **IOS** — accès avec les outils IOS (IO Supervisor). Dans ce cas, le type d'appel du disque est défini selon les règles suivantes: (si un accès aux disques de 32 bits est utilisé (utilisation de disques VFAT ("Dragon") ou si des programmes de compression de disques de mode protégé (DriveSpace), ou si l'accès au disque est fourni par les outils Real Mode Mapper, on utilise l'appel direct du pilote d'accès aux disques (IOS) 32 bits. Dans le cas contraire, on utilise l'appel des disques par les outils INT 13h, ou on passe par le biais de l'accès via le pilote du disque. En d'autres termes, dans presque tous les cas, on utilisera l'accès au disque via IO Supervisor. Cette option n'est accessible que pour Windows 9x.

14.5.2.3. Eléments du disque à vérifier

Vérifier sur le disque — éléments du disque devant être vérifiés:

- **Le secteur d'amorçage** — le programme permet de désactiver la vérification du secteur d'amorçage du disque. Ceci s'avère indispensable, par exemple, pour les disques créés par le programme Stacker (système de compression des disques) parce que ce programme modifie constamment le contenu du secteur d'amorçage.
- **Les clusters défectueux** — le programme permet d'activer ou de désactiver le contrôle de l'apparition de nouveau clusters défectueux sur le disque.
- **La structure des répertoires** — le programme permet d'activer ou de désactiver le contrôle de la modification de la structure de l'arborescence des répertoires du disque (recherche des répertoires nouveaux et effacés).

14.5.2.4. Procédés de calcul des sommes de contrôle pour les fichiers d'un disque donné

☑ **Vérifier tous les fichiers** — indépendamment des paramètres communs de vérification des fichiers. Dans ce cas, le programme Kaspersky® Inspector vérifiera tous les fichiers de ce disque.

Ici on peut définir l'algorithme le plus pratique de calcul des sommes de contrôle:

- **Sans CRC** — ne pas calculer les sommes de contrôle pour les fichiers ayant cette extension. Dans les tables ne sont stockées que les informations sur la taille, l'heure et la date de création du fichier.
- **CRC rapide** — ce type de somme de contrôle dépend de la structure interne des fichiers exécutables DOS et Windows, et avec des pertes insignifiantes de temps, elle permet de contrôler de manière fiable l'intégrité de ces fichiers. Il est instamment recommandé pour les fichiers du type COM, EXE, VXD, DLL, 386, CPL, SCR et autres fichiers exécutables.
- **CRC complet** — calcul de la CRC dans tout le fichier. Le contrôle de l'intégrité du fichier est le plus complet, mais ce procédé exige sensiblement plus de temps pour la vérification. Recommandé pour les fichiers BAT et SYS.
- **Macro - CRC rapide** — ce type de somme de contrôle dépend de la structure interne des macrodocuments (Documents Microsoft Word®, Microsoft Excel® et Microsoft Access®) et permet de contrôler efficacement l'intégrité des documents OLE2. Recommandé pour les fichiers avec une extension DOC, DOT (DO?), XLS, XLA, (XL?), MDB.
- **Macro - CRC complet** — calcul de la totalité de la CRC dans toutes les macros. Le contrôle de l'intégrité des documents est le plus complet.

Il est recommandé de choisir "macro – CRC" uniquement pour les fichiers contenant des macros OLE2. A l'heure actuelle, les applications suivantes sont supportées — (Microsoft Word®, Excel® et Access®).

14.5.3. Vérification de la présence de virus furtifs

Vérifier la présence de virus furtifs — vérifier la présence sur le disque de virus furtifs:

- **Tous les fichiers** — tous les fichiers.
- **Uniquement les nouveaux fichiers** — uniquement les nouveaux fichiers.

En cas de vérification de l'ordinateur avec l'option Tous les fichiers activée, seule la recherche des virus furtifs est effectuée.

La vérification de la présence de virus furtifs avec accès par le biais des outils du système d'exploitation n'est pas **effectuée**.

14.5.3.1. Réglages complémentaires

- **Vérifier les répertoires actifs** — vérifier sur un disque donné les répertoires actifs.
- **Sauvegarder les informations pour le module de réparation** — pour ce disque, activer l'assistance de réparation.
- **Vérifier le registre système** — vérifier les fichiers du registre.

14.5.4. Sauvegarde des réglages sur le disque et chargement des réglages depuis le disque

Tous les réglages peuvent être sauvegardés dans un fichier spécial avec une extension *.klr.

Pour sauvegarder les réglages effectués sur le disque dur de l'ordinateur,

1. Dans le menu Fichier, sélectionnez la commande Enregistrer le profil sous.
2. Dans la boîte de dialogue standard Windows qui apparaît, indiquez le chemin d'accès et le nom du fichier dans lequel vous voulez sauvegarder les réglages effectués.
3. Cliquez sur le bouton **Enregistrer**.

Pour charger les réglages effectués antérieurement depuis le fichier,

1. Dans le menu **Fichier** sélectionnez la commande **Charger un profil**.

2. Dans la boîte de dialogue standard Windows qui apparaît, indiquez le chemin d'accès et le nom du fichier depuis lequel vous voulez charger les réglages.
3. Cliquez sur le bouton **Ouvrir**.

14.6. Consultation des résultats de la vérification des disques

14.6.1. Consultation des informations générales sur le travail de Kaspersky® Inspector

Pour consulter les informations générales sur le travail de Kaspersky® Inspector,

1. Après le lancement de la procédure de vérification des disques, cliquez avec la souris sur l'icône de la catégorie 

.
2. Après quoi, une fenêtre apparaît (Illustration 117), dans laquelle sont affichées les informations générales sur la procédure de vérification.

