KASPERSKY LAB

Kaspersky Anti-Virus® Personal 5.0

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS® PERSONAL 5.0

Manuel de l'utilisateur

NB : Cette documentation, traduite en français à partir du russe, décrit les fonctionalités et services inclus avec la version russe. Il se peut que certaines fonctionalités ou services décrits, ne soient pas disponibles en France.

http://www.kaspersky.fr/

Date d'édition: avril 2006

Sommaire

CHAPITRE 1. INTRODUCTION

1.1. Virus informatiques et programmes malicieux

Le développement des technologies informatiques et des moyens de communication permet aux individus mal intentionnés de propager les menaces par divers canaux. Nous allons les aborder en détail.

Internet

Le réseau des réseaux se caractérise par le fait qu'il n'appartient à personne et qu'il n'a pas de limites territoriales. Ces deux éléments contribuent pour beaucoup au développement de nombreuses ressources Internet et à l'échange d'informations. A l'heure actuelle, n'importe qui peut accéder à des données sur Internet ou créer son propre site.

Ce sont ces mêmes caractéristiques du réseau Internet qui permettent aux individus mal intentionnés de commettre leurs méfaits sans risquer d'être attrapés et punis.

Les individus mal intentionnés placent des virus et d'autres programmes malveillants sur des sites Web après les avoir « dissimulés » sous l'apparence d'un programme utile et gratuit. De plus, les scripts exécutés automatiquement à l'ouverture d'une page Web peuvent lancer des actions malveillantes sur votre ordinateur, y compris la modification de la base de registres système, le vol de données personnelles et l'installation de programmes malveillants.

Grâce aux technologies de réseau, les individus mal intentionnés lancent des attaques sur des ordinateurs personnels ou des serveurs d'entreprise distants. Le bilan de ces attaques peut être la mise hors service de la source, l'obtention de l'accès total à l'ordinateur et, par conséquent, aux informations qu'il contient ou l'utilisation de la ressource en tant que partie du réseau de zombies.

La popularité croissante des cartes de crédit et des paiements électroniques utilisés pour régler des achats en ligne (magasins en ligne, ventes aux enchères, sites de banque, etc.) s'accompagne d'une augmentation du nombre d'escroqueries en ligne qui sont devenues l'un des crimes les plus répandus.

Intranet

Un intranet est un réseau interne développé afin de gérer les informations au sein de l'entreprise ou un réseau privé. L'intranet est le seul espace du réseau prévu pour la sauvegarde, l'échange et l'accès aux informations de tous les ordinateurs du réseau. Aussi, lorsqu'un ordinateur du réseau est infecté, les ordinateurs restant sont exposés à un risque plus important. Afin d'éviter toute situation similaire, il faut non seulement protéger le périmètre du réseau mais également chaque ordinateur qui en fait partie.

Courrier électronique

La présence d'un client de messagerie électronique sur presque tous les ordinateurs et l'exploitation du carnet d'adresses électroniques pour trouver de nouvelles adresses favorisent énormément la diffusion des programmes malveillants. L'utilisateur d'une machine infectée, sans se douter de quoi que ce soit, envoie des messages infectés à divers destinataires qui, à leur tour, envoient des messages infectés, etc. Il arrive même fréquemment qu'un document infecté se retrouve, suite à une erreur, dans les listes de diffusion commerciales d'une grande société. Dans ce cas, le nombre de victimes ne se chiffrent pas à quelques malheureux mais bien en centaines, voire en milliers de destinataires qui diffuseront, à leur tour, les fichiers infectés à des dizaines de milliers d'autres abonnés.

En plus du risque d'être infecté par un programme malveillant, il y a également le problème lié à la réception de messages non sollicités. Bien que le courrier indésirable ne constitue pas une menace directe, il augmente la charge des serveurs de messagerie, génère un trafic complémentaire, encombre les boîtes aux lettres et entraîne une perte de temps productif, ce qui peut avoir des répercussions financières sérieuses.

Il convient de noter que les individus mal intentionnés ont commencé à recourir aux technologies de diffusion massive du courrier indésirable et à l'ingénierie sociale pour amener l'utilisateur à ouvrir le message, à cliquer sur un lien vers un site quelconque, etc. Pour cette raison, la possibilité de filtrer le courrier indésirable est importante en elle-même mais également pour lutter contre les nouveaux types d'escroquerie en ligne comme le phishing ou la diffusion de programmes malveillants.

Média amovibles

Les disques amovibles (disquettes, cédéroms, cartes Flash) sont beaucoup utilisés pour conserver des données ou les transmettre.

Lorsque vous exécutez un fichier infecté par le code malicieux depuis un disque amovible, vous pouvez endommager les données sauvegardées

sur votre ordinateur ou propager le virus sur d'autres disques de votre ordinateur ou des ordinateurs du réseau.

A l'heure actuelle, votre ordinateur peut être endommagé par un nombre assez important de menaces. Cette rubrique se penche plus particulièrement sur les menaces bloquées par Kaspersky Internet Security :

Vers

Ce type de programmes malveillants se propage principalement en exploitant les vulnérabilités des systèmes d'exploitation. 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 permet à de nombreux vers de se diffuser à une très grande vitesse.

Ils s'introduisent dans l'ordinateur, relèvent les adresses des autres machines connectées 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.

Virus

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*.

Chevaux de Troie

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 " crash " du système. Ces programmes malicieux ne sont pas des virus au sens traditionnel du terme (en effet, ils ne peuvent infecter les autres applications ou les données). 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 ». Ceci étant dit, les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnelles.

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.

Adwares

Ce code est intégré, à l'insu de l'utilisateur, dans un logiciel afin d'afficher des messages publicitaires. En règle générale, les adwares sont intégrés à des logiciels distribués gratuitement. La publicité s'affiche dans l'espace de travail. Bien souvent, ces programmes recueillent également des données personnelles sur l'utilisateur qu'ils transmettent à leur auteur, ils modifient divers paramètres du navigateur (page d'accueil et recherche, niveau de sécurité, etc.) et ils créent un trafic sur lequel l'utilisateur n'a aucun contrôle. Tout cela peut entraîner une violation de la politique de sécurité, voire des pertes financières.

Logiciels espion

Ces programmes sont capables de récolter des informations sur un individu particulier ou sur une organisation à son insu. Il n'est pas toujours facile de définir la présence de logiciels espion sur un ordinateur. En règle générale, ces programmes poursuivent un triple objectif :

- Suivre les actions de l'utilisateur sur l'ordinateur ;
- Recueillir des informations sur le contenu du disque dur ; il s'agit bien souvent du balayage de certains répertoires ou de la base de registres système afin de dresser la liste des applications installées sur l'ordinateur ;
- Recueillir des informations sur la qualité de la connexion, les modes de connexion, la vitesse du modem, etc.

Riskwares

Il s'agit d'un programme qui n'a aucune fonction malicieuse mais qui pourrait être exploité par un individu mal intentionné en guise de soutien à un programme malicieux en raison des failles ou des erreurs qu'il contient. Dans certains cas, la présence de tels programmes sur votre ordinateur expose vos données à un certain risque. Cette catégorie de programme contient par exemple certains utilitaires d'administration à distance, des programmes de permutation automatique de la disposition du clavier, des clients IRC, des serveurs FTP, des utilitaires d'arrêt de processus ou de dissimulation de leur fonctionnement.

Une autre catégorie de programmes présentant un risque potentiel, proche des adwares, spywares et riskwares, contient les programmes qui s'intègrent au navigateur et qui réorientent le trafic. Il vous est certainement déjà arrivé de cliquer de vouloir accéder à un site particulier et de vous retrouvez sur la page d'accueil d'un site totalement différent.

Jokewares

Ces programmes ne vont causer aucun dégât direct à votre ordinateur mais ils s'affichent des messages qui indiquent que des dégâts ont déjà

été commis ou qu'ils seront commis sous certaines conditions. Ces programmes préviennent souvent les utilisateurs d'une menace inexistante telle que le formatage du disque dur (alors qu'aucun formatage n'est exécuté), découvrent des virus dans des fichiers sains, etc.

Rootkit

Utilitaires qui permettent de dissimuler une activité malveillante. Ils masquent la présence de programmes malveillants afin que ceux-ci ne soient pas identifiés par les logiciels antivirus. Les rootkits modifient le système d'exploitation de l'ordinateur et remplacent ses fonctions fondamentales afin de dissimuler sa propre présence et les actions exécutées par l'individu mal intentionné sur l'ordinateur infecté.

Autres programmes dangereux

Programmes développés pour mener des attaques par déni de service sur des serveurs distants, pour s'introduire dans d'autres ordinateurs ou qui servent au développement de logiciels malicieux. Cette catégorie reprend les utilitaires d'attaque informatique, les constructeurs de virus, les balayeurs de vulnérabilités, les programmes d'identification de mots de passe, les programmes de pénétration des réseau ou du système attaqué.

Attaques de pirates informatiques

Les attaques de pirates informatiques sont le fait d'individus mal intentionnés ou de programmes malveillants qui veulent s'emparer d'informations sauvegardées sur l'ordinateur de la victime, mettre le système hors service ou obtenir un contrôle total sur les ressources de l'ordinateur.

Certains types d'escroquerie via Internet

Le **phishing** est un type d'escroquerie en ligne qui consiste à diffuser un message électronique visant à voler des informations confidentielles, à caractère financier dans la majorité des cas. Un message de phishing doit ressembler le plus possible à un message que pourrait envoyer une banque ou une entreprise connue. Le message contient un lien vers un site fictif créé spécialement par l'individu mal intentionné et qui est une copie conforme du site de l'organisation prétendument à l'origine du message. Une fois qu'elle arrive sur ce site, la victime est invitée à saisir, par exemple, son numéro de carte de crédit ou d'autres informations confidentielles.

La n**umérotation vers un site Internet payant** est un type d'escroquerie qui repose sur l'utilisation non autorisée de sites Internet payants (bien souvent, des sites à contenu pornographique). Les programmes installés par l'individu mal intentionné (les dialers) ouvrent une connexion par

modem entre votre ordinateur et le numéro payant. Dans la majorité des cas, le tarif de cet appel est très élevé, ce qui se traduit par une lourde facture de téléphone pour l'utilisateur.

Publicités envahissantes

Il s'agit des fenêtres pop up et des bannières qui apparaissent lorsque vous visitez un site Internet quelconque. En règle générale, les informations présentées n'ont aucun intérêt. Les fenêtres pop up et les bannières distraient l'utilisateur et augmentent le volume de trafic.

Courrier indésirable

Il s'agit de l'envoi anonyme de messages non sollicités. On peut ranger dans cette catégorie les messages publicitaires, les messages à caractères politique ou de propagande, les messages qui vous invitent à venir en aide à une personne quelconque, etc. Il existe une catégorie spéciale de messages non sollicités qui reprend les propositions pour obtenir des quantités importantes d'argent ou qui invitent le destinataire à participer à une pyramide. Il ne faut pas oublier les messages qui visent à voler les mots de passe, les messages dont le contenu doit être transmis à vos amis (les chaînes), etc. Le courrier indésirable augmente considérablement la charge des serveurs de messagerie et le risque de perte d'informations cruciales pour l'utilisateur.

Dans ce manuel, le terme " virus " désignera les programmes malveillants. L'objet infecté sera dénommé "objet dangereux". Le type de programme malveillant sera précisé au besoin.

1.2. Présentation et fonctions principales de Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal est un logiciel qui a été développé pour garantir la protection antivirus des ordinateurs personnels tournant sous le système d'exploitation Microsoft Windows® (cf. point 1.4, p. 15).

Le logiciel installé sur votre ordinateur assure les fonctions suivantes :

- **Protection contre les virus et les programmes malicieux** : il identifie et neutralise les programmes malicieux qui infiltrent votre ordinateur. Le logiciel fonctionne selon deux modes (utilisables séparément ou au sein de la suite) :

- **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 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.

- **Restauration des capacités opérationnelles après une attaque de virus**. Les fonctions d'analyse et de réparation selon les critères recommandés par les experts de Kaspersky Lab vous permettent de découvrir l'ensemble des virus qui ont infecté vos données.
- **Analyse et réparation du courrier entrant et sortant.** Le courrier entrant et sortant est analysé et réparé en temps réel[1]. De plus, il est possible de procéder à l'analyse à la demande[2] des bases de messagerie électronique de clients (cf. Chapitre 10, p. 72).
- **Protection de l'ordinateur contre les attaques de réseau.** Recherche d'éventuelles attaques de réseau dans l'ensemble des données qui arrivent via le réseau (réseau local ou Internet) sur l'ordinateur de l'utilisateur. En cas de découverte d'une telle attaque, elle sera bloquée et l'ordinateur à l'origine de cette attaque sera bloqué. De plus, le logiciel autorise l'utilisation du mode furtif dans le cadre duquel l'ordinateur accepte uniquement les données des ordinateurs lorsque l'utilisateur est à l'origine de l'échange de données.
- **Mise à jour des bases antivirus, des bases d'attaque de réseau et des modules de programme** afin de toujours disposer des dernières informations sur les nouveaux virus et les nouvelles attaques, des moyens de réparer les objets infectés ainsi que des dernières versions des modules du programme (pour autant que cette option n'ait pas été désactivée). Les mises à jour sont téléchargées depuis les serveurs de mise à jour de Kaspersky Lab ou installées depuis un répertoire local.
- **Recommandations sur la configuration du logiciel et son utilisation**. Les conseils des experts de Kaspersky Lab vous accompagnent tout au long de l'utilisation du programme ainsi que les recommandations pour une configuration optimale de la protection antivirus.

[1] L'analyse porte uniquement sur le courrier entrant via le protocole POP3 et sur le courrier sortant via le protocole SMTP.

[2] Kaspersky Anti-Virus peut procéder à l'analyse antivirus des bases de messagerie électronique de n'importe quel client mais ne peut réparer que les bases de MS Outlook et MS Outlook Express.

La fenêtre principale de Kaspersky Anti-Virus® affiche en permanence des recommandations sur l'exécution de telle ou telle tâche et sur les raisons qui les justifient en cas de découverte d'objets dangereux, lorsque le contenu des bases antivirus est fortement dépassé ou lorsqu'il est grand temps de réaliser l'analyse complète de l'ordinateur.

Les experts de Kaspersky Lab se sont efforcés de configurer ce logiciel de la meilleure manière possible en intégrant la riche expérience dans la lutte contre les virus et les nombreux commentaires reçus par le Service d'assistance technique de la part de nombreux utilisateurs. Les paramètres de protection antivirus recommandés par nos experts sont appliqués dès l'installation et le lancement du logiciel.

- **Utilisation de différents profils.** Création et application de fichiers de configuration spéciaux appelés *profils* où sont conservés les paramètres de l'application. En enregistrant ces paramètres dans un profil, vous pouvez facilement modifier la configuration de Kaspersky Anti-Virus. Ainsi, vous pouvez configurer le fonctionnement uniquement en mode de protection en temps réel ou à la demande et utiliser ces configurations uniquement lorsque vous en avez besoin. A tout moment de l'utilisation de Kaspersky Anti-Virus, vous pouvez rétablir les paramètres recommandés.

- **Placement des objets en quarantaine**. Il est possible de placer les objets potentiellement infectés par un virus ou l'une de ses variantes dans un répertoire particulier sécurisé. Vous pouvez ensuite réparer, supprimer ou restaurer le fichier incriminé dans son répertoire d'origine ou l'envoyer aux experts de Kaspersky Lab en vue d'un examen approfondi. Les fichiers en quarantaine sont convertis dans un format spécial et ne présentent aucun danger.

- **Création de copies de sauvegarde des objets**. Création de copies de sauvegarde des objets avant leur réparation ou suppression dans un répertoire particulier. Ces copies sont créées afin de permettre la restauration du fichier au cas où il contiendrait des données critiques ou afin de reconstituer le scénario de l'infection. Les copies sont conservées sous un format spécial et ne représentent aucun danger.

- **Création d'un rapport**. Tous les résultats de l'activité de Kaspersky Anti-Virus® Personal sont consignés dans un rapport. Le rapport détaillé sur les résultats de l'analyse reprend des statistiques générales relatives aux objets analysés, la configuration en vigueur pour l'exécution de la tâche et préserve la chronologie de l'analyse et du traitement de chaque objet. Les résultats de la mise à jour sont également consignés dans le rapport.

1.3. Nouveautés de la version 5.0

La version 5.0 du logiciel Kaspersky Anti-Virus® Personal décrite dans ce manuel inclut les nouveautés suivantes :

- *Introduction d'une base de données contenant les informations relatives aux objets analysés.* Kaspersky Anti-Virus® 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.
- *Analyse et réparation du courrier entrant et sortant de tous les clients de messagerie utilisant le protocole POP3* pour la réception des messages et le protocole SMTP pour leur envoi. La version antérieure garantissait la protection antivirus uniquement pour Microsoft Office Outlook.
- *Réparation des archives infectées.* Kaspersky Anti-Virus® Personal est capable de réparer les archives infectées au format *zip, arj, cab, rar, lha* et *ice*. La version antérieure du logiciel était capable uniquement d'identifier les fichiers infectés dans les archives et de réparer les objets infectés dans les archives zip.

  Kaspersky Anti-Virus® analyse les archives multivolumes des formats indiqués ainsi que les archives auto-extractibles mais ne les répare pas.
- *Protection contre les attaques de réseau.* Cette version de Kaspersky Anti-Virus protège votre ordinateur contre toutes les attaques de réseau et de pirates informatiques les plus répandues actuellement.
- *Compatibilité améliorée entre Kaspersky Anti*-Virus et les autres logiciels antivirus. Pendant l'installation du programme, vous pouvez décider de ne pas activer la protection du système de fichiers, du courrier, du réseau ou de ne pas analyser les scripts exécutés si d'autres applications offrent déjà cette protection sur votre ordinateur.
- *Interface simplifiée.* L'attribution de chacune des fonctions particulières de la protection antivirus à un module de programme distinct caractéristique de la version antérieure a été abandonnée au profit d'une application unifiée. Cette démarche se traduit par une simplification de l'utilisation et de l'administration des fonctions les plus critiques de Kaspersky Anti-Virus. Désormais, le réglage du niveau de protection antivirus ne s'opère plus via l'édition de paramètres mais en déplaçant simplement un curseur sur une échelle des niveaux.
- *Paramètres recommandés et conseils des experts.* Cette version du logiciel est distribuée avec un ensemble de paramètres d'analyse à la

demande prédéfinis par les experts de Kaspersky Lab, ce qui simplifie l'utilisation. Il n'est donc pas nécessaire, dans la majorité des cas, de configurer le logiciel avant de l'utiliser. En cas de sélection du niveau de protection le plus faible, le logiciel affiche le message adéquat et propose différentes options pour renforcer la protection.

- *Administration des profils de l'application*. Possibilité d'enregistrer les paramètres du programme dans un fichier spécial en vue d'une utilisation ultérieure. Si les paramètres recommandés ne vous conviennent pas, modifiez-les selon vos besoins et enregistrez cette configuration dans le *profil*.
- *Prolongation de la licence d'utilisation du logiciel.* Kaspersky Anti-Virus® Personal 5.0 vous permet d'activer les clés de licence afin de pouvoir utiliser le logiciel plus longtemps.
- *Envoi d'objets à Kaspersky Lab pour étude approfondie.* Il est désormais possible d'envoyer à Kaspersky Lab en vue d'un examen approfondi les objets potentiellement infectés découverts par Kaspersky Anti-Virus® Personal ainsi que les objets que vous soupçonnez être infectés.
- *Interdiction de la suppression des objets de bases*. Désormais, vous ne pouvez plus supprimer par accidents les objets suivants à l'aide de Kaspersky Anti-Virus® : archives auto-extractibles ou autres, bases de données de messagerie électronique, fichiers au format du courrier électronique. Vous pouvez toutefois toujours les supprimer indépendamment. Les archives auto-extractibles font exception à cette règle.
- *Restriction de suppression des bases de messagerie infectées.* Pour des raisons de sauvegarde, les bases de messagerie infectées ne seront pas supprimées automatiquement par Kaspersky Anti-Virus. Ce sera à vous de les supprimer manuellement le cas échéant.
- *Protection par mot de passe de l'accès à l'administration des paramètres de Kaspersky Anti-Virus*. Vous pouvez définir un mot de passe qu'il faudra saisir pour passer du mode utilisateur au mode administrateur. En mode utilisateur, il sera impossible de modifier les paramètres du logiciel, de désactiver la protection en temps réel et de décharger Kaspersky Anti-Virus Personal de la mémoire de l'ordinateur.

1.4. Configuration matérielle et logicielle requise

Pour garantir le fonctionnement normal de Kaspersky Anti-Virus® Personal, votre ordinateur doit répondre aux critères suivants.

Configuration générale :

- 50 Mo disponibles sur le disque dur ;
- Lecteur de CD-ROM/DVD-ROM (pour l'installation de Kaspersky Anti-Virus® au départ d'un CD) ;
- Microsoft Internet Explorer version 5.5 et suivante (pour la mise à jour des bases antivirus et des modules du programme via Internet).

Microsoft Windows 98 :

- Processeur Intel Pentium® de 133 Mhz minimum ;
- 32 Mo de RAM.

Microsoft Windows ME :

- Processeur Intel Pentium® de 150 Mhz minimum ;
- 32 Mo de RAM.

Microsoft Windows NT Workstation 4.0 (Service Pack 6a) :

- Processeur Intel Pentium® de 133 Mhz minimum ;
- 32 Mo de RAM.

Microsoft Windows 2000 Professional (Service Pack 2 ou suivant) :

- Processeur Intel Pentium® de 133 Mhz minimum ;
- 64 Mo de RAM.

Microsoft Windows XP Home Edition ou XP Professional (Service Pack 1 ou suivant) :

- Processeur Intel Pentium® de 300 Mhz minimum ;
- 128 Mo de RAM.

1.5. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Anti-Virus® Personal chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr – rubrique **E-Store / Particuliers**).

Le pack logiciel en boîte contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés; la clé de licence 365 jours est inclue et présente sur le CDROM, séparément ou incluse dans le fichier exécutable.

- Le manuel de l'utilisateur avec le contrat de licence utilisateur imprimé à la fin de ce manuel.

Si vous achetez Kaspersky Anti-Virus® Personal en ligne, et dés la réception de votre paiement, vous recevrez un email contenant des liens personnels pointant sur le site Web de Kaspersky Lab pour télécharger :

- le fichier d'installation contenant votre clé de licence d'un an,
- votre clé de licence un an seule (utile dans le cas où vous auriez déjà installé une version avec une clé d'essai),
- la version électronique de ce manuel (format Adobe PDF).

La licence utilisateur constitue l'accord juridique passé entre vous et Kaspersky Lab, stipulant les conditions d'utilisation du progiciel que vous avez acquis. Lisez la attentivement !

1.6. 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®.

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.

CHAPITRE 2. INSTALLATION DU LOGICIEL

Afin d'installer Kaspersky Anti-Virus® Personal sur votre ordinateur, vous devez exécuter le fichier exécutable repris sur le CD-ROM d'installation.

L'installation réalisée au départ du fichier d'installation téléchargé sur Internet correspond entièrement à l'installation au départ du CD-ROM.

Le programme d'installation se compose d'une succession de boîtes de dialogue. Chacune de ces boîtes présente différents boutons destinés à contrôler la procédure. En voici une brève description :

- **Suivant >** confirme l'action et passe au point suivant dans le processus d'installation.
- **< Précédent** revient au point précédent dans l'installation.
- **Annuler** interrompt l'installation.
- **Fermer** conclut l'installation du logiciel sur l'ordinateur.

Les pages suivantes expliquent étape par étape l'installation du logiciel.

Etape 1. Vérification de la version du système d'exploitation installé sur votre ordinateur

Avant d'installer le logiciel, le système vérifie si le système d'exploitation de votre ordinateur et les Services Packs répondent aux conditions minimales d'installation de Kaspersky Anti-Virus® Personal.

Au cas où l'une des conditions ne serait pas remplie, le message adéquat apparaîtra à l'écran. Il est conseillé d'installer les logiciels et les mise à jour nécessaires de Microsoft Windows à l'aide du service **Mise à jour Windows** (ou un autre moyen) avant d'installer Kaspersky Anti-Virus® Personal.

Etape 2. Recherche d'autres logiciels antivirus éventuellement installés

Au cours de cette étape, le programme d'installation vérifie si d'autres logiciels antivirus, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation

conjointe avec Kaspersky Anti-Virus® Personal pourraient engendrer des conflits, ne sont pas déjà installés sur votre ordinateur.

En cas de découverte d'une version antérieure de Kaspersky Anti-Virus® (ex. : version 4.5), vous serez invité à conserver la clé de licence de ce logiciel si elle est toujours valide.

Nous vous conseillons de conserver la clé de licence utilisée jusqu'à présent. Vous pourrez en effet l'utilisez avec Kaspersky Anti-Virus Personal 5.0.

Une fois que vous aurez enregistré la clé, un message vous invitera à supprimer l'ancienne version du logiciel car il est impossible de l'utiliser conjointement avec Kaspersky Anti-Virus 5.0 Personal.

Cliquez sur **OK** afin d'interrompre l'installation. Supprimez ensuite la version antérieure de Kaspersky Anti-Virus et lancez à nouveau le programme d'installation.

Si vous avez conservé la clé de licence active de Kaspersky Anti-Virus 4.x à l'étape précédente en vue de l'utiliser avec la version 5.0, la fenêtre d'installation de la clé de licence (cf. Etape 8, p. 22) ne s'affichera pas. La clé sera utilisée par le logiciel.

En cas de découverte d'un logiciel antivirus développé par un autre éditeur, le programme d'installation vous suggèrera de le supprimer avant d'installer Kaspersky Anti-Virus® Personal.

Nous vous conseillons de suivre cette suggestion et de supprimer le programme en question. Pour ce faire, cliquez sur **Non** afin d'interrompre l'installation. Supprimez ensuite le logiciel indiqué puis lancez à nouveau le programme d'installation de l'application.

Les experts de Kaspersky Lab ne recommandent pas l'installation de plusieurs logiciels antivirus car cela peut entraîner des conflits.

Si Kaspersky Anti-Virus Personal Pro 5.0 est déjà installé sur votre ordinateur , le message correspondant s'affichera. Si vous poursuivez l'installation, cette copie du programme remplacera la version antérieure.

En cas de mise à jour de la version 5.0, la fenêtre d'installation de la clé de licence (cf. Etape 8, p. 22) ne contiendra pas d'informations sur la clé, mais la clé installée antérieurement sera toujours utilisée.

Etape 3. Fenêtre d'accueil de la procédure d'installation

Dès l'exécution du fichier exécutable, et pour autant que le programme d'installation n'ait pas découvert d'autres logiciels antivirus sur votre ordinateur,

une fenêtre d'accueil reprenant les informations sur le lancement du programme d'installation de Kaspersky Anti-Virus® Personal sur votre ordinateur apparaît à l'écran.

Pour continuer l'installation, cliquez sur **Suivant >**. Cliquez sur **Annuler** pour interrompre l'installation.

Etape 4. Examen de la licence utilisateur

Cette fenêtre reprend le contrat de licence entre l'utilisateur et Kaspersky Lab. Il convient de le lire attentivement. Cliquez sur **J'accepte** si vous êtes d'accord avec tous les termes de la licence utilisateur. En marquant votre accord, vous poursuivez la procédure d'installation.

Etape 5. Informations utilisateur

La saisie du nom de l'utilisateur et de l'organisation s'opère à cette étape. Les données reprises par défaut sont celles qui figurent dans le registre du système d'exploitation. Vous avez la possibilité de les modifier.

Pour continuer l'installation, cliquez sur **Suivant >.**

Etape 6. Lecture des informations importantes relatives au logiciel

Cette fenêtre vous donne la possibilité de prendre connaissance de renseignements importants sur Kaspersky Anti-Virus avant de commencer à l'utiliser.

Cliquez sur **Suivant >** pour poursuivre l'installation

Etape 7. Utilisation des technologies de Kaspersky Lab

Cette étape de l'installation de Kaspersky Anti-Virus vous oblige à décider d'appliquer ou non les technologies suivantes développées par Kaspersky Lab :

Protection en temps réel du système de fichiers : analyse antivirus de tous les fichiers exécutés, ouverts et enregistrés sur l'ordinateur. La protection des fichiers est activée par défaut. Si vous ne souhaitez pas que Kaspersky Anti-Virus analyse les fichiers à chaque requête, désélectionnez la case **Utiliser la protection en temps réel du système de fichiers**.

