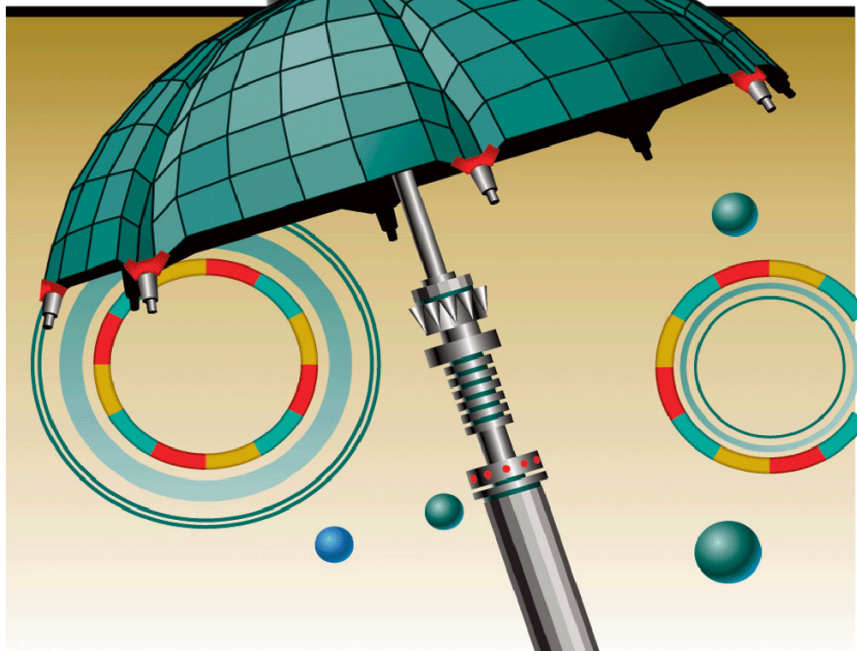


KASPERSKY LABS

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



KASPERSKY™



Kaspersky Anti-Virus® Personal 5.0

MANUEL DE L'UTILISATEUR

KASPERSKY ANTI-VIRUS® PERSONAL 5.0

Manuel de l'utilisateur

© Kaspersky Labs Ltd.
<http://www.kaspersky.com/>

Date d'édition: avril 2004

Sommaire

CHAPITRE 1. INTRODUCTION	5
1.1. Virus informatiques et programmes malicieux	5
1.2. Présentation et fonctions principales de Kaspersky Anti-Virus® Personal	6
1.3. Nouveautés de la version 5.0	8
1.4. Configuration matérielle et logicielle requise	9
1.5. Contenu du pack logiciel	10
1.6. Services réservés aux utilisateurs enregistrés	11
CHAPITRE 2. INSTALLATION DU LOGICIEL.....	12
CHAPITRE 3. QUE FAIRE EN CAS D'INFECTION DE VOTRE ORDINATEUR.....	16
3.1. Signes d'une infection	16
3.2. Que faire lorsque les symptômes d'une infection sont présents ?	17
CHAPITRE 4. PROTECTION DE L'ORDINATEUR SANS CONFIGURATION COMPLEMENTAIRE DE L'ANTIVIRUS.....	19
4.1. Protection en temps réel	19
4.2. Analyse de l'ordinateur à la demande	20
4.3. Mise à jour des bases antivirus.....	22
CHAPITRE 5. INTERFACE DU LOGICIEL	23
5.1. Icône de la barre des tâches.....	23
5.2. Menu contextuel	23
5.3. Fenêtre principale du logiciel : structure générale.....	24
5.3.1. Onglet <i>Protection</i>	26
5.3.2. Onglet <i>Paramètres</i>	28
5.3.3. Onglet <i>Assistance technique</i>	29
5.4. Fenêtre du processus d'analyse	30
5.5. Aide	31
CHAPITRE 6. PREVENTION DES INFECTIONS DE VOTRE ORDINATEUR.....	32
6.1. Quand faut-il lancer une analyse antivirus de l'ordinateur ?	34
6.2. Configuration à utiliser pour l'analyse	35
6.3. Analyse à la demande.....	40
6.4. Analyse complète programmée.....	41
6.5. Analyse d'objets individuels	42

6.6. Analyse des archives	44
CHAPITRE 7. ANALYSE D'UN CD-ROM OU D'UNE DISQUETTE	47
CHAPITRE 8. CONFIGURATION DE LA PROTECTION EN TEMPS REEL.....	49
8.1. Vérification de l'état de la protection	49
8.2. Actions réalisées par le logiciel et niveau de protection.....	50
CHAPITRE 9. PROTECTION DU COURRIER CONTRE LES VIRUS	55
CHAPITRE 10. TRAITEMENT DES VIRUS.....	57
CHAPITRE 11. RENOUELEMENT DE LA LICENCE.....	59
CHAPITRE 12. TELECHARGEMENT DES MISES A JOUR	61
12.1. Nécessité de la mise à jour	61
12.2. Téléchargement des mises à jour depuis Internet	62
12.3. Téléchargement des mises à jour depuis un répertoire local.....	63
12.4. Mise à jour des modules du logiciel Kaspersky Anti-Virus® Personal.....	65
12.5. Configuration des mises à jour. Programmation.....	65
12.6. Mise à jour manuelle. Téléchargement des mises à jour	66
CHAPITRE 13. POSSIBILITES COMPLEMENTAIRES.....	68
13.1. Configuration des paramètres de la protection en temps réel.....	68
13.2. Configuration des paramètres d'analyse à la demande	71
13.3. Traitement des objets en quarantaine	72
13.4. Configuration complémentaire de la quarantaine	75
13.5. Utilisation des rapports	76
13.5.1. Représentation des informations	79
13.5.2. Exportation et envoi des rapports	80
13.6. Configuration complémentaire de Kaspersky Anti-Virus® Personal.....	81
ANNEXE A. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE	84
ANNEXE B. GLOSSAIRE	86
ANNEXE C. KASPERSKY LABS LTD.	91
C.1. Autres produits antivirus	91
C.2. Coordonnées	95
ANNEXE D. CONTRAT DE LICENCE	96

CHAPITRE 1. INTRODUCTION

1.1. Virus informatiques et programmes malicieux

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

Afin de pouvoir identifier les menaces qui planent sur vos données, il convient de définir les différents types de programmes malicieux et leur *modus operandi*. Il en existe trois catégories :

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

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

- **Les virus** : 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 savoir *l'infection*. La vitesse de propagation des virus est légèrement inférieure à celle des vers.
- **Les 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. La mise en place d'une procédure de sauvegarde régulière des informations vous permettra de réduire au minimum les risques de perte d'informations.

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.

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



Dans ce manuel, le terme " virus " désignera aussi bien les virus que les chevaux de Troie et les vers. 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 Windows® (cf. point 1.4, p. 9).

Kaspersky Anti-Virus® Personal assure les fonctions suivantes :

- **Protection contre les virus et les programmes malicieux** : il identifie et neutralise les programmes malicieux qui se propagent via le courrier électronique, les protocoles Internet et les média fixes ou amovibles. Le logiciel fonctionne selon deux modes (utilisables séparément ou conjointement) :
 - La **protection en temps réel** permet de rechercher la présence éventuelle de virus dans tous les objets exécutés, ouverts et enregistrés sur l'ordinateur.
 - **L'analyse à la demande** permet de rechercher la présence éventuelle de virus et de réparer, le cas échéant, les objets infectés sur tout l'ordinateur ou sur des disques, dans des

fichiers ou des dossiers particuliers. Cette analyse peut-être lancée manuellement ou automatiquement selon un horaire défini.

- **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 Labs vous permettent de vous débarrasser de l'ensemble des virus qui ont infecté vos données.
- **Analyse et réparation du courrier entrant et sortant.** Le courrier entrant est analysé et les réparations nécessaires sont effectuées avant que les messages n'arrivent dans la boîte aux lettres tandis que le courrier sortant est analysé en temps réel¹. De plus, il est possible de procéder à l'analyse à la demande² des bases de messagerie électronique de différents clients et de réaliser les réparations qui s'imposent (cf. Chapitre 9, p. 55).
- **Mise à jour des bases antivirus et des modules de programme** afin de toujours disposer des dernières informations sur les nouveaux virus, des moyens de réparer les objets infectés ainsi que des dernières versions des modules du programme. Les mises à jour sont téléchargées depuis les serveurs de mise à jour de Kaspersky Labs ou installées depuis un répertoire local.
- **Recommandations sur la configuration du logiciel et son utilisation.** Pour chaque opération réalisée à l'aide de Kaspersky Anti-Virus[®] Personal, vous bénéficiez des conseils des experts de Kaspersky Labs afin d'utiliser le niveau de protection antivirus optimum.

La fenêtre principale de Kaspersky Anti-Virus[®] affiche en permanence des recommandations sur l'exécution de telles ou telles tâches et sur les raisons qui les justifient en cas de découverte de fichiers infectés ou potentiellement infectés, lorsque le contenu des bases antivirus est fortement dépassé ou lorsqu'il est grand temps de réaliser l'analyse complète de l'ordinateur. Nous nous sommes efforcés de configurer ce logiciel de la meilleure manière possible en intégrant la riche expérience des experts de Kaspersky Labs 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

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.

recommandés par nos experts sont appliqués dès l'installation et le lancement du logiciel.

- **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 Labs en vue d'un examen approfondi. Les fichiers en quarantaine sont convertis dans un format spécial et ne présentent 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 n'importe quel système de messagerie utilisant le protocole POP3 pour la réception des messages et le protocole SMTP pour leur envoi.* Les versions antérieures garantissaient la protection antivirus uniquement pour les clients de messagerie compatibles avec Microsoft Exchange.
- *Réparation des archives infectées.* Kaspersky Anti-Virus® Personal est capable de réparer les archives infectées au format *zip*, *arj*, *cab* et *rar*. 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 auto-extractibles mais ne les répare pas.

- *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 du logiciel. 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 Labs, ce qui simplifie l'utilisation. Il n'est donc pas nécessaire 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.
- *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 Labs pour étude approfondie.* Il est désormais possible d'envoyer à Kaspersky Labs 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 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.

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 (pour l'installation de Kaspersky Anti-Virus® au départ d'un CD) ;
- Microsoft Internet Explorer version 5.5 (pour la mise à jour des bases antivirus et des modules du programme via Internet).

Windows 98 :

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

Windows ME :

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

Windows NT Workstation 4.0 (Service Pack 6a) :

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

Windows 2000 Professional (Service Pack 2 ou suivant) :

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

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 **Achat en ligne**).

Le pack logiciel contient :

- Une enveloppe cachetée contenant le CD d'installation où les fichiers du logiciel sont enregistrés
- Le manuel de l'utilisateur ;
- La clé de licence, enregistrée sur une disquette spéciale ;
- La licence utilisateur.



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

Si vous achetez Kaspersky Anti-Virus® Personal en ligne, le fichier d'installation du produit est téléchargé du site Web de Kaspersky Labs. Ce fichier d'installation

inclut ce guide de l'utilisateur et la clé de licence. La clé de licence sera envoyée par courrier électronique dès la réception du paiement.

La licence utilisateur constitue l'accord juridique passé entre vous et Kaspersky Labs Ltd., stipulant les conditions d'utilisation du progiciel que vous avez acquis.

Lisez attentivement la licence utilisateur !

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

L'ouverture de l'enveloppe cachetée contenant le CD d'installation implique que vous acceptez les termes de la licence utilisateur.

1.6. Services réservés aux utilisateurs enregistrés

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

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

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



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 *kavsetup.exe* repris sur le CD-ROM d'installation.

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 de lancer l'installation du logiciel, le système vérifie si le système d'exploitation de votre ordinateur répond aux conditions minimales d'installation de Kaspersky Anti-Virus® Personal.