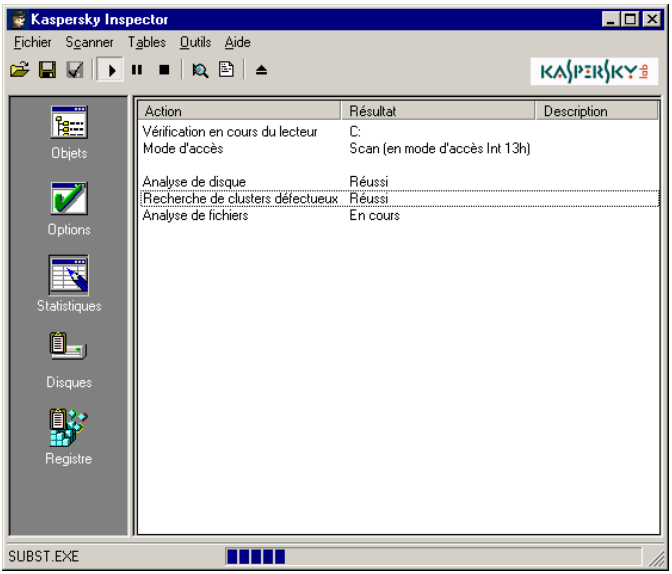


Illustration 117. affichant les informations sur la procédure de vérification

14.6.2. Consultation des informations générales sur les modifications

A la fin de la procédure de vérification, une boîte de dialogue apparaît, vous demandant de confirmer le passage à la consultation des modifications détectées (Illustration 118).

Pour basculer dans la fenêtre de consultation des modifications, cliquer sur le bouton **Oui**.

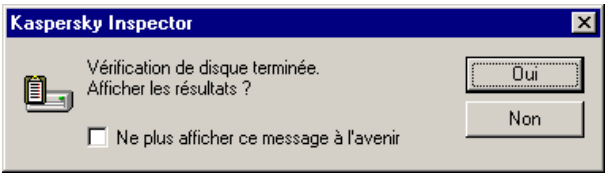


Illustration 118. Confirmation du passage à la consultation des modifications détectées

Après quoi, dans la fenêtre active s'affiche la liste générale des modifications détectées par Kaspersky® Inspector durant la procédure de travail avec l'indication du nombre de modifications pour chaque type (Illustration 119).

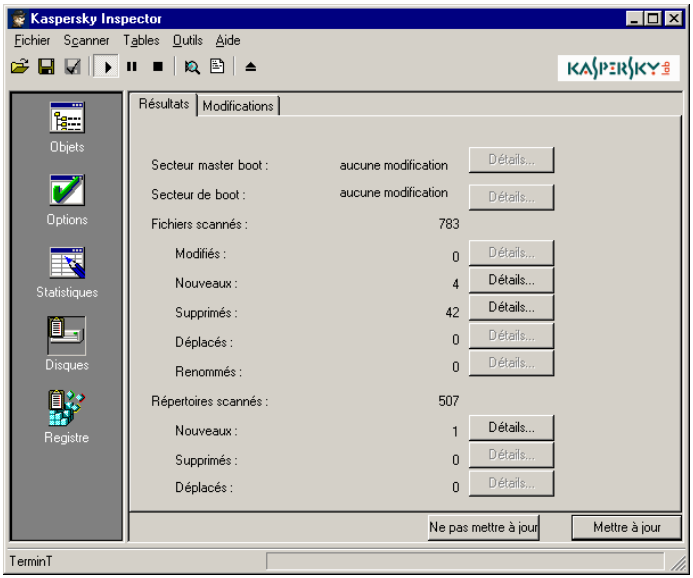


Illustration 119. Liste des modifications détectées

Si parmi les modifications se trouvent des cas suspects, caractéristiques de manifestations virales, Kaspersky® Inspector affiche une fenêtre d'alerte contenant la liste de toutes les modifications suspectes, avant même d'afficher la fenêtre avec les résultats de la vérification.

Dans cette liste se trouvent les informations sur les modifications survenues depuis la dernière vérification du disque: nombre de fichiers modifiés, nouveaux, supprimés, déplacés, renommés, de répertoires nouveaux, supprimés, déplacés, ainsi que les modifications dans les secteurs Master Boot et Boot. Pour recevoir des informations détaillées sur ces objets, cliquez sur le bouton **Détails**.

Si nécessaire, toutes les modifications décelées peuvent être consultées sous forme de liste hiérarchique en passant dans l'onglet **Modifications** (Illustration 120).

En utilisant le menu contextuel de cette liste hiérarchique, il est possible d'exécuter sur les fichiers et les dossiers modifiés toutes les opérations prévues par le programme (voir paragraphe 14.6.3).

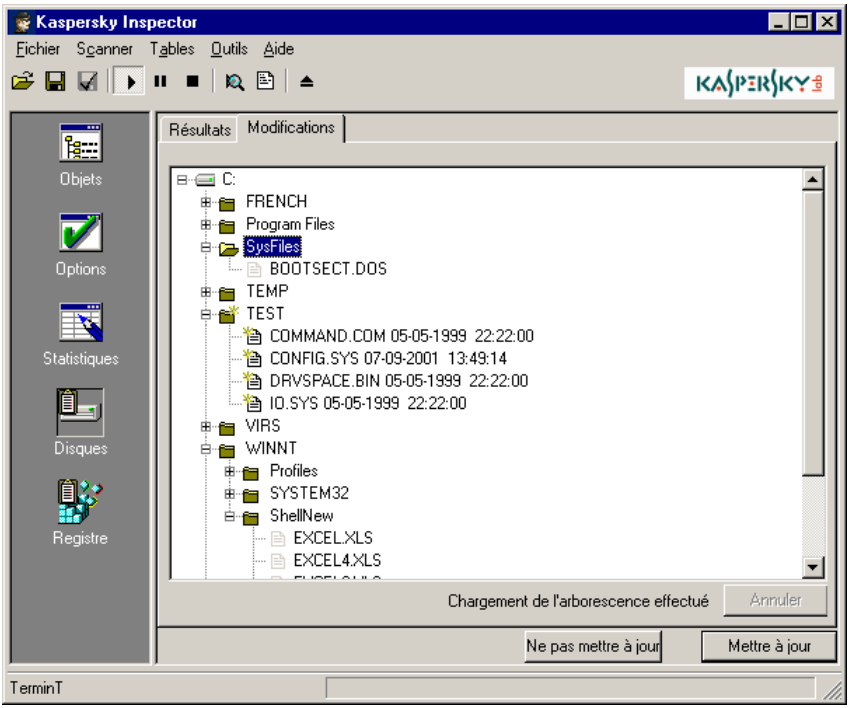


Illustration 120. Arborescence des modifications

14.6.3. Opérations autorisées sur les fichiers et les répertoires modifiés

Pour consulter les informations détaillées sur les fichiers et les dossiers modifiés, cliquez avec la souris sur le bouton **Détails** sur la ligne correspondant au type de modifications que vous souhaitez consulter.

Après cela, la boîte de dialogue avec la liste détaillée des modifications détectées (Illustration 121) apparaît.

