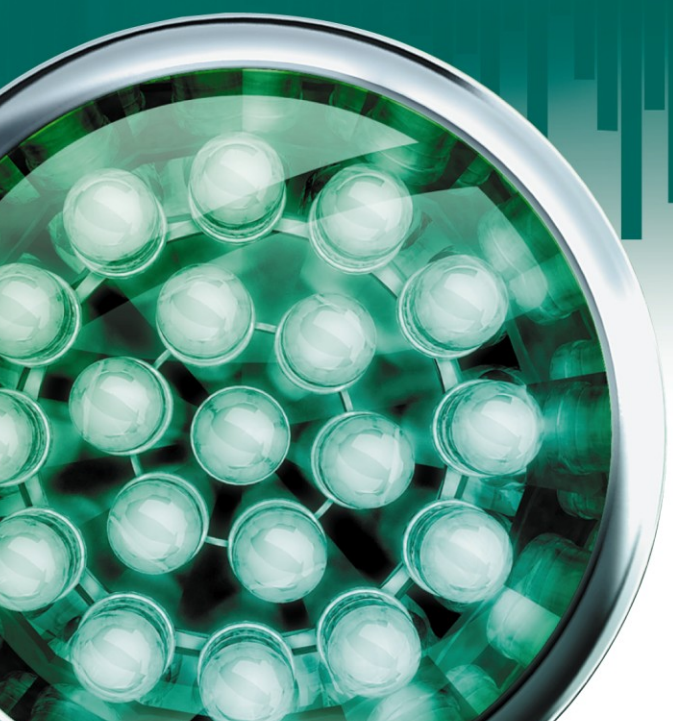
Kaspersky Internet Security 2010

MANUEL DE L'UTILISATEUR

VERSION DE L'APPLICATION : 9.0 CRITICAL FIX 2



KASPERSKY lab

Chers utilisateurs !

Nous vous remercions d'avoir choisi notre logiciel. Nous espérons que ce manuel vous sera utile et qu'il répondra à la majorité des questions.

Date d'édition : 08/10/09

http://www.kaspersky.com/fr
http://support.kaspersky.com/fr

TABLE DES MATIERES

INTRODUCTION

DANS CETTE SECTION

DISTRIBUTION

Vous pouvez acheter Kaspersky Internet Security chez nos partenaires (version en boîte) ou en ligne (par exemple, http://www.kaspersky.com/fr, rubrique **Boutique en ligne**).

Si vous achetez le logiciel en boîte, vous recevrez :

- Une enveloppe cachetée contenant le cédérom d'installation avec les fichiers du logiciel et la documentation au format .pdf.
- La documentation en version "papier" présentée par les documents suivants : Manuel de l'utilisateur et Démarrage rapide.
- Contrat de licence (dépend de la région).
- La carte d'activation contenant le code d'activation et les instructions d'activation de l'application (dépend de la région).

Le contrat de licence est un accord juridique conclu entre vous et Kaspersky Lab qui prévoit les conditions dans lesquelles vous pouvez utiliser le logiciel que vous avez acheté.

Lisez attentivement le contrat de licence !

Si vous n'acceptez pas les termes du contrat de licence, vous pouvez rendre la boîte avec le logiciel au magasin où vous l'aviez acheté en échange du remboursement intégral. Dans ce cas, l'enveloppe contenant le cédérom ou les disquettes ne peut avoir été ouverte.

L'ouverture de l'enveloppe contenant le cédérom (ou les disquettes) d'installation marque votre accord avec les termes du contrat de licence.

Avant d'ouvrir l'enveloppe contenant le cédérom (ou les disquettes), veuillez lire attentivement le contrat de licence.

Si vous achetez Kaspersky Internet Security en ligne, vous copiez le logiciel depuis le site Internet de Kaspersky Lab. Cette distribution, outre le logiciel, reprend également ce guide. Le code d'activation vous sera envoyé par courrier électronique après le paiement.

SERVICES POUR LES UTILISATEURS ENREGISTRES

Kaspersky Lab offre à ses utilisateurs légitimes un vaste éventail de services qui leur permettent d'accroître l'efficacité de l'utilisation de l'application.

En obtenant une licence, vous devenez un utilisateur enregistré et vous pouvez bénéficier des services suivants pendant la durée de validité de la licence :

- Mise à jour toutes les heures des bases de l'application et accès aux nouvelles versions de ce logiciel ;
- Consultation par téléphone ou courrier électronique sur des questions liées à l'installation, à la configuration et à l'exploitation du logiciel ;
- Notifications de la sortie de nouveaux logiciels de Kaspersky Lab ou de l'émergence de nouveaux virus. Ce service est offert aux utilisateurs qui se sont abonnés au bulletin d'informations de Kaspersky Lab sur le site du service d'Assistance technique (http://support.kaspersky.com/fr/subscribe).

Aucune aide n'est octroyée pour les questions relatives au fonctionnement et à l'utilisation des systèmes d'exploitation, de logiciels tiers ou de diverses technologies.

CONFIGURATION MATERIELLE ET LOGICIELLE REQUISES

Pour que Kaspersky Internet Security 2010 puisse fonctionner normalement, l'ordinateur doit répondre aux exigences minimales suivantes :

Recommandations d'ordre général :

- 375 Mo d'espace disponible sur le disque dur.
- CD-ROM (pour l'installation de Kaspersky Internet Security 2010 depuis un cédérom).
- Microsoft Internet Explorer 6.0 ou suivant (pour la mise à jour des bases et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (Service Pack 2), Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition :

- Processeur Intel Pentium 300 Mhz minimum (ou similaire).
- 256 Mo de mémoire vive disponible.

Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate :

- Processeur Intel Pentium 800 Mhz 32 bits (x86)/ 64-bit (x64) minimum (ou similaire).
- 512 Mo de mémoire vive disponible.

Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Processeur Intel Pentium 1 GHz 32 bits (x86)/ 64-bit (x64) minimum (ou similaire).
- 1 Go de mémoire vive disponible (32-bit) ; 2 Go de mémoire vive disponible (64-bit).

KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 représente la nouvelle génération d'applications de protection des informations.

Ce qui distingue Kaspersky Internet Security 2010 des autres applications existantes, y compris des applications de Kaspersky Lab, c'est la démarche complexe adoptée pour la protection des informations stockées sur l'ordinateur de l'utilisateur.

DANS CETTE SECTION

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur la sélection, l'achat, l'installation ou l'utilisation de Kaspersky Internet Security, vous pouvez trouver la réponse rapidement.

Kaspersky Lab offre diverses sources d'informations sur l'application. Vous pouvez ainsi choisir celle qui s'adapte le mieux à votre situation en fonction de l'importance et de l'urgence de la question.

DANS CETTE SECTION

SOURCES D'INFORMATIONS POUR UNE AIDE AUTONOME

Vous pouvez consulter les sources d'informations suivantes sur l'application :

- La page de l'application sur le site de Kaspersky Lab ;
- La page de l'application sur le site du service d'assistance technique (dans la banque de solutions) ;
- La page du service d'assistance interactive ;
- L'aide électronique ;
- La documentation.

Page du site de Kaspersky Lab

http://www.kaspersky.com/fr/kaspersky_internet_security

Cette page fournit des informations générales sur l'application, ses possibilités et ses particularités.

Page sur le site du service d'assistance technique (banque de solutions)

http://support.kaspersky.com/fr/kis2010

Cette page reprend des articles publiés par les experts du service d'assistance technique.

Ces articles proposent des informations utiles, des recommandations et des réponses aux questions fréquemment posées sur l'achat, l'installation et l'utilisation de l'application. Ils sont regroupés par sujets tels que "Utilisation des licences", "Configuration de la mise à jour des bases" ou "Suppression des échecs". Les articles peuvent répondre à des questions en rapport non seulement avec l'application mais également en rapport avec d'autres applications de Kaspersky Lab ; ils peuvent également fournir des nouvelles sur le service d'assistance technique dans son ensemble.

Service d'assistance interactive

La page de ce service propose une base fréquemment actualisée avec les questions fréquemment posées. L'utilisation de ce service requiert une connexion Internet.

Pour accéder à la page du service, dans la fenêtre principale de l'application, cliquez sur le lien **Assistance technique** et dans la fenêtre qui s'ouvre, cliquez sur le bouton **Assistance interactive**.

Aide électronique

La distribution de l'application reprend le fichier d'aide complète et contextuelle qui contient les informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, analyse de divers secteurs de l'ordinateur, exécution d'autres tâches ainsi que les informations relatives à chaque fenêtre de l'application : description des paramètres qui figurent dans chacune d'entre elles et liste des tâches exécutées.

Pour ouvrir le fichier d'aide, cliquez sur le bouton **Aide** dans la fenêtre qui vous intéresse ou sur la touche **<F1>** du clavier.

Documentation

La distribution de Kaspersky Internet Security reprend le document **Manuel de l'utilisateur** (au format .pdf). Ce document contient une description des fonctions et des possibilités de l'application ainsi que des principaux algorithmes de fonctionnement.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur la sélection, l'achat de Kaspersky Internet Security ou le renouvellement de la licence, vous pouvez contacter notre service Commercial par courrier électronique en écrivant à :

info@fr.kaspersky.com

ou consulter notre boutique en ligne sur :

http://kaspersky.telechargement.fr/

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez acheté Kaspersky Internet Security, vous pouvez contacter les experts du service d'assistance technique par téléphone ou par Internet afin d'obtenir des informations sur cette application.

Les experts du service d'assistance technique répondront à vos questions sur l'installation et l'utilisation de l'application et en cas d'infection, ils vous aideront à supprimer les dégâts provoqués par les applications malveillantes.

Avant de contacter le service d'assistance technique, veuillez prendre connaissance des règles d'assistance (http://support.kaspersky.com/fr/support/rules).

Assistance Technique en ligne

Vous pouvez retrouver toutes nos options de support à partir de notre portail de support : http://support.kaspersky.fr/kis2010 requête envoyée par voie électronique au service d'assistance technique.

Les experts du service d'assistance technique vous transmettront leur réponse via votre Espace personnel (https://my.kaspersky.com/fr) et via le courrier électronique que vous aurez indiqué dans votre demande.

Décrivez le problème rencontré de la manière la plus détaillée possible dans le formulaire de contact. Saisissez les informations suivantes dans les champs obligatoires :

- **Type de demande**. Choisissez le sujet qui correspond le mieux à votre problème, par exemple « Suppression de virus » ou « Installation/désinstallation du programme ». Si aucune des propositions ne correspond à votre situation, choisissez l'option « Question générale »
- **Nom et version de l'application**.
- **Texte de la demande**. Décrivez le problème rencontré avec le plus de détails possibles.
- **Code client et mot de passe**. Saisissez le code client et le mot de passe que vous avez obtenu après l'enregistrement sur le site du service d'assistance technique.
- **Courrier électronique**. Il s'agit de l'adresse à laquelle les experts du service d'assistance technique enverront la réponse à votre demande.

DISCUSSION SUR LES LOGICIELS DE KASPERSKY LAB DANS LE FORUM EN LIGNE

Si votre question n'est pas urgente, vous pouvez en discuter avec les experts de Kaspersky Lab et d'autres utilisateurs dans notre forum à l'adresse http://forum.kaspersky.com.

Une fois que vous avez accédé au forum, vous pouvez consulter les sujets publiés, écrire vos commentaires, créer de nouveaux sujets ou lancer des recherches.

NOUVEAUTES DE KASPERSKY INTERNET SECURITY 2010

Kaspersky Internet Security 2010 : une solution universelle de protection de l'information. Cette application vous protégera non seulement contre les virus, mais également contre le courrier indésirable et les attaques de réseau. Les différents composants de l'application permettent de protéger l'ordinateur contre les menaces inconnues et fraudes sur Internet ainsi que de contrôler l'accès des utilisateurs à Internet.

Tous les canaux de transfert d'informations sont couverts par la protection sophistiquée. La souplesse de la configuration de chacun des composants permet d'adapter au maximum Kaspersky Internet Security aux besoins de chaque utilisateur.

Examinons maintenant en détail les nouveautés de Kaspersky Internet Security 2010.

Nouveautés au niveau de la protection :

- Kaspersky Internet Security comprend un composant Contrôle des Applications (cf. page 74) qui assure avec la Défense Proactive et le Pare-Feu une protection universelle contre n'importe quelle menace. Le composant enregistre les actions réalisées par les applications dans le système et réglemente leur activité sur la base du niveau de confiance attribué. Le composant contrôle l'accès aux données personnelles de l'utilisateur, aux paramètres et aux objets du système d'exploitation, aussi il empêche l'exécution d'actions dangereuses par des applications.

- Le nouveau composant Antivirus IM ("Chat") (cf. page 71) garantit une utilisation sans danger de plusieurs systèmes de messagerie instantanée. Le composant analyse les messages sur la présence des objets malveillants.

- Le mécanisme permettant d'exécuter les applications dans un milieu virtuel protégé, à savoir l'Environnement protégé (cf. page 84) a été développé. Le lancement des navigateurs Internet dans l'environnement protégé garantit la sécurité de consultation des sites Internet, y compris la protection contre les applications malveillantes et la protection des données personnelles de l'utilisateur contre les modifications et suppressions non autorisées, ainsi que la possibilité de supprimer tous les objets accumulés lors des séances d'utilisation d'Internet (fichiers temporaires, cookies, historique des visites, etc.).

- Kaspersky Internet Security propose un module d'analyse des liens (cf. page 68) qui est administré par l'Antivirus Internet. Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.

- Le contrôle de l'accès aux sites de phishing et la protection contre les attaques de phishing s'opèrent via l'analyse des liens contenus dans les messages et sur les pages Web, ainsi que lors des tentatives d'ouverture de sites, par rapport à la base des URL de phishing. La recherche des URL dans les bases de phishing est une fonction offerte par l'Antivirus Internet (cf. page 67), l'Antivirus IM ("Chat") (cf. page 72) et l'Anti-Spam (cf. page 110).

- La liste des analyses contient un nouvel instrument, à savoir la Recherche de Vulnérabilités (cf. page 146) qui facilite la recherche et la suppression des menaces pour la sécurité, des vulnérabilités dans les applications installées et les paramètres du système d'exploitation.

Nouveautés de l'interface :

- Une nouvelle approche pour administrer la sécurité a été réalisée, à savoir la Protection (cf. page 19). La protection de l'ordinateur est assurée à trois niveaux : au niveau des fichiers et des données personnelles, au niveau des objets du système d'exploitation et des applications installées, et au niveau de l'utilisation du réseau. Un groupe de composants distincts est responsable pour chaque aspect de la protection. La centrale de protection permet d'évaluer la participation de chaque composant dans la protection d'une ressource particulière et d'accéder rapidement à la configuration de ses paramètres.

- La nouvelle section Contrôle des Applications (cf. page 19) assure un accès rapide à l'administration des paramètres de la protection qui aident à empêcher l'exécution des actions (dangereuses pour le système) par les applications et contrôler l'accès à vos données personnelles. Ainsi, le démarrage des applications dans l'environnement protégé est réalisé.

- Les Assistants et les outils (cf. page 20) qui aident à résoudre les tâches spécifiques pour la sécurité de l'ordinateur sont repris dans une section particulière **Utilitaires+**.

CONCEPT DE LA PROTECTION DE VOTRE ORDINATEUR

Kaspersky Internet Security protège votre ordinateur contre les menaces connues et nouvelles, les attaques de réseau et les escroqueries, les messages non sollicités et d'autres données indésirables. Chaque type de menace est traité par un composant distinct de l'application. Une telle conception de la protection permet de réaliser une configuration souple de l'application en fonction des besoins concrets de chaque utilisateur ou entreprise.

Kaspersky Internet Security contient les composants de protection suivants :

- Les composants de la protection qui assurent la protection :
  - Des fichiers et des données personnelles ;
  - Du système ;
  - De l'utilisation du réseau.
- Les tâches d'analyse (cf. page 18) qui permettent de rechercher la présence éventuelle de virus dans des fichiers, des répertoires, des disques ou des secteurs déterminés ou de lancer une analyse complète de l'ordinateur.
- La mise à jour (cf. page 19) qui garantit l'actualité des modules internes de l'application et des bases utilisées pour identifier les applications malveillantes, repérer les attaques de réseau et isoler les messages non sollicités.
- Les assistants et les outils (cf. page 20) qui facilitent l'exécution des tâches découlant du fonctionnement de Kaspersky Internet Security.
- Les fonctions de service (cf. page 20) qui offrent des informations sur l'utilisation des applications et qui permettent d'élargir leurs fonctions.

DANS CETTE SECTION

TACHES DE RECHERCHE D'EVENTUELS VIRUS

Outre la protection de toutes les sources d'introduction d'applications malveillantes, il est primordial de réaliser à intervalle régulier une analyse de votre ordinateur. Cette opération s'impose pour exclure la possibilité de propager des applications malveillantes qui n'auraient pas été décelées par les composants de la protection en raison, par exemple, d'un niveau de protection faible ou pour toute autre raison.

Kaspersky Internet Security contient les tâches suivantes pour la recherche de virus :

- **Analyse des Objets**. Analyse des Objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.
- **Analyse Complète**. Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse Rapide**. Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

MISE A JOUR

Afin d'être toujours prêt à faire face à n'importe quelle activité de réseau, à supprimer des virus ou d'autres applications dangereuses, il faut maintenir Kaspersky Internet Security à jour. Le composant **Mise à jour** a été développé à cette fin. Il est chargé de la mise à jour des bases et des modules de l'application utilisés.

Le service de copie des mises à jour permet d'enregistrer les mises à jour des bases et des modules de l'application récupérées sur les serveurs de Kaspersky Lab dans un répertoire local et puis, d'octroyer l'accès à ce répertoire aux autres ordinateurs du réseau dans le but d'économiser le trafic Internet.

PROTECTION DES DONNEES ET DE L'ACTIVITE EN LIGNE

Kaspersky Internet Security protège les données de votre ordinateur contre les applications malveillantes et l'accès non autorisé, et garantit également la sécurité de l'accès au réseau local et à Internet.

Les objets protégés sont scindés en trois groupes :

- Les fichiers, les données personnelles, les paramètres d'accès à diverses ressources (nom d'utilisateur et mot de passe), les informations relatives aux cartes bancaires, etc. La protection de ces objets est garantie par l'Antivirus Fichiers, le Contrôle des Applications et la Défense proactive.
- Les applications installées sur l'ordinateur et les objets du système d'exploitation. La protection de ces objets est garantie par l'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM ("Chat"), le Contrôle des Applications, la Défense proactive, la Prévention des intrusions et l'Anti-Spam.
- Utilisation du réseau : consultation de sites, utilisation de systèmes de paiement en ligne, protection du courrier contre les messages non sollicités et les virus, etc. La protection de ces objets est garantie par l'Antivirus Courrier, l'Antivirus Internet, l'Antivirus IM ("Chat"), le Pare-feu, la Prévention des intrusions, l'Anti-Spam, la Surveillance du réseau, l'Anti-bannière et le Contrôle Parental.

CONTROLE DES APPLICATIONS ET DE L'ACCES AUX DONNEES

Kaspersky Internet Securit empêche l'exécution d'actions dangereuses pour le système, contrôle l'accès aux données personnelles et exécute les applications en environnement protégé à l'aide des outils suivants :

- **Contrôle des Applications** (cf. page 74). Le composant enregistre les actions réalisées par les applications dans le système et réglemente l'activité des applications sur la base du groupe auquel elles appartiennent. Un ensemble de règles a été défini pour chaque groupe d'applications. Ces règles définissent l'accès des applications à diverses ressources.
- **Protection des Données Personnelles** (cf. page 77). Le Contrôle des Applications gère les privilèges des applications pour l'exécution d'actions sur les données personnelles de l'utilisateur. Il s'agit des fichiers, des répertoires et des clés du registre qui contiennent les paramètres de fonctionnement et les données importantes

des applications les plus souvent utilisées ainsi que les fichiers de l'utilisateur (répertoire Mes Documents, les cookies, les données relatives à l'activité de l'utilisateur).

- **Exécution en environnement protégé** (cf. page 84). Kaspersky Internet Security garantit une sécurité maximale pour les objets du système d'exploitation et les données de l'utilisateur grâce à l'exécution des applications d'éditeurs tiers en environnement protégé.

ASSISTANTS ET OUTILS

Garantir la protection de l'ordinateur est une tâche complexe qui requiert des connaissances sur les particularités de fonctionnement du système d'exploitation et sur les moyens d'exploiter ses points faibles. De plus, le volume important des informations sur la protection du système et la diversité de celles-ci complique l'analyse et le traitement.

Pour faciliter l'exécution de tâches spécifiques pour la sécurité de l'ordinateur, Kaspersky Internet Security contient plusieurs assistants et outils :

- Assistant de configuration du navigateur (cf. page 193) qui analyse les paramètres du navigateur Microsoft Internet Explorer et qui les évalue avant tout du point de vue de la sécurité.
- Assistant de restauration après infection (cf. page 196) permet de liquider les traces de la présence d'objets malveillants dans le système.
- Assistant de suppression des traces d'activité (cf. page 196) recherche et supprime les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent d'accumuler des données sur l'activité de l'utilisateur.
- Disque de dépannage (cf. page 190) est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il intervient dans les cas d'infection qui rendent la réparation de l'ordinateur impossible à l'aide des logiciels antivirus ou des outils de réparation.
- Recherche de vulnérabilités (cf. page 146) pose un diagnostic sur la sécurité de l'ordinateur et recherche les vulnérabilités dans le système d'exploitation et les applications installées.
- Analyse des paquets de réseau (cf. page 194) qui intercepte les paquets de réseau et qui affiche des informations détaillées à leur sujet.
- Surveillance du réseau (cf. page 197) qui fournit des informations détaillées sur l'activité de réseau sur votre ordinateur.
- Clavier virtuel (cf. page 189) qui permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

FONCTIONS DE SERVICE DE L'APPLICATION

Kaspersky Internet Security propose diverses fonctions de service. Ces fonctions visent à maintenir l'application à jour, à élargir les possibilités d'utilisation et à faciliter l'utilisation.

Fichiers de données et rapports

Un rapport est créé sur chaque composant de la protection, chaque analyse ou chaque mise à jour pendant l'utilisation de l'application. Ce rapport contient des informations sur les opérations exécutées et sur les résultats des tâches, ce qui vous permet de toujours connaître en détails le fonctionnement de n'importe quel composant de Kaspersky Internet Security. En cas de problèmes, les rapports peuvent être envoyés à Kaspersky Lab où les experts pourront étudier la situation plus en détails et vous aider à résoudre le problème le plus vite possible.

Tous les objets suspects du point de vue de la sécurité sont placés par Kaspersky Internet Security dans un répertoire spécial : la *quarantaine*. Les objets sont conservés sous forme chiffrée afin d'éviter l'infection de l'ordinateur. Vous pouvez soumettre ces objets à une analyse, les restaurer dans leur emplacement d'origine, les supprimer ou les ajouter vous-même à la quarantaine. Tous les objets considérés comme sains suite à l'analyse sont restaurés automatiquement dans leur emplacement d'origine.

La *sauvegarde* abrite les copies des objets réparés ou supprimés par Kaspersky Internet Security. Ces copies sont créées au cas où il faudrait restaurer les objets ou reproduire le scénario de l'infection. Les copies de sauvegarde des objets sont conservées également sous forme chiffrée afin d'éviter l'infection de l'ordinateur.

Vous pouvez restaurer l'objet depuis la sauvegarde vers son emplacement d'origine ou supprimer la copie.

Licence

Au moment d'acheter Kaspersky Internet Security, vous et Kaspersky Lab signez un contrat de licence qui vous donne le droit d'utiliser l'application, de recevoir les mises à jour des bases de l'application et de contacter le service d'assistance technique durant une période déterminée. La durée d'utilisation ainsi que toute autre information requise pour le fonctionnement de l'application figurent dans la licence.

Le menu **Licence** vous permet d'obtenir des informations détaillées sur la licence que vous utilisez, d'acheter une nouvelle licence ou de renouveler la licence en cours.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Internet Security peuvent utiliser le service d'assistance technique. Pour connaître les conditions d'octroi de l'assistance, utilisez le menu **Assistance technique**.

Grâce aux liens correspondant, vous pouvez accéder au forum des utilisateurs des applications de Kaspersky Lab ou envoyer au service d'assistance technique un message sur une erreur ou un commentaire sur le fonctionnement de l'application en remplissant un formulaire spécial sur le site.

Vous avez également accès au service d'assistance technique en ligne, à l'Espace personnel de l'utilisateur et, bien évidemment, aux consultations téléphoniques avec nos collaborateurs qui sont toujours prêts à vous aider dans votre utilisation de Kaspersky Internet Security.

INSTALLATION DE KASPERSKY INTERNET SECURITE SUR L'ORDINATEUR

L'installation de l'application se déroule en mode interactif à l'aide de l'Assistant d'installation de l'application.

Avant de lancer l'installation, il est conseillé de quitter toutes les applications en cours d'exécution.

Pour installer l'application, lancez le fichier de distribution (extension *.exe) sur le cédérom du logiciel.