Protection en temps réel du courrier : analyse antivirus des tous les messages envoyés ou reçus sur votre ordinateur, ainsi que de message des bases de données de messagerie. La protection du courrier est activée par défaut. Si vous ne souhaitez pas que Kaspersky Anti-Virus analyse les messages,

désélectionnez la case **Utiliser la protection en temps réel du courrier**.

Analyse des scripts exécutés : recherche de virus dans les scripts VBScript et JavaScript avant leur exécution. L'analyse des scripts est activée par défaut. Si vous ne souhaitez utiliser Kaspersky Anti-Virus pour analyser les scripts, désélectionnez la case **Utiliser l'analyse des scripts**.

Protection en temps réel du réseau est une technologie qui protège votre ordinateur contre les attaques des pirates informatiques. Cette technologie bloque les attaques qui ciblent votre ordinateur via le réseau et protège vos données contre le vol, l'accès non autorisé et la destruction. La protection en temps réelle du réseau est activée par défaut. Pour désactiver la protection, désélectionnez la case **Utiliser la protection en temps réel contre les attaques de réseau**.

Si vous désactivez l'utilisation des technologies citées ci-dessus à cette étape, vous devrez réinstaller le logiciel pour les installer.

Si à cette étape vous avez décidé de ne pas utiliser ces technologies, vous devrez à nouveau installer le logiciel le jour où vous déciderez de les utiliser et sélectionner les technologies dont vous avez besoin.

Si pendant l'utilisation de Kaspersky Anti-Virus vous décidez de ne pas utiliser une forme quelconque de protection en temps réel ou la technologie iStreams™, vous devrez installer à nouveau l'application et désélectionner à cette étape les cases correspondantes.

La *technologie iStreams*™ est une technologie permettant l'accélération de l'analyse antivirus des objets (consultez l'Annexe B à la page 127 pour obtenir de plus amples informations). Pour désactiver l'utilisation de cette technologie, il suffit de désélectionner la case **Utiliser la technologie iStreams™**.

Cette technologie est applicable uniquement sur les ordinateurs possédant un système de fichiers NTFS.

Si vous désactivez la technologie iStreams à cette étape, vous devrez réinstaller Kaspersky Anti-Virus pour activer à nouveau cette technologie.

Cliquez sur **Suivant >** pour poursuivre l'installation.

Etape 8. Activation de la clé de licence

Normalement cette étape est automatique et vous ne la voyez pas. Le programme trouve lui-même la clé et l'installe sans rien vous demander. Il peut cependant arriver que le programme ne trouve pas votre licence. Elle vous sera alors demandée. Dans ce cas, veuillez suivre les indications ci-dessous.

Cette étape correspond à l'activation de la clé de licence de Kaspersky Anti-Virus® Personal. Cette clé est votre clé personnelle qui reprend toutes les informations fonctionnelles indispensables au fonctionnement de Kaspersky Anti-Virus®, à savoir:

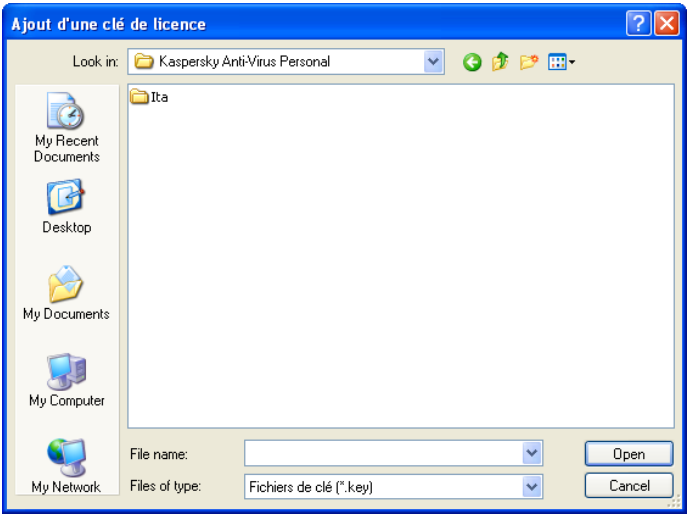
- Les informations sur l'assistance technique (qui l'assure et comment l'obtenir) ;
- Le nom et le numéro de licence ainsi que sa date d'expiration.

Le logiciel ne fonctionnera pas sans clé de licence.

Pour installer une nouvelle clé de licence :

a. Cliquez sur **Parcourir** et dans la fenêtre qui s'ouvre, sélectionnez le répertoire qui abrite le fichier de la clé de licence:

   - Si vous avez acheté Kaspersky Anti-Virus dans un magasin, la clé de licence se trouve sur la disquette. Vous devrez l'introduire dans le lecteur et y accéder (cf. ill. 1).



Ilustration 1. Sélection du chemin d'accès au fichier de clé de licence

- Si vous avez acheté la licence en ligne, vous devrez enregistrer le fichier de clé de licence reçu par courrier électronique dans un répertoire du disque dur. Vous devrez ensuite indiquer le chemin d'accès à ce répertoire.

b. La liste des clés de licence disponibles apparaît à l'écran.

c. Sélectionnez la clé de licence nécessaire (fichier **.key**) et cliquez sur **Ouvrir** (cf.ill. 2).

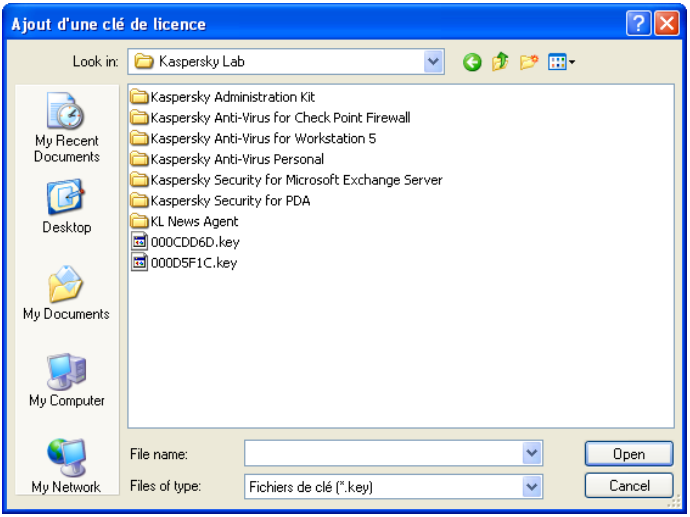


Illustration 2. Sélection du fichier de clé de licence

La fenêtre de l'Assistant d'installation reprendra les informations générales sur la licence et sur le chemin d'accès à celle-ci.

Cliquez sur **Suivant >** pour poursuivre l'installation.

Si vous ne disposiez pas encore de la clé de licence au moment de l'installation du logiciel (ex. : vous l'avez commandée par Internet chez Kaspersky Lab mais ne l'avez pas encore reçue), sachez qu'il est possible de l'activer ultérieurement lorsque vous lancerez le programme ou à l'aide de l'utilitaire spécial d'installation de la clé de licence (cf. Chapitre 12 à la page 78). N'oubliez pas qu'il est impossible d'utiliser Kaspersky Anti-Virus® sans cette clé.

Etape 9. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le dossier dans lequel vous souhaitez installer Kaspersky Anti-Virus®. Il s'agit par défaut de :

<Disque>\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus Personal.

Vous pouvez modifier le chemin manuellement ou l'indiquer en cliquant sur **Parcourir** dans la boîte de dialogue standard de sélection du dossier.

Si vous réalisez une mise à jour au départ de Kaspersky Anti-Virus Personal 5.0, il vous sera proposé de procéder à l'installation dans le même répertoire (option recommandée). Vous pouvez néanmoins choisir un autre répertoire. Dans ce cas, les fichiers de la version précédente resteront sur le disque et ils seront supprimés uniquement lors de la suppression complète du logiciel.

Pour poursuivre l'installation, cliquez sur **Installer**. Vous lancerez ainsi la copie des fichiers de Kaspersky Anti-Virus® Personal sur votre ordinateur.

Etape 10. Fin de la procédure d'installation

La boîte de dialogue **Fin de l'installation** reprend les informations relatives à la fin de l'installation de Kaspersky Anti-Virus® Personal sur votre ordinateur.

Si l'enregistrement d'une série de services dans le système est indispensable en vue de terminer l'installation, un message vous invitera à redémarrer l'ordinateur. Cette étape est INDISPENSABLE pour terminer correctement l'installation du logiciel.

Pour conclure l'installation du logiciel :

1. Choisissez l'une des deux options :
   - **Redémarrer maintenant**
   - **Je souhaite redémarrer moi-même plus tard**
2. Cliquez sur **Terminer**.

Lorsqu'il n'est pas nécessaire de redémarrer l'ordinateur en vue d'achever la procédure d'installation :

1. Décochez la case **Lancer Kaspersky Anti-Virus Personal 5.0** si vous ne souhaitez pas activer la protection antivirus de votre ordinateur directement après la fin de l'installation.

Si vous décochez cette case, la protection antivirus de votre ordinateur sera lancée automatiquement après le redémarrage de votre ordinateur. Il est possible d'activer la protection antivirus au départ du menu principal de Microsoft Windows (**Démarrer → Programmes → Kaspersky Anti-Virus Personal**)

2. Cliquez sur **Terminer**.

Suite à l'installation et au lancement de Kaspersky Anti-Virus:

- L'icône de l'application  sera reprise dans la barre des tâches.
- Les liens du logiciel seront ajoutés au menu principal de Windows (**Démarrer → Programme → Kaspersky Anti-Virus Personal**).

CHAPITRE 3. QUE FAIRE EN CAS D'INFECTION DE L'ORDINATEUR

Il est parfois difficile pour une personne non avertie de découvrir la présence de virus 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.

3.1. Signes d'une infection

Il existe toute une série d'indices qui peuvent laisser présager de 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/de DVD ;
- 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 ne soyez à l'origine d'un tel comportement ;

Si vous remarquez n'importe lequel des susdits signes, vous êtes alors plus que probablement victime d'un virus informatique.

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

- 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 " gèle " ou se comporte bizarrement (ex. :impossible de fermer les fenêtres du logiciel).

Dans la majorité 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 procéder à une analyse complète de votre ordinateur selon les paramètres définis par les experts de Kaspersky Lab dès qu'ils se manifestent.

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

Si vous remarquez que votre ordinateur a un comportement suspect :

2. 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.
3. Déconnectez l'ordinateur d'Internet.
4. Le cas échéant, déconnectez l'ordinateur du réseau local.
5. 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 Microsoft Windows que vous avez créé au moment de l'installation du système d'exploitation.

6. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD, une carte Flash, etc.

Avant de transférer les données enregistrées sur l'ordinateur réparé, il est vivement recommandé de les analyser à l'aide de Kaspersky Anti-Virus (cf. Chapitre 7 à la page 61).

7. Installez Kaspersky Anti-Virus® Personal.

8. Téléchargez les dernières mises à jour des bases antivirus. Dans la mesure du possible, réalisez cette opération depuis l'ordinateur sain d'un ami, d'un cybercafé ou du travail. Il est en effet préférable d'utiliser un autre ordinateur car si le vôtre 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 ou du réseau local 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. Il est possible également d'obtenir les mises à jour des bases antivirus sur une disquette ou sur un disque en s'adressant à Kaspersky Lab ou à l'un de ses distributeurs. Dans ce cas, la mise à jour s'effectue localement (pour de plus amples informations, consultez le point 13.4 à la page 85).

9. Sélectionnez le niveau de protection recommandé par les experts de Kaspersky Lab (cf. point 6.2, p. 48).

10. Lancez l'analyse complète de votre ordinateur (cf. point 6.3, p. 53).

CHAPITRE 4. PROTECTION DE L'ORDINATEUR SANS CONFIGURATION COMPLEMENTAIRE DE KASPERSKY ANTI-VIRUS

Vous pouvez commencer à utiliser Kaspersky Anti-Virus® Personal directement après son installation sans avoir à réaliser de configuration car le logiciel contient par défaut des configurations optimales définies et recommandées par les experts de Kaspersky Lab. Le niveau de protection antivirus ainsi obtenu assure un équilibre parfait entre l'efficacité de la protection et la rapidité de votre ordinateur.

Vous trouverez ci-après une description du fonctionnement de Kaspersky Anti-Virus® en fonction des différentes recommandations des experts.

4.1. Protection en temps réel

La protection en temps réel de votre ordinateur est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du programme.

La protection en temps réel est enclenchée dès le démarrage du système d'exploitation et jusqu'à ce que l'ordinateur soit éteint. L'icône rouge  de la barre des tâches indique que le logiciel tourne.

Dès le démarrage de l'ordinateur, Kaspersky Anti-Virus® analyse *les objets exécutés au démarrage*, la *mémoire de l'ordinateur* et ses *propres modules*. Ensuite, il procède à l'analyse des objets ouverts, enregistrés et exécutés.

Par défaut, la protection en temps réel fonctionne conformément à la configuration définie par les spécialistes de Kaspersky Lab, à savoir :

- L'analyse antivirus porte uniquement sur les objets ouverts, sauvegardés et exécutés du disque dur ou des disques amovibles de l'ordinateur *qui pourraient être infectés*, c'est-à-dire :
    - *Les secteurs d'amorçage des disques* (ces objets sont analysés directement après le démarrage du logiciel) ;

- *Les fichiers compactés* et les objets associés ou intégrés à d'autres fichiers *(les objets OLE)* ;
- Les messages entrants.

La protection en temps réel ignore les fichiers qui ne peuvent pas contenir de virus.

- En cas de découverte d'un *objet infecté*, l'accès à celui-ci est bloqué et une boîte de dialogue reprenant les options de traitement apparaît à l'écran ;
- En cas de découverte d'un *objet potentiellement infecté par un virus ou l'une de ses variantes*, le logiciel en bloque l'accès et vous consulte sur la suite des événements ;
- En cas de découverte d'une *attaque de réseau*, le logiciel affiche le message de circonstance et bloque l'attaque ;
- Les résultats des différentes opérations sont consignés dans le rapport (cf. point 14.8, p. 105).

La protection en temps réel peut être suspendue pour une période définie ou complètement désactivée. Les experts de Kaspersky Lab vous conseillent vivement de ne jamais désactiver la protection en temps réel car cela augmente considérablement la probabilité d'une infection. Si vous devez malgré tout désactiver la protection en temps réel pour une raison quelconque, faites-le uniquement pour une période définie.

Il est possible de désactiver la protection en temps réel pour une période définie, pour ce faire :

1. Faites un clic droit sur l'icône  dans la barre des tâches.
2. Sélectionnez **Arrêter la protection en temps réel** dans le menu contextuel qui apparaît.
2. Dans la fenêtre qui s'ouvre, sélectionnez la durée souhaitée de la désactivation. Pour de plus amples informations, consultez le point 8.3 à la page 68.

La protection en temps réel sera interrompue. Pour confirmer ce changement d'état, l'icône  (de couleur rouge) est remplacée par l'icône  (de couleur grise).

4.2. Analyse de l'ordinateur à la demande

La fonction **Analyse à la demande** vous permet de rechercher la présence éventuelle de virus sur votre ordinateur, sur des disques ou dans des répertoires ou des fichiers particuliers. Cette analyse s'opère par défaut selon la configuration recommandée par les spécialistes de Kaspersky Lab.

- En cas d'analyse complète de votre ordinateur, la recherche d'éventuels virus porte sur la *mémoire vive* de l'ordinateur sollicitée par les processus lancés et touche tous les objets du disque dur de l'ordinateur, notamment :
  - *Les objets exécutés au démarrage du système d'exploitation et les secteurs d'amorçage* ;
  - *Les archives, les modules exécutables et les archives auto-extractibles* ;
  - Les objets intégrés ou associés à d'autres fichiers (*objets OLE*);

  Les boîtes aux lettres utilisées ne sont pas analysées lors de l'analyse complète.

- En cas d'analyse d'un disque, d'un répertoire ou d'un fichier particulier, la recherche d'éventuels virus porte sur tous les fichiers de la zone d'analyse, à savoir :
  - *Les archives, les fichiers exécutables et les archives auto-extractibles* ;
  - Les objets associés ou intégrés à *d'autres* fichiers (les *objets OLE*).
- La liste des objets dangereux traités à la fin de l'analyse; les actions envisageables sont reprises pour chaque objet ;.
- Les résultats des différentes opérations sont consignés dans le rapport (cf. point 14.8, p. 105).

Par défaut, l'analyse complète de votre ordinateur aura lieu automatiquement chaque vendredi à 20h00. Le texte  **L'analyse complète de votre ordinateur est en cours…** qui apparaît dans la partie droite de l'onglet **Protection** (cf. ill. 5) témoigne de l'exécution de l'analyse complète.

Si votre ordinateur n'est pas allumé à cette heure, l'analyse ne sera pas réalisée.

Il est possible de lancer manuellement une analyse complète. Pour ce faire :

Cliquez avec le bouton droit de la souris sur l'icône dans la barre des tâches. Sélectionnez **Analyser mon Poste de travail** dans le menu contextuel qui apparaît.

Ou :

Sélectionnez l'onglet **Protection** dans la fenêtre principale du logiciel et cliquez sur le lien Analyser le Poste de travail dans la partie gauche.

4.3. Mise à jour des bases antivirus

Une base de données reprenant les définitions de virus, c'est-à-dire l'ensemble des informations sur les programmes malicieux connus à ce jour et les moyens disponibles pour réparer les objets dangereux, sert de référence à l'analyse antivirus et à la réparation des objets infectés.

Comme de nouveaux virus font leur apparition chaque jour, il est primordial de maintenir l'actualité de ces bases.

La **Mise à jour des bases antivirus** est une autre fonction capitale remplie par Kaspersky Anti-Virus®. Par défaut, ces bases sont téléchargées depuis les serveurs de mises à jour de Kaspersky Lab et installées sur votre ordinateur toutes les 3 heures. Si vous utilisez votre ordinateur moins de 3 heures par jour, les bases antivirus seront actualisées lors du prochain lancement de Kaspersky Anti-Virus.

Il est possible de procéder à la mise à jour manuelle des bases antivirus. Pour ce faire :

Faites un clic droit sur l'icône dans la barre des tâches. Sélectionnez **Mettre à jour les bases antivirus** dans le menu contextuel qui apparaît à l'écran.

Ou :

Sélectionnez l'onglet **Protection** (cf. ill. 5) de la fenêtre principale du logiciel et cliquez sur le lien Mettre à jour maintenant dans la partie gauche.

Ou :

Cliquez sur le lien mettre à jour les bases antivirus dans la partie droite de l'onglet **Protection**.

Pour de plus amples informations sur la mise à jour des bases antivirus, consultez le Chapitre 13 à la page 81.

CHAPITRE 5. INTERFACE DU LOGICIEL

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

5.1. Icône de la barre des tâches

Dès que le logiciel a été lancé, une icône dont l'apparence varie en fonction de l'état de la protection apparaît dans la barre des tâches.

Si l'icône est active (de couleur rouge) , cela signifie que tous les fichiers de votre ordinateur sont sous le contrôle de Kaspersky Anti-Virus. Si l'icône n'est pas active (grise) , cela signifie que la protection en temps réel des fichiers est désactivée (par exemple, si vous aviez suspendu la protection en temps réel, désactivé la protection en temps réel des fichiers ou décidé de ne pas l'utiliser au moment de l'installation).

Lorsque l'analyse d'un objet quelconque est en cours, un dossier bleu et blanc clignotant apparaît sous l'icône : / . Lors de l'analyse du courrier, le dossier est remplacé par une enveloppe . Pendant le téléchargement des mises à jour, l'icône devient .

Si l'animation de l'icône dans la barre des tâches n'a pas été sélectionnée dans les options avancées (cf. point 14.9, p. 111), l'icône n'aura qu'une seule apparence : active ou inactive.

Lorsqu'un événement important au niveau de la protection antivirus survient, un message reprenant les recommandations des experts de Kaspersky Lab apparaît au-dessus de l'icône (cf. ill. 3).

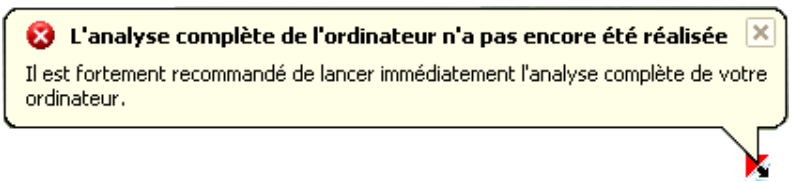


Illustration 3. Message d'informations

5.2. Menu contextuel

Un clic-droit sur l'icône dans la barre des tâches vous permettra d'afficher un menu contextuel (cf. ill. 4) proposant les éléments suivants :

- **Ouvrir Kaspersky Anti-Virus** : ouvre la fenêtre principale du logiciel à l'onglet **Protection**. Vous pouvez également cliquer sur l'icône  du programme dans la barre des tâches.
- **Passer en mode utilisateur/Passer en mode administrateur** : permute d'un mode de sécurité à l'autre.
- **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** : télécharge les dernières mises à jour des bases antivirus.
- **Rétablir la protection en temps réel / Arrêter la protection en temps réel** : active ou désactive pour un certain temps la protection en temps réel de l'ordinateur. Ce point figure dans le menu uniquement si vous avez décidé d'utiliser la protection en temps réel contre les fichiers au moment de l'installation de Kaspersky Anti-Virus Personal. Selon que la protection en temps réel sera activée ou non, l'icône de l'application changera.

  Il est conseillé de ne pas désactiver la protection en temps réel car cela augmente considérablement le risque d'infection de l'ordinateur par des virus.

- **A propos du produit** : affiche la fenêtre de renseignements comportant les principales informations sur Kaspersky Anti-Virus® Personal.
- **Quitter** : décharge Kaspersky Anti-Virus® Personal de la mémoire de votre ordinateur.

  L'élément **Quitter** est accessible uniquement si vous jouissez des privilèges d'administrateur sur l'ordinateur.

  Si vous travaillez avec un ordinateur tournant sous Windows 98/ME et que vous devez limiter le nombre d'utilisateurs pouvant administrer Kaspersky Anti-Virus, utilisez un mot de passe (cf. point 14.9 à la page 111).

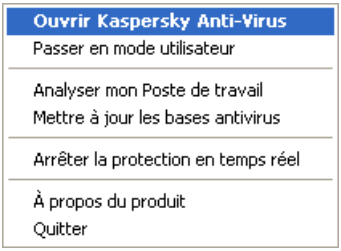


Illustration 4. Menu contextuel

5.3. Fenêtre principale du logiciel : structure générale

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

- Configurer la protection antivirus ;
- Lancer et interrompre la recherche d'éventuels virus ou autres programmes malveillants sur l'ordinateur, sur les disques, dans des répertoires ou des fichiers ;
- Télécharger les mises à jour des bases antivirus, des bases d'attaques de réseau et des modules de programme ;
- Configurer l'exécution automatique de l'analyse complète et des mises à jour ;
- Travailler avec les objets en quarantaine ;
- Manipuler les copies d'objets créées dans le dossier de sauvegarde avant leur réparation ou leur suppression;
- Consulter les rapports;
- Administrer les configurations du logiciel, etc.

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

- L'onglet **Protection** affiche les informations relatives à l'état des tâches liées à la protection antivirus (analyse des objets et mise à jour des bases antivirus). Vous pouvez, au départ de cet onglet, manipuler les objets en quarantaine ou dans le dossier de sauvegarde et consulter les rapports. Il s'agit de l'onglet qui apparaît en premier à chaque utilisation du logiciel (cf. point 5.3.1, p. 38).

- L'onglet **Paramètres** regroupe toutes les tâches liées à la configuration des principaux paramètres de la protection antivirus (cf. point 5.3.2, p. 40).
- L'onglet **Assistance technique** reprend les informations relatives à la clé de licence et à son renouvellement, ainsi que l'accès à l'aide et les coordonnées pour envoyer des requêtes au service d'assistance technique (cf. point 5.3.3, p. 41).

Chacun de ces onglets est divisé en deux parties :

- *La partie gauche* contient une liste de liens permettant d'exécuter les tâches incontournables de Kaspersky Anti-Virus. La composition de cette liste varie en fonction de l'onglet sélectionné.

Ainsi, pour l'onglet **Protection**, cette liste reprend toutes les tâches possibles en matière d'analyse antivirus de votre ordinateur. Sur l'onglet **Paramètres**, il s'agira des liens vers la configuration de ces différentes tâches tandis que l'onglet **Assistance technique** proposera toutes les tâches qui vous apporteront l'assistance dont vous avez besoin.

- La *partie droite* quant à elle affiche les renseignements sur l'état actuel de la protection antivirus de votre ordinateur (protection en temps réel, analyse à la demande, bases de données et renseignements sur la clé de licence).

L'onglet **Protection** affiche l'état de la protection antivirus, l'onglet **Paramètres** reprend les informations sur la configuration et l'onglet **Assistance technique** vous renseigne sur la clé de licence, fournit des liens vers le Service d'assistance technique et procure des informations sur le logiciel et votre système d'exploitation.

Il existe quatre états de la protection antivirus qui sont repris dans les onglets **Protection** et **Paramètres**. Ils sont représentés par les symboles suivants :

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.

La protection antivirus a été suspendue. Cet état indique que la protection antivirus de votre ordinateur a été temporairement suspendue.

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 indispensable 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.

Les informations présentées dans la partie droite de l'onglet concernent dans l'ordre : la protection en temps réel, l'analyse à la demande et le degré d'actualité des bases antivirus.

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 celui-ci sous prétexte qu'il confère une meilleure protection à votre ordinateur.

5.3.1. Onglet *Protection*

C'est au départ de l'onglet **Protection** (cf. ill. 5) que vous lancerez les tâches d'analyse de votre ordinateur ou de disques, de dossiers ou de fichiers particuliers. Vous pourrez :

- Lancer la mise à jour des bases antivirus, des modules de l'application et des bases d'attaque de réseaux ;
- Manipuler les rapports sur l'exécution de toutes les tâches lancées (consultation, suppression, exportation) ;
- Manipuler les objets potentiellement infectés par un virus ou l'une de ses modifications et mis en quarantaine ;
- Manipuler les copies de sauvegarde des objets réparés ou supprimés.

Il est possible de lancer des tâches individuelles en cliquant sur le lien correspondant dans la partie gauche.

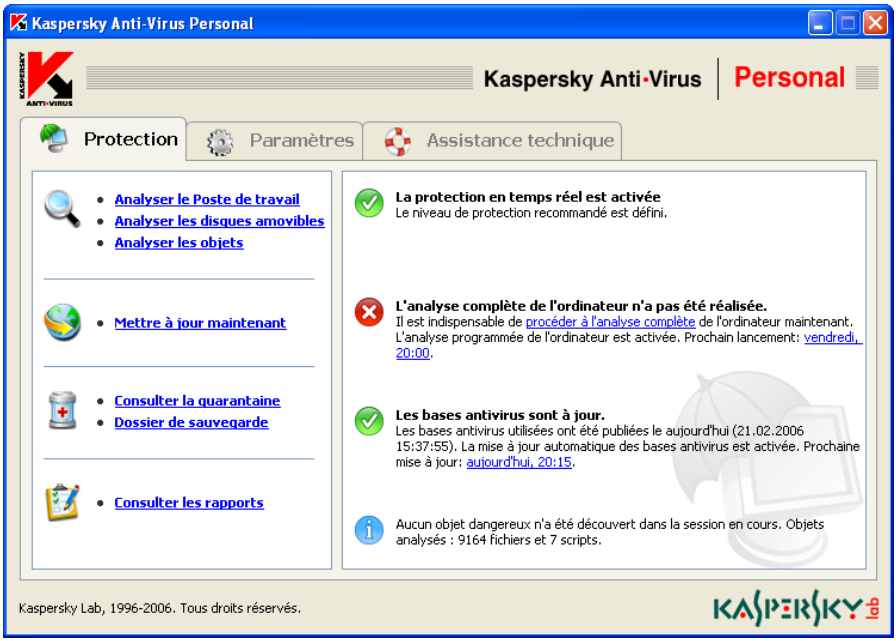


Illustration 5. Onglet **Protection**

La partie droite reprend *l'état actuel* de la *protection en temps réel*, de *l'analyse à la demande* et des *bases antivirus*. L'illustration 5 représente le cas de figure où l'analyse en temps réel de l'ordinateur est activée mais où l'analyse complète n'a pas encore été réalisée. Des commentaires sur l'état de chacune des tâches de la protection antivirus sont également proposés.