Au cas où l'un des services pack indispensable ne serait pas installé, le message adéquat apparaîtra à l'écran. Installez le service pack à l'aide du service **Mise à jour Windows** puis, recommencez la procédure d'installation de Kaspersky Anti-Virus® Personal.

Etape 2. Recherche d'autres logiciels antivirus éventuellement installés



Cette étape s'applique uniquement au cas de figure où un autre logiciel antivirus est installé sur votre ordinateur.

Cette étape est une autre étape préalable à l'installation du logiciel proprement dite. Il s'agit pour le système de vérifier si d'autres logiciels antivirus, y compris d'autres logiciels de Kaspersky Labs, 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 la supprimer car son utilisation conjointe avec Kaspersky Anti-Virus® Personal 5.0 est impossible.

Cliquez sur **OK** afin de supprimer la version antérieure de Kaspersky Anti-Virus® et exécutez à nouveau le fichier *kavsetup.exe*.

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**, supprimez le logiciel indiqué et exécutez à nouveau le fichier *kavsetup.exe*.

Si le programme d'installation détecte que Kaspersky Anti-Virus® Personal 5.0 est déjà installé, le message adéquat sera affiché. En choisissant de poursuivre l'installation, vous remplacerez la version déjà installée par la nouvelle.

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

Dès l'exécution du fichier *kavsetup.exe*, 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 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 Labs. 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 le logiciel avant de commencer à l'utiliser.

Vous y trouverez une brève description des principales caractéristiques de Kaspersky Anti-Virus®, les particularités de son fonctionnement, etc.

Cliquez sur **Suivant** > lorsque vous aurez lu ces renseignements.

Etape 7. Activation de la clé de licence



Cette étape est d'application uniquement lorsque le programme d'installation de Kaspersky Anti-Virus® Personal n'a pu trouver lui-même la clé de licence !

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.

Sélectionnez la clé de licence dans la boîte de dialogue standard de sélection de fichiers puis, cliquez sur **Suivant** > afin de 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 Labs mais ne l'avez pas encore reçue), sachez qu'il est possible de l'activer ultérieurement lorsque vous lancerez le programme pour la première fois. N'oubliez pas qu'il est impossible d'utiliser Kaspersky Anti-Virus® sans cette clé.

Etape 8. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le répertoire dans lequel vous souhaitez installer Kaspersky Anti-Virus®. Il s'agit par défaut de : **C:\ProgramFiles\Kaspersky Lab\Kaspersky Anti-Virus Personal.**

Si vous souhaitez choisir un autre répertoire, cliquez sur **Parcourir...** Dans la boîte de dialogue qui apparaît, sélectionnez le nouveau répertoire puis cliquez sur **Suivant** > pour poursuivre l'installation.

Vous lancerez ainsi la copie des fichiers de Kaspersky Anti-Virus® Personal sur votre ordinateur.

Etape 9. 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 Windows (**Démarrer → Programmes → Kaspersky Anti-Virus Personal**)

2. Cliquez sur **Terminer**.

CHAPITRE 3. QUE FAIRE EN CAS D'INFECTION DE VOTRE 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 indiquer l'infection de l'ordinateur. Si vous remarquez que votre ordinateur a un comportement bizarre, comme:

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

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

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

- 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 90% des cas, ces symptômes sont causés par des problèmes matériels ou logiciels. Même si ces symptômes ne sont pas nécessairement la manifestation d'une infection, il est fortement conseillé de procéder à une analyse complète de votre ordinateur selon les paramètres définis par les experts de Kaspersky Labs 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 :

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


5. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD, une carte Flash, etc.
6. Installez Kaspersky Anti-Virus® Personal, si cela n'a pas encore été fait.
7. 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 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 Labs 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 12.3 à la page 63).
8. Sélectionnez le niveau de protection recommandé par les experts de Kaspersky Labs (cf. point 6.2, p. 35).
9. Lancez l'analyse complète de votre ordinateur (cf. point 6.3, p. 40).

CHAPITRE 4. PROTECTION DE L'ORDINATEUR SANS CONFIGURATION COMPLEMENTAIRE DE L'ANTIVIRUS

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 Labs. 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

Dès le lancement (comme en témoigne l'icône  dans la barre des tâches), Kaspersky Anti-Virus® analyse *les objets exécutés au démarrage du système d'exploitation, la mémoire de l'ordinateur et ses propres modules.*

La protection en temps réel fonctionne conformément à la configuration définie par les spécialistes de Kaspersky Labs, 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 (uniquement à l'arrivée).



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 ;
- Les résultats des différentes opérations sont consignés dans le rapport (cf. point 13.5, p. 76).

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



Il est possible de désactiver la protection en temps réel. Pour ce faire :

- Faites un clic droit sur l'icône  dans la barre des tâches.
- Sélectionnez **Désactiver la protection en temps réel** dans le menu contextuel qui apparaît.

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



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

4.2. Analyse de l'ordinateur à la demande

Il existe également une fonction d'**Analyse à la demande** qui 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 Labs.

- En cas d'analyse complète de votre ordinateur, la recherche d'éventuels virus 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*);
 - *La mémoire vive de l'ordinateur sollicitée par les processus en cours.*
- 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*).
- En cas de découverte d'un *objet infecté*, une boîte de dialogue reprenant les différentes 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*, une boîte de dialogue reprenant les différentes options de traitement apparaît à l'écran.
- Les résultats des différentes opérations sont consignés dans le rapport (cf. point 13.5, p. 76).


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. 3) 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 :

Faites un clic droit 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 qu'ils auraient infectés, 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 Labs et installées sur votre ordinateur toutes les 3 heures. Si vous utilisez votre ordinateur moins de 3 heures par jour, il est conseillé soit de changer la fréquence des mises à jour, soit de ne pas éteindre l'ordinateur ou soit de lancer la mise à jour manuellement. Autrement, la mise à jour ne pourra pas avoir lieu.



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. 3) 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 12 à la page 61.



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.

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 antivirus apparaît dans la barre des tâches.

L'icône (de couleur rouge)  indique que la protection en temps réel des fichiers est activée tandis que l'icône (grise)  signale que la protection en temps réel n'est pas activée. L'icône grise apparaît même lorsque l'analyse du courrier et des scénarios est en cours.

Quand l'analyse complète de l'ordinateur, l'analyse d'un fichier ou d'un disque particulier ou l'analyse en temps réel d'un objet particulier est en cours d'exécution, un dossier bleu et blanc clignotant apparaît sous l'icône :  / . Lors de l'analyse du courrier, le dossier est remplacé par une enveloppe.

Lorsqu'un événement important au niveau de la protection antivirus survient, un message reprenant les recommandations des experts de Kaspersky Labs apparaît au-dessus de l'icône (cf. ill. 1).

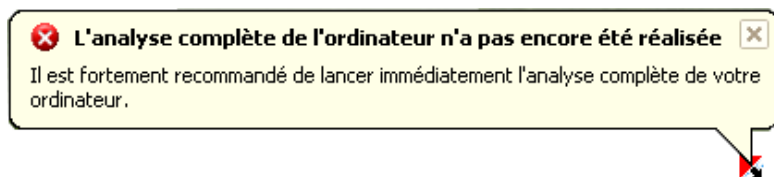



Illustration 1. Message d'informations

5.2. Menu contextuel

Un clic-droit sur l'icône dans la barre des tâches vous permettra d'afficher un menu contextuel (cf. ill. 2) proposant les éléments suivants :

- **Ouvrir Kaspersky Anti-Virus** : ouvre la fenêtre principale du logiciel à l'onglet **Protection**. Vous pouvez également double-cliquer sur l'icône  du programme dans la barre des tâches.

- **Analyser mon poste de travail** : lance l'analyse antivirus complète de l'ordinateur conformément au niveau de protection sélectionné.
- **Mettre à jour les bases antivirus** : télécharge les dernières mises à jour des bases antivirus depuis les serveurs de Kaspersky Labs.
- **Activer la protection en temps réel / Désactiver la protection en temps réel** : active ou désactive la protection en temps réel de l'ordinateur. 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.

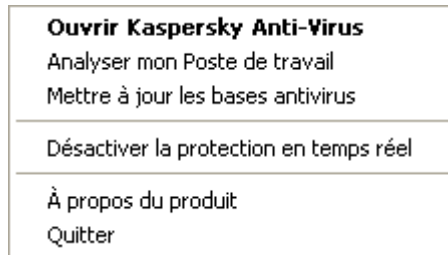


Illustration 2. Menu contextuel

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 et des modules de programme ;
- Configurer l'exécution automatique de l'analyse complète et des mises à jour ;
- Travailler avec les objets en quarantaine ;
- Consulter les rapports, 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. Il s'agit de l'interface principale du logiciel (cf. point 5.3.1, p. 26).
- L'onglet **Paramètres** regroupe toutes les tâches liées à la configuration des principaux paramètres de la protection antivirus (cf. point 5.3.2, p. 28).
- L'onglet **Assistance technique** reprend les informations utiles en cas de problèmes ou lorsque vous devez vous adresser à Kaspersky Labs (cf. point 5.3.3, p. 29).

Chacun de ces onglets est divisé en deux parties :

- *La partie gauche* contient une liste de lien permettant d'exécuter les tâches qui contribuent à la protection antivirus. 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 de la configuration de ces différentes tâches tandis que l'onglet **Assistance technique** proposera toutes les tâches qui pourront vous apporter 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 trois 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.



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 Labs. Cet état indique également qu'il est indispensable d'exécuter certaines tâches particulières liées à la protection antivirus.



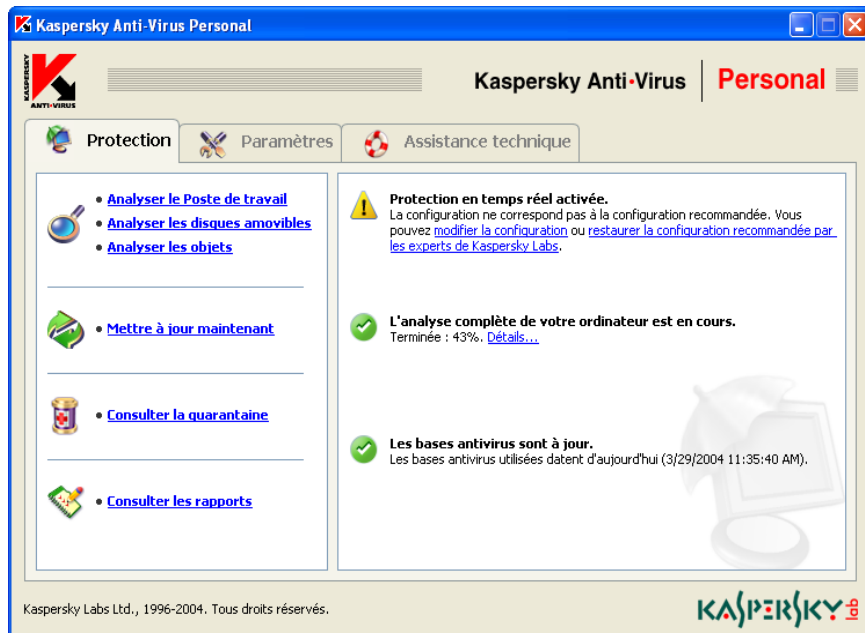
Le niveau de la protection antivirus est conforme aux recommandations. La configuration de la protection antivirus appliquée correspond parfaitement à celle recommandée par les experts de Kaspersky Labs

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. 3) que vous lancerez les tâches d'analyse de votre ordinateur ou de disques, de dossiers ou de fichiers particuliers.

Illustration 3. Onglet **Protection**

De cet onglet vous pourrez également procéder à la mise à jour des bases antivirus et des modules du programme ou consulter les rapports sur l'exécution des tâches. Il est possible de lancer des tâches individuelles en cliquant sur le lien correspondant dans la partie gauche.