L'installation de Kaspersky Internet Security au départ d'une distribution téléchargée depuis Internet est identique à l'installation depuis le cédérom.

Vient ensuite la recherche du paquet d'installation de Kaspersky Internet Security (fichier doté de l'extension *.msi). Si le fichier est présent, le système vérifiera l'existence d'une version plus récente sur les serveurs de Kaspersky Lab via Internet. Si le fichier du paquet d'installation est introuvable, vous serez invité à le télécharger. L'installation de Kaspersky Internet Security sera lancée à la fin du téléchargement. En cas de refus du téléchargement, l'installation de l'application se poursuivra en mode normal.

Le programme d'installation se présente sous la forme d'un Assistant. Chaque fenêtre contient une sélection de boutons qui permettent d'administrer le processus d'installation. Voici une brève description de leur fonction :

- **Suivant** : exécute l'action et passe à l'étape suivante de l'installation.
- **Précédent** : revient à l'étape précédente de l'installation.
- **Annuler** : annule l'installation du logiciel.
- **Terminer** : termine la procédure d'installation de l'application.

Examinons en détail chacune des étapes de la procédure d'installation.

DANS CETTE SECTION

ETAPE 1. RECHERCHE D'UNE VERSION PLUS RECENTE DE L'APPLICATION

Avant l'installation une recherche d'une version plus actuelle de Kaspersky Internet Security sur les serveurs des mises à jour de Kaspersky Lab s'effectue.

Si les serveurs de Kaspersky Lab n'hébergent pas une version plus récente, l'Assistant d'installation de la version actuelle est lancé.

Si les serveurs de mises à jour hébergent une version plus récente, vous serez invité à la télécharger et à l'installer sur votre ordinateur. Si vous refusez d'installer la version plus récente, l'Assistant d'installation de la version actuelle sera lancé. Si vous décidez d'installer la nouvelle version, les fichiers de la distribution seront copiés sur l'ordinateur et l'Assistant d'installation sera lancé automatiquement.

ETAPE 2. VERIFICATION DES CONFIGURATIONS MINIMUM REQUISES POUR L'INSTALLATION

Avant de procéder à l'installation de l'application, le système vérifie si le système d'exploitation et les Service Pack installés répondent aux exigences pour l'installation. Egalement, la présence du logiciel requis ainsi que des droits d'installation du logiciel est vérifiée.

Si une des conditions n'est pas remplie, le message de circonstance apparaîtra. En ce cas, avant l'installation de l'application de Kaspersky Lab, il est recommandé d'installer les paquets des mises à jour requis à l'aide du service Windows Update et les programmes nécessaires.

ETAPE 3. SELECTION DU TYPE D'INSTALLATION

Si votre système répond parfaitement aux exigences, s'il n'existe pas une version plus récente de l'application sur les serveurs de mise à jour de Kaspersky Lab ou si vous avez décidé de ne pas installer cette version plus récente, l'Assistant d'installation de la version actuelle s'ouvre.

Cette étape d'installation correspond à la sélection du type d'installation qui vous convient le mieux :

- *Installation rapide*. Si vous choisissez cette option (la case **Installation personnalisée** est cochée), l'application sera installée en entier sur l'ordinateur avec les paramètres de protection recommandés par les experts de Kaspersky Lab. L'Assistant de configuration (à la page 29) sera lancé à la fin de l'installation.

- *Installation personnalisée*. Dans ce cas de figure (la case **Installation personnalisée** est cochée), vous êtes invité à sélectionner les composants de l'application que vous souhaitez installer, et à désigner le répertoire dans lequel l'application sera installée, ainsi qu'à activer l'application et à la configurer à l'aide d'un Assistant spécial.

Quand vous sélectionnez la première option, l'Assistant d'installation de l'application vous proposera de prendre connaissance avec le contrat de licence ainsi qu'avec le règlement d'utilisation de Kaspersky Security Network. Ensuite, le programme sera installé sur votre ordinateur.

Dans le deuxième cas, vous devrez saisir ou confirmer certaines données à chaque étape de l'installation.

Pour poursuivre l'installation, cliquez sur **Suivant**. Pour annuler l'installation, cliquez sur le bouton **Annuler**.

ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Cette étape vous recommande de prendre connaissance avec le contrat de licence qui est conclu entre vous et Kaspersky Lab.

Lisez-le attentivement et si vous n'avez aucune objection à formuler, cliquez sur le bouton **J'accepte**. L'installation de l'application sur votre ordinateur se poursuivra.

Pour arrêter l'installation, cliquez sur le bouton **Annuler**.

ETAPE 5. REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Cette étape vous offre la possibilité de participer au programme Kaspersky Security Network. La participation dans le programme prévoit l'envoi de l'information sur les nouvelles menaces, découvertes sur votre ordinateur, envoi de l'identificateur unique, attribué à votre ordinateur par Kaspersky Internet Security, et de l'information sur le système à Kaspersky Lab. Vous recevrez la garantie que des données personnelles ne seront pas transmises.

Lisez attentivement le règlement d'utilisation de Kaspersky Security Network. Si vous n'avez aucune objection à formuler, cochez la case **J'accepte les conditions de participation à Kaspersky Security Network**.

Cliquez sur **Suivant**. L'installation se poursuit.

ETAPE 6. SELECTION DU REPERTOIRE D'INSTALLATION

Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Etape 3. Sélection du type d'installation" à la page 24).

Vous devez désigner le répertoire dans lequel l'application sera installée. Le chemin proposé par défaut est le suivant :

- **<Disque> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2010** : pour les systèmes 32 bits.
- **<Disque> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2010** : pour les systèmes 64 bits.

Vous pouvez choisir un autre dossier à l'aide du bouton **Parcourir** qui ouvre la fenêtre standard de sélection de dossier ou saisir le chemin d'accès dans le champ prévu à cet effet.

N'oubliez pas que si vous saisissez manuellement le chemin d'accès complet au dossier d'installation, le nom ne pourra pas compter plus de 200 caractères ni contenir des caractères spéciaux.

Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 7. SELECTION DES COMPOSANTS DE L'APPLICATION A INSTALLER

Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Etape 3. Sélection du type d'installation" à la page 24).

En cas d'installation personnalisée, vous devez désigner les composants de l'application que vous souhaitez installer. Tous les composants de Kaspersky Internet Security sont sélectionnés par défaut pour l'installation : les composants de protection, les tâches d'analyse et les mises à jour.

Les brèves informations fournies pour chaque composant vous aideront à choisir les composants que vous ne souhaitez pas installer. Il suffit de sélectionner le composant dans la liste et de lire les informations qui apparaissent dans le champ inférieur. Il s'agit d'une brève description de la fonction du composant et de l'espace requis sur le disque.

Si vous décidez de ne pas installer un composant quelconque, ouvrez le menu contextuel en cliquant sur l'icône située à côté du nom du composant puis sélectionnez le point **Le composant sera inaccessible**. N'oubliez pas qu'en annulant l'installation d'un composant quelconque, vous vous privez de la protection contre toute une série de programmes dangereux.

Afin de sélectionner le composant à installer, ouvrez le menu contextuel en cliquant sur l'icône située à côté du nom du composant et sélectionnez le point **Le composant sera installé sur un disque dur local**.

Une fois que la sélection des composants est terminée, cliquez sur le bouton **Suivant**. Pour revenir à la liste des composants à installer par défaut, cliquez sur le bouton **Abandon**.

ETAPE 8. DESACTIVATION DU PARE-FEU DE MICROSOFT WINDOWS

Cette étape a lieu uniquement si Kaspersky Internet Security est installé sur un ordinateur avec un pare-feu Microsoft Windows actif et que le composant Pare-feu figure parmi les composants à installer.

Lors de cette étape de l'installation de Kaspersky Internet Security vous êtes invité à désactiver le pare-feu du système d'exploitation Microsoft Windows car le composant Pare-feu de Kaspersky Internet Security offre une protection complète pendant votre utilisation du réseau, si bien que vous pouvez vous passer de la protection complémentaire offerte par les outils du système d'exploitation.

Si vous souhaitez utiliser Pare-feu en guise de moyen principal de protection pendant l'utilisation du réseau, cliquez sur **Suivant**. Le pare-feu de Microsoft Windows sera désactivé automatiquement.

Si vous souhaitez protéger votre ordinateur à l'aide du pare-feu de Microsoft Windows, sélectionnez l'option **Utiliser le pare-feu de Microsoft Windows**. Dans ce cas, Pare-feu de Kaspersky Internet Security sera installé mais il sera désactivé afin d'éviter les conflits pendant l'utilisation de l'application.

ETAPE 9. UTILISATION DES PARAMETRES DE L'APPLICATION CONSERVES DE L'INSTALLATION ANTERIEURE

Cette étape vous permet de décider si vous souhaitez utiliser les paramètres de protection, les bases de l'application ainsi que les bases d'Anti-Spam, si elles ont été préservées sur votre ordinateur, lors de la suppression de la version antérieure de Kaspersky Internet Security.

Examinons en détail la manière d'utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Internet Security était installée sur l'ordinateur et que lors de sa suppression, vous avez conservé les bases de l'application, vous pouvez les activer en vue d'une utilisation avec la nouvelle version installée. Pour ce faire, cochez la case **Bases de l'application**. Les bases reprises dans la distribution de l'application ne seront pas copiées sur l'ordinateur.

Pour utiliser les paramètres de protection configurés dans la version antérieure et préservés sur l'ordinateur, cochez la case **Paramètres de fonctionnement de l'application**.

Il est également conseillé d'utiliser les bases d'Anti-Spam, si celles-ci ont été préservées lors de la suppression de la version antérieure de l'application. Ainsi, vous n'aurez pas besoin de réaliser à nouveau l'apprentissage d'Anti-Spam. Afin de tenir compte de la base que vous avez déjà composée, cochez la case **Base d'Anti-Spam**.

ETAPE 10. RECHERCHE D'AUTRES LOGICIELS ANTIVIRUS

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation simultanée avec cette application pourrait entraîner des conflits.

Si de tels programmes existent sur l'ordinateur, une liste reprenant leur nom s'affichera. Vous serez invité à les supprimer avant de poursuivre l'installation.

Sous la liste des logiciels antivirus découverts, vous pouvez choisir une des options de suppression : automatiquement ou manuellement.

Si une application de Kaspersky Lab version 2009 figure dans la liste, il est conseillé de conserver le fichier de licence utilisé par cette application avant de la supprimer manuellement. Vous pourrez l'appliquer à la nouvelle version de l'application. Il est également conseillé de conserver les objets de la quarantaine et de la sauvegarde. Ils seront placés automatiquement dans la quarantaine de la nouvelle version de Kaspersky Internet Security et vous pourrez continuer à les manipuler.

En cas de suppression automatique d'une application de la version 2009, les informations relatives à l'activation seront conservées par le programme et réutilisées lors de l'installation de la version 2010.

Pour poursuivre l'installation, cliquez sur **Suivant**.

ETAPE 11. DERNIERS PREPARATIFS POUR L'INSTALLATION DE L'APPLICATION

Lors de cette étape, vous êtes invité à réaliser les derniers préparatifs pour l'installation de l'application.

En cas d'installation initiale et personnalisée (cf. section "Etape 3. Sélection du type d'installation" à la page 24) de l'application, il est déconseillé de désélectionner la case **Protéger l'installation de l'application**. Si, lors de l'installation les erreurs surviennent, la protection activée permet de remettre correctement l'installation à l'état antérieur. En cas de nouvelle tentative d'installation, il est conseillé de désélectionner cette case.

En cas d'installation à distance via *Windows Bureau distant*, il est conseillé de désélectionner la case **Protéger l'installation de l'application**. Si cette case est cochée, l'installation peut ne pas être réalisée ou être réalisée de manière incorrecte.

Pour poursuivre l'installation, cliquez sur **Installer**.

Durant l'installation des composants de Kaspersky Internet Security qui interceptent le trafic de réseau, les connexions de réseau ouvertes sont interrompues. La majorité des connexions interrompues seront rétablies après un certain temps.

ETAPE 12. FIN DE LA PROCEDURE D'INSTALLATION

La fenêtre Fin de l'installation **Fin de l'installation** contient des informations sur la fin du processus d'installation de l'application.

Pas suivant – c'est la configuration de l'application pour assurer la protection maximale de votre information sur l'ordinateur. L'Assistant de configuration (cf. section "Assistant de configuration de l'application" à la page 29) aidera à configurer Kaspersky Internet Security rapidement et correctement.

Cliquez sur le bouton **Suivant** pour passer à la configuration de l'application.

PREMIERE UTILISATION

Une des principales tâches des experts de Kaspersky Lab dans le cadre du développement de Kaspersky Internet Security fut de veiller à la configuration optimale de tous les paramètres du logiciel. Ainsi, tout utilisateur, quelles que soient ses connaissances en informatique, peut assurer la protection de son ordinateur dès l'installation du logiciel sans devoir s'encombrer de la configuration.

Afin de rendre l'utilisation plus conviviale, nous avons tenté de regrouper les étapes de configuration préliminaire au sein d'une interface unique : l'Assistant de configuration de l'application (cf. section "Assistant de configuration de l'application" à la page 29) qui démarre à la fin de la procédure d'installation de l'application. Grâce aux instructions de l'Assistant, vous pourrez activer Kaspersky Internet Security, configurer les paramètres de la mise à jour, limiter l'accès au programme à l'aide d'un mot de passe et configurer d'autres paramètres.

Votre ordinateur peut être infecté par des programmes malveillants avant l'installation de l'application. Afin de découvrir les programmes malveillants présents, lancez l'analyse de l'ordinateur.

Les valeurs des paramètres de votre ordinateur peuvent être corrompues suite à l'action de programmes malveillants ou aux échecs du système. Lancez la tâche de recherche de vulnérabilités (cf. section "Recherche de vulnérabilités sur l'ordinateur" à la page 34) afin de trouver des vulnérabilités dans les logiciels installés ou des anomalies dans les configurations du système.

Les bases livrées avec l'application peuvent être dépassées au moment de l'installation de celle-ci. Lancez la mise à jour de l'application (au cas où cela n'aurait pas été réalisé à l'aide de l'Assistant de configuration ou automatiquement après l'installation de l'application).

Le composant Anti-Spam, qui fait partie de l'application, identifie les messages non sollicités à l'aide d'un algorithme d'auto-apprentissage. Lancez l'Assistant d'apprentissage d'Anti-Spam (cf. section "Entraînement à l'aide de l'Assistant d'apprentissage" à la page 106), afin de configurer le composant pour votre correspondance.

Une fois que les actions ci-dessus auront été réalisées, Kaspersky Internet Security sera prêt à fonctionner. Pour évaluer le niveau de protection de votre ordinateur, utilisez l'Assistant d'administration de la sécurité (cf. la section "Administration de la sécurité" à la page 37).

DANS CETTE SECTION

ASSISTANT DE CONFIGURATION DE L'APPLICATION

L'Assistant de configuration de l'application démarre pendant l'installation. Son rôle est de vous aider à réaliser la configuration initiale du logiciel sur la base des particularités et des tâches de votre ordinateur.

L'interface de l'Assistant de configuration se présente sous la forme d'une succession de fenêtres (étapes) et la navigation entre celles-ci s'opère à l'aide des liens **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur le lien **Annuler**.

VOICI, EN DETAILS, LES ETAPES DE L'ASSISTANT :

ETAPE 1. ACTIVATION DE L'APPLICATION

La procédure d'activation de l'application consiste en l'enregistrement de la licence à l'aide de l''installation du fichier clé. Sur la base de la licence l'application déterminera l'existence des droits d'utilisation et de leur durée.

La licence contient les informations de service indispensables pour assurer le parfait fonctionnement de Kaspersky Internet Security, ainsi que des renseignements complémentaires :

- les informations sur l'assistance technique (qui l'assure et comment l'obtenir) ;
- le nom et le numéro du fichier clé ainsi que sa date d'expiration.

Une connexion à Internet est indispensable pour activer l'application.

Afin de recevoir le fichier de licence pendant l'activation, il faut posséder le code d'activation. Le code d'activation est fourni à l'achat de l'application. Vous avez les options d'activation de Kaspersky Internet Security suivantes :

- **Activer la version commerciale**. Sélectionnez cette option si vous avez acheté une version commerciale du logiciel et que vous avez reçu le code d'activation. Vous recevrez, sur la base de ce code, le fichier de licence qui vous donnera accès à l'ensemble des fonctions de l'application pendant toute la durée de validité de la licence.
- **Activer la version d'évaluation**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. Vous recevrez un fichier de licence gratuite dont la durée de validité sera limitée par la licence associée à la version d'évaluation de l'application.
- **Activer plus tard**. Si vous choisissez cette option, l'activation de Kaspersky Internet Security sera ignorée. Le programme sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser Kaspersky Internet Security une seule fois après l'installation). L'option

Activer plus tard est accessible uniquement au premier lancement de l'Assistant d'activation, juste après l'installation de l'application.

Si Kaspersky Internet Security avait été installé puis supprimé sans perdre les données relatives à l'activation, alors cette étape n'est pas présentée. Dans ce cas, l'Assistant de configuration récupère automatiquement les informations relatives à la licence et les affiche dans la fenêtre de l'Assistant (cf. page 31).

VOIR EGALEMENT

ACTIVATION DE LA VERSION COMMERCIALE

Si vous choisissez cette option, l'activation du programme s'opère via le serveur Web de Kaspersky Lab. Une connexion à Internet est nécessaire dans ce cas.

L'activation repose sur la saisie du code d'activation que vous recevez par courrier électronique après avoir acheté Kaspersky Internet Security dans un magasin en ligne. Dans le cas d'achat de l'application en boîte, le code d'activation est indiqué sur le côté interne du clapet de l'enveloppe avec le disque ou sous le film protecteur de l'étiquette sur le côté interne de la boîte DVD.

Le code d'activation se présente sous la forme d'une série de chiffres et de lettres séparés par des traits d'union en 4 groupes de cinq chiffres, sans espace : par exemple, 11111-11111-11111-11111. N'oubliez pas que le code doit être saisi en caractères romains.

L'Assistant d'activation établit une connexion avec le serveur d'activation de Kaspersky Lab sur Internet et les envoie votre code d'activation, ensuite le code est analysé. Si le code d'activation est valide, l'assistant télécharge le fichier de licence qui s'installe alors automatiquement. L'activation est terminée et une fenêtre s'affiche avec les informations détaillées sur la licence acquise.

En cas d'activation de l'abonnement, outre les informations citées ci-dessus, les données relatives à l'état de l'abonnement (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page 35) seront également disponibles.

Si le code d'activation n'est pas reconnu, un message vous le signalera. Dans ce cas, contactez la société où vous avez acheté Kaspersky Internet Security pour obtenir des informations.

Si le nombre d'activations autorisé pour le code a été dépassé, un message s'affiche à l'écran. Le processus d'activation est alors interrompu et l'application vous redirige vers l'assistance technique de Kaspersky Lab.

Si une erreur s'est produite au moment de se connecter au serveur d'activation ou si vous n'avez pas pu récupérer le fichier de licence, contactez le service d'assistance technique.

ACTIVATION DE LA VERSION D'EVALUATION

Sélectionnez cette option si vous souhaitez installer une version d'évaluation de Kaspersky Internet Security avant de décider d'acheter la version commerciale. Vous recevrez un fichier de licence gratuit dont la durée de validité sera déterminée par le contrat de licence de la version d'évaluation de l'application. A l'expiration du délai de validité de la licence d'évaluation, la possibilité d'activation secondaire de la version d'évaluation sera inaccessible.

Si une erreur s'est produite au moment de se connecter au serveur d'activation ou si vous n'avez pas pu récupérer le fichier de licence, contactez le service d'assistance technique.

FIN DE L'ACTIVATION

L'Assistant d'activation vous signale la réussite de l'activation de Kaspersky Internet Security. Il propose également des informations sur la licence : type (commerciale, évaluation, etc.), fin de validité de la licence et nombre d'ordinateurs pouvant utiliser cette licence.

Dans le cas d'activation de l'abonnement, à la place de la date d'expiration de la licence, l'information sur le statut d'abonnement (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page 35) est affichée.

ETAPE 2. SELECTION DU MODE DE PROTECTION

Sélectionnez le mode de protection proposé par Kaspersky Internet Security.

Deux choix s'offrent à vous :

- *Automatique*. Lorsque des événements importants surviennent, Kaspersky Internet Security exécute automatiquement l'action recommandée par les experts de Kaspersky Lab. Lorsque l'application découvre une menace, il tente de réparer l'objet et si cela est impossible, il le supprime. Les objets suspects sont ignorés sans traitement. Des messages contextuels signalent les événements qui se produisent.

- *Interactif*. Dans ce mode, l'application réagit aux événements conformément à vos choix. Lorsqu'un événement qui requiert votre intervention se manifeste, l'application affiche des notifications (à la page 205) offrant un choix d'actions.

La notification sur la découverte d'une infection active est affichée quel que soit le mode de protection sélectionné.

ETAPE 3. CONFIGURATION DE LA MISE A JOUR DE L'APPLICATION

Cette étape de l'Assistant de configuration de l'application n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

La qualité de la protection de votre ordinateur dépend de l'actualité des bases et des modules du logiciel. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de mise à jour de logiciel et de la programmer :

- **Mise à jour automatique**. Kaspersky Internet Security vérifie selon la fréquence définie la présence de fichiers de mise à jour sur la source de la mise à jour. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si l'application découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur. Ce mode est utilisé par défaut.

- **Mise à jour programmée** (l'intervalle varie en fonction des paramètres de la programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. La programmation est configurée dans la fenêtre qui s'ouvre à l'aide du bouton **Configuration**.

- **Mise à jour manuelle**. Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules de l'application qui font partie de l'installation peuvent être dépassés au moment de l'installation de Kaspersky Internet Security. C'est la raison pour laquelle nous vous conseillons d'utiliser les mises à jour les plus récentes de Kaspersky Internet Security. Il suffit simplement de cliquer sur **Mettre à jour maintenant**. Dans ce cas, le programme recevra les mises à jour requises depuis les serveurs de mise à jour via Internet et les installera sur l'ordinateur.

Si les bases reprises dans la distribution sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Si vous souhaitez accéder aux paramètres de la mise à jour (cf. section "Mise à jour" à la page 150) (sélectionner la ressource d'où la mise à jour sera téléchargée, configurer le lancement de la mise à jour selon les privilèges d'un compte

utilisateur en particulier ou activer le service de copie des mises à jour sur une source locale), cliquez sur le bouton **Configuration**.

ETAPE 4. RESTRICTION DE L'ACCES A L'APPLICATION

Cette étape de l'Assistant de configuration de Kaspersky Internet Security n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

Dans la mesure où l'ordinateur peut être utilisé par plusieurs personnes dont les connaissances en informatique peuvent varier et étant donné que des programmes malveillants pourraient désactiver la protection, vous avez la possibilité de limiter l'accès à Kaspersky Internet Security à l'aide d'un mot de passe. Le mot de passe permet de protéger le programme contre les tentatives de désactivation non autorisée de la protection ou contre les modifications des paramètres de Kaspersky Internet Security.

Pour activer cette protection, cochez la case ☑ **Activer la protection par mot de passe** et remplissez les champs **Nouveau mot de passe** et **Confirmation du mot de passe**.

Indiquez ensuite l'ampleur de la restriction :

- ☑ **Configuration de l'application** : l'utilisateur est invité à saisir le mot de passe lorsqu'il tente de sauvegarder les modifications des paramètres de Kaspersky Internet Security.
- ☑ **Arrêt de l'application** : l'utilisateur doit saisir le mot de passe s'il souhaite arrêter le programme.

ETAPE 5. SELECTION DES MENACES IDENTIFIEES

Cette étape de l'Assistant de configuration de l'application n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

Cette étape vous permet de sélectionner les catégories de menace qui seront identifiées par Kaspersky Internet Security. Kaspersky Internet Security découvre toujours les programmes capables de nuire à votre ordinateur. Les virus, les vers et les chevaux de Troie appartiennent à cette catégorie d'applications.

ETAPE 6. DESACTIVATION DE LA MISE EN CACHE DES NOMS DE DOMAINE (DNS)

Cette étape de l'Assistant de configuration de l'application n'apparaît pas si vous avez choisi l'installation express. Les paramètres de l'application configurables à cette étape reçoivent les valeurs par défaut.

La mise en cache des noms de domaine réduit considérablement la durée de la connexion de l'ordinateur aux sites requis. Toutefois, il s'agit d'une vulnérabilité dangereuse que les individus malveillants pourraient exploiter afin d'obtenir l'accès à vos données.

Cochez la case ☑ **Désactiver la mise en cache du DNS** afin d'augmenter le niveau de protection de votre ordinateur.

Après la désactivation de la mise en cache du DNS, des problèmes peuvent se présenter dans le fonctionnement des applications qui utilisent des connexions multiples (par exemple, les clients de réseaux d'échange de fichiers).

Cette étape vous permet d'indiquer, s'il faut montrer les enregistrements sur les événements non critiques dans le rapport de protection. Pour ce faire, cochez la case ☑ **Consigner les événements non critiques**.

