KASPERSKY LAB

Kaspersky Anti-Virus® 5.0 for Windows Workstations

Guide de l'utilisateur

KASPERSKY ANTI-VIRUS® 5.0
FOR WINDOWS WORKSTATIONS

Guide de l'utilisateur

http://www.kaspersky.com/fr

Date d'édition : décembre 2004

Sommaire

CHAPITRE 1. VIRUS INFORMATIQUES ET PROGRAMMES MALVEILLANTS

L'augmentation du nombre d'utilisateurs d'ordinateurs et des moyens d'échange de données par courrier électronique ou via Internet accroît le risque d'infection des ordinateurs par des virus informatiques et de dégradation ou de vol de données par des programmes malicieux.

Afin de pouvoir identifier les menaces qui planent sur vos données, il convient de définir les différents types de programmes malveillants et leur *modus operandi*.

On distingue les familles suivantes de programmes malveillants en fonction de la manière dont ils se manifestent :

- **Les vers** *(Worms)* : ils se propagent sur les ressources du réseau. Les vers doivent leur nom à leur manière de passer d'un ordinateur à l'autre en exploitant le courrier électronique ainsi que d'autres canaux d'information. Cette technique leur permet de se diffuser à une très grande vitesse.

  Ils s'introduisent dans l'ordinateur, relèvent les adresses des autres machines raccordées au réseau et y envoient leur copie. De plus, les vers exploitent également les données contenues dans le carnet d'adresses des clients de messagerie. Certains représentants de cette catégorie de programmes malveillants peuvent créer des fichiers de travail sur les disques du système, mais ils peuvent très bien ignorer les ressources de l'ordinateur, à l'exception de la mémoire vive.

- **Les virus** *(Viruses)* : il s'agit de programmes qui infectent d'autres programmes. Ils insèrent leur code dans celui de l'application ciblée afin de pouvoir prendre les commandes au moment de l'exécution des fichiers infectés. Cette définition simple permet d'identifier l'une des principales actions exécutées par les virus, à s'avoir *l'infection*. La vitesse de propagation des virus est légèrement inférieure à celle des vers.
- **Les chevaux de Troie** *(Trojans)* : il s'agit d'applications qui réalisent diverses opérations sur l'ordinateur infecté à l'insu de l'utilisateur. Cela va de la destruction de données sauvegardées sur le disque dur au vol d'informations confidentielles en passant par le « plantage » du système. Ces programmes malicieux ne sont pas des virus au sens traditionnel du

terme. En effet, les chevaux de Troie sont incapables de s'introduire eux-mêmes dans un ordinateur. Au contraire, ils sont diffusés par des personnes mal intentionnées qui les présentent sous les traits d'applications « utiles ».

Les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnelles. La mise en place d'une procédure de sauvegarde régulière des données vous permettra de réduire les risques au minimum.

Ces derniers temps, ce sont les vers qui constituent la majorité des programmes malicieux en circulation. Viennent ensuite, par ordre de diffusion, les virus et les chevaux de Troie. Certains programmes malicieux répondent aux définitions de deux, voire trois, des types mentionnés ci-dessous.

Les types de riskwares suivants sont très répandus :

- **Adware** : programme introduit dans des applications à l'insu de l'utilisateur et dont l'objectif est d'afficher des publicités. Ces programmes sont diffusés gratuitement. Les publicités s'affichent sur l'interface de travail. Bien souvent, ces programmes recueillent des données personnelles sur l'utilisateur et les transmettent à l'auteur du programme, modifient les paramètres du navigateur (page d'ouverture, paramètres de sécurité, etc.) et créent un trafic non contrôlé par l'utilisateur. Tout ceci peut entraîner une violation de la sécurité, voire des pertes financières.
- **Riskwares** : logiciels qui n'ont pas de fonctions malfaisantes mais qui peuvent être utilisés par des personnes mal intentionnées en qualité de complément à un programme malfaisant car ils contiennent des failles. Cette catégorie reprend les programmes d'administration à distance, les clients IRC, les serveurs FTP et tous les utilitaires servant à arrêter des processus ou à dissimuler des activités..
- **Spyware** : programme qui vise à accéder de manière illicite aux données de l'utilisateur, de suivre les actions réalisées avec l'ordinateur et de recueillir les informations stockées sur le disque dur. Ce type de programme permet non seulement à son auteur de recueillir des informations, mais également de prendre les commandes des ordinateurs. Le spywares sont diffusés au sein d'applications gratuites et sont installés à l'insu de l'utilisateur. Les programmes de suivi de frappe de clavier, les programmes de déchiffrage de mot de passe et les programmes qui recueillent les informations confidentielles (comme les numéros de carte de crédit) appartiennent à cette catégorie.
- **Pornware** : programme établissant une connexion par modem vers un site Internet payant, généralement à contenu pornographique.
- **Outils d'attaque :** programme utilisé par des personnes malveillantes pour s'instroduire dans l'ordinateur d'autrui. Cette catégorie comprend les dispositifs de balayage, les programmes de déchiffrage de mot de passe

et tout autre programme qui vise à pénétrer dans les ressources d'un réseau.

Le courrier électronique et Internet restent les principaux vecteurs de diffusion des virus et des programmes malveillants. Toutefois, l'infection peut également avoir lieu par le biais d'une disquette ou d'un CD-ROM. Dans ce contexte, il convient de délaisser les analyses simples et régulières de l'ordinateur à la recherche d'éventuels virus au profit d'une protection complexe et permanente du poste de travail contre les risques d'infection.

CHAPITRE 2. QUE FAIRE EN CAS D'INFECTION DE VOTRE ORDINATEUR

Il est parfois difficile pour une personne non avertie de découvrir la présence d'un virus ou d'un cheval de Troie dans un ordinateur car ceux-ci se fondent parmi les fichiers habituels. Ce chapitre vous fournira une description détaillée des signes d'une infection, des moyens existants pour réparer les données après une attaque de virus et des mesures à prendre pour prévenir les infections par des programmes malicieux.

2.1. Signes d'une infection

Il existe toute une série d'indices qui peuvent indiquer l'infection de l'ordinateur. Si vous remarquez que votre ordinateur a un comportement bizarre, comme

- l'affichage à l'écran de messages ou de dessins inhabituels ;
- l'émission de sons étranges ;
- l'ouverture et la fermeture inattendue du lecteur de CD-ROM;
- le lancement aléatoire d'une application quelconque sans votre intervention;
- l'affichage par le logiciel Kaspersky Anti-Hacker de messages d'alerte vous annonçant qu'un logiciel installé sur votre ordinateur tente de se connecter à Internet sans que vous soyez à l'origine d'un tel comportement.

vous êtes alors plus que probablement victime d'un virus informatique.

Certains symptômes laissant présager une infection se manifestent également via le courrier électronique :

- Vous recevez un message vous informant que vous avez envoyé un message infecté à un destinataire quelconque et le logiciel antivirus du destinataire a rejeté votre message. Mais vous êtes certain de ne pas avoir envoyé un tel message ou d'avoir envoyé un message sain.
- Vos amis ou vos connaissances parlent de vos messages alors que vous ne leur avez rien envoyé ;
- Votre boîte aux lettres contient énormément de messages sans objet et sans adresse d'expéditeur.

Il convient de préciser que ces signes n'indiquent pas toujours la présence de virus. Ils peuvent être en effet la manifestation d'un autre problème. Ainsi, il est possible que les messages infectés reprennent votre adresse en tant qu'adresse de l'expéditeur même s'ils ont été envoyés depuis un autre ordinateur.

L'infection de votre ordinateur peut également se manifester au travers de toute une série de signes secondaires :

- Gel et échecs fréquents dans le fonctionnement de l'ordinateur ;
- Lenteur au moment du lancement des logiciels ;
- Impossibilité de charger le système d'exploitation ;
- Disparition de fichiers et de répertoires ou altération de leur contenu ;
- Requêtes fréquentes vers le disque dur (la petite lampe sur la tour clignote fréquemment) ;
- Microsoft Internet Explorer « plante » ou se comporte bizarrement (ex. :impossible de fermer les fenêtre du logiciel) ;
- L'ordinateur ne peut pas démarrer depuis le disque dur (un message d'erreur s'affiche à l'allumage).

Dans 90% des cas, ces symptômes sont causés par des problèmes matériels ou logiciels. Même si ces symptômes ne sont pas nécessairement la manifestation d'une infection, il est fortement conseillé de contacter votre administrateur de système et de procéder à une analyse complète de votre ordinateur.

2.2. Que faire lorsque les symptômes d'une infection sont présents ?

Si vous remarquez que votre ordinateur a un comportement suspect :

1. Ne paniquez pas ! La règle d'or dans ce type de situation est de garder son calme afin d'éviter de supprimer des données importantes et de se faire du soucis inutilement.
2. Si le symptôme observé vous empêche de démarrer l'ordinateur depuis le disque dur (un message d'erreur apparaît lorsque vous allumez l'ordinateur), essayez de démarrer en mode Sans échec ou au départ du disque de démarrage que vous avez créé au moment de l'installation du système d'exploitation.

3. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD, une carte Flash, etc.
4. Installez Kaspersky Anti-Virus, si cela n'a pas encore été fait.
5. Téléchargez les dernières mises à jour des bases antivirus. Dans la mesure du possible, téléchargez ces bases non pas au départ de votre ordinateur mais bien depuis un ordinateur sain. Il est en effet préférable d'agir ainsi car si votre ordinateur est bel et bien infecté, sa connexion à Internet permettra plus que probablement au virus d'envoyer des informations importantes à une personne mal intentionnée ou de se propager en envoyant une copie à tous les contacts de votre carnet d'adresses. C'est pour cette même raison qu'il est toujours conseillé de déconnecter votre ordinateur d'Internet si vous soupçonnez une infection. Dans la mesure où vous ne pourriez pas télécharger les dernières bases antivirus depuis un autre ordinateur, vous pouvez tenter d'exécuter cette opération depuis votre ordinateur juste avant de le mettre hors ligne.
6. Déconnectez l'ordinateur d'Internet.
7. Le cas échéant, déconnectez l'ordinateur du réseau local.
8. Lancez l'analyse complète de votre ordinateur (cf. point 5.2.2, p. 28).
9. Signalez le comportement suspect de votre ordinateur à l'administrateur de système.

2.3. Présence de virus

En cas de découverte de virus, Kaspersky Anti-Virus procèdera indépendamment au traitement antivirus de votre ordinateur et à la restauration des données conformément à la configuration établie.

Les infections sont dues dans 99% des cas à des vers de courrier électronique, des chevaux de Troie ou des virus (pour de plus amples informations sur les programmes malicieux, consultez le Chapitre 1 à la p. 5). L'intégrité des données peut quant à elle être pratiquement toujours restaurée.

Afin de supprimer les virus et de restaurer les données endommagées :

1. N'interrompez pas le fonctionnement de Kaspersky Anti-Virus. Lors de l'analyse complète de l'ordinateur, le logiciel répare les fichiers infectés, met en quarantaine les fichiers suspects et supprime les vers de courrier électronique et les chevaux de Troie. Avant de

procéder aux réparations à la fin de l'analyse complète, Kaspersky Anti-Virus reprend tous les fichiers suspects, les virus, les vers de courrier électronique et les chevaux de Troie. Vous pourrez également consulter par la suite le rapport d'activité du logiciel pour obtenir le nom des programmes malveillants qui avaient infecté votre ordinateur (cf. point 5.4.2, p. 39).

2. Dans certains cas, vous devrez utiliser un utilitaire spécial pour terminer la réparation des données. Rendez-vous sur le site de Kaspersky Lab (http://www.kaspersky.com/fr) et lisez les informations relatives au virus, au cheval de Troie ou au ver responsable de l'infection. Le cas échéant, téléchargez l'outil de réparation des données développé pour le code malicieux en question. Par exemple, il faudra télécharger et exécuter le programme *clrav.com* pour réparer les données endommagées par le virus **Klez**.

3. Lisez attentivement toutes les informations en rapport avec votre situation. Vous devrez peut-être également adopter des mesures complémentaires.

4. Si votre ordinateur a été victime d'un virus exploitant une vulnérabilité de Microsoft Outlook Express (ex. : **Nimda**, **Klez** ou **Badtrans**), il est fort possible que l'infection se répète si vous lisez des anciens messages infectés. Pour cette raison, il est primordial d'activer la réparation des bases de messagerie électronique (contactez votre administrateur de système pour obtenir de plus amples informations). Installez les correctifs de Microsoft Outlook pour renforcer la sécurité de votre client de messagerie.

Malheureusement, il n'est pas toujours possible de supprimer correctement les virus des objets infectés. Certains d'entre eux détruisent littéralement les informations au moment de l'infection.

2.4. Si rien n'y fait...

Lorsque l'analyse complète de l'ordinateur, la vérification du matériel et des logiciels ne donnent aucun résultat et que les symptômes persistent, votre dernière option consiste à envoyer une description détaillée de votre problème au Service d'assistance technique de Kaspersky Lab.

Vous pouvez également envoyer les fichiers infectés ou les chevaux de Troie à Kaspersky Lab en vue d'un examen approfondi.

Consultez l'Annexe B à la page 51 pour obtenir de plus amples informations sur la marche à suivre pour envoyer vos messages et les objets à Kaspersky Lab.