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 3 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 Labs 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 Labs, 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.

5.3.2. Onglet Paramètres

L'onglet **Paramètres** (cf. ill. 4) 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.

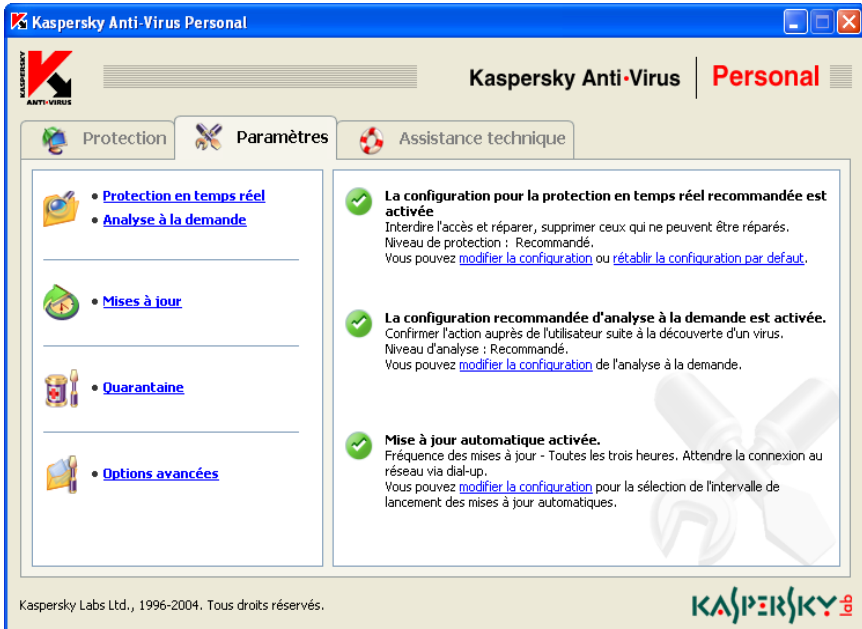


Illustration 4. Onglet Paramètres

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 et des modules du programme. 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 configurer la quarantaine où sont placés tous les objets potentiellement infectés par un virus ou l'une de ses variantes. Le lien [Options](#)

[avancées](#) ouvre la fenêtre de configuration des paramètres complémentaires de Kaspersky Anti-Virus® Personal.

5.3.3. Onglet *Assistance technique*

L'onglet **Assistance technique** (cf. ill. 5) reprend toutes les informations relatives au Service d'assistance technique que vous pouvez contacter en cas de difficultés ou lorsque vous n'êtes pas en mesure de résoudre seul le problème auquel vous êtes confronté.



Illustration 5. 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 Labs. 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 Labs 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 les fichiers d'aide sur l'exécution des tâches et la résolution des problèmes.
- Le lien [Comment faire pour...](#) ouvre des fenêtres d'aide générale sur l'utilisation du logiciel.
- Le lien [Encyclopédie des virus](#) vous emmène sur le site www.viruslist.com qui contient une description détaillée de tous les programmes malicieux connus à ce jour.
- Le lien [Site Web de Kaspersky Labs](#) vous conduira sur le site Internet de Kaspersky Labs.

5.4. Fenêtre du processus d'analyse

La fenêtre du processus d'analyse (cf. ill. 6) apparaît dès le lancement de l'analyse complète de l'ordinateur ou de l'un de ses disques, fichiers ou répertoires.

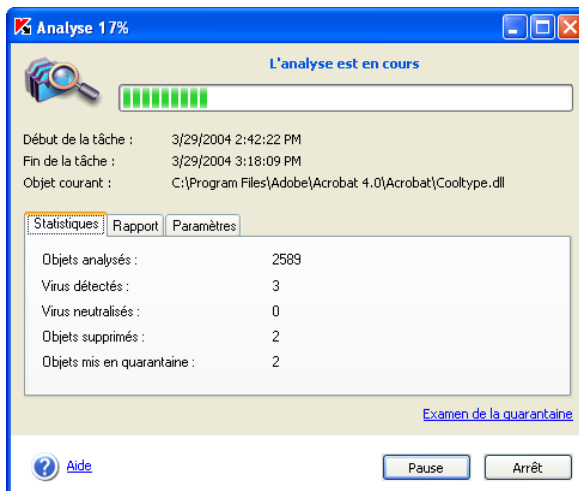


Illustration 6. Fenêtre du processus d'analyse

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. Elle reprend également l'heure du début et l'heure estimée de fin ainsi que le nom de l'objet en cours d'analyse.
- La partie inférieure 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 de plus amples informations sur l'utilisation du rapport, consultez le point 13.5 à la page 76.

5.5. Aide

Toutes les rubriques d'aide du logiciel sont accessibles via l'onglet **Assistance technique**. Il suffit de cliquer sur le lien [Comment faire pour...](#) 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 quotidienne 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 Labs immédiatement dans ce genre de situation).
- Etablissez la protection en temps réel au niveau recommandé par les experts de Kaspersky Labs. 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 Labs pour l'analyse complète de l'ordinateur et prévoyez son exécution une 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 Labs.*

Généralement, Kaspersky Labs 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 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 ".


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 ou soit une analyse de disques, de fichiers ou de répertoires particuliers.



Dans le cadre de l'analyse complète de l'ordinateur, 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 bien plus élevé d'objets que la protection en temps réel. Il est donc conseillé de l'effectuer au moins une fois par semaine à titre préventif. Le logiciel vous avertira lorsqu'il est indispensable de lancer cette analyse. Au cas où la fenêtre principale du logiciel serait fermée, un message vous invitant à lancer immédiatement l'analyse complète de l'ordinateur apparaîtra au-dessus de l'icône  de Kaspersky Anti-Virus® Personal dans la barre des tâches (pour autant que cette option n'ait pas été désactivée, cf. point 13.6, p. 81).

Pour obtenir de plus amples informations, il suffira d'ouvrir la fenêtre principale de l'application et de sélectionner l'onglet **Protection** (cf. ill. 3). 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 Labs.



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 Labs vous conseillent de programmer le lancement de l'analyse complète (cf. point 6.4, p. 41). L'état de l'analyse indique notamment si ce mode est activé ou non.



L'analyse complète de l'ordinateur a réussi.

La dernière analyse complète de l'ordinateur a été réalisée il y a 8 jour(s) (2/24/2004 7:30:36 PM).

L'analyse programmée de l'ordinateur est activée. Vous pouvez [modifier l'horaire](#) de l'analyse.



Illustration 7. Renseignements sur la nécessité de procéder à l'analyse complète

6.2. Configuration à utiliser pour l'analyse

Après l'installation de Kaspersky Anti-Virus® Personal, chaque analyse (analyse complète de l'ordinateur, analyse d'objets distincts et analyse de disques amovibles) est réalisée selon les paramètres recommandés par les experts de Kaspersky Labs (pour de plus amples informations, consultez le Chapitre 3 à la page 16). L'état de la configuration de l'analyse apparaît dans la partie droite de l'onglet **Paramètres** (cf. ill. 4) 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 13.2, p. 71), il vous sera impossible de l'analyser si vous le sélectionnez pour une analyse particulière (cf. point 6.5, p. 42). Les boîtes aux lettres de Microsoft Outlook et Microsoft Outlook Express sont les seules exceptions à cette règle.

Elles pourront être analysées individuellement même si elles ont été exclues de l'analyse.



Pour modifier le niveau d'analyse et/ou les actions à exécuter en cas de découverte d'objets infectés, de programmes malicieux ou d'objets potentiellement infectés par un virus ou l'une de ses variantes :

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 de protection* qui vous convient dans la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 8). 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 16.

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

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 (y compris de la mémoire et des secteurs d'amorçage) 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	+	+	-
Boîtes aux lettres MS Outlook et MS Outlook	+	+	-
Base de données de messagerie et messages	+	-	-

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

Il est possible de définir des *exclusions*, c'est-à-dire des objets qui ne seront pas analysés (cf. point 13.2, p. 71), pour chacun de ces niveaux de protection. Ceci étant dit, ces exclusions devraient être définies uniquement en cas de problème lors de l'utilisation de Kaspersky Anti-Virus® Personal, par exemple si vous remarquez un ralentissement de l'ordinateur.

3. Précisez l'action que le logiciel exécutera à chaque découverte d'un objet infecté, d'un programme malicieux (ver, cheval de Troie) ou d'un objet potentiellement infecté par un virus ou l'une de ses variantes :

- **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 Labs. Sélectionnez ce mode si vous avez l'intention de rester à proximité de votre ordinateur pendant l'analyse.

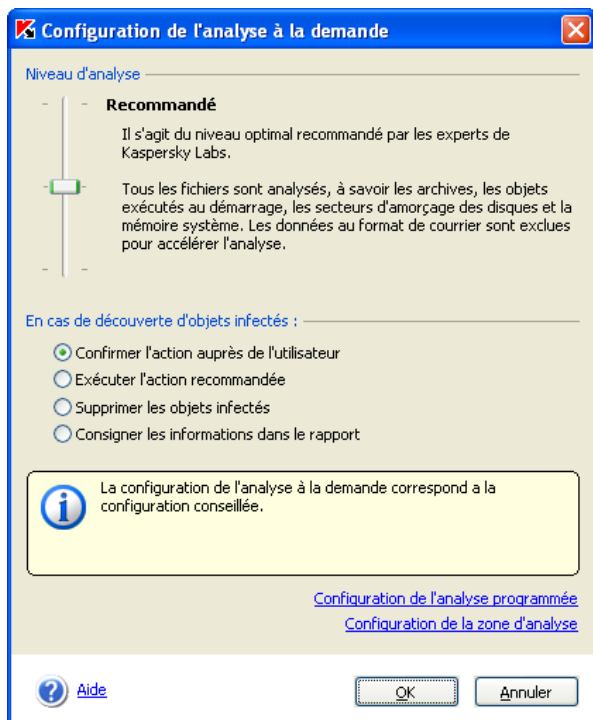


Illustration 8. Configuration de l'analyse à la demande

🔍 **Exécuter l'action recommandée** : exécute l'action recommandée par les experts de Kaspersky Labs. 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 physiquement : 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 qui font partie d'une archive auto-extractible

- *Supprimer* les programmes malicieux (chevaux de Troie et vers) ou l'objet infecté en cas d'échec de la réparation.

🔍 **Supprimer les objets infectés** assure la suppression des objets infectés découverts pendant l'analyse sans tenter de réparation ni demander de confirmation auprès de l'utilisateur. 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 rapport. Il est conseillé d'utiliser ce mode avec parcimonie car il ne débarrasse pas votre ordinateur des objets infectés et des programmes malicieux et il pratiquement impossible dans ce cas d'éviter la propagation de l'infection.

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 réparer à ce moment. Un message apparaîtra alors à l'écran (cf. ill. 9) 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.

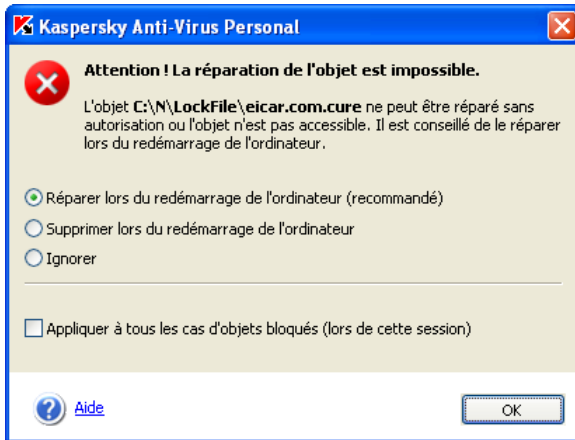


Illustration 9. La réparation immédiate de l'objet impossible



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. 3).