Les recommandations des experts de Kaspersky Lab seront toujours reprises lorsque le niveau de la protection antivirus est jugé critique ou différent du niveau recommandé. Pour accroître l'efficacité de la protection antivirus, vous aurez la possibilité de modifier la configuration actuelle, de rétablir la configuration recommandée par les experts de Kaspersky Lab, de lancer telle ou telle tâche, etc. Toutes ces suggestions apparaissent sous la forme d'un lien hypertexte qui vous conduira directement à l'action en question.

Vous pouvez toujours consulter les statistiques du logiciel dans la partie inférieure de l'onglet **Protection**. C'est ici que vous découvrirez le total des objets analysés au cours de cette séance et le nombre de riskwares découverts.

5.3.2. Onglet *Paramètres*

L'onglet **Paramètres** (cf. ill. 6) vous permet d'évaluer les configurations appliquées et de modifier les paramètres de base ou les options avancées qui régissent le fonctionnement de Kaspersky Anti-Virus® Personal.

Illustration 6. Onglet **Paramètres**

La partie droite indique la configuration actuelle de la protection en temps réel, de l'analyse à la demande et de la mise à jour automatique des bases antivirus, des modules de l'application et des bases des attaques de réseau connues. Ces informations sont accompagnées de commentaires détaillés et de conseils portant sur la modification de certains paramètres. Par exemple, si vous procédez manuellement à la mise à jour des bases antivirus, le logiciel vous proposera d'automatiser cette tâche et d'établir un horaire pour le lancement du téléchargement de la mise à jour.

Les liens repris dans la partie gauche vous permettent d'accéder directement aux fenêtres de configuration de la protection en temps réel, de l'analyse à la demande et des mises à jour. Vous pouvez également composer une liste d'objets exclus de la protection et indiquer le type de bases antivirus utilisées.

Vous pouvez également configurer la quarantaine où sont placés tous les objets potentiellement infectés par un virus ou l'une de ses variantes et le dossier de

sauvegarde, prévu pour le stockage des copies de sauvegarde des objets. Le lien Options avancées ouvre la fenêtre de configuration des paramètres complémentaires de Kaspersky Anti-Virus® Personal.

Kaspersky Anti-Virus vous permet de créer plusieurs configurations et de les enregistrer dans des fichiers spéciaux appelés *profils*. Par la suite, vous pourrez aisément revenir à l'une ou l'autre configuration. Il ne sera pas nécessaire de reconfigurer l'application mais uniquement de charger le profil requis. Cliquez sur Administration des profils pour créer et gérer les profils.

5.3.3. Onglet Assistance technique

L'onglet **Assistance technique** (cf. ill. 7) reprend toutes les informations relatives au Service d'assistance technique que vous pouvez contacter en cas de difficultés d'utilisation de Kaspersky Anti-Virus ou lorsque vous n'êtes pas en mesure de résoudre seul le problème auquel vous êtes confronté.

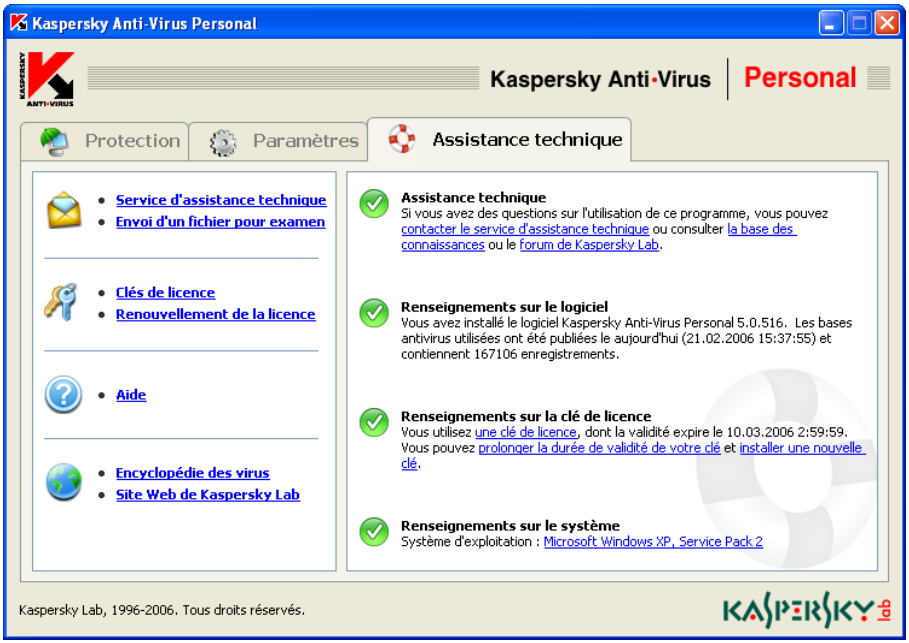


Illustration 7. Onglet **Assistance technique**

Cet onglet affiche également toutes les informations sur le logiciel, la clé de licence et le système d'exploitation installé sur votre ordinateur afin que toutes ces informations soit à votre portée en cas d'appel au Service d'assistance

technique de Kaspersky Lab. Tous ces renseignements figurent dans la partie droite.

La partie gauche propose des liens qui vous permettent de :

- Contacter le Service d'assistance technique et d'envoyer pour examen à Kaspersky Lab des objets potentiellement infectés par un virus ou l'une de ses modifications.
- Renouveler la licence d'utilisation de Kaspersky Anti-Virus® Personal (activer une nouvelle clé de licence).

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

- Le lien Aide ouvre des fenêtres d'aide générale sur l'utilisation du logiciel.
- Le lien Encyclopédie des virus vous emmène sur le site www.viruslist.com/fr 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.

5.4. Fenêtre du processus d'analyse

La fenêtre du processus d'analyse (cf. ill. 8) 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 en pour cent la progression de l'analyse, le nom de l'objet en cours d'analyse, l'heure estimée de fin, des statistiques générales sur le nombre d'objets analysés à ce stade ainsi que sur le nombre d'objets réparés, supprimés ou mis en quarantaine.
- La partie inférieure se déroule en cliquant sur le bouton  . Elle renferme trois onglets : **Statistiques**, pour les résultats 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. Pour refermer cette partie, il suffit de cliquer sur  .

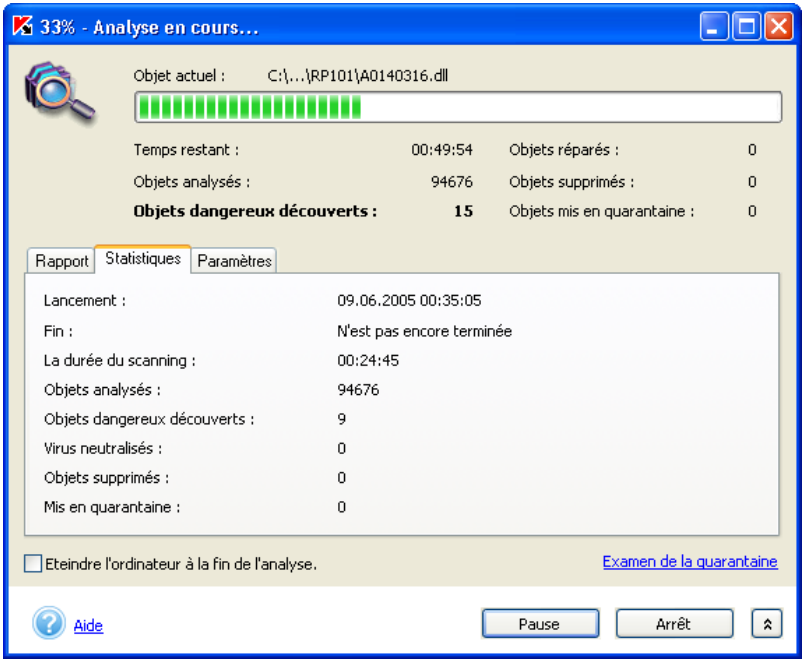


Illustration 8. Fenêtre du processus d'analyse

Pour de plus amples informations sur l'utilisation du rapport, consultez le point 14.8 à la page 105.

Si vous réalisez une analyse complète, vous pouvez également configurer, au départ de cette fenêtre, l'ordinateur afin qu'il s'éteigne à la fin de l'analyse. Ce mode est pratique pour ceux qui lancent une analyse antivirus à la fin de leur journée de travail et qui ne veulent pas attendre jusque la fin.

Toutefois, ce mode de fonctionnement nécessite une vérification préalable : il convient de s'assurer, avant le début de l'analyse, que la demande du mot de passe pour l'analyse des objets est désactivée (cf. point 14.4, p. 96) et il faut sélectionner le mode de traitement automatique des objets dangereux ou leur suppression ou mise en quarantaine ou la consignation des informations dans le rapport (cf. point 6.2, p. 48). Ces différents réglages suppriment l'interactivité dans l'utilisation du logiciel. Le logiciel n'affichera pas de boîtes de dialogue nécessitant une action de votre part et interrompant le processus d'analyse.

Pour éteindre l'ordinateur après l'analyse, cochez la case correspondante dans la fenêtre d'analyse.

5.5. Aide

Toutes les rubriques d'aide du logiciel sont accessibles via l'onglet **Assistance technique**. Il suffit de cliquer sur le lien Aide 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® Personal. Vous pourrez y lire une description détaillée des principales tâches de protection antivirus exécutées par Kaspersky Anti-Virus® Personal, 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 6. PREVENTION 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® Personal.
- Procédez à la mise à jour régulière des bases antivirus. Réalisez cette opération plusieurs fois par jour en cas d'épidémie (les bases antivirus sont publiées sur les serveurs de mises à jour de Kaspersky Lab immédiatement dans ce genre de situation).
- Etablissez la protection en temps réel au niveau recommandé par les experts de Kaspersky Lab. La protection en temps réel est active dès le démarrage de l'ordinateur et complique la tâche des virus qui souhaiteraient l'infecter.
- Appliquez les paramètres recommandés par les experts de Kaspersky Lab pour l'analyse complète de l'ordinateur et prévoyez son exécution au moins une fois par semaine.
- 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 via 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® Personal 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 : *Ne croyez pas 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'exploitation Microsoft 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.*

Règle N°8 : *Réduisez le risque de mauvaises surprises en cas d'infection :*

- Réalisez régulièrement des copies de sauvegarde de vos données. Celles-ci vous permettront de restaurer assez rapidement le système en cas de perte de données. Conservez en lieu sûr les CD et les disquettes d'installation ainsi que tout média contenant des logiciels et des informations de valeur.

- Créez une disquette de démarrage qui vous permettra, le cas échéant, de redémarrer l'ordinateur à l'aide d'un système d'exploitation " sain ".

Règle N°9 : *Consultez régulièrement la liste des programmes installés sur votre ordinateur*. Utilisez pour ce faire l'option **Ajouter/supprimer des programmes** du **Panneau de configuration** ou vérifiez simplement le contenu du répertoire **Program Files** et du répertoire de démarrage automatique. Vous pourrez ainsi découvrir des logiciels qui auraient été

installé sur l'ordinateur à votre insu, par exemple pendant que vous étiez connecté à Internet et que vous aviez installé un programme quelconque. Il est probable que certains d'entre eux soient des programmes malicieux.

6.1. Quand faut-il lancer une analyse antivirus de l'ordinateur ?

Grâce à Kaspersky Anti-Virus® Personal, vous pouvez réaliser soit une analyse complète de l'ordinateur, une analyse de disques, de fichiers ou de répertoires particuliers, du courrier, de la mémoire système, des objets de démarrage ou des secteurs d'amorçage.

Dans le cadre de l'analyse complète, les boîtes aux lettres, les disques amovibles et les disques de réseau (s'ils sont connectés à votre ordinateur) sont ignorés.

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® Personal veille particulièrement à ce que les analyses portent sur tout l'ordinateur.

L'analyse complète est capable d'analyser un nombre 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® Personal dans la barre des tâches (pour autant que cette option n'ait pas été désactivée, cf. point 14.9, p. 111).

Pour obtenir de plus amples informations, il suffira d'ouvrir la fenêtre principale de l'application et de sélectionnez l'onglet **Protection** (cf. ill. 5). La partie droite reprend l'état exact de l'analyse complète. Il existe trois états possibles :

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 récemment ou est en cours d'exécution.

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

Les experts de Kaspersky Lab vous conseillent de programmer le lancement de l'analyse complète (cf. point 6.4, p. 54). L'état de l'analyse indique notamment si ce mode est activé ou non.

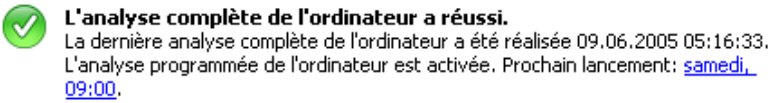


Illustration 9. Renseignements sur la nécessité de procéder à l'analyse complète

6.2. Configuration à utiliser pour l'analyse

Kaspersky Anti-Virus® Personal réalise l'analyse à la demande selon les paramètres recommandés par les experts de Kaspersky Lab (pour de plus amples informations, consultez le Chapitre 3 à la page 27). L'état de la configuration de l'analyse apparaît dans la partie droite de l'onglet **Paramètres** (cf. ill. 6) et est identifié par l'un des symboles suivants :

La configuration diffère de la configuration recommandée.

La configuration correspond à la configuration recommandée ou à la sécurité maximale.

Au besoin, il est possible de modifier les paramètres de la configuration par défaut. Pour n'importe quel type d'analyse (analyse complète ou analyse d'un des disques), vous pouvez modifier le niveau de la protection et les actions à exécuter en cas de découverte d'un objet infecté ou potentiellement infecté par un virus ou l'une de ses variantes.

N'oubliez pas que le niveau de protection que vous définissez, ainsi que les autres paramètres, sera COMMUN à l'analyse complète de l'ordinateur et à l'analyse de disques, de fichiers ou de répertoires distincts.

Si vous excluez de l'analyse à la demande un disque particulier (cf. point 14.2, p. 93), il vous sera impossible de l'analyser si vous le sélectionnez pour une analyse particulière (cf. point 6.5, p. 56).

Pour modifier le niveau d'analyse et/ou les actions à exécuter en cas de découverte d'un objet dangereux :

1. Cliquez sur le lien modifier la configuration dans le texte de la partie droite de l'onglet **Paramètres** ou sur Analyse à la demande dans la partie gauche.
2. Sélectionnez le *niveau d'analyse* qui vous convient dans la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 10). Le niveau **Recommandé** est le niveau appliqué par défaut. Pour le modifier, déplacez le curseur de l'échelle **Niveau d'analyse** vers le haut ou vers le bas. Voici une description des niveaux existants et des situations auxquelles ils sont le mieux adaptés.

   - **Sécurité maximale** pour l'analyse complète en profondeur de votre ordinateur ou d'un disque, d'un répertoire ou d'un dossier particulier.

     Ce niveau est recommandé lorsque vous pensez que votre ordinateur a été infecté par un virus. Pour une description détaillée des symptômes d'infection, consultez le point 3.1 à la page 27.

   - **Recommandé** pour l'analyse de l'ordinateur ou d'un objet sélectionné conformément aux paramètres recommandés par les experts de Kaspersky Lab.

     Ce niveau convient pour la majorité des situations car il assure un équilibre optimal entre la vitesse de l'analyse et la quantité d'objets analysés.

   - **Vitesse maximale** pour la rapidité de l'analyse antivirus de l'ordinateur ou d'un objet sélectionné.

     La vitesse de l'exécution de l'analyse est obtenue au détriment du nombre d'objets analysés.

   Le tableau ci-après reprend tous les objets sur lesquels peut porter l'analyse antivirus. Le signe **+** indique que le niveau d'analyse prend en charge cet objet, tandis que le signe **-** indique que l'objet n'est pas analysé à ce niveau.

	Sécurité maximale	Recommandé	Vitesse maximale
Secteur, défini par l'utilisateur (ordinateur, disque, fichier, etc.)	+	+	+[3]
Secteurs d'amorçage, mémoire	+	+	+
Objets OLE	+	+	+
Fichiers compactés	+	+	+
Archives auto-extractibles	+	+	+
Objets, exécutés au démarrage du système d'exploitation	+	+	–
Archives	+	+	–
Base de données de messagerie et messages	+	–	–

Il est possible de définir des *exclusions*, c'est-à-dire des objets qui ne seront pas analysés (cf. point 14.4, p. 96), pour chacun de ces niveaux de protection. Ceci étant dit, ces exclusions devraient être définies uniquement pour des cas particuliers.

3. Précisez l'action que le logiciel exécutera à chaque découverte d'un objet dangereux :

Confirmer l'action à la fin de l'analyse : le logiciel affiche la liste des objets infectés ou potentiellement infectés à la fin de l'analyse

[3] La recherche d'éventuels virus porte uniquement sur les objets potentiellement infectés.

dans une fenêtre spéciale. Ce mode est activé par défaut et ne requiert pas votre présence permanente à proximité de l'ordinateur. Dans la mesure où une analyse peut durer longtemps ce mode vous permet d'économiser le temps que vous passez à utiliser Kaspersky Anti-Virus.

- **Confirmer l'action auprès de l'utilisateur** : le logiciel affiche une boîte de dialogue vous permettant de décider de la suite des opérations. Cette boîte de dialogue reprend toutes les options possibles, dont une recommandée par les experts de Kaspersky Lab. Sélectionnez ce mode si vous avez l'intention de rester à proximité de votre ordinateur pendant l'analyse.
- **Exécuter l'action recommandée** : exécute l'action recommandée par les experts de Kaspersky Lab. Celle-ci est toujours fondée, si bien que ce mode est adapté dans la majorité des cas. Les recommandations sont les suivantes :

  - *Réparer* l'objet infecté ;
  - *Mettre* l'objet potentiellement infecté par un virus ou l'une de ses variantes *en quarantaine*.

    Parfois, lorsqu'un objet a été mis en quarantaine, un message apparaît et vous informe que l'objet ne peut être supprimé. Ceci s'explique par le fait que les objets mis en quarantaine sont déplacés : ils sont copiés dans la quarantaine et supprimés de leur emplacement d'origine. Toutefois, il n'est pas toujours possible de supprimer l'objet lors du déplacement. C'est le cas par exemple pour les objets utilisés à ce moment par une autre application.

  - *Supprimer* l'objet dangereux en cas d'échec ou d'impossibilité de la réparation.

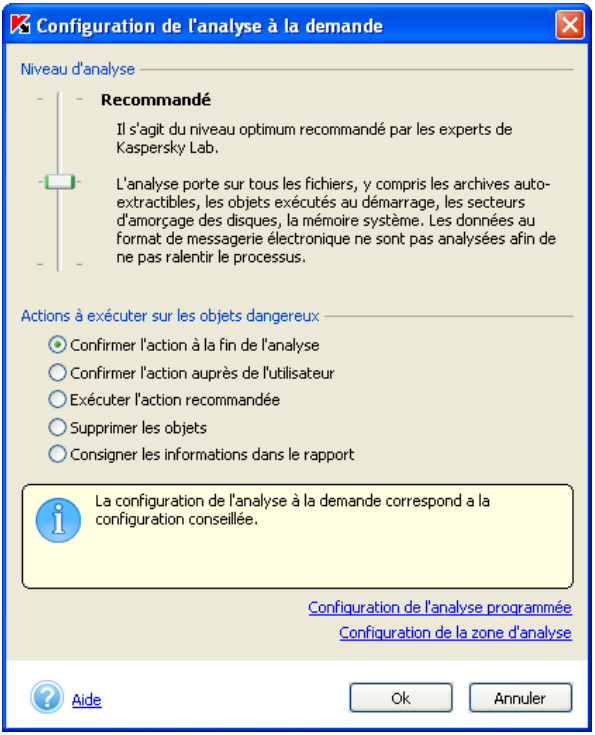


Illustration 10. Configuration de l'analyse à la demande

- **Supprimer les objets dangereux** assure la suppression des objets dangereux découverts pendant l'analyse sans tenter de réparation ni demander de confirmation auprès de l'utilisateur. Une copie de l'objet supprimé sera conservée dans le dossier de sauvegarde. Nous vous conseillons d'adopter ce mode uniquement si vous êtes certain de ne pas perdre d'informations cruciales.
- **Consigner les informations dans le rapport** : aucune action n'est réalisée et les informations relatives à l'infection sont simplement consignées dans le rapportt. Il est conseillé d'utiliser ce mode avec parcimonie car il ne débarrasse pas votre ordinateur des objets infectés et des programmes malicieux.

Il peut arriver qu'il soit impossible d'exécuter l'action sur l'objet. C'est le cas, par exemple, lorsque l'objet infecté utilise une autre application au moment de l'analyse et qu'il est impossible de le traiter à ce moment. Un message apparaîtra alors à l'écran (cf. ill. 11) et proposera les actions suivantes:

- *Réparer lors du redémarrage de l'ordinateur*. Cette action est exécutée uniquement lorsque la réparation de l'objet est possible ;
- *Supprimer lors du redémarrage de l'ordinateur* ;
- *Ignorer*. Aucune action n'est réalisée et les informations sont simplement consignées dans le rapport.

Si vous fermez la boîte de dialogue en cliquant sur dans le coin supérieur gauche, l'action que vous auriez sélectionnée dans cette fenêtre ne sera pas exécutée et l'objet sera ignoré.

Illustration 11. La réparation immédiate de l'objet est impossible

Le traitement des objets lors du démarrage (qu'il s'agisse de la réparation ou de la suppression) ne peut s'opérer qu'une fois les opérations d'analyses terminées. Si vous interrompez l'analyse qui a permis de découvrir ces objets, ceux-ci ne seront ni réparés, ni supprimés.

6.3. Analyse à la demande

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. ill. 5).

La fenêtre d'analyse (cf. ill. 8) apparaît à l'écran. Elle reprend la progression en pour cent de la tâche, le nom de l'objet en cours d'analyse, l'heure estimée de fin, des statistiques générales sur le nombre d'objets analysés à ce stade ainsi que sur le nombre d'objets réparés, supprimés ou mis en quarantaine.

Vous pouvez fermer la fenêtre d'analyse (cf. ill. 8) en cliquant sur dans le coin supérieur droit ou en sélectionnant l'option **Fermer la fenêtre, poursuivre l'analyse** dans la fenêtre qui s'ouvre.

Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 14.8 à la page 105).

6.4. Analyse complète programmée

Vous pouvez programmer l'analyse complète de l'ordinateur. Par exemple, si vous prenez votre pause déjeuner à 14h00, vous pouvez décider de lancer l'analyse complète automatiquement à cette heure. Pour ce faire, vous devez avant tout définir l'horaire de lancement de l'analyse.

Pour établir l'horaire de lancement de l'analyse de l'ordinateur :

1. Cliquez sur le lien Analyse à la demande dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).
2. Cliquez sur le lien Configuration de l'analyse programmée dans la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 10).
3. Définissez la fréquence d'exécution de la tâche dans la fenêtre **Configuration de l'analyse programmée** (cf. ill. 12) :

   - **Analyser avec un intervalle de jours** : l'analyse aura lieu tous les X jours. Par défaut, l'analyse est lancée tous les jours à 20h00. Si vous souhaitez réduire la fréquence de l'analyse et/ou modifier l'heure de lancement, rendez-vous dans la section **Paramètres d'analyse** et sélectionnez l'intervalle désiré dans la liste déroulante du champ **Tous les**. Précisez dans le champ **Début de l'analyse** l'heure à laquelle l'analyse débutera.
   - **Analyser les jours définis de la semaine** : procède à l'analyse certains jours de la semaine. Par défaut, l'analyse est exécutée chaque vendredi à 20h00. Pour changer la fréquence de l'analyse, rendez-vous dans la section **Paramètres d'analyse** afin de sélectionner les jours de la semaine puis définissez l'heure de lancement dans le champ **Début de l'analyse**.

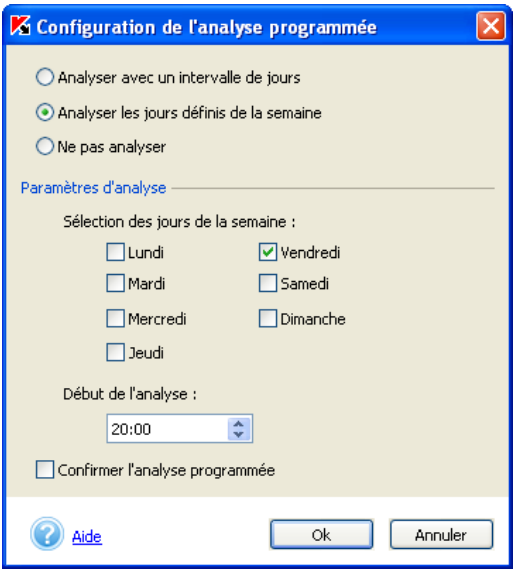


Illustration 12. Configuration de l'analyse programmée

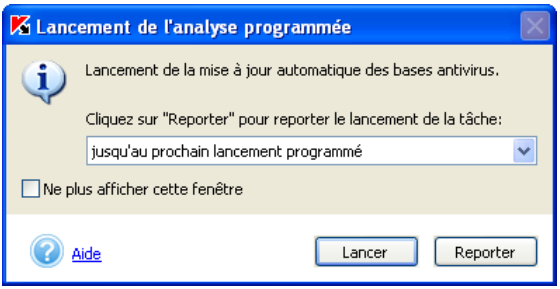


Illustration 13. Confirmation du lancement de la tâche programmée

Ne pas analyser : l'analyse programmée n'est pas réalisée. Il conviendra dans ce cas de lancer l'analyse complète manuellement.

Confirmer l'analyse automatique : active la notification du lancement de l'analyse programmée de l'ordinateur. Si cette case est cochée, la boîte de dialogue **Lancement de l'analyse programmée** (cf. ill. 13) s'affichera avant le lancement de l'analyse. Cliquez sur **Lancer** si vous souhaitez lancer l'analyse programmée. Pour remettre l'analyse à plus tard, sélectionné le report souhaité et cliquez sur **Reporter**. Si

aucune décision n'est prise après trois minutes, la tâche sera lancée automatiquement.

- **Charge minimum de la batterie pour lancer l'analyse programmée** – annule le lancement de l'analyse à la demande sur un ordinateur portable lorsque la charge de la batterie est inférieure à la valeur prescrite. Vous pouvez définir, à l'aide du curseur **ou** directement dans le champ prévu à cet effet, la valeur de la charge minimum de la batterie (en %) en-deçà de laquelle le lancement de l'analyse programmée n'aura pas lieu.

  Cette option est accessible uniquement lorsque Kaspersky Anti-Virus est installé sur un ordinateur portable et que celui-ci tourne sur sa batterie.

4. Cliquez sur **OK**.

6.5. Analyse d'objets individuels

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® Personal ou à l'aide des méthodes traditionnelles du système d'exploitation Microsoft Windows (via l'**Assistant** ou sur le **Bureau**, etc.).

Pour analyser l'objet sélectionné au départ de Microsoft Windows :

Placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 14).

Suivez les instructions fournies ci-après pour choisir et analyser un objet sans quitter Kaspersky Anti-Virus® Personal.

Pour sélectionner l'objet à analyser au départ de Kaspersky Anti-Virus® :

Cliquez sur le lien Analyser les objets dans la partie gauche de l'onglet **Protection** (cf. ill. 5).

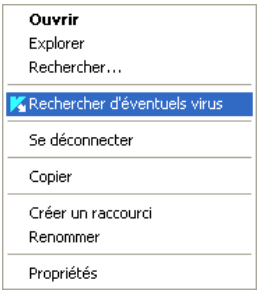


Illustration 14. Analyse antivirus d'un objet sélectionné à l'aide des outils Microsoft Windows

La boîte de dialogue **Sélection des objets à analyser** (cf. ill. 15) 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.

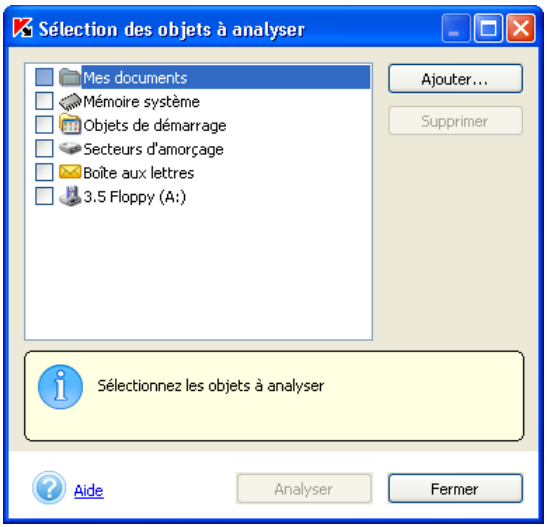


Illustration 15. Sélection des objets à analyser

La liste originale reprend les éléments suivants :

- Les disques amovibles (y compris les disquettes et les CD-rom) ;
- Les disques durs ;
- Les boîtes aux lettres Microsoft Office Outlook et Microsoft Outlook Express ;

- Le dossier **Mes documents**,
- La mémoire système;
- Les objets de démarrage ;
- Les secteurs d'amorçage des disques.