2.5. Après la suppression des conséquences de l'infection

Une fois débarrassé des conséquences de l'infection, analysez tous les disques ou les disquettes qui pourraient être infectés par un virus.

Veillez à utiliser la version la plus récente de Kaspersky Anti-Virus, les versions actuelles des bases antivirus et les paramètres recommandés par les experts de Kaspersky Lab (Contactez votre administrateur de système pour obtenir de plus amples informations sur les paramètres utilisés par Kaspersky Anti-Virus).

Lisez attentivement le chapitre **Prévention des infections de votre ordinateur** (cf. point 5.2, p. 26) et accordez une attention toute particulière aux règles de sécurité qui vous permettront d'éviter une nouvelle infection de votre machine.

CHAPITRE 3. KASPERSKY ANTI-VIRUS® FOR WINDOWS WORKSTATIONS

Kaspersky Anti-Virus® for Windows Workstations (ci-après Kaspersky Anti-Virus également) vise à protéger les postes de travail contre les virus et les programmes malveillants.

Le logiciel offre les fonctions suivantes :

- *Protection en temps réel du système de fichiers contre les codes malicieux en mode surveillance :* interception et analyse des requêtes adressées au système de fichiers de l'ordinateur et aux répertoires de réseau, réparation, suppression des objets infectés et isolement des objets suspects en vue d'une analyse ultérieure.
- *Recherche et neutralisation des codes malicieux à la demande de l'utilisateur ou de l'administrateur :* recherche et analyse des objets infectés et suspects dans les zones d'analyse définies ; réparation, suppression des objets infectés et isolement des objets suspects en vue d'une analyse ultérieure.
- *Analyse des riskwares :* analyse des programmes exécutés sur l'ordinateur ou téléchargés depuis Internet, ou se trouvant sur le disque dur ou des disques amovibles. Lors de la découverte d'un riskware, l'application (en fonction des paramètres) autorise ou non son exécution ou le supprime.
- *Analyse du courrier électronique en mode de surveillance :* analyse des requêtes de réception et d'envoi de messages via courrier électronique. Kaspersky Anti-Virus empêche l'arrivée dans la boîte aux lettres de l'utilisateur de messages contenant un code malicieux et l'envoi d'objets suspects ou infectés. L'analyse porte sur tout le courrier reçu et envoyé via Microsoft Outlook, de même que sur le courrier reçu et envoyé par n'importe quel client de messagerie compatible avec les protocoles SMTP et POP3.
- *Protection en temps réel des applications de bureautique utilisant les macros VBA :* analyse des macros avant leur exécution et blocage de l'exécution des macros qui présentent un risque.
- *Protection en temps réel contre les scripts VBScript et JavaScript dangereux.* L'analyse a lieu avant l'exécution du script par le module de traitement des scripts du système d'exploitation ; blocage de l'exécution des scripts dangereux.

- *Placement des objets suspects en quarantaine :* les objets suspects découverts sont conservés dans le répertoire de quarantaine ; envoi d'objets définis à Kaspersky Lab en vue d'une analyse approfondie ; restauration des objets à la demande de l'administrateur/de l'utilisateur.
- *Création d'une copie de l'objet infecté dans le dossier de sauvegarde avant la réparation et la suppression* afin de pouvoir éventuellement le restaurer au cas où il contiendrait des données importantes.
- *Mise à jour des bases antivirus et des modules* faisant partie de Kaspersky Anti-Virus depuis les serveurs de mise à jour de Kaspersky Lab ; création d'une copie de sauvegarde de tous les fichiers actualisés au cas où la dernière mise à jour devrait être annulée ; placement des mises à jours dans un répertoire de distribution afin de réduire l'intensité du trafic Internet.

N'oubliez pas que de nouveaux virus font leur apparition chaque jour. Pour cette raison, nous vous conseillons de sélectionner la mise à jour automatique afin que l'application dispose des informations les plus récentes.

3.1. Contenu du pack logiciel

Vous pouvez acquérir ce logiciel chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr - rubrique **Achat en ligne**).

Le pack logiciel contient :

- Une enveloppe cachetée contenant le CD d'installation avec les fichiers du logiciel ;
- Le manuel de l'utilisateur ;
- La clé de licence, incluse dans le fichier d'installation ou enregistrée sur une disquette spéciale ;
- La carte d'enregistrement (avec le numéro de série du logiciel) ;
- Le contrat de licence.

Avant de décacheter l'enveloppe contenant le CD, lisez attentivement le contrat de licence.

Si vous achetez ce logiciel en ligne, le fichier d'installation est téléchargé du site Web de Kaspersky Lab. Ce fichier d'installation inclut ce manuel et la clé de licence. La clé de licence est soit reprise dans la distribution ou soit envoyée par courrier électronique après réception de votre paiement.

3.1.1. Contrat de licence

Le contrat de licence constitue l'accord juridique passé entre vous et Kaspersky Labs Ltd., stipulant les conditions d'utilisation du progiciel 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 Anti-Virus 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.

3.1.2. Carte d'enregistrement

Veuillez remplir le talon détachable de la carte d'enregistrement en indiquant de manière exhaustive vos coordonnées : nom de famille, prénom, numéro de téléphone, adresse électronique (le cas échéant) et envoyez-le au distributeur chez qui vous avez acheté ce progiciel.

Veuillez signaler toute modification de vos coordonnées (Adresse postale/électronique et numéro de téléphone) à l'organisation à laquelle vous aviez envoyé le talon détachable de la carte d'enregistrement.

La carte d'enregistrement est le document attestant votre statut d'utilisateur enregistré auprès de notre société. Ceci vous donne accès à notre service d'assistance technique pendant la durée de votre souscription. De plus, les utilisateurs enregistrés qui s'abonnent au bulletin d'informations de Kaspersky Labs Ltd. sont régulièrement informés du lancement de nouveaux logiciels.

3.2. Services réservés aux utilisateurs enregistrés

Kaspersky Lab 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, fournies gratuitement ;
- Assistance téléphonique et par voie électronique sur l'installation, la configuration et l'utilisation de ce logiciel antivirus ;
- Avis de lancement des nouveaux logiciels de la société Kaspersky Lab et informations sur l'apparition de nouveaux virus dans le monde (ne bénéficient de ce dernier service que les utilisateurs ayant souscrit un abonnement au bulletin de Kaspersky Lab).

Le service d'assistance technique ne répond ni aux questions portant sur le fonctionnement et l'utilisation des systèmes d'exploitation, ni à celles sur le fonctionnement des différentes technologies.

3.3. Notations conventionnelles

Le texte de la documentation se distingue par divers éléments de mise en forme en fonction de son affectation sémantique. Le tableau ci-après illustre les conventions typographiques utilisées dans ce manuel.

Mise en forme	Fonction sémantique
Caractères gras	Nom du menu, des options du menu, des fenêtres, des éléments des boîtes de dialogue, etc.
 Remarque.	Informations complémentaires.
 Attention !	Informations auxquelles il est recommandé d'accorder une attention particulière.
 *Pour exécuter une action,* 1. Etape 1. 2. …	Description de la succession des étapes que l'utilisateur doit suivre ou des actions possibles.
 Tâche ou exemple	Formulation du problème ou exemple d'utilisation du logiciel.

CHAPITRE 4. INTERFACE DU LOGICIEL

L'interface de Kaspersky Anti-Virus est à la fois simple et conviviale. Ce chapitre est consacré à ses principaux éléments, à savoir : l'icône de la barre de tâches, le menu contextuel, la fenêtre principale et quelques boîtes de dialogue.

4.1. Icône de la barre des tâches

Dès que l'application a été lancée, une icône permettant de définir l'état de la protection antivirus apparaît dans la barre des tâches : protection en temps réel active ou analyse à la demande en cours d'exécution.

L'icône (de couleur rouge)  indique que la protection en temps réel est activée tandis que l'icône (grise)  signale que la protection en temps réel n'est pas activée.

Quand l'analyse complète de l'ordinateur, l'analyse d'un fichier ou d'un disque particulier ou l'analyse en temps réel d'un objet particulier est en cours d'exécution, l'icône clignotante  apparaît dans la barre des tâches.Lors de l'analyse du courrier entrant, l'icône  apparaît. L'icône  , quant à elle, indique l'échec du lancement d'une des tâches de la protection en temps réel

Lorsqu'un événement important au niveau de la protection antivirus survient, un message reprenant les recommandations des experts de Kaspersky Lab apparaît pendant quelques instants au-dessus de l'icône (Cette fonction n'est pas disponible sous Windows 98/NT).

4.2. Menu contextuel

Un clic-droit sur l'icône de l'application dans la barre des tâches vous permettra d'afficher un menu contextuel (cf. Illustration 1) proposant les éléments suivants :

- **Ouvrir Kaspersky Anti-Virus…** : ouvre la fenêtre principale du logiciel à l'onglet **Protection**. Vous pouvez également obtenir le même résultat en double-cliquant sur l'icône  du programme dans la barre des tâches.
- **Analyser mon Poste de travail** : lance l'analyse antivirus complète de l'ordinateur conformément au niveau de protection sélectionné.

- **Mettre à jour les bases antivirus** : procède à la mise à jour des bases antivirus.
- **Tâches exécutées** : ce point apparaît dans le menu contextuel lorsqu'une tâche programmée quelconque est en cours d'exécution . La sélection de ce point entraîne l'ouverture d'un sous-menu reprenant toutes les tâches programmées en cours d'exécution à l'instant. Pour afficher la fenêtre de l'état de la progression (cf. ill. 4), sélectionnez la tâche dans la liste.
- **A propos du logiciel** : affiche la fenêtre de renseignements comportant les informations relatives à Kaspersky Anti-Virus 5.0 for Windows Workstations.
- **Passer en mode utilisateur / Passer en mode administrateur** (uniquement sous MS Windows 98/ME) : alterne entre l'interface utilisateur et l'interface administrateur élargie. La sélection de **Passer en mode administrateur** entraîne l'apparition d'une boîte de dialogue dans laquelle il convient de saisir le mot de passe d'administrateur de la protection antivirus.

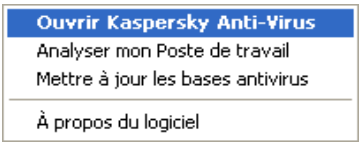

Illustration 1. Menu contextuel

4.3. Fenêtre principale du logiciel : structure générale

La fenêtre principale de Kaspersky Anti-Virus est l'élément qui permet d'exploiter toutes les possibilités de l'application en matière de protection antivirus de votre ordinateur. Vous pouvez notamment :

- Configurer la protection antivirus ;
- Télécharger les mises à jour des bases antivirus ;
- Manipuler les objets qui se trouvent en quarantaine ou dans le dossier de sauvegarde ;
- Consulter les rapports, etc.

Tous les paramètres de la protection antivirus, les informations indispensables et les tâches sont répartis entre les trois onglets suivants de la fenêtre principale :

- **Protection** : état et tâches spécifiques à la protection antivirus. Il s'agit de l'onglet principal dans l'utilisation de l'application.

- **Assistance technique** : renseignements indispensables pour réagir face à des problèmes ou pour contacter le Service d'assistance technique de Kaspersky Lab.

Chacun de ces onglets est divisé en deux parties :

- **La liste des tâches** : la partie gauche contient une liste des tâches qui interviennent dans la protection antivirus. La composition de cette liste varie en fonction de l'onglet sélectionné. Ainsi, la liste des tâches de l'onglet **Protection** reprend les tâches possibles liées à la recherche d'éventuels virus sur votre ordinateur.
- **Etat de la protection antivirus** : la partie droite de l'onglet reprend les informations relatives à l'état actuel de la protection antivirus de votre ordinateur (protection en temps réel, analyse complète et bases antivirus). L'onglet **Protection** affiche le statut de la protection antivirus.

Il existe trois états possibles, chacun étant représenté par un symbole particulier :

Niveau critique de la protection antivirus. La protection en temps réel est désactivée, certaines tâches (comme la mise à jour des bases antivirus ou l'analyse complète) n'ont plus été réalisées depuis longtemps ou la configuration sélectionnée n'assure pas le niveau de protection requis de votre ordinateur. Cette icône indique également un échec lors de l'exécution quelconque d'une tâche liée à la protection antivirus.

Le niveau de la protection antivirus ne correspond pas au niveau recommandé. L'utilisateur a configuré lui-même la protection antivirus et elle diffère de celle recommandée par les experts de Kaspersky Lab. Cet état indique également qu'il est indisspensable d'exécuter certaines tâches particulières liées à la protection antivirus.

Le niveau de la protection antivirus est conforme aux recommandations. La configuration de la protection antivirus appliquée correspond parfaitement à celle recommandée par les experts de Kaspersky Lab.

Chacun des trois états repris ci-dessus est toujours accompagné de commentaires et de recommandations. Ainsi, lorsque le niveau de protection antivirus diffère du niveau recommandé, vous verrez apparaître un message vous invitant à adopter ce dernier car il confère une protection optimale à votre ordinateur.

4.3.1. Onglet *Protection*

C'est au départ de l'onglet **Protection** (cf. Illustration 2) que vous lancerez les tâches d'analyse de votre ordinateur ou de disques, de répertoires ou de fichiers particuliers. Vous pourrez également procéder à la mise à jour des bases antivirus. Il est possible de lancer des tâches individuelles en cliquant sur le lien correspondant dans la partie gauche.