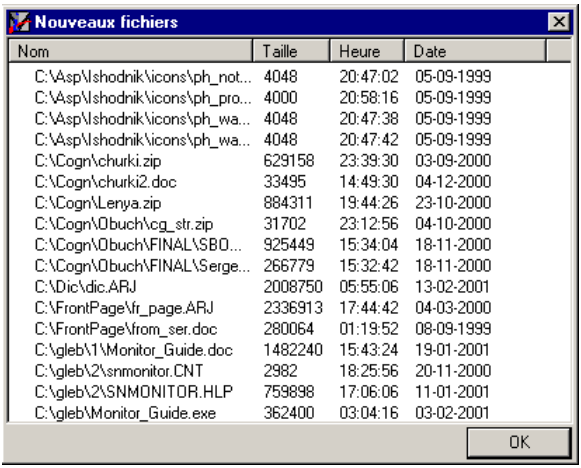


Illustration 121. Liste des modifications (nouveaux fichiers)

Si nécessaire, il est possible d'exécuter (sur les types suivants d'objets modifiés) la série d'opérations qui sont prévues par Kaspersky® Inspector:

- **fichiers modifiés** — ligne **Modifiés** du groupe **Fichiers scannés**
- **nouveaux fichiers** — ligne **Nouveaux** du groupe **Fichiers scannés**
- **fichiers déplacés** — ligne **Déplacés** du groupe **Fichiers scannés**
- **fichiers renommés** — ligne **Renommés** du groupe **Fichiers scannés**
- **nouveaux répertoires** — ligne **Nouveaux** du groupe **Répertoires scannés**.

Les autres types de modifications détectées ne peuvent pas être édités.

Toutes les opérations prévues par le programme sur les objets modifiés sont initialisées depuis le menu contextuel.

Pour les **fichiers modifiés** et les **nouveaux fichiers** les opérations suivantes sont prévues:

- **Supprimer** — supprimer le fichier.
- **Ajouter à la liste d'exclusion** — ajouter le fichier à la liste des fichiers exclus du nombre des fichiers vérifiés.
- **Ajouter à la liste stable** — ajouter le fichier à la liste des fichiers stables.
- **Vérifier avec Kaspersky AV** — vérifier le fichier sélectionné à l'aide de l'anti-virus.

- **Tout vérifier avec Kaspersky AV** — vérifier tous les fichiers de la liste à l'aide du scanner anti-virus. Les **fichiers renommés et les fichiers déplacés** peuvent être uniquement supprimés, pour cela, sélectionnez la commande **Supprimer** du menu contextuel.

Lors de la consultation de la liste des **nouveaux répertoires**, il est possible d'utiliser une des deux commandes du menu contextuel:

- **Vérifier avec Kaspersky AV** — vérifier le répertoire sélectionné à l'aide du scanner anti-virus.
- **Tout vérifier avec Kaspersky AV** — vérifier tous les répertoires de la liste à l'aide du scanner anti-virus.

14.6.4. Boîte de dialogue du secteur de Master Boot

En cas de détection dans le secteur Master Boot de l'ordinateur, Kaspersky® Inspector affiche sur l'écran une boîte de dialogue avec un message d'alerte sur les modifications détectées.

Pour la consultation détaillée des modifications détectées, cliquez sur le bouton **Détails** de la ligne correspondante.

La boîte de dialogue **Secteur de master boot** (Illustration 122) s'affiche.

Dans cette boîte de dialogue, il est possible de voir quels champs de la table de partitions ont été modifiés. Habituellement, en cas d'infection virale, la table de partitions reste intacte et seul est modifié le chargeur, c'est-à-dire les virus, mais il existe des virus qui changent l'adresse d'origine de la partition active tout en laissant intact le chargeur. En outre, le changement de système d'exploitation (ou de version de SE) entraîne une modification du chargeur.

Analysez soigneusement la cause des modifications dans le secteur de master boot !

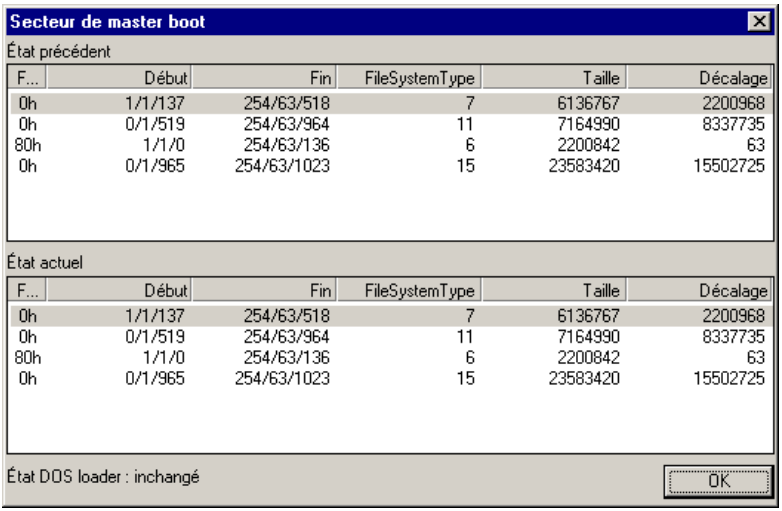


Illustration 122. Secteur de Master Boot

14.6.5. Boîte de dialogue du secteur de Boot

Si, durant son activité, Kaspersky® Inspector détecte des modifications dans le secteur de Boot, une boîte de dialogue avec un message d'alerte sur les modifications détectées s'affiche à l'écran.

Pour consulter le détail les modifications détectées, cliquez sur le bouton **Détails** de la ligne **Secteur d'amorçage**.

Après quoi, la boîte de dialogue **Secteur de boot** (Illustration 123) apparaît.

Dans cette boîte de dialogue, il est possible de voir quels champs du bloc de paramètres BIOS (BPB) ont été modifiés. Ordinairement, en cas d'infection virale, le BPB reste intact, alors que seul le chargeur est modifié (il arrive souvent que le passage vers le chargeur [Loader JMP] et le nom de la société productrice du système d'exploitation soient modifiés). En outre, le changement de système d'exploitation (ou de version du système d'exploitation) entraîne une modification du chargeur.

Analysez minutieusement la cause des modifications dans le secteur de boot!