La fenêtre **Analyse** (cf. ill. 6) apparaît à l'écran. Elle reprend la progression en pour-cent de la tâche, l'heure de début, l'heure de fin prévue ou définitive ainsi que le nom de l'objet analysé.

Il est possible de consulter les résultats de l'analyse dans le rapport (pour plus de détails, consultez le point 13.5 à la page 76).

6.4. Analyse complète programmée

Vous pouvez programmer l'analyse complète de l'ordinateur afin qu'elle se déroule certains jours à certaines heures. 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. 4).
2. Cliquez sur le lien [Configuration de l'analyse programmée](#) dans la fenêtre **Configuration de l'analyse à la demande** (cf. ill. 8).
3. Définissez la fréquence d'exécution de la tâche dans la fenêtre **Configuration de l'analyse programmée** (cf. ill. 10) :

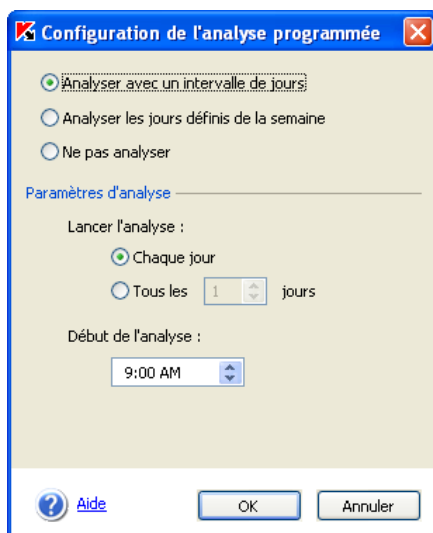


Illustration 10. Configuration de l'analyse programmée

- **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**.

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 Windows (via l'**Assistant** ou sur le **Bureau**, etc.).



Pour analyser l'objet sélectionné au départ de Windows :

Placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 11).

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. 3).

La boîte de dialogue **Sélection des objets à analyser** (cf. ill. 12) 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.

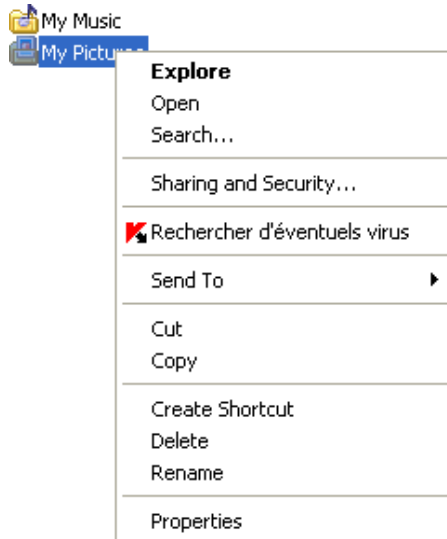


Illustration 11. Analyse antivirus d'un objet sélectionné à l'aide des outils Windows



Illustration 12. 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 Outlook et Microsoft Outlook Express ;
- Le dossier **Mes documents**.

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 Windows ou au départ de la liste des objets de Kaspersky Anti-Virus® Personal), la boîte de dialogue **Analyse** (cf. ill. 6) 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 13.5 à la page 76).

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 13.2, p. 71).



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. Kaspersky Anti-Virus® NE REPARÉ PAS les archives auto-extractibles ! En cas de découverte d'un virus dans une archive auto-extractible, celle-ci sera supprimée !

Au cas où l'objet à l'intérieur de l'archive serait protégée par un mot de passe, une boîte de dialogue pour la saisie du mot de passe (cf. ill. 13) apparaîtra avant son analyse.



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 13.2, p. 71).



Illustration 13. Saisie du mot de passe pour l'analyse d'une archive

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.

CHAPITRE 7. ANALYSE D'UN CD-ROM OU D'UNE DISQUETTE

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 CD-Rom) est infectée par un virus d'amorçage et que vous l'avez introduite dans le lecteur avant de redémarrer, les résultats pourraient être catastrophiques.

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

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



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

Sélectionnez les disques (il est possible de sélectionner directement le CD et la disquette), ouvrez le menu contextuel de Windows d'un clic droit et choisissez **Rechercher d'éventuels virus** (cf. ill. 11).



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. 3).

Ou

Cliquez sur le lien [Analyser les objets](#) pour ouvrir la boîte de dialogue **Sélection des objets à analyser** (cf. ill. 12) puis, sélectionnez les disques amovibles et cliquez sur **Analyser**.

La fenêtre **Analyse** (cf. ill. 6) 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 recherche d'éventuels virus d'amorçage sur ce disque.

CHAPITRE 8. CONFIGURATION DE LA PROTECTION EN TEMPS RÉEL

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. 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. 3) 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 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 13.1, p. 68) 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 infectés, aux programmes malicieux (vers et chevaux de Troie) et aux objets infectés par un virus ou l'une de ses modifications 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, les bases de données de messagerie et les messages au format de courrier NE SONT PAS ANALYSES. Les archives auto-extractibles constituent la seule exception, 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 infecté, d'un programme malicieux ou d'un objet potentiellement infecté par un virus ou l'une de ses modifications.



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. 4) 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. ill14). 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.

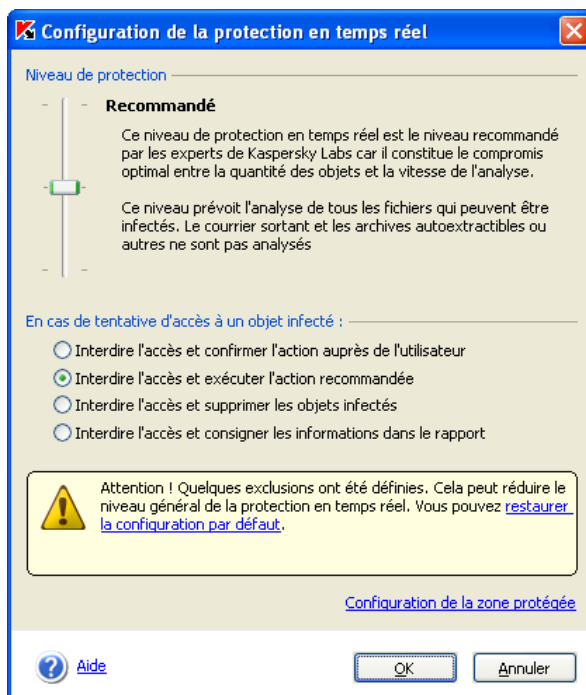


Illustration 14. Configuration de la protection en temps réel



Nous vous rappelons que la protection en temps réel ne prévoit pas l'analyse et la réparation des archives. Pour ce faire, vous devrez procéder à l'analyse complète de votre ordinateur (cf. point 6.3, p. 40).

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 Labs. La protection porte sur les mêmes objets que pour le niveau **Sécurité maximale**, à l'exception des archives auto-extractibles et du courrier sortant.
- **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	+	+	+
Courrier entrant⁴	+	+	+
Courrier sortant⁵	+	–	–
Archives auto-extractibles⁶	+	–	–
Bases de messagerie électronique et messages individuels	–	–	–


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

Il est possible de définir des *exclusions* et de désactiver la protection en temps réel. Pour obtenir de plus amples informations, consultez le point 13.1 à la page 68.

3. Précisez l'action que le logiciel exécutera à chaque découverte d'un objet infecté, d'un programme malicieux (ver, cheval de Troie) ou d'un objet potentiellement infecté par un virus ou l'une de ses variantes.

 **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):

- o *Réparer* l'objet infecté ;
- o *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 physiquement : 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 qui font partie d'une archive auto-extractible

- o *Supprimer* les programmes malicieux (chevaux de Troie et vers) ou l'objet infecté en cas d'échec de la réparation, soit en raison d'une erreur ou parce qu'elle est impossible.
- o *Ignorer* les objets infectés. Aucune action n'est réalisée et les informations sont simplement consignées dans le rapport.



Si vous souhaitez mettre l'objet infecté découvert en quarantaine, il vous faudra choisir *Ignorer* avant de placer vous-même l'objet en quarantaine (pour de plus amples informations, consultez le point 13.3 à la page 72).

- **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 infectés** : 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.

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. 9) 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*.



Remarquez que les actions reprises ci-dessus ne concernent ni les messages électroniques ni les scripts dangereux :

- En cas de découverte d'un message électronique infecté ou potentiellement infecté, Kaspersky Anti-Virus® exécute l'action recommandée sans avertir l'utilisateur.
- En cas de découverte d'un scénario dangereux, vous en serez averti et vous pourrez décider de l'action à prendre.

CHAPITRE 9. PROTECTION DU COURRIER CONTRE LES VIRUS

Kaspersky Anti-Virus® Personal assure une protection en temps réel du courrier entrant et sortant.



Pour protéger votre courrier contre les virus :

Il suffit d'activer la protection en temps réel 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 13.1, p. 68).

Les trois 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 utilisé⁷. Le courrier est analysé à l'envoi et à la réception, que cette opération soit réalisée par vous-même 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.

Les bases de données de messagerie électronique transférées d'un autre ordinateur, mais qui n'ont pas encore été importées, peuvent être analysées à la demande.

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

1. Assurez-vous que la case **Ne pas analyser les boîtes aux lettres** (cf. point 13.2, p. 71) n'a pas été cochée dans la fenêtre **Configuration de l'analyse**.
2. Cliquez sur le lien [Analyser les objets](#) dans la partie gauche de l'onglet **Protection** (cf. ill. 3).
3. Sélectionnez **Boîte aux lettres** dans la fenêtre **Sélection des objets à analyser** (cf. ill. 12).
4. Cliquez sur **Analyser**.

Les bases de données de messagerie électronique Microsoft Outlook et Microsoft Outlook Express seront ainsi analysées.



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





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. 3).
2. Dans la boîte de dialogue **Sélection des objets à analyser** (cf. ill. 12), sélectionnez le disque ou le répertoire dans lequel se trouve les bases.
3. Cliquez sur **Analyser**.

CHAPITRE 10. TRAITEMENT DES VIRUS

Les actions exécutées par Kaspersky Anti-Virus® Personal en cas de découverte d'un objet infecté, 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.

Cela se produit lorsque vous avez sélectionné :

- dans la configuration de la protection en temps réel (cf. ill. 14):
 -  **Interdire l'accès et confirmer l'action auprès de l'utilisateur**
- dans la configuration de l'analyse à la demande (cf. ill. 8):
 -  **Confirmer l'action auprès de l'utilisateur**

En cas de découverte d'un objet infecté, d'un code malicieux ou d'un objet potentiellement infecté par un virus ou l'une de ses variantes, une boîte de dialogue apparaît à l'écran (cf. ill. 15). Elle reprend :

- Une description détaillée de l'objet avec le nom du virus à l'origine de l'infection, confirmée ou éventuelle, ou le nom du programme malicieux dont il s'agit.
- 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 Labs. 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.
 - **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 Labs ou de sa suppression (cf. point 13.3, p. 72).

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)**.

L'objet sera ignoré si vous fermez la fenêtre en cliquant sur dans le coin supérieur droit.

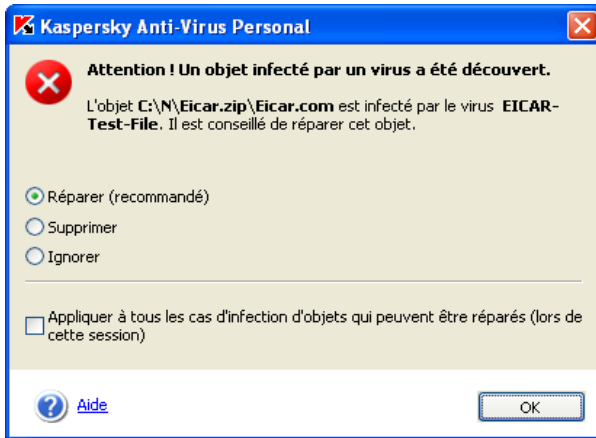


Illustration 15. Message affiché suite à la découverte d'un objet infecté

CHAPITRE 11.