ETAPE 7. ANALYSE DU SYSTEME

Cette étape correspond à la collecte d'informations sur les applications reprises dans Microsoft Windows. Ces applications figurent dans la liste des applications de confiance et elles ne sont soumises à aucune restriction sur les actions qu'elles peuvent réaliser dans le système.

ETAPE 8. FIN DE L'ASSISTANT

La dernière fenêtre de l'Assistant vous signale la fin de l'installation du programme. Pour commencer à utiliser Kaspersky Internet Security, assurez-vous que la case ☑ **Lancer Kaspersky Internet Security** est cochée puis cliquez sur le bouton **Terminer**.

SELECTION DU TYPE DE RESEAU

Une fois l'application installée, le composant Pare-feu analyse les connexions de réseau actives sur votre ordinateur. Chaque connexion de réseau reçoit un état qui détermine l'activité de réseau autorisée.

Si vous avez choisi le mode interactif de fonctionnement (cf. section "Etape 2. Sélection du mode de protection" à la page 31) de Kaspersky Internet Security, une notification apparaît dès qu'une connexion de réseau est découverte. La fenêtre de la notification vous permet de sélectionner l'état du nouveau réseau :

- **Réseau public**. Les connexions de réseau dotées de cet état ne peuvent accéder à votre ordinateur depuis l'extérieur. L'accès aux dossiers partagés et aux imprimantes est interdit dans ce type de réseau. Cet état est recommandé pour le réseau Internet.

- **Réseau local**. Les connexions de réseau de cet état ont accès aux dossiers partagés et aux imprimantes de réseau. Cet état est conseillé pour un réseau local protégé tel que le réseau d'une entreprise.

- **Réseau de confiance**. Toutes les activités sont autorisées pour les connexions de cet état. Cet état doit être utilisé uniquement pour les zones qui ne présentent aucun danger.

Kaspersky Internet Security propose pour chaque état de réseau un ensemble de règles qui régissent l'activité de réseau. L'état de réseau attribué après la première découverte du réseau peut être modifié par la suite.

MISE A JOUR DE L'APPLICATION

La mise à jour de Kaspersky Internet Security nécessite une connexion Internet

Kaspersky Internet Security est livré avec des bases qui contiennent les signatures des menaces et des exemples d'expressions caractéristiques du courrier indésirable ainsi que des descriptions d'attaques de réseau. Toutefois, il se peut que les bases soient dépassées au moment d'installer Kaspersky Internet Security car Kaspersky Lab actualise régulièrement les bases et les modules de l'application.

L'Assistant de configuration de l'application vous permet de sélectionner le mode d'exécution des mises à jour (cf. section "Etape 3. Configuration de la mise à jour de l'application" à la page 31). Kaspersky Internet Security vérifie automatiquement la présence des mises à jour sur les serveurs de mises à jour de Kaspersky Lab. Si le serveur héberge les mises à jour les plus récentes, Kaspersky Internet Security les télécharge et les installe en arrière plan.

Si les bases reprises dans la distribution sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Pour maintenir la protection de votre ordinateur à jour, il est conseillé d'actualiser Kaspersky Internet Security directement après l'installation.

Pour procéder à la mise à jour manuelle de Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur **Lancer la Mise à jour**.

RECHERCHE DE VIRUS SUR L'ORDINATEUR

Les développeurs d'applications malveillantes déploient beaucoup d'efforts pour masquer leur activité et pour cette raison, il se peut que vous ne remarquiez pas la présence d'applications malveillantes sur votre ordinateur.

Au moment de l'installation, l'application exécute automatiquement la tâche **Analyse rapide** de l'ordinateur. Cette tâche est orientée sur la recherche et la neutralisation de programmes malveillants dans les objets chargés au démarrage du système d'exploitation.

Les experts de Kaspersky Lab conseillent également d'exécuter la tâche **Analyse complète** de l'ordinateur.

Pour lancer la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton **Lancer l'analyse complète** afin de commencer l'analyse.

RECHERCHE DE VULNERABILITES SUR L'ORDINATEUR

Les paramètres du système d'exploitation reçoivent souvent des valeurs inexactes suite à une activité non sollicitée qui peut résulter d'un échec du système et de l'activité de programmes malveillants. De plus, les applications installées peuvent abriter des vulnérabilités exploitées par les individus mal intentionnés pour nuire à votre ordinateur.

Pour identifier ces problèmes de sécurité et les résoudre, les experts de Kaspersky Lab recommandent de lancer *la tâche de Recherche de vulnérabilités* (cf. page 146) après l'installation de l'application. Cette tâche consiste à rechercher des vulnérabilités dans les applications ainsi que des anomalies ou des corruptions dans les paramètres du système d'exploitation et du navigateur.

Pour lancer la tâche de recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le bouton **Ouvrir la fenêtre de recherche de vulnérabilités**.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Lancer la recherche de vulnérabilités**.

ADMINISTRATION DE LA LICENCE

Kaspersky Internet Security fonctionne grâce à une clé. Le fichier de licence vous est attribué en vertu du code d'activation reçu à l'achat de l'application, et permet de l'utiliser à partir du jour d'activation. Le fichier de licence contient l'information sur la licence : type, durée de validité, nombres d'ordinateurs sur lesquels elle se propage.

Sans le fichier de licence, si la version d'évaluation de Kaspersky Internet Security n'a pas été activée, l'application fonctionnera en mode de mise à jour unique. Par la suite, les mises à jour disponibles sur le serveur ne seront pas téléchargées.

Si la version d'évaluation avait été activée, Kaspersky Internet Security ne fonctionnera plus une fois que la clé sera arrivée à échéance.

Une fois la clé commerciale expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettre à jour les bases. Vous pourrez toujours analyser l'ordinateur à l'aide de la recherche de virus et utiliser l'Antivirus Fichiers, mais uniquement sur la base des bases de l'application d'actualité à la fin de validité de la licence. Par conséquent, nous ne pouvons pas garantir une protection totale contre les nouveaux virus qui apparaîtraient après l'expiration de la licence.

Afin que l'ordinateur ne soit pas contaminé par de nouveaux virus, nous vous conseillons de prolonger la validité de la licence de Kaspersky Internet Security. L'application vous préviendra deux semaines avant l'expiration de la licence. Le message de circonstance apparaîtra à chaque exécution de l'application pendant un certain temps.

L'information sur la licence utilisée est présentée dans la fenêtre **Gestionnaire de licences** : type (commerciale, commerciale avec abonnement, commerciale avec abonnement pour la protection, évaluation), nombre maximum d'ordinateurs sur lesquels elle peut être installée, date d'expiration et nombre de jours restant avant cette date. Les informations relatives à la fin de la validité de la licence n'apparaissent pas pour les licences commerciales avec abonnement ou les licences commerciales avec abonnement pour la protection (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page 35).

Pour lire les termes du contrat de licence pour l'utilisation de l'application, cliquez sur le bouton **Lire le contrat de licence**. Pour supprimer le fichier de licence cliquez sur le bouton ✖ à droite de la licence, en regard du fichier de licence que vous voulez supprimer. Pour activer une nouvelle licence, utilisez le bouton **Activer la nouvelle licence**.

A l'aide des boutons **Acheter une licence** (**Renouveler la licence**) vous pouvez passer à l'achat (renouvellement) de la licence dans la boutique en ligne de Kaspersky Lab.

Kaspersky Lab organise à intervalles réguliers des actions qui permettent de renouveler la licence d'utilisation de ses logiciels en bénéficiant de remises considérables. Soyez à l'affût de ces actions sur le site de Kaspersky Lab dans la rubrique **Produits → Actions et offres spéciales**.

ABONNEMENT POUR LE RENOUVELLEMENT AUTOMATIQUE DE LA LICENCE

L'abonnement permet de renouveler automatiquement la durée de validité de la licence. L'activation de l'abonnement requiert un code d'activation délivré par la boutique en ligne lors de l'achat de Kaspersky Internet Security est requis.

Si au moment d'activer l'abonnement vous aviez déjà activé une licence avec une validité limitée, elle sera remplacée par une licence avec abonnement. Si vous ne souhaitez pas utiliser le service d'abonnement, vous devrez contacter le magasin en ligne où vous avez acheté Kaspersky Internet Security.

L'abonnement peut avoir un des états suivants :

- *Définition en cours*. La demande d'activation de l'abonnement n'a pas encore été traitée (le traitement des requêtes sur le serveur requiert un certain temps). Kaspersky Internet Security fonctionne en mode plein-fonctionnel. Si l'abonnement n'a pas été traité à la fin d'un délai déterminé, vous recevrez un message indiquant que l'actualisation de l'abonnement n'a pas été réalisée. Les bases de l'application ne seront plus actualisées (pour les licences avec abonnement) et l'ordinateur ne sera plus protégé (pour les licences avec abonnement pour la protection).

- *Activé*. L'abonnement a été activé pour une durée indéterminée ou non (la date de fin de validité est alors précisée).

- *Renouvelé*. L'abonnement a été renouvelé pour une durée indéterminée ou non.

- *Erreur*. Une erreur s'est produite lors de l'actualisation de l'état de l'abonnement.

- *Expiré. La période de grâce est en cours.* La durée de validité de l'abonnement ou le délai pour l'actualisation de l'abonnement est écoulé. Si le délai pour l'actualisation est écoulé, actualisez l'état de l'abonnement

manuellement. Si la durée de validité de l'abonnement est écoulée, vous pouvez le renouveler en contactant le magasin en ligne où vous avez acheté Kaspersky Internet Security. Avant de pouvoir utiliser un autre code d'activation, il faut d'abord supprimer le fichier de licence pour l'abonnement utilisé.

- *Expiré. La période de grâce est écoulée.* La durée de validité de l'abonnement ou la période de grâce pour le renouvellement de celui-ci est écoulée. Contactez le fournisseur de l'abonnement pour obtenir un nouvel abonnement ou renouveler l'abonnement actuel.

- *Refus d'abonnement*. Vous avez refusé d'utiliser l'abonnement pour le renouvellement automatique de la licence.

- *Actualisation requise*. L'état de l'abonnement n'a pas été actualisé à temps pour une raison quelconque. Cliquez sur le bouton **Renouveler l'état de l'abonnement** pour actualiser l'état de l'abonnement.

- *Suspendu*. L'abonnement pour le renouvellement automatique de la licence a été suspendu.

- *Renouvelé*. L'abonnement a été renouvelé.

Si la durée de validité de l'abonnement est écoulée ainsi que la période complémentaire durant laquelle le renouvellement est possible (état *Expiré*), Kaspersky Internet Security vous le signale et cesse de tenter d'obtenir la licence actualisée depuis le serveur. Dans le cas des licences avec abonnement, les fonctions de l'application sont préservées à l'exception de la mise à jour des bases de l'application. Dans le cas d'une licence avec abonnement pour la protection, les bases de l'application ne seront plus actualisées, l'ordinateur ne sera plus protégé et les analyses ne seront plus exécutées.

Si la licence n'a pas été renouvelée pour une raison quelconque (état *Actualisation requise*) à temps (par exemple, l'ordinateur n'était pas allumé pendant la période où le renouvellement de la licence était possible), vous pouvez actualiser son état manuellement. Avant le renouvellement de l'abonnement, Kaspersky Internet Security n'actualise plus les bases de l'application (pour les licences avec abonnement) et cesse de protéger l'ordinateur et de lancer l'analyse (pour les licences commerciales avec abonnement pour la protection).

En cas d'utilisation de l'abonnement, vous ne pouvez pas utiliser un autre code d'activation pour prolonger la durée de validité de la licence. Ceci sera possible uniquement à l'échéance de l'abonnement (état *A expiré*). Pour renouveler la durée de validité de l'application, vous bénéficierez d'une période de remise au cours de laquelle les fonctions de l'application seront préservées.

N'oubliez pas que si vous devez réinstaller l'application et que vous utilisez l'abonnement, vous devrez actualiser à nouveau le logiciel manuellement à l'aide du code d'activation reçu à l'achat de l'application.

La liste des actions possibles avec l'abonnement varie en fonction du fournisseur. Il est possible également qu'aucune période de grâce ne soit accordée pour le renouvellement de l'abonnement.

PARTICIPATION AU KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaissent. Pour accélérer la collecte de statistiques sur le type de nouvelles menaces, sur leur source et sur les moyens de les neutraliser, Kaspersky Lab vous propose de participer au Kaspersky Security Network.

L'utilisation de Kaspersky Security Network permet d'envoyer les informations suivantes à Kaspersky Lab :

- L'identificateur unique attribué à votre ordinateur par Kaspersky Internet Security. Cet identificateur définit les paramètres matériels de l'ordinateur et ne contient aucune information personnelle.

- Les informations relatives aux menaces découvertes par les composants du programme. Le contenu de ces informations dépend du type de menace identifiée.

- Informations relatives au système : version du système d'exploitation, mises à jour installées, services et pilotes téléchargés, version des navigateurs et des clients de messagerie, modules externes des navigateurs, numéro de la version de l'application de Kaspersky Lab installée.

Kaspersky Security Network collecte également des statistiques très diverses qui contiennent, entre autres, les informations sur les éléments suivants :

- les fichiers exécutables et les applications signées téléchargées sur l'ordinateur ;
- les applications exécutées sur l'ordinateur.

L'envoi des informations statistiques se produit à la fin de la mise à jour de l'application.

Kaspersky Lab garantit qu'aucune donnée personnelle n'est recueillie ni envoyée dans le cadre de Kaspersky Security Network.

Pour configurer les paramètres de l'envoi de statistiques, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Retour d'informations**.
3. Cochez la case ☑ **J'accepte de rejoindre le Kaspersky Security Network** pour confirmer votre participation au Kaspersky Security Network.

ADMINISTRATION DE LA SECURITE

La présence d'un problème dans la protection de l'ordinateur est signalée par l'état de la protection de l'ordinateur (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) : l'icône de l'état de la protection et du panneau sur lequel elle se trouve change de couleur. Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se manifestent.

Illustration 1: Etat actuel de la protection de l'ordinateur

Vous pouvez consulter la liste des problèmes, leur description et les solutions éventuelles sous l'onglet **Etat** (cf. ill. ci-dessous), dont la sélection s'opère via l'icône de l'état, ou via le panneau où il se trouve (cf. ill. ci-dessus).

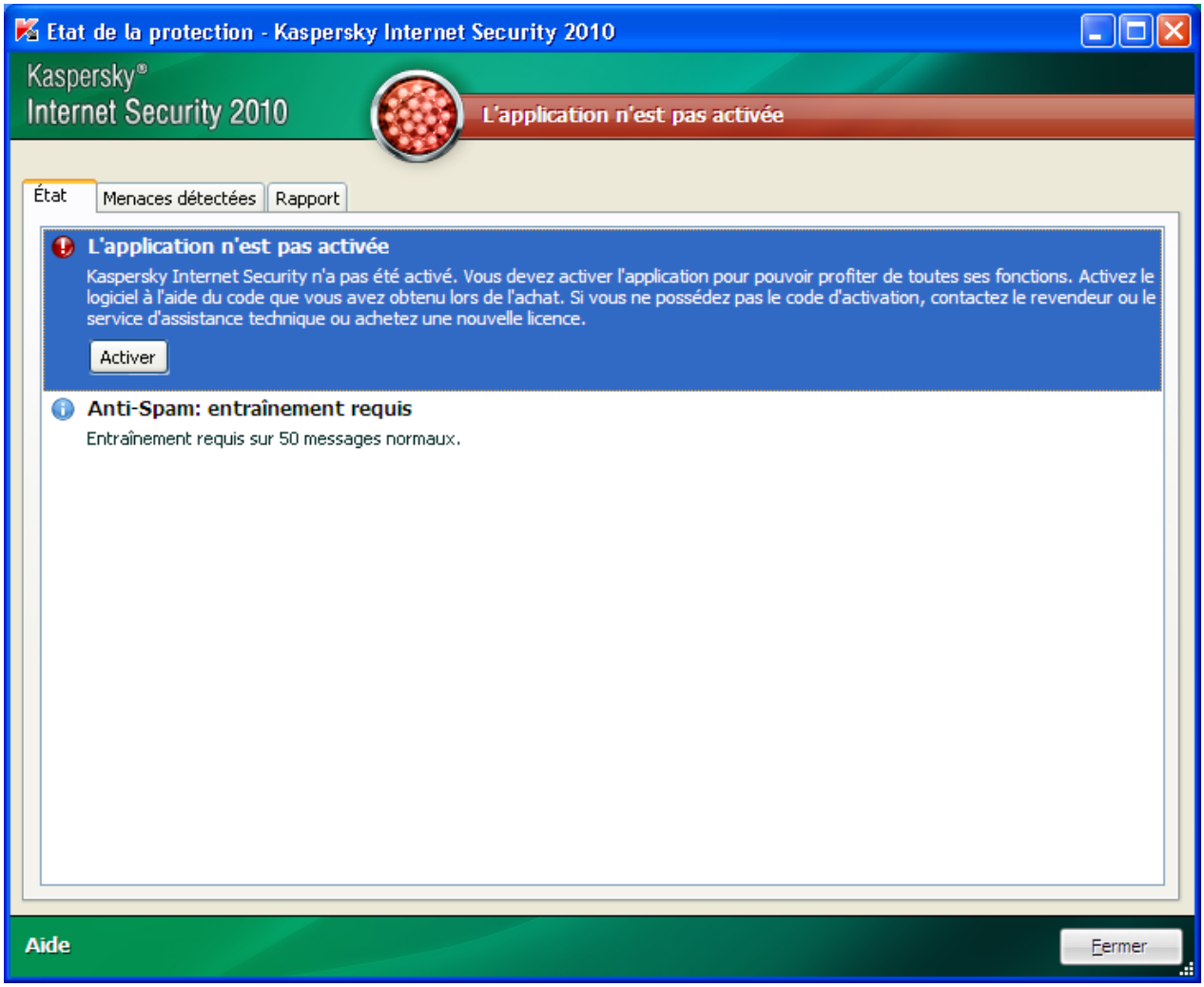


Illustration 2 : Résolution des problèmes de sécurité

Vous pouvez consulter la liste des problèmes rencontrés. Les problèmes sont classés par ordre de gravité : viennent d'abord les problèmes les plus graves, à savoir ceux dont l'état est marqué par une icône rouge ; ensuite viennent les problèmes moins importants (icône d'état jaune) et en dernier lieu, nous avons les messages informatifs. Chaque problème est accompagné d'une description et les actions suivantes sont proposées :

- *Résolution immédiate*. Grâce aux boutons correspondants, vous pouvez passer à la suppression directe du problème, ce qui est l'action recommandée.

- *Reporter la suppression*. Si pour une raison quelconque il est impossible de résoudre les problèmes sur le champ, on peut reporter l'action et y revenir plus tard. Pour ce faire, cliquez sur le bouton **Ignorer le message**.

  Sachez toutefois que cette possibilité n'est pas reprise pour les problèmes graves. Il s'agit par exemple de la présence d'objets malveillants non neutralisés, de l'échec d'un ou de plusieurs composants ou de la corruption de fichiers de l'application.

Pour que des messages dissimulés soient à nouveau visibles dans la liste générale, cochez la case **Afficher les messages dissimulés**.

VOIR EGALEMENT

Etat de la protection.....39

ETAT DE LA PROTECTION

Le travail des composants de Kaspersky Internet Security ou des tâches d'analyse est consigné dans un rapport contenant des informations de synthèse sur l'état de la protection de l'ordinateur. Vous pouvez voir ici le nombre d'objets dangereux ou suspects découverts pendant l'utilisation de l'application ainsi que le nombre d'objets réparés, supprimés ou placés en quarantaine.

La découverte d'objets malveillants est indiquée par l'état de la protection de l'ordinateur (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) via un changement de couleur de l'icône et du panneau sur lequel elle apparaît. En cas de découverte d'objet malveillant, l'icône et le panneau deviennent rouge. Dans ce cas, il faut supprimer immédiatement toutes les menaces.

- *Pour connaître l'état de la protection de l'ordinateur, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapport**.

- *Pour supprimer les problèmes de la protection de l'ordinateur, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapport**.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Etat**, exécutez les actions requises. Pour que des messages dissimulés soient à nouveau visibles dans la liste générale, cochez la case **Afficher les messages ignorés**.

- *Pour exécuter une action sur l'objet trouvé, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapport**.
  3. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées**, sélectionnez l'objet souhaité et ouvrez le menu contextuel avec le bouton droit de la souris dans la liste des objets.
  4. Dans le menu contextuel qui s'ouvre, sélectionnez l'action requise.

- *Pour voir le rapport sur le fonctionnement des composants de la protection, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Cliquez sur le lien **Rapport**.
  3. Dans la fenêtre qui s'ouvre sélectionnez l'onglet **Rapport**.

VOIR EGALEMENT

Administration de la sécurité 37

SUSPENSION DE LA PROTECTION

La suspension de la protection signifie la désactivation de tous ses composants pour un certain temps.

Cette action suspend le fonctionnement de tous les composants de la protection en temps. Les éléments suivants permettent de confirmer la désactivation :

- l'icône de l'application (cf. section "Icône dans la zone de notification" à la page 41) dans la zone de notification de la barre des tâches est en grise ;
- la couleur rouge de l'icône d'état et du panneau de la fenêtre principale de Kaspersky Internet Security.

Si des connexions de réseau étaient ouvertes au moment de la suspension de l'application, un message sur l'interruption de ces connexions sera affiché.

Pour suspendre la protection de l'ordinateur, procédez comme suit :

1. Dans le menu contextuel (cf. section "Menu contextuel" à la page 42) de l'application sélectionnez **Suspension de la protection**.
2. Dans la fenêtre **Suspension de la protection** qui s'ouvre, sélectionnez la durée à l'issue de laquelle la protection sera à nouveau activée :
   - **Suspendre pendant <intervalle> :** la protection sera restaurée à l'issue de l'intervalle désigné. Pour sélectionner la valeur, utilisez la liste déroulante.
   - **Suspendre jusqu'au redémarrage –** la protection sera activée après le redémarrage de l'application ou du système (pour autant que le mode de lancement de Kaspersky Internet Security au démarrage de l'ordinateur ait été activé).
   - **Suspendre** : la protection sera réactivée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Lancement de la protection** dans le menu contextuel de l'application.

INTERFACE DE L'APPLICATION

L'interface de Kaspersky Internet Security est simple et conviviale. Ce chapitre aborde en détail les principaux éléments de l'interface.

Kaspersky Internet Security possède des modules externes pour Microsoft Office Outlook (recherche de virus et recherche de courrier indésirable), Microsoft Outlook Express (recherche de courrier indésirable), The Bat! (recherche de virus et recherche de courrier indésirable), Thunderbird (recherche de courrier indésirable), Microsoft Internet Explorer, Microsoft Windows Explorer. Les modules externes élargissent les possibilités des programmes cités et permettent de configurer, depuis leur interface, les paramètres des composants **Antivirus Courrier** et **Anti-Spam** et de les administrer.

DANS CETTE SECTION

ICONE DANS LA ZONE DE NOTIFICATION

L'icône de l'application apparaît dans la zone de notification de la barre des tâches de Microsoft Windows directement après son installation.

L'icône indique le fonctionnement de l'application. Elle représente l'état de la protection et montre également plusieurs actions fondamentales exécutées par l'application.

Si l'icône est active  (en couleur), cela signifie que la protection est complètement activée ou que certains de ses composants fonctionnent. Si l'icône est inactive  (noir et blanc), cela signifie que tous les composants de la protection sont désactivés.

L'icône de l'application varie en fonction de l'opération exécutée :

-  – analyse d'un message électronique en cours ;
-  – analyse du trafic web ;
-  – mise à jour des bases et des modules de l'application en cours ;
-  – redémarrage de l'ordinateur requis pour appliquer les mises à jour ;
-  – échec du fonctionnement d'un composant quelconque de l'application.

L'icône permet également d'accéder aux éléments fondamentaux de l'interface de l'application que sont le menu contextuel (cf. section "Menu contextuel" à la page 42) et la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43).

Pour ouvrir le menu contextuel, cliquez avec le bouton droit de la souris sur l'icône de l'application.

Pour ouvrir la fenêtre principale de Kaspersky Internet Security, cliquez avec le bouton gauche de la souris sur l'icône de l'application.

L'icône  apparaît dans la barre des tâches de Microsoft Windows lorsque des infos sont émises par Kaspersky Lab. Cliquez deux fois sur l'icône pour prendre connaissance du texte des informations.

MENU CONTEXTUEL

Le menu contextuel permet d'exécuter toutes les tâches principales liées à la protection.