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, sélectionnez-le 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. Sélectionnez les objets dans la liste ;
2. Cliquez sur **Analyser**.

Quel que soit le moyen utilisé pour lancer l'analyse d'un objet (via le menu contextuel de Microsoft Windows ou au départ de la liste des objets de Kaspersky Anti-Virus® Personal), la boîte de dialogue **Analyse** (cf. ill. 8) 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 14.8 à la page 105).

6.6. Analyse des archives

Kaspersky Anti-Virus® Personal analyse les archives lorsque les niveaux **Sécurité maximale** ou **Recommandé** ont été sélectionnés pour autant que leur analyse n'ait pas été désactivée (cf. point 14.2, p. 93).

Kaspersky Anti-Virus® Personal analyse tous les objets à l'intérieur des archives et répare uniquement les objets dans les archives *zip, arj, cab, rar, lha et ice*. Kaspersky Anti-Virus® NE REPARE PAS les archives auto-extractibles !

Au cas où l'objet à l'intérieur de l'archive serait protégée par un mot de passe, et pour autant que le mode de requête du mot de passe soit activé, une boîte de dialogue pour la saisie du mot de passe (cf. ill. 16) apparaîtra avant son analyse.

Si le mode de traitement différé des objets a été sélectionné (l'option **Confirmer l'action à la fin de l'analyse** a été sélectionnée dans les paramètres, cf. point 6.2 à la page 48), le mot de passe sera demandé à la fin de l'analyse.

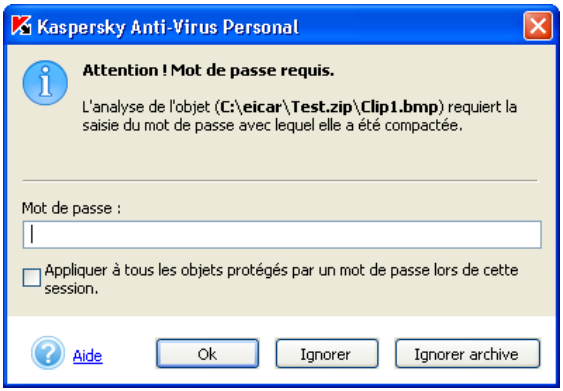


Illustration 16. Saisie du mot de passe pour l'analyse d'une archive

La case ☐ **Ne pas demander le mot de passe lors de l'analyse des objets**, dans les paramètres de configuration de l'analyse, permet d'afficher ou non la fenêtre de saisie du mot de passe (cf. point 14.2, p. 93).

Saisissez le mot de passe d'accès à l'objet ou à l'archive dans le champ **Mot de passe** puis cliquez sur **OK**. Cela marquera le début de l'analyse antivirus de l'archive et de tous les objets qu'elle contient.

Si Kaspersky Anti-Virus® découvre à l'intérieur de l'archive un autre objet protégé par un mot de passe, il tentera d'utiliser le mot de passe saisi pour le premier objet. 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.

Cliquez sur **Ignorer** pour ne pas analyser un objet individuel protégé par un mot de passe inclus dans une archive.

Si vous ne connaissez pas le mot de passe, l'analyse de l'archive protégée et de tous les objets qu'elle contient sera impossible. Il est recommandé dans ce cas de cliquer sur **Ignorer archive** et de poursuivre.

La case ☐ **Appliquer à tous les objets protégés par un mot de passe lors de cette session** concerne l'action que vous sélectionnerez par la suite.

Ainsi, si vous cochez la case et que vous sélectionnez **Ignorer archive**, aucune des archives protégées par un mot de passe ne sera soumise à l'analyse antivirus durant la session en cours.

Si vous saisissez le mot de passe, cochez la case et cliquez sur **OK**, le mot de passe en question sera appliqué automatiquement à tous les objets protégés par un mot de passe au sein de toutes les archives de cette session. Si le mot de passe n'est pas valide, les objets ne seront pas analysés.

Lors de la détection d'un objet infecté dans les archives, Kaspersky Anti-Virus traitera l'objet. Si le traitement n'est pas possible, l'objet sera supprimé de l'archive.

Si l'archive est incurable et si vous avez configuré l'analyse antivirus à l'aide de la fonction **Exécuter l'action recommandée**, lors d'une détection d'une archive incurable, l'antivirus ne la supprimera pas, mais informera l'utilisateur dans le rapport.

Si vous avez configuré l'analyse antivirus à l'aide de la fonction **Confirmer l'action à la fin de l'analyse** ou **Confirmer l'action auprès de l'utilisateur** (voir 6.2 page 48), l'anti-virus pourra supprimer l'archive incurable, en choisissant l'option **Supprimer** dans la fenêtre de dialogue (voir Illustration 21). De plus, vous aurez la possibilité de supprimer manuellement l'archive en question.

CHAPITRE 7. ANALYSE D'UN DISQUE AMOVIBLE

Votre ordinateur peut facilement être infecté par un virus introduit via une disquette, un CD ou un autre disque amovible. Si la disquette (ou le cédérom) 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® Personal ou depuis le menu contextuel de Microsoft Windows ouvert via l'**Assistant** ou le **Bureau.**

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

Sélectionnez les disques (il est possible de sélectionner directement le CD et la disquette), ouvrez le menu contextuel de Microsoft Windows d'un clic droit et choisissez **Rechercher d'éventuels virus** (cf. ill. 14).

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

1. Introduisez le CD ou la disquette dans le lecteur. Le logiciel est en mesure d'analyser le CD et la disquette en une session.
2. Cliquez sur le lien Analyser les disques amovibles dans la partie gauche de l'onglet **Protection** (cf. ill. 5).

Ou

Cliquez sur le lien Analyser les objets pour ouvrir la boîte de dialogue **Sélection des objets à analyser** (cf. ill. 15) puis, sélectionnez les disques amovibles et cliquez sur **Analyser**.

La fenêtre **Analyse** (cf. ill. 8) apparaît à l'écran dès le lancement de l'analyse et illustre la progression de la tâche pour les objets sélectionnés dans la liste.

Si vous avez sélectionné un seul disque amovible, Kaspersky Anti-Virus® Personal vous proposera d'introduire le suivant à la fin de l'analyse.

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 lecteur de 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.

Lorsque le disque amovible est monté dans le système d'exploitation (lorsque celui-ci définit le disque en tant que nouveau périphérique), Kaspersky Anti-Virus recherche d'éventuels virus d'amorçage sur ce disque, pour autant que la protection en temps réel soit activée.

CHAPITRE 8. CONFIGURATION DE LA PROTECTION EN TEMPS REEL

La protection en temps réel de votre ordinateur est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du programme.

La *protection en temps réel* signifie que Kaspersky Anti-Virus® Personal surveille de près toutes les actions qui peuvent se révéler dangereuses pour la *protection* antivirus et la sécurité du réseau. Parmi celles-ci, citons l'ouverture d'un fichier, l'enregistrement des modifications apportées à un fichier, l'examen du courrier entrant et sortant ainsi que l'exécution des fichiers sur l'ordinateur ou des scénarios dans Microsoft Internet Explorer. Lorsque vous, ou l'ordinateur, tentez d'exécuter une de ses actions, Kaspersky Anti-Virus® intercepte le processus, analyse l'objet et en fonction des résultats obtenus autorise ou non l'action sollicitée ou affiche un message à l'écran.

8.1. Vérification de l'état de la protection

Toutes les informations relatives à l'état actuel de la protection en temps réel sont reprises sur le panneau de droite de l'onglet **Protection** (cf. ill. 5) de la fenêtre principale de Kaspersky Anti-Virus® Personal.

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 antivirus est suspendue. Cet état signifie que la protection de votre ordinateur a été temporairement désactivée.

La protection en temps réel est désactivée ou ne fonctionne pas. Dans le premier cas, il est conseillé de l'activer et dans le deuxième cas il faut configurer ses paramètres (cf. point 14.1, p. 91) et la lancer.

8.2. Actions réalisées par le logiciel et niveau de protection

Par défaut, la configuration de la protection en temps réel assurée par Kaspersky Anti-Virus® Personal correspond à la configuration recommandée. L'accès à tous les objets dangereux que vous avez voulu ouvrir, enregistrer ou modifier est bloqué et un message reprenant les options de traitement apparaît à l'écran.

N'oubliez pas qu'en mode de protection en temps réel, les archives et les bases de données de messagerie NE SONT PAS ANALYSES. Les archives auto-extractibles constituent la seule exception (du moins, la partie responsable du décompactage et non pas le contenu en lui-même), uniquement lorsque le niveau **Sécurité maximale** a été sélectionné.

Il est possible de définir pour la protection en temps réel le niveau de protection et les actions à exécuter en cas de découverte d'un objet dangereux.

Pour définir les actions exécutées par le logiciel en mode protection en temps réel suite à la découverte d'un objet dangereux :

1. Cliquez sur le lien Protection en temps réel dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6) ou sur modifier la configuration dans le texte de description de l'état de l'onglet **Protection**.
2. Sélectionnez le niveau de protection désiré en déplaçant le curseur de l'échelle dans la fenêtre **Configuration de la protection en temps réel** cf. ill 17). Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre d'objets soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée.

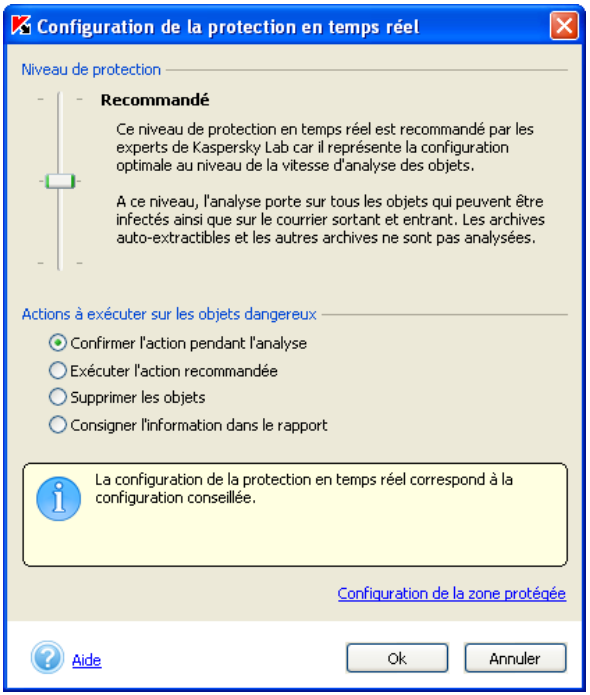


Illustration 17. Configuration de la protection en temps réel

Kaspersky Anti-Virus® Personal propose trois niveaux de protection :

- **Sécurité maximale** : le contrôle des objets ouverts, enregistrés et modifiés est total.
- **Recommandé** : cette configuration repose sur les paramètres recommandés par les experts de Kaspersky Lab. La protection porte sur les mêmes objets que pour le niveau **Sécurité maximale**, à l'exception des archives auto-extractibles.
- **Vitesse maximale** : ce niveau vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume d'objets analysés est réduit.

Le tableau ci-après reprend tous les objets sur lesquels peut porter l'analyse antivirus. Le signe **+** indique que le niveau d'analyse prend en charge cet objet, tandis que le signe **–** indique que l'objet n'est pas analysé à ce niveau.

	Sécurité maximale	Recommandé	Vitesse maximale
Fichiers potentiellement infectés	+	+	+
Secteurs d'amorçage des disques	+	+	+
Fichiers compactés	+	+	+
Objets OLE	+	+	+
Données en provenance du réseau	+	+	+
Courrier entrant[4]	+	+	+
Courrier sortant[5]	+	+	–
Archives auto-extractibles[6]	+	–	–
Bases de messagerie électronique et messages individuels	–	–	–

Il est possible de définir des *exclusions* et de désactiver la protection en temps réel. Pour obtenir de plus amples informations, consultez le point 14.4 à la page 96.

3. Précisez l'action que le logiciel exécutera à chaque découverte d'un objet dangereux.

[4] C'est à dire le courrier reçu via le protocole POP3
[5] C'est à dire le courrier envoyé via le protocole SMTP
[6] Les archives auto-extractibles sont analysées uniquement dans la partie exécutable

Interdire l'accès et confirmer l'action auprès de l'utilisateur : bloque l'accès à l'objet et affiche un message reprenant les différentes options de traitement possibles. Il s'agit du mode de fonctionnement par défaut.

Si vous ne réagissez pas dans les 30 secondes qui suivent l'affichage du message, l'action recommandée sera exécutée par défaut. Pour chaque type d'objet identifié, il existe une action recommandée. Ainsi, l'action *Réparer* est recommandée pour les objets infectés. Le texte **(recommandé)** est repris à droite de l'action qu'il convient d'exécuter.

Voici la liste de toutes les actions que Kaspersky Anti-Virus peut proposer (le contenu de la liste peut varier en fonction du type d'objet):

- *Réparer* l'objet infecté ;
- *Mettre* l'objet potentiellement infecté par un virus ou l'une de ses variantes *en quarantaine*.

Parfois, lorsqu'un objet a été mis en quarantaine, un message apparaît et vous informe que l'objet ne peut être supprimé. Ceci s'explique par le fait que les objets mis en quarantaine sont déplacés : ils sont copiés dans la quarantaine et supprimés de leur emplacement d'origine. Toutefois, il n'est pas toujours possible de supprimer l'objet lors du déplacement. C'est le cas par exemple pour les objets utilisés à ce moment par une autre application.

- *Supprimer objets dangereux* en cas d'échec de la réparation, soit en raison d'une erreur ou parce qu'elle est impossible.
- *Ignorer* les objets infectés. Aucune action n'est réalisée et les informations sont simplement consignées dans le rapport.

Interdire l'accès et exécuter l'action recommandée : bloque l'accès à l'objet et exécute l'action recommandée pour ce type d'objet. Pour les objets infectés, l'action recommandée est *Réparer*. Pour les objets potentiellement infectés, l'action est *Mettre en quarantaine* et pour les chevaux de Troie et les vers, il s'agit de *Supprimer*.

Interdire l'accès et supprimer les objets dangereux : supprime l'objet sans avertissement particulier à l'utilisateur.

- **Interdire l'accès et consigner les informations dans le rapport** : bloque l'accès à l'objet sans afficher de message particulier à l'écran sur le traitement adopté.

8.3. Pour arrêter la protection

Il peut arriver que vous deviez arrêter la protection en temps réel. Pour ce faire, ouvrez le menu contextuel et sélectionnez le point **Arrêter la protection en temps réel**.

Etant donné qu'il n'est pas recommandé de désactiver entièrement la protection en temps réel, Kaspersky Anti-Virus vous offre la possibilité de la désactiver pour une brève période.

Sélectionnez, dans la fenêtre **Arrêt de la protection en temps réel** (cf. ill. 18), l'une des options :

- **Dans 5/10/15 minutes :** la protection sera activée après le délai spécifié
- **Lors de la prochaine connexion au réseau** : la protection sera à nouveau activée que l'ordinateur sera à nouveau raccordé au réseau (cette option apparaît dans la liste quand l'ordinateur n'est pas connecté au réseau).
- **Lors du prochain lancement de Kaspersky Anti-Virus Personal** : la protection sera à nouveau activée lorsque vous lancerez le programme au départ du menu **Démarrer → Programmes → Kaspersky Anti-Virus Personal** ou après le redémarrage du système (si le mode de lancement du programme au démarrage du système d'application a été sélectionné).
- **Uniquement sur demande de l'utilisateur** : la protection sera uniquement réactivée lorsque vous l'aurez décidé.

Le cas échéant, vous pouvez décider de désactiver complètement un des composants de l'application : protection du système de fichiers, protection du courrier ou protection contre les attaques de réseau (cf. point 14.1, p. 91).

Illustration 18. Désactivation temporaire de la protection antivirus

CHAPITRE 9. PROTECTION CONTRE LES ATTAQUES DE RESEAU

La protection de votre ordinateur contre les attaques de réseau est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du logiciel.

Kaspersky Anti-Virus Personal 5.0 protège votre ordinateur contre les attaques de pirates informatiques depuis le réseau local ou depuis Internet.

L'identification d'une attaque de pirates informatiques s'opère sur la base de données reprenant les attaques de réseau les plus connues à ce jour. Ces bases sont mises à jour et téléchargées en même temps que les bases antivirus(Pour de plus amples informations, consultez le Chapitre 13 à la page 81).

Par défaut, la protection contre les attaques de réseau est activée dès le lancement de Kaspersky Anti-Virus. Le logiciel surveille toutes les connexions au réseau et analyse les données obtenues via le réseau, quelle que soit la source ; réseau local ou Internet.

Si la protection contre les attaques de réseau est désactivée, nous vous conseillons de l'activer de la manière suivante :

1. Cliquez sur Protection en temps réel dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6) ou sur modifier la configuration dans le texte indiquant le statut de la protection dans l'onglet **Protection**.
2. Dans la fenêtre **Configuration de la protection en temps réel** (cf. ill. 17), cliquez sur Configuration de la protection en temps réel et désélectionnez la case ☑ **Désactiver la protection contre les attaques de réseaux** dans la fenêtre qui s'affiche.

La moindre tentative d'attaque contre votre ordinateur sera bloquée. Le message correspondant (cf. ill. 19) apparaîtra à l'écran et vous transmettra les informations relatives au type d'attaque, à l'adresse IP de l'ordinateur à l'origine de l'attaque et au port local (si possible). La notification ne sera pas affichée si la case ☑ **Ne pas m'avertir en cas d'attaque de réseau** (cf. ill. 32) a été cochée.

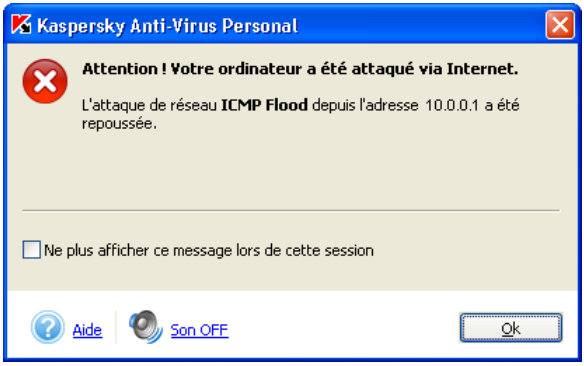


Illustration 19. Notification relative à une attaque de réseau

Pour de plus amples informations sur la configuration de la protection contre les attaques de réseau, consultez le point 14.3 à la page 94.

CHAPITRE 10. PROTECTION DU COURRIER CONTRE LES VIRUS

La protection du courrier entrant et sortant est garantie uniquement si vous avez décidé de l'utiliser au moment de l'installation du logiciel.

Kaspersky Anti-Virus® Personal assure une protection en temps réel du courrier entrant et sortant. Vu que le courrier est couvert par la protection en temps réel, celle-ci est activée dès le lancement de Kaspersky Anti-Virus. L'analyse du courrier entrant a lieu lors de la réception tandis que celle du courrier sortant a lieu pendant l'envoi. L'icône de Kaspersky Anti-Virus dans la barre des tâches indique la vérification du courrier : lors de l'analyse d'un message, l'icône se transforme en une enveloppe clignotante.

Les aspects suivants du traitement du courrier par Kaspersky Anti-Virus® Personal sont à retenir :

- Kaspersky Anti-Virus® Personal assure la protection antivirus du courrier quel que soit le client de messagerie utilisé[7]. Le courrier est analysé à l'envoi et à la réception, que cette opération soit réalisée par vous via le client de messagerie ou par une application quelconque de votre ordinateur.
- Lors de la découverte d'un objet infecté dans un courrier électronique, l'action recommandée est exécutée : Kaspersky Anti-Virus® tente de réparer l'objet et si cette opération échoue, il le supprime du message.
- Par contre, si vous relevez votre courrier sur des serveurs Web distants à l'aide d'un navigateur comme Internet Explorer par exemple, seules les pièces jointes seront analysées lorsque vous les ouvrirez ou les enregistrerez sur le disque dur.

[7] Kaspersky Anti-Virus® Personal assure la protection en temps réel de tout le courrier entrant via le protocole POP3 et de tout le courrier sortant via le protocole SMTP. Pour les messages distribués via le protocole HTTP, l'analyse porte uniquement sur les pièces jointes au moment de leur exécution ou de l'enregistrement sur le disque.

Pour protéger votre courrier contre les virus :

Il suffit d'activer la protection en temps réel (si elle avait été suspendue ou désactivée) et de s'assurer que la case ☐ **Désactiver la protection en temps réel du courrier** dans la fenêtre **Configuration de la zone protégée** n'est pas cochée (cf. point 14.1, p. 91).

L'analyse du courrier sortant est régie par la case ☑ **Ne pas analyser le courrier sortant**.

Pour analyser les boîtes aux lettres Microsoft Office Outlook ou Microsoft Outlook Express :

1. Cliquez sur le lien Analyser les objets dans la partie gauche de l'onglet **Protection** (cf. ill. 5).
2. Sélectionnez ☑ **Boîte aux lettres** dans la fenêtre **Sélection des objets à analyser** (cf. ill. 15).
3. Cliquez sur **Analyser**.

Les boîtes de messagerie électronique Microsoft Office Outlook et Microsoft Outlook Express seront ainsi analysées.

Suite au traitement des boîtes de messagerie électronique Microsoft Office Outlook et Microsoft Outlook Express et quel que soit le type d'action sélectionné, la date et l'heure de modification des objets sont toujours changées.

Les bases de messagerie provenant d'ordinateurs tiers peuvent être analysées à la demande. Par défaut, lors de détection de telles bases de messagerie infectées, Kaspersky Anti-Virus affichera l'information dans le rapport. Pour rappel, on ne peut supprimer les bases infectées que manuellement.

Pour vérifier les bases de messagerie électronique d'autres clients (ex. : TheBat) ou les bases que vous avez ramenées du bureau sur une disquette :

1. Cliquez sur le lien Analyser les objets dans la partie gauche de l'onglet **Protection** (cf. ill. 5).
2. Dans la boîte de dialogue **Sélection des objets à analyser** (cf. ill. 15), sélectionnez le disque ou le répertoire dans lequel se trouve les bases.
3. Cliquez sur **Analyser**.

CHAPITRE 11. TRAITEMENT DES VIRUS

Les actions exécutées par Kaspersky Anti-Virus® Personal en cas de découverte d'un objet dangereux, d'un programme malicieux ou d'un objet potentiellement infecté par un virus ou l'une de ses variantes dépendent entièrement et uniquement de la manière dont vous avez configuré la protection en temps réel et l'analyse à la demande. Ce chapitre aborde les situations où Kaspersky Anti-Virus® Personal vous propose un choix d'actions à exécuter sur un objet dangereux lors de l'analyse ou à la fin de celle-ci.

Cela se produit lorsque vous avez sélectionné :

- dans la configuration de la protection en temps réel (cf. ill. 17):

  Interdire l'accès et confirmer l'action auprès de l'utilisateur. Dans ce cas, la demande sera soumise à l'utilisateur dès qu'un objet dangereux sera découvert.

- dans la configuration de l'analyse à la demande (cf. ill. 10):

  Confirmer l'action auprès de l'utilisateur. La sélection de l'action à réaliser sur l'objet dangereux s'opère dès la découverte de cet objet par Kaspersky Anti-Virus.

  ou

  Confirmer l'action à la fin de l'analyse. La sélection de l'action à réaliser sur les objets dangereux est proposée uniquement si vous avez lancé le traitement de ces objets, c'est-à-dire si vous avez cliquez sur **Réparer...** dans la fenêtre reprenant les résultats de l'analyse(cf. ill. 20).

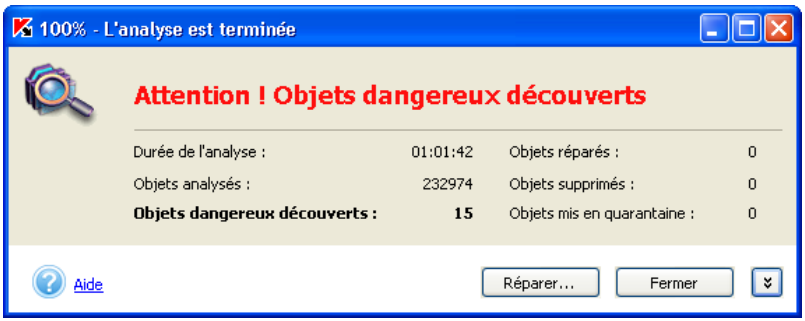


Illustration 20. Traitement différé des objets dangereux

En cas de découverte d'un objet dangereux, une boîte de dialogue apparaît à l'écran (cf. ill. 21). Elle reprend :

- Une description détaillée de l'objet dangereux
- Une sélection des actions qui peuvent être exécutées sur l'objet. Cette sélection reprend toujours au moins une action recommandée par les experts de Kaspersky Lab. Le terme **(recommandé)** est repris à côté de celle-ci. Voici l'ensemble des actions possibles (les actions proposées en réalité dépendent du type d'objet découvert) :
  - **Réparer** : tente de réparer l'objet si possible.
  - **Supprimer** : supprime l'objet infecté ou potentiellement infecté.
  - **Ignorer** : aucune action n'est réalisée, seules les informations sont consignées dans le rapport.

    L'objet dangereux sera ignoré si vous fermez la boîte de dialogue relative à sa découverte en cliquant sur le bouton dans le coin supérieur droit.
  - **Quarantaine** : l'objet potentiellement infecté par un virus ou l'une de ses modifications est mis en quarantaine en vue d'une nouvelle analyse, d'une réparation, d'un envoi pour examen à Kaspersky Lab ou de sa suppression (cf. point 14.4, p. 96).
  - **Ignorer, ajouter aux exclusions** : ajouter le programme découvert à la liste des exclusions de l'analyse antivirus et de la protection en temps réel.

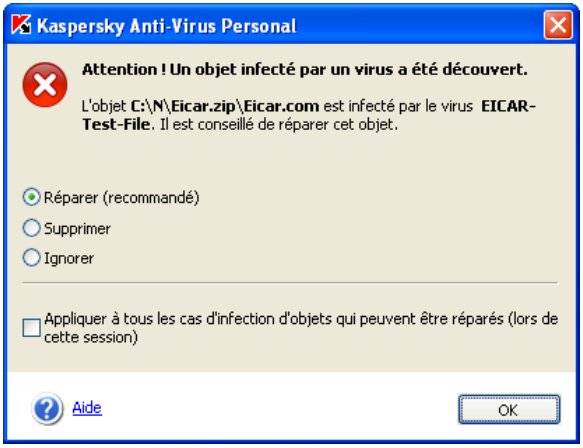


Illustration 21. Message affiché suite à la découverte d'un objet infecté

Vous pouvez appliquer l'action sélectionnée à tous les objets identiques en cochant la case adéquate. Ainsi, pour appliquer une action à tous les objets infectés qui ne peuvent être réparés, cochez **Appliquer à tous les cas d'objets qui ne peuvent être réparés (lors de cette session)**.

Si pour une raison quelconque vous avez décidé de ne pas traiter des objets en sélectionnant l'option **Ignorer**, vous pourrez les traiter ultérieurement. Pour ce faire, cliquez sur le lien traiter ces objets dans la partie droite de l'onglet **Protection**. Cette action entraîne l'ouverture de la boîte de dialogue **Objets dangereux découverts** (cf. ill. 22) qui propose une description détaillée de chacun des objets dangereux ainsi qu'un lien vers l'article consacré à l'objet dans l'encyclopédie des virus consultable à l'adresse http://www.viruslist.com/fr.