La partie gauche de l'onglet affiche également les liens vers le dossier de quarantaine, le dossier de sauvegarde et le fichier journal :

- Quarantaine : affiche la fenêtre du dossier où se trouvent les objets suspects.
- Dossier de sauvegarde : affiche la fenêtre du dossier où se trouvent les copies de sauvegarde des objets infectés.
- Rapports : affiche le fichier journal.

La partie droite reprend l'état actuel de la *protection en temps réel*, de *l'analyse complète* et des *bases antivirus*. Les *recommandations de Kaspersky Anti-Virus* sont indissociables des niveaux critique et moyen de la protection.

Illustration 2. Onglet **Protection**

La partie droite de cet onglet reprend les informations relatives au statut de la protection antivirus et plus précisément celles relatives au nombre d'objets

analysés et au nombre de virus découverts depuis le lancement de Kaspersky Anti-Virus.

Ces informations changent en cliquant sur le lien Virus découverts lorsque des objets infectés ou suspects ont été découverts pendant les tâches liées à l'analyse programmée. Ce lien vous conduira à la liste des tâches pour le traitement différés des objets (Consultez le point 5.2.5 à la page 32 pour obtenir de plus amples informations).

4.3.2. Onglet *Assistance technique*

L'onglet **Assistance technique** (cf. Illustration 3) reprend toutes les informations relatives au Service d'assistance technique. Il vous indique qui contacter en cas de problèmes de fonctionnement de Kaspersky Anti-Virus ou lorsque vous n'êtes pas en mesure de résoudre seul le problème auquel vous êtes confronté. Il affiche également toutes les informations sur le logiciel, la clé de licence et le système d'exploitation installé sur votre ordinateur. Tous ces renseignements figurent dans la partie droite.

La partie gauche de l'onglet contient les liens suivants :

- Service d'assistance technique : pour envoyer au Service d'assistance technique des questions liées à l'utilisation de Kaspersky Anti-Virus.
- Envoi d'un fichier suspect : envoi d'un message à Kaspersky Lab avec l'objet suspect en vue d'un examen.
- Aides-nous à améliorer notre produit ! : envoi d'un message au service d'assistance technique via l'interface automatisée de traitement des requêtes des clients. Ce lien vous emmène vers un formulaire de collecte des commentaires.

La partie gauche reprend également des liens vers des rubriques d'aide :

- Le lien Manuel ouvre des fenêtres d'aide générale sur l'utilisation du logiciel.
- Le lien Aide ouvre les fichiers d'aide sur l'exécution des tâches et la résolution des problèmes.
- Le lien Encyclopédie des virus vous emmène sur le site www.viruslist.com qui contient une description détaillée de tous les programmes malicieux connus à ce jour.
- Le lien Site Web de Kaspersky Lab vous conduira sur le site Internet de Kaspersky Lab.

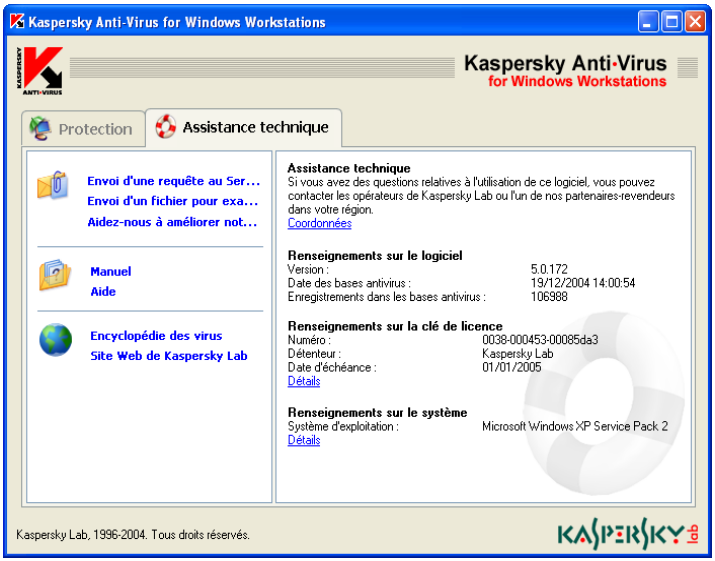

Illustration 3. Onglet **Assistance technique**

4.4. Fenêtre du processus d'analyse

La fenêtre du processus d'analyse (cf. ill. 4) apparaît dès le lancement de l'analyse complète de l'ordinateur ou de l'un de ses disques, fichiers ou répertoires.

La fenêtre est constituée de deux parties :

- La partie supérieure contient une barre d'état qui indique la progression de l'analyse. Elle reprend également l'heure du début et l'heure estimée de fin ainsi que le nom du fichier en cours d'analyse.
- La partie inférieure renferme trois onglets : **Statistiques**, pour les résultats statistiques de l'analyse ; **Rapport** pour le rapport des événements survenus lors de l'analyse ; **Paramètres** pour une description de la configuration appliquée à cette analyse.

Le lien Quarantaine vous conduira directement dans le répertoire de quarantaine (cf. point 5.4.1.1, p. 36).

Cliquez sur Exporter le rapport dans le fichier si vous souhaitez conserver le rapport dans un fichier au format texte. Dans la fenêtre standard de Windows, définissez le nom du fichier, sélectionnez le répertoire de sauvegarde et cliquez sur **Enregistrer.**

En cas de découverte d'objets infectés ou suspects dont le traitement a été différé, le lien Virus découverts vous conduira à la boîte de dialogue d'administration des objets infectés (cf. point 5.2.5, p. 32).

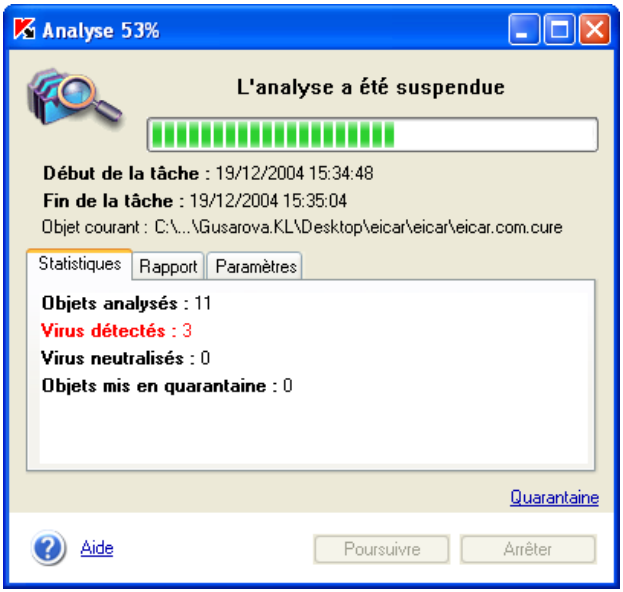

Illustration 4. Fenêtre du processus d'analyse

4.5. Aide

Toutes les rubriques d'aide du logiciel sont accessibles via l'onglet **Assistance technique**. Il suffit de cliquer sur le lien Manuel repris dans la colonne de gauche.

Si vous désirez savoir comment réaliser une tâche particulière, cliquez sur le lien Aide dans la fenêtre principale de Kaspersky Anti-Virus. Vous pourrez y lire une description détaillée des principales tâches de protection antivirus exécutées par Kaspersky Anti-Virus for Windows Workstations, ainsi que les réponses aux questions les plus souvent posées.

Si votre question porte sur une boîte de dialogue en particulier, enfoncez la touche **<F1>** ou cliquez sur le lien Aide dans le coin inférieur gauche de la boîte de dialogue en question.

CHAPITRE 5. UTILISATION DU PROGRAMME

5.1. Téléchargement des mises à jour

Kaspersky Lab offre à ses utilisateurs la possibilité de mettre à jour les bases antivirus utilisées par Kaspersky Anti-Virus pour identifier les virus et réparer les objets infectés.

La mise à jour des bases antivirus est la garantie de la sécurité de votre ordinateur. Des centaines de nouveaux virus voient le jour chaque jour et les experts de Kaspersky Lab actualisent quotidiennement le contenu des bases antivirus. Il est recommandé de réaliser la mise à jour des bases antivirus toutes les heures.

Kaspersky Anti-Virus va chercher les mises à jour sur n'importe lequel *des serveurs de mises à jour de Kaspersky Lab* en ligne.

Le téléchargement de la mise à jour s'opère soit automatiquement selon l'horaire défini par l'installation ou par l'administrateur ou soit manuellement. Kaspersky Anti-Virus copie les bases de mise à jour depuis le serveur sur l'ordinateur avant de les installer.

5.1.1. Nécessité de la mise à jour

Le logiciel vous prévient lorsqu'il est temps de procéder à la mise à jour. Vous pouvez également vous rendre compte par vous-même de la nécessité d'une mise à jour en lisant une description de l'état des bases antivirus dans la partie droite de l'onglet **Protection** (cf. Illustration 2).

L'état des bases de données est indiqué par l'une des trois icônes suivantes :

 – La mise à jour des bases antivirus n'est pas nécessaire ou est en cours d'exécution ;

 – La mise à jour des bases antivirus est nécessaire. Si cette mise à jour est impossible en raison de la fin de validité de la licence, le logiciel

affichera les informations sur la marche à suivre pour renouveler la licence.

 – La mise à jour des bases antivirus est urgente car elles sont soit très dépassées, soit manquantes.

5.1.2. Téléchargement des mises à jour

Afin de lancer manuellement la mise à jour :

Cliquez sur le lien Mettre à jour maintenant dans la partie gauche de l'onglet **Protection** ;

Ou :

Cliquez sur le lien Mettre à jour les bases antivirus dans le texte décrivant l'état des bases antivirus dans la partie droite de l'onglet **Protection** ;

Ou :

Sélectionnez le point **Mettre à jour les bases antivirus** dans le menu contextuel qui apparaît suite au clic-droit sur l'icône du programme dans la barre des tâches.

En cliquant sur le lien, vous entraînez l'ouverture d'une fenêtre (cf. ill. 5) reprenant des renseignements sur l'exécution de la mise à jour des bases antivirus et des modules de l'application.

Le téléchargement des mises à jour est un processus qui peut être décomposé de la manière suivante :

1. Le serveur des mises à jour de Kaspersky Lab envoie au logiciel la liste des mises à jour et leur taille respective.
2. Ensuite, le logiciel compare l'état des bases antivirus aux informations fournies par le serveur. Si les bases antivirus installées sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran.
3. Le champ **Taille de la mise à jour** de la fenêtre **Mise à jour** (cf. ill. 5) reprend la taille totale des mises à jour des bases antivirus indispensables. Si la mise à jour n'est pas nécessaire, la procédure s'arrêtera. Dans le cas contraire, les fichiers sont copiés depuis les serveurs de mises à jour de Kaspersky Lab via Internet. Une barre d'état montre la progression de la copie. Le champ **Téléchargement** reprend la quantité de données (en Ko) déjà

copiées. Une fois le téléchargement terminé, les bases antivirus sont installées automatiquement sur votre ordinateur.

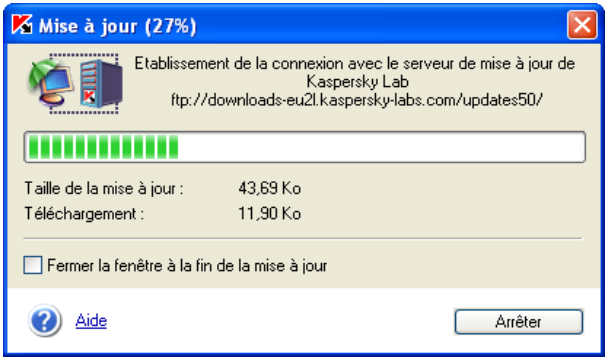

Illustration 5. Mise à jour des bases antivirus et des composants du logiciel

5.2. Prévention des infections de votre ordinateur

Il n'existe aucune mesure fiable et raisonnable qui puisse réduire à zéro le risque d'infection de votre ordinateur par des virus ou des chevaux de Troie. Toutefois, vous pouvez réduire considérablement ce risque en suivant un certain nombre de règles.

Tout comme en médecine, la *prévention* est une des méthodes de base à appliquer pour lutter contre les virus. La prévention informatique repose sur un nombre restreint de règles dont le respect réduira fortement le risque d'infection par un virus et le danger de perdre des données quelconques.

Vous trouverez ci-après des règles de base en matière de sécurité informatique qui vous permettront d'éviter les attaques de virus.

Règle N°1 : Protégez votre ordinateur à l'aide d'un antivirus et de logiciels assurant la sécurité de l'utilisation d'Internet. Pour ce faire :

- Installez absolument Kaspersky Anti-Virus.
- Procédez à la mise à jour quotidienne des bases antivirus. Réalisez cette opération plusieurs fois par jour en cas d'épidémie (les bases antivirus sont actualisées immédiatement dans ce genre de situation).
- Il est conseillé également d'installer Kaspersky Anti-Hacker pour protéger votre ordinateur lorsqu'il est connecté à Internet.