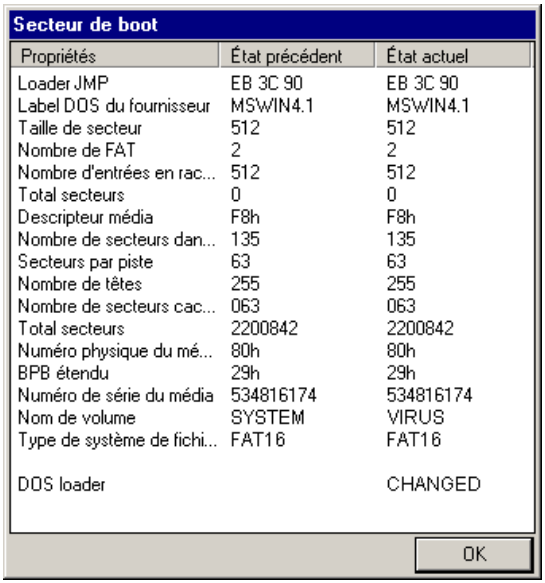


Illustration 123. Secteur de boot

14.6.6. Consultation des modifications des fichiers du registre

Si dans les réglages du programme il a été spécifié de vérifier les fichiers du registre de l'ordinateur (voir p. 14.5.3.1), pour consulter la liste des modifications détectées par Kaspersky® Inspector, cliquez avec la souris sur l'icône 

dans la zone des catégories. Après quoi, la fenêtre active affichera un récapitulatif des informations sur les modifications (Illustration 124).

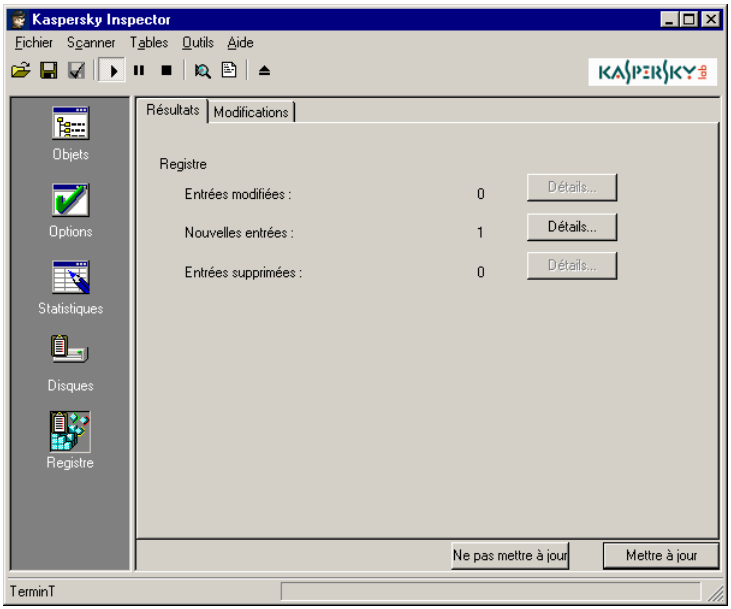


Illustration 124. Liste des modifications détectées dans le registre

Si nécessaire, toutes les modifications détectées peuvent être consultées sous forme de liste hiérarchique. Pour ce faire, passez dans l'onglet **Modifications** (Illustration 125).

Pour consulter les informations détaillées sur les modifications, les clés du registre, qu'elles soient neuves ou supprimées depuis la dernière vérification, cliquez sur le bouton **Détails** situé dans la ligne correspondante. Après quoi, la boîte de dialogue avec la description détaillée de toutes les modifications (Illustration 126) s'affiche à l'écran.

Kaspersky® Inspector ne vérifie pas la présence de modifications dans toutes les clés du registre de l'ordinateur mais seulement dans les copies des clés responsables du lancement automatique des programmes. Voici les principales d'entre elles:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones

HKEY_CURRENT_USER\Software\Microsoft\Office\8.0

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
ex

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runservi
ces

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runservi
cesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runonce
ex

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservi
ces

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservi
cesonce

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion

HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps

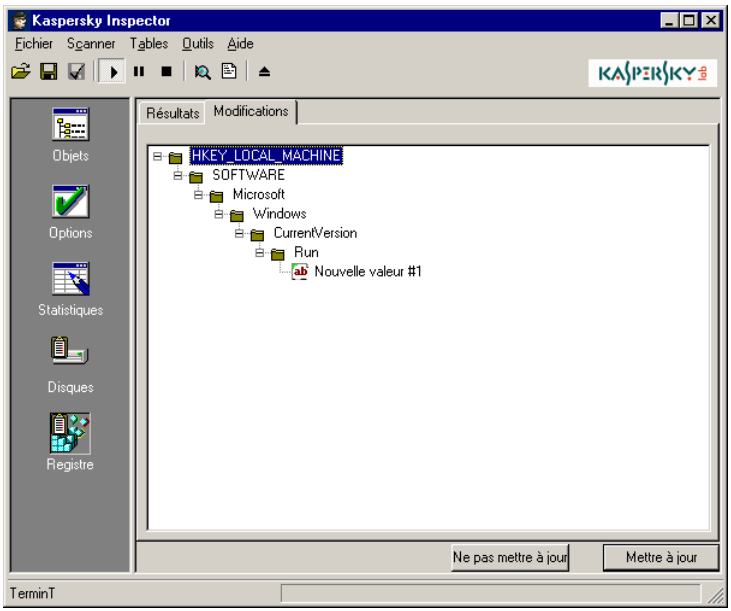


Illustration 125. Arborescence des modifications des clés du registre

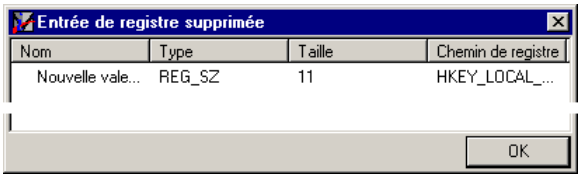


Illustration 126. Liste des clés du registre supprimées

14.6.7. Adoption/Rejet des modifications des tables

Pour inscrire dans les tables du programme Kaspersky® Inspector les modifications détectées lors de la vérification des fichiers, des répertoires et du registre de l'ordinateur, cliquez sur le bouton **Mettre à jour** (Illustration 119 et Illustration 124). Après quoi, toutes les modifications seront reportées dans les tables et, lors des vérifications ultérieures, Kaspersky® Inspector comparera l'état des disques en cours avec ces nouvelles données.