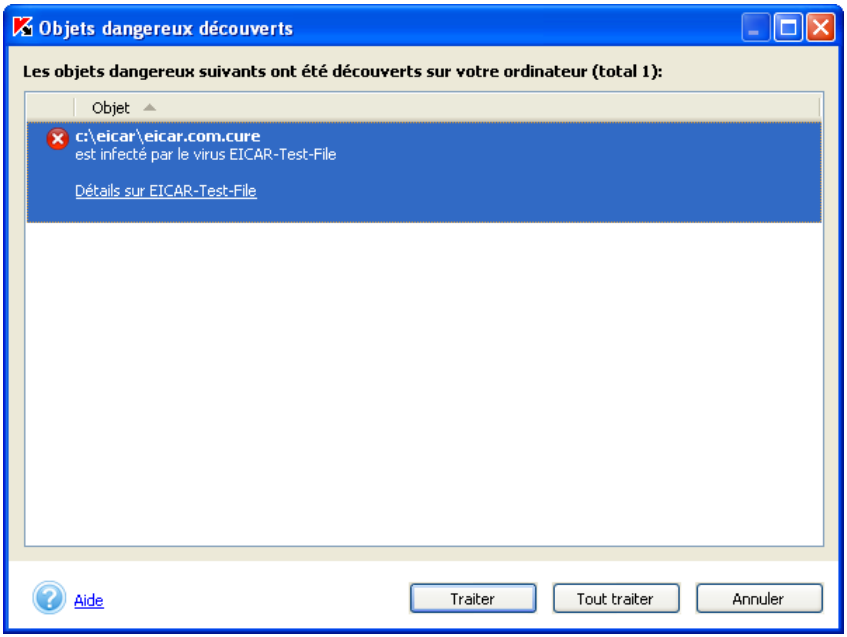


Illustration 22. Liste des objets dangereux découverts

Grâce au bouton **Traiter**, vous pouvez traiter l'objet sélectionné dans la liste. Le bouton **Traiter tous** vous permet de lancer le traitement de tous les objets de la liste. Un message apparaîtra (cf. ill. 21). Vous pourrez ensuite sélectionner l'action à réaliser sur l'objet (pour de plus amples informations sur les actions proposées voir les sections correspondantes).

Pour supprimer un objet de la liste sans le traiter, utilisez la commande du menu contextuel **Supprimer de la liste** (cf. ill. 23).

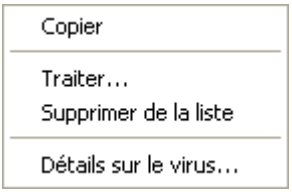


Illustration 23. Menu contextuel de la fenêtre **Objets dangereux découverts**

Au cas où un objet dangereux quelconque aurait été supprimé manuellement, il ne figurera pas dans la liste des objets découverts lors de la tentative de traitement.

CHAPITRE 12. RENOUVELLEMENT DE LA LICENCE

Vous pourrez utiliser Kaspersky Anti-Virus® Personal uniquement après avoir installé la *clé de licence* qui fait partie du pack logiciel.

Kaspersky Anti-Virus® Personal NE PEUT FONCTIONNER sans la clé de licence !

A la fin de la période de validité de la licence, Kaspersky Anti-Virus® continue à fonctionner mais la mise à jour des bases antivirus n'est plus possible. Les bases antivirus qui étaient d'actualité à la date d'expiration de la licence sont celles qui seront utilisées pour l'analyse antivirus de l'ordinateur et du courrier ainsi que pour la réparation des objets dangereux. Par conséquent, la protection contre les nouveaux virus qui apparaîtraient après la fin de validité de la licence de Kaspersky Anti-Virus n'est pas garantie.

Pour éviter que votre ordinateur ne soit infecté par de nouveaux virus, il est recommandé de renouveler la licence d'utilisation de Kaspersky Anti-Virus® Personal.

Deux semaines avant la date d'expiration, Kaspersky Anti-Virus® vous signalera qu'il est bientôt temps de renouveler la licence. Ce message apparaîtra à chaque démarrage du logiciel pendant cette période de deux semaines.

Pour renouveler la licence, vous devez absolument acheter et activer une nouvelle clé de licence pour Kaspersky Anti-Virus® Personal. Pour ce faire :

1. Contactez le distributeur chez lequel vous avez acheté le logiciel et demandez une prolongation de la licence d'utilisation de Kaspersky Anti-Virus® Personal.

Ou :

Achetez une nouvelle clé de licence directement chez Kaspersky Lab en cliquant sur le lien Renouvellement de la licence dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 7) ou en cliquant **Renouveler** dans la boîte de dialogue **Gestion des clés de licence** (cf. ill. 24). Remplissez le formulaire requis sur notre site Internet. Une fois le paiement effectué, vous recevrez à l'adresse

électronique spécifiée lors de la commande une référence qui vous permettra de télécharger la clé de licence.

2. Activez la clé de licence. Pour ce faire :

   - Cliquez sur le lien Clés de licence dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 7).
   - Cliquez sur le bouton **Ajouter** dans la boîte de dialogue **Gestion des clés de licence** (cf. ill. 24) qui apparaît et sélectionnez la nouvelle clé de licence.
   - Dans la fenêtre de sélection, ouvrez le répertoire qui contient la clé de licence (fichier **.key**). Sélectionnez la clé nécessaire puis, cliquez sur **Ouvrir**.
   - Dans la fenêtre qui apparaît – **Activation de la clé**, lisez les informations relatives à la clé que vous venez d'ajouter et cliquez sur **Activer** pour utiliser cette clé.

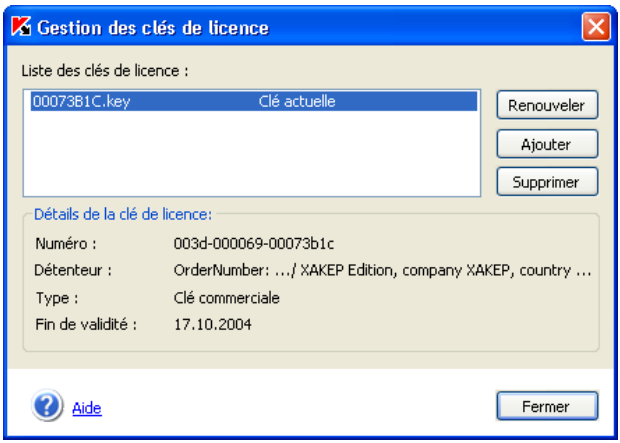


Illustration 24. Fenêtre de gestion des clés de licence

Ou :

- Dans le menu **Démarrer** → **Programme**, sélectionnez le groupe Kaspersky Anti-Virus Personal et sélectionnez **Installer une clé de licence** dans le menu déroulant.

a. Indiquez Dans la fenêtre le nom du fichier de clé de licence. Pour ce faire, cliquez sur **Parcourir** et et passez au répertoire qui contient la clé de licence.

b. Sélectionnez la clé de licence nécessaire puis, cliquez sur **Ouvrir**.

c. Dans la partie inférieure de la fenêtre (cf. ill. 25), cochez la case en regard de l'application pour laquelle vous souhaitez installer la clé de licence. Cliquez sur **OK**.

Si la liste de la partie inférieure de la fenêtre est vide, cela signifie que la clé choisie ne convient à aucune des applications de Kaspersky Lab installées sur l'ordinateur.

Sélectionnez un autre fichier de clé de licence.

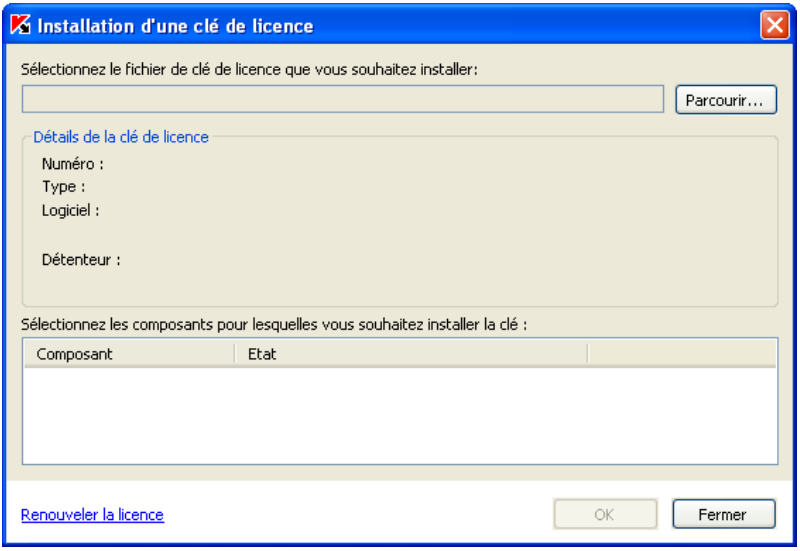


Illustration 25. Fenêtre **Installation de la clé de licence**

d. Dans la fenêtre **Activation de la clé**, lisez les informations relatives à la clé ajoutée puis, cliquez sur **Activer** pour utiliser la clé.

CHAPITRE 13. TELECHARGEMENT DES MISES A JOUR

Kaspersky Lab offre à ses utilisateurs la possibilité de mettre à jour les modules de Kaspersky Anti-Virus® Personal, les bases antivirus qui interviennent dans l'identification des programmes malicieux et la réparation des objets infectés ainsi que les bases d'attaques de réseau pour s'en protéger.

La mise à jour des bases est la garantie de la sécurité de votre ordinateur. Des dizaines de nouveaux virus et d'attaques de réseau voient le jour chaque jour et les experts de Kaspersky Lab actualisent quotidiennement le contenu des bases antivirus. Il est conseillé de procéder à la mise à jour des bases antivirus au moins une fois toutes les 3 heures. Lors d'une épidémie, la fréquence devrait être la plus courte possible, par exemple au moins une fois toutes les heures.

Kaspersky Anti-Virus® Personal va chercher les mises à jour sur *les serveurs de mise à jour de Kaspersky Lab* ou dans un répertoire de l'ordinateur. Le choix de la source dépend de la configuration (voir plus loin pour les détails).

Le téléchargement des mises à jour peut être soit programmé soit réalisé manuellement. Afin de pouvoir télécharger ces bases depuis Internet, votre ordinateur doit absolument être connecté au réseau. La progression du téléchargement est illustrée par l'indicateur de copie. Après la réussite de la mise à jour, Kaspersky Anti-Virus commence à utiliser les nouvelles bases afin d'analyser l'ordinateur.

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

1. Kaspersky Anti-Virus vérifie la connexion et établit la connexion avec la source de la mise à jour.
2. Le serveur des mises à jour de Kaspersky Lab envoie au logiciel la liste des mises à jour et leur taille respective.
3. Ensuite, le logiciel compare l'état des bases antivirus et des modules de Kaspersky Anti-Virus® aux informations fournies. Si les bases antivirus installées sur votre ordinateur sont toujours d'actualité, la mise à jour sera interrompue. Dans le cas contraire, la copie des fichiers depuis les serveurs de mise à jour de Kaspersky Lab est lancée. Le téléchargement est illustré par une barre d'état (cf. ill. 26).

4. Le programme connecte les bases téléchargées. Si la connexion réussi, Kaspersky Anti-Virus commencera à utiliser les bases lors de l'analyse de l'ordinateur. En cas d'erreur lors de la connexion des base, l'annulation de la mise à jour sera automatiquement lancé au profit d'une version antérieure.

Après la réception et la connexion des mises à jour, il se peut qu'il faille redémarrer l'ordinateur. Dans ce cas, le message de circonstance apparaîtra à l'écran.

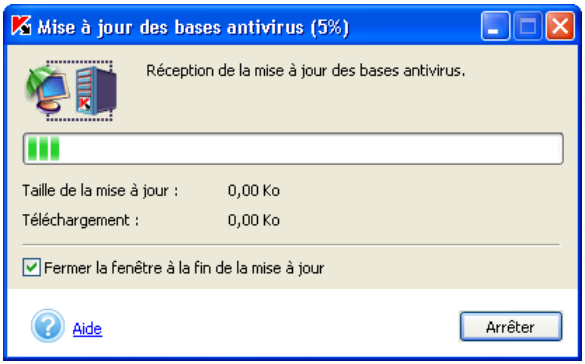


Illustration 26. Boîte de dialogue **Mise à jour**

Parfois, le logiciel vous invite à redémarrer l'ordinateur après la mise à jour des bases antivirus. Cela se produit généralement après la mise à jour des modules de l'application ou des bases des attaques de réseau. Le redémarrage du système s'impose afin d'installer tous les nouveaux composants et de les activer.

13.1. 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. ill. 5).

L'état des bases de données est indiqué par l'un des trois signes suivants :

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

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 absentes, soit corrompues.

13.2. Quelles mises à jour télécharger ?

Kaspersky Anti-Virus vous offre deux types de bases antivirus :

Bases standard : bases antivirus contenant les définitions de tous les virus connus à ce jour et les outils permettant de les neutraliser.

Si vous souhaitez protéger votre ordinateur contre les riskwares, il vous faudra alors télécharger les bases étendues. En plus des définitions de virus traditionnels, ces bases contiennent les descriptions d'adwares, de spywares, d'outils d'attaque et d'autres riskwares.

Les bases antivirus standard suffisent amplement pour assurer la protection normale de votre ordinateur. Si vous décidez d'utiliser les bases étendues, vous pourriez observer un ralentissement de Kaspersky Anti-Virus. De plus, certains des logiciels que vous utilisez pourraient être considérés comme des riskwares.

Pour choisir le type de bases antivirus utilisées par Kaspersky Anti-Virus :

1. Cliquez sur Menaces et exclusions dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).
2. Dans la section **Menaces identifiées** de la fenêtre qui s'ouvre (cf. ill. 27), cochez la case ☑ **Adwares, riskwares, dialers** si vous souhaitez utiliser les bases étendues. Pour éviter la suppression des programmes que vous utilisez, il est conseillé de définir une action qui requiert la confirmation de l'utilisateur (cf. point 6.2 p. 48 et point 8.2, p. 64).

La case ☑ **Virus, vers, chevaux de Troie, utilitaires d'attaque et logiciels espion** est cochée par défaut et il est impossible de la désélectionner. Elle indique que les bases antivirus standard seront utilisées pendant l'analyse.

Vous pouvez vous familiariser au contenu de n'importe quelle base. Pour ce faire, sélectionnez le nom de la base et cliquez sur Bases antivirus utilisées. Les

définitions apparaîtront dans une nouvelle fenêtre. Cliquez sur **Détails** après avoir sélectionné la définition. Cette action entraînera l'ouverture du site www.viruslist.com/fr où vous pourrez lire une description détaillée des types de menaces les plus répandues.

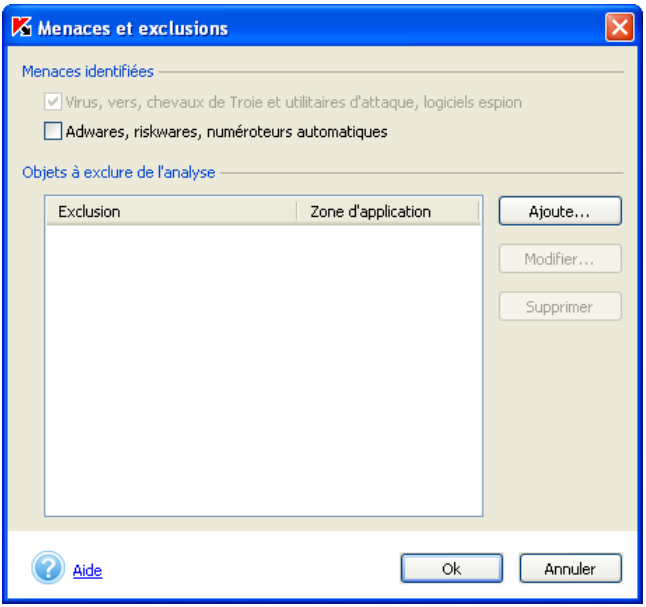


Illustration 27. Sélection du type de bases antivirus

13.3. Téléchargement des mises à jour depuis Internet

Kaspersky Lab publie les mises à jour des bases antivirus une fois toutes les heures sur ses serveurs.

Les serveurs de mises à jour de Kaspersky Lab sont les sites Internet que Kaspersky Lab utilise pour diffuser les mises à jour des bases antivirus.

Afin de procéder à la mise à jour des bases antivirus via Internet au départ des serveurs de mises à jour de Kaspersky Lab, il est indispensable de configurer le logiciel de la manière suivante :

1. Cliquez sur le lien Mises à jour dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).

2. Dans menu déroulant **Source de la mise à jour** de la boîte de dialogue **Configuration des mises à jour** (cf. Illustration 28), sélectionnez *via Internet.*

3. Cliquez sur **OK**.

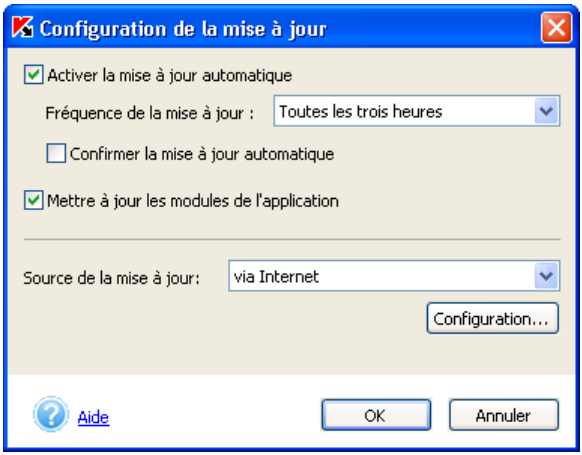


Illustration 28. Boîte de dialogue **Configuration des mises à jour**

Les paramètres de la connexion Internet seront identiques à ceux repris dans le panneau de configuration de Microsoft Internet Explorer. Pour consulter ou modifier ces paramètres, sélectionnez **Démarrer → Paramètres → Panneau de configuration → Options Internet → Connexions**.

Si vous vous connectez à Internet via un serveur proxy, vous pouvez en définir les paramètres. Pour configurer les paramètres du serveur proxy, cliquez sur **Configuration** (pour de plus amples informations, consultez le point 13.6 à la page 87).

13.4. Téléchargement des mises à jour depuis un répertoire local

Pour configurer la mise à jour des bases antivirus depuis un répertoire local :

1. Cliquez sur le lien Mises à jour dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).

2. Sélectionnez *Depuis le catalogue local* dans le menu déroulant **Source de la mise à jour** de la boîte de dialogue **Configuration des mises à jour** (cf. ill. 29).
3. Dans le champ **Répertoire local**, sélectionnez le répertoire dans le lequel vous avez extrait le contenu des archives zip.
4. Cliquez sur **OK**.

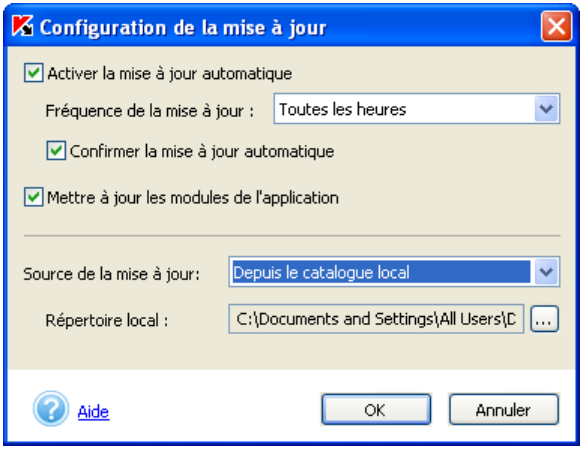


Illustration 29. Boîte de dialogue **Configuration des mises à jour**

13.5. Mise à jour des modules du logiciel Kaspersky Anti-Virus® Personal

En plus des bases antivirus, vous pouvez également mettre à jour les propres modules de Kaspersky Anti-Virus® Personal. Ces mises à jour sont publiées sur le serveur au fur et à mesure de leur publication.

Il est possible de procéder à la mise à jour des modules depuis les serveurs de mise à jour ou depuis un répertoire local. Pour ce faire, il suffit de cocher la case **Mettre à jour les modules de l'application** dans la boîte de dialogue **Configuration des mises à jour** (cf. ill. 29).

La boîte de dialogue de confirmation apparaît lors de la réception des mises à jour des modules (cf. ill. 30). Sélectionnez une des options suivantes :

Installer la mise à jour des modules de l'application.

- **Ne pas mettre à jour des modules de l'application et me rappeler plus tard** : rappelle la nécessité d'installer la mise à jour des modules du programme lors du prochain démarrage de Kaspersky Anti-Virus.
- **Désactiver l'installation de la mise à jour des modules de l'application** : si vous choisissez cette option, la case **Mettre à jour les modules de l'application** sur la boîte de dialogue **Configuration de la mise à jour** (cf. ill. 29) sera désélectionnée et la mise à jour des modules du programme sera désactivée.

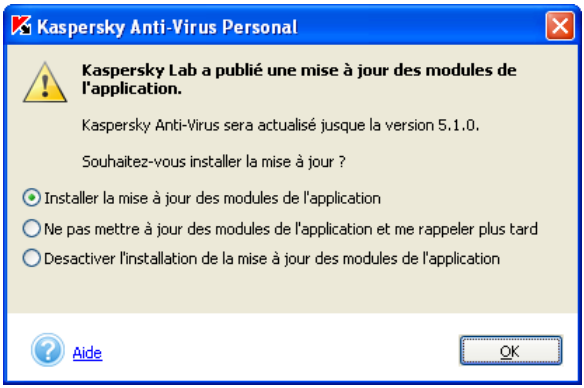


Illustration 30. Confirmation de l'installation de la mise à jour des modules du programme

13.6. Configuration du serveur proxy

Par défaut, les paramètres de connexion à Internet utilisés lors de la mise à jour des bases antivirus sont ceux repris dans Microsoft Internet Explorer. Si votre connexion à Internet s'opère via un serveur proxy, vous devrez définir ses paramètres, à savoir l'adresse IP, le port, les paramètres d'authentification, etc. Contactez votre fournisseur d'accès Internet ou votre administrateur système pour obtenir ces informations.

Les paramètres du serveur proxy sont définis dans la boîte de dialogue **Configuration du serveur proxy** (cf. ill. 31).

Pour ouvrir cette boîte de dialogue :

1. Cliquez sur le lien Mises à jour dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).

2. Dans la fenêtre **Configuration de la mise à jour** (cf. ill. 29) qui s'affiche, cliquez sur **Configuration**, dans la zone contenant les informations.

Les paramètres du serveur proxy peuvent être définis de deux manières différentes:

- **Définir automatiquement les paramètres du serveur proxy**
- **Utiliser un autre serveur proxy**

La première option est choisie par défaut. Les paramètres du serveur proxy seront tirés de Microsoft Internet Explorer.

Si le serveur proxy requiert une autorisation, sélectionnez la deuxième option et définissez les paramètres du serveur proxy :

Adresse : adresse IP du serveur proxy au format *aaa.bbb.ccc.ddd* ou son nom.

Port : numéro du port sur lequel est installé le serveur proxy. Sélectionnez l'une des valeurs proposées dans la liste déroulante : *3128*, *8080*, *8082*, *8903* ou saisissez une valeur spécifique.

Lorsque l'enregistrement est requis sur le serveur proxy, cochez la case

☑ **Utiliser l'autorisation sur le serveur proxy** et saisissez votre nom et votre mot dans passe dans les champs prévus à cet effet.

Si l'autorisation sur le serveur proxy est indispensable et que soit vous n'avez pas indiqué le nom et le mot de passe ou que soit les données, pour une raison quelconque, n'ont pas été acceptées par le serveur proxy, la fenêtre de saisie du nom d'utilisateur et du mot de passe apparaîtra lors du lancement de la mise à jour. Si l'autorisation est accordée, le nom et le mot de passe utilisés seront sauvegardés pour la prochaine mise à jour. Dans le cas contraire, il faudra à nouveau saisir les paramètres d'autorisation.

Si votre serveur est muni d'un pare-feu et que vous ne parvenez pas à vous connecter au site FTP en mode actif, cochez la case ☑ **Utiliser le FTP en mode passif**.

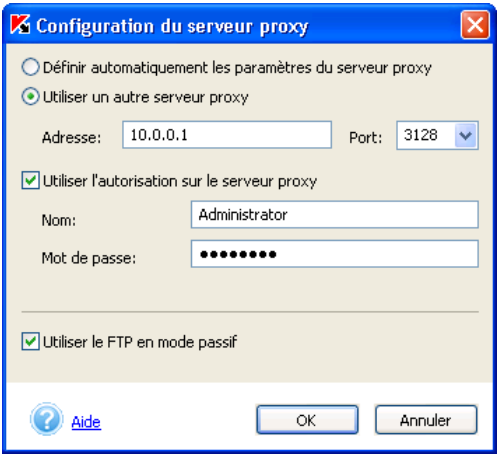


Illustration 31. Configuration des paramètres du serveur proxy

13.7. Configuration des mises à jour. Programmation

Les experts de Kaspersky Lab conseillent de programmer le téléchargement des mises à jour et de choisir un intervalle de 12 heures. Lors d'une épidémie, la fréquence devrait être la plus courte possible, par exemple au moins une fois toutes les trois heures ou le plus souvent possible en cas d'épidémie.

Pour programmer le téléchargement régulier des mises à jour des bases antivirus :

- Cliquez sur le lien Mises à jour dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6).
- Cochez la case **Activer la mise à jour automatique** dans la boîte de dialogue **Configuration des mises à jour** (cf. ill. 29).

3. Sélectionnez la valeur désirée dans la liste déroulante **Fréquence de la mise à jour**.
4. Cochez la case **Confirmer la mise à jour automatique** si vous souhaitez que le message adéquat s'affiche avant le téléchargement des bases antivirus (cf. ill. 13).

Si vous avez programmé la mise à jour pour qu'elle ait lieu toutes les trois heures et que l'ordinateur est resté éteint pendant une période dépassant cet intervalle (par exemple, 10 heures), la mise à jour des bases antivirus sera lancée dès que vous démarrerez votre ordinateur.

13.8. Mise à jour manuelle

Pour lancer le téléchargement des mises à jour des bases antivirus :

Cliquez sur le lien Mettre à jour maintenant dans la partie gauche de l'onglet **Protection** (cf. ill. 5) ou dans le message vous informant de l'urgence de la mise à jour dans la partie droite de la fenêtre ou sélectionnez le point Mettre à jour les bases antivirus dans le menu contextuel de Kaspersky Anti-Virus.

Afin que le logiciel puisse lancer le téléchargement des mises à jours, programmé ou manuel, via Internet, votre ordinateur doit être connecté. Dans le cas contraire, la mise à jour ne pourra avoir lieu si la connexion à Internet est inexistante.

CHAPITRE 14. POSSIBILITES COMPLEMENTAIRES

Kaspersky Anti-Virus® Personal propose les possibilités suivantes au niveau de la configuration et de l'utilisation telles que :

- La configuration des paramètres de protection en temps réel et de l'analyse complète de l'ordinateur.
- Le travail avec les objets placés en quarantaine.
- L'analyse du rapport sur l'activité du logiciel.
- Les options avancées

Ce chapitre aborde en détails chacun de ces groupes.

14.1. Configuration des paramètres de la protection en temps réel

Par défaut, la protection en temps réel de l'ordinateur correspond à la configuration recommandée par les experts de Kaspersky Lab. En plus de la modification des paramètres principaux de la protection en temps réel (cf. Chapitre 8, p. 63), Kaspersky Anti-Virus® Personal vous permet de configurer des *paramètres de protection complémentaires* et plus exactement, la possibilité d'exclure des groupes distincts d'objets de la protection en temps réel. Vous pouvez limiter la protection en temps réel à certaines parties ou la désactiver totalement. Ces paramètres vous permettent de réduire le volume d'objets analysés dans le cadre de la protection en temps réel en excluant par exemple le courrier, les fichiers de script et de limiter le temps maximum d'analyse (en secondes) de l'objet.

La configuration des paramètres complémentaires de protection est appliquée à tous les niveaux de protection en temps réel (**Sécurité maximale**, **Recommandé** et **Vitesse maximale**).

La configuration des paramètres de protection s'effectue dans la fenêtre du même nom (cf. ill. 32) qui s'ouvre lorsque vous cliquez sur le lien Configuration de la zone protégée dans la fenêtre **Configuration de la protection en temps réel** (cf. ill. 17).