Le menu de l'application contient les points suivants :

- **Mise à jour** : lance la mise à jour des bases et des modules de l'application et l'installe sur l'ordinateur.
- **Analyse complète** : lance l'analyse complète de l'ordinateur afin d'identifier la présence éventuelle d'objets malveillants. Les objets de tous les disques, y compris sur les disques amovibles, seront analysés.
- **Recherche de virus** : passe à la sélection d'objets et au lancement de la recherche de virus. La liste contient par défaut une multitude d'objets tels que le répertoire **Mes documents** et les boîtes aux lettres. Vous pouvez enrichir la liste, sélectionner des objets à analyser et lancer la recherche de virus.
- **Surveillance du réseau** : affiche la liste des connexions de réseau établies (cf. section "Surveillance du réseau" à la page 197), des ports ouverts et du trafic.
- **Clavier virtuel** : accès au clavier virtuel.
- **Kaspersky Internet Security** : ouvre la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43).
- **Configuration** : permet d'afficher et de configurer les paramètres de fonctionnement de l'application.
- **Activation** : passe à l'activation de Kaspersky Internet Security. Pour bénéficier des privilèges accordés aux utilisateurs enregistrés, vous devez impérativement activer votre copie de l'application. Ce point du menu est visible uniquement si l'application n'a pas été activée.
- **A propos du programme** : ouvre une boîte de dialogue contenant des informations sur l'application.
- **Suspension de la protection / Lancement de la protection** : suspension temporaire / activation des composants de la protection en temps réel. Ce point du menu n'a aucune influence sur la mise à jour de l'application, ni sur l'exécution de la recherche de virus.
- **Bloquer le trafic de réseau / Débloquer le trafic de réseau** : blocage temporaire / déblocage de toutes les connexions de réseau de l'ordinateur.
- **Contrôle Parental** : permutation rapide des profils actifs du composant (cf. section "Contrôle Parental" à la page 126). Ce point du menu est présent uniquement si le contrôle parental est lancé et que l'utilisation des profils est utilisée.

- **Terminer** : arrêt du fonctionnement de Kaspersky Internet Security (si vous choisissez cette option, l'application sera déchargée de la mémoire vive de l'ordinateur).

Illustration 3: Menu contextuel

Si une tâche quelconque de recherche de virus est lancée quand vous ouvrez le menu contextuel, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez passer à la fenêtre principale avec le rapport contenant les résultats détaillés de l'exécution.

FENETRE PRINCIPALE DE KASPERSKY INTERNET SECURITY

La fenêtre principale de l'application est scindée en trois parties :

- La partie supérieure reprend une évaluation globale de l'état de la protection de votre ordinateur.

Illustration 4: Etat actuel de la protection de l'ordinateur

Il existe trois états possibles pour la protection. Chacun d'entre eux est associé à une couleur particulière, comme pour les feux signalisation. Le vert indique que la protection de l'ordinateur est assurée au niveau requis. Le jaune et le rouge signalent la présence de menaces de divers types pour la sécurité. Les menaces sont non seulement les applications malveillantes, mais également les bases de l'application dépassée, certains composants désactivés, les paramètres minimes de fonctionnement de l'application, etc.

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent. Pour en obtenir des informations détaillées et de les supprimer rapidement, passez à l'Assistant d'administration de la sécurité, cliquez sur l'icône de l'état ou du panneau sur lequel elle est située (cf. ill. ci-dessus).

- La partie gauche de la fenêtre permet d'accéder rapidement à n'importe quelle fonction de l'application, au lancement de la recherche de virus ou de la mise à jour, etc.

Illustration 5: Partie gauche de la fenêtre principale

- La partie droite de la fenêtre contient des informations relatives à la fonction de l'application choisie dans la partie gauche. Vous pouvez configurer les paramètres de la fonction, utiliser des outils pour exécuter les recherches de virus et la récupération des mises à jour, etc.

Illustration 6: Partie droite de la fenêtre principale

Vous pouvez également cliquer sur les boutons et les liens suivants :

- **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application.
- **Menaces en quarantaine** : passe à la manipulation des objets placés en quarantaine.
- **Rapport** : passe à la liste des événements survenus pendant le fonctionnement de l'application.
- **Aide** : ouvre l'aide de Kaspersky Internet Security.
- **Mon Espace Personnel** : ouvre l'espace personnel de l'utilisateur (https://my.kaspersky.com/fr) sur le site du service d'assistance technique.
- **Assistance technique** : ouvre la fenêtre contenant les informations relatives au système et les liens vers les sources d'informations de Kaspersky Lab (site du service d'assistance technique, forum).
- **Licence** : passe à l'activation de Kaspersky Internet Security et au renouvellement de la licence.

Vous pouvez également modifier l'apparence de l'application en créant et en utilisant des éléments graphiques particuliers et la palette de couleurs.

NOTIFICATIONS

Lorsqu'un événement survient durant l'utilisation de Kaspersky Internet Security, des notifications apparaissent à l'écran sous la forme de messages contextuels au-dessus de l'icône de l'application dans la barre des tâches de Microsoft Windows.

En fonction du degré d'importance de l'événement (au niveau de la sécurité de l'ordinateur), les notifications peuvent être de divers type :

- **Alertes**. Un événement critique est survenu, par exemple : découverte d'un virus ou d'une activité dangereuse dans le système. Il faut immédiatement décider de la suite des événements. Les notifications de ce type apparaissent en rouge.

- **Attention**. Un événement qui présente un risque potentiel s'est produit, par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système. Vous devez décider du danger que représente cet événement. Les notifications de ce type apparaissent en jaune.

- **Informations**. Ce message vous signale un événement qui n'est pas critique. Il s'agit par exemple des messages affichés pendant le fonctionnement du composant Filtrage du contenu. Les messages d'informations sont en vert.

VOIR EGALEMENT

Notifications.....205

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de Kaspersky Internet Security peut être ouverte de la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) ou du menu contextuel (cf. section "Menu contextuel" à la page 42). Pour ce faire, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre ou choisissez l'option du même nom dans le menu contextuel de l'application.

La fenêtre de configuration contient deux parties :

- la partie gauche permet d'accéder aux fonctions de Kaspersky Internet Security, aux tâches de recherche de virus, à la mise à jour, etc. ;

- la partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionnés dans la partie gauche.

VOIR EGALEMENT

Configuration des paramètres de l'application.....156

PROTECTION DU SYSTEME DE FICHIERS DE L'ORDINATEUR

L'*Antivirus Fichiers* permet d'éviter l'infection du système de fichiers de l'ordinateur. Ce composant est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, l'Antivirus Fichiers analyse uniquement les nouveaux fichiers et les fichiers modifiés. L'analyse des fichiers se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Quand l'Antivirus Fichiers découvre une menace, il exécute l'action définie.

Le niveau de protection des fichiers et de la mémoire est défini par les groupes de paramètres suivants qui :

- définissent la zone protégée ;
- définissent la méthode d'analyse utilisée ;
- définissent l'analyse des fichiers composés (y compris les fichiers composés de grande taille) ;
- définissent le mode d'analyse ;
- permettent de suspendre le fonctionnement du composant selon la programmation ou pendant l'utilisation d'applications définies.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Fichiers. Dans la majorité des cas, la modification du niveau de protection suffit. Vous pouvez restaurer les paramètres de fonctionnement par défaut de l'Antivirus Fichiers. Pour ce faire, sélectionnez un des niveaux de protection.

➡ *Afin de modifier les paramètres de fonctionnement de l'Antivirus Fichiers, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

L'*Antivirus Fichiers* est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

Par défaut, l'Antivirus Fichiers analyse uniquement les nouveaux fichiers ou les fichiers modifiés, c.-à-d. les fichiers qui ont été ajoutés, ou modifiés depuis la dernière fois qu'ils ont été sollicités. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Le composant intercepte les requêtes de l'utilisateur ou d'un programme quelconque adressé à chaque fichier.

2. L'Antivirus Fichiers recherche des informations sur le fichier intercepté dans les bases iChecker et iSwift et sur la base des informations obtenues, il décide s'il faut analyser ou non le fichier.

Les actions suivantes sont réalisées durant l'analyse :

3. Le fichier est soumis à la recherche d'éventuels virus. L'identification des objets malveillants s'opère à l'aide des bases de Kaspersky Internet Security. Les bases contiennent la définition de tous les programmes malveillants, menaces et attaques de réseau connus à ce jour et leur mode de neutralisation.

4. Selon les résultats de l'analyse, Kaspersky Internet Security peut adopter les comportements suivants :

   a. Si le fichier contient un code malveillant, l'Antivirus Fichiers le bloque, place une copie dans le dossier de sauvegarde et tente de le réparer. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier est supprimé.

   b. Si le fichier contient un code semblable à un code malveillant et que ce verdict ne peut pas être garanti à 100%, le fichier est réparé et placé dans un répertoire spécial : la quarantaine.

   c. Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

Quand l'application découvre un objet infecté ou potentiellement infecté, elle vous le signale. Suite à la découverte d'un objet infecté ou potentiellement infecté, un message interrogeant l'utilisateur sur la suite des opérations s'affichera. Vous aurez le choix entre les options suivantes :

- placer la menace en quarantaine en vue d'une analyse et d'un traitement ultérieur à l'aide de bases actualisées ;
- supprimer l'objet ;
- ignorer l'objet si vous êtes absolument convaincu qu'il n'est pas malveillant.

MODIFICATION DU NIVEAU DE PROTECTION DES FICHIERS ET DE LA MEMOIRE

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Fichiers. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix entre l'un des niveaux de protection suivants :

- **Elevé**. Choisissez ce niveau si vous pensez que la probabilité d'une infection de votre ordinateur est très élevée.
- **Recommandé**. Ce niveau assure l'équilibre optimal entre les performances et la sécurité et convient à la majorité des cas.
- **Bas.** Si vous travaillez dans un milieu pourvu d'une protection (par exemple, dans un réseau d'entreprise avec une sécurité centralisée), le niveau Bas vous conviendra. Ce niveau peut également être choisi en cas d'utilisation d'applications gourmandes en ressources.

Avant d'activer le niveau de protection bas pour les fichiers, il est conseillé de lancer une analyse complète de l'ordinateur au niveau de protection élevé.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du système de fichiers de l'ordinateur" à la page 47) de l'Antivirus Fichiers. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➡ *Pour modifier le niveau proposé de protection des fichiers et de la mémoire, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

Suite à l'analyse, l'Antivirus Fichiers attribue un des états suivants aux objets découverts :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;
- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Internet Security vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse. Vous devrez réagir à la menace en sélectionnant une action à exécuter sur l'objet. En cas de sélection de l'option **Confirmer l'action** pour les actions à réaliser sur l'objet identifié, le comportement de Kaspersky Internet Security sera le comportement par défaut. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, vous pourrez choisir l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page 31), alors Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible** et pour les objets suspects : **Ignorer**.

Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone de protection fait référence non seulement à l'emplacement où se trouvent les objets analysés mais également au type de fichiers à analyser. Kaspersky Internet Security analyse par défaut uniquement les fichiers qui pourraient être infectés et qui sont exécutés sur tous les disques durs, les disques amovibles et les disques de réseau.

Vous pouvez étendre ou restreindre la zone d'analyse en ajoutant ou en supprimant des objets à analyser ou en modifiant le type de fichiers à analyser. Par exemple, vous souhaitez analyser uniquement les fichiers *exe* lancés depuis les disques de réseau. Il faut toutefois être certain de ne pas exposer l'ordinateur à un risque d'infection lors de la définition de la zone d'analyse.

Lors de la sélection du type de fichiers, il convient de garder à l'esprit les éléments suivants :

- La probabilité d'insertion d'un code malveillant et de son activation dans les fichiers de certains formats (par exemple, *txt*) est assez faible. Il existe également des formats qui contiennent ou qui pourraient contenir un code exécutable (*exe*, *dll*, *doc*). Le risque d'intrusion et d'activation ultérieure d'un code malveillant dans ces fichiers est assez élevé.
- La personne mal intentionnée peut envoyer un virus sur votre ordinateur dans un fichier dont l'extension est *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Fichiers analysés selon le format**, l'Antivirus Fichiers ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier *exe*. Le fichier sera alors soumis à une analyse antivirus.

Afin de modifier la liste des objets à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans la section **Zone d'analyse** cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Sélection de l'objet à analyser**, sélectionnez l'objet et cliquez sur le bouton **Ajouter**.

6. Après avoir ajouté tous les fichiers requis, cliquez sur **OK** dans la fenêtre **Sélection de l'objet à analyser**.

7. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

Afin de modifier la priorité de la règle, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le bloc **Type de fichiers** sélectionnez le paramètre requis.

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse est réalisée à l'aide des bases qui contiennent une description des menaces connues et les méthodes de réparation. Kaspersky Internet Security compare l'objet décelé aux enregistrements des bases, ce qui vous permet d'obtenir une réponse univoque sur la nature indésirable de l'objet analysé et sur la catégorie de programmes malveillants à laquelle il appartient. C'est ce qu'on appelle *l'analyse sur la base de signature* et cette méthode est toujours utilisée par défaut.

Entre temps, chaque jour voit l'apparition de nouveaux objets malveillants dont les enregistrements ne figurent pas encore dans les bases. L'analyse heuristique permet de découvrir ces objets. La méthode repose sur l'analyse de l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus.

En cas de découverte d'un objet malveillant, vous recevrez un message avec une requête sur la marche à suivre.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau définit l'équilibre entre la minutie de la recherche des menaces, la charge des ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans la section **Méthodes d'analyse**, cochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

OPTIMISATION DE L'ANALYSE

Pour réduire la durée de l'analyse et accélérer le fonctionnement de Kaspersky Internet Security, vous pouvez analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

- *Afin d'analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans la section **Optimisation de l'analyse**cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Les paquets d'installation et les fichiers qui contiennent des objets OLE sont exécutés à l'ouverture, ce qui les rend plus dangereux que des archives. Vous pouvez protéger votre ordinateur contre l'exécution d'un code malveillant et réduire en même temps la durée de l'analyse en désactivant l'analyse des archives et en activant l'analyse des fichiers de type donné.

Par défaut, Kaspersky Internet Security analyse uniquement les objets OLE joints.

- *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés**, cochez les cases en regard des types d'objets composés qui seront analysés par l'application.

ANALYSE DES OBJETS COMPOSES DE GRANDE TAILLE

Lors de l'analyse des fichiers composés de grande taille, le décompactage préalable peut prendre un certain temps. La durée peut être réduite si l'analyse des fichiers est réalisée en arrière-plan. Si un objet malveillant est découvert pendant l'utilisation de ces fichiers, Kaspersky Internet Security vous le signale.

Pour réduire la durée du temps d'attente avant de pouvoir accéder à des fichiers composés, il est possible de désactiver le décompactage de fichiers dont la taille est supérieure à la valeur définie. L'analyse des fichiers aura toujours lieu au moment de l'extraction de l'archive.

- *Pour que Kaspersky Internet Security décompacter les fichiers de grande taille en arrière-plan, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés** cliquez sur le bouton **Avancé**.

5. Dans la fenêtre **Fichiers composés** cochez la case **Décompacter les fichiers composés en arrière-plan** et définissez la taille minimale du fichier dans le champ en dessous.

Afin que Kaspersky Internet Security ne décompacte par les fichiers de grande taille, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Performance** dans le groupe **Analyse des fichiers composés** cliquez sur le bouton **Avancé**.

5. Dans la fenêtre **Fichiers composés** cochez la case **Ne pas décompacter les fichiers composés de grande taille** et définissez la taille maximale du fichier dans le champ du dessous.

MODIFICATION DU MODE D'ANALYSE

Le mode d'analyse désigne la condition de déclenchement d'Antivirus Fichiers. Kaspersky Internet Security utilise par défaut le mode intelligent dans lequel la décision d'analyser un objet est prise sur la base des opérations exécutées avec celui-ci. Ainsi, lors de l'utilisation d'un document Microsoft Office, Kaspersky Internet Security analyse le fichier à la première ouverture et à la dernière ouverture. Toutes les opérations intermédiaires sur le fichier sont exclues de l'analyse.

Vous pouvez modifier le mode d'analyse des objets. La sélection du mode dépend du type de fichiers que vous manipulez le plus souvent.

Afin de modifier la mode d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Mode d'analyse** sélectionnez le mode requis.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée par l'Antivirus Fichiers :

- **iChecker**. Cette technologie permet d'accélérer l'analyse en excluant certains objets. Les objets sont exclus de l'analyse à l'aide d'un algorithme spécial qui tient compte de la date d'édition des bases de Kaspersky Internet Security, de la date de l'analyse antérieure de l'objet et des modifications des paramètres d'analyse.

  Admettons que vous possédiez une archive qui a reçu l'état *sain* après l'analyse. Lors de l'analyse suivante, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases, l'archive sera analysée à nouveau.

  La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers *exe*, *dll*, *lnk*, *ttf*, *inf*, *sys*, *com*, *chm*, *zip* ou *rar*).

- **iSwift**. Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

Afin de modifier la technologie d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Technologies d'analyse** sélectionnez les paramètres requis.

SUSPENSION DU COMPOSANT : PROGRAMMATION

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant pendant un certain temps.

Illustration 7: Programmation

Pour programmer la suspension du composant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Suspension de la tâche** cochez la case **Selon la programmation** puis cliquez sur **Programmation**.
5. Dans la fenêtre **Suspension de la tâche**, indiquez l'heure (au format HH:MM) pendant laquelle la protection sera suspendue (champs **Pause à partir de** et **Reprendre à**).

SUSPENSION DU COMPOSANT : COMPOSITION DE LA LISTE DES APPLICATIONS

Lorsque vous exécutez des tâches qui requièrent beaucoup de ressources du système d'exploitation, vous pouvez suspendre temporairement l'Antivirus Fichiers. Pour réduire la charge et permettre l'accès rapide aux objets, vous pouvez configurer la suspension du composant lors de l'utilisation de certains programmes.

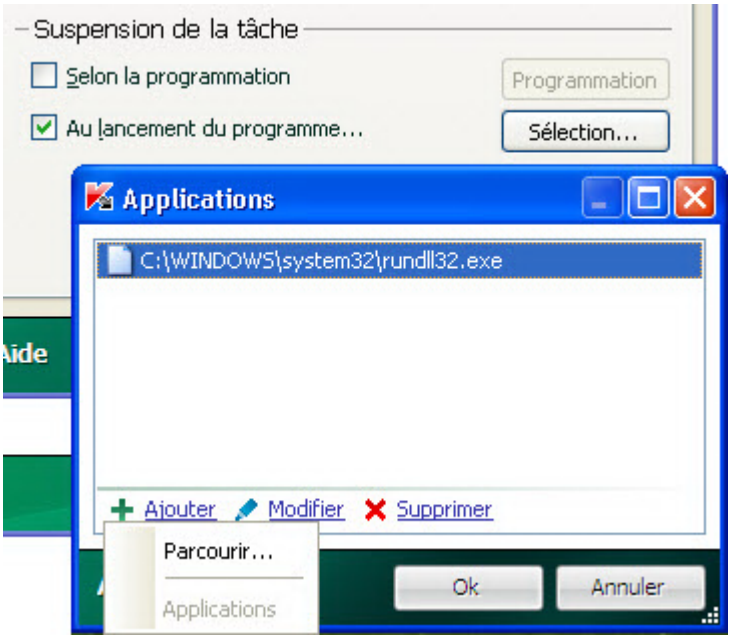


Illustration 8 : Composition de la liste des applications

La configuration de l'arrêt de l'Antivirus Fichiers en cas de conflits avec des applications déterminées est une mesure extrême ! Si des conflits se sont manifestés pendant l'utilisation du composant, contactez le Service d'assistance technique de Kaspersky Lab (http://support.kaspersky.com/fr). Les experts vous aideront à résoudre les problèmes de compatibilité entre Kaspersky Internet Security et les applications de votre ordinateur.

➡ *Pour configurer la suspension du composant pendant l'utilisation des applications indiquées, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Suspension de la tâche**, cochez la case **Au lancement de l'application** puis cliquez sur **Sélection**.
5. Dans la fenêtre **Applications** composez la liste des applications pendant l'utilisation desquelles le composant sera suspendu.

RESTAURATION DES PARAMETRES DE PROTECTION PAR DEFAUT

Lorsque vous configurez l'Antivirus Fichiers, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de protection par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU COURRIER

L'Antivirus Courrier recherche la présence d'objets dangereux dans le courrier entrant et sortant. Il démarre au lancement du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages transmis via les protocoles POP3, SMTP, IMAP, MAPI et NNTP.

L'analyse du courrier se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Une fois menace découverte, Antivirus Courrier exécute l'action définie (cf. section "Modification de l'action à réaliser sur les objets identifiés" à la page 59). Les règles d'analyse du courrier sont définies à l'aide de paramètres. Ils peuvent être scindés selon les groupes qui définissent les détails suivants :

- Flux protégé de messages ;
- Utilisation des méthodes d'analyse heuristique ;
- Analyse des fichiers composés ;
- Filtrage des fichiers joints.

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Courrier. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection. Vous pouvez restaurer les paramètres de fonctionnement par défaut de l'Antivirus Courrier. Pour ce faire, sélectionnez un des niveaux de protection.

Afin de modifier les paramètres de fonctionnement de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Kaspersky Internet Security comprend un composant qui analyse le courrier à la recherche d'objets dangereux : il s'agit de l'*Antivirus Courrier*. Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI1 et NNTP ainsi que les messages en mode sécurisé (SSL) via les protocoles POP3 et IMAP.

L'icône dans la zone de notification de la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un message est analysé.

La protection du courrier est réalisée par défaut selon l'algorithme suivant :

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par le composant.

2. Le message est décomposé selon ses parties constitutives, à savoir : l'en-tête du message, le corps du message et la pièce jointe.

3. Le corps et la pièce jointe (y compris les objets OLE) sont soumis à la recherche d'éventuels objets dangereux. Les objets malveillants sont identifiés à l'aide de bases utilisées par Kaspersky Internet Security et à l'aide d'un Algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.

4. Les comportements suivants sont envisageables à l'issue de l'analyse :

   - Si le corps du message ou la pièce jointe contient un code malveillant, l'Antivirus Courrier bloque le message, crée une copie de sauvegarde et tente de réparer l'objet. Si la réparation réussit, le message reste accessible à l'utilisateur. Si la réparation échoue, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial est inclus dans l'objet du message. Ce texte indique que le message a été traité par Kaspersky Internet Security.

   - Si le corps du message ou la pièce jointe contient un code semblable à un code malveillant, sans garantie, la partie suspecte du message est placée dans un dossier spécial : la quarantaine.

   - Si aucun code malveillant n'a été découvert dans le message, le destinataire pourra y accéder immédiatement.

Un plug-in spécial (cf. section "Analyse du courrier dans Microsoft Office Outlook" à la page 60) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Office Outlook.

Si vous utilisez The Bat!, Kaspersky Internet Security peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. section "Analyse du courrier dans The Bat!" à la page 61) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de l'application.

S'agissant des autres clients de messagerie (dont Microsoft Outlook Express, Mozilla Thunderbird, Eudora, Incredimail), l'Antivirus Courrier analyse le courrier entrant et sortant via les protocoles SMTP, POP3, IMAP et NNTP.

N'oubliez pas qu'en cas d'utilisation du client de messagerie Thunderbird, les messages transmis via le protocole IMAP ne sont pas analysés si des filtres pour le transfert des messages depuis le répertoire **Courrier entrant** sont utilisés.

MODIFICATION DU NIVEAU DE PROTECTION DU COURRIER

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Courrier. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix parmi les niveaux de protection suivant :

- **Elevé.** Si vous travaillez dans un environnement dangereux, le niveau de protection maximale du courrier sera préférable. Parmi les environnements dangereux, citons la connexion à un service de messagerie en ligne gratuit depuis votre domicile sans protection centralisée du courrier.

- **Recommandé**. Ce niveau assure l'équilibre optimal entre les performances et la sécurité et convient à la majorité des cas. Il est sélectionné par défaut.

- **Bas.** Si vous travaillez dans un environnement bien protégé, le niveau faible sera suffisant. Parmi ce genre d'environnement, citons le réseau d'une entreprise dotée d'un système centralisé de protection du courrier.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du courrier" à la page 57) de l'Antivirus Courrier. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

➧ *Afin de modifier le niveau de protection du courrier, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.

3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

L'Antivirus Courrier analyse le message électronique. Si l'analyse antivirus d'un message électronique indique que le message ou l'un de ses objets (corps ou pièce jointe) est infecté ou soupçonné d'être infecté, la suite des opérations du composant dépendra du statut de l'objet et de l'action sélectionnée.

Suite à l'analyse, l'Antivirus Courrier attribue un des états suivants aux objets trouvés :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;

- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le message ou la pièce jointe contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Internet Security vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse. Vous devrez réagir à la menace en sélectionnant une action à exécuter sur l'objet. Par défaut, ce comportement de Kaspersky Internet Security défini quand l'action à exécuter sur l'objet sélectionné est **Confirmer l'action**. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, vous pourrez choisir l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page 31), Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible** et pour les objets suspects : **Ignorer**.

➧ *Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.

3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse désigne les types de message qu'il faut analyser. Kaspersky Internet Security analyse par défaut aussi bien les messages entrant que les messages sortant. Si vous avez choisi l'analyse uniquement des messages entrant, il est conseillé au tout début de l'utilisation de Kaspersky Internet Security d'analyser le courrier sortant car le risque existe que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

La zone de protection reprend également les paramètres d'intégration de l'Antivirus Courrier dans le système ainsi que les protocoles analysés. Par défaut, l'Antivirus Courrier s'intègre aux clients de messagerie Microsoft Office Outlook et The Bat!.