Si, pour une raison quelconque, il est nécessaire de ne pas reporter les modifications dans les tables, cliquez sur le bouton **Ne pas mettre à jour**. Dans ce cas, lors de vérification suivante, Kaspersky® Inspector détectera à nouveau les mêmes modifications.

ANNEXE A. AUTRES MODES DE VERIFICATION

A.1. Analyse heuristique

L'analyseur heuristique (Code Analyzer) vérifie dans les codes des fichiers et des secteurs la présence d'instructions ayant l'aspect de virus. S'il trouve des instructions suspectes (telles que l'ouverture d'un autre fichier, l'ajout de code, l'interception d'interruptions système, etc.), le fichier vérifié est considéré comme **suspect** et un message approprié s'affiche à l'écran :

Suspicion: <TYPE>, où <TYPE> est une des lignes:

- **Com** — le fichier a l'aspect d'un fichier infecté par un virus inconnu infectant les fichiers com
- **Exe** — le fichier a l'aspect d'un fichier infecté par un virus inconnu infectant tous les fichiers exe
- **ComExe** — le fichier a l'aspect d'un fichier infecté par un virus inconnu infectant les fichiers aux formats COM et EXE
- **ComTSR**, **ExeTSR**, **SysTSR**, **ComExeTSR** — le fichier a l'aspect d'un fichier infecté par un virus résident inconnu infectant les fichiers aux formats COM, EXE, SYS
- **Boot** — le fichier/secteur à l'aspect d'un fichier infecté par un virus de boot ou d'un installateur de virus de boot
- **Trojan** — le fichier a l'aspect d'un programme de Troie
- **Trivial** — le fichier a l'aspect d'un fichier infecté par un virus inconnu qui efface les fichier exécutables dans le répertoire courant (la taille de ce virus excède rarement 300 octets)
- **HLL** — le fichier a l'aspect d'un fichier infecté par un virus inconnu infectant les fichiers exécutables. Il est écrit dans un langage de haut niveau (C, Pascal)
- **Win32** — le fichier a l'aspect d'un fichier infecté par un virus Windows inconnu
- **Formula** — le fichier Excel contient des commandes suspectes
- **Macro.Word97.Fs –** suspicion de virus de la famille Macro.Word97.Fs

- **RemoteTemplate** – le document contient une référence à un modèle chargé automatiquement lors de l'ouverture du fichier
- **HTML.SecurityBreach.2** – le fichier HTML ou la lettre de la messagerie électronique au format HTML comporte une référence à un objet suspect
- **IRC-Worm.generic –** le fichier a l'aspect d'un fichier infecté par un ver inconnu se diffusant via les canaux IRC
- **BAT –** le fichier a l'aspect d'un fichier infecté par un virus inconnu infectant les fichiers au format BAT
- **VBS.I-Worm –** le fichier a l'aspect d'un fichier infecté par un ver inconnu se diffusant via la messagerie électronique.

Bien sûr, comme n'importe quel outil de ce genre, cet analyseur peut provoquer de fausses alertes et considérer comme infecté un fichier sain. Si vous rencontrez une fausse alerte lors de la vérification de fichiers, signalez-le nous et envoyez-nous une copie de ces fichiers afin que nous puissions les étudier.

Lorsqu'il effectue sa vérification, l'analyseur heuristique examine la structure d'un programme dans ses moindres détails. Ce mécanisme détecte environ 92% des virus contenus dans la base de données de la société Kaspersky Labs, c'est pourquoi nous estimons que les nouveaux virus encore inconnus seront détectés avec le même taux de probabilité.

A.2. L'analyse redondante

Dans de nombreux cas, un virus s'enregistre lui-même au point d'entrée d'un fichier en indiquant une référence à son corps qui est en général ajouté au contenu du fichier. Pour détruire de tels virus, il convient simplement de lancer une procédure d'analyse ordinaire qui se charge d'effacer l'adresse du virus au point d'entrée du fichier puis le corps lui-même vers lequel pointe cette adresse.

Toutefois, il arrive que le virus divise son corps en plusieurs parties et les place dans des zones libres du fichier. Dans ce cas, une analyse ordinaire pourra neutraliser le virus (c'est-à-dire que l'adresse au point d'entrée et la partie principale du corps du virus seront éliminées) mais il restera certains éléments indésirables au sein du fichier. Dans ce cas, vous devez lancer une *analyse redondante* – qui ne se contente pas de vérifier les points d'entrée du fichier, mais son contenu complet.

Le mode d'analyse redondante n'est recommandé que si l'analyse ordinaire n'a détecté aucun virus mais que des phénomènes **étranges** sont observés dans le fonctionnement du système (réinitialisations **spontanées**, ralentissement du travail de certains programmes, et autres comportements bizarres). Dans les autres cas, l'utilisation de ce mode est déconseillée car la procédure d'analyse est très ralentie et parce que la probabilité de fausses alertes augmente également.

ANNEXE B. GLOSSAIRE

Kaspersky Anti-Virus® Control Centre – programme permettant de piloter les autres modules. Il est utilisé pour le lancement automatique des tâches planifiées, ainsi que pour le contrôle des résultats de leur exécution.

Kaspersky Anti-Virus® Mail Checker – programme de protection antivirale destiné aux utilisateurs qui se servent d'un gestionnaire de courrier électronique compatible avec Microsoft Exchange Client pour l'envoi et la réception des messages .

Kaspersky Anti-Virus® Monitor (Monitor) – moniteur anti-virus résident. En cas de détection de virus, Monitor interdira l'appel d'un objet dangereux et en avisera l'utilisateur.

Kaspersky Anti-Virus® Rescue Disk – programme destiné à la création des disques de secours.

Kaspersky Anti-Virus® Scanner (Scanner) – programme de vérification antivirale de l'ordinateur et de suppression des virus éventuellement détectés, fonctionnant à la demande de l'utilisateur .

Kaspersky Anti-Virus® Updater – programme de mise à jour automatique des bases de données anti-virus ainsi que des composants logiciels.

Kaspersky® Inspector (Inspector) – programme d'inspection du disque, Kaspersky® Inspector vérifie la présence/l'absence de modifications au niveau du contenu des fichiers/répertoires, et prévient l'utilisateur en cas de détection de modifications suspectes. Ce programme peut être utilisé comme programme anti-virus auxiliaire ou de contrôle des modifications intervenues sur le disque. Il diminue la durée de l'analyse car il ne soumet au scannage que les fichiers nouveaux ou modifiés.