RENOUVELLEMENT DE LA LICENCE

Kaspersky Anti-Virus® Personal fonctionne grâce à une *clé de licence*. Elle fait partie du pack logiciel et vous donne le droit d'utiliser Kaspersky Anti-Virus® depuis le jour d'acquisition et d'activation de la licence.



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 infectés. Par conséquent, la protection contre les nouveaux virus qui apparaîtraient après la fin de validité de la licence 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 licence d'utilisation de 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 :

Contactez directement le Service Ventes (sales@kaspersky.com) de Kaspersky Labs pour acheter une nouvelle clé.

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

- Cliquez sur [Clés de licence](#) dans la partie gauche de l'onglet **Assistance technique** (cf. ill. 5).
- Cliquez sur **Ajouter** dans la boîte de dialogue **Gestion des clés de licence** (cf. ill. 16) qui apparaît et sélectionnez la nouvelle clé de licence.

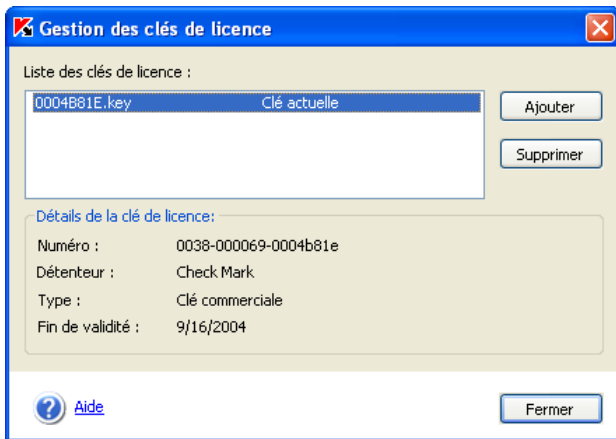


Illustration 16. Fenêtre de gestion des clés de licence

CHAPITRE 12.

TELECHARGEMENT DES MISES A JOUR

Kaspersky Labs offre à ses utilisateurs la possibilité de mettre à jour les modules de Kaspersky Anti-Virus® Personal ainsi que les bases antivirus qui interviennent dans l'identification des programmes malicieux et la réparation des objets infectés.



La mise à jour des bases antivirus est la garantie de la sécurité de votre ordinateur. Des centaines de nouveaux virus voient le jour chaque jour et les experts de Kaspersky Labs 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 12 heures. Lors d'une épidémie, la fréquence devrait être la plus courte possible, par exemple au moins une fois toutes les 3 heures.

Kaspersky Anti-Virus® Personal va chercher les mises à jour sur *les serveurs de mise à jour de Kaspersky Labs* ou dans un répertoire local de votre 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. Kaspersky Anti-Virus® Personal copie les bases de mise à jour depuis le serveur sur l'ordinateur avant de les installer.

12.1. 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. 3).

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 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.

12.2. Téléchargement des mises à jour depuis Internet

Kaspersky Labs publie les mises à jour des bases antivirus une fois toutes les 3 heures sur ses serveurs.

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



Afin de toujours procéder à la mise à jour des bases antivirus via Internet au départ des serveurs de mises à jour de Kaspersky Labs, 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. 4).
2. Sélectionnez le type de mise à jour dans le menu déroulant **Type de mise à jour** de la boîte de dialogue **Configuration des mises à jour** (cf. ill. 17). Vous avez le choix entre :
 - *via Internet, bases standard* : bases antivirus capables d'identifier tous les programmes malicieux connus à ce jour et de réparer les objets et les données qu'ils auraient endommagés.
 - *via Internet, bases étendues* : bases standard augmentées de bases complémentaires capables de déceler les programmes offrant un accès à distance à vos données.



Les bases antivirus standard suffisent amplement pour assurer la protection normale de votre ordinateur. L'utilisation des bases étendues peut avoir un impact sur la vitesse de Kaspersky Anti-Virus®.

3. Cochez la case **Attendre la connexion au réseau Internet** si vous êtes connecté à Internet via dial-up et que vous ne souhaitez pas que Kaspersky Anti-Virus® interrompe la mise à jour en cas de déconnexion momentanée.



Cette configuration est applicable uniquement lorsque la mise à jour automatique des bases antivirus est activée !

4. Cliquez sur **OK**.

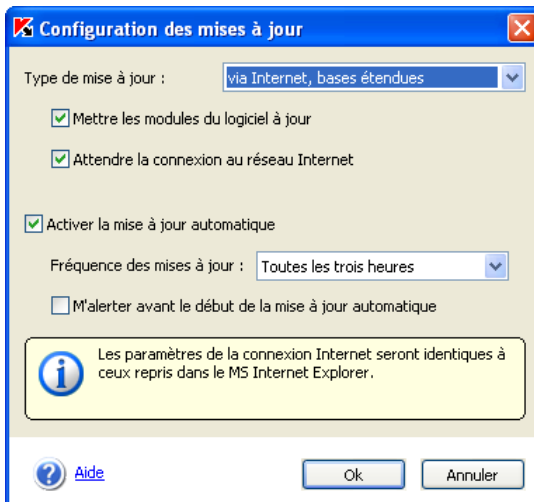


Illustration 18. Boîte de dialogue **Configuration des mises à jour**



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

12.3. Téléchargement des mises à jour depuis un répertoire local

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Labs (ex. : pas de connexion à Internet), vous pouvez contacter nos bureaux au +7 95 797 87 00 pour obtenir l'adresse d'un partenaire de Kaspersky Labs qui pourra vous donner les bases antivirus sur disquette ou sur CD-ROM dans un fichier zip.



N'oubliez pas de préciser le type de bases antivirus que vous souhaitez recevoir : standard ou étendues.

Vous devrez extraire le contenu des fichiers zip reçus, à savoir les bases antivirus, dans n'importe quel répertoire de votre ordinateur.



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. 4).
2. Sélectionnez *Depuis le catalogue local* dans le menu déroulant **Type de mise à jour** de la boîte de dialogue **Configuration des mises à jour** (cf. ill. 19).
3. Dans le champ **Répertoire local**, sélectionnez le répertoire dans le lequel vous avez extrait le contenu des archives zip.
4. Cliquez sur **OK**.

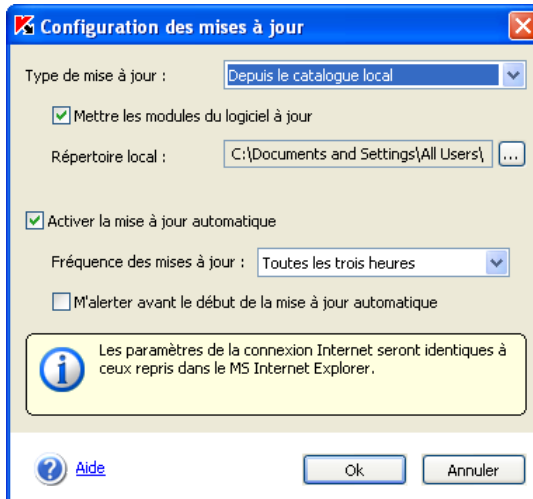


Illustration 19. Boîte de dialogue **Configuration des mises à jour**

12.4. 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 en cas de besoin.

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 les modules du logiciel à jour** dans la boîte de dialogue **Configuration des mises à jour** (cf. ill. 19).



Si vous allez procéder à la mise à jour depuis un répertoire local, n'oubliez pas de préciser au moment de la demande que vous souhaitez obtenir également les mises à jour des modules du logiciel en plus des mises à jour des bases antivirus.

12.5. Configuration des mises à jour. Programmation

Les experts de Kaspersky Labs 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 3 heures.



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

1. Cliquez sur le lien [Mises à jour](#) dans la partie gauche de l'onglet **Paramètres** (cf. ill. 4).
2. Cochez la case **Activer la mise à jour automatique** dans la boîte de dialogue **Configuration des mises à jour** (cf. ill. 19).
3. Sélectionnez la valeur désirée dans la liste déroulante **Fréquence des mises à jour**.

12.6. Mise à jour manuelle.

Téléchargement des mises à jour



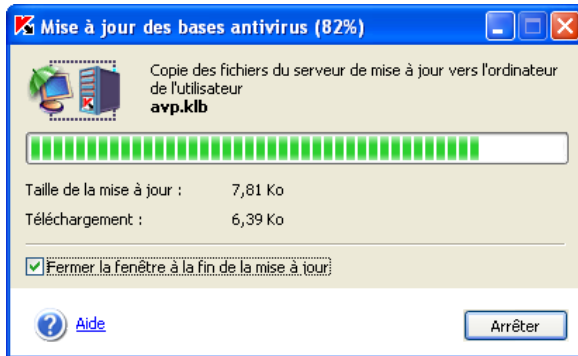
Pour lancer le téléchargement des mises à jour des bases antivirus :

Cliquez sur le lien [Mettre à jour maintenant](#) dans la partie gauche de l'onglet **Protection** (cf. ill. 3) ou dans le message vous informant de l'urgence de la mise à jour dans la partie droite de la fenêtre.

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.

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

1. Le serveur des mises à jour de Kaspersky Labs envoie au logiciel la liste des mises à jour et leur taille respective.
2. Ensuite, le logiciel compare l'état des bases antivirus et des modules de Kaspersky Anti-Virus® aux informations fournies par le serveur. Si les bases antivirus installées sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran.
3. Le champ **Taille de la mise à jour** de la fenêtre **Mises à jour** (cf. ill. 20) reprend la taille totale des mises à jour des bases antivirus indispensables. Si le téléchargement des mises à jour n'est pas nécessaire, la procédure s'arrêtera. Dans le cas contraire, les fichiers sont copiés depuis les serveurs de mises à jour de Kaspersky Labs. Une barre d'état montre la progression de la copie. Le champ **Téléchargement** reprend la quantité de données (en Ko) déjà copiées. Une fois le téléchargement terminé, les bases antivirus sont installées automatiquement sur votre ordinateur.

Illustration 20. Boîte de dialogue **Mise à jour**

CHAPITRE 13. POSSIBILITES COMPLEMENTAIRES

Kaspersky Anti-Virus® Personal propose toute une série de possibilités supplémentaires 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.

13.1. 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 Labs. En plus de la modification des paramètres principaux de la protection en temps réel (cf. Chapitre 8, p. 49), 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. 21) 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. 14).

Pour exclure de l'analyse certains types de fichiers ou des répertoires particuliers, il suffit de définir les masques (par exemple, *.bmp) ou de préciser le chemin d'accès après avoir coché la case **Activer la liste des objets exclus** puis cliquez sur **Modifier**.

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



La saisie des masques *.* et * sans indication du chemin est interdite.

Modifiez la liste reprise dans la boîte de dialogue **Liste des exclusions** (cf. ill. 22) à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**. Une fois que vous aurez dressé la liste des exclusions, cliquez sur **OK**. L'entrée en vigueur de ces exclusions est immédiate.

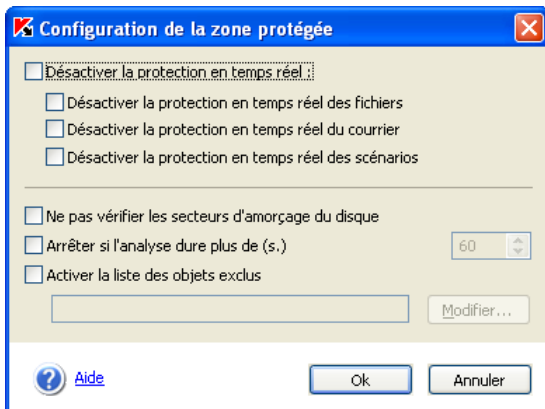


Illustration 21. Configuration des exclusions de la protection en temps réel

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** ou **Protection** (cf. ill. 23).