Pour désactiver la protection du courrier sortant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Général** dans le groupe **Zone d'analyse**, définissez les paramètres requis.

Pour sélectionner les paramètres d'intégration de l'Antivirus Courrier au système ainsi que les protocoles à analyser, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Intégration au système** sélectionnez les paramètres requis.

ANALYSE DU COURRIER DANS MICROSOFT OFFICE OUTLOOK

Si votre client de messagerie est Microsoft Office Outlook, vous pouvez réaliser une configuration avancée de l'analyse du courrier.

Lors de l'installation de Kaspersky Internet Security, un plug-in spécial est intégré à Microsoft Outlook. Il vous permet de passer rapidement à la configuration des paramètres de l'Antivirus Courrier et de définir à quel moment la recherche d'éventuels objets dangereux sera lancée.

Le plug-in prend la forme de l'onglet **Protection du courrier** dans le menu **Services** → **Paramètres**. Sur l'onglet vous pouvez définir le mode du contrôle du courrier.

Pour définir le mode d'analyse du courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de Microsoft Office Outlook.
2. Sélectionnez le point **Service** → **Paramètres** dans le menu du programme.
3. Sélectionnez le mode requis d'analyse du courrier sur l'onglet **Protection du courrier**.

ANALYSE DU COURRIER DANS THE BAT!

Les actions à réaliser sur les objets infectés des messages électroniques dans The Bat! sont définies par le programme en lui-même.

Les paramètres de l'Antivirus Courrier qui définissent la nécessité d'analyser le courrier entrant et sortant ainsi que les actions sur les objets dangereux ou les exclusions sont ignorés. Le seul élément pris en compte par The Bat!, c'est l'analyse des archives en pièce jointe.

Les paramètres de protection du courrier sont appliqués à tous les modules antivirus de l'ordinateur compatibles avec The Bat!

Il convient de se rappeler que lors de la réception de messages, ceux-ci sont d'abord analysés par l'Antivirus Courrier puis uniquement après par le module externe pour le client de messagerie The Bat! Kaspersky Internet Security vous préviendra sans faute en cas de découverte d'un objet malveillant. Si vous avez sélectionné l'action **Réparer** (**Supprimer**) dans la fenêtre de notification de l'Antivirus Courrier, alors c'est l'Antivirus Courrier qui se chargera des actions de suppression de la menace. Si vous choisissez **Ignorer** dans la fenêtre de notification, alors l'objet sera neutralisé par le module externe de The Bat! Lors de l'envoi de courrier, les messages sont d'abord analysés par le module externe puis par l'Antivirus Courrier.

Vous devez définir :

- Le flux de messagerie qui sera soumis à l'analyse (courrier entrant, sortant).
- Le moment auquel aura lieu l'analyse des objets du message (à l'ouverture du message, avant l'enregistrement sur le disque).
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :
  - **Tenter de réparer les parties infectées** : si cette option est choisie, l'application tentera de réparer l'objet infecté et si cette réparation est impossible, l'objet restera dans le message.
  - **Supprimer les parties infectées** : si cette option est choisi, l'objet dangereux sera supprimé du message qu'il soit infecté ou potentiellement infecté.

Par défaut, tous les objets infectés des messages sont placés en quarantaine par The Bat! sans réparation.

Les messages électroniques qui contiennent des objets dangereux ne sont pas différenciés dans The Bat! par un titre spécial.

Pour passer à la configuration de la protection du courrier indésirable dans The Bat!, procédez comme suit :

1. Ouvrez la fenêtre principale de The Bat!
2. Sélectionnez l'élément **Configuration** dans le menu **Propriétés** du client de messagerie.
3. Sélectionnez le nœud **Protection contre les virus** dans l'arborescence des paramètres.

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus. L'analyse heuristique est activée par défaut.

Kaspersky Internet Security vous signale la découverte d'un objet malveillant dans le message. Il convient de réagir à ce message en choisissant une action.

Vous pouvez qui plus est définir le niveau de détail de l'analyse : **superficielle**, **moyenne** ou **profonde**. Il suffit de déplacer le curseur sur la position souhaitée.

Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Méthodes d'analyse**, cochez / décochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

ANALYSE DES FICHIERS COMPOSES

La sélection du mode d'analyse des fichiers complexes a une influence sur les performances de Kaspersky Internet Security. Vous pouvez activer ou désactiver l'analyse des archives jointes et limiter la taille maximale des archives à analyser.

Pour configurer les paramètres d'analyse des fichiers composés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Général**, sélectionnez le mode d'analyse des fichiers composés.

FILTRAGE DES PIECES JOINTES

Vous pouvez configurer les conditions de filtrage des objets joints aux messages. L'utilisation d'un filtre offre une protection supplémentaire car les programmes malveillants se propagent via le courrier électronique sous la forme de pièces jointes. Le changement de nom ou la suppression de la pièce jointe permet de protéger votre ordinateur contre l'exécution automatique d'une pièce jointe à la réception du message.

Si votre ordinateur n'est protégé par aucun moyen du réseau local et si l'accès à Internet s'opère sans serveur proxy ou pare-feu, il est conseillé de ne pas désactiver l'analyse des archives en pièce jointe.

Pour configurer le filtrage des pièces jointes, procédez comme suit :

1. Ouvrde l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Filtre des pièces jointes**, définissez les conditions de filtrages des objets joints au message. Lorsque les deux derniers modes sont sélectionnés, la liste des types d'objet devient active. Elle vous permet de sélectionner les types requis ou d'ajouter un masque d'un nouveau type.

   Si l'ajout du masque du nouveau type est indispensable, cliquez sur le lien **Ajouter** et dans la fenêtre **Masque de nom de fichier** qui s'ouvre, saisissez les données requises.

RESTAURATION DES PARAMETRES DE PROTECTION DU COURRIER PAR DEFAUT

Lorsque vous configurez l'Antivirus Courrier, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de protection de courrier par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU TRAFIC INTERNET

Chaque fois que vous utilisez Internet, vous exposez les données conservées sur votre ordinateur à un risque d'infection par des programmes dangereux. Ils peuvent s'infiltrer dans votre ordinateur tandis que vous téléchargez des programmes gratuits ou que vous consultez des informations sur des sites apparemment inoffensifs (mais soumis à des attaques de pirates avant votre visite). De plus, les vers de réseau peuvent s'introduire sur votre ordinateur avant l'ouverture des pages Web ou le téléchargement d'un fichier, à savoir directement dès l'ouverture de la connexion Internet.

Le composant *Antivirus Internet* a été développé pour protéger votre ordinateur durant l'utilisation d'Internet. Il protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

La protection Internet prévoit le contrôle du trafic http qui transite uniquement via les ports indiqués dans la liste des ports contrôlés. La liste des ports le plus souvent utilisés pour le transfert du courrier et du trafic HTTP est livrée avec Kaspersky Internet Security. Si vous utilisez des ports absents de cette liste, vous devrez les ajouter afin de protéger le trafic qui transite via ces derniers.

Si vous utilisez Internet dans un environnement dépourvu de protection, il est conseillé d'utiliser l'Antivirus Internet. Si votre ordinateur fonctionne dans un réseau protégé par un pare-feu ou des filtres de trafic HTTP, l'Antivirus Internet vous offrira une protection supplémentaire.

L'analyse du trafic se déroule selon un ensemble défini de paramètres désigné sous le concept de niveau de protection. Quand l'Antivirus Internet découvre une menace, il exécute l'action définie.

Le niveau de protection du trafic Internet sur votre ordinateur est défini par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent la zone protégée ;
- Les paramètres qui définissent la productivité de la protection du trafic (utilisation de l'analyse heuristique, optimisation de l'analyse).

Les experts de Kaspersky Lab vous déconseillent de configurer vous-même les paramètres de l'Antivirus Internet. Dans la majorité des cas, il suffit de sélectionner un autre niveau de protection.

➡ *Afin de modifier les paramètres de fonctionnement de l'Antivirus Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

L'Antivirus Internet protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

Examinons les détails du fonctionnement de ce composant. La protection du trafic HTTP s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP est intercepté et analysé par l'Antivirus Internet pour découvrir la présence de code malveillant. L'identification des objets malveillants est réalisée à l'aide des bases utilisées par Kaspersky Internet Security et d'un algorithme heuristique. Les bases contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les bases.

2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :

   - Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandée est infecté.

   - Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

L'analyse des scripts est réalisée selon l'algorithme suivant :

1. Chaque script lancé sur une page Web est intercepté par l'Antivirus Internet et soumis à une analyse antivirus.

2. Si le script contient un code malveillant, l'Antivirus Internet le bloque et avertit l'utilisateur à l'aide d'un message contextuel.

3. Si le script ne contient aucun code malicieux, il est exécuté.

Les scripts sont uniquement interceptés dans les pages ouvertes dans Microsoft Internet Explorer

MODIFICATION DU NIVEAU DE PROTECTION DU TRAFIC HTTP

Le niveau de protection désigne un ensemble prédéfini de paramètres de l'Antivirus Internet. Les experts de Kaspersky Lab ont configuré trois niveaux de protection. La sélection du niveau de protection est déterminée par l'utilisateur en fonction des conditions de travail et la situation en vigueur. Vous avez le choix entre un des niveaux de protection suivant :

- **Elevé.** Ce niveau de protection est recommandé dans les milieux agressifs lorsque d'autres moyens de protection du trafic HTTP ne sont pas prévus.
- **Recommandé**. Ce niveau de protection est le niveau optimum pour la majorité des situations.
- **Bas.** Ce niveau est recommandé si votre ordinateur est doté de moyens complémentaires de protection du trafic HTTP.

Si aucun des niveaux proposés ne répond pas à vos besoins, vous pouvez configurer les paramètres de fonctionnement (cf. section "Protection du trafic Internet" à la page 64) de l'Antivirus Internet. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut du composant, sélectionnez un des niveaux proposés.

Afin de modifier le niveau de sécurité défini du trafic Internet, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Définissez le niveau de protection requis pour le composant sélectionné.

MODIFICATION DE L'ACTION A REALISER SUR LES OBJETS IDENTIFIES

Si l'analyse d'un objet du trafic HTTP détermine la présence d'un code malveillant, la suite des opérations dépendra de l'action que vous aurez spécifiée.

S'agissant des actions sur les scripts dangereux, l'Antivirus Internet bloque toujours leur exécution et affiche à l'écran une infobulle qui informe l'utilisateur sur l'action exécutée. La modification de l'action à réaliser sur un script dangereux n'est pas possible. Seule la désactivation du fonctionnement du module d'analyse des scripts est autorisée (cf. section "Sélection du type d'analyse" à la page 67).

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page 31), alors Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux.

Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Désignez l'action requise pour le composant sélectionné.

CONSTITUTION DE LA ZONE DE PROTECTION

La constitution de la zone d'analyse signifie la sélection du type d'analyse (cf. section "Sélection du type d'analyse" à la page 67) des objets par l'Antivirus Internet et la création d'une liste d'URL de confiance dont les données ne seront pas analysées par le composant pour voir si elles contiennent des objets dangereux.

Vous pouvez composer la liste des URL de confiance dont le contenu ne présente absolument aucun danger. L'Antivirus Internet n'analysera pas les informations en provenance de ces adresses. Cela peut être utile lorsque l'antivirus Internet gêne le téléchargement d'un certain fichier qui est à chaque fois bloqué par l'antivirus Internet.

Pour constituer la liste des URL de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Optimisation de l'analyse** cochez la case ☑ **Ne pas analyser le trafic HTTP en provenance des URL de confiance** puis cliquez sur **Sélection**.
5. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, cliquez sur **Ajouter**.
6. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse de confiance (ou son masque).

SELECTION DU TYPE D'ANALYSE

La tâche de composition de la zone d'analyse (cf. page 67) propose également, outre la création d'une liste d'URL de confiance, la possibilité de choisir le type d'analyse du trafic par Antivirus Internet. Les analyses proposées sont l'analyse des scripts et l'analyse du trafic HTML.

Par défaut, l'Antivirus Internet analyse le trafic HTTP et les scripts simultanément.

L'analyse du trafic HTTP désigne non seulement la recherche de virus mais également la vérification des liens afin de voir s'ils appartiennent à la liste des URL suspectes et/ou de phishing.

L'analyse des liens pour vérifier s'ils appartiennent à la liste des adresses de phishing permet d'éviter les attaques de phishing qui, en règle générale, se présentent sous la forme de messages électroniques prétendument envoyés par une institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message amène le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche.

Puisque le lien vers un site de phishing peut être envoyé non seulement par courrier électronique, mais également par d'autres moyens tels que les messages ICQ, le composant Antivirus Internet suit les tentatives d'ouverture du site de phishing au niveau de l'analyse du trafic HTTP et les bloque.

La vérification des liens pour voir s'ils appartiennent à la liste des URL suspectes permet de repérer les sites qui figurent sur la liste noire. La liste est composée par les experts de Kaspersky Lab et est livrée avec l'application.

Pour qu'Antivirus Internet analyse les scripts, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Antivirus Internet**, qui s'ouvre, dans le groupe **Avancé**, assurez-vous que la case ☑ **Bloquer les scripts dangereux dans Microsoft Internet Explorer** est cochée. L'Antivirus Internet analysera tous les scripts traités par Microsoft Internet Explorer ainsi que n'importe quel script WSH (JavaScript, Visual Basic Script, etc.) lancé tandis que l'utilisateur travaille sur l'ordinateur, notamment sur Internet.

   De plus, vous pouvez utiliser le module d'analyse des liens (cf. page 68) en cochant la case ☑ **Signaler les liens suspects ou d'hameçonnage dans Microsoft Internet Explorer et Mozilla Firefox**. L'Antivirus Internet mettra en évidence dans les navigateurs (Microsoft Internet Explorer et Mozilla Firefox) les liens suspects ou d'hameçonnage dans les URL.

➧ *Pour vérifier si un lien appartient à la liste des URL suspectes et/ou de phishing, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Méthodes d'analyse**, assurez-vous que la case ☑ **Analyser les liens selon la base des URL suspectes** et / ou la case ☑ **Analyser les liens selon la base des URL de phishing** sont cochées.

MODULE D'ANALYSE DES LIENS

Kaspersky Internet Security propose un module d'analyse des liens qui est administré par l'Antivirus Internet. Le module analyse tous les liens sur une page afin de voir s'il s'agit de liens suspects ou de phishing. Vous pouvez composer la liste des adresses de confiance des sites dont le contenu ne doit pas être analysé ainsi que la liste des sites dont le contenu doit absolument être analysé. Le module est intégré aux navigateurs Microsoft Internet Explorer et Mozilla Firefox sous la forme d'un plug-in.

➧ *Pour activer le module d'analyse des liens, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cochez la case ☑ **Signaler les liens suspects ou d'hameçonnage dans Microsoft Internet Explorer et Mozilla Firefox**.

➧ *Pour constituer la liste des URL de confiance, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option ◉ **Pour toutes les URL** puis cliquez sur le bouton **Exclusions**.
6. Dans la fenêtre **Liste des URL de confiance** qui s'ouvre, cliquez sur **Ajouter**.
7. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse de confiance (ou son masque).

Pour composer la liste des URL des sites dont le contenu doit absolument être analysé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Niveau de protection**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Avancé** cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Module d'analyse des liens** qui s'ouvre, sélectionnez l'option **Pour les URL indiqués** puis cliquez sur le bouton **Sélection**.
6. Dans la fenêtre **Liste des URL analysées** qui s'ouvre, cliquez sur **Ajouter**.
7. Dans la fenêtre **Masque d'adresse (URL)** qui s'ouvre, saisissez l'adresse (ou son masque).

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. Si cet activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. Ainsi, les nouvelles menaces seront identifiées avant que leur activité ne soit remarquée par les spécialistes des virus. L'analyse heuristique est activée par défaut.

Kaspersky Internet Security vous signale la découverte d'un objet malveillant dans le message. Il convient de réagir à ce message en choisissant une action.

Vous pouvez qui plus est définir le niveau de détail de l'analyse : **superficiel**, **moyen** ou **profond**. Il suffit de déplacer le curseur sur la position souhaitée.

Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Méthodes d'analyse**, cochez / décochez la case **Analyse heuristique** et définissez le niveau de détail de l'analyse en dessous.

OPTIMISATION DE L'ANALYSE

Afin d'accroître le taux de détection des codes malveillants, l'Antivirus Internet utilise la technologie de mise en cache de fragments des objets envoyés via Internet. Dans cette méthode, l'analyse est réalisée uniquement une fois que l'objet entier a été reçu. Ensuite, l'objet est soumis à une recherche de virus et il est transmis à l'utilisateur ou bloqué en fonction des résultats de cette analyse.

Sachez toutefois que la mise en cache augmente la durée de traitement de l'objet et du transfert à l'utilisateur. Elle peut également provoquer des problèmes au niveau de la copie et du traitement de gros objets en raison de l'écoulement du délai de connexion du client HTTP.

Pour résoudre ce problème, nous vous proposons de limiter dans le temps la mise en cache des fragments des objets. Une fois le délai écoulé, chaque partie du fichier reçue sera transmise à l'utilisateur sans vérification et l'objet sera analysé complètement une fois qu'il sera copié. Ainsi, la durée du transfert de l'objet à l'utilisateur est réduite et les problèmes liés à la déconnexion sont réglés sans pour autant réduire le niveau de la protection pendant l'utilisation d'Internet.

Par défaut, la limitation dans le temps de la mise en cache des fragments est de 1 seconde. L'augmentation de cette valeur ou la levée de la restriction de la durée de la mise en cache augmente le niveau de l'analyse antivirus mais entraîne un certain ralentissement au niveau de l'accès à l'objet.

Pour établir une restriction dans le temps pour la mise en cache des fragments ou pour lever cette restriction, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Antivirus Internet** qui s'ouvre, dans le groupe **Optimisation de l'analyse**, cochez / décochez la case **Limiter la durée de mise en cache des fragments** et définissez le temps (en secondes) dans le champ de droite.

RESTAURATION DES PARAMETRES DE PROTECTION INTERNET PAR DEFAUT

Lorsque vous configurez l'Antivirus Internet, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de l'Antivirus Internet par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Internet** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

PROTECTION DU TRAFIC DES MESSAGERIES INSTANTANEES

Les applications très populaires ces derniers temps pour l'échange de messages instantanés (par la suite, les *clients de messagerie instantanée*) facilitent la communication via Internet mais constituent également une menace pour la sécurité de l'ordinateur. Les clients de messagerie instantanée peuvent envoyer des messages contenant des liens vers des sites suspects ou vers des sites utilisés par les individus mal intentionnés pour les attaques d'hameçonnage. Les programmes malveillants utilisent les clients de messagerie instantanées pour diffuser des messages non sollicités et des liens vers des programmes (ou les programmes eux-mêmes) développés pour dérober le compte de l'utilisateur.

Le composant *Antivirus IM ("Chat")* a été mis au point pour garantir votre protection durant l'utilisation de clients de messagerie instantanée. Il protège les informations envoyées vers votre ordinateur via les protocoles des clients de messagerie instantanée.

Ce logiciel garantit une utilisation sans danger des systèmes de messagerie instantanée tels qu'ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru.Agent et IRC.

Les applications Yahoo! Messenger et Google Talk fonctionnent via le protocole SSL. Pour que l'Antivirus IM analyse le trafic de ces applications, il faut utiliser l'analyse des connexions sécurisées (cf. page 178). Pour ce faire, cochez la case **Analyse des connexions sécurisées** dans la section **Réseau**.

L'analyse du trafic est réalisée selon un ensemble défini de paramètres. Dès que l'Antivirus IM détecte une menace dans un message, il remplace le contenu du message par un avertissement pour l'utilisateur.

Le niveau de protection du trafic des messageries instantanées sur votre ordinateur est défini par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Paramètres définissant la zone d'analyse ;
- Paramètres définissant les méthodes d'analyse.

Afin de modifier les paramètres de fonctionnement de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, modifiez comme il se doit les paramètres.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Kaspersky Internet Security propose un composant qui analyse les messages transmis via les clients de messagerie instantanée afin de voir s'ils contiennent des objets dangereux. Il s'agit de l'*Antivirus IM ("Chat")*. Il est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les messages entrant ou sortant.

Par défaut, la protection du trafic des clients de messagerie instantanée s'opère selon l'algorithme suivant.

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par le composant.

2. L'Antivirus IM analyse le message afin de voir s'il contient des objets dangereux ou des liens repris dans les bases des URL suspectes ou de phishing. Lorsqu'une menace est détectée, le texte du message est remplacé par un avertissement à l'attention de l'utilisateur.

3. Si aucune menace pour la sécurité n'est détectée, le message est accessible à l'utilisateur.

Les fichiers transmis via les clients de messagerie instantanée sont analysés par le composant Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page 47) au moment de la tentative de sauvegarde.

CONSTITUTION DE LA ZONE DE PROTECTION

La zone d'analyse désigne les types de message qu'il faut analyser :

- **Analyser le courrier entrant et sortant**. L'Antivirus IM analyse par défaut les messages entrant et sortant.

- **Analyser uniquement le courrier entrant**. Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir d'objets dangereux, sélectionnez ce paramètre. L'Antivirus IM analysera uniquement les messages entrant.

Kaspersky Internet Security analyse par défaut aussi bien les messages entrant que les messages sortant des clients de messagerie instantanée.

Si vous êtes convaincu que les messages que vous envoyez ne peuvent contenir aucun objet dangereux, vous pouvez vous passer de l'analyse du trafic sortant.

➡ *Pour désactiver l'analyse des messages sortant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.

3. Pour le composant sélectionné, choisissez l'option **Analyser uniquement le courrier entrant** dans le groupe **Zone d'analyse**.

SELECTION DE LA METHODE D'ANALYSE

La méthode d'analyse désigne l'analyse des liens, inclus dans les messages envoyés par messagerie instantanée, pour savoir s'ils appartiennent à la liste des adresses suspectes et / ou à la liste des adresses de phishing :

- **Analyser les liens selon la base des URL suspectes**. L'Antivirus IM analysera les liens dans les messages afin de voir s'ils appartiennent à la liste noire.

- **Analyser les liens selon la base des URL de phishing**. Les bases de Kaspersky Internet Security contiennent les sites connus à l'heure actuelle qui sont utilisés lors des attaques de phishing. Les experts de

Kaspersky Lab y ajoutent les adresses fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). Cette liste est enrichie lors de la mise à jour des bases de Kaspersky Internet Security.

Pour analyser les liens des messages selon la base des adresses suspectes, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez la case **Analyser les liens selon la base des URL suspectes** dans le groupe **Méthodes d'analyse**.

Pour analyser les liens des messages selon la base des adresses de phishing, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez la case **Analyser les liens selon la base des URL de phishing** dans le groupe **Méthodes d'analyse**.

UTILISATION DE L'ANALYSE HEURISTIQUE

La méthode heuristique consiste à analyser l'activité de l'objet dans le système. C'est ainsi que tout script contenu dans un message d'un client de messagerie instantanée est exécuté dans un milieu sûr. Si l'activité du script est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect. L'analyse heuristique est activée par défaut.

Kaspersky Internet Security vous signale la découverte d'un objet malveillant dans le message.

Vous pouvez qui plus est sélectionner le niveau de détail de l'analyse : **superficielle**, **moyenne** ou **profonde**. Il suffit de déplacer le curseur sur la position souhaitée.

Pour activer / désactiver l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquezsur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cochez ou décochez la case **Analyse heuristique** dans le groupe **Analyse heuristique** puis établissez le niveau de détail de l'analyse.

CONTROLE DES APPLICATIONS

Du point de vue de la sécurité du système, toutes les applications peuvent être réparties en trois groupes :

- *Inoffensives*. Ce groupe reprend les applications développées par des éditeurs connus et dotées de signatures numériques. Vous pouvez autoriser n'importe quelle action de ces applications dans le système.
- *Dangereuses*. Ce groupe reprend les menaces connues à ce jour. L'activité de ces applications doit absolument être bloquée.
- *Inconnues*. Ce groupe est constitué par les applications développées personnellement qui ne possèdent pas de signature numérique. Elles ne sont pas nécessairement nuisibles au système mais seule l'analyse de leur comportement permettra de prendre une décision catégorique sur la sécurité de l'utilisation de celles-ci. Avant de décider de la dangerosité d'une application inconnue, il est préférable de limiter ses accès aux ressources du système.

Le Contrôle des Applications enregistre les actions réalisées par les applications dans le système et réglemente l'activité des applications sur la base du groupe (cf. section "Groupes d'applications" à la page 76) auquel elles appartiennent. Un ensemble de règles (cf. section "Règles du Contrôle des Applications" à la page 79) a été défini pour chaque groupe d'applications. Ces règles définissent l'accès des applications à diverses ressources :

- Fichiers et dossiers ;
- Clés de registre ;
- Adresses de réseau ;
- Environnement d'exécution.

Lorsque l'application sollicite une ressource, le composant vérifie si l'application jouit des privilèges d'accès requis puis exécute l'action prévue par la règle.

➡ *Afin de modifier les paramètres de fonctionnement du Contrôle des Applications, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.
3. Pour le composant sélectionné, introduisez les modifications requises dans les paramètres.