Kaspersky® Office Guard – programme destiné à la protection des documents Microsoft Office 2000 contre des virus de macro connus ou inconnus.

Kaspersky® Report Viewer – programme de consultation et de gestion des rapports générés par les composants du package Anti-Virus Kaspersky®.

Alerte – message électronique envoyé automatiquement par le composant d'Anti-Virus Kaspersky® à une adresse déterminée lors de la survenue d'un événement déterminé (détection de virus, panne de programme, etc.).

Analyse – procédure de vérification de la zone scannée dans le but de détecter d'éventuels virus (Scanner) ou modifications suspectes (Inspector). La mémoire de l'ordinateur, des disques, les dossiers, etc. sont des zones susceptibles d'être analysées.

Anti-virus – logiciel protégeant l'ordinateur contre la pénétration/diffusion de virus.

Arborescence des réglages – élément de l'interface dans lequel toutes les données sont présentées sous la forme d'une arborescence, dont les nœuds sont les éléments standards de gestion (boutons, listes, cases à cocher, etc.).

Attaque virale – série de tentatives ciblées d'infection virale de l'ordinateur.

Bases anti-virus – les bases anti-virus contiennent la description des virus et des méthodes d'éradication ou de réparation. Le Laboratoire Kaspersky complète chaque semaine les bases anti-virus avec des informations sur les nouveaux virus et les met à disposition sur son site Web d'où il est possible de les télécharger à l'aide du programme de mise à jour.

Catégorie – ce mot est utilisé pour désigner l'ensemble des réglages s'appliquant à un ensemble. Les boutons permettant de basculer entre les catégories sont disposés dans une zone déterminée (habituellement la partie gauche de la fenêtre).

"Cheval de Troie" – programme ou partie de programme exécutant des actions de destruction ou illégales. Les principales fonctions des chevaux de Troie consistent à perturber l'administration de l'ordinateur, à détourner des informations, à affecter le monitorage, etc.

Commande de macro suspecte – commande de macro susceptible d'avoir des conséquences dangereuses pour le système (par exemple suppression de fichier)®. Kaspersky® Office Guard permet à l'utilisateur de définir la succession des actions à réaliser en cas de détection d'une telle commande de macro.

Contrôleur anti-virus – voir Programme d'inspection du disque.

Disquettes de secours – jeu de disquettes à partir desquelles il est possible de démarrer l'ordinateur et de lancer la vérification anti-virus. Ces disquettes permettent de restaurer les capacités opérationnelles du système après une attaque virale. Elles contiennent un système d'exploitation, un anti-virus et les bases anti-virus. On peut les créer à l'aide du programme Kaspersky Anti-Virus® Rescue Disk.

Dysfonctionnement – situation dans laquelle un objet indemne est considéré par l'anti-virus comme infecté.

Fichier de réglages (*Profil*) – fichier dans lequel sont stockés les principaux réglages du programme. On peut exporter (sauvegarder) les réglages dans le fichier ou les importer (charger) à partir du fichier. Lors du démarrage du programme, les réglages sont pris dans le "Profil par défaut".

Interface utilisateur du package Anti-Virus Kaspersky – partie du programme servant à l'échange d'informations entre les différents outils et l'utilisateur.

Masque intelligent – pour accélérer le travail des programmes anti-virus (par exemple, Kaspersky Anti-Virus® Scanner), il est possible d'exclure des fichiers à vérifier tous ceux qui ne peuvent pas être infectés par un virus. Ce tri est possible en activant la vérification par masque intelligent (commande "Analyser tous les fichiers infectables"). La liste des fichiers exposés à une infection est stockée dans les bases anti-virus et est mise à jour en même temps que les bases.

Mécanisme heuristique de recherche de virus – trois opérations sont mises en œuvre : analyse de la succession des commandes dans chaque objet vérifié, étude de certaines statistiques et jugement du type **infection possible** ou **indemne**. Ce mécanisme est utilisé pour la recherche des virus inconnus.

Moniteur anti-virus résident – programme situé en permanence dans la mémoire de l'ordinateur et vérifiant l'ensemble des flux de données (documents ouverts, fichiers sauvegardés, etc.).

Objet suspect – objet dont les actions ou le contenu sont comparables à ceux d'un virus. Il peut s'agir d'une zone de la mémoire, d'un fichier, d'une macro, etc.

Partie Outils du composant du package Anti-Virus Kaspersky® – partie du programme se trouvant en permanence dans la mémoire et accomplissant un travail de base (analyse, monitorage).

Piratage du système – accès illégal aux données/ressources du système. Le piratage du système utilise souvent des programmes de virus.

Quarantaine – dossier spécial dans lequel sont placées les copies cryptées des fichiers suspects. Ces fichiers peuvent être restaurés à l'aide du programme Kaspersky Anti-Virus® Control Centre, s'ils ont été supprimés par erreur. Il est également possible de les envoyer au Laboratoire Kaspersky pour en déterminer le degré d'infection.

Vérificateur de disque – programme de vérification des éventuelles modifications du disque (voir aussi Kaspersky® Inspector).

Scanner anti-virus – programme recherchant dans l'ordinateur d'éventuels objets suspects (voir aussi Kaspersky Anti-Virus® Scanner).

Serveur de mises à jours – serveur Internet sur lequel sont stockées les bases anti-virus récentes ou les modules logiciels.

Tableau d'informations sur la base de registre – fichier créé par Kaspersky® Inspector, dans lequel sont stockés les renseignements sur les clés importantes de la base de registre (chargement initial, fichiers clés).

Tableau d'informations sur les disques – fichier créé par Kaspersky® Inspector, dans lequel sont stockés les renseignements sur le contenu des disques logiques de l'ordinateur (fichiers CRC, structure des répertoires).

Ver – virus qui se répand dans un réseau informatique. En cas d'infection d'un ordinateur, le ver calcule les adresses des autres ordinateurs sur le réseau et diffuse ses copies vers ces adresses. Ces virus créent parfois des fichiers de travail sur les disques du système mais ils ne peuvent pas appeler les ressources de l'ordinateur (à part la mémoire vive).

Virus – un des traits caractéristique du virus informatique est son aptitude à créer ses propres doubles (sans qu'il y ait forcément duplication à l'identique de l'original) et à les introduire dans les réseaux informatiques et/ou dans les fichiers, les zones système de l'ordinateur et autres objets exécutables. En outre, les doubles conservent une aptitude à se répandre (voir l'ouvrage de E. Kaspersky "Les Virus informatiques").