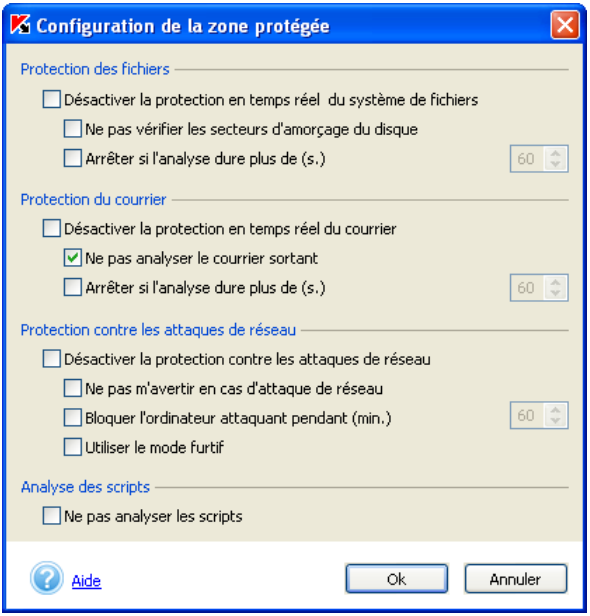


Illustration 32. Configuration de la protection en temps réel

Kaspersky Anti-Virus® Personal vous offre la possibilité de rétablir à n'importe quel moment la configuration recommandée, remplaçant ainsi votre configuration.

Pour rétablir la configuration recommandée de la protection en temps réel, cliquez sur lien rétablir la configuration par défaut dans la partie droite de l'onglet **Paramètres** dans les commentaires sur l'état de la protection en temps réel (cf. ill. 33) ou à l'aide de l'administration des profils (cf. point 14.11, p. 116).

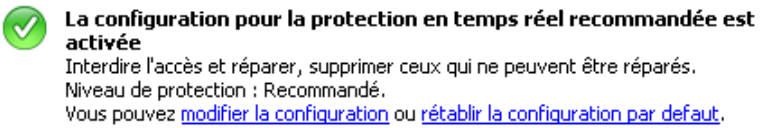


Illustration 33. Informations sur l'état de la protection en temps réel

Si vous avez décidé de ne pas utiliser l'une ou l'autre des technologies de protection au moment de l'installation de Kaspersky Anti-Virus (fichiers, courrier, attaques de réseau ou scripts), vous ne pourrez pas la configurer dans cette fenêtre.

14.2. Configuration des paramètres d'analyse à la demande

Par défaut, l'analyse complète exécutée par Kaspersky Anti-Virus® Personal porte sur tous les objets du disque dur de l'ordinateur (cf. Chapitre 3, p. 27), conformément à la configuration définie par les experts de Kaspersky Lab.

En plus de la modification du niveau de protection et du choix des actions exécutées par Kaspersky Anti-Virus® en cas de découverte d'un objet infecté (cf. point 8.2, p. 64), vous pouvez définir pour tous les niveaux de protection des *paramètres d'analyse* complémentaires. Tout comme pour la protection en temps réel, la définition de ces paramètres complémentaires réduit le volume d'objets analysés.

La configuration des paramètres d'analyse complémentaires est unique pour tous les niveaux d'analyse (**Sécurité maximale**, **Recommandé** et **Vitesse maximale**).

La configuration des paramètres d'analyse s'effectue au départ de la fenêtre **Configuration de l'analyse** (cf. ill. 34), qui s'ouvre en cliquant sur le lien Configuration de la zone d'analyse de la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 10).

Vous pouvez exclure de l'analyse n'importe quel type d'objet en cochant la case adéquate ou en sélectionnant le répertoire ou les fichiers (masques de fichiers) à exclure de la même manière que celle décrite pour la protection en temps réel (cf. point 14.1, p. 91).

Il n'est pas conseillé de ranger le disque logique formé sur la base du répertoire du système de fichiers à l'aide de la commande *subst* parmi les exclusions. Cela est dépourvu de sens car, pendant l'analyse, Kaspersky Anti-Virus® Personal considère ce disque logique comme un répertoire et l'analyse par conséquent.

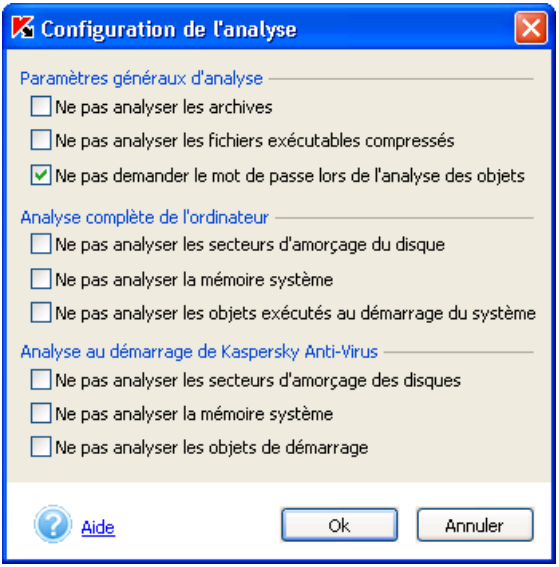


Illustration 34. Exclusions de l'analyse à la demande

Kaspersky Anti-Virus® Personal vous offre la possibilité de rétablir à n'importe quel moment la configuration recommandée, remplaçant ainsi votre configuration.

Pour revenir à la configuration recommandée pour n'importe quel niveau, il suffit de cliquer sur le lien rétablir la configuration par défaut dans la partie droite de l'onglet **Paramètres** ou **Protection**, dans les commentaires sur l'état de la protection en temps réel.

14.3. Configuration de la protection contre les attaques de réseau

La configuration des paramètres contre les attaques de réseau s'opère dans la fenêtre **Configuration de la protection en temps réel** (cf. ill. 32).

Lors de l'activation/désactivation de la protection en temps réel depuis le menu contextuel de Kaspersky Anti-Virus, la protection en temps réel contre les attaques de réseau est désactivée (cf. point 8.3, p. 68).
Si vous souhaitez désactiver uniquement la protection contre les attaques de réseau, sans désactiver pour autant la protection du courrier et des fichiers, cochez la case ☑ **Désactiver la protection contre les attaques de réseau**

dans la fenêtre **Configuration de la protection en temps réel**. Il est nécessaire de redémarrer l'ordinateur pour activer/désactiver la protection.

De plus, il est possible de configurer d'autres paramètres :

- **Notifications sur les attaques de réseau**. Par défaut, le logiciel vous avertit chaque fois qu'il détecte une tentative d'attaque sur votre ordinateur. L'écran affiche alors une boîte de dialogue (cf. ill. 19), qui reprend le type d'attaque exécutée, l'adresse IP d'origine et le port local victime (s'il est possible de définir cette information). Dans la mesure où il s'agit d'un message purement informatif, vous pouvez décider de ne pas l'afficher en cochant la case ☑ **Ne pas m'avertir en cas d'attaque de réseau** ; l'information est néanmoins consignée dans les rapports.

- **Blocage de l'ordinateur à l'origine de l'attaque**. Kaspersky Anti-Virus peut bloquer tous les ordinateurs qui tentent d'attaquer le vôtre. Par défaut, le blocage de l'ordinateur à l'origine de l'attaque est désactivé. Si vous décidez de l'activer, il sera limité à 60 minutes. Pendant cette période, tout paquet de données en provenance de l'ordinateur attaquant sera bloqué. Pour modifier cette durée, saisissez la valeur souhaitée pour le paramètre **Bloquer l'ordinateur attaquant pendant (min.)**. Désélectionnez la case à côté de ce paramètre si vous souhaitez désactiver cette fonction.

- **Utiliser le mode furtif**. Ce mode autorise uniquement les activités réseau initialisées par l'utilisateur ou par un des logiciels installés sur son ordinateur. Toutes les autres activités (connexion à distance à votre ordinateur, etc.) sont interdites. Cela signifie que votre ordinateur devient en quelque sorte « invisible » pour le monde extérieur. Le mode furtif permet également de déjouer n'importe quel type d'attaque par déni de service (DoS). Ce mode de fonctionnement n'a aucune répercussion négative sur votre utilisation d'Internet. Kaspersky Anti-Virus autorise les activités réseau qui émanent de l'utilisateur.

  Attention ! Le mode furtif ne vous met pas à l'abri des chevaux de Troie!

  Le mode furtif est désactivé par défaut. Pour l'activer, cochez la case ☑ **Utiliser le mode furtif**.

14.4. Constitution d'une liste d'exclusions dans Kaspersky Anti-Virus

Si vous souhaitez exclure un objet quelconque de l'analyse ou de la protection en temps réel, vous pouvez soit saisir le chemin d'accès à cet objet ou définir des masques (ex. : *.bmp) dans la fenêtre **Menaces et exclusions** (cf. Illustration 27).

Cliquez sur Menaces et exclusions dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6). Afin d'ouvrir cette fenêtre et utilisez les divers boutons proposés pour rédiger la liste.

*Pour ajouter une exclusion, cliquez sur **Ajouter**.*

Cette action entraîne l'ouverture de la fenêtre **Objet exclus** (cf. ill. 35) dans laquelle vous pourrez définir les exclusions de Kaspersky Anti-Virus.

Les exclusions suivantes peuvent être définies :

- Disques, répertoires, fichiers et masques de fichier.
- *Menaces* : type de programme malveillant ou riskware.
- *Fichiers représentant une menace définie* : des fichiers concrets qui corresponde à une menace définie après analyse.

Afin d'exclure un répertoire ou un fichier quelconque (selon un masque) :

Il est indispensable de remplir le champ **Objet exclus** à l'aide du bouton ...

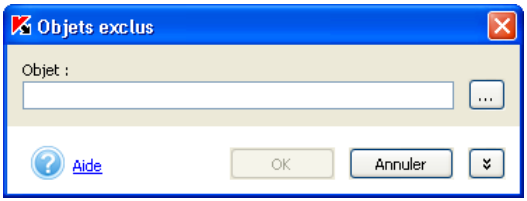


Illustration 35. Exclusions définies

Voici quelques exemples de masques admis :

- • Masques sans chemin vers l'objet
  - ***.exe** : tous les fichiers **.exe*
  - ***.ex?** : tous les fichiers **.ex?* où " ? " représente n'importe quel caractère
  - **test** : tous les fichiers appelés *test*
- Masque avec un chemin absolu vers l'objet
  - **C:\dir*.*** : tous les fichiers du répertoire *C:\dir\ :*
  - **C:\dir*.exe** : tous les fichiers *.exe du répertoire *C:\dir*
  - **C:\dir*.ex?** : tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère
  - **C:\dir\test** : uniquement le fichier *C:\dir\test*
  - **C:\dir**: tous les fichiers du répertoire *C:\dir* et de ses sous-répertoires
- • Masque avec un chemin relatif vers l'objet
  - **dir*.*** : tous les fichiers dans tous les répertoires *dir*
  - **dir\test** : tous les fichiers *test* dans tous les répertoires *dir*
  - **dir*.exe** : tous les fichiers *.*exe* dans tous les répertoires *dir*
  - **dir*.ex?** : tous les fichiers *.*ex*? dans tous les répertoires dir\ où " ? " peut représenter n'importe quel caractère
  - **dir*.*** : tous les fichiers dans tous les répertoires *dir* et leurs sous-répertoires

Il n'est pas conseillé de saisir des masques du ***.*** ou *, car cela reviendrait à désactiver la protection en temps réel.

Il n'est pas conseillé d'inclure le disque virtuel, créé à l'aide de la commande *subst* au départ du répertoire du système de fichier. dans la liste des exclusions. Cela n'aurait pas de sens car lors de l'analyse, Kaspersky Anti-Virus Personal considère ce disque virtuel comme un répertoire et, par conséquent, l'analyse.

Pour exclure du traitement antivirus tous les fichiers qui ont été rangés dans une catégorie de menace distincte après l'analyse :

Déroulez le reste de la fenêtre (cf. ill . 36) en cliquant sur et sélectionnez le type de menace dans la fenêtre **Liste des menaces identifiées** (cf . ill. 37) qui s'ouvre à l'aide du bouton .

Cette fenêtre vous permet de rechercher une menace sur une partie du nom, de trier la liste de menaces en cliquant sur l'en-tête de la colonne **Nom** et de copier le nom des menaces dans le presse-papier à l'aide des commandes du menu contextuel. Vous pouvez également consulter une description détaillée de la menace sur le site www.viruslist.com. Pour ce faire, sélectionnez la menace dans la liste et cliquez sur **Détails** dans le menu contextuel.

Par exemple, vous souhaitez utiliser les bases étendues mais vous ne voulez pas que Kaspersky Anti-Virus découvre les adwares. Dans ce cas, vous devrez sélectionner le type **not-a-virus:Adware.*** correspondant dans le champ **Menace**.

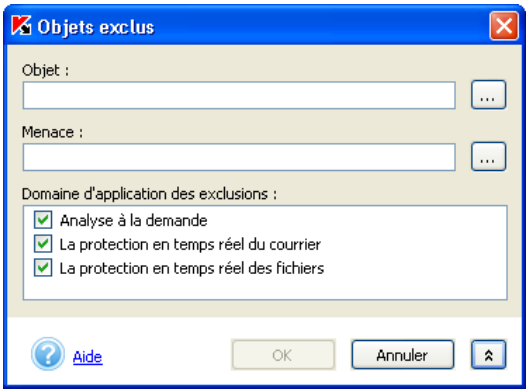


Illustration 36. Constitution de la liste des exclusions

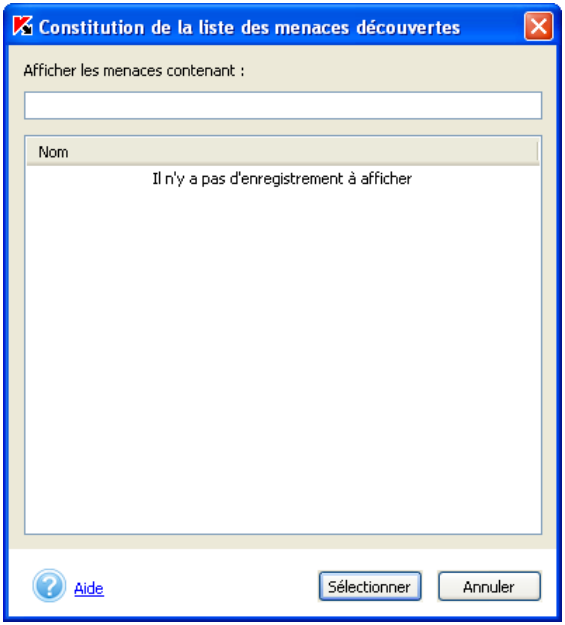


illustration 37. Liste de menaces identifiées

Pour exclure de la protection un objet particulier rangé dans une catégorie de menace que vous connaissez:

1. Saisissez le nom de l'objet dans le champ **Objet**.
2. Définissez la menace dans le champ **Menace**.

Par exemple, vous utilisez souvent les chats IRC qui sont considérés comme des riskwares par Kaspersky Anti-Virus. Pour les exclure de l'analyse, indiquez le fichier exécutable dans le champ **Objets**, puis saisissez **not-a-virus:Riskware.*** dans le champ **Menace**

Il est possible également d'exclure un fichier constituant une menace définie au départ de la notification qui s'affiche lorsque Kaspersky Anti-Virus découvre un tel fichier (cf. ill. 38).

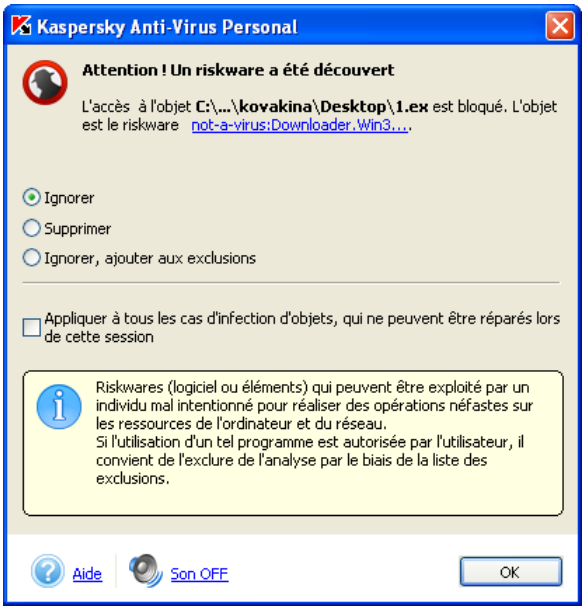


Illustration 38. Notification d'une menace

Vous pouvez définir également à quelle tâche les exclusions se rapportent. Vous avez le choix entre :

- **Analyse à la demande** : les exclusions définies seront utilisées uniquement lors de l'analyse complète
- **La protection en temps réel du courrier** : l'exclusion définie sera ignorée si elle est rencontrée dans un courrier électronique
- **La protection en temps réel des fichiers** : l'objet indiqué ne sera pas analysé par Kaspersky Anti-Virus lors de l'ouverture, de l'exécution ou de la sauvegarde.

14.5. Traitement des objets en quarantaine

Kaspersky Anti-Virus® Personal met en quarantaine tous les objets potentiellement infectés par un virus ou l'une de ses variantes découverts pendant l'analyse de l'ordinateur, de ses disques ou de ses fichiers ou pendant la protection en temps réel. Vous pouvez traiter les fichiers en quarantaine

(analyse, restauration, suppression, etc.). Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

L'*analyseur heuristique de code*, qui permet de déceler jusqu'à 92% des nouveaux virus, détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est relativement efficace et donne très rarement de fausses alertes.

Avant d'analyser les fichiers en quarantaine, 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 potentiellement infectés s'opère dans la fenêtre **Quarantaine** (cf. ill. 39) accessible en cliquant sur le lien Consulter la quarantaine de l'onglet **Protection** (cf. ill. 5) ou sur le lien Examen de la quarantaine dans la boîte de dialogue d'analyse (cf. ill. 8).

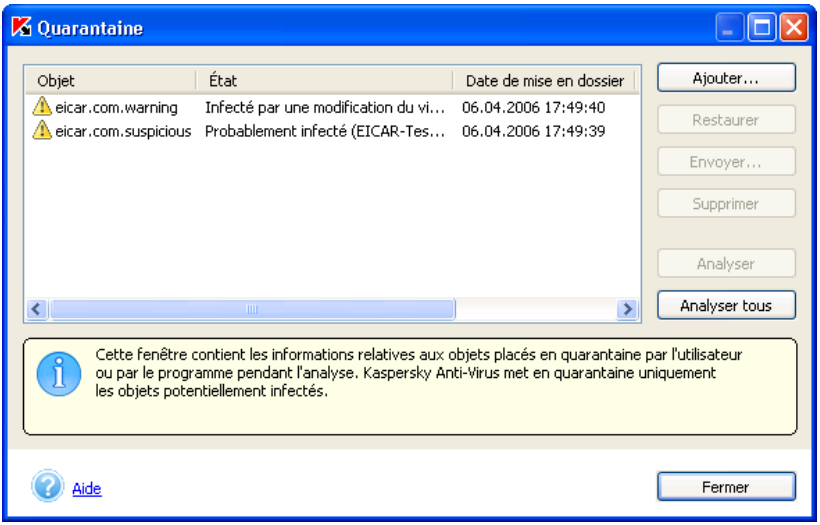


Illustration 39. Quarantaine avec des objets infectés

Vous pouvez réaliser les opérations suivantes :

- Mettre en quarantaine un fichier que vous croyez être infecté par un virus et qui n'aurait pas été découvert par Kaspersky Anti-Virus®. Cliquez pour ce faire sur **Ajouter** et sélectionnez le fichier potentiellement infecté. Il sera ajouté à la liste sous le signe *Mise en quarantaine par l'utilisateur.*
- Analyser et réparer à l'aide des dernières bases antivirus tous les objets potentiellement infectés ou uniquement certains d'entre eux. Pour ce

faire, cliquez sur **Analyser tous** 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*, *probablement infecté*, *fausse alerte, sain, etc*. Dans ce cas, un message de circonstance apparaît à l'écran et propose différents traitements possibles.

L'état *infecté* signifie que l'objet est bien dangereux 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 Probablement *infecté*, n'a pas été confirmé par Kaspersky Anti-Virus® Personal.

- Restaurer les fichiers dans leur répertoire d'origine, là où ils se trouvaient avant d'être mis en quarantaine. Pour restaurer un objet, sélectionnez-le dans la liste et cliquez sur **Restaurer**. Pour restaurer des objets issus d'archives, de bases de données de messagerie électronique ou de courriers individuels et placés en quarantaine, il est indispensable de désigner le répertoire dans lequel ils seront restaurés.

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

- Envoyer les objets potentiellement infectés aux experts de Kaspersky Lab en vue d'un examen. Veuillez envoyer ces objets uniquement si l'état *Probablement infecté* ne change pas en dépit d'analyses et de tentatives de réparation répétées. Pour ce faire, cliquez sur **Envoyer** (Consultez l'Annexe A à la page 124 pour de plus amples informations).

Nous attirons votre attention sur le fait que chaque fichier que vous envoyez à Kaspersky Lab doit avoir été analysé par Kaspersky Anti-Virus® Personal à l'aide des bases antivirus mises à jour au plus tard un jour avant l'envoi.

- Supprimer n'importe quel objet ou groupe d'objets de la quarantaine. Supprimez uniquement les objets qui ne peuvent être réparés. Afin de supprimer un objet, sélectionnez-le dans la liste puis cliquez sur **Supprimer**.

14.6. Manipulation des copies de sauvegarde

Le dossier de sauvegarde est un dossier spécial qui renferme les copies de sauvegarde des objets. La copie de sauvegarde est créée lors de la première tentative de réparation ou de suppression d'un objet. La principale fonction du dossier de sauvegarde est de permettre, à n'importe quel moment, la restauration de l'objet original !

Les manipulations sur les copies de sauvegarde ont lieu au départ de la boîte de dialogue **Dossier de sauvegarde** (cf. ill. 40). Pour ouvrir cette boîte de dialogue, cliquez sur Dossier de sauvegarde dans la partie gauche de l'onglet **Protection** (cf. ill. 5).

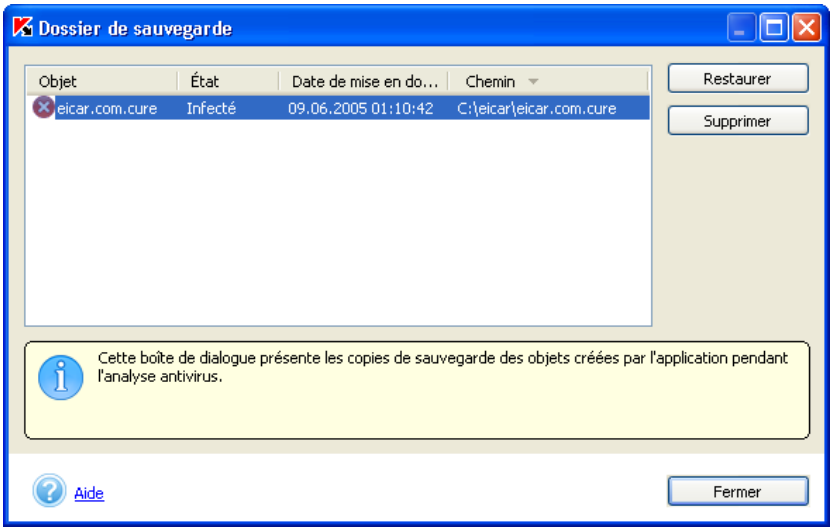


Illustration 40. Dossier renfermant les copies de sauvegarde des objets

La partie centrale de la fenêtre reprend la liste des copies de sauvegarde. Les informations suivantes sont fournies pour chaque copie : nom de l'objet pour lequel la copie a été créée, état de l'objet, date de création de la copie et chemin d'accès complet à l'emplacement d'origine de l'objet.

Vous pouvez restaurer une ou plusieurs copies ou les supprimer à l'aide des boutons correspondant.

L'objet est restauré au départ de la copie de sauvegarde et reçoit le même nom que celui qu'il avait avant la réparation.

Si l'emplacement d'origine de l'objet contient un autre objet portant un nom identique (une telle situation peut se présenter lors de la restauration d'un objet dont la copie avait été créée avant la réparation), le logiciel affichera le message de circonstance. Vous pouvez modifier le lieu de restauration de l'objet ou lui donner un autre nom.

Quand peut-on restaurer les copies de sauvegarde ?

Il n'est pas toujours possible de préserver l'intégrité d'un objet lors de sa réparation. Lorsque le fichier réparé contient des informations importantes et que ces informations sont devenues totalement ou partiellement inaccessibles, il est possible de tenter de restaurer l'objet à son état d'origine au départ de la copie de sauvegarde. Nous vous recommandons de rechercher la présence d'éventuels virus directement après la restauration. Il sera peut-être possible de le réparer avec les bases antivirus les plus récentes tout en préservant son intégrité.

Nous vous recommandons de ne pas restaurer les copies de sauvegarde des objets si cela n'est pas nécessaire. Cela pourrait en en effet entraîner l'infection de votre ordinateur.

Par défaut, la durée de conservation maximale des copies de sauvegarde et la taille maximale du dossier de sauvegarde ne sont pas limitées. Nous vous recommandons de passer régulièrement en revue le contenu du dossier afin de le nettoyer. Vous pouvez également configurer le logiciel de tel sorte qu'il supprime automatiquement les objets les plus anciens ou qu'il vous avertisse lorsque le dossier de sauvegarde a atteint sa capacité maximale (pour de plus amples informations, consultez le point 14.7 à la page 104).

14.7. Configuration complémentaire de la quarantaine

Vous pouvez configurer les paramètres de constitution et de fonctionnement de la quarantaine et du dossier de sauvegarde. Pour ce faire, cliquez sur le lien Quarantaine et dossier de sauvegarde de l'onglet **Paramètres** (cf. ill. 6) de la fenêtre principale et modifiez les paramètres suivants dans les sections correspondantes à la quarantaine et au dossier de sauvegarde (cf. ill. 41) :

- **Vérifier automatiquement tous les objets en quarantaine après chaque mise à jour des bases antivirus**. Ce mode de fonctionnement de Kaspersky Anti-Virus® vous permet de procéder automatiquement à une nouvelle analyse des objets en quarantaine après chaque mise à jour des bases antivirus.

Kaspersky Anti-Virus® ne pourra pas analyser les objets en quarantaine directement après la mise à jour des bases antivirus si vous travaillez avec ceux-ci.

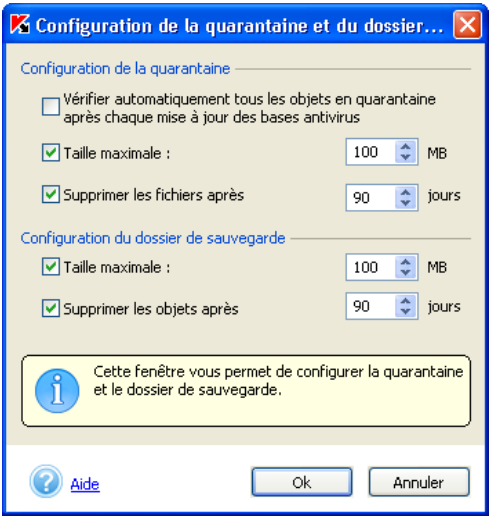


Illustration 41. Configuration de la quarantaine et du dossier de sauvegarde

Taille maximale… MB. Par défaut, la taille du dossier de quarantaine n'est pas définie (la case n'est pas cochée). Si vous souhaitez limiter la taille totale des fichiers mis en quarantaine, cochez la case adéquate et précisez la taille souhaitée dans la liste déroulante (la valeur de 100 Mo est sélectionnée par défaut. Lorsque la limite est atteinte, un message vous avertit.)

Supprimer les fichiers après … jours. Par défaut, la durée de conservation des fichiers en quarantaine n'est pas définie. Vous pouvez précisez cette durée en cochant la case adéquate et en saisissant la valeur souhaitée dans le champ (la durée proposée par défaut est de 90 jours).

La taille maximale du dossier et la durée de conservation des copies de sauvegarde sont identiques à celles de la quarantaine.

14.8. Utilisation des rapports

Des rapports sont constitués lors de l'analyse de l'ordinateur ou d'objets individuels, 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 à exécuter ou exécutées dans la fenêtre **Rapports** (cf. ill. 42). Pour ouvrir cette fenêtre, cliquez sur le lien Consulter les rapports dans la partie gauche de l'onglet **Protection** (cf. ill. 5).