Règle N°2 : Soyez prudent lors de l'enregistrement de nouvelles données sur l'ordinateur :

- Recherchez la présence d'éventuels virus sur tous les disques amovibles (disquettes, CD, cartes Flash, etc.) avant de les utiliser.
- Traitez les courriers électroniques avec prudence. N'ouvrez jamais les fichiers que vous recevez par courrier électronique si vous n'êtes pas certain qu'ils vous sont bel et bien destinés, même s'ils ont été envoyés par vos connaissances. Soyez particulièrement méfiant à l'encontre des messages envoyés par de prétendus éditeurs d'antivirus.
- Soyez attentif aux données reçues depuis Internet. Si un site Internet vous invite à installer une nouvelle application, veillez à vérifier son certificat de sécurité.
- Lorsque vous copiez un fichier exécutable depuis Internet ou depuis un répertoire local, analysez-le avec Kaspersky Anti-Virus avant de l'ouvrir.
- Soyez prudent dans le choix des sites que vous visitez. En effet, certains sites sont infectés par des virus de script dangereux ou par des vers Internet.

Règle N°3 : *Suivez attentivement les informations diffusées par Kaspersky Lab*.

Généralement, Kaspersky Lab avertit ses utilisateurs de l'existence d'une nouvelle épidémie bien longtemps avant qu'elle n'atteigne son pic. A ce moment, le risque d'infection est encore faible et le téléchargement des bases de virus actualisées en temps opportun vous permettra de vous protéger.

Règle N°4 : *Evitez de croire les canulars présentés sous la forme d'un message évoquant* un risque d'infection.

Règle N°5 : *Utilisez Windows Update et installez régulièrement les mises à jour du système d'application Windows*.

Règle N°6 : *Achetez les copies d'installation des logiciels auprès de vendeurs agréés.*

Règle N°7 : *Limitez le nombre de personnes autorisées à utiliser votre ordinateur.*

5.2.1. Quand faut-il lancer la recherche d'éventuels virus sur l'ordinateur ou dans des objets individuels ?

Grâce à Kaspersky Anti-Virus, vous pouvez réaliser soit une analyse de tout l'ordinateur ou soit une analyse d'objets distincts comme des disques, des fichiers ou des répertoires particuliers.

La non découverte de virus suite à l'analyse ponctuelle d'un élément ne signifie pas que votre ordinateur est sain. Pour cette raison, Kaspersky Anti-Virus veille particulièrement à ce que les analyses porte sur tout l'ordinateur.

L'analyse complète est capable d'analyser un nombre bien plus élevé d'objets que la protection en temps réel. Il est donc conseillé de l'effectuer au moins une fois par semaine à titre préventif. Le logiciel vous avertira lorsqu'il est indispensable de lancer cette analyse. Au cas où la fenêtre principale du logiciel serait fermée, un message vous invitant à lancer immédiatement l'analyse complète de l'ordinateur apparaîtra au-dessus de l'icône  de Kaspersky Anti-Virus dans la barre des tâches.

Pour obtenir de plus amples informations, il suffira d'ouvrir la fenêtre principale de l'application et de sélectionner l'onglet **Protection** (cf. Illustration 2). La partie droite reprend l'état exact de l'analyse complète. Il existe trois états possible :

 - Vous devez réaliser sans plus attendre l'analyse complète de votre ordinateur.

 - Il est temps de procéder à l'analyse complète, non sans avoir au préalable rétabli la configuration recommandée par les experts de Kaspersky Lab.

 - L'analyse complète a été réalisée dans les temps ou est en cours d'exécution.

Le cas échéant, vous pouvez lancer directement l'analyse complète en cliquant sur procéder à l'analyse complète.

5.2.2. Analyse complète manuelle

Pour lancer l'analyse antivirus complète de l'ordinateur :

Cliquez sur le lien Analyser le Poste de Travail dans la partie gauche de l'onglet **Protection** (cf. Illustration 2). Le même résultat s'obtient en cliquant sur le lien procéder à l'analyse complète dans la partie droite de l'onglet **Protection** ou en sélectionnant le point **Analyser mon Poste de travail** dans le menu contextuel qui apparaît après avoir fait un clic-droit sur l'icône  dans la barre des tâches.

La fenêtre **Analyse** (cf. ill. 4) apparaît à l'écran. Elle reprend la progression en pour cent de la tâche, l'heure de début, l'heure de fin prévue ou définitive ainsi que le nom de l'objet analysé.

Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 5.4.2 à la page 39).

5.2.3. Analyse de fichiers ou de répertoires sélectionnés

Il arrive parfois que vous deviez absolument rechercher la présence d'éventuels virus non pas dans tout l'ordinateur mais uniquement dans un objet particulier comme l'un des disques durs où sont enregistrés les logiciels et les jeux, une base de données de messagerie ramenée de l'ordinateur de votre bureau, une archive envoyée par courrier électronique, etc. Vous pouvez sélectionner l'objet à analyser au départ de Kaspersky Anti-Virus ou à l'aide des méthodes traditionnelles du système d'exploitation Windows (via l'**Assistant** ou sur le **Bureau**, etc.)

Pour analyser l'objet sélectionné au départ de Windows :

Placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 6).

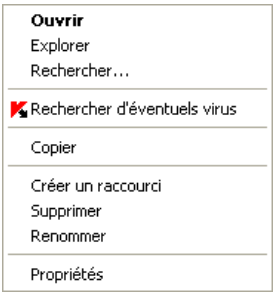

Illustration 6. Recherche d'éventuels virus dans un objet sélectionné au départ de Windows

N'oubliez pas de lancer Kaspersky Anti-Virus avant de lancer l'analyse d'un objet au départ de Windows !

*Afin de lancer l'analyse de l'ordinateur ou d'un objet particulier, rendez-vous dans l'onglet **Protection** et sélectionnez dans la partie gauche :*

- Analyser les disques amovibles : lance l'analyse des disques amovibles.
- Analyser les objets : sélectionnez l'objet (fichier, répertoire, disque) et lancez son analyse. La boîte de dialogue **Sélection des objets à analyser** (cf. ill. 7) qui apparaît reprend une liste des objets qui peuvent

être analysés, ainsi qu'un bouton de modification du contenu de la liste et un bouton de gestion de l'analyse.

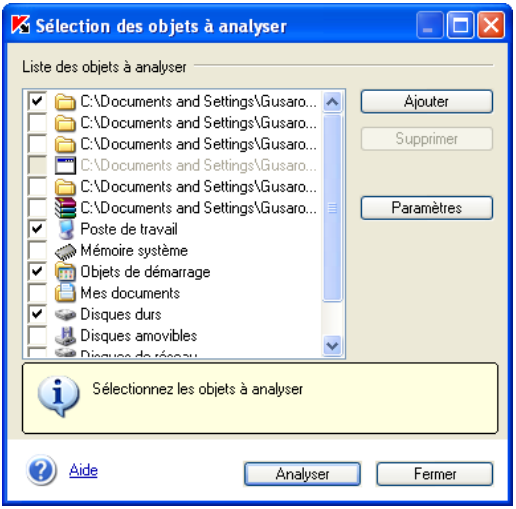

Illustration 7. Sélection des objets à analyser

Cliquez sur **Ajouter** pour ajouter de nouveaux objets à la liste et sélectionnez-le dossier ou le fichier souhaité. Tous les objets que vous aurez ajoutés à la liste seront préservés jusqu'à la prochaine analyse.

Pour effacer un objet de la liste, cochez la case ☑ qui se trouve à côté de son nom et cliquez sur **Supprimer**. Sachez cependant que vous ne pouvez supprimer que les objets que vous aurez ajoutés manuellement. Les objets présents dans la liste d'origine ne peuvent être supprimés.

Pour analyser simultanément plusieurs objets de la liste :

1. Cochez la case à la gauche des objets à analyser ;
2. Cliquez sur **Analyser**.

Quel que soit le moyen utilisé pour lancer l'analyse d'un objet (via le menu contextuel de Windows ou au départ de la liste des objets de Kaspersky Anti-Virus), la boîte de dialogue **Analyse** (cf. ill. 4) apparaît à l'écran. Cette boîte reprend l'état d'avancement de la tâche en pour cent, l'heure de début, l'heure de fin prévue ou définitive ainsi que le nom de l'objet analysé.

Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 5.4.2 à la page 39).

5.2.4. Analyse des archives

Kaspersky Anti-Virus analyse uniquement les archives lorsque le niveau **Sécurité maximale** ou **Recommandé** a été sélectionné et pour autant qu'aucune exclusion ait été définie (pour de plus amples informations, contactez votre administrateur de système).

Sachez que Kaspersky Anti-Virus® ne répare pas les archives multivolume. En cas de découverte d'un tel objet, l'écran affichera un message avec l'action recommandée **Ignorer**.

Au cas où l'archive serait protégée, une boîte de saisie du mot de passe (cf. Illustration 8) apparaîtra avant l'analyse des objets contenus dans l'archive.

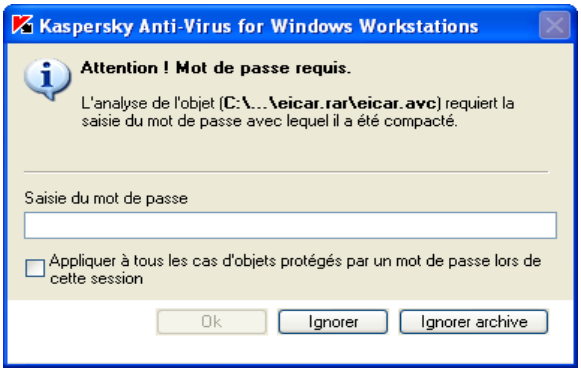

Illustration 8. Saisie du mot de passe pour l'analyse de l'archive

Saisissez dans le champ **Saisie du mot de passe** le mot de passe d'accès aux objets renfermés dans l'archive analysée puis cliquez sur **OK**. L'analyse antivirus de l'archive et des objets qu'elle contient se poursuivra.

Si Kaspersky Anti-Virus découvre pendant l'analyse une autre archive protégée, il tentera d'utiliser le mot de passe saisi pour l'analyse des objets de la première archive. La boîte de dialogue de saisie du mot de passe apparaîtra à nouveau à l'écran uniquement si ce premier mot de passe n'est pas valide.

Si vous ne connaissez pas le mot de passe, il sera impossible de procéder à l'analyse des objets repris dans l'archive protégée. Il est recommandé dans ce cas de cliquer sur **Ignorer** et de poursuivre.

Cliquez sur **Ignorer archive** afin d'exclure de l'analyse en cours tous les objets protégés par un mot de passe et repris dans l'archive analysée. Dans ce cas, tous les objets à l'intérieur de l'archive qui ne sont pas protégés par un mot de passe seront analysés et traités conformément aux paramètres de l'analyse antivirus.

Appliquer à tous les cas d'objets protégés par un mot de passe lors de cette session : applique l'action sélectionnée à tous les objets protégés par un mot de passe au sein de l'archive et découverts lors de la session en cours.
Ainsi, si vous cochez cette case et que vous aviez choisi **Ignorer**, **Ignorer archive**, les objets restants protégés par un mot de passe ne seront pas analysés. Par contre, si vous aviez saisi un mot de passe et cliquez sur **OK**, ce mot de passe sera appliqué à tous les objets restants sans que la boîte de saisie n'apparaisse.

5.2.5. Traitement des objets écartés

Le besoin de gérer les objets infectés fait surface lorsque l'option *Confirmer l'action auprès de l'utilisateur à la fin de l'analyse* a été sélectionnée par l'administrateur et que des objets infectés ou suspects ont été décelés.

Suite à la fin ou à l'interruption de l'analyse, la boîte de dialogue **Gestion des objets infectés** (cf. Illustration 10) apparaîtra et vous permettra de sélectionner les actions à exécuter sur ces objets. Il est possible également d'afficher cette fenêtre directement depuis la fenêtre d'analyse (cf. ill. 4) en cliquant sur le lien Virus découverts.

En cas de découverte de quelques objets infectés ou suspects à la fin de l'analyse programmée exécutée en arrière-plan, la liste des tâches accessibles apparaîtra dans la boîte de dialogue ouverte (cf. Illustration 9) grâce au lien Virus découverts dans la partie droite de l'onglet **Protection**. Pour consulter les objets et procéder au traitement différé, sélectionnez la tâche dans la lise et cliquez sur **Objets…**

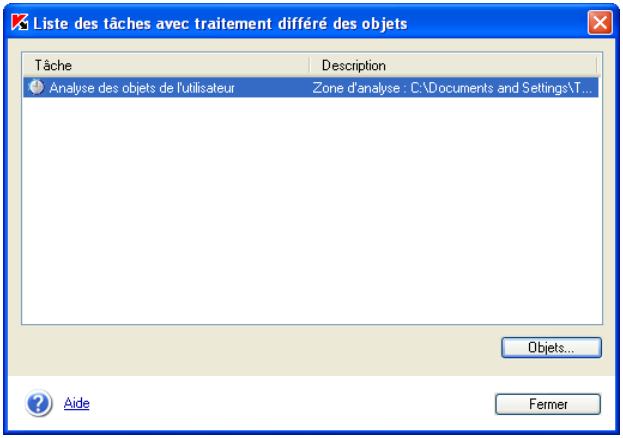

Illustration 9. Liste des tâches liées au traitement différé des objets

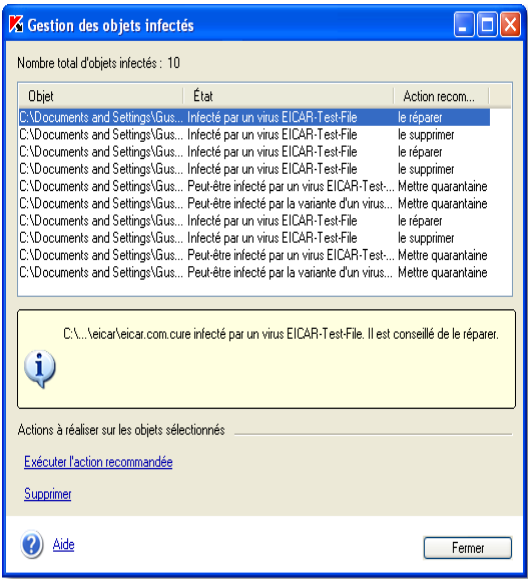

Illustration 10. Fenêtre d'administration des objets infectés et suspects

Nous attirons votre attention sur le fait les fichiers protégés par un mot de passe dans les archives NE SONT NI ANALYSES NI REPARES lorsque le mode de traitement différés des objets a été sélectionné.