Virus de script – virus écrit en langage de script. Ce type de virus s'insère dans une page Web et se lance lors de la consultation de la page infectée. Les virus de script peuvent aussi se trouver dans le courrier écrit au format HTML.

Virus de zone d'amorçage (virus de Boot) – ce type de virus infecte le secteur d'amorçage (secteur de boot) de la disquette et le Master Boot Record (MBR) du disque dur. Ce virus ''contraint'' le système, lors de son redémarrage, à mettre en mémoire et à transmettre la gestion non pas au code original du chargeur mais au code du virus, c'est-à-dire que l'infection se produit au moment de l'amorçage à partir d'une source déjà infectée.

Virus furtif (Stealth) – virus qui par tous les moyens cherche à cacher sa présence dans le système. Les fonctions Stealth peuvent être présentes dans tous les types de virus.

Virus macro – virus écrit en langage de macro. Ce virus est activé lors de l'exécution d'une macro, de plus il infecte les autres fichiers susceptibles de contenir des macros (documents Word, tableaux Excel, etc.).

Virus polymorphe – virus prenant des mesures spéciales pour compliquer sa détection et son analyse. Ce virus n'a pas de signature, c'est-à-dire ne contient aucun secteur permanent de code.

Virus Windows – virus utilisant pour son travail les spécificités du système d'exploitation Microsoft Windows.

ANNEXE C. KASPERSKY LABS LTD.

Fondée en 1997, Kaspersky Labs Ltd. est actuellement la société de développement de logiciels de sécurité informatique la plus connue en Russie. Son large éventail de solutions comprend vous protège contre les virus informatiques, le courrier non sollicité et les intrusions de pirates informatiques.

Kaspersky Labs est une société internationale. Le siège social se situe en Russie et la société dispose de représentations commerciales au Royaume-Uni, en France, en Allemagne, au Japon, au Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Le Centre européen d'études des virus, le dernier-né des départements de la société, a vu le jour en France. Notre réseau de partenaires réunit plus de 500 sociétés dans le monde entier.

La compagnie est constituée actuellement de plus de 250 spécialistes hautement qualifiés dont 10 sont titulaires d'un MBA (diplôme d'administration d'entreprises), 15 possèdent un doctorat et 2 sont membres de l'éminente organisation informatique de recherche antivirus (CARO).

La valeur essentielle de la société – c'est le savoir et l'expérience uniques accumulés par ses collaborateurs au cours de 14 années d'une lutte impitoyable contre les virus informatiques. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Labs. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Labs a été une des premières sociétés à développer plusieurs normes modernes pour les logiciels antivirus. Kaspersky Anti-Virus®, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : postes de travail, serveurs de fichiers, serveurs Web, serveurs de courrier électronique, pare-feu et ordinateurs de poche. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux éditeurs de logiciels étrangers utilisent dans leurs produits le noyau de Kaspersky Anti-Virus®. Citons par exemple : Nokia ICG (Etats-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Labs bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la

moindre de leurs attentes. Nous élaborons, mettons en oeuvre et accompagnons les dispositifs de protection antivirale pour entreprise. Notre base antivirus est mise à jour toutes les douze heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

C.1. Autres produits antivirus

Kaspersky Anti-Virus® Lite

Le logiciel antivirus le plus facile à utiliser de Kaspersky Labs est conçu pour protéger les ordinateurs à usage personnel sous Windows 98/Me, Windows 2000/NT Workstation et Windows XP.

Kaspersky Anti-Virus® Lite comprend :

- **Un analyseur antivirus** qui vérifie de manière exhaustive le contenu de tous les disques locaux et partagés à la demande de l'utilisateur ;
- **Un moniteur antivirus** qui vérifie automatiquement et en temps réel tous les fichiers utilisés ;
- **Un analyseur de bases de données de courrier** MS Outlook Express, capable de détecter des virus à la demande.

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Windows 98/ME, Windows 2000/NT et Windows XP contre tous les types de virus connus, y compris les chevaux de Troie, les vers Internet, les virus de script, les ActiveX et les applets Java dangereux, etc. Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Kaspersky Anti-Virus® Personal comprend un module de mise à jour quotidienne via Internet. Le système unique d'analyse heuristique des données de deuxième génération neutralise efficacement les virus inconnus. L'interface utilisateur conviviale permet de modifier rapidement la configuration et facilite au maximum l'utilisation du logiciel.

Kaspersky Anti-Virus® Personal permet :

- **L'analyse antivirale à la demande** des disques locaux ;
- **L'analyse antivirale automatique en temps réel** de tous les fichiers utilisés ;
- **Le filtrage du courrier** pour analyser en arrière-plan les messages entrants et sortants.

Kaspersky Anti-Virus® Personal est compatible avec plus de 700 formats de fichiers archivés ou compressés et assure l'analyse antivirale automatique de leur contenu. Il peut également supprimer tout code malveillant des fichiers archivés au format ZIP.

Kaspersky Anti-Virus® Personal Pro

Ce logiciel a été conçu pour la protection antivirale globale des ordinateurs personnels qui tournent sous Windows 95/98/ME, Windows 2000/NT et Windows XP avec les applications de la suite MS Office 2000. Kaspersky Anti-Virus® Personal Pro renferme un programme qui assure le téléchargement quotidien des mises à jour des bases antivirus ou des modules du logiciel. Le système unique d'analyse heuristique des données de deuxième génération neutralise efficacement les virus inconnus. L'interface utilisateur, simple et conviviale, permet de modifier rapidement la configuration et facilite au maximum l'utilisation du logiciel.