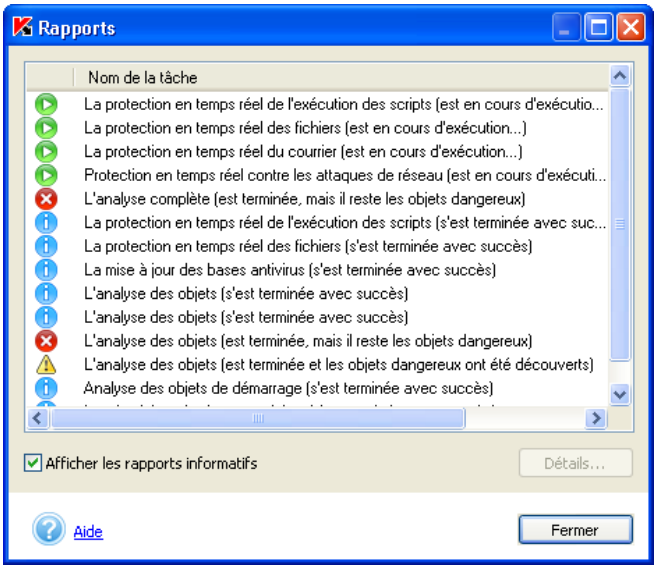


Illustration 42. Rapports

Les rapports peuvent appartenir à l'une des catégories suivantes :

- ou – *les rapports informatifs* contiennent de simples renseignements (ex. : tâche lancée, tâche exécutée, tâche en cours d'exécution, tâche interrompue).
- – *Les rapports d'avertissement* reprennent des informations critiques (ex. : Attention ! Il reste des objets qui n'ont pas été traités).
- – *Les rapports de remarque* apportent des commentaires sur quelques moments clé du fonctionnement de l'application (ex. : la tâche a été interrompue).

En général, les rapports informatifs n'ont aucun intérêt particulier. Vous pouvez en désactiver l'affichage. Pour ce faire, désélectionnez la case **Afficher les rapports informatifs**. Veuillez remarquer que les rapports relatifs à une tâche en cours et indiqués par l'icône seront toujours affichés.

Les rapports peuvent être classés par type, par nom (classement alphabétique) ou par heure de fin d'exécution. Pour annuler le classement, il suffit d'un clic gauche sur le titre de la colonne selon laquelle les rapports avaient été classés.

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…** ou faites un double-clic gauche.

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

Lorsque l'analyse complète est en cours, vous pouvez suivre son évolution sur les onglets correspondants (cf. ill. 8).

Ainsi, l'onglet **Statistiques** (cf. ill. 43) 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. Lors des mises à jour, cet onglet affiche les informations relatives à la taille totale de la mise à jour (sur le serveur de Kaspersky Lab ou dans le répertoire local) et au volume de données déjà téléchargé.

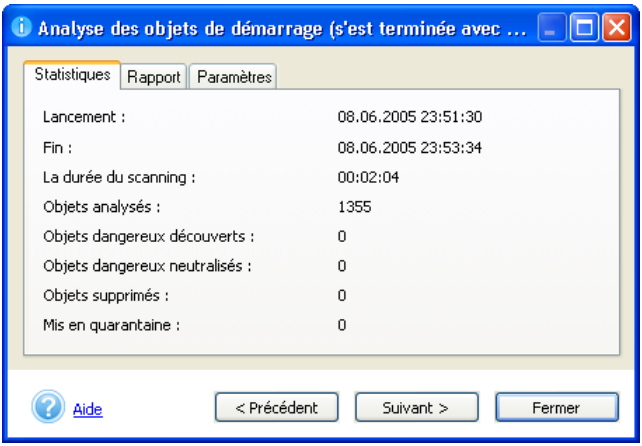


Illustration 43. Onglet **Statistiques**

L'onglet **Rapport** (cf. ill. 44) n'affiche par défaut aucune information sur les objets sains. Seules les informations sur les virus découverts sont affichées. Pour changer cet état de fait, il convient de cocher la case ☑ **Enregistrer tous les rapports** dans les options avancées de Kaspersky Lab (cf. 14.9, p. 111). Dès cet instant, l'onglet affichera les informations relatives à chacun des objets analysés. Pendant la mise à jour, il affichera des informations sur chacune des étapes de la procédure : connexion au serveur de mise à jour, fichiers

téléchargés, informations sur l'installation des mises à jour. Ces informations particulières sont toujours reprises, même si la case **Enregistrer tous les rapports** dans les options avancées de Kaspersky Anti-Virus® Personal n'a pas été cochée.

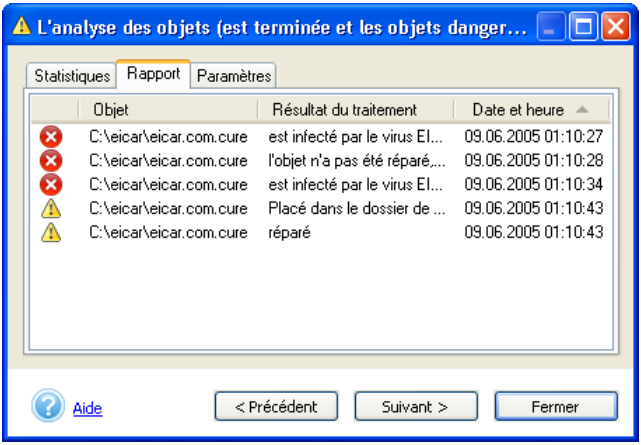


Illustration 44. Onglet **Rapport**

L'onglet **Paramètres** (cf. ill. 45) reprend les paramètres utilisés pour l'exécution des différentes tâches. Il reprend notamment les objets de l'analyse et le niveau de protection défini pour cette tâche, les actions exécutées sur les objets infectés, les programmes malicieux et les fichiers potentiellement infectés. On y retrouve également, le cas échéant, les exclusions définies. Pendant la mise à jour, cet onglet affiche les paramètres de la mise à jour, son type et sa source.

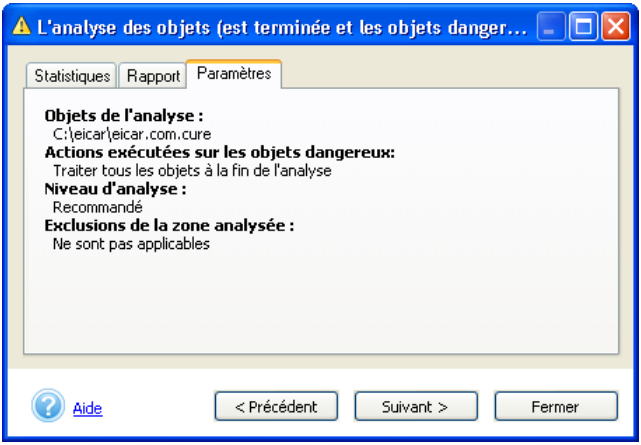


Illustration 45. Onglet **Paramètres**

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.

14.8.1. Représentation des rapports

Kaspersky Anti-Virus® Personal vous permet de configurer la nature des informations consignées dans le rapport. Ainsi, vous pouvez choisir de consigner uniquement les informations cruciales et d'ignorer les messages à caractère purement informatif.

Pour consigner tous les rapports, il suffit de cocher la case

☑ **Enregistrer tous les rapports**, dans la fenêtre **Options avancées** (cf. point 14.9, p. 111). Vous pouvez suivre la constitution des rapports en cliquant sur l'onglet **Rapport** dans la fenêtre d'analyse (cf. ill. 6) lors de l'analyse complète de votre ordinateur.

Lorsque la case est cochée, le rapport reprendra toutes les informations relatives à la tâche exécutée, y compris celles sur la réussite du traitement d'un objet.

Lorsque cette case n'est pas cochée, seuls les rapports d'avertissement et les rapports de remarque seront affichés, par exemple le fait qu'un objet n'ait pu être vérifié suite à une erreur, etc. Les messages relatifs à la réussite d'une analyse sont ignorés.

Afin de ne pas afficher les messages à caractère purement informatif lors de la session en cours, sans pour autant désélectionner la case

☑ ***Enregistrer les messages pour le rapport détaillé*** *:*

Lors de la consultation d'un rapport dans l'onglet **Rapport**, affichez le menu contextuel d'un clic droit (cf. ill. 46) et décochez **Afficher rapport détaillé**.

Illustration 46. Menu contextuel des rapports

Si la case ☑ **Enregistrer tous les rapports** dans les options avancées n'est pas cochée, la case **Afficher rapport détaillé** dans le menu contextuel est inactive. Vous ne pourrez donc configurer la nature des informations reprises dans le rapport.

Lors de la consultation du rapport en mode de surveillance (dans l'onglet **Rapport** pendant l'analyse), c'est la dernière entrée du rapport qui est toujours affichée par défaut. Pour désactiver ce mode, ouvrez le menu contextuel d'un clic droit et désélectionnez **Afficher la dernière entrée du rapport** ou sélectionnez simplement n'importe quelle entrée qui vous intéresse dans le rapport.

Vous pouvez également copier les informations relatives à un événement particulier dans le presse-papier. Pour ce faire, sélectionnez l'événement qui vous intéresse et cliquez sur la commande **Copier** dans le menu contextuel.

14.8.2. Exportation et envoi des rapports

Kaspersky Anti-Virus® Personal vous permet d'éditer la liste des rapports obtenus suite à l'exécution de telle ou telle action. Pour ce faire, utilisez le menu contextuel (cf. ill. 47) que vous pouvez ouvrir d'un clic droit dans la fenêtre **Rapports** (cf. ill. 42)

Illustration 47. Menu contextuel pour le travail avec les rapports

Il est impossible de supprimer les rapports pour les tâches qui sont toujours en cours d'exécution.

L'exportation d'un rapport détaillé vous permet de consulter les informations dans un tableau Microsoft Office Excel ou dans un fichier texte par exemple.

Si la tâche (ex. : analyse de l'ordinateur ou mise à jour des bases antivirus) a été interrompue ou si elle s'est soldée par un échec et que vous en ignorez les causes, vous pouvez envoyer le rapport relatif à cette tâche à Kaspersky Lab.

Pour ce faire, sélectionnez le rapport que vous souhaitez dans la boîte de dialogue **Rapports**, ouvrez le menu contextuel d'un clic droit et sélectionnez l'élément **Envoyer le rapport à Kaspersky Lab**. Cette action entraînera l'ouverture automatique du client de messagerie installé sur votre ordinateur, comme Microsoft Outlook Express, et la création d'un nouveau message reprenant le rapport en annexe. Ensuite, envoyez le message et les spécialistes de Kaspersky Lab tenteront de résoudre votre problème le plus rapidement possible.

La création automatique d'un message électronique s'opère uniquement dans les clients Microsoft Office Outlook et Microsoft Outlook Express. Si vous utilisez un autre client de messagerie (ex. : The Bat !), vous devrez configurer le soutien Simple MAPI de votre client de messagerie.

14.9. Configuration complémentaire de Kaspersky Anti-Virus® Personal

En plus des tâches concrètes, Kaspersky Anti-Virus® Personal vous permet de configurer toute une série de paramètres généraux et de services (cf. Illustration 48.).

Pour passer à la configuration avancée de Kaspersky Anti-Virus :

cliquez sur le lien Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6). Cette action entraîne l'ouverture d'une fenêtre contenant les onglets **Général**, **Performance** et **Sécurité**.

Pour ce faire, cliquez sur le lien Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6) et faites votre choix parmi les options proposées :

Sur l'onglet **Général** (cf. ill. Illustration 48.), vous pouvez configurer les paramètres suivants :

- **Afficher les infos-bulles** : active l'affichage à l'écran de tous les messages prévus pendant l'utilisation de Kaspersky Anti-Virus®. Nous vous conseillons de laisser ce mode activé car l'utilisateur est parfois sollicité, notamment pour définir le traitement des objets.

  Cette fonction n'est pas disponible sous Microsoft Windows 98 ou Microsoft Windows NT Workstation 4.0.

- **Utiliser la sonorisation** : active l'émission d'effets sonores lors d'événemens définis qui surviennent pendant l'utilisation de Kaspersky Anti-Virus. Vous pouvez consulter la liste des événements et modifier la sélection de son à l'aide des outils du système d'exploitation Microsoft Windows (**Démarrer → Paramètre → Panneau de configuration → Sons et périphériques audio → Sons**).
- **Animer l'icône dans la barre des tâches** : active l'animation de l'icône en fonction de l'opération exécutée par Kaspersky Anti-Virus. Ainsi, lors de l'analyse d'un message, l'icône se transforme en enveloppe qui clignote.

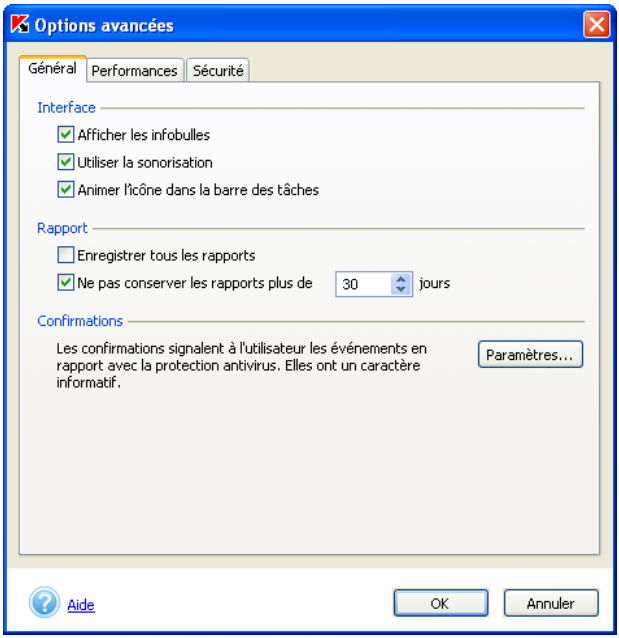


Illustration 48. Options avancées de Kaspersky Anti-Virus Personal. Onglet **Général**

- **Enregistrer tous les rapports**: enregistre tous les rapports générés pendant l'utilisation du logiciel : les messages informatifs, les avertissements d'erreur Ce mode est désactivé par défaut. Le rapport contiendra uniquement les messages les plus importants comme les erreurs survenues à la fin d'une tâche, l'interruption de l'exécution d'une tâche, etc.
- **Ne pas conserver les rapports plus de … jours** : Par défaut, les rapports sont conservés trente jours. Vous pouvez modifier cette durée en saisissant une nouvelle valeur dans le champ adéquat ou lever toute restriction en désélectionnant la case. La vérification de la durée de conservation des rapports et la suppression des anciens rapports s'opèrent lors du démarrage de Kaspersky Anti-Virus.

La section **Confirmation de l'action** règlemente l'affichage des notifications des événements survenus pendant l'utilisation de Kaspersky Anti-Virus. Ces messages ont en général un caractère purement informatif. Pour obtenir de plus amples informations sur la configuration des notifications, consultez le point 14.10 à la page 115.

L'onglet **Performance** (cf. ill. 49) vous permet de limiter l'analyse à la demande afin d'économiser la batterie (en cas d'utilisation d'un ordinateur portable) et les ressources du système d'exploitation (pour de plus amples informations, consultez le point 14.11 à la page 116).

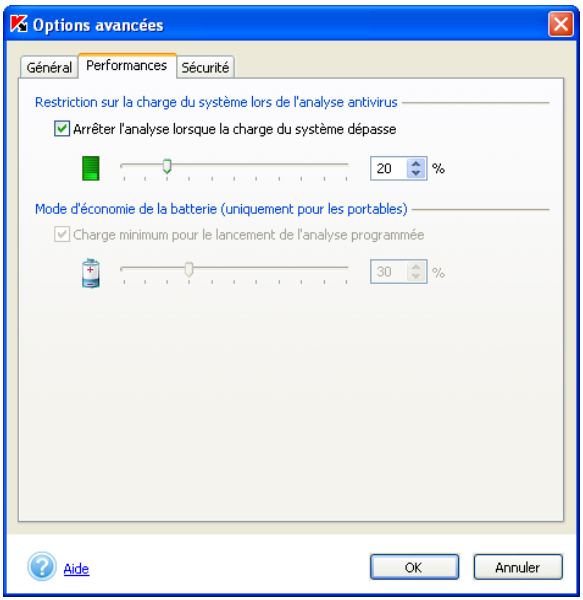


Illustration 49. Options avancées de Kaspersky Anti-Virus Personal. Onglet **Performances**

L'onglet **Sécurité** (cf. ill. 51) contient les paramètres suivants :

- **Lancer Kaspersky Anti-Virus Personal au démarrage du système** : démarre Kaspersky Anti-Virus® Personal après le démarrage du système d'exploitation.

  Nous insistons sur la nécessité de ne jamais fermer Kaspersky Anti-Virus® car cela pourrait entraîner une infection de votre ordinateur.

  Cette option ne vous sera pas proposée si vous ne jouissez pas des privilèges d'administrateur sur l'ordinateur.

- **Utiliser le système de restauration après les échecs** : active le système de restauration du travail de Kaspersky Anti-Virus en cas d'échec. Si le fonctionnement de l'application a été perturbé, la fenêtre principale de Kaspersky Anti-Virus se minimise(si elle était ouverte) et un message apparaît au-dessus de l'icône dans la barre des tâches (cf. ill. 50). La restauration automatique du travail de l'application se produit ensuite.

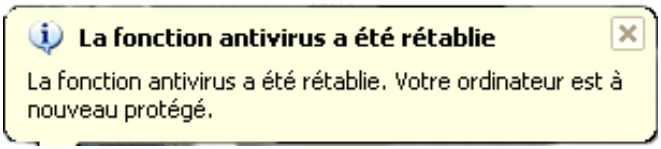


Illustration 50. Echec de l'application

- **Protéger le logiciel avec un mot de passe** : active la saisie obligatoire d'un mot de passe pour le passage en mode administrateur. Nous vous recommandons ce mode si d'autres personnes ont accès à votre ordinateur et si vous voulez empêcher celles-ci de modifier la configuration de la protection antivirus, de désactiver la protection en temps réel ou de décharger Kaspersky Anti-Virus (pour de plus amples informations, consultez le point 14.12 à la page 117) ou d'exécuter n'importe quelle tâche à l'aide de Kaspersky Anti-Virus® Personal. Vous devrez saisir un mot de passe de 1 à 32 caractères alpha-numériques dans le champ **Mot de passe** et le confirmer dans le champ **Confirmation du mot de passe**.

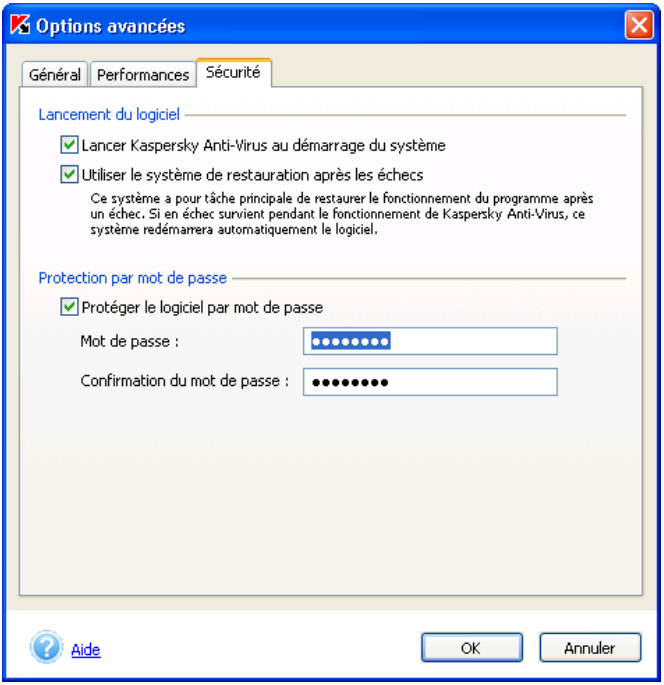


Illustration 51. Options avancées de Kaspersky Anti-Virus Personal. Onglet **Sécurité**

La section **Confirmations** vous permet de gérer l'affichage des notifications relatives à certains événements dans le cadre de l'utilisation de Kaspersky Anti-Virus. Ces confirmations ont un caractère purement informatif. Pour en savoir plus sur la configuration des confirmations, consultez le point 14.10 à la page 115.

14.10. Configuration des confirmations

Si vous souhaitez être averti chaque fois qu'un événement défini survient lors de l'utilisation du logiciel, cliquez sur le lien Options avancées dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6). Dans la fenêtre qui s'ouvre, cliquez sur **Paramètres…** dans la section **Confirmations**. Cette action entraînera l'ouverture de la fenêtre de configuration des confirmations (cf. ill. 52).

Les événements suivants ont été pris en compte:

- **Confirmer l'annulation de l'analyse** : affiche à l'écran une boîte de dialogue demandant la confirmation de l'annulation de l'analyse à la demande. Suite à l'annulation de l'analyse, une info-bulle reprenant la cause de l'annulation de l'analyse apparaîtra au-dessus de l'icône de l'application dans la barre des tâches.
- **Confirmer le chargement/déchargement de l'application** : affiche à l'écran une boîte de dialogue demandant la confirmation du lancement/de l'arrêt de Kaspersky Anti-Virus Personal.

Illustration 52. Configuration de la confirmation

- **Confirmer l'arrêt de la protection en temps réel** : affiche à l'écran un message vous avertissant de la désactivation totale de la protection en temps réel de votre ordinateur. Cette option n'est pas disponible si vous avez décidé de ne pas utiliser la protection en temps réel des fichiers au moment de l'installation de Kaspersky Anti-Virus Personal.
- **Confirmer le traitement des objets dangereux** : affiche à l'écran un message vous avertissant que certains objets infectés non pas été traités.

14.11. Restriction des performances de Kaspersky Anti-Virus

Vous pouvez limiter le lancement de l'analyse à la demande de Kaspersky Anti-Virus lorsqu'il est nécessaire d'économiser les ressources de l'ordinateur. Pour ce faire, cliquez sur le lien Options avancées dans la partie gauche de l'onglet

Paramètres (cf. ill. 6). Dans la fenêtre qui s'affiche, passez à l'onglet **Performance** (cf. ill. 49).

Voici les restrictions prévues :

- **Arrêter l'analyse antivirus si la charge du système est supérieure à …%** : arrête l'analyse à la demande si la charge du système de fichiers est supérieure à la valeur indiquée. Dès que celle-ci revient au niveau admis, l'analyse reprend. Vous pouvez définir la valeur du niveau de charge du système (en pour cent) admise à l'aide du curseur ou via une saisie directe dans le champ. L'analyse programmée ne sera pas lancée si la charge dépasse cette valeur.

  Ce paramètre porte uniquement sur l'analyse à la demande (par exemple, l'analyse d'un objet sélectionné). La protection en temps réel n'est pas touchée.

- **Ne pas réaliser l'analyse programmée si la charge de la batterie est inférieure à :** annule le lancement de l'analyse à la demande sur un ordinateur portable si le niveau de charge de la batterie est inférieur au niveau admis. Vous pouvez définir ce niveau (en pour cent) à l'aide du curseur ou via une saisie directe dans le champ à droite. L'analyse programmée ne sera pas lancée si la charge est inférieure à cette valeur.

  Ce paramètre est disponible uniquement si Kaspersky Anti-Virus est installé sur un ordinateur portable et que celui-ci est alimenté par une batterie.

14.12. Utilisation des modes administrateur et utilisateur

Kaspersky Anti-Virus peut fonctionner en mode administrateur ou en mode utilisateur. L'utilisation de ces modes peut s'avérer utile si d'autres personnes ont accès à votre ordinateur. Vous pouvez ainsi empêcher les autres utilisateurs de modifier la configuration de la protection antivirus, de désactiver la protection en temps réel ou de décharger Kaspersky Anti-Virus. En mode utilisateur, l'interface du logiciel est différente car les paramètres inaccessibles sont cachés (par exemple l'onglet **Paramètres** ne figure pas dans la fenêtre principale du logiciel).

Afin d'activer la permutation entre mode utilisateur et mode administrateur :

Cochez la case **Protéger le logiciel avec un mot de passe** sur l'onglet **Sécurité** (cf. ill. 51) de la fenêtre des options avancées de

Kaspersky Anti-Virus. Saisissez, dans le champ **Mot de passe**, le mot de passe souhaité et sa confirmation dans le champ **Confirmation du mot de passe**.

Cette action entraîne l'apparition du point **Passer au mode utilisateur** dans le menu contextuel (cf. ill. 4) grâce auquel vous pouvez passer en mode utilisateur. Pour revenir au mode administrateur, cliquez sur **Passer au mode administrateur** dans le menu contextuel et saisissez le mot de passe dans la fenêtre qui apparaît (cf. ill. 53).

Si la case **Protéger le logiciel avec un mot de passe** (cf. ill. 51) n'est pas cochée, Kaspersky Anti-Virus est lancé en mode administrateur.

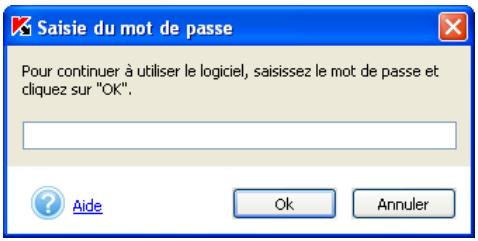


Illustration 53. Saisie du mot de passe

14.13. Gestion des configurations de Kaspersky Anti-Virus

Kaspersky Anti-Virus vous permet de créer et d'utiliser différentes configurations de travail. Vous pouvez désormais élaborer une configuration, la sauvegarder dans un fichier de configuration, *un profil*, et l'utiliser où et quand vous en aurez besoin.

Cliquez sur Administration des profils dans la partie gauche de l'onglet **Paramètres** (cf. ill. 6) si vous souhaitez gérer les configurations du logiciel.

Le bouton **Sauvegarder profil** vous permet de sauvegarder la configuration actuelle dans un fichier de configuration spécial. Le bouton **Charger profil** quant à lui vous permet d'appliquer un fichier de configuration quelconque pour Kaspersky Lab défini antérieurement. Il est possible que le chargement d'une nouvelle configuration entraîne le redémarrage de l'ordinateur car certains modes de fonctionnement sont activés lors du démarrage du système.

Pour rétablir la configuration recommandée, cliquez sur **Restaurer**.

CHAPITRE 15. QUESTIONS FREQUEMMENT POSEES

Ce chapitre est consacré aux questions les plus fréquentes des 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 : *Kaspersky Anti-Virus peut-il être utilisé simultanément avec les logiciels d'autres éditeurs* ?

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 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 Kaspersky Anti-Virus est le processeur. De plus, chaque nouveau virus ajouté à la base antivirus rallonge la durée de l'analyse.

A la différence des autres logiciels antivirus qui réduisent la durée de l'analyse en ignorant les virus les plus difficiles à déceler ou les plus rares (dans la zone géographique où l'éditeur est présent) ou en ignorant les formats plus complexe (par exemple, les pdf), Kaspersky Lab estime que la tâche d'un antivirus est de garantir la véritable protection antivirus des utilisateurs.

Kaspersky Anti-Virus permet à l'utilisateur expérimenté d'accélérer l'analyse antivirus en excluant divers type de fichiers de l'analyse. Il convient de remarque toutefois que cela s'accompagne d'une diminution du niveau de protection.

Kaspersky Anti-Virus est capable d'analyser 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 iChecker™ et iStream™.

Question : *A quoi sert la clé de licence? Kaspersky Anti-Virus 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, vous pouvez télécharger une version d'évaluation sur le site dans la rubrique **Téléchargements → Versions d'évaluation** La version d'évaluation fonctionnera pendant 15 jours. 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, contactez la société où vous avez acheté Kaspersky® Anti-Virus ou Kaspersky Lab directement.

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 offert par Kaspersky Lab présent 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 : *j'ai perdu ma connexion au réseau/à Internet après l'installation de Kaspersky Anti-Virus. Que faire* ?

Cela signifie qu'il y a eu un conflit entre le module de protection contre les attaques de réseau de Kaspersky Anti-Virus et le pare-feu installé sur votre ordinateur.

Pour rétablir la connexion au réseau local/à Internet, il faut désactiver la protection contre les attaques de réseau. Pour ce faire :

1. Ouvrez la fenêtre principale de Kaspersky Anti-Virus Personal Pro et passez à l'onglet **Paramètres** (cf. ill. 6)
2. Ouvrez, à l'aide du lien Protection en temps réel, la fenêtre **Configuration de la protection en temps réel** et sélectionnez l'onglet **Réseau.**
3. Désélectionnez la case **Activer la protection en temps réel contre les attaques de réseau** et cliquez sur **OK**.

Pour que les paramètres que vous avez sélectionnés entrent en vigueur, vous devez redémarrer l'ordinateur. Pour ce faire, cliquez sur **Oui** dans la fenêtre adéquate. Si vous souhaitez redémarrer l'ordinateur plus tard, cliquez sur **Non**.