➡ *de même :*

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique Contrôle des Applications.
2. Dans la partie droite de la fenêtre, cliquez sur le lien **Surveillance des Applications**.
3. Dans la fenêtre **Contrôle des Applications** qui s'ouvre introduisez les modifications requises.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Au lancement de l'application, le Contrôle des Applications la surveille selon l'algorithme suivant :

1. Recherche de la présence éventuelle de virus dans l'application.

2. Vérification de la signature numérique de l'application. Si la signature numérique est présente, l'application entre dans le groupe **De confiance**. Si l'application ne possède pas de signature numérique (et si la signature numérique est endommagée ou reprise dans la liste "noire"), le composant passe à l'étape suivante.

3. Recherche de la présence de l'application lancée dans la base interne des applications connues livrée avec Kaspersky Internet Security. Si la base contient un enregistrement correspondant à l'application exécutée, alors celle-ci sera reprise dans le groupe correspondant. Si la base ne contient pas l'enregistrement de l'application lancée, alors le composant passe à une étape spéciale.

4. Envoi des informations relatives au fichier exécutable de l'application dans la base des applications connues hébergée sur un serveur de Kaspersky Lab. Si la base contient un enregistrement qui correspond aux informations envoyées, alors l'application est placée dans le groupe correspondant. S'il n'est pas possible d'établir la communication avec la base (par exemple, pas de connexion Internet), le composant passe à l'étape suivante.

5. Calcul du niveau de danger de l'application à l'aide de l'analyse heuristique. Les applications dont le degré de danger est faible sont classées dans le groupe **Restrictions faibles**. Si le classement de l'application est élevé, Kaspersky Internet Security vous en avertit et vous proposer de choisir le groupe dans lequel il faudra placer l'application.

Une fois que toutes les vérifications ont été exécutées, un message apparaît à l'écran et indique la décision prise vis-à-vis de l'application. La notification par défaut est désactivée.

Au deuxième lancement de l'application, le Contrôle des Applications vérifie son intégrité. Si l'application n'a pas été modifiée, le composant applique la règle existante. Si l'application a été modifiée, le Contrôle des Applications la vérifie selon l'algorithme décrit ci-dessus.

VOIR EGALEMENT

HERITAGE DES PRIVILEGES

Le mécanisme d'*héritage des privilèges* est une partie importante du composant Contrôle des Applications. Il empêche l'utilisation d'applications de confiance par des applications douteuses ou dont les privilèges sont réduits pour exécuter des actions avec des privilèges.

Lorsque l'application tente d'accéder à la ressource contrôlée, le Contrôle des Applications analyse les privilèges de tous les processus parent de cette application afin de voir s'ils peuvent accéder à la ressource. Dans ce cas, c'est la *règle de la priorité minimale* qui est appliquée : lorsque les privilèges d'accès de l'application et du processus parent sont comparés, les privilèges d'accès avec la priorité minimale seront appliqués à l'activité de l'application.

Priorité des privilèges d'accès :

1. **Autoriser**. Ces privilèges d'accès ont une priorité élevée.
2. **Confirmer auprès de l'utilisateur**.
3. **Bloquer**. Ces privilèges d'accès ont une priorité faible.

Exemple :

un cheval de Troie tente d'utiliser *regedit.exe* pour modifier la base de registres de Microsoft Windows. Dans la règle pour le cheval de Troie, l'action **Bloquer** a été sélectionnée en guise de réaction en cas d'accès à la base de registres, et pour *regedit.exe* – l'action **Autoriser**.

Dans ce cas, l'activité de *regedit.exe* lancée par le cheval de Troie sera bloquée car les privilèges de *regedit.exe* sont hérités du processus parent. La règle de la priorité minimale est appliquée : l'action sera bloquée même si l'application *regedit.exe* possède des privilèges d'autorisation.

Si l'activité de l'application est bloquée à cause du manque des droits chez un des processus parental, vous pouvez changer ces règles (cf. section "Modification de la règle pour l'application" à la page 81).

Il faut modifier les privilèges du processus parent et désactiver l'héritage des restrictions uniquement si vous êtes absolument certain que l'activité du processus ne menace pas la sécurité du système !

VOIR EGALEMENT

Séquence de lancement de l'application 77

CLASSEMENT DU DANGER

Pour chaque application exécutée sur l'ordinateur, le Contrôle des Application établit, avec l'aide de l'analyse heuristique, un classement du danger. *Le classement du danger* est un indicateur du danger de l'application pour le système. Il est calculé sur la base de critères de deux types :

- Statistiques (ces critères regroupent les informations relatives au fichier exécutable de l'application : taille du fichier, date de création, etc.) ;
- Dynamique (ces critères sont appliqués lors de la modélisation du fonctionnement de l'application en environnement protégé (analyse des requêtes de l'application vers les fonctions système). L'analyse de ces critères permet d'identifier les comportements typiques des applications malveillantes.

Les applications sont rangées en différents groupes (cf. section "Groupes d'applications" à la page 76) selon les valeurs du classement établi par le Contrôle des Applications. Plus le classement est bas, plus le nombre d'actions autorisées pour l'application est élevé.

GROUPES D'APPLICATIONS

Toutes les applications exécutées sur l'ordinateur sont réparties par le Contrôle des Applications en groupes selon le niveau de danger qu'elles constituent pour le système et selon les privilèges d'accès des applications aux ressources.

Il existe quatre groupes d'applications :

- **De confiance**. Ces applications possèdent une signature numérique d'éditeurs de confiance ou cette signature est présente dans la base des applications de confiance. Ces applications ne sont soumises à aucune restriction quant aux actions exécutées dans le système. L'activité de ces applications est contrôlée par la Défense Proactive et l'Antivirus Fichiers.
- **Restrictions faibles**. Applications qui ne possèdent pas une signature numérique d'éditeurs de confiance ou absente de la base des applications de confiance. Toutefois, ces applications figurent en bas du classement du

danger (à la page 76). Elles peuvent réaliser certaines opérations, accéder à d'autres processus, administrer le système, accéder de manière dissimulée au réseau. L'autorisation de l'utilisateur est requise pour la majorité des opérations.

- **Restrictions fortes**. Applications qui ne possèdent pas une signature numérique ou absente de la base des applications de confiance. Ces applications figurent dans le haut du classement du danger. La majorité des actions réalisées par les applications de ce groupe dans le système doit être autorisée par l'utilisateur ; certaines actions de ces applications sont interdites.

- **Douteuses**. Applications qui ne possèdent pas une signature numérique ou absente de la base des applications de confiance. Ces applications figurent en tête du classement du danger. Le Contrôle des Applications bloque la moindre action de ces applications.

Les applications placées dans un groupe déterminé par le Contrôle des Applications reçoivent l'état correspondant et héritent des privilèges d'accès aux ressources des règles (cf. section "Règles du Contrôle des Applications" à la page 79) définies pour le groupe.

Les experts de Kaspersky Lab déconseillent de déplacer les applications dans les groupes. En cas de besoin, il est préférable de modifier les règles d'accès de l'application à une ressource particulière du système (cf. section "Modification de la règle pour l'application" à la page 81).

SEQUENCE DE LANCEMENT DE L'APPLICATION

L'utilisateur ou une autre application en cours d'exécution peut être à l'origine du lancement de l'application.

Si l'application a été lancée par une autre, alors la séquence de lancement est composée des applications mère et fille. La séquence de lancement peut être enregistrée.

Lors de l'enregistrement de la séquence de lancement, chaque application qui appartient à cette séquence demeure dans son propre groupe.

VOIR EGALEMENT

CONSTITUTION DE LA ZONE DE PROTECTION

Le Contrôle des Applications gère les privilèges des applications pour l'exécution de certaines actions sur les catégories de ressources suivantes :

Système d'exploitation. Cette catégorie reprend :

- clés de registre contenant les paramètres de lancement automatique ;
- clés de registre contenant les paramètres d'utilisation d'Internet ;
- clés de registre influant sur la sécurité du système ;
- clés de registre contenant les paramètres des services système ;
- fichiers et répertoires systèmes ;
- dossiers de lancement automatique

Les experts de Kaspersky Lab ont composé une liste de paramètres et de ressources du système d'exploitation qui doivent toujours être protégés par Kaspersky Internet Security. Il n'est pas permis de modifier cette liste. Mais vous pouvez décider de ne pas contrôler tel ou tel objet du système d'exploitation dans la catégorie sélectionnée ou vous pouvez augmenter la liste.

Données personnelles. Cette catégorie reprend :

- fichiers de l'utilisateur (répertoires Mes Documents, fichiers cookies et données sur l'activité de l'utilisateur) ;
- fichiers, répertoires et clés de la base de registres qui contiennent les paramètres de fonctionnement et des données importantes des applications les plus souvent utilisées : navigateurs Internet, gestionnaires de fichiers, clients de messagerie, client de messagerie instantanée, porte-monnaies électroniques.

Les experts de Kaspersky Lab ont composé une liste de catégories de ressources qui devront toujours être protégées par Kaspersky Internet Security. Il n'est pas permis de modifier cette liste. Vous pouvez toutefois désactiver le contrôle d'une catégorie de ressource ou d'une autre ou enrichir la liste.

Pour enrichir la liste des données personnelles protégées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Données personnelles** choisissez dans la liste déroulante **Catégorie** la catégorie d'objets de données personnelles requise puis cliquez sur le lien **Ajouter** (cliquez sur le lien **Ajouter une catégorie**, s'il faut ajouter une nouvelle catégorie de ressources protégées et saisissez son nom dans la fenêtre qui s'ouvre).
5. Dans la fenêtre **Ressource de l'utilisateur** qui s'ouvre, cliquez sur **Parcourir** et saisissez les données requises en fonction de la ressource ajoutée :
   - **Fichier ou répertoire**. Dans la fenêtre **Choix du fichier ou du répertoire**, indiquez le fichier ou le répertoire.
   - **Clé de registre**. Dans la fenêtre **Choix de l'objet dans le registre** qui s'ouvre, définissez la clé de registre protégée.
   - **Service de réseau**. Dans la fenêtre **Service de réseau** donnez les paramètres de connexion de réseau contrôlée (cf. section "Configuration des paramètres du service de réseau" à la page 94).
   - **Adresse IP**. Dans la fenêtre **Adresses de réseau**, désignez la plage d'adresses à protéger.

   Une fois que la ressource a été ajoutée à la zone d'analyse vous pouvez la modifier ou la supprimer à l'aide des liens du même nom dans la partie inférieure de l'onglet. Si vous souhaitez exclure une ressource de la zone d'analyse, décochez la case ☑ en regard.

Pour élargir la liste des paramètres et des ressources du système d'exploitation protégés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Système d'exploitation**, choisissez dans la liste déroulante **Catégorie** la catégorie d'objets du système d'exploitation puis cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Ressource de l'utilisateur** qui s'ouvre, cliquez sur **Parcourir** et saisissez les données requises en fonction de la ressource ajoutée :

   - **Fichier ou répertoire**. Dans la fenêtre **Choix du fichier ou du répertoire**, indiquez le fichier ou le répertoire.

   - **Clé de registre**. Dans la fenêtre **Choix de l'objet dans le registre** qui s'ouvre, définissez la clé de registre protégée.

   Une fois que la ressource a été ajoutée à la zone d'analyse vous pouvez la modifier ou la supprimer à l'aide des liens du même nom dans la partie inférieure de l'onglet. Si vous souhaitez exclure une ressource de la zone d'analyse, décochez la case ☑ en regard.

REGLES DU CONTROLE DES APPLICATIONS

La règle est un ensemble de réactions du Contrôle des Applications face aux actions d'une application sur les ressources contrôlées (cf. section "Constitution de la zone de protection" à la page 77).

Réactions possibles du composant :

- **Hériter**. Le Contrôle des Applications appliquera à l'activité de l'application la règle créée pour le groupe auquel appartient l'application. Cette réaction est appliquée par défaut.

- **Autoriser**. Le Contrôle des Applications autorise l'exécution de l'action.

- **Interdire**. Le Contrôle des Applications interdit l'exécution de l'action.

- **Confirmer l'action**. Le Contrôle des Applications signale à l'utilisateur qu'une application tente d'exécuter une action et demande à l'utilisateur de confirmer la suite des événements.

- **Consigner dans le rapport**. Les informations relatives à l'activité de l'application ainsi que les réactions du Contrôle des Applications seront consignées dans le rapport. La consignation des informations dans le rapport peut être utilisée avec n'importe quelle autre action du composant.

L'application hérite par défaut des privilèges d'accès du groupe auquel elle appartient. Vous pouvez modifier la règle pour l'application. Dans ce cas, les paramètres de la règle pour l'application auront une priorité supérieure à celle des paramètres de la règle pour le groupe auquel l'application.

VOIR EGALEMENT

REPARTITION DES APPLICATIONS EN GROUPE

Les applications placées par le Contrôle des Applications dans le groupe (cf. section "Groupes d'applications" à la page 76) **De confiance** ne constituent aucun danger pour le système.

Vous pouvez exploiter la possibilité de définir le cercle d'applications de confiance dont l'activité ne sera pas analysée par le Contrôle des Applications. Les applications de confiance peuvent être les applications possédant une signature numérique ou les applications présentes dans la base de Kaspersky Security Network.

Pour les autres applications qui n'appartiennent pas au groupe des applications de confiance, vous pouvez utiliser l'analyse heuristique dans le but de définir le groupe ou désigner directement le groupe auquel l'application sera ajoutée automatiquement.

- *Pour que le Contrôle des Applications considère comme application de confiance toute application dotée d'une signature numérique et/ou reprise dans la base de Kaspersky Security Network et ne vous communique aucune information relative à l'activité, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

  3. Pour le composant sélectionné, cochez les cases ☑ **Avec une signature numérique (Editeurs connus)** et / ou ☑ **Présentes dans la base de Kaspersky Security Network** dans le groupe **Applications de confiance**.

- *Pour que le Contrôle des Applications utilise l'analyse heuristique afin de répartir les applications douteuses en groupes, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

  3. Pour le composant sélectionné dans le groupe **Applications de confiance**, sélectionnez l'option ◉ **Déterminer l'état à l'aide de l'analyse heuristique**. Une fois l'état de l'application aura été défini, celle-ci sera placée dans le groupe correspondant.

- *Pour que le Contrôle des Applications attribue automatiquement l'état indiqué pour la répartition des applications douteuses, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

  3. Pour le composant sélectionné, dans le groupe **Applications de confiance**, sélectionnez l'option ◉ **Attribuer automatiquement l'état** et choisissez l'état requis dans la liste déroulante à droite. Les applications seront réparties dans les groupes correspondant à l'état.

MODIFICATION DE L'HEURE D'ATTRIBUTION DE L'ETAT DE L'APPLICATION

Si l'état de l'application est défini via l'analyse heuristique, alors le Contrôle des Applications étudie l'application durant 30 secondes. Si le calcul du niveau de danger ne peut être réalisé au cours de cette période, l'application reçoit l'état *Restrictions faibles* et elle se retrouve dans le groupe correspondant.

Le calcul du niveau de danger se poursuit en arrière-plan. Une fois que l'application a été soumise à l'analyse heuristique, elle reçoit l'état correspondant au classement du danger et elle est placée dans le groupe correspondant.

Vous pouvez modifier la durée de la période que le composant consacre à l'analyse des applications exécutées. Si vous êtes convaincu que toutes les applications exécutées sur votre ordinateur ne menacent pas la sécurité, vous pouvez réduire la durée de l'analyse. Si, au contraire, vous installez une application dont vous ne pouvez garantir la fiabilité en matière de sécurité, il est conseillé d'augmenter la durée de l'analyse.

Pour modifier la durée de l'analyse des applications inconnues, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

3. Pour le composant sélectionné, dans le groupe **Avancé**, définissez la valeur du paramètre **Durée maximale pour déterminer l'état de l'application**.

MODIFICATION DE LA REGLE POUR L'APPLICATION

Lorsqu'une application est lancée pour la première fois, le Contrôle des Applications définit son état et la place dans le groupe correspondant. Ensuite, le composant enregistre les actions de cette application dans le système et réglemente son activité sur la base du groupe (cf. section "Groupes d'applications" à la page 76) auquel elle appartient. Lorsque l'application sollicite une ressource, le composant vérifie si l'application jouit des privilèges d'accès requis puis exécute l'action prévue par la règle. Vous pouvez modifier la règle créée pour l'application au moment où son état a été défini et où elle a été placée dans le groupe correspondant.

Pour modifier une règle pour l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Contrôle des Applications**.

2. Dans la fenêtre qui s'ouvre, dans le groupe **Contrôle des Applications**, cliquez sur le lien **Surveillance des Applications**.

3. Dans la fenêtre **Contrôle des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

4. Pour l'application requise, dans la colonne **Etat**, cliquez avec le bouton gauche de la souris sur le lien indiquant l'état de l'application.

5. Dans le menu déroulant, sélectionnez le point **Paramètres de l'utilisateur**.

6. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles** modifiez les privilèges d'accès pour la catégorie de ressources requise.

MODIFICATION DE LA REGLE POUR UN GROUPE D'APPLICATIONS

Lorsqu'une application est lancée pour la première fois, le Contrôle des Applications définit son état et la place dans le groupe correspondant. Ensuite, le composant enregistre les actions de cette application dans le système et réglemente son activité sur la base du groupe (cf. section "Groupes d'applications" à la page 76) auquel elle appartient. Le cas échéant, vous pouvez modifier la règle pour le groupe.

Pour modifier une règle pour un groupe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

3. Pour le composant sélectionné, dans le groupe **Règles pour les états des applications**, cliquez sur le bouton **Configuration des règles**.

4. Dans la fenêtre **Configuration des règles du contrôle de l'activité** qui s'ouvre, sélectionnez le groupe requis.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles** modifiez les privilèges d'accès pour la catégorie de ressources requise.

CREATION D'UNE REGLE DE RESEAU POUR L'APPLICATION

Après la première exécution de l'application, le Contrôle des Applications la place par défaut dans un des groupes prédéfinis. La règle de groupe régit l'accès de l'application aux réseaux correspondant à un état particulier. Si vous devez traiter d'une manière particulière l'accès de l'application à un service de réseau défini, vous pouvez créer une règle de réseau.

Pour créer une règle qui va régir l'activité de réseau de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et sélectionnez la section **Contrôle des Applications**.

2. Dans la fenêtre qui s'ouvre, dans le groupe **Contrôle des Applications**, cliquez sur le lien **Surveillance des Applications**.

3. Dans la fenêtre **Contrôle des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

4. Pour l'application requise, dans la colonne **Etat**, cliquez avec le bouton gauche de la souris sur le lien indiquant l'état de l'application.

5. Dans le menu déroulant, sélectionnez le point **Paramètres de l'utilisateur**.

6. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles** sélectionnez, dans la liste déroulante la catégorie **Règles de réseau** puis cliquez sur le lien **Ajouter**.

7. Dans la fenêtre **Règle de réseau** qui s'ouvre, configurez les paramètres de la règle paquet.

8. Définissez la priorité de la règle créée.

CONFIGURATION DES EXCLUSIONS

Lors de la création de règles pour les applications, Kaspersky Internet Security contrôle par défaut toutes les actions de l'application : accès aux fichiers et aux répertoires, accès au milieu d'exécution et accès au réseau. Vous pouvez exclure certaines actions de l'analyse.

Pour exclure de l'analyse des actions de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et sélectionnez la section **Contrôle des Applications**.

2. Dans la fenêtre qui s'ouvre, dans le groupe **Contrôle des Applications**, cliquez sur le lien **Surveillance des Applications**.

3. Dans la fenêtre **Contrôle des Applications** sélectionnez la catégorie requise dans la liste **Catégorie**.

4. Pour l'application requise, dans la colonne **Etat**, cliquez avec le bouton gauche de la souris sur le lien indiquant l'état de l'application.

5. Dans le menu déroulant, sélectionnez le point **Paramètres de l'utilisateur**.

6. Dans la fenêtre qui s'ouvre, onglet **Exclusions** cochez les cases qui correspondent aux actions exclues. En cas d'exclusion de l'analyse du trafic de réseau de l'application, configurez des paramètres complémentaires d'exclusion.

   Toutes les exclusions créées dans les règles pour les applications sont accessibles dans la fenêtre de configuration des paramètres de l'application, dans le groupe **Menaces et exclusions**.

SUPPRESSION DE REGLES POUR LES APPLICATIONS

Vous pouvez supprimer les règles pour les applications qui n'ont plus été exécutées depuis un certain temps.

Pour supprimer les règles pour les applications qui n'ont plus été lancées depuis un certain temps, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle des Applications** dans la rubrique **Protection**.

3. Pour le composant sélectionné dans le groupe **Avancé**, cochez la case **Supprimer les règles des applications qui n'ont plus été lancées depuis** et dans le champ à droite, définissez le nombre de jours requis.

EXECUTION DES APPLICATIONS EN ENVIRONNEMENT PROTEGE

Sous Microsoft Windows XP x64 l'environnement protégé d'exécution des applications n'est pas disponible.

Pour garantir la protection maximale des objets du système d'exploitation et des données personnelles des utilisateurs, les experts de Kaspersky Lab ont développé la possibilité d'exécuter les applications dans un milieu virtuel protégé, à savoir l'*Environnement protégé*.

Il est conseillé de lancer dans l'environnement protégé les applications dont vous ne pouvez garantir l'authenticité. Ceci permettra d'éviter les modifications des objets du système d'exploitation qui peuvent amener à son fonctionnement incorrect.

Sous Microsoft Windows XP x64 et Microsoft Windows 7 x64 les fonctions de certaines applications dans l'environnement protégé sont limitées. Quand une application de ce genre est lancée, un message apparaîtra à l'écran, si les notifications (cf. page 181) pour l'événement **La fonction de l'application en environnement protégé est limitée** ont été définies.

Le lancement des navigateurs Internet dans l'environnement protégé garantit la sécurité de consultation des sites Internet, y compris la protection contre les applications malveillantes et la protection des données personnelles de l'utilisateur contre les modifications et suppressions non autorisées, ainsi que la possibilité de supprimer tous les objets accumulés lors des séances d'utilisation d'Internet (fichiers temporaires, cookies, historique des visites, etc.). Microsoft Internet Explorer figure dans la liste des applications lancées dans l'environnement protégé par défaut.

Le lancement de l'application dans l'environnement protégé s'opère conformément au mode sélectionné. Afin de pouvoir lancer rapidement une application dans l'environnement protégé, il est possible de créer des raccourcis.

Pour que pendant le fonctionnement dans l'environnement normal les fichiers enregistrés ou modifiés dans l'environnement protégé soient accessibles, il faut utiliser le Dossier partagé de la Sandbox, spécialement créé et accessible aussi bien dans l'environnement protégé que dans l'environnement normal. Les fichiers placés dans ce dossier ne seront pas supprimés en cas de purge de l'environnement protégé (cf. page 88).

Il est recommandé d'installer les applications avec lesquelles vous envisagez de travailler dans l'environnement protégé dans l'environnement normal Microsoft Windows.

DANS CETTE SECTION

LANCEMENT D'UNE APPLICATION DANS L'ENVIRONNEMENT PROTEGE

Si le mode **Toujours exécuter en environnement protégé** a été sélectionné pour l'application, celle-ci pourra être lancée dans l'environnement protégé d'une des manières suivantes :

- depuis le menu contextuel de Microsoft Windows ;
- depuis la fenêtre principale de Kaspersky Internet Security (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) ;
- via un raccourci créé (cf. section "Création de raccourcis pour le lancement d'applications" à la page 85) au préalable.

Si le mode **Toujours exécuter en environnement protégé** a été sélectionné pour l'application, celle-ci sera lancée dans l'environnement protégé quel que soit le mode d'exécution.

Les applications lancées dans l'environnement protégé sont marquées par le cadre vert autour de la fenêtre de l'application. Aussi, elles sont soulignées par la couleur verte dans la liste des applications controlées par le Contrôle des Applications (cf. section "Contrôle des Applications" à la page 74.

Pour lancer une application dans l'environnement protégé à l'aide d'un raccourci, procédez comme suit :

1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.
2. Lancez l'application à l'aide d'un double-clic sur le raccourci.

Pour lancer l'application dans l'environnement protégé depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans la partie inférieure de la fenêtre, sélectionnez l'icône de l'application requise.
4. Exécutez l'application en double-cliquant sur son icône ou choisissez l'option **Exécuter** dans le menu contextuel.

Pour lancer l'application dans l'environnement protégé depuis le menu contextuel de Microsoft Windows, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le nom de l'objet sélectionné : le raccourci ou le fichier exécutable de l'application.
2. Dans le menu déroulant, sélectionnez **Exécuter en environnement protégé**.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'APPLICATIONS

Afin de pouvoir lancer rapidement les applications dans l'environnement protégé, vous pouvez créer des raccourcis dans Kaspersky Internet Security. Il vous sera ainsi possible de lancer l'application requise dans l'environnement protégé sans devoir ouvrir la fenêtre principale de l'application ou le menu contextuel de Microsoft Windows.