Le tableau reprend la liste des les objets infectés ou suspects découverts pendant l'analyse (cf. Illustration 10). La colonne **Objet** contient le nom de l'objet et le chemin d'accès. La colonne **Etat** vous renseigne sur l'état de l'objet tandis que la colonne **Action recommandée** reprend l'action recommandée pour l'objet par les experts de Kaspersky Lab.

Afin de sélectionner l'objet et d'exécuter une action quelconque, cochez la case correspondante. Vous pouvez sélectionner simultanément plusieurs objets dans la liste. Afin de sélectionner tous les objets, cochez la case dans l'en-tête de la colonne.

Vous pouvez exécuter l'une des actions suivantes sur n'importe quel des objets de la liste.

- Exécuter l'action recommandée : exécute l'action recommandée par les experts de Kaspersky Lab. Pour les objets infectés, les actions proposées sont **réparer** ou **supprimer**. Pour les objets suspects, il s'agit de **mettre en quarantaine**.
- Supprimer : supprime l'objet.

Dès que vous aurez lancé n'importe quelle action, une fenêtre affichant la progression de la tâche pour les objets sélectionnés apparaîtra. Vous pouvez interrompre le traitement en cliquant sur **Arrêter**.

Une fois que les objets ont été traités en fonction de l'action sélectionnée, ils disparaissent de la liste.

Les objets traités sont retirés de la liste. Cliquez sur **Fermer** lorsque tous les objets repris dans la liste auront été traités.

5.2.6. Analyse d'un CD-ROM ou d'une disquette

Votre ordinateur peut facilement être infecté par un virus introduit par une disquette, un CD ou un autre disque amovible. Si la disquette (ou le CD-Rom) est infectée par un virus d'amorçage et que vous l'avez introduite dans le lecteur avant de redémarrer, les résultats pourraient être catastrophiques.

Il est vivement conseillé d'analyser tous les disques amovibles avant de les utiliser.

Vous pouvez lancer l'analyse des disques amovibles depuis la fenêtre principale de Kaspersky Anti-Virus ou depuis le menu contextuel de Windows ouvert via l'**Assistant** ou le **Bureau.**

Pour analyser les disques amovibles au départ du menu contextuel de Windows :

1. Introduisez le CD ou la disquette dans le lecteur
2. Sélectionnez les disques (il est possible de sélectionner directement le CD et la disquette), ouvrez le menu contextuel de Windows d'un clic droit et choisissez **Rechercher d'éventuels virus** (cf. ill. 6).

Pour rechercher d'éventuels virus sur le CD ou la disquette au départ de la fenêtre principale de Kaspersky Anti-Virus :

- Introduisez le CD ou la disquette dans le lecteur. Le logiciel est en mesure d'analyser le CD et la disquette en une session.
- Cliquez sur le lien Analyser les disques amovibles dans la partie gauche de l'onglet **Protection** (cf. Illustration 2).

La fenêtre **Analyse** (cf. Ill .4) apparaît à l'écran dès le lancement de l'analyse et illustre la progression de la tâche pour les objets sélectionnés dans la liste.

Voici quelques caractéristiques du fonctionnement du logiciel auxquelles il convient de prêter attention.

- Si au moment de lancer l'analyse vous avez oublié d'introduire le disque ou la disquette ou si le lecteur ou le CD-ROM n'est pas branché, l'analyse n'aura pas lieu et le logiciel n'affichera aucun message à ce sujet.
- Les disquettes introduites dans le lecteur après le début de l'analyse ne seront pas analysées. Il en va de même pour les CD-ROM et les autres types de disques amovibles
- Si vous éjectez la disquette ou éteignez le disque amovible pendant l'analyse, le logiciel consignera l'erreur dans le rapport mais il n'affichera aucun message à ce sujet. Le logiciel passera, le cas échéant, à l'analyse du disque amovible suivant.

5.3. Protection en temps réel de l'ordinateur

En mode *protection en temps réel*, Kaspersky Anti-Virus se trouve en permanence dans la mémoire vive et contrôle toutes les requêtes vers les objets du système de fichiers ainsi que les scripts VBScript et JavaScript et les macros utilisées dans les applications bureautiques. Il identifie également les riskwares.

Avant d'autoriser l'accès à l'objet, l'application vérifie que l'objet est exempt de virus. Si elle en détecte un, elle propose soit de réparer l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction des paramètres définis). Ainsi, l'application permet de détecter et d'éradiquer les codes malicieux avant que le système soit réellement infecté.

La protection en temps réel est activée par défaut depuis le démarrage du système d'exploitation jusqu'au moment où vous éteignez l'ordinateur.

Toutes les informations relatives à l'état de la protection en temps réel sont reprises sur le panneau de droite de l'onglet **Protection** (cf. Illustration 2) de la fenêtre principale de Kaspersky Anti-Virus.

L'état peut être caractérisé par l'un des symboles suivants :

 – La protection en temps réel est activée et la configuration correspond à celle recommandée ;

 – La protection en temps réel est activée et la configuration ne correspond pas à celle recommandée ;

 – La protection en temps réel est désactivée ou ne fonctionne pas.

Pour confirmer la désactivation de la protection en temps réel, l'icône  (de couleur rouge) est remplacée par l'icône  (de couleur grise).

5.4. Possibilités complémentaires

Kaspersky Anti-Virus propose toute une série de possibilités supplémentaires au niveau de la configuration et de l'utilisation telles que :

- La manipulation des objets suspects placés en quarantaine ;
- La manipulation des copies des objets supprimés ou modifiés par Kaspersky Anti-Virus et placées dans le dossier de sauvegarde ;
- Consultation du rapport sur l'activité du logiciel.

5.4.1. Quarantaine et dossier de sauvegarde

Kaspersky Anti-Virus permet d'isoler les objets suspects en quarantaine et de conserver une copie des objets infectés dans un dossier de sauvegarde avant de les réparer ou de les supprimer.

En cas de découverte d'un objet suspect, l'application l'isole dans le répertoire de quarantaine. Là, il pourra être à nouveau analysé, supprimé, restauré ou envoyé à Kaspersky Lab pour analyse.

La copie de sauvegarde est créée lors de la première suppression ou réparation après la découverte de l'objet. Elle est placée dans le dossier de sauvegarde. L'objet pourra être restauré s'il renferme des informations capitales.

5.4.1.1. Utilisation de la quarantaine

Par défaut, tous les objets suspects découverts pendant l'analyse antivirus ou interceptés par la protection en temps réel sont mis en quarantaine par Kaspersky Anti-Virus. Vous pouvez continuer à manipuler ces fichiers une fois qu'ils sont en quarantaine (analyse, restauration, suppression, etc.)

Après chaque mise à jour des bases antivirus, Kaspersky Anti-Virus® analyse les objets qui se trouvent en quarantaine. Au cas où l'analyse manuel des fichiers en quarantaine serait indispensable, nous vous conseillons de mettre les

bases antivirus à jour. Il se peut en effet que ces nouvelles bases contiennent les définitions des virus qui auraient infecté les fichiers, ce qui permettrait leur réparation.

Le traitement des objets suspects s'opère dans la fenêtre **Quarantaine** (cf. Illustration 11) accessible en cliquant sur le lien Quarantaine de l'onglet **Protection** (cf. Illustration 2) ou sur le lien du même nom dans la boîte de dialogue d'analyse (cf. ill. 4).

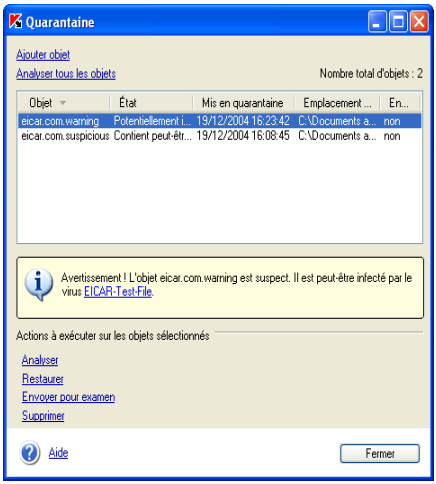

Illustration 11. Fenêtre des objets mis la quarantaine

Vous pouvez réaliser les opérations suivantes au départ de cette boîte de dialogue :

- Mettre en quarantaine un fichier que vous croyez être infecté par un virus et qui n'aurait pas été découvert par Kaspersky Anti-Virus. Pour ce faire, cliquez sur Ajouter objet et sélectionnez l'objet suspect dans la boîte de dialogue. Il sera ajouté à la liste. Il sera transféré de son emplacement d'origine vers la liste.
- Analyser et réparer à l'aide des dernières bases antivirus tous les objets suspects ou uniquement certains d'entre eux. Pour ce faire, cliquez sur Analyser tous les objets ou Analyser (après avoir sélectionné les objets à analyser).
  L'état de chaque objet en quarantaine après l'analyse et la réparation peut être soit *infecté, réparé* ou *fausse alerte*.
  L'état *infecté* signifie que l'objet est bien infecté mais qu'il n'a pas pu être réparé. Il est recommandé de supprimer de tels objets.
  Tous les objets dont l'état est qualifié de *fausse alerte* peuvent être

restaurés sans crainte car leur état antérieur, à savoir *suspect*, avait été erronément attribué par Kaspersky Anti-Virus.

Par défaut, les fichiers en quarantaine sont analysés automatiquement après chaque mise à jour des bases antivirus.

- Restaurer les fichiers dans leur répertoire d'origine, là où ils se trouvaient avant d'être mis en quarantaine ou bien dans le répertoire de restauration (en fonction des paramètres définis par l'administrateur). Pour restaurer un objet, sélectionnez-le dans la liste et cliquez sur Restaurer.

Nous vous conseillons de restaurer uniquement les objets dont l'état correspond à une *fausse alerte*. La restauration d'autres types d'objets pourrait entraîner l'infection de votre ordinateur !

- Envoyer les objets suspects aux experts de Kaspersky Lab en vue d'un examen. Veuillez envoyer ces objets uniquement si l'état de l'objet suspect ne change pas en dépit d'analyses et de tentatives de réparation répétées. Pour ce faire, cliquez sur Envoyer pour examen.
- Supprimer n'importe quel fichier ou groupe de fichiers de la quarantaine. Supprimez uniquement les fichiers qui ne peuvent être réparés. Pour supprimer un fichier, sélectionnez-le dans la liste puis cliquez sur Supprimer.

5.4.1.2. Utilisation du dossier de sauvegarde

Avant la réparation ou la suppression d'un objet infecté ou suspect, Kaspersky Anti-Virus crée une copie de celui-ci dans le dossier de sauvegarde.

Le cas échéant, vous pourrez restaurer n'importe lequel de ces objets par exemple si des données ont été perdues pendant la réparation, si l'objet a été supprimé par accident ou si vous souhaitez essayer de le réparer une fois de plus à l'aide des bases antivirus actualisées.

Les manipulations sur les copies de sauvegarde sont réalisées dans la fenêtre **Dossier de sauvegarde** (cf. Illustration 12) qui apparaît en cliquant sur Dossier de sauvegarde dans l'onglet **Protection** (cf. Illustration 2) de la fenêtre principale de l'application.

Vous pouvez réaliser les opérations suivantes dans le dossier de sauvegarde :

- Restaurer les objets dans leur répertoire d'origine, là où ils se trouvaient avant d'être mis dans le dossier de sauvegarde ou dans le dossier de restauration (en fonction des paramètres définis par l'administrateur). Pour restaurer un objet, sélectionnez-le dans la liste et cliquez sur Restaurer.

- Supprimer n'importe quel fichier ou groupe de fichiers du dossier de sauvegarde. Pour supprimer un fichier, sélectionnez-le dans la liste puis cliquez sur Supprimer.

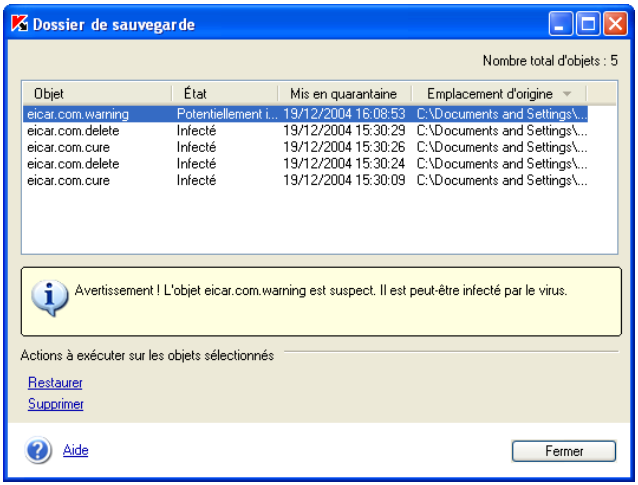

Illustration 12. Fenêtre du dossier de sauvegarde

5.4.2. Utilisation des rapports

Des rapports sont constitués lors de l'analyse complète de l'ordinateur, lors de la mise à jour des bases antivirus ainsi que pendant la protection en temps réel. Ces rapports fournissent des indications sur les objets analysés et le résultat de leur traitement ainsi que des statistiques d'ordre général.