Illustration 22. Configuration des exclusions pour la protection en temps réel

**La configuration pour la protection en temps réel recommandée est activée**

Interdire l'accès et réparer, supprimer ceux qui ne peuvent être réparés.

Niveau de protection : Recommandé.

Vous pouvez [modifier la configuration](#) ou [rétablir la configuration par défaut](#).

Illustration 23. Informations sur l'état de la protection en temps réel

13.2. 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. 16), conformément à la configuration définie par les experts de Kaspersky Labs.

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. 50), 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 appliquée à tous les niveaux d'analyse complète (**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. 24), 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. 8).

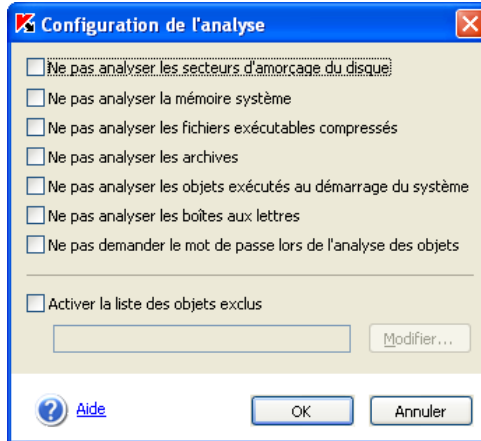


Illustration 24. Configuration de l'analyse

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 13.1, p. 68).



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.

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.

13.3. Traitement des objets en quarantaine

L'*analyseur heuristique de code*, qui permet de détecter jusqu'à 92% des nouveaux virus, détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est relativement efficace mais il donne parfois de fausses alertes. Comment savoir si le fichier est bel et bien infecté par un virus pour lequel il n'existe pas encore de définition dans les bases antivirus ou s'il s'agit simplement d'une fausse alerte ?

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.

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. 25) 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. 6).

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 infecté mais qu'il n'a pas pu être réparé. Il est recommandé de supprimer de tels objets.

Tous les objets dont l'état est qualifié de *fausse alerte* peuvent être restaurés sans crainte car leur état antérieur, à savoir *Probablement infecté*, avait été erronément attribué par Kaspersky Anti-Virus® Personal.

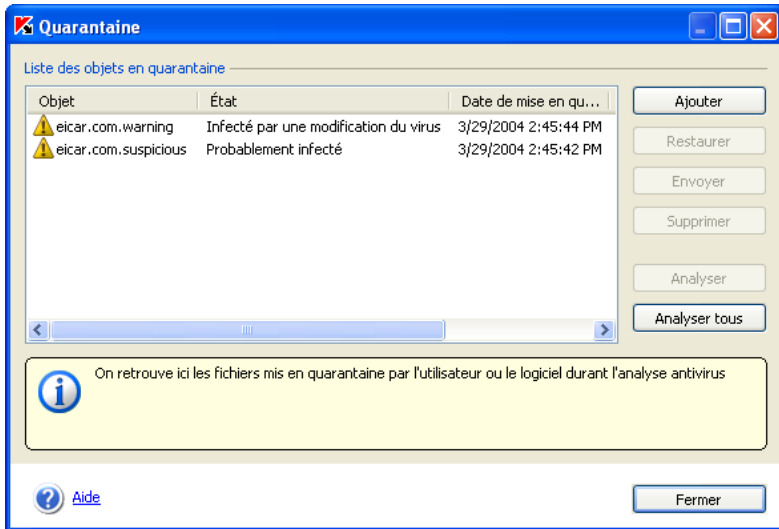


Illustration 25. Quarantaine avec des objets infectés

- 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 Labs 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 84 pour de plus amples informations).



Nous attirons votre attention sur le fait que chaque fichier que vous envoyez à Kaspersky Labs 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**.

13.4. Configuration complémentaire de la quarantaine

Vous pouvez configurer les paramètres de constitution et de fonctionnement de la quarantaine. Pour ce faire, cliquez sur le lien [Quarantaine](#) de l'onglet **Paramètres** (cf. ill. 4) de la fenêtre principale et modifiez les paramètres suivants dans la fenêtre ainsi ouverte (cf. ill. 26) :

- 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.

- Taille maximum du dossier de quarantaine ... Mo.** 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.)

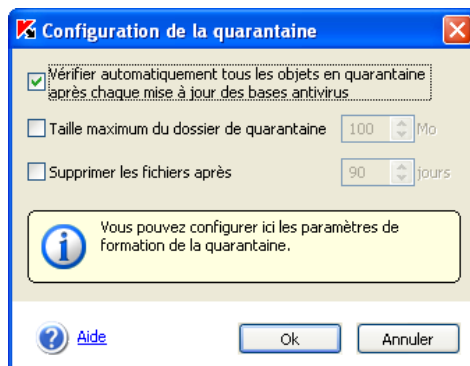


Illustration 26. Configuration de la quarantaine

- Supprimer les fichiers après ... jours.** Par défaut, la durée de conservation des fichiers en quarantaine n'est pas définie. Vous pouvez préciser 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).

13.5. 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.





Illustration 27. Rapports

Kaspersky Anti-Virus® tient une liste de toutes les actions exécutées dans la fenêtre **Rapports** (cf. ill. 27). Pour ouvrir cette fenêtre, cliquez sur le lien [Consulter les rapports](#) dans la partie gauche de l'onglet **Protection** (cf. ill. 3). Le rapport reprend l'état de chaque tâche, ainsi que la date et l'heure de la fin d'exécution.

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

-  ou  – *Informations* (ex. : tâche lancée, tâche exécutée, tâche en cours d'exécution, tâche interrompue).

 – *Avertissement* (ex. : Attention ! Il reste des objets qui n'ont pas été traités).

 – *Remarque* (ex. : la tâche a été interrompue).

En général, les messages à caractère purement informatif n'ont aucun intérêt particulier. Vous pouvez désactiver l'affichage de ce type de message. Pour ce faire, désélectionnez la case **Afficher les rapports informatifs**.

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. 6).

Ainsi, l'onglet **Statistiques** (cf. ill. 28) 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 Labs ou dans le répertoire local) et au volume de données déjà téléchargé.

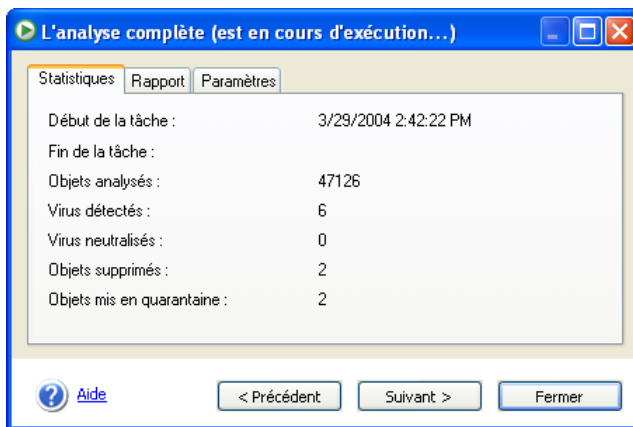


Illustration 28. Onglet **Statistiques**

L'onglet **Rapport** (cf. ill. 29) 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 les messages pour le rapport détaillé** dans les options avancées de Kaspersky Labs. 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 les messages pour le rapport détaillé** dans les options avancées de Kaspersky Anti-Virus® Personal n'a pas été cochée.

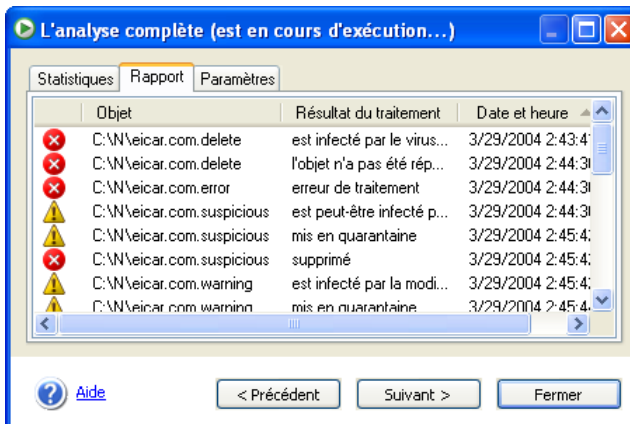
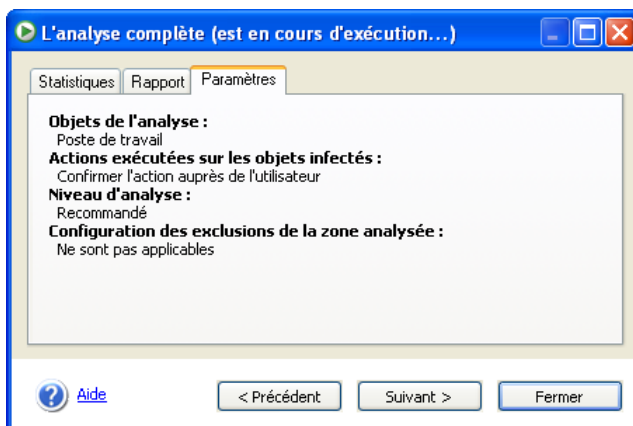


Illustration 29. Onglet **Rapport**

L'onglet **Paramètres** (cf. ill. 30) 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 30. 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.

13.5.1. Représentation des informations

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 messages dans le rapport, il suffit de cocher la case **Enregistrer les messages pour le rapport détaillé**, dans la fenêtre **Options avancées** (cf. point 13.6, p. 81). Vous pouvez suivre la constitution du rapport 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 l'analyse, y compris celles sur la réussite de l'analyse d'un objet.

Lorsque cette case n'est pas cochée, le rapport reprend uniquement les informations importantes, 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. 31) et décochez **Afficher rapport détaillé**.

- Afficher la dernière entrée du rapport
- Afficher rapport détaillé

Illustration 31. Menu contextuel des rapports



Si la case **Enregistrer les messages pour le rapport détaillé** 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.

13.5.2. 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. 32) que vous pouvez ouvrir d'un clic droit dans la fenêtre **Rapports** (cf. ill. 27)

- Exporter le rapport détaillé dans le fichier ...
- Envoyer le rapport à Kaspersky Labs

- Supprimer le rapport
- Supprimer tous les rapports

Illustration 32. Menu contextuel pour le travail avec les rapports

Le type d'actions disponibles dans le menu contextuel varie en fonction du type de rapports (*Avertissement*, *Remarque*, *Informations*).

Ainsi, la possibilité d'exporter le rapport dans un fichier et de l'envoyer à Kaspersky Labs existe uniquement pour les *Avertissements* (par exemple, pour

les tâches qui se sont soldées par une erreur). Il est aussi 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 MS Excel 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 Labs.

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 Labs**. 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 Labs tenteront de résoudre votre problème le plus rapidement possible.



La création automatique d'un message électronique s'opère uniquement dans les clients Microsoft 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.

13.6. 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. ill. 33). Pour ce faire, cliquez sur le lien [Options avancées](#) dans la partie gauche de l'onglet **Paramètres** (cf. ill. 4) et faites votre choix parmi les options proposées :

- 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.
- Utiliser la sonorisation** : active l'émission d'effets sonores pour avertir l'utilisateur de l'affichage d'un message particulier. Vous pouvez sélectionner différents sons pour ces tâches à l'aide des outils du système d'exploitation Windows (**Démarrer** → **Paramètre** → **Panneau de configuration** → **Sons et périphériques audio** → **Sons**).
- Enregistrer les messages pour le rapport détaillé** : consigne dans le rapport détaillé tous les messages diffusés pendant l'exécution des

tâches : les messages à caractères purement informatifs, les avertissements suite à une erreur, etc. 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 le rapport 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.

Lancer le programme lors du chargement 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.