Pour créer un raccourci pour le lancement d'applications dans l'environnement protégé, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans le champ **Applications exécutées en environnement protégé** de la partie inférieure de la fenêtre, sélectionné l'icône de l'application souhaitée.
4. Cliquez avec le bouton droit de la souris pour ouvrir le menu contextuel et choisissez l'option **Créer un raccourci**.
5. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci. Les raccourcis sont créés par défaut dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur et ils portent le nom du processus de l'application.

COMPOSITION DE LA LISTE DES APPLICATIONS LANCEES DANS L'ENVIRONNEMENT PROTEGE

Dans la fenêtre principale de l'application vous pouvez créer la liste des applications lancées dans l'environnement protégé. La liste est présentée dans la section **Contrôle des Applications**.

Si vous ajoutez dans la liste l'application, qui permet de fonctionner en même temps avec plusieurs propres copies (par exemple, Windows Internet Explorer), alors après l'ajout dans la liste chaque sa nouvelle copie fonctionnera en environnement protégé. Lors de l'ajout dans la liste de l'application, qui permet d'utiliser uniquement une de ses copies, il faudra la redémarrer après l'ajout.

Pour ajouter une application à la liste des applications de l'environnement protégé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans la partie inférieure de la fenêtre, champ **Applications exécutées en environnement protégé**, cliquez sur le lien **Ajouter**.
4. Sélectionnez l'application dans le menu déroulant. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution. Après cela, l'icône de l'application sera ajoutée au champ.

   Pour supprimer une application de la liste des applications lancées dans l'environnement protégé, sélectionnez-la puis cliquez sur le lien **Supprimer**.

SELECTION DU MODE : LANCEMENT D'UNE APPLICATION

Par défaut, toutes les applications installées peuvent être lancées en mode normal ou dans l'environnement protégé. Lorsqu'une application est ajoutée à la liste des applications lancées dans l'environnement protégé, il est possible de l'associer au mode **Toujours exécuter en environnement protégé**. Cela signifie que l'application sera lancer dans l'environnement protégé quel que soit le mode d'exécution : via les méthodes standard de Microsoft Windows ou via les méthodes de Kaspersky Internet Security.

Il n'est pas recommandé d'utiliser le mode **Toujours exécuter en environnement protégé** pour les applications de système et les utilitaires, puisque cela peut amener au fonctionnement incorrect du système d'exploitation.

Pour qu'une application soit toujours lancée dans l'environnement protégé, quel que soit le mode d'exécution, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans la partie inférieure, sélectionnez l'icône de l'application requise.
4. Ouvrez le menu contextuel en cliquant sur le bouton droit de la souris.
5. Sélectionnez l'option **Toujours exécuter en environnement protégé**. Une coche apparaîtra à côté de l'option dans le menu .

   Pour que l'application soit lancée en mode normal, sélectionnez à nouveau cette option dans le menu.

SELECTION DU MODE : PURGE DES DONNEES DE L'ENVIRONNEMENT PROTEGE

Lors du lancement de l'application dans l'environnement protégé, toutes les modifications (qui sont la conséquence du fonctionnement de l'application) se passent uniquement dans le cadre de l'environnement protégé. Par défaut, au prochain lancement de l'application, toutes les modifications introduites et les fichiers enregistrés seront à nouveau accessible au cours de la séance dans l'environnement protégé.

Si les données sauvegardées dans l'environnement protégé ne sont plus nécessaires, il est possible de les purger (cf. page 88).

Si vous ne souhaitez pas que les modifications introduites pour une application quelconque soient accessibles au prochain lancement dans l'environnement protégé, vous pouvez activer le mode **Purger les données de l'environnement protégé à la fermeture**. Cela signifie que les modifications introduites durant la séance de fonctionnement de l'application seront perdues. Les applications lancées dans ce mode sont accompagnées de l'icône .

Pour que les données de l'environnement protégé soient purgées chaque fois que l'application est arrêtée, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans la partie inférieure, sélectionnez l'icône de l'application requise.
4. Ouvrez le menu contextuel en cliquant sur le bouton droit de la souris.
5. Sélectionnez l'option **Purger les données de l'environnement protégé à la fermeture**. Une coche apparaîtra à côté de l'option dans le menu

   et l'icône apparaîtra sur l'icône de l'application dans la liste des applications lancées dans l'environnement protégé. .

   Pour que les données sauvegardées pendant le fonctionnement de l'application dans l'environnement protégé ne soient pas purgées à la fin du fonctionnement de l'application, sélectionnez à nouveau ce point.

UTILISATION DU DOSSIER PARTAGE

Lors du fonctionnement dans l'environnement protégé, toutes les modifications (qui sont la conséquence du fonctionnement de l'application) se passent uniquement dans le cadre de l'environnement protégé et n'exercent pas une

influence sur l'environnement normal. De ce fait, les fichiers sauvegardés dans l'environnement protégé, ne se trouvent pas dans l'environnement normal.

Pour que les fichiers utilisés dans l'environnement protégé soient accessibles dans l'environnement normal, Kaspersky Internet Security a prévu la possibilité d'utiliser le *Dossier partagé de la Sandbox*. Tous les fichiers enregistrés dans ce dossier durant l'utilisation de l'environnement protégé seront accessibles dans l'environnement normal.

Le répertoire partagé est un répertoire sur le disque dur créé pendant l'installation de Kaspersky Internet Security.

Le Dossier partagé est créé dans le dossier *%AllUsersProfile%\Application Data\Kaspersky Lab\SandboxShared* pendant l'installation de l'application, et il est impossible de modifier son emplacement.

Dans l'Assistant de Microsoft Windows, le répertoire partagé est indiqué par l'icône . Il est possible également d'accéder au répertoire partagé depuis la fenêtre principale de Kaspersky Internet Security.

Pour ouvrir le répertoire partagé depuis la fenêtre principale de Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Cliquez sur le lien **Dossier partagé**. Le répertoire s'ouvrir dans une fenêtre standard de Microsoft Windows.

PURGE DE L'ENVIRONNEMENT PROTEGE

S'il vous est nécessaire de supprimer les données de l'environnement protégé, ou rétablir (pour toutes les applications lancées) les paramètres actuels dans l'environnement normal Microsoft Windows, vous purger l'environnement protégé.

Avant de purger les données enregistrés dans l'environnement protégé, il convient de s'assurer que toutes les informations dont vous pourriez avoir besoin ultérieurement se trouvent dans le dossier partagé. Dans le cas contraire, les données seront supprimées et il sera impossible de les rétablir.

Pour purger les données de l'environnement protégé, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Contrôle des Applications**.
3. Dans la partie inférieure de la fenêtre, champ **Applications exécutées en environnement protégé**, cliquez sur le lien **Purger**.
4. Dans la fenêtre qui s'ouvre, confirmez la purge des données en cliquant sur **OK** ou cliquez sur **Annuler** afin de ne pas réaliser la purge.

PARE-FEU

Afin de protéger votre travail sur les réseaux locaux et sur Internet, Kaspersky Internet Security vous propose un composant spécial : le *Pare-feu*. Il filtre toute l'activité de réseau selon deux types de règles : *les règles pour les applications* et *les règles pour les paquets*.

Le Pare-feu analyse les paramètres de réseau, aux quels vous couplez l'ordinateur. Si l'application fonctionne en mode interactif (cf. section "Utilisation du mode de protection interactif" à la page 159), le Pare-feu vous informera de l'état du réseau contacté lors de la première connexion. Si le mode interactif est désactivé, le Pare-feu déterminera l'état en fonction du type de réseau, de la plage d'adresses et d'autres caractéristiques. Selon l'état de réseau, le Pare-feu applique des règles différentes pour le filtrage de l'activité de réseau.

Afin de modifier les paramètres de fonctionnement du Pare-Feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous les onglets **Règles de filtrage** et **Réseaux** modifiez les paramètres de fonctionnement du **Pare-feu**.

DANS CETTE SECTION

MODIFICATION DE L'ETAT DU RESEAU

Toutes les connexions de réseau établies sur votre ordinateur sont contrôlées par le Pare-feu. Le Pare-feu attribue à chaque connexion un état déterminé et applique diverses règles de filtrage de l'activité de réseau en fonction de cet état.

Lors d'une connexion à un nouveau réseau, le pare-feu affiche un message (cf. page 211). Afin de choisir le mode de filtrage de l'activité de réseau, il faut attribuer un *état* au réseau découvert. Choisissez l'un des états suivants :

- **Réseau public (Internet)**. Cet état est recommandé pour les réseaux non protégés par les applications d'antivirus quelconques, les pare-feux, les filtres (ex : pour les réseaux des café Internet). Les utilisateurs de ce genre de réseau ne peuvent accéder aux fichiers et aux imprimantes de votre ordinateur. Même si vous avez créé un dossier partagé, les informations qu'il contient ne seront pas accessibles aux utilisateurs d'un-réseau de ce type. Si vous avez autorisé l'accès à distance au Bureau, les utilisateurs de ce réseau n'y auront pas droit. Le filtrage de l'activité réseau de chaque application s'effectue aux termes des règles pour cette application. Cet état est attribué au réseau Internet par défaut.
- **Réseau local**. Cet état est recommandé pour les réseaux aux utilisateurs desquels vous faites suffisamment confiance pour autoriser l'accès aux fichiers et aux imprimantes de votre ordinateur (par exemple, réseau interne d'une entreprise ou réseau domestique).

- **Réseau de confiance**. Cet état doit être réservé aux zones qui, d'après vous, ne présentent aucun danger car l'ordinateur ne risque pas d'être attaqué ou victime d'un accès non autorisé. Le choix de cet état implique l'autorisation de n'importe quelle activité de réseau dans le cadre de ce réseau.

Les types de l'activité réseau, autorisés pour les réseaux avec l'état déterminé, dépendent des paramètres des règles paquets, établis par défaut. Vous pouvez changer ces règles.

L'état du réseau définit la liste des règles qui sont utilisées pour le filtrage de l'activité réseau, correspondant à ce réseau.

Pour changer l'état de la connexion réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Réseau**, sélectionnez la connexion de réseau active puis, cliquez sur le lien **Modifier**.
5. Dans la fenêtre qui s'ouvre, sous l'onglet **Propriétés**, sélectionnez l'état requis dans la liste déroulante.

EXTENSION DE LA PLAGE D'ADRESSES DE RESEAU

Une ou plusieurs plages d'adresses IP correspondent à un réseau. Si vous vous connectez à un réseau dont l'accès aux sous-réseaux s'opère via un routeur, vous pouvez ajouter manuellement les sous-réseaux accessibles via celui-ci.

Exemple : vous vous connectez au réseau d'un des bureaux de votre société et vous souhaitez que les règles de filtrage soient identiques pour le bureau auquel vous êtes connecté et pour les bureaux accessibles via Internet.

Demandez à l'administrateur de réseau de vous communiquer les plages d'adresses des réseaux de ces bureaux et ajoutez-les.

Pour élargir la page d'adresses de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Réseau**, sélectionnez la connexion de réseau active puis, cliquez sur le lien **Modifier**.
5. Dans la fenêtre qui s'ouvre, onglet **Propriétés**, groupe **Sous-réseaux complémentaires**, cliquez sur le lien **Ajouter**.
6. Dans la fenêtre **Adresse IP** qui s'ouvre, saisissez l'adresse IP ou le masque d'adresses.

SELECTION DU MODE DE NOTIFICATION SUR LES MODIFICATIONS DU RESEAU

Les paramètres des connexions de réseau peuvent changer pendent l'utilisation. Vous pouvez recevoir des notifications relatives aux modifications suivantes :

- Lors de la connexion au réseau.

- Lors de la modification de l'équivalence entre l'adresse MAC et l'adresse IP Cette notification s'ouvre lors du changement d'adresse IP d'un des ordinateurs du réseau.

- Lors de l'apparition de l'adresse MAC. Cette notification s'ouvre lors de l'apparition d'un nouvel ordinateur dans le réseau.

Pour activer les notifications relatives aux modifications des paramètres des connexions de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Réseau**, sélectionnez la connexion de réseau active puis, cliquez sur le lien **Modifier**.

5. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, cochez les cases des événements au sujet desquels vous souhaitez être averti.

LES PARAMETRES COMPLEMENTAIRES DE FONCTIONNEMENT DU PARE-FEU

Les paramètres avancés du fonctionnement du Pare-feu reprennent les éléments suivants :

- Autorisation du mode FTP actif. Le mode actif suppose qu'un port sera ouvert sur le poste client pour la connexion entre celui-ci et le serveur. Le serveur établit ensuite la connexion (à la différence du mode passif où le client établit lui-même la connexion avec le serveur). Le mode permet de contrôler quel port exactement sera ouvert. Le mécanisme fonctionne même si une règle d'interdiction a été créée. Par défaut, le mode FTP actif est autorisé.

- Blocage de la connexion, s'il est impossible de confirmer l'action (l'interface de l'application n'est pas chargée). Le paramètre permet de ne pas suspendre le fonctionnement du Pare-feu quand l'interface de Kaspersky Internet Security n'est pas chargée. L'action est exécutée par défaut.

- Fonctionnement du Pare-feu avant l'arrêt complet du système. Le paramètre permet de ne pas arrêter le Pare-feu avant l'arrêt complet du système. L'action est exécutée par défaut.

Afin de définir les paramètres avancés de fonctionnement du Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, cliquez sur le lien **Avancé**.

5. Dans la fenêtre **Avancé** qui s'ouvre, assurez-vous que les cases adéquates sont cochées.

REGLES DU PARE-FEU

Une règle du Pare-feu est une action que le Pare-feu exécute lorsqu'il détecte une tentative de connexion selon des paramètres déterminés : sens et protocole de transfert des données, plage d'adresses et de ports intervenant dans la connexion.

Le Pare-feu fonctionne sur la base de règles de deux types :

- *Les règles de paquet* (cf. section "Création d'une règle pour un paquet" à la page 92) sont utilisées pour définir les restrictions pour les paquets et les flux de données peu importe les applications.

- *Les règles pour les applications* (cf. section "Création de règles pour l'application" à la page 93) sont utilisées pour définir les restrictions pour l'activité de réseau d'une application particulière. Ces règles permettent de configurer en détail le filtrage lorsque, par exemple, un type déterminé de flux de données est interdit pour certaines applications mais autorisé pour d'autres.

La priorité des règles pour les paquets est plus élevée que la priorité des règles pour les applications. Si des règles pour les paquets et des règles pour les applications sont définies pour la même activité de réseau, celle-ci sera traitée selon les règles pour les paquets.

VOIR EGALEMENT

CREATION D'UNE REGLE POUR UN PAQUET

Le plus souvent, les règles pour les paquets limitent l'activité de réseau entrante sur des ports particuliers des protocoles TCP et UDP et filtrent les messages ICMP¨.

Une règle pour un paquet est un ensemble de conditions et d'actions à réaliser sur les paquets et les flux de données lorsque les conditions définies sont vérifiées.

Au moment de créer des règles pour les paquets, n'oubliez pas qu'elles ont priorité sur les règles pour les applications.

Au moment de définir les conditions de la règle, vous devez indiquer le service de réseau et l'adresse de réseau. En guise d'adresse de réseau, vous pouvez utiliser l'adresse IP ou désigner l'état du réseau. Dans le dernier cas, les adresses proviennent de tous les réseaux connectés à ce moment et possédant l'état indiqué.

Pour créer une règle pour les paquets, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, sélectionnez le groupe **Règles pour les paquets** puis cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Règle de réseau** qui s'ouvre, configurez les paramètres de la règle.

6. Définissez la priorité de la règle créée.

Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case ☑ en regard de son nom.

CREATION DE REGLES POUR L'APPLICATION

Le pare-feu analyse l'activité de chaque application lancée sur l'ordinateur. En fonction du degré de danger, chaque application, après la première exécution, sera placée dans un des groupes suivants :

- **De confiance**. N'importe quelle activité de réseau, quel que soit l'état du réseau, est autorisée pour les applications de ce groupe.
- **Restrictions faibles**. N'importe quelle activité de réseau en mode automatique est autorisée pour les applications de ce groupe. En mode interactif, des messages qui vous permettent d'autoriser ou d'interdire une connexion ou de créer une règle à l'aide d'un Assistant (cf. section "Assistant de rédaction de règles" à la page 94) apparaissent.
- **Restrictions fortes**. N'importe quelle activité de réseau en mode automatique est interdite pour les applications de ce groupe. En mode interactif, des messages qui vous permettent d'autoriser ou d'interdire une connexion ou de créer une règle à l'aide d'un Assistant (cf. section "Assistant de rédaction de règles" à la page 94). apparaissent.
- **Douteuses**. N'importe quelle activité de réseau est interdite pour les applications de ce groupe.

Vous pouvez modifier les règles pour le groupe entier ou pour une application en particulier ainsi que créer des règles complémentaires pour un filtrage plus précis de l'activité de réseau.

Les règles définies par l'utilisateur pour des applications en particulier ont une priorité supérieure à celle des règles héritées du groupe.

Une fois que le Pare-feu a analysé l'activité de l'application, il crée une règle qui définit l'accès de l'application aux réseaux répondant à un état défini. Vous pouvez créer des règles complémentaires qui permettront de gérer avec une plus grande souplesse l'activité de réseau de Kaspersky Internet Security.

Pour créer une règle pour l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage** sélectionnez le groupe de règles pour l'application puis cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle de réseau** qui s'ouvre, configurez les paramètres de la règle.
6. Définissez la priorité de la règle créée.

Une fois que vous aurez créé une règle, vous pourrez modifier ses paramètres ou la supprimer à l'aide des liens de la partie inférieure de l'onglet. Pour désactiver une règle, décochez la case ☑ en regard de son nom.

ASSISTANT DE REDACTION DE REGLES

Lorsqu'une règle dont l'action est **Confirmer** (cette action est choisie par défaut pour les applications appartenant aux groupes (cf. section "Groupes d'applications" à la page 76) **Restrictions faibles** ou **Restrictions élevées**) se déclenche, une notification (cf. page 211) apparaît. La fenêtre des notifications vous permet de sélectionner une des options suivantes :

- **Autoriser**.
- **Interdire**.
- **Créer une règle**. Le choix de cette sélection entraîne l'ouverture de *l'Assistant de création de règle* qui vous aidera à créer la règle pour régir l'activité de réseau de l'application.

L'action associée à la règle peut devenir **Autoriser** ou **Interdire** ; pour cela, il faut cochez la case **Enregistrer pour cette application**.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

SELECTION DE L'ACTION EXECUTEE PAR LA REGLE

Lorsque la règle est appliquée, le Pare-feu réalise une des actions suivantes sur le paquet ou le flux de données :

- **Autoriser**.
- **Bloquer**.
- **Traiter selon les règles pour les applications**. Dans ce cas le traitement du paquet ou du flux de données par la règle paquet se termine. Les règles pour les applications sont appliquées à la connexion.

Si vous souhaitez consigner les informations relatives à la tentative de connexion et aux actions du Pare-feu dans le rapport, activez le mode **Consigner dans le rapport.**

Afin de modifier le mode de fonctionnement du Pare-Feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle de réseau** qui s'ouvre, dans le groupe **Action** sélectionnez l'action requise.

CONFIGURATION DES PARAMETRES DU SERVICE DE RESEAU

Les paramètres qui définissent l'activité de réseau pour laquelle la règle est créée sont décrits par le *service de réseau*. Le service de réseau possède les paramètres suivants :

- *Nom*. Ce texte apparaît dans la liste les services de réseau qui peuvent être sélectionnés.
- *Direction*. Le pare-feu contrôle les connexions dans les sens suivants :
  - **Entrant**. La règle est applicable pour les paquets de données, admis par votre ordinateur. N'est pas applicable pour les règles des applications.

- **Entrant (flux)**. La règle s'applique aux connexions de réseau ouvertes par un ordinateur distant.
- **Entrant / sortant**. La règle s'applique aux paquets ou aux flux de données entrant et sortant quel que soit l'ordinateur (le vôtre ou le distant) à l'origine de la connexion de réseau.
- **Sortant**. La règle concerne les paquets de données transmis depuis votre ordinateur. N'est pas applicable pour les règles des applications.
- **Sortant (flux)**. La règle s'applique exclusivement aux connexions de réseau ouvertes par votre ordinateur.

- *Protocole*. Le Pare-feu contrôle la connexion selon les protocoles TCP, UDP, ICMP, ICMPv6, IGMP et GRE. Si vous avez sélectionné le protocole ICMP ou ICMPv6, vous pouvez définir le type et le code de paquet ICMP.

Les règles pour les applications contrôlent les connexions uniquement sur les protocoles TCP et UDP.

- *Ports distants et locaux*. Pour les protocoles TCP et UDP vous pouvez définir les ports de votre poste et du poste distant. La connexion entre eux sera contrôlée.

Kaspersky Internet Security contient des services de réseau qui décrivent les connexions de réseau les plus souvent utilisées. Lors de la création de règle du Pare-feu, vous pouvez sélectionner un des services de réseau proposés ou en créer un nouveau.

Pour configurer les paramètres de la connexion réseau traitée par la règle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle de réseau** qui s'ouvre, groupe **Service de réseau**, cliquez sur le lien **Ajouter**.
6. Dans la fenêtre **Service de réseau** qui s'ouvre, configurez les paramètres de la connexion de réseau.

SELECTION DE LA PLAGE D'ADRESSES

La règle du Pare-feu s'applique aux adresses de réseau des catégories suivantes :

- **Adresse quelconque** : la règle s'applique à n'importe quelle adresse IP ;
- **Adresse de sous-réseau avec l'état** : la règle s'appliquera aux adresses IP de tous les réseaux connectés en ce moment et possédant l'état indiqué ;
- **Adresses du groupe** : la règle s'appliquera aux adresses IP reprises dans la plage définie.

Pour définir la plage des adresses IP, auxquels la règle sera applicable, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Pare-feu** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles de filtrage**, cliquez sur le lien **Ajouter**.

5. Dans la fenêtre **Règle de réseau** qui s'ouvre, groupe **Adresses**, définissez la plage d'adresses :

   a. sélectionnez l'état du réseau dans la liste déroulante si vous avez choisi l'option **Adresse de sous-réseau avec l'état** ;

   b. sélectionnez un des groupes d'adresses existants si vous avez sélectionné l'option **Adresse du groupe**. Si la plage d'adresses d'aucun des groupes ne vous convient, définissez-en une nouvelle. Pour ce faire, cliquez sur le lien **Ajouter** dans la partie inférieure du groupe et dans la fenêtre **Adresses de réseau** qui s'ouvre, saisissez les adresses appartenant au groupe.

DEFENSE PROACTIVE

Kaspersky Internet Security offre une protection non seulement contre les menaces connues mais également contre les nouvelles menaces qui ne figurent pas dans les bases de Kaspersky Internet Security. Cette possibilité est garantie par un composant développé spécialement – la *Défense Proactive*.

Les technologies préventives sur lesquelles repose la défense proactive évitent ces pertes de temps et permettent de neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. A la différence des technologies réactives qui réalisent l'analyse selon les enregistrements des bases de Kaspersky Internet Security, les technologies préventives identifient les nouvelles menaces en suivant les séquences d'actions exécutées par une application quelconque. Si l'analyse de la séquence d'actions de l'application éveille des soupçons, Kaspersky Internet Security bloque l'activité de cette application.

L'analyse de l'activité a lieu pour toutes les applications, y compris pour celles placées dans le groupe **De confiance** par le composant Contrôle des Applications (à la page 74). Vous pouvez désactiver les notifications de la Défense Proactive pour ces applications.

A la différence du composant Contrôle des Applications, la Défense Proactive réagit précisément à la séquence d'actions du programme.

Afin de modifier les paramètres de fonctionnement de la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, introduisez les modifications requises dans les paramètres.

DANS CETTE SECTION

UTILISATION DE LA LISTE DES ACTIVITES DANGEREUSES

N'oubliez pas que la configuration du contrôle de l'activité dans Kaspersky Internet Security installé sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64 est différente de la configuration pour Kaspersky Internet Security installé sous d'autres systèmes d'exploitation.

Particularités de la configuration du contrôle de l'activité des applications sous Microsoft Windows XP

Kaspersky Internet Security surveille l'activité des applications sur votre ordinateur. La Défense Proactive réagit à une séquence définie d'actions de l'application quelconque. Ainsi, si un programme se copie dans une ressource de réseau, dans le répertoire de démarrage, dans la base de registres et qu'il diffuse ces copies, on peut affirmer sans crainte qu'il s'agit d'un ver. Parmi les séquences d'actions dangereuses, citons également :

- actions typiques des chevaux de Troie ;

- tentative d'interception des saisies au clavier ;
- installation cachée de pilotes ;
- tentative de modification du noyau du système d'exploitation ;
- tentative de création d'objets cachés et de processus avec un identifiant (PID) négatif ;
- tentative de modification du fichier HOSTS ;
- tentative d'intrusion dans un autre processus ;
- apparition d'un processus cherchant a réorienté les données entrantes/sortantes ;
- tentative d'envoi des demandes DNS.

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Internet Security et il est impossible de la modifier. Vous pouvez néanmoins refuser de contrôler une activité dangereuse.

Pour refuser de contrôler une activité dangereuse, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Défense Proactive** qui s'ouvre, décochez la case  située en regard du nom de l'activité dont vous refusez le contrôle.