Kaspersky Anti-Virus tient une liste de toutes les actions exécutées dans le journal des tâches (cf. Illustration 13). Pour ouvrir ce journal, cliquez sur le lien Rapports dans la partie gauche de l'onglet **Protection** (cf. Illustration 2). Le rapport reprend l'état de chaque tâche, ainsi que la date et l'heure de la fin d'exécution.

Les informations relatives au traitement d'un objet peuvent être de cinq types :

- *Message sur la réussite* (ex. : l'objet est sain, l'objet a été réparé ou a été supprimé).
- ou *Message d'information* (ex. :la tâche a été lancée, la tâche est terminée, la tâche est en cours d'exécution, la tâche a été interrompue.
- *Avertissement* (ex : un objet suspect ou une archive protégée par un mot de passe a été découvert).

Evénement critique (ex. : découverte d'un virus) ou *Refus de fonctionnement* (ex. : la licence n'est plus valide).

En règle générale, les messages confirmant la réussite d'une opération ou de simples informations sont fournis à titre purement informatif et n'ont aucune importance critique. Vous pouvez décider de ne pas afficher dans les rapports ces messages à caractère purement informatif. Pour ce faire, désélectionnez la case **Afficher les rapports informatifs**.

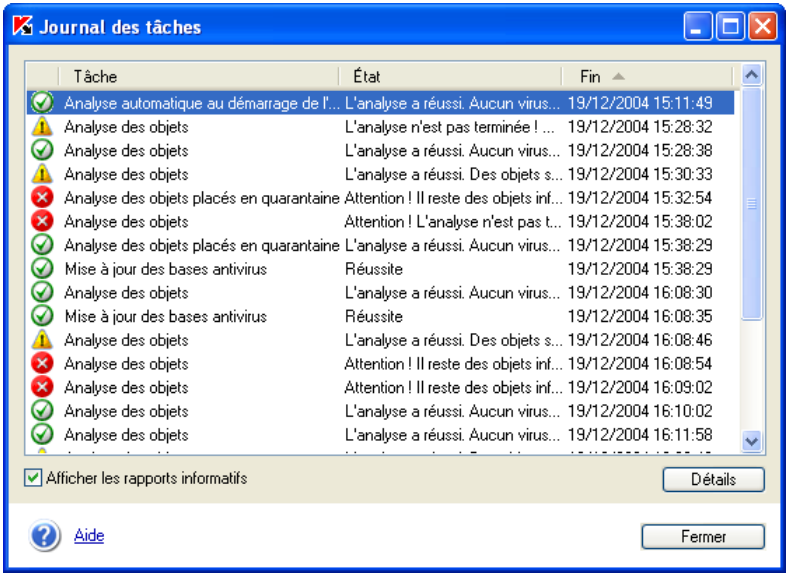

Illustration 13. Journal des tâches

Il est possible, pour n'importe quelle tâche reprise dans le journal, d'étudier ses paramètres, ses statistiques et de consulter le rapport sur les objets découverts. Il suffit simplement de cliquer sur **Détails**.

Les onglets **Statistiques**, **Rapports** et **Paramètres** de la fenêtre qui s'affiche vous fourniront tous les détails demandés.

Ainsi, l'onglet **Statistiques** (cf. Illustration 14) reprend les informations générales sur le travail exécuté par Kaspersky Anti-Virus dans le cadre de cette tâche : date et heure de lancement, nombre d'objets analysés, nombre d'objets infectés et réparés ainsi que le nombre d'objets mis en quarantaine.

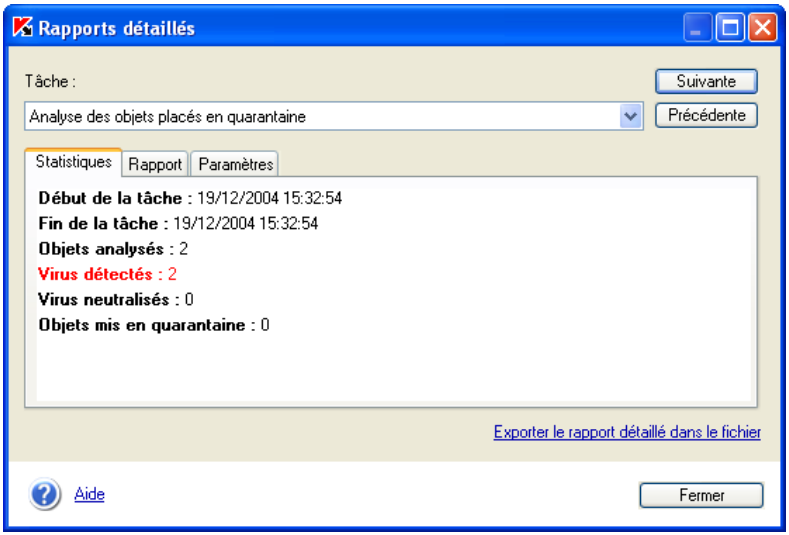

Illustration 14. Onglet **Statistiques**

L'onglet **Rapport** (cf. Illustration 15) contient des renseignements détaillés sur chacun des objets analysés.

L'onglet **Paramètres** (cf. ill. 16) reprend les paramètres utilisés pour l'exécution des différentes tâches. Il reprend notamment la zone d'analyse et le niveau de protection définis pour cette tâche, les actions exécutées sur les fichiers infectés et suspects. On y retrouve également, le cas échéant, les exclusions définies.

Pour passer d'une tâche à l'autre dans le journal ou dans le rapport détaillé, vous pouvez utiliser les boutons **Suivant** et **Précédent** ou sélectionnez le nom de la tâche dans la liste déroulante.

Vous pouvez également obtenir le rapport sous la forme d'un fichier texte. Pour ce faire, cliquez sur Exporter le rapport dans le fichier. Dans la fenêtre Windows, saisissez le nom du fichier, l'emplacement pour le sauvegarder puis cliquez sur **Enregistrer**.

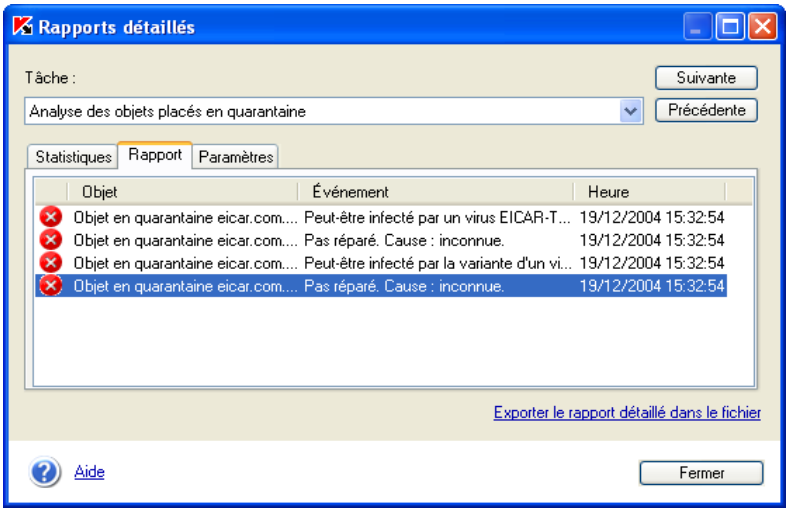

Illustration 15. Onglet **Rapports**

Illustration 16. Onglet **Paramètres**

ANNEXE A. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquemment posées par les utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Anti-Virus. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : l'utilisation simultanée de Kaspersky Anti-Virus avec des logiciels antivirus d'autres éditeurs est-elle possible ?

Afin d'éviter tout risque de conflit, nous vous conseillons de supprimer les logiciels antivirus d'éditeurs tiers avant d'installer Kaspersky Anti-Virus.

Question : Kaspersky Anti-Virus n'analyse pas le fichier une deuxième fois. Pourquoi ?

En effet, Kaspersky Anti-Virus ne procèdera pas à une nouvelle analyse d'un fichier si ce dernier n'a pas été modifié depuis la dernière analyse.

Et cela, grâce aux nouvelles technologies iChecker et iStreams. Ces technologies reposent sur l'utilisation d'une base de données des sommes de contrôle des objets et la conservation des sommes de contrôle dans les flux NTFS complémentaires.

Question : Pourquoi Kaspersky Anti-Virus entraîne-t-il une baisse des performances de mon ordinateur et surcharge le processeur ?

La détection des virus est avant tout une tâche mathématique liée à l'analyse de la structure, de la somme de contrôle et des données mathématiques. Pour cette raison, la principale ressource utilisée par tout logiciel antivirus est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse. C'est le prix à payer pour garantir la fiabilité et la sécurité des données.

A la différence d'autres logiciels antivirus qui réduisent la durée de l'analyse en éliminant des bases antivirus les virus les plus complexes à identifier ou les plus rares (à l'endroit où est basé l'éditeur), ainsi que les fichiers les plus difficiles à analyser (comme les fichiers PDF), Kaspersky Lab estime que la tâche attendue de tout antivirus est de garantir une véritable protection de l'utilisateur contre les virus. Il ne peut être question de protection partielle. Qui plus est, la " protection

partielle " est pire que l'absence de protection (dans ce cas au moins, l'utilisateur adopte lui-même des mesures de prévention).

Kaspersky Anti-Virus confère à l'utilisateur un sentiment de protection totale. Il va de soi que Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer la vitesse de l'analyse au détriment du niveau global de sécurité grâce à l'exclusion de toute une série de différents fichiers. Toutefois, nous ne vous conseillons pas d'agir ainsi si vous souhaitez vous sentir vraiment en sécurité.

Signe de la protection maximale qu'il assure aux utilisateurs, Kaspersky Anti-Virus reconnaît plus de 700 formats de fichiers archivés ou compressés. Ceci est très important au niveau de la sécurité antivirus car chacun des formats reconnus ci-dessus peut contenir un code malicieux exécutable. Néanmoins, il convient de remarquer que chaque nouvelle version du logiciel est plus rapide que la précédente, malgré l'augmentation quotidienne du nombre de virus identifiés par Kaspersky Anti-Virus (plus de 30 nouveaux virus chaque jour) et l'augmentation constante des formats pris en charge. Tout ceci est rendu possible grâce aux nouvelles technologies développées par Kaspersky Lab comme i-Checker™ et i-Stream™. Ces technologies permettent de rechercher d'éventuels virus dans les fichiers une seule fois, lors de la première analyse. Si ce fichier n'a pas été modifié depuis la dernière analyse, il ne sera pas repris dans l'analyse suivante. Autrement dit, les performances du logiciel antivirus sont nettement accrues après la première analyse du fichier.

Question : A quoi sert la clé de licence? Mon antivirus fonctionnera-t-il sans elle ?

Kaspersky Anti-Virus ne peut fonctionner sans la clé de licence.

Si vous n'avez pas encore décidé d'acheter Kaspersky Anti-Virus, nous pouvons vous fournir une clé d'évaluation (trial-key) qui fonctionnera deux semaines ou un mois. Passé ce délai, la clé sera bloquée.

Question : Que se passe-t-il lorsque la licence d'utilisation du logiciel arrive à échéance ?

Lorsque la licence est parvenue à échéance, Kaspersky Anti-Virus continue à fonctionner mais il n'est plus possible de procéder aux mises à jour des bases antivirus. Le programme continuera à réparer les objets infectés en utilisant les vieilles bases antivirus.

Lorsque cette situation se présente, vous devez contacter votre administrateur de système ou la société où vous avez acheté Kaspersky Anti-Virus ou Kaspersky Lab directement.

Question : Mon antivirus ne fonctionne pas.

Que puis-je faire ?

Avant tout, vérifiez si la solution de votre problème n'est pas décrite dans les pages de ce manuel, et plus particulièrement dans cette rubrique. Consultez également la rubrique d'assistance technique de notre site Internet.

Nous vous conseillons également de contacter le magasin où vous avez acheté Kaspersky Anti-Virus ou d'écrire directement au Service d'assistance technique (support@kaspersky.com) ou à l'adresse indiquées dans les informations relatives à la clé de licence.