En plus de l'analyse automatique de tous les fichiers en temps réel ou à la demande, Kaspersky Anti-Virus® Personal Pro propose également un filtre de courrier électronique ainsi qu'un **inhibiteur de comportement** qui garantit une protection totale contre les virus de macro.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable contre les virus les données conservées dans un PDA sous système d'exploitation Palm OS ou Windows CE, ainsi que toute information transférée à partir d'un PC ou une carte mémoire, les fichiers ROM et les bases de données. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien sur le PDA que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[5] intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet

[5] En fonction du type de livraison

logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- Flux de données qui passent par les pare-feu ;
- Ordinateurs de poche.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

C.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Labs Ltd. (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://www.kaspersky.com/supportinter.html
Informations générales	WWW : http://www.kaspersky.com http://www.viruslist.com E-mail : sales@kaspersky.com

ANNEXE D. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB. ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN OUVRANT LE BOÎTIER DU CD, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. VOUS DEVEZ RETOURNER CE LOGICIEL POUR UN REMBOURSEMENT TOTAL. VOTRE DROIT AU RETOUR ET AU REMBOURSEMENT EXPIRE 30 JOURS APRES L'ACHAT CHEZ UN DISTRIBUTEUR OU REVENDEUR AGREE PAR KASPERSKY LAB. LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel ("Fichier Clé d'Identification") qui vous sera fournie par Kaspersky Labs comme faisant partie du Logiciel.

1. *Octroi de la Licence*. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Labs vous offre le droit non-exclusif et non-transférable d'utiliser une copie de cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer une copie du Logiciel sur un ordinateur, poste de travail, assistant digital personnel, ou tout autre appareil électronique pour lequel le Logiciel a été conçu (un "Système Client"). Si le Logiciel est inscrit en tant que suite ou paquet avec plus d'un seul Logiciel, cette licence s'applique à tous les Logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée sur le tarif en vigueur ou l'emballage du produit qui concerne chacun de ces Logiciels.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un Système Client ou par plus d'un utilisateur à la fois, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un Système Client lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de ce Système Client. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez le Système Client sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Labs contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Labs vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur ("Serveur") dans un environnement multi-utilisateurs ou en réseau ("Mode-Serveur") uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est exigée pour chaque Système Client ou "siège" pouvant se connecter au Serveur à tout moment, indifféremment du fait que de tels Systèmes Clients inscrits ou sièges sont connectés en même temps au Logiciel, y accèdent ou l'utilisent. L'utilisation d'un logiciel ou de matériel réduisant le nombre de Systèmes Clients ou sièges qui accèdent au Logiciel

ou l'utilisent directement (e.g., un logiciel ou matériel de "multiplexage" ou de "regroupement") ne réduit pas le nombre de licences exigées (i.e., le nombre requis de licences égalerait le nombre d'entrées distinctes au logiciel ou matériel de multiplexage ou de regroupement frontal). Si le nombre de Systèmes Clients ou sièges pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. Cette licence vous permet d'effectuer ou de télécharger autant de copies de la Documentation que le réseau compte de Systèmes Clients ou sièges possédant une licence d'utilisation du Logiciel, et pourvu que chaque copie contienne les notes de propriété de la Documentation.

1.3 Licences de volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en oeuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous permet d'effectuer ou de télécharger une copie de la Documentation pour chaque copie additionnelle autorisée par la licence de volume, pourvu que chaque copie contienne toutes les notes de propriété de la Documentation.

2. *Durée*. Ce Contrat est valable pour la période indiquée dans le Fichier Clé d'Identification (Ce fichier est unique et est nécessaire à l'activation complète du Logiciel, voir Aide/ sur Logiciel ou « à propos de ». Pour les versions Unix/Linux du Logiciel voir les notification sur la date d'expiration du Fichier Clé) à moins que celle-ci n'arrive à terme avant pour l'une des raisons notées ci-après. Ce contrat se terminera automatiquement si vous n'en respectez les termes, limites ou conditions décrites. Au-delà du terme ou expiration de ce Contrat, vous devez immédiatement détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez mettre un terme à ce Contrat à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. *Assistance technique*.

   (i) Kaspersky Labs vous fournira une assistance technique ("Assistance Technique") comme décrit ci-dessous pour une période d'un an à condition que:

      (a) le paiement des frais de l'assistance technique en cours ait été fait; et

      (b) le Formulaire d'Inscription à l'Assistance Technique fourni avec ce Contrat ou disponible sur le site web de Kaspersky Labs ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Labs avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Labs de juger si vous

remplissez les conditions nécessaires pour un accès aux services d'Assistance Technique.

(ii) L'Assistance technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Politique de Confidentialité de Kaspersky Labs jointe à ce Contrat, et vous consentez explicitement au transfert de données vers d'autres pays que le votre en accord avec les termes de la Politique de Confidentialité.

(iv) "Assistance Technique" signifie

(a) Mises à jour quotidiennes des bases de données antivirales;

(b) Mises à jour gratuites du logiciel, incluant des mises à niveau de versions;

(c) Assistance Technique étendue par E-mail et assistance téléphonique fournie par votre Vendeur et/ou Distributeur;

(d) Mises à jour de détection et désinfection de virus sous 24 heures.

4. *Droits de Propriété*. Le Logiciel est protégé par les lois sur le copyright. Kaspersky Labs et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.
5. *Confidentialité*. Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Labs reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Lab. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.
6. *Limites de Garantie*

(i) Kaspersky Labs garantit que pour une durée de [90] jours suivant le téléchargement ou l'installation du logiciel, ce dernier fonctionnera correctement comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Labs ne garantit pas que le Logiciel

et/ou la Documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions et d'erreurs;

(iii) Kaspersky Labs ne garantit pas que ce Logiciel reconnaîtra tous les virus connus ou n'affichera de message de détection erroné;

(iv) L'entière responsabilité de Kaspersky Labs ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Labs de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Labs ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel;

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Lab, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat;

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (v) ont effet entre Kaspersky Labs et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

7. Limites de Responsabilité

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Labs en cas (i) de non-satisfaction de l'utilisateur, (ii) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, (iii) de toute infraction aux obligations impliquées par la loi "s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982" ou (iv) de responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i), le Fournisseur ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Labs (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

8. Le sens et l'interprétation de ce Contrat devront être déterminés en accord avec les lois d'Angleterre et du Pays de Galles. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Labs était autorisé en tant que requérant à entamer des procédures dans n'importe quelle juridiction compétente.
9. (i) Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet. En dehors des situations prévues dans les termes des paragraphes (ii) – (iii), vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat ("Fausse Représentation") et Kaspersky Labs ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé expressément dans ce Contrat.

(i) Rien dans ce Contrat n'engagera la responsabilité de Kaspersky Labs pour toute Fausse Représentation faite en connaissance de cause.

(ii) La responsabilité de Kaspersky Labs pour Fausse Déclaration quant à une question fondamentale pour la capacité du créateur à exécuter ses engagements envers ce Contrat, sera sujette à la limitation de responsabilité décrite dans le paragraphe 7 (iii).