Protéger le logiciel avec un mot de passe : active la saisie obligatoire d'un mot de passe lors de l'ouverture de la fenêtre principale ou d'une tentative de désactivation de la protection en temps réel. 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 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**.

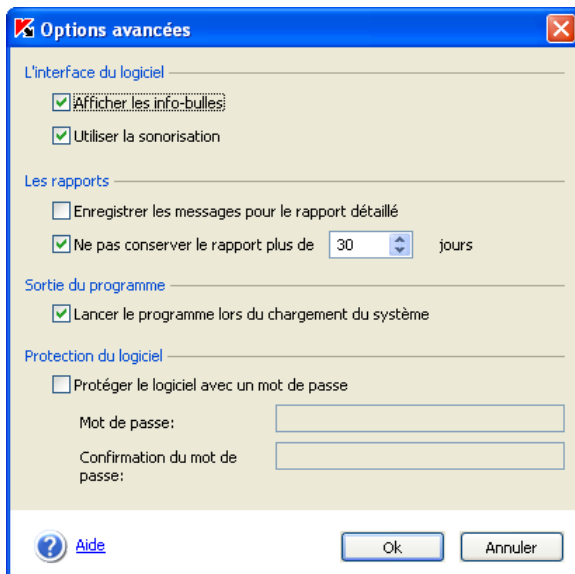


Illustration 33. Options avancées de Kaspersky Anti-Virus® Personal

ANNEXE A. CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Kaspersky Anti-Virus® vous permet de contacter le Service d'assistance technique de Kaspersky Labs 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 Labs 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. 5) de la fenêtre principale du logiciel.

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

Lorsque Kaspersky Anti-Virus® met en quarantaine un fichier potentiellement infecté, vous pouvez tenter de le réparer après avoir mis les bases antivirus à jour (pour de plus amples informations, consultez le point 13.3 à la page 72). 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 Labs 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 Labs uniquement s'ils ont été analysés avec les bases antivirus du jour.



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

Sélectionnez le fichier dans la fenêtre **Quarantaine** (cf. ill. 25) 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 Labs 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 Labs 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 Labs en vue d'un examen.



Pour envoyer à Kaspersky Labs 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. 5). 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 Labs 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.

B

Bases antivirus : il s'agit des bases de données développées par les experts de Kaspersky Labs. 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 sortants 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 Labs. 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

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

O

Objet infecté : objet qui renferme un virus. Nous vous conseillons vivement de ne pas travailler avec de tels objets car cela pourrait entraîner une infection de votre ordinateur. En cas de découverte d'un objet infecté, tentez de le réparer à l'aide de Kaspersky Anti-Virus® Personal ou supprimez-le 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 Excel dans un document Microsoft 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 Labs. 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 infecté 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 découverts lors de l'analyse ou pendant la *protection en temps réel*.

R

Réparation des objets infectés : 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 dans son répertoire d'origine, c'est-à-dire le répertoire où il se trouvait avant sa mise en quarantaine, sa réparation ou sa suppression.

S

Scénario : 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. Selon les résultats de l'analyse, vous pouvez exécuter différentes actions telles qu'autoriser l'exécution du scénario ou, au contraire, l'interdire.

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 Labs : listes des serveurs http et ftp de Kaspersky Labs 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 infectés qui ne peuvent être réparés pour une raison ou l'autre.

V

Virus de démarrage : virus qui a infecté le *secteur d'amorçage* des disques et du système d'exploitation installé sur 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 LABS LTD.

Fondée en 1997, Kaspersky Labs Ltd. est actuellement la société de développement de logiciels de sécurité informatique la plus connue en Russie. Son large éventail de solutions comprend vous protège contre les virus informatiques, le courrier non sollicité et les intrusions de pirates informatiques.

Kaspersky Labs est une société internationale. Le siège social se situe en Russie et la société dispose de représentations commerciales au Royaume-Uni, en France, en Allemagne, au Japon, au Benelux, en Chine, en Pologne, en Roumanie et aux Etats-Unis (Californie). Le Centre européen d'études des virus, le dernier-né des départements de la société, a vu le jour en France. Notre réseau de partenaires réunit plus de 500 sociétés dans le monde entier.

La compagnie est constituée actuellement de plus de 250 spécialistes hautement qualifiés dont 10 sont titulaires d'un MBA (diplôme d'administration d'entreprises), 15 possèdent un doctorat et 2 sont membres de l'éminente organisation informatique de recherche antivirus (CARO).

La valeur essentielle de la société – c'est le savoir et l'expérience uniques accumulés par ses collaborateurs au cours de 14 années d'une lutte impitoyable contre les virus informatiques. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malveillants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Labs. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

C.1. Autres produits antivirus

Kaspersky Anti-Virus® Personal Pro

Ce logiciel a été conçu pour la protection antivirale globale des ordinateurs personnels qui tournent sous Windows 95/98/ME, Windows 2000/NT et Windows XP avec les applications de la suite MS Office 2000. Kaspersky Anti-Virus® Personal Pro renferme un programme qui assure le téléchargement quotidien des mises à jour des bases antivirus ou des modules du logiciel. Le système unique d'analyse heuristique des données de deuxième génération neutralise efficacement les virus inconnus. L'interface utilisateur, simple et conviviale, permet de modifier rapidement la configuration et facilite au maximum l'utilisation du logiciel.

- **L'analyse antivirale à la demande** des disques locaux ;

- **L'analyse antivirus automatique en temps réel** de tous les fichiers utilisés ;
- **Le filtrage du courrier** pour analyser en arrière-plan les messages entrants et sortants ;
- **inhibiteur de comportement** qui garantit une protection totale contre les virus de macro.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker est un pare-feu personnel destiné à la protection d'un ordinateur sous système d'exploitation Windows. Il le protège contre l'accès non autorisé aux données contenues et contre les attaques extérieures d'intrus provenant d'un réseau local adjacent et d'Internet.

Kaspersky® Anti-Hacker surveille l'activité réseau sous protocole TCP/IP de toutes les applications fonctionnant sur votre machine. Le logiciel détecte n'importe quelle action d'une application suspecte et bloque son accès au réseau. Cette solution permet de protéger vos données confidentielles sur votre machine.

La technologie SmartStealth™ rend la détection de votre ordinateur depuis l'extérieur très difficile: en étant invisible, votre ordinateur est protégé contre les attaques des pirates informatiques et cela n'a absolument aucune influence négative sur votre utilisation d'Internet. Le logiciel garantit la transparence et l'accès normal aux données.

Kaspersky® Anti-Hacker bloque les attaques réseau malicieuses les plus fréquentes et est à l'affût des tentatives d'analyse des ports de votre ordinateur.

Le logiciel permet une administration simplifiée, avec un choix de cinq niveaux de sécurité. Par défaut, le logiciel démarre en mode apprentissage, qui configure automatiquement la sécurité de votre système en fonction de vos réponses à des événements variés. Ce mode permet de configurer le pare-feu pour un utilisateur et un ordinateur particulier.

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable contre les virus les données conservées dans un PDA sous système d'exploitation Palm OS ou Windows CE, ainsi que toute information transférée à partir d'un PC ou une carte mémoire, les fichiers ROM et les bases de données. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien sur le PDA que sur n'importe quel type de carte mémoire ;

- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

Kaspersky® Security for PDA est également conçu pour protéger les données stockées dans les ordinateurs de poche (les PDA) contre les accès non autorisés grâce au chiffrement de l'accès à l'appareil et à l'ensemble des données sauvegardées des ordinateurs portables ou des cartes mémoire.

Kaspersky Anti-Virus® Business Optimal

Ce paquet logiciel offre une protection intégrale des données sur des réseaux des petites et moyennes entreprises.

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale⁸ intégrale de :

- Postes de travail sous Windows 98/ME, Windows NT/2000 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; MS ISA Server.

Kaspersky Anti-Virus® Business Optimal comprend également un système d'installation et d'administration centralisé : le Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Corporate Suite

Ce paquet logiciel offre une protection intégrale des données sur des réseaux de toutes dimensions et de tous degrés de complexité. Les composants du paquet logiciel assurent la protection de tous les postes d'un réseau d'entreprise. Compatibles avec la majorité des systèmes d'exploitation et des applications utilisés actuellement, les composants sont unis par un système d'administration centralisé et disposent d'une interface utilisateur identique. La flexibilité de cette solution antivirus permet de créer un système de protection efficace prenant en charge de manière parfaitement appropriée toutes les configurations de votre réseau.

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

⁸ En fonction du type de livraison

- Postes de travail sous Windows 98/ME, Windows NT/2000 Workstation et Linux ;
- *Serveurs de fichiers* sous Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD et Linux ;
- *Système de messagerie* Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;
- *Passerelle-Internet* : CheckPoint Firewall –1; MS ISA Server ;
- *Ordinateurs de poche* sous Windows CE et Palm OS.

Kaspersky® Corporate Suite dispose également d'un *système d'installation et d'administration centralisé* : Kaspersky® Administration Kit.

Vous pouvez choisir librement les logiciels antivirus en fonction du système d'exploitation et des applications que vous utilisez.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

Kaspersky® Anti-Spam se comporte comme un filtre, placé à l'entrée du réseau, qui analyse les flux entrants de courrier électronique à la recherche d'objets identifiés en tant que courrier indésirable. Le logiciel est compatible avec tous les systèmes de messagerie existants sur votre réseau et il peut être installé aussi bien sur un serveur de messagerie existant ou sur un serveur dédié.

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

Kaspersky® Anti-Spam Personal

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

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

Tous les attributs du message sont analysés au moment du filtrage : l'adresse de l'expéditeur, l'adresse du destinataire et l'objet du message. Le filtrage a

également lieu au niveau du contenu. Autrement dit, le corps du message (y compris l'objet) et les pièces jointes sont analysés en fonction d'algorithmes linguistiques et heuristiques uniques.

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

C.2. Coordonnées

Si vous avez des questions, vous pouvez vous adresser à nos distributeurs ou directement à Kaspersky Labs Ltd. (en anglais). Nous vous garantissons un traitement détaillé de votre demande par téléphone ou par courrier électronique. Nous nous efforçons d'apporter des réponses complètes à vos questions.

Support technique	Pour une assistance technique, adressez-vous à : http://www.kaspersky.com/supportinter.html
Informations générales	WWW : http://www.kaspersky.com http://www.viruslist.com E-mail : sales@kaspersky.com

ANNEXE D. CONTRAT DE LICENCE

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

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

SI VOUS AVEZ ACHETE CE LOGICIEL DE MANIERE PHYSIQUE, EN OUVRANT LE BOÎTIER DU CD, VOUS (SOIT UN PARTICULIER OU UN INDIVIDU SEUL) ACCEPTEZ DE RESPECTER CE CONTRAT. SI VOUS N'ACCEPTEZ PAS LA TOTALITE DE CES TERMES, N'OUVREZ PAS LE BOÎTIER DU CD, NE TELECHARGEZ, N'INSTALLEZ OU N'UTILISEZ PAS CE LOGICIEL. VOUS DEVEZ RETOURNER CE LOGICIEL POUR UN REMBOURSEMENT TOTAL. VOTRE DROIT AU RETOUR ET AU REMBOURSEMENT EXPIRE 30 JOURS APRES L'ACHAT CHEZ UN DISTRIBUTEUR OU REVENDEUR AGREE PAR KASPERSKY LABS. LE DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL.

Toutes les références au "Logiciel" apparaissant dans le présent contrat de licence incluent la clé d'activation du logiciel ("Fichier Clé d'Identification") qui vous sera fournie par Kaspersky Labs comme faisant partie du Logiciel.