En vue de garantir le traitement le plus rapide possible de votre demande :

1. Indiquez dans le sujet du message la version du système d'exploitation installé sur votre ordinateur, le nom du logiciel de Kaspersky Lab que vous utilisez et le problème. Par exemple : **MS Windows 2000, Kaspersky Anti-Virus 5.0 for Windows Workstation, la mise à jour des bases antivirus ne fonctionne pas**.
2. Composez votre message au format texte.
3. Mentionnez au début de votre message la version exacte du système d'exploitation, la distribution de Kaspersky Anti-Virus et le numéro de votre licence.
4. Décrivez le problème de manière claire et concise. Rappelez-vous que l'opérateur du service d'assistance technique ne sait encore rien de votre problème au moment où il reçoit votre message et qu'il pourra vous venir en aide efficacement uniquement après l'avoir compris et reproduit.
5. Envoyez au service d'assistance technique les fichiers suivants, que vous aurez préalablement archivés :
   - le fichier de rapport de Kaspersky Anti-Virus.
   - la clé de licence.
6. Ne manquez pas d'indiquer également la présence :
   - D'un contrôleur SCSI ;
   - D'un processeur très ancien ou récent, de plusieurs processeurs ;
   - D'une mémoire inférieure à 64 Mo ou supérieure à 2 Go.

Question : à quoi servent les mises à jour quotidiennes ?

Il y a encore quelques années, les virus étaient transmis via disquette et afin de protéger l'ordinateur, il suffisait d'installer un logiciel antivirus et de procéder de temps à autre à la mise à jour des bases antivirus. Les épidémies les plus récentes se sont répandues à travers le monde entier en quelques heures uniquement et dans ces conditions, un logiciel antivirus équipé d'anciennes bases antivirus est impuissant face aux nouvelles menaces. Afin de ne pas devenir victime de la prochaine épidémie de virus, il est indispensable de mettre à jour les bases antivirus quotidiennement.

Chaque année, Kaspersky Lab augmente la fréquence de mise à jour des bases antivirus. Actuellement, les mises à jour sont diffusées toutes les heures.

La mise à jour des modules de l'application est une fonction supplémentaire. Ces mises à jour corrigent les défauts et apportent de nouvelles possibilités.

Question : qu'est-ce qui a changé dans le service de mise à jour de la version 5.0 ?

La nouvelle gamme de produits de la version 5.0 offerte par Kaspersky Lab présente un nouveau service de mise à jour. Le développement de cette nouvelle fonction s'est fondé sur les remarques des utilisateurs et sur les impératifs du marketing. De plus, il fallait renforcer le degré technologique de l'ensemble de la procédure de mise à jour, depuis la préparation chez Kaspersky Lab jusque l'actualisation des fichiers chez l'utilisateur.

Voici les avantages du nouveau système de mise à jour :

- *Fin du téléchargement des fichiers en cas de déconnexion :* désormais, il n'est plus *nécessaire* de télécharger à nouveau les données obtenues avant la déconnexion.
- *Réduction de moitié de la taille de la mise à jour cumulée.* La mise à jour cumulée contient toute la base antivirus, ce qui explique pourquoi la taille de la mise à jour cumulée est de loin supérieur à la taille de la mise à jour traditionnelle. Le nouveau service introduit une nouvelle *technologie* qui permet d'utiliser les bases antivirus qui existent déjà pour la mise à jour cumulée.

- *Accélération du téléchargement depuis Internet.* Kaspersky Anti-Virus sélectionne le serveur de mise à jour situé dans votre région. De plus, la charge du serveur est répartie en fonction de ses performances. *Autrement* dit, vous ne serez pas connecté à un serveur surchargé pendant qu'un autre n'est pas sollicité.

- *Application des « listes noires » des clés.* Ceci permet d'exclure des mises à jour les utilisateurs qui ne disposent pas de la licence d'utilisation de Kaspersky Anti-Virus. *Ainsi*, les utilisateurs qui possèdent une licence ne sont pas pénalisés à cause de serveurs surchargés.

- *Les logiciels destinés aux entreprises autorisent la création d'un répertoire local pour la mise à jour des bases antivirus*. Cette fonction est prévue pour les entreprises où les ordinateurs, protégés par les *applications* de Kaspersky Lab, sont regroupés au sein d'un réseau. N'importe quel ordinateur peut jouer le rôle de serveur de mise à jour. C'est lui qui recevra les mises à jour depuis Internet. Elles seront enregistrées dans un répertoire local accessible aux autres ordinateurs du réseau.

Question : *une personne mal intentionnée pourrait-elle remplacer les bases antivirus ?*

Chaque base antivirus dispose d'une signature unique que Kaspersky Anti-Virus vérifie lorsqu'il consulte ces bases. Si la signature ne correspond pas à celle octroyée par Kaspersky Lab et que la date de la base de données est postérieure à la date d'expiration de la licence, Kaspersky Anti-Virus n'utilisera pas cette base.

Question : comment configurer la mise à jour pour un ordinateur via Internet afin qu'il devienne ensuite le serveur de mise à jour pour les autres ordinateurs du réseau ?

Le serveur sera l'ordinateur mis à jour via Internet tandis que les autres ordinateurs du réseau seront les clients de ce serveur.

Il est possible de configurer la mise à jour via le réseau local de l'une des manières suivantes :

- Activer l'utilisation de la source de mise à jour locale sur le serveur Kaspersky Administration Kit 5.0.

  Kaspersky Administration Kit est équipé d'un outil de diffusion des mises à jour via le réseau de l'entreprise. Il peut, selon l'horaire défini, mettre à jour les ressources d'accès commun et lancer la mise à jour des autres ordinateurs. Kaspersky Administration Kit veillera à ce que le volume de données

téléchargées ne dépasse les besoins des applications installées. Il est possible de voir sur le serveur la liste des correctifs disponibles. La procédure de configuration est décrite en détail dans le manuel de l'administrateur de Kaspersky Administration Kit 5.0.

- Activer l'utilisation de la source de mise à jour locale dans l'un des logiciels de Kaspersky Lab.

  Cette méthode doit être suivie lorsque l'utilisation de Kaspersky Administration Kit est impossible ou lorsqu'il faut obtenir une structure du réseau des serveurs de mise à jour plus complexe. Pour ce faire :

  - Sélectionnez les ordinateurs qui serviront de serveur de mise à jour. La version 5.01 des applications de Kaspersky Lab devront être installées sur cet ordinateur.
  - Il faut absolument créer sur chaque ordinateur sélectionné une ressource de réseau qui servira à la diffusion de la mise à jour. Il peut s'agir d'un répertoire de réseau sur un ordinateur Windows, un serveur FTP ou un serveur HTTP. Les privilèges d'accès à ce répertoire devront être définis correctement. Pour un répertoire de réseau partagé, l'accès en lecture doit être autorisé pour tous (everyone).
  - Créez la tâche de mise à jour ou modifiez la tâche existante. Activez l'utilisation de la mise à jour depuis la source locale et indiquez le chemin d'accès au répertoire.
  - Précisez le répertoire de source locale de la mise à jour du serveur sur tous les ordinateurs qui devront être mis à jour au départ de ce serveur.

- Utiliser n'importe quel autre moyen pour la mise à jour au départ du dossier partagé du réseau.

  L'origine de la mise à jour n'a pas d'importance pour Kaspersky Anti-Virus, ce qui compte c'est que toute l'information nécessaire à la mise à jour se trouve à l'endroit spécifié.
  Supposons que vous souhaitiez que tous les ordinateurs de votre réseau procèdent à la mise à jour au départ du dossier

[1] Autre que Kaspersky Anti-Virus 5.0 Personal et Kaspersky Anti-Virus 5.0 for Microsoft ISA Server

\\server\klupdates (ou ftp://server/pub/klupdates, autre variante). Pour ce faire :

1. Il est indispensable de créer la ressource klupdates sur l'ordinateur \\server et d'autoriser l'accès en lecture pour tout le monde. Pour la deuxième variante : configurez et lancez le serveur FTP et créez le dossier pub/updates dans la racine.
2. Créez les sous-répertoires suivants dans le dossier klupdates :
   - index : placez-y sans faute les fichiers du dossier index des serveurs de Kaspersky Lab.
   - updates : pour la mise à jour des bases antivirus, il convient de placer dans ce dossier les fichiers du dossier updates des serveurs de Kaspersky Lab ;
   - kasbases : pour la mise à jour des bases antispam, il convient de placer dans ce dossier les fichiers du dossier kasbases des serveurs de Kaspersky Lab ;
3. Sur tous les ordinateurs qui devront être mis à jour au départ de ce serveur, indiquez en guise de dossier de mise à jour \\server\klupdates (ftp://server/pub/klupdates pour la deuxième variante).

Question : j'utilise un serveur proxy et la mise à jour ne fonctionne pas. Que faire ?

L'échec de la réception des mises à jour en cas d'utilisation d'un serveur proxy peut provenir de l'une des causes suivantes :

- Configuration incorrecte des paramètres du réseau.

  Lors de la configuration du service de mise à jour, il est possible de configurer les paramètres du réseau de deux manières : soit en utilisant les paramètres de MS Internet Explorer, soit en utilisant des paramètres individuels. Le service de mise à jour n'utilise pas toujours correctement les paramètres de MS Internet Explorer, surtout dans les cas suivants :

  - La connexion Internet n'est pas configurée sur l'ordinateur ;
  - Les paramètres de MS Internet Explorer ne sont pas accessibles lorsqu'aucun utilisateur n'est enregistré dans le système d'exploitation.
  - Le serveur proxy requiert une autorisation.

Dans tous ces cas, il est nécessaire de définir les paramètres du réseau directement dans les paramètres du service de mise à jour.

- Utilisation d'un serveur proxy qui n'est pas compatible avec le service de mise à jour de Kaspersky Anti-Virus.

  Le service de mise à jour ne fonctionne pas avec Kerio WinRoute car WinRoute ne résout pas entièrement le protocole http 1.0. Dans ce cas, nous vous recommandons d'utiliser n'importe quel autre serveur proxy.

De même, le service de mise à jour ne fonctionne pas via le protocole FTP avec Microsoft ISA Server. Dans ce cas, il est conseillée de procéder à la mise à jour au départ des serveurs de Kaspersky Lab via le protocole HTTP.

ANNEXE B. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Kaspersky Anti-Virus vous permet de contacter le Service d'assistance technique de Kaspersky Lab dans les cas suivants :

- Vous avez l'impression que le logiciel ne fonctionne pas normalement ou de nombreuses erreurs se produisent.
- Kaspersky Anti-Virus a découvert un objet potentiellement infecté par un virus ou l'une de ses variantes et l'accès à cet objet contenant des données importantes est bloqué. Vous souhaiteriez pouvoir continuer à travailler avec ce fichier.

Pour envoyer un message au Service d'assistance technique de Kaspersky Lab au sujet d'échec dans le fonctionnement du logiciel :

Cliquez sur le lien Service d'assistance technique situé dans la partie gauche de l'onglet **Assistance technique** (cf. Illustration 3) de la fenêtre principale du logiciel.

Cette action entraînera l'ouverture du client de messagerie installé sur votre ordinateur, par exemple MS Outlook, et la création d'un nouveau message avec un fichier texte en pièce jointe reprenant une description de votre système et toutes les informations indispensables au sujet de Kaspersky Anti-Virus. Décrivez avec le plus de détails possibles le problème que vous rencontrez lors de l'utilisation de Kaspersky Anti-Virus et envoyez le message. Les opérateurs du Service d'assistance technique tenteront de répondre à vos questions le plus rapidement possible.

Lorsque Kaspersky Anti-Virus met en quarantaine un fichier potentiellement infecté, vous pouvez tenter de le réparer après avoir mis les bases antivirus à jour (pour de plus amples informations, consultez le point 5.4.1.1 à la page 36). Toutefois, lorsque la réparation de l'objet est impossible et que vous devez absolument le réparer le plus vite possible, vous pouvez l'envoyer à Kaspersky Lab en vue d'un examen. Il se peut en effet que ce fichier est infecté par un virus encore inconnu ou qu'il s'agisse simplement d'une fausse alerte.

Pour envoyer vos demandes au service d'assistance technique via le système de traitement automatique des requêtes des clients :

Cliquez sur Commentaires, dans la partie gauche de l'onglet Assistance technique (cf. ill. Illustration 3) de la fenêtre principale.

Cette action entraînera l'ouverture de MS Internet Explorer à un formulaire situé sur le site de Kaspersky Lab. Saisissez les informations requises et formulez votre demande. Les opérateurs du service d'assistance technique tenteront de la traiter le plus rapidement possible.

Pour envoyer un fichier particulier à Kaspersky Lab en vue d'un examen :

Sélectionnez le fichier dans la fenêtre **Quarantaine** (cf. point 5.4.1.1, p. 36) puis cliquez sur **Envoyer**.

Cette action entraînera l'ouverture automatique du client de messagerie installé sur votre ordinateur, par exemple Microsoft Outlook Express, et la composition d'un nouveau message qui reprendra en pièce jointe l'objet suspect. Envoyez le message. Les experts de Kaspersky Lab étudieront attentivement le fichier reçu et tenteront de restaurer les données qu'il contient. Quels que soient les résultats de l'examen, vous recevrez une réponse exhaustive.

Nous attirons votre attention sur le fait que vous pouvez envoyer à Kaspersky Lab un maximum de trois fichiers par jour. De plus, chacun de ces fichiers doit avoir été analysé par Kaspersky Anti-Virus au plus tard trois jours avant l'envoi.

Il peut arriver que Kaspersky Anti-Virus n'identifie pas lors de l'analyse des fichiers potentiellement infectés alors que vous êtes convaincu qu'un ou plusieurs fichiers de votre ordinateur sont infectés par un nouveau type de virus. Vous pouvez envoyer ces fichiers également à Kaspersky Lab en vue d'un examen.