Question : *depuis l'installation de Kaspersky Anti-Virus, l'ordinateur a un comportement bizarre (« écran bleu », redémarrage constant, etc.) Que faire ?*

Cela signifie qu'il y a un conflit entre Kaspersky Anti-Virus et une application installée sur l'ordinateur. Pour rétablir le bon fonctionnement de votre système d'exploitation, suivez ces instructions :

1. Appuyez sur **F8** au tout début du démarrage de l'ordinateur jusqu'à ce que le menu de sélection du mode de démarrage apparaisse.
2. Sélectionnez le point **Mode sans échec** et chargez le système d'exploitation.
3. Lancez Kaspersky Anti-Virus
4. Ouvrez l'onglet **Paramètres** de la fenêtre principale et cliquez sur le lien Options avancées.
5. Dans la fenêtre **Options avancées** qui s'ouvre, ouvrez l'onglet **Sécurité** (cf. ill. 51) et désélectionnez la case **Lancer Kaspersky Anti-Virus au démarrage du système**. Cliquez sur **Ok**.
6. Redémarrer le système d'exploitation en mode normal.

Ensuite, contactez le service d'assistance technique via le site Internet de Kaspersky Lab (rubrique **Services → Centre de support → Résoudre un problème**, Décrivez avec le plus de précision possible le problème et les conditions dans lesquelles il survient.

Il faudra joindre à la demande le fichier du tampon complet de la mémoire du système d'exploitation Microsoft Windows. Pour ce faire, suivez ces instructions :

1. Cliquez avec le bouton droit de la souris sur l'icône **Poste de travail** et sélectionnez **Propriétés** dans le menu contextuel qui s'affiche.
2. Dans la fenêtre **Propriétés du système**, sélectionnez l'onglet **Avancé** et dans la section **Démarrage et récupération**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Démarrage et récupération**, sélectionnez **Image mémoire complète** dans la liste déroulante de la section **Ecriture des informations de débogage**.

   Par défaut le fichier de l'image est sauvegardé dans le répertoire système *memory.dmp*. Vous pouvez modifier l'emplacement de sauvegarde en modifiant le nom du répertoire dans le champ correspondant.
4. Reproduisez le problème qui entraîne le gel de Kaspersky Anti-Virus.
5. Assurez-vous que l'image mémoire complète a bien été enregistrée.

ANNEXE A. 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. ill. 7) de la fenêtre principale du logiciel.

.

Cette action entraînera l'ouverture automatique d'une page Web reprenant un formulaire de contact du Service d'assistance technique. Vous devez remplir ce formulaire. La première fenêtre vous invite à saisir les données relatives au problème rencontré et à la licence de Kaspersky Anti-Virus :

- Sélectionnez le **Type de requête** dans la liste déroulante en indiquant le problème qui survient pendant l'utilisation de Kaspersky Anti-Virus Personal.
- Sélectionnez **Kaspersky Anti-Virus Personal** parmi les logiciels de Kaspersky Lab et décrivez en détails le problème que vous rencontrez dans le champ **Informations détaillées de la requête**.
- Sélectionnez le type d'enregistrement du programme en choisissant **Clé de licence** si vous avez achetez le logiciel dans un magasin ou si vous avez installé la licence depuis une disquette ou **commande en ligne** si vous avez acheté le logiciel en ligne.
- Saisissez le numéro de série de votre clé dans le champ **Numéro de sérié de la licence ou commande en ligne**. Ces informations figurent

dans le champ **Numéro** de la fenêtre **Administration des clés de licence** (cf. ill. 24).

- Saisissez votre adresse électronique dans le champ **Adresse électronique.**
- Cliquez sur **Suivant**.

La page suivante vous invite à décrire la configuration matériel et logiciel de l'ordinateur et les périphériques utilisés. Vous pouvez saisir ces informations manuellement ou utilisez le service de collecte automatique de ces informations. Pour ce faire, assurez-vous que votre navigateur accepte les objets Active-X puis cliquez sur **Saisir**. Fournissez également les informations suivantes:

- Si le problème est survenu pendant l'utilisation conjointe de Kaspersky Anti-Virus et d'un autre programme, veuillez saisir son nom dans le champ **Incompatibilités identifiées**.
- Saisissez vos coordonnées dans la rubrique **Coordonnées** afin que nous puissions vous contacter pour vous aider à résoudre le plus vite possible le problème.

Saisissez le code numérique spécial affiché dans la section **Protection contre l'enregistrement automatique** puis cliquez sur **Envoyer**.

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 14.5 à la page 100). 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.

Attention ! Vous pouvez envoyer les fichiers suspects à Kaspersky Lab uniquement s'ils ont été analysés avec les bases antivirus actualisées le jour de l'envoi.

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

Sélectionnez le fichier dans la fenêtre **Quarantaine** (cf. ill. 39) 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 potentiellement infecté. 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® Personal au plus tard un jour avant l'envoi.

Il peut arriver que Kaspersky Anti-Virus® Personal 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 pour examen dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 7). 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 B. GLOSSAIRE

Ce manuel reprend des termes et des concepts qui ont une signification particulière car ils sont en rapport avec le domaine de la protection antivirus. Cet appendice vise à expliquer ces différents concepts. Pour simplifier la consultation du glossaire, les termes ont été classés par ordre alphabétique.

A

Analyse à la demande : mode de fonctionnement du logiciel lancé par l'utilisateur et qui permet l'analyse de tous les fichiers de l'ordinateur.

Analyse heuristique : technologie qui augmente la probabilité de découvrir les virus inconnus. C'est grâce à elle que tous les objets soupçonnés d'être infectés par un virus inconnu ou une nouvelle variante d'un virus connu sont découverts.

Archives : fichiers contenant un ou plusieurs autres objets qui peuvent à leur tour être des archives.

Attaque de virus : ensemble de tentatives visant à infecter un ordinateur avec un virus

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. Ces bases de données évoluent au fil de l'apparition de nouveaux virus. Il est donc primordial que vous les *mettiez à jour* le plus souvent possible.

Bases de données de messagerie électronique : bases de données qui reprennent les messages électroniques sauvegardés sur votre ordinateur et qui ont un format particulier. Chaque message entrant/sortant est repris dans la base après son envoi ou sa réception. Ces bases sont couvertes lors de l'analyse complète de votre ordinateur.

Les messages entrants et sortant sont soumis à la recherche en temps réel de la présence éventuelle de virus au moment de l'envoi ou de la réception, lorsque la protection en temps réel est activée.

C

Clé de licence : fichier avec une extension *.key* qui représente votre clé personnelle, indispensable à l'utilisation de Kaspersky Anti-Virus® Personal. 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.

Correctif : ensemble de fichiers pour la mise à jour d'une application téléchargé via Internet et installé sur votre ordinateur.

D

Dossier de sauvegarde (BACKUP) : dossier spécial prévu pour conserver les copies de sauvegarde des objets créées avant la réparation ou la suppression.

Durée de validité de la licence : période pendant laquelle vous pouvez utiliser toutes les fonctions de Kaspersky Anti-Virus® Personal. 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 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 à la demande*. 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.

F

Fausse alerte : situation qui se produit lorsque le logiciel antivirus classe un objet sain dans la catégorie des objets infectés car son code évoque celui d'un virus.

Fichiers compactés : fichiers qui contiennent une application et les instructions du système d'exploitation pour l'exécuter.

I

Ignorer le fichier : mode de traitement qui consiste à bloquer l'accès au fichier (uniquement pour la protection en temps réel). Aucune action n'est réalisée, si ce n'est que les informations sont consignées dans le rapport.

M

Mémoire de l'ordinateur : mémoire vive de votre ordinateur.

Mise à jour des bases antivirus : l'une des fonctions exécutées par Kaspersky Anti-Virus® Personal. Elle permet de tenir la protection antivirus de l'ordinateur à jour. Les *bases antivirus* sont copiées depuis les *serveurs de mise à jour* de Kaspersky Lab sur votre ordinateur et installées automatiquement.

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

Modules de Kaspersky Anti-Virus® Personal : il s'agit des fichiers qui constituent le fichier d'installation de Kaspersky Anti-Virus® Personal et qui permettent au logiciel d'assurer ses principales fonctions. Chaque tâche réalisée par Kaspersky Anti-Virus® (*protection en temps réel*, *analyse à la demande* et *mise à jour*) dispose de son propre module exécutable. Lorsque vous lancez l'analyse complète depuis la fenêtre principale de l'application, vous lancez le module en charge de cette tâche.

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 dangereux : objet qui contient un virus. Il n'est pas conseillé de manipuler de tels objets car votre ordinateur risquerait d'être infecté. En cas de découverte d'un objet dangereux, il est conseillé de le réparé à l'aide de Kaspersky Anti-Virus Personal ou de le supprimer si la réparation n'est pas possible.

Objet OLE : objet joint ou intégré dans d'autres fichiers. Kaspersky Anti-Virus® Personal peut rechercher la présence éventuelle de virus dans de tels objets. Par exemple, si vous insérez un tableau Microsoft Office Excel dans un document Microsoft Office Word, il sera traité par Kaspersky Anti-Virus® comme un objet OLE.

Objet probablement infecté : 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. Les objets probablement infectés sont identifiés par *l'analyse heuristique*.

Objet potentiellement infecté : objet que vous soupçonnez être infecté. Il s'agit généralement de fichiers exécutables comme les fichiers *com* ou *exe* par exemple.

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

Prévention des infections : ensemble de mesures qui ont pour objectif d'empêcher l'infection de votre ordinateur par des virus. Ces mesures consistent notamment à garantir la protection antivirus et mettre à jour le logiciel, etc.

Protection en temps réel : mode d'utilisation de Kaspersky Anti-Virus® Personal pendant lequel le logiciel démarre automatiquement après le démarrage du système d'exploitation. Le logiciel intercepte toutes les tentatives de lecture, d'enregistrement et d'exécution d'un fichier et y recherche la présence éventuelle de virus. S'il ressort de l'analyse que l'objet est dangereux ou potentiellement infecté, Kaspersky Anti-Virus® en bloque l'accès et, en fonction de la configuration établie, tente de le traiter (réparation, suppression, mise en quarantaine, etc.).

Q

Quarantaine : répertoire utilisé par Kaspersky Anti-Virus® Personal pour entreposer tous les objets potentiellement infectés découvert lors de l'analyse ou pendant la *protection en temps réel*.

R

Réparation des objets dangereux : ensembles des moyens de traitement appliqués aux objets *infectés* qui débouchent sur une suppression complète ou partielle du code malicieux 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*.

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

S

Script : succession d'actions exécutées lors de l'utilisation de Microsoft Internet Explorer. Ces scénarios sont lancés par exemple à l'ouverture d'un site Internet quelconque. En mode de *protection en temps réel*, Kaspersky Anti-Virus® Personal surveille le lancement de ces scénarios, les intercepte et recherche la présence éventuelle de virus. En cas de découverte d'un script suspect, son exécution est bloquée.

Sécurité maximale : niveau de protection de votre ordinateur qui offre la protection antivirus la plus complète que Kaspersky Anti-Virus® Personal est capable de garantir. Dans ce mode, tous les fichiers de l'ordinateur, les disques amovibles et les unités de réseau (si elles sont raccordées à l'ordinateur) sont soumis à l'analyse antivirus.

Secteur d'amorçage : secteur se trouvant sur le disque dur de l'ordinateur ou tout autre média amovible (disque, cd-rom) est réparti. Il existe toute une famille de virus qui infectent ces secteurs : les *virus de démarrage*. Kaspersky Anti-Virus® Personal peut rechercher la présence éventuelle de virus sur ces secteurs et, le cas échéant, les *réparer*.

Secteur de démarrage : section spéciale du disque qui contient le programme de lancement du système d'exploitation sur votre ordinateur.

Serveurs de mises à jour de Kaspersky Lab : listes des serveurs http et ftp de Kaspersky Lab à partir desquels Kaspersky Anti-Virus® Personal copie les bases antivirus sur votre ordinateur.

Suppression d'un objet : mode de traitement d'un objet qui consiste à le supprimer de votre ordinateur. Ce traitement est recommandé pour les objets dangereux qui ne peuvent être réparés pour une raison ou l'autre.

T

Technologie iChecker™ : technologie qui permet d'accélérer l'analyse antivirus grâce à l'exclusion des objets qui n'ont pas été modifiés depuis l'analyse précédente, pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Les informations relatives à ce sujet sont conservées dans une base de données spéciales.

Admettons que vous ayez une archive qui a été analysé par Kaspersky Anti-Virus et qui est sain. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apporté au fichier en question ou aux paramètres de l'analyse. Si vous avez changé le contenu de l'archive (ex. : ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

La technologie iChecker™ a ses limites : elle ne s'applique qu'aux objets dont la structure est connue de Kaspersky Anti-Virus (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

Technologie iStreams™ : technologie similaire à **iChecker™**. La différence réside dans le fait que dans le cadre de la technologie iStreams™, les informations relatives à l'analyse d'un objet sont conservées dans le flux complémentaire de l'objet. De plus, la technologie iStreams™ est applicable à n'importe quel type d'objet, que sa structure soit connue ou non de Kaspersky Anti-Virus.

La technologie iStreams™ a ses limites : elle ne peut être utilisée dans sur les disques avec un système de fichiers NTFS.

V

Virus de démarrage : virus qui a infecté le *secteur d'amorçage* des disques de votre ordinateur. Le virus " oblige " le système lors du redémarrage à lire en mémoire et transmettre la gestion non pas au code original mais bien au code du virus.

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 *potentiellement infectés*.

Vitesse maximale : niveau de protection pour lequel seuls les objets potentiellement infectés sont soumis à l'analyse. C'est ce qui permet d'accélérer la vitesse de l'analyse.

ANNEXE C. KASPERSKY LAB

Fondé en 1997, Kaspersky Lab est devenu un leader reconnu en technologies de sécurité de l'information. Il produit un large éventail de logiciels de sécurité des données, et distribue des solutions techniquement avancées et complètes afin de protéger les ordinateurs et les réseaux contre tous types de programmes malveillants, les courriers électroniques non sollicités ou indésirables, et contre les tentatives d'intrusion.

Kaspersky Lab est une compagnie internationale. Son siège principal se trouve dans la Fédération Russe, et la société possède des délégations au Royaume Uni, en France, en Allemagne, au Japon, aux États-Unis (Canada), dans les pays du Benelux, en Chine et en Pologne. Un nouveau service de la compagnie, le centre européen de recherches anti-Virus, a été récemment installé en France. Le réseau de partenaires de Kaspersky Lab compte plus de 500 entreprises du monde entier.

Aujourd'hui, Kaspersky Lab emploie plus de 250 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Une analyse complète du comportement des virus d'ordinateur permet à la société de fournir une protection complète contre les risques actuels, et même contre les menaces futures. La résistance à de futures attaques est la stratégie de base mise en œuvre dans toutes les applications Kaspersky Lab. Les produits de la société ont toujours fait preuve d'une longueur d'avance sur ceux de ses nombreux concurrents, pour améliorer la protection antivirus aussi bien des utilisateurs domestiques que des entreprises clientes.

Des années de dur travail ont fait de notre société l'un des leaders de la fabrication de logiciels de sécurité. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. Ses outils de gestion intuitifs et faciles à utiliser se prêtent à une automation avancée, en vue d'une protection antivirus rapide à l'échelle de l'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Antivirus : Nokia ICG (États-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (États-Unis), G Data (Allemagne), Deerfield (États-Unis), Alt-N (États-Unis), Microworld (Inde), BorderWare (Canada), etc.

Les clients de Kaspersky Lab profitent d'un large éventail de services supplémentaires qui leur assurent non seulement un bon fonctionnement des applications, mais également l'adaptation à certaines exigences spécifiques de leurs entreprises. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. La société offre à ses clients un service technique 24/24, disponible en plusieurs langues, et adapté à une clientèle internationale.

C.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal Pro

Le paquet logiciel est conçu pour offrir une protection antivirale intégrale des ordinateurs personnels sous système d'exploitation Microsoft Windows 98/ME, Microsoft Windows 2000/NT, et Microsoft Windows XP, ainsi que des applications Microsoft Office. Kaspersky Anti-Virus® Personal Pro dispose d'un outil intégré de mise à jour pour le téléchargement des bases de données antivirus et des modules de programmes. Un système exclusif d'analyse heuristique détecte efficacement même les virus inconnus. Ce système d'analyse heuristique de seconde génération parvient à neutraliser les virus inconnus. L'utilisateur peut facilement configurer l'application à travers une interface simple et facile.

Kaspersky Anti-Virus® Personal Pro possède les caractéristiques suivantes :

- **Analyse à la demande** des unités locales ;
- **Protection automatique en temps réel** de tous les fichiers, contre les virus;
- **Filtre de courrier** qui analyse et désinfecte automatiquement tout le trafic de messagerie entrant et sortant de n'importe quel client de messagerie utilisant les protocoles POP3 et SMTP et détecte efficacement les virus dans les bases de données de messagerie ;
- **Bloqueur de comportements** qui assure une protection maximale des applications MS Office contre les virus ;
- **Analyseur de fichier compressés –** Kaspersky Anti-Virus prend en charge plus de 700 formats de fichiers d'archives ou compressés ; il assure l'analyse antivirale automatique de leur contenu, ainsi que la suppression de tout code dangereux dans les fichiers au format **ZIP**, **CAB**, **RAR**, **ARJ**, **LHA** ou **ICE**.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Microsoft 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® Personal Security Suite

Kaspersky® Personal Security Suite est une suite logicielle conçue pour organiser la protection intégrée des ordinateurs personnels tournant sous Microsoft Windows. Cette solution bloque l'intrusion des programmes malveillants et des riskwares via toutes les sources d'infection possible, vous protège contre l'accès non-autorisés à vos données et lutte contre le courrier indésirable.

Kaspersky® Personal Security Suite possède les fonctions suivantes :

- Protection des données de votre ordinateur contre les virus.
- Protection des utilisateurs des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express contre le courrier indésirable.
- Protection de l'ordinateur contre l'accès non-autorisé aux données ainsi que contre les attaques de pirates informatiques réalisées depuis le réseau local ou Internet.

Kaspersky Lab News Agent

Le programme News Agent a été développé pour communiquer les informations relatives à Kaspersky Lab, la “météo” des virus et les dernières infos. Le programme se connecte selon une fréquence déterminée au serveur d’informations de Kaspersky Lab afin de relever les infos des différents canaux.

News Agent permet également de:

- Visualiser la « météo » des virus dans la barre des tâches;
- S’abonner et se désabonner aux canaux d’information de Kaspersky Lab;
- Recevoir selon une fréquence définie les informations des canaux auxquels on est abonné et de recevoir une notification en cas d’informations non lues;
- Lire les informations dans les canaux auxquels on est abonné;
- Consulter la liste des canaux et leur contenu;
- Ouvrir dans le navigateur une page contenant la version complète de l’information.

News Agent tourne sous Microsoft Windows et peut être utilisé comme produit autonome ou être intégré à diverses solutions de Kaspersky Lab.

Kaspersky OnLine Scanner

Il s’agit d’un service gratuit offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace en ligne de l’ordinateur. Kaspersky OnLine Scanner fonctionne directement dans le navigateur à l’aide de la technologie Microsoft ActiveX®. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes sur une infection éventuelle. Dans le cadre de l’analyse, l’utilisateur peut :

- Exclure les archives et les bases de données de messagerie;
- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l’analyse au format txt ou html.

Kaspersky® OnLine Scanner Pro

Il s’agit d’un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l’ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro fonctionne directement dans le navigateur à l’aide de la technologie Microsoft ActiveX®. Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes sur une infection éventuelle. Dans le cadre de l’analyse, l’utilisateur peut :

- Exclure les archives et les bases de données de messagerie;

- Sélectionner les bases standard ou étendues;
- Enregistrer le rapport sur les résultats de l'analyse au format txt ou html;

Kaspersky Anti-Virus 6.0

Kaspersky Anti-Virus 6.0 a été développé pour protéger les ordinateurs personnels contre les programmes malveillants. Il présente une combinaison optimale de méthodes traditionnelles de lutte contre les virus et de technologies proactives.

Le programme assure une analyse antivirus sophistiquée, notamment :

- Analyse antivirus du trafic de messagerie au niveau du protocole de transfert des données (POP3, IMAP ou NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé et analyse et réparation des bases antivirus.
- Analyse en temps réel du trafic Internet transmis via le protocole HTTP.
- Analyse antivirus de n'importe quel fichier, répertoire ou disque. De plus, au départ de la tâche proposée, il est possible de lancer la recherche d'éventuels virus uniquement dans les secteurs critiques du système d'exploitation ou dans les objets chargés au démarrage du système d'exploitation de Microsoft Windows.

La défense proactive permet de :

- **Contrôler les modifications du système de fichiers**. Le programme autorise la création de listes d'applications dont la composition sera contrôlée. Les programmes malveillants ne pourront pas ainsi violer l'intégrité de l'application.
- **Observer les processus dans la mémoire vive**. Kaspersky Anti-Virus 6.0 avertit en temps utiles l'utilisateur en cas de détection de processus dangereux, suspects ou dissimulés ou en cas de modification non autorisée des processus normaux.
- **Surveiller les modifications de la base de registres système** grâce au contrôle de l'état de la base de registres.
- **Bloquer les macros Visual Basic for Applications dangereuses** dans les documents Microsoft Office.
- **Restaurer le système** après les actions malveillantes des logiciels espion : grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 est une solution sophistiquée de protection des ordinateurs personnels contre les principales menaces informatiques que sont les virus, les pirates, le courrier indésirable et les logiciels espion. L'interface utilisateur unique permet de configurer et d'administrer tous les composants de la solution.

Les fonctions antivirus proposées sont les suivantes :

- **Analyse antivirus du flux de messagerie** au niveau du protocole de transfert des données (POP3, IMAP et NNTP pour le courrier entrant et SMTP pour le courrier sortant) quel que soit le client de messagerie utilisé. La réparation des messages infectés dans les bases de messagerie et des plug in sont prévus pour les clients de messagerie les plus utilisés (Microsoft Office Outlook, Microsoft Outlook Express et The Bat!)
- **Analyse en temps réel du trafic Internet** transmis via le protocole HTTP.
- **Protection du système de fichiers :** n'importe quel fichier, répertoire ou disque peut être soumis à l'analyse antivirus. Il est possible également d'analyser uniquement les secteurs critiques du système d'exploitation et les objets lancés au démarrage de Microsoft Windows.
- **Protection proactive** : le programme surveille en permanence l'activité des applications et des processus exécutés dans la mémoire vive de l'ordinateur, empêche les modifications dangereuses du système de fichiers et rétablit le système arpès une action malveillante.

La **protection contre les escroqueries en ligne** est assurée grâce à l'identification des attaques de phishing. La fuite d'informations confidentielles est ainsi évitée (il s'agit avant tout des mots de passe, des numéros de compte et de carte bancaires, blocage de l'exécution de scripts dangereux, des fenêtres pop up et des bannières). La **fonction de blocage des appels téléphoniques payants** permet d'identifier les programmes qui tentent d'établir une connexion cachée via votre modem à des services téléphoniques payant et de les bloquer.

Kaspersky® Internet Security 6.0 **identifie les tentatives de balayage des ports de votre ordinateur**, signe précurseur des attaques de réseau et bloque avec succès les attaques de pirates informatiques les plus répandues. **Sur la base des règles définies**, le programme surveille toutes les interactions au niveau du réseau et contrôle tous **les paquets entrants et sortants**. **Le mode furtif (**technologie SmartStealth™**) empêche la découverte de votre ordinateur de l'extérieur du réseau**. Lorsque ce mode est activé,toutes les activités de réseau sont bloquées, à l'exception de celles autorisées par les règles d'exception définies par l'utilisateur.

Le programme adopte une démarche complexe pour le filtrage du courrier entrant afin d'identifier les messages non sollicités :

- Vérification selon des listes « blanche » ou « noire » d'adresses (y compris les adresses de sites de phishing) ;
- Analyse des expressions dans le corps des messages ;
- Analyse du corps des messages à l'aide d'un algorithme d'auto-apprentissage ;
- Identification du spam sous forme graphique.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. 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 dans la mémoire du PDA ou du téléphone intelligent 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[8] intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;

[8] En fonction du type de livraison

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

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 Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition ;
- *Ordinateurs de poche* sous Microsoft Windows CE et Palm OS et téléphones intelligents tournant sous Microsoft Windows Mobile 2003 for Smartphone et Microsoft Smartphone 2002.

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 SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix est une solution conçue pour le traitement antivirus des messages livrés via le protocole SMTP. L'application contient toute une série d'outils de filtrage du flux de messagerie : selon le nom et le type MIME des fichiers joints ainsi que plusieurs moyens permettant de réduire la charge du système de messagerie et de prévenir les attaques de pirates informatiques. Citons, entre autres, les restrictions au niveau de la taille des messages, du nombre de destinataires, etc. La prise en charge de la technologie DNS Black List évite de recevoir des messages en provenance de serveurs repris dans la liste des serveurs de diffusion de courrier indésirable.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange recherche la présence éventuelle de virus dans le courrier entrant et sortant, ainsi que dans les messages enregistrés sur le serveur, y compris les messages dans les dossiers partagés. Il rejette également le courrier indésirable grâce à l'exploitation de technologies intelligentes d'identification des messages non sollicités conjointement aux technologies développées par Microsoft. L'application recherche la présence d'éventuels virus dans tous les messages qui arrivent sur le serveur Exchange via le protocole SMTP à l'aide de technologies mises au point par Kaspersky Lab et identifie le courrier indésirable grâce à des filtres formels (adresse électronique, adresse IP, taille du message, en-tête) et à l'analyse du contenu du message et des pièces jointes à l' aide de technologies intelligentes dont des signatures graphiques uniques qui permettent d'identifier le courrier indésirable sous forme graphique. Le corps du message et les pièces jointes sont soumis à l'analyse.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway est une solution universelle pour la protection avancée des utilisateurs des systèmes de messagerie. L'application, qui est installée entre le pare-feu de l'entreprise et Internet, analyse tous les éléments du message électronique et recherche la présence éventuelle de virus et d'autres programmes malveillants (spyware, adware, etc.). Il opère également un filtrage centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie.

C.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://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE D. CONTRAT DE LICENCE

NOTE A TOUS LES UTILISATEURS: VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT DE LICENCE ("LICENCE") SUIVANT QUI CONCERNE LE LOGICIEL ("LOGICIEL") CONÇU PAR KASPERSKY LAB ("KASPERSKY LAB").

SI VOUS AVEZ ACHETE CE LOGICIEL VIA INTERNET EN CLIQUANT SUR LE BOUTON ACCEPTER, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER ET DE DEVENIR PARTIE DE CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, CLIQUEZ SUR LE BOUTON INDIQUANT QUE VOUS N'ACCEPTEZ PAS LES TERMES DE CE CONTRAT ET QUE VOUS N'INSTALLEZ PAS LE LOGICIEL.

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN OUVRANT LE BOÎTIER DU CD VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL.

CONFORMÉMENT À LA LÉGISLATION, LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) ACHETÉS EN LIGNE VIA INTERNET CHEZ KASPERSKY LAB BÉNÉFICIENT D'UN DÉLAI DE RÉTRACTATION DE 7 JOURS FRANCS À COMPTER DE LA RÉCEPTION DES BIEN ACHETÉS, SI CES LOGICIELS N'ONT PAS ÉTÉ DESCELLÉS.

CONCERNANT LES LOGICIELS KASPERSKY DESTINÉS AUX PARTICULIERS (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY ANTI-SPAM PERSONAL, KASPERSKY SECURITY SUITE PERSONAL, KASPERSKY SECURITY FOR PDA) NON ACHETÉS EN LIGNE VIA INTERNET, ILS NE SERONT NI REPRIS NI ÉCHANGÉS SAUF DISPOSITIONS CONTRAIRES PROPRES AU PARTENAIRE CHEZ QUI LE PRODUIT A ÉTÉ ACHETÉ. DANS CE CAS, KASPERSKY LAB N'EST EN AUCUN CAS ENGAGÉ PAR LES CLAUSES DES PARTENAIRES.

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 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, 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*. Kaspersky Lab vous fournira une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

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 six (6) mois suivant le téléchargement ou l'installation du logiciel, acheté de manière physique, 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 (vi) 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 (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i) au-dessus, 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. (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) ci-dessous, 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).