1. *Octroi de la Licence.* Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Labs vous offre le droit non-exclusif et non-transférable d'utiliser une copie de cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer une copie du Logiciel sur un ordinateur, poste de travail, assistant digital personnel, ou tout autre appareil électronique pour lequel le Logiciel a été conçu (un "Système Client"). Si le Logiciel est inscrit en tant que suite ou paquet avec plus d'un seul Logiciel, cette licence s'applique à tous les Logiciels de la suite, en respectant toute restriction ou limite d'utilisation spécifiée sur le tarif en vigueur ou l'emballage du produit qui concerne chacun de ces Logiciels.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un Système Client ou par plus d'un utilisateur à la fois, sauf comme décrit ci-dessous dans cette section.

1.1.1 Le Logiciel est "en utilisation" sur un Système Client lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de ce Système Client. Cette licence vous permet d'effectuer autant de copies de sauvegarde du Logiciel nécessaires pour un usage légal et uniquement à des fins de sauvegarde, pourvu que toutes ces copies contiennent les notes de propriété du Logiciel. Vous conserverez des traces du nombre et de l'endroit de chaque copie du Logiciel et de la Documentation et prendrez des précautions nécessaires pour protéger le Logiciel contre toute copie ou utilisation illégale.

1.1.2 Si vous cédez le Système Client sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées.

1.1.3 Il est interdit de décompiler, faire l'ingénierie amont, désassembler ou altérer autrement toute partie de ce Logiciel sous forme lisible par l'homme, et de permettre à un tiers de le faire. Les informations d'interface nécessaires pour réaliser l'interopérabilité du Logiciel avec des programmes informatiques indépendants seront fournies par Kaspersky Labs contre une rémunération en rapport avec le coût et les dépenses qu'impliquent de telles informations. Au cas où Kaspersky Labs vous informerait qu'il ne souhaite pas vous fournir de telles informations pour n'importe quelle raison, incluant les coûts (sans limitation), vous serez autorisé à réaliser l'interopérabilité à condition que vous ne fassiez l'ingénierie amont ou ne décompiliez pas hors les limites autorisées par la loi.

1.1.4 Il est interdit de copier (au-delà de ce qui est permis expressément ici), d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

1.1.5 Il est interdit de louer ou prêter le Logiciel à un tiers ou de transférer la licence et votre droit d'utilisation à un tiers.

1.2 Utilisation en Mode Serveur. Vous devez utiliser le Logiciel sur un Système Client ou sur un serveur ("Serveur") dans un environnement multi-utilisateurs ou en réseau ("Mode-Serveur") uniquement si une telle utilisation est autorisée dans le tarif en vigueur ou sur l'emballage du Logiciel. Une licence spécifique est exigée pour chaque Système Client ou "siège" pouvant se connecter au Serveur à tout moment, indifféremment du fait que de tels Systèmes Clients inscrits ou sièges sont connectés en même temps au Logiciel, y accèdent ou l'utilisent. L'utilisation d'un logiciel ou de matériel réduisant le nombre de Systèmes Clients ou sièges qui accèdent au Logiciel ou l'utilisent directement (e.g., un logiciel ou matériel de "multiplexage" ou de "regroupement") ne réduit pas le nombre de licences exigées (i.e., le nombre requis de licences égalerait le nombre d'entrées distinctes au logiciel ou matériel de multiplexage ou de regroupement frontal). Si

le nombre de Systèmes Clients ou sièges pouvant se connecter au Logiciel peut dépasser le nombre de licences dont vous disposez, il vous incombe de prendre des mesures pour vous assurer que l'utilisation du Logiciel ne dépasse pas les limites d'utilisation spécifiées dans la licence obtenue. Cette licence vous permet d'effectuer ou de télécharger autant de copies de la Documentation que le réseau compte de Systèmes Clients ou sièges possédant une licence d'utilisation du Logiciel, et pourvu que chaque copie contienne les notes de propriété de la Documentation.

1.3 Licences de volume. Si le Logiciel est inscrit avec des termes de Licences de volume spécifiés sur la facture en vigueur ou l'emballage du Logiciel, vous devez effectuer, utiliser ou installer autant de copies additionnelles du Logiciel sur le nombre de Systèmes Clients que les termes de la licence de volume le spécifient. Vous devez tout mettre en oeuvre pour vous assurer que le nombre de Systèmes Clients sur lesquels le Logiciel a été installé ne dépasse pas le nombre de licences obtenues. Cette licence vous permet d'effectuer ou de télécharger une copie de la Documentation pour chaque copie additionnelle autorisée par la licence de volume, pourvu que chaque copie contienne toutes les notes de propriété de la Documentation.

2. *Durée.* Ce Contrat est valable pour la période indiquée dans le Fichier Clé d'Identification (Ce fichier est unique et est nécessaire à l'activation complète du Logiciel, voir Aide/ sur Logiciel ou " à propos de ". Pour les versions Unix/Linux du Logiciel voir les notifications sur la date d'expiration du Fichier Clé) à moins que celle-ci n'arrive à terme avant pour l'une des raisons notées ci-après. Ce contrat se terminera automatiquement si vous n'en respectez les termes, limites ou conditions décrites. Au-delà du terme ou expiration de ce Contrat, vous devez immédiatement détruire toutes les copies du Logiciel et de la Documentation. Vous pouvez mettre un terme à ce Contrat à tout moment en détruisant toutes les copies du Logiciel et de la Documentation.

3. Assistance technique.

(i) Kaspersky Labs vous fournira une assistance technique ("Assistance Technique") comme décrit ci-dessous pour une période d'un an à condition que:

(a) le paiement des frais de l'assistance technique en cours ait été fait; et

(b) le Formulaire d'Inscription à l'Assistance Technique fourni avec ce Contrat ou disponible sur le site web de Kaspersky Labs ait été rempli, ce qui nécessitera que vous communiquiez le Fichier Clé d'Identification fourni par Kaspersky Labs avec ce Contrat. Il restera à l'entière discrétion de Kaspersky Labs de juger si vous remplissez les conditions nécessaires pour un accès aux services d'Assistance Technique.

(ii) L'Assistance technique se termine sauf si renouvelée annuellement par le paiement des droits requis et par l'envoi d'un nouveau Formulaire d'Inscription.

(iii) En remplissant le Formulaire d'Inscription de l'Assistance Technique, vous acceptez les termes de la Politique de Confidentialité de Kaspersky Labs jointe à

ce Contrat, et vous consentez explicitement au transfert de données vers d'autres pays que le votre en accord avec les termes de la Politique de Confidentialité.

(iv) "Assistance Technique" signifie:

(a) Mises à jour quotidiennes des bases de données antivirales;

(b) Mises à jour gratuites du logiciel, incluant des mises à niveau de versions;

(c) Assistance Technique étendue par E-mail et assistance téléphonique fournie par votre Vendeur et/ou Distributeur;

(d) Mises à jour de détection et désinfection de virus sous 24 heures.

4. *Droits de Propriété.* Le Logiciel est protégé par les lois sur le copyright. Kaspersky Labs et ses fournisseurs possèdent et conservent tous les droits, titres et intérêts applicables au Logiciel, incluant tous les copyrights, brevets, marques déposées et autres droits de propriété intellectuelle concernés. Votre possession, installation ou utilisation du Logiciel ne vous transmet pas le droit de propriété intellectuelle sur le Logiciel, et ne vous donne aucun droit sur le Logiciel sauf si décrit expressément ci-après dans ce Contrat.

5. *Confidentialité.* Vous acceptez que le Logiciel et la Documentation, toutes ses applications et le Fichier Clé d'Identification constituent des informations confidentielles dont Kaspersky Labs reste propriétaire. Vous ne dévoilerez, fournirez ou ne mettrez en aucun cas à disposition ces informations confidentielles sous quelque forme que ce soit à un tiers sans autorisation expresse et écrite de Kaspersky Labs. Vous mettrez en oeuvre des mesures de sécurité raisonnables visant à assurer que la confidentialité du Fichier Clé d'Identification soit respectée.

6. *Limites de Garantie*

(i) Kaspersky Labs garantit que pour une durée de [90] jours suivant le téléchargement ou l'installation du logiciel, ce dernier fonctionnera correctement comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

(ii) Vous assumez l'entière responsabilité du choix du logiciel comme répondant à vos besoins. Kaspersky Labs ne garantit pas que le Logiciel et/ou la Documentation répondront à ces besoins et que leur utilisation sera exempte d'interruptions et d'erreurs;

(iii) Kaspersky Labs ne garantit pas que ce Logiciel reconnaîtra tous les virus connus ou n'affichera de message de détection erroné;

(iv) L'entière responsabilité de Kaspersky Labs ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Labs de réparer, remplacer ou rembourser le logiciel si le problème est signalé directement à Kaspersky Labs ou à un ayant-droit au cours

de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel;

(v) La garantie comme décrite au paragraphe (i) ne s'appliquera pas si (a) vous modifiez ou faites modifier le logiciel sans le consentement de Kaspersky Labs, (b) vous utilisez le Logiciel d'une façon différente de son but initial ou (c) vous utilisez le Logiciel d'une façon non prévue par ce Contrat;

(vi) Les garanties et conditions fixées dans ce Contrat prévalent sur toutes autres conditions et garanties légales ou termes qui concernent la fourniture ou la prétendue fourniture, le manquement ou délai à fournir le Logiciel ou la Documentation, mais qui pour ce paragraphe (v) ont effet entre Kaspersky Labs et vous ou sont implicites ou intégrés dans ce Contrat ou autre contrat collatéral, soit par statut, loi commune ou tout ce qui est exclu ici (incluant sans limitation les conditions, garanties ou autres termes relatifs à la qualité de satisfaction, justesse d'utilisation ou pour le respect de compétences et du bon sens).

7. Limites de Responsabilité

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Labs en cas (i) de non-satisfaction de l'utilisateur, (ii) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, (iii) de toute infraction aux obligations impliquées par la loi "s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982" ou (iv) de responsabilité qui ne peut être exclue par la loi.

(ii) Selon les termes du paragraphe (i), le Fournisseur ne pourra être tenu pour responsable (si dans le contrat, acte dommageable, compensation ou autres) pour les dommages et pertes suivants (si de tels dommages ou pertes étaient prévus, prévisibles, connus ou autres):

(a) Perte de revenus;

(b) Perte de revenus réels ou potentiels (incluant les pertes de revenus sur contrats);

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données; ou

(j) Tout dommage ou toute perte qu'ils soient directs ou indirects, ou causés de quelque façon que ce soit (incluant, pour éviter le doute, ces dommages ou pertes spécifiés dans les paragraphes (ii), (a) jusque (ii), (i).

(iii) Selon les termes du paragraphe (i), la responsabilité de Kaspersky Labs (si dans le contrat, acte dommageable, compensation ou autres) survenant lors de la fourniture du Logiciel n'excèdera en aucun cas un montant égal à celui du prix d'achat du Logiciel.

8. Le sens et l'interprétation de ce Contrat devront être déterminés en accord avec les lois d'Angleterre et du Pays de Galles. Les parties se soumettent ici à la juridiction des cours d'Angleterre et du Pays de Galles, sauf si Kaspersky Labs était autorisé en tant que requérant à entamer des procédures dans n'importe quelle juridiction compétente.

9. (i) Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Labs, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'Effet. En dehors des situations prévues dans les termes des paragraphes (ii) – (iii), vous n'aurez aucun recours au cas où vous auriez fourni des informations erronées et sur lesquelles vous vous basiez en acceptant ce Contrat ("Fausse Représentation") et Kaspersky Labs ne sera pas tenu pour responsable envers tout autre poursuivant que celui déterminé expressément dans ce Contrat.

(i) Rien dans ce Contrat n'engagera la responsabilité de Kaspersky Labs pour toute Fausse Représentation faite en connaissance de cause.

(ii) La responsabilité de Kaspersky Labs pour Fausse Déclaration quant à une question fondamentale pour la capacité du créateur à exécuter ses engagements envers ce Contrat, sera sujette à la limitation de responsabilité décrite dans le paragraphe 7 (iii).