Pour envoyer à Kaspersky Lab les fichiers que vous pensez être infectés en vue d'un examen :

Cliquez sur le lien Envoi d'un fichier suspect dans la partie gauche de l'onglet **Assistance technique** (cf. Illustration 3). Dans la boîte de dialogue qui apparaît, sélectionnez les fichiers sur lesquels portent vos soupçons.

La marche à suivre pour l'envoi d'un courrier électronique à Kaspersky Lab est entièrement identique à celle décrite pour l'envoi de fichiers potentiellement infectés depuis la quarantaine.

ANNEXE C. GLOSSAIRE

Ce manuel reprend des termes et des notions propres à la lutte contre les virus informatiques. Ce glossaire vise à vous offrir une définition de ces différents termes. Les termes sont présentés par ordre alphabétiques.

A

Analyse complète : mode de fonctionnement qui permet à l'utilisateur de rechercher quand il le souhaite la présence d'éventuels virus dans tout l'ordinateur et de réparer ou de supprimer les objets suspects ou infectés découverts.

B

Bases antivirus : il s'agit des bases de données développées par les experts de Kaspersky Lab. Elles reprennent une description détaillée de tous les virus connus à l'heure actuelle ainsi que des méthodes utilisées pour les identifier et réparer les dégâts qu'ils causent. Elles sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouveaux virus apparaissent. Afin d'accroître l'efficacité de la découverte des virus, nous vous recommandons de procéder à la mise à jour régulière des bases antivirus.

Bases de données de messagerie électronique : bases de données qui reprennent les messages électroniques sauvegardés sur votre ordinateur. Chaque message entrant/sortant est repris dans la base après son envoi ou sa réception. Ces bases sont couvertes par la protection en temps réel de votre ordinateur.

C

Clé de licence actuelle : clé de licence installée et utilisée actuellement par Kaspersky Anti-Virus. Elle définit la durée de validité de la licence et la politique de licence par rapport au logiciel. Il ne peut pas y avoir plus de deux clés « actuelles » activées.

Clé de licence de réserve : clé de licence installée, mais pas encore activée pour Kaspersky Anti-Virus. La clé de licence de réserve entrera en vigueur dès la fin de la période de validité de la clé de licence actuelle.

Clé de licence : fichier avec une extension **.key* qui représente votre clé personnelle, indispensable à l'utilisation de Kaspersky Anti-Virus. La clé de licence est reprise dans le pack logiciel lorsque vous achetez celui-ci chez un revendeur Kaspersky Lab. Par contre, elle vous sera envoyée par courrier électronique si vous achetez le logiciel en ligne. Kaspersky Anti-Virus NE PEUT FONCTIONNER sans la clé de licence.

Copie de sauvegarde : création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et mise de cette copie dans le dossier

de sauvegarde. Le fichier pourra être restauré, par exemple pour l'analyse avec des bases antivirus actualisées.

D

Disques virtuels (Disques RAM) : secteur de la mémoire vive (RAM) de l'ordinateur personnel qui émule et qui se comporte comme un disque physique normal de l'ordinateur.

Dossier de sauvegarde : dossier spécial prévu pour accueillir pendant un laps de temps défini les copies de sauvegarde des fichiers avant leur réparation ou leur suppression.

Durée de validité de la licence : période pendant laquelle vous pouvez utiliser toutes les fonctions de Kaspersky Anti-Virus. Cette durée est définie par la clé de licence et est égale à une année calendaire à partir du jour d'acquisition du logiciel. Lorsque la licence est arrivée à échéance, les fonctions du logiciel sont réduites : il n'est plus possible de mettre les *bases antivirus et les modules de l'application à jour*.

E

Etat de la protection antivirus : état actuel de la protection antivirus, caractérisé par le niveau de protection de l'ordinateur.

Exclusions : ensemble de paramètres qui permettent d'exclure certains objets de l'analyse. Vous pouvez configurer ces exclusions aussi bien pour la *protection en temps réel* que pour *l'analyse complète*. Par exemple, vous pouvez exclure les *archives* de l'analyse complète de votre ordinateur ou définir les masques des fichiers que vous ne souhaitez pas analyser.

L

Liste noire : base de données reprenant les informations relatives aux clés de licence dont les détenteurs ont violé les conditions d'utilisation ou aux clés qui ont été livrées mais qui pour une raison quelconque n'ont pas été vendues. Le contenu de la « liste noire » est mis à jour chaque jour en même temps que les bases antivirus et sans celui-ci, Kaspersky Anti-Virus ne fonctionnera pas.

M

Mise à jour : procédure de remplacement/d'ajout de nouveaux fichiers (bases antivirus ou modules logiciels de l'application) depuis les serveurs de mises à jour de Kaspersky Lab.

Mise en quarantaine des objets : mode de traitement d'un objet *suspect* qui consiste à bloquer l'accès et à le mettre en quarantaine pour la suite du traitement.

N

Niveau recommandé : niveau de protection antivirus qui repose sur les paramètres recommandés par les experts de Kaspersky Lab et qui

assure la protection optimale de votre ordinateur. Ce niveau est sélectionné par défaut.

O

Objet infecté : objet qui renferme un code malicieux. Nous vous conseillons vivement de ne pas travailler avec de tels objets car cela pourrait entraîner une infection de votre ordinateur.

Objet OLE : objets ou documents intégrés à d'autres fichiers via la technologie OLE.

Objet suspect : objet dont le code renferme une modification du code d'un virus connu ou d'un code qui évoque celui d'un virus qui n'a pas encore été découvert par Kaspersky Lab.

Objets exécutés au démarrage du système d'exploitation : ensemble des programmes indispensables au lancement et au fonctionnement correct du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont lancés à chaque démarrage du système d'exploitation. Il existe des virus capables d'infecter de tels objets, ce qui peut par exemple bloquer le lancement du système d'exploitation.

P

Protection en temps réel : mode de fonctionnement pendant lequel l'application se trouve en permanence dans la mémoire vive de l'ordinateur et surveille les requêtes adressées aux objets des systèmes de fichiers. Avant d'autoriser l'accès à l'objet, l'application vérifie que l'objet est exempt de virus. S'il en détecte un, il propose soit de réparer l'objet infecté, soit de le supprimer, soit de bloquer l'accès à l'objet (en fonction des paramètres définis).

Q

Quarantaine : dossier spécial prévu pour l'isolation des objets suspects et infectés.

R

Réparation des objets : ensemble des moyens de traitement appliqués aux *objets infectés* qui débouchent sur une restauration complète ou partielle des données ou sur un constat d'incapacité à réparer l'objet en question La réparation des objets s'opère sur la base des enregistrements contenus dans les *bases antivirus*. Lorsque la réparation est la première action prévue pour un objet (autrement dit, la première action exercée sur cet objet directement après sa découverte), une *copie de sauvegarde* de l'objet sera créée avant de procéder à la réparation. En effet, une partie des données peut être endommagée pendant la réparation. La copie vous donne la possibilité de restaurer l'objet à l'état antérieur à la réparation.

Réparation des objets au redémarrage : mode de traitement des objets infectés, utilisés par d'autres applications au moment de la réparation.

Ce mode consiste à créer une copie du fichier infecté, à réparer la copie et remplace, au redémarrage, le fichier original infecté par la copie réparée. Dans les systèmes d'exploitation MS Windows 9x, les grands noms d'objet sont remplacés au redémarrage par des noms raccourcis, ce qui peut entraîner un mauvais fonctionnement des applications qui utilisent les objets réparés.

Restauration : rétablissement de l'objet en *quarantaine* ou dans le *dossier de sauvegarde* vers le répertoire de restauration ou le répertoire d'origine, c'est-à-dire le répertoire où il se trouvait avant sa mise en quarantaine, sa réparation ou sa suppression.

S

Sécurité maximale : niveau de protection de l'ordinateur correspondant au niveau de protection maximum, au détriment d'un léger recul des performances du système.

Suppression d'un objet : mode de traitement d'un objet qui consiste à le supprimer de votre ordinateur. Ce traitement doit être appliqué aux objets infectés. Lorsque la suppression est la première action prévue, le logiciel crée d'abord une copie de *sauvegarde de l'objet*. Cette copie vous permettra de restaurer l'objet original.

V

Virus inconnu : nouveau virus au sujet duquel il n'existe aucune information dans les *bases antivirus*. En règle générale, les virus inconnus peuvent être malgré tout identifiés par Kaspersky Anti-Virus grâce à *l'analyse heuristique* et ces objets reçoivent le statut de *suspects*

Vitesse maximale : niveau de protection de l'ordinateur correspondant à la vitesse maximale de fonctionnement, au détriment d'un léger recul de la protection antivirus.

ANNEXE D. KASPERSKY LAB

Fondée en 1997, Kaspersky Lab 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 Lab 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 Lab. 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 Lab 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, passerelles-Internet 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 Lab 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 trois heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

D.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal protège les ordinateurs personnels tournant sous Windows 98/ME, 2000/NT/XP contre tous les types de virus connus, y compris les logiciels à risque (riskware). Le programme contrôle en permanence toute les sources d'infection potentielles : le courrier électronique, Internet, les disquettes, les CD-Rom, etc. Le système unique d'analyse heuristique des données neutralise efficacement les virus inconnus. Le logiciel peut fonctionner dans l'un des modes suivants (ces différents modes peuvent être utilisés séparément ou conjointement) :

- La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
- **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

Kaspersky Anti-Virus® Personal ignore à chaque analyse les objets qui n'ont pas été modifiés depuis la dernière analyse, aussi bien dans le cadre de l'analyse en temps réel qu'à la demande. Ceci se traduit par une **nette augmentation de la rapidité d'exécution de l'application**.

Le logiciel représente donc un obstacle de taille pour les virus qui tenteraient d'infecter l'ordinateur via le courrier électronique. Kaspersky Anti-Virus® Personal analyse et répare automatiquement tous les messages entrants et sortants via les protocoles POP3 et SMTP. Il décèle également avec efficacité les virus dans les bases de données de messagerie.

Le logiciel 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, CAB, RAR, ARJ**.

La simplicité de la configuration du logiciel est assurée grâce à l'existence de trois niveaux prédéfinis : **Sécurité maximale**, **Recommandé** et **Vitesse maximale**.

Les bases de données antivirus sont actualisées toutes les trois heures. Leur distribution est garantie même en cas de coupure ou de modification de la connexion.

Kaspersky Anti-Virus® Personal Pro

Ce logiciel a été conçu pour la protection antivirale globale des ordinateurs personnels qui tournent sous Windows 98/ME, Windows 2000/NT et Windows XP avec les applications de la suite MS Office. 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.

Kaspersky Anti-Virus® Personal Pro 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 et réparer tout le courrier entrant et sortant via les protocole POP3 et SMTP et déceler efficacement les virus dans les bases de données de messagerie ;
- **L'inhibiteur de comportement** qui garantit une protection totale contre les virus de macro.
- **L'analyse antivirus** de plus de 900 types de formats de fichiers compressés et archivés. Cela permet de rechercher automatiquement la présence éventuelle de virus dans le contenu et de supprimer le code malveillant des fichiers comprimés aux formats **ZIP**, **CAB**, **RAR et ARJ**.

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[2] 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, Windows 2003 Server, Novell Netware, FreeBSD et OpenBSD et Linux ;

[2] En fonction du type de livraison

- *Système de messagerie* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; MS ISA Server.

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 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 ;
- *Passerelle-Internet* : CheckPoint Firewall –1; MS ISA Server ;
- *Ordinateurs de poche* sous Windows CE et Palm OS.

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.

Kaspersky® Anti-Spam Personal

Kaspersky® Anti-Spam Personal a été conçu pour protéger les utilisateurs des clients de messagerie Microsoft Outlook et Microsoft Outlook Express des méfaits du courrier indésirable.

Kaspersky® Anti-Spam Personal est un outil puissant qui permet d'identifier le courrier indésirable dans le flux de courrier entrant via les protocoles POP3 et IMAP4 (uniquement pour Microsoft Outlook).

Tous les attributs du message sont analysés au moment du filtrage : l'adresse de l'expéditeur, l'adresse du destinataire et l'objet du message. Le filtrage a également lieu au niveau du contenu. Autrement dit, le corps du message (y compris l'objet) et les pièces jointes sont analysés en fonction d'algorithmes linguistiques et heuristiques uniques.

Les hautes performances de Kaspersky® Anti-Spam sont possibles grâce à des mises à jour quotidiennes automatiques des bases de données utilisées par les filtres, à partir des échantillons fournis par les spécialistes linguistiques du laboratoire.

D.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Lab (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/fr http://www.viruslist.com E-mail : sales@kaspersky.com

ANNEXE E. INDEX

ANNEXE F. 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 Lab 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 Lab 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 Lab contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Lab 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.

1.1.6 Ce logiciel ne peut-être utilisé dans des outils automatiques, semi-automatiques ou manuels conçus pour la création de définitions de virus, de routines de détection de virus ou de n'importe quel autre type de données ou de codes servant à détecter des données ou des codes malicieux.

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 notifications 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 Lab 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 Lab ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Lab avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Lab 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 Lab 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 Lab 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 Lab 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 Lab 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 Lab 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 Lab 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 Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Lab 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 Lab 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 Lab 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 Lab (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 Lab 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 Lab 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 Lab pour toute Fausse Représentation faite en connaissance de cause.

(ii) La responsabilité de Kaspersky Lab 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).