Particularités de la configuration du contrôle de l'activité des applications sous Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou Microsoft Windows 7 x64

Si l'ordinateur tourne sous un des systèmes d'exploitation cités ci-dessus, alors certains événements ne seront pas contrôlés. Ceci s'explique par les particularités de ces systèmes d'exploitation. Ainsi, les types suivants d'événements ne seront pas contrôlés : *envoi des données par les applications de confiance*, *activité suspecte dans le système*.

MODIFICATION D'UNE REGLE DE CONTROLE DE L'ACTIVITE DANGEREUSE

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Internet Security et il est impossible de la modifier. Vous pouvez :

- refuser de contrôler une activité quelconque (cf. page 97) ;
- modifier la règle qui définit le fonctionnement de la défense proactive lors de la découverte d'activités dangereuses.
- composer une liste d'exclusions (cf. page 174), reprenant les applications que vous n'estimez pas dangereuses.

Afin de modifier une règle, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Défense Proactive** qui s'ouvre, dans le groupe **Evénements** sélectionnez l'événement nécessaire, pour lequel la règle sera modifiée.

5. Pour l'événement sélectionné, configurez les paramètres nécessaires de la règle à l'aide des liens dans le bloc de description de la règle :

   - cliquez sur le lien indiquant l'action établie et dans la fenêtre **Sélection des actions** ouverte, sélectionnez l'action nécessaire parmi les actions proposées ;

   - cliquez sur le lien indiquant la période (n'est pas définie pour tous les types d'activité) et dans la fenêtre **Découverte des processus cachés** ouverte, indiquez l'intervalle selon lequel la recherche de découverte des processus cachés s'exécutera ;

   - cliquez sur le lien Act. / Désact., pour indiquer la nécessité de créer un rapport sur l'opération exécutée.

CONSTITUTION D'UN GROUPE D'APPLICATIONS DE CONFIANCE

Les applications placées par le Contrôle des Applications dans le groupe (cf. section "Groupes d'applications" à la page 76) **De confiance** ne constituent aucun danger pour le système. Toutefois, leur activité est également contrôlée par la Défense Proactive.

Exploitez la possibilité de définir le cercle de programmes de confiance dont l'activité ne sera pas analysée par la Défense proactive. Les applications de confiance peuvent être les applications possédant une signature numérique ou les applications présentes dans la base de Kaspersky Security Network.

Pour que la Défense proactive considère comme programme de confiance tout programme doté d'une signature numérique et/ou repris dans la base de Kaspersky Security Network et ne vous communique aucune information relative à l'activité, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cochez les cases ☑ **Avec une signature numérique (Editeurs connus)** et / ou
   ☑ **Présentes dans la base de Kaspersky Security Network** dans le groupe **Applications de confiance**.

CONTROLE DES COMPTES UTILISATEUR SYSTEME

Les comptes utilisateur réglementent l'accès au système et définissent l'utilisateur et son environnement de travail, ce qui permet d'éviter d'endommager le système d'exploitation ou les données des autres utilisateurs. Les processus système sont les processus qui ont été lancés par le compte système.

Pour que Kaspersky Internet Security surveille l'activité des processus système, ceci excluant les processus utilisateurs, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Défense Proactive** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cochez la case ☑ **Contrôler les comptes Systèmes** dans le groupe **Avancé**.

PROTECTION CONTRE LES ATTAQUES DE RESEAU

La Prévention des intrusions est lancée au démarrage du système d'exploitation et surveille l'activité du trafic entrant caractéristique des attaques de réseau. Dès qu'il décèle une tentative d'attaque contre votre ordinateur, Kaspersky Internet Security bloque toute activité de réseau de l'ordinateur qui vous attaque. Le blocage dure par défaut pendant une heure. Un message vous avertit (cf. section "Notifications" à la page 205) qu'une attaque de réseau a été menée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

Les descriptions des attaques de réseau connues à l'heure actuelle (cf. section "Types d'attaques de réseau identifiées" à la page 100) et les moyens de lutter contre celles-ci figurent dans les bases de Kaspersky Internet Security. L'enrichissement de la liste avec les attaques découvertes par la Protection contre les attaques de réseau a lieu lors de la mise à jour (cf. section "Mise à jour" à la page 150) des bases.

DANS CETTE SECTION

BLOCAGE DES ORDINATEURS A L'ORIGINE DE L'ATTAQUE

Par défaut la Prévention des intrusions (à la page 100) bloque l'activité de l'ordinateur attaquant durant une heure.

- *Pour modifier la durée du blocage de l'ordinateur attaquant, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Prévention des intrusions** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, cochez la case **Ajouter l'ordinateur à l'origine de l'attaque à la liste de blocage pendant** puis définissez la durée du blocage.

- *Afin d'annuler le blocage de l'ordinateur en attaque, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et choisissez la rubrique **Protection**.
  2. Dans la partie droite de la fenêtre, rubrique **Utilisation d'Internet**, cliquez sur le lien **Surveillance du réseau**.
  3. Dans la fenêtre **Ordinateurs bloqués** qui s'ouvre, sélectionnez l'ordinateur bloqué puis cliquez sur le lien **Débloquer**.

TYPES D'ATTAQUES DE RESEAU IDENTIFIEES

Il existe actuellement une grande diversité d'attaques de réseau qui exploitent aussi bien les failles des systèmes d'exploitation ou celles d'applications système ou autre.

Afin de garantir la protection de l'ordinateur en permanence, il est bon de connaître les menaces qui planent sur lui. Les attaques de réseau connues peuvent être scindées en trois grands groupes :

1. *Balayage des ports* : ce type de menace n'est pas une attaque en tant que telle mais elle devance d'habitude l'attaque car il s'agit d'une des principales manières d'obtenir des informations sur le poste distant. Cette méthode consiste à balayer les ports UDP/TCP utilisés par les services de réseau sur l'ordinateur convoité afin de définir leur état (ouvert ou fermé).

   Le balayage des ports permet de comprendre les types d'attaque qui pourraient réussir. De plus, les informations obtenues suite au balayage donnent au malfaiteur une idée du système d'exploitation utilisé sur l'ordinateur distant. Ceci limite encore plus le cercle des attaques potentielles et, par conséquent, le temps consacré à leur organisation et cela permet également d'utiliser des vulnérabilités propres à ce système d'exploitation.

2. *Les attaques par déni de service* sont des attaques qui rendent le système pris pour cible instable ou totalement inopérationnel. Parmi les conséquences de genre d'attaque, citons l'impossibilité d'utiliser les ressources d'information ciblées par l'attaque (par exemple, impossible d'accéder à Internet).

   Il existe deux types principaux d'attaques DoS :

   - envoi vers la victime de paquets spécialement formés et que l'ordinateur n'attend pas. Cela entraîne une surcharge ou un arrêt du système ;

   - envoi vers la victime d'un nombre élevé de paquets par unité de temps; l'ordinateur est incapable de les traiter, ce qui épuise les ressources du système.

   Voici des exemples frappants de ce groupe d'attaques :

   - *L'attaque Ping of death* : envoi d'un paquet ICMP dont la taille dépasse la valeur admise de 64 Ko. Cette attaque peut entraîner une panne dans certains systèmes d'exploitation.

   - *L'attaque Land* consiste à envoyer vers le port ouvert de votre ordinateur une requête de connexion avec lui-même. Suite à cette attaque, l'ordinateur entre dans une boucle, ce qui augmente sensiblement la charge du processeur ainsi qu'entraîne une panne éventuelle du système d'exploitation.

   - *L'attaque ICMP Flood* consiste à envoyer vers l'ordinateur de l'utilisateur un grand nombre de paquets ICMP. Cette attaque fait que l'ordinateur est obligé de répondre à chaque nouveau paquet, ce qui entraîne une surcharge considérable du processeur.

   - *L'attaque SYN Flood* consiste à envoyer vers votre ordinateur un nombre élevé de requêtes pour l'ouverture d'une connexion. Le système réserve des ressources définies pour chacune de ces connexions. Finalement, l'ordinateur gaspille toutes ses ressources et cesse de réagir aux autres tentatives de connexion.

3. *Attaques d'intrusion* qui visent à s'emparer du système. Il s'agit du type d'attaque le plus dangereux car en cas de réussite, le système passe entièrement aux mains du malfaiteur.

   Ce type d'attaque est utilisé lorsque l'individu mal intentionné doit absolument obtenir des informations confidentielles sur l'ordinateur distant (par exemple, numéro de carte de crédit, mots de passe) ou simplement pour s'introduire dans le système en vue d'utiliser ultérieurement les ressources au profit du malfaiteur (utilisation du système dans un réseau de zombies ou comme base pour de nouvelles attaques).

   Ce groupe reprend le plus grand nombre d'attaques. Elles peuvent être réparties en trois sous-groupes en fonction du système d'exploitation utilisés par les victimes : attaques sous Microsoft Windows, attaques sous Unix et un groupe commun pour les services de réseau utilisés dans les deux systèmes d'exploitation.

   Les attaques utilisant les services de réseau du système d'exploitation les plus répandues sont :

   - *Les attaques de débordement du tampon* : type de vulnérabilité dans un logiciel qui résulte de l'absence de contrôle (ou de contrôle insuffisant) lors de la manipulation de données massives. Il s'agit de l'une des vulnérabilités les plus anciennes et des plus faciles à exploiter.

   - *Les attaques qui reposent sur des erreurs dans les chaînes de format* : type de vulnérabilités dans les applications qui résultent d'un contrôle insuffisant des valeurs des paramètres entrée de la fonction d'entrée/de sortie de format de type *printf()*, *fprintf()*, *scanf()* ou autres de la bibliothèque standard du langage C. Lorsqu'une telle vulnérabilité est présente dans un logiciel, le malfaiteur, qui peut envoyer des requêtes formulées spécialement, peut prendre le contrôle complet du système.

Système de détection des intrusions analyse automatiquement l'utilisation de telles vulnérabilité et les bloque dans les services de réseau les plus répandus (FTP, POP3, IMAP), s'ils fonctionnent sur l'ordinateur de l'utilisateur.

Les attaques ciblant les ordinateurs tournant sous Microsoft Windows, repose sur l'exploitation de vulnérabilités d'un logiciel installée (par exemple, des programmes tels que Microsoft SQL Server, Microsoft Internet Explorer, Messenger ainsi que les composants systèmes accessibles via le réseau tels que DCom, SMB, Wins, LSASS, IIS5).

De plus, dans certains cas, les attaques d'intrusion exploitent divers types de scripts malveillants, y compris des scripts traités par Microsoft Internet Explorer et diverses versions du ver Helkern. L'attaque Helkern consiste à envoyer vers l'ordinateur distant des paquets UDP d'un certain type capable d'exécuter du code malveillant.

ANTI-SPAM

Kaspersky Internet Security propose l'*Anti-Spam*, un composant spécial capable d'identifier le courrier indésirable (spam) et de le traiter conformément aux règles de votre client de messagerie, ce qui permet de gagner du temps lors de l'utilisation du courrier électronique.

L'Anti-Spam utilise l'Algorithme d'auto-apprentissage (cf. section "Algorithme de fonctionnement du composant" à la page 104), ce que permet au composant de distinguer d'une façon exacte avec le temps le spam et le courrier utile. Le contenu du message constitue la source de données pour l'algorithme. Afin que l'Anti-Spam puisse établir efficacement une distinction entre courrier indésirable et courrier normal, il faut l'entraîner (cf. section "Entraînement de l'Anti-Spam" à la page 106).

Il est vivement recommandé d'étudier l'algorithme de fonctionnement de l'Anti-Spam !

L'Anti-Spam se présente sous la forme d'un plug-in dans les clients de messagerie suivants :

- Microsoft Office Outlook (cf. section "Configuration du traitement du courrier indésirable dans Microsoft Office Outlook" à la page 119) ;
- Microsoft Outlook Express (Windows Mail) (cf. section "Configuration du traitement du courrier indésirable dans Microsoft Outlook Express (Windows Mail)" à la page 120) ;
- The Bat! (cf. section "Configuration du traitement du courrier indésirable dans The Bat!" à la page 121) ;
- Thunderbird (cf. section "Configuration du traitement du courrier indésirable dans Thunderbird" à la page 121).

La constitution des listes d'expéditeurs autorisés (cf. page 113) et interdits (cf. page 111) vous permet d'indiquer à l'Anti-Spam les messages qu'il faudra considérer comme du courrier normal ou comme du courrier indésirable. De plus, l'Anti-Spam peut analyser un message afin de voir s'il contient des expressions figurant dans la liste des expressions autorisées (cf. page 114) et interdites (cf. page 112) ou des mots de la liste des expressions vulgaires (cf. page 112).

L'Anti-Spam permet de consulter le courrier sur le serveur (cf. section "Filtrage des messages sur le serveur. Gestionnaire de messages" à la page 117) et de supprimer les messages inutiles avant qu'ils ne soient téléchargés sur l'ordinateur.

➡ *Afin de modifier les paramètres de fonctionnement de l'Anti-Spam, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Le fonctionnement du composant Anti-Spam est scindé en deux étapes :

1. Application de critères de filtrages stricts aux messages. Ceux-ci permettent de déterminer rapidement si un message appartient ou non au courrier indésirable. L'Anti-Spam attribue l'état *courrier indésirable* ou *courrier normal*, l'analyse est suspendue et le message est transmis au client de messagerie pour traitement (cf. étapes 1 à 5 ci-après).

2. Etude des messages qui ont répondu aux critères précis de sélection des étapes précédentes. Ces messages ne peuvent pas être automatiquement considérés comme du courrier indésirable. Pour cette raison, l'Anti-Spam doit calculer la *probabilité* de leur appartenance au courrier indésirable.

L'algorithme de fonctionnement de l'Anti-Spam contient les étapes suivantes :

1. L'adresse de l'expéditeur du message est contrôlée afin de voir si elle figure dans les listes des expéditeurs autorisés ou interdits.

   - Si l'adresse de l'expéditeur se trouve dans la liste des adresses autorisées, le message reçoit l'état *courrier normal*.

   - Si l'adresse de l'expéditeur figure dans la liste des adresses interdites, le message reçoit l'état *courrier indésirable*.

2. Si le message a été envoyé via Microsoft Exchange Explorer et que l'analyse de tels messages est désactivée (cf. page 118), le message reçoit l'état *courrier normal*.

3. Le composant vérifie si le message contient des expressions tirées de la liste des expressions autorisées (cf. page 114). Si le message contient ne serait-ce qu'une expression de la liste, le message reçoit l'état *courrier normal*. Cette étape est ignorée par défaut.

4. Le composant vérifie si le message contient des expressions tirées de la liste des expressions interdites (cf. page 112). La présence de mots de cette liste dans le message augmente la probabilité qu'il s'agisse d'un message non sollicité. Si la probabilité dépasse la valeur définie (cf. page 115), le message reçoit l'état *courrier indésirable* ou *courrier indésirable potentiel*. Le composant vérifie si le message contient des expressions tirées de la liste des expressions vulgaires (cf. page 112). Cette étape est ignorée par défaut.

5. Si le texte contient une adresse reprise dans la base des URL de phishing ou suspectes (cf. page 110), le message reçoit l'état *courrier indésirable*.

6. Les courriers électroniques sont analysés selon les règles heuristiques. Si l'analyse met en évidence des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

7. Le message est analysé à l'aide de la technologie GSG. L'Anti-Spam analyse les images incluses dans le message. Si celles-ci contiennent des éléments caractéristiques du courrier indésirable, la probabilité que le message appartienne au courrier indésirable augmente.

8. Les documents joints au format *.rtf* sont analysés. L'Anti-Spam recherche les éléments caractéristiques du courrier indésirable dans les documents joints. A la fin de l'analyse, l'Anti-Spam calcule l'augmentation de la probabilité qu'un message appartienne au courrier indésirable. La technologie est désactivée par défaut.

9. Le composant procède à la recherche d'indices complémentaires (cf. page 116) caractéristiques du courrier indésirable. Chaque fois qu'un de ces indices est identifié, la probabilité que le message appartienne au courrier indésirable augmente.

10. Si l'Anti-Spam a été entraîné, l'analyse des messages s'opère à l'aide de la technologie iBayes. L'algorithme d'auto-apprentissage iBayes calcule la probabilité qu'un message appartienne au courrier indésirable sur la base de la fréquence d'utilisation d'expressions propres au courrier indésirable dans le message.

La probabilité d'appartenance du message au courrier indésirable est le résultat de l'analyse. Les auteurs de messages non sollicités ne cessent d'améliorer leurs techniques de dissimulation et c'est la raison pour laquelle la probabilité obtenue atteint rarement la valeur définie (cf. section "Définition des indices de courrier indésirable et de courrier indésirable potentiel" à la page 115). Afin de filtrer au mieux possible le flux des messages, l'Anti-Spam utilise deux facteurs :

- *L'indice de courrier indésirable* qui est la valeur du seuil au-delà duquel un message est considéré comme appartenant au *courrier indésirable*. Si la probabilité est inférieure à cette valeur, alors l'Anti-Spam attribue l'état *courrier indésirable potentiel* au message ;

- *L'indice de courrier indésirable potentiel* qui est la valeur du seuil au-delà duquel un message est considéré comme courrier indésirable potentiel. Si la probabilité est inférieure à cette valeur, alors l'Anti-Spam considère le message comme un message normal.

En fonction des valeurs attribuées aux indices de courrier indésirable et de courrier indésirable potentiel, le message recevra l'état *courrier indésirable* ou *courrier indésirable potentiel*. De plus, les messages reçoivent par défaut le texte **[!! SPAM]** ou **[!! Probable Spam]** dans le champ **Objet** en fonction de l'état attribué. Après ils sont traités selon les

règles (cf. section "Actions à réaliser sur le courrier indésirable" à la page 118), que vous avez défini pour votre client de courrier.

ENTRAINEMENT DE L'ANTI-SPAM

Un des outils d'identification du courrier indésirable est l'algorithme d'auto-apprentissage iBayes. Cet algorithme décide d'octroyer un état au message sur la base des expressions que celui-ci contient. Avant de pouvoir utiliser l'algorithme iBayes, il faut lui présenter des échantillons de phrases de messages utiles et de messages non sollicités, c.-à-d. l'entraîner.

Il existe plusieurs approches pour entraîner l'Anti-Spam :

- Utilisation de l'Assistant d'apprentissage (cf. section "Entraînement à l'aide de l'Assistant d'apprentissage" à la page 106) (apprentissage groupé). L'entraînement à l'aide de l'Assistant d'apprentissage est préférable au tout début de l'utilisation de l'Anti-Spam.

- Entraînement de l'Anti-Spam sur le courrier sortant (cf. section "Entraînement sur le courrier sortant" à la page 107).

- L'apprentissage directement pendant les opérations avec le courrier (cf. section "Apprentissage à l'aide du client de messagerie" à la page 108), en utilisant les touches spécifiques dans le panneau d'instruments du client de courrier ou les points du menu.

- Entraînement lors de l'utilisation des rapports de l'Anti-Spam (cf. section "Entraînement à l'aide des rapports" à la page 109).

ENTRAINEMENT A L'AIDE DE L'ASSISTANT D'APPRENTISSAGE

L'Assistant d'apprentissage permet d'entraîner l'Anti-Spam par lot. Pour ce faire, il faut désigner les répertoires des comptes utilisateur des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) qui contiennent le courrier indésirable et le courrier normal.

Pour assurer une identification efficace du courrier indésirable, il est indispensable de réaliser l'entraînement sur un minimum de 50 exemplaires de courrier normal et de 50 exemplaires de courrier indésirable. L'algorithme iBayes ne fonctionnera pas si ces actions ne sont pas exécutées.

Afin de gagner du temps, l'Assistant réalisera l'entraînement uniquement sur 50 messages de chaque dossier sélectionné.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné dans le groupe **Entraînement d'Anti-Spam**, cliquez sur le bouton **Entraîner**.

Lors de l'entraînement sur le courrier utile, l'ajout de l'adresse de l'expéditeur dans la liste des expéditeurs autorisés a lieu.

Afin de désactiver l'ajout de l'adresse de l'expéditeur dans la liste des adresses autorisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier utile**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.
5. Dans la fenêtre **Liste des expéditeurs autorisés** qui s'ouvre, cochez la case **Ajouter les adresses des expéditeurs autorisés pendant l'apprentissage d'Anti-Spam dans le client de messagerie**.

VOIR EGALEMENT

Entraînement à l'aide des rapports.....109

Apprentissage à l'aide du client de messagerie.....108

Entraînement d'Anti-Spam sur le courrier sortant.....107

ENTRAINEMENT DE L'ANTI-SPAM SUR LE COURRIER SORTANT

Vous pouvez entraîner l'Anti-Spam sur la base de 50 exemples de messages sortants. Les adresses des destinataires de ces messages seront ajoutés automatiquement à la liste des expéditeurs autorisés.

Pour entraîner l'Anti-Spam sur la base du courrier sortant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Courrier sortant**, cochez la case **Apprentissage sur le courrier sortant**.

Afin de désactiver l'ajout de l'adresse de l'expéditeur dans la liste des expéditeurs autorisés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier utile**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.
5. Dans la fenêtre **Liste des expéditeurs autorisés** qui s'ouvre, cochez la case **Ajouter les adresses des expéditeurs autorisés pendant l'apprentissage d'Anti-Spam dans le client de messagerie**.

VOIR EGALEMENT

APPRENTISSAGE A L'AIDE DU CLIENT DE MESSAGERIE

L'entraînement de l'Anti-Spam pendant l'utilisation du courrier électronique suppose l'utilisation des éléments spéciaux de l'interface de votre client de messagerie.

Les boutons pour l'entraînement de l'Anti-Spam apparaissent dans l'interface des clients de messagerie Microsoft Office Outlook et Microsoft Outlook Express (Windows Mail) uniquement après l'installation de Kaspersky Internet Security.

Pour entraîner l'Anti-Spam à l'aide du client de messagerie, procédez comme suit :

1. Lancez le client de messagerie.
2. Sélectionnez le message à l'aide duquel vous souhaitez entraîner l'Anti-Spam.
3. Exécutez une des actions suivantes en fonction du client de messagerie que vous utilisez :
   - cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Office Outlook ;
   - cliquez sur le bouton **Courrier indésirable** ou **Courrier normal** dans la barre d'outils de Microsoft Outlook Express (Windows Mail) ;
   - utilisez les éléments **Marquer comme courrier indésirable** ou **Marquer comme courrier normal** dans le menu **Spécial** du client de messagerie The Bat! ;
   - utilisez le bouton **Courrier indésirable/Courrier normal** dans la barre d'outils du client de messagerie Mozilla Thunderbird.

Une fois que vous aurez choisi une des actions ci-dessus, Anti-Spam poursuivra son entraînement sur la base du message sélectionné. Si vous sélectionnez plusieurs messages, l'entraînement portera sur tous les messages sélectionnés.

Si le message est considéré comme normal, l'adresse de l'expéditeur est ajoutée à la liste des expéditeurs autorisés.

Afin de désactiver l'ajout de l'adresse de l'expéditeur dans la liste des expéditeurs autorisés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier normal**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.
5. Dans la fenêtre **Liste des expéditeurs autorisés** qui s'ouvre, cochez la case **Ajouter les adresses des expéditeurs autorisés pendant l'apprentissage de l'Anti-Spam dans le client de messagerie**.

Si vous êtes forcé de sélectionner directement plusieurs messages ou si vous êtes convaincus qu'un dossier ne contient des messages que d'une seule catégorie (courrier indésirable ou courrier normal), il est possible de réaliser un entraînement groupé à l'aide de l'Assistant d'apprentissage (cf. section "Apprentissage de l'Anti-Spam" à la page 106).

VOIR EGALEMENT

ENTRAINEMENT A L'AIDE DES RAPPORTS

Il est possible d'entraîner l'Anti-Spam sur la base de ses rapports. Les rapports du composant permettent de conclure de la précision de la configuration et, au besoin, d'introduire des modifications dans le fonctionnement de l'Anti-Spam.

Afin d'identifier une lettre quelconque comme le spam ou pas le spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Le lien **Rapport** ouvre la fenêtre des rapports de Kaspersky Internet Security.
3. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
4. Pour le composant **Anti-Spam**, sélectionnez le message sur la base duquel vous souhaitez réaliser l'apprentissage complémentaire.
5. Ouvrez le menu contextuel du message et sélectionnez une des actions suivantes :
   - **Marquer comme courrier indésirable** ;
   - **Marquer comme courrier normal** ;
   - **Ajouter à la liste des expéditeurs autorisés** ;
   - **Ajouter à la liste des expéditeurs interdits** ;

VOIR EGALEMENT

MODIFICATION DU NIVEAU DE PROTECTION

L'Anti-Spam filtre les messages selon deux indicateurs :

- *L'indice de courrier indésirable* est la valeur du seuil au-delà duquel un message est considéré comme appartenant au courrier indésirable. Si la probabilité est inférieure à cette valeur, alors l'Anti-Spam attribue l'état *courrier indésirable potentiel* au message.

- *L'indice de courrier indésirable potentiel* qui est la valeur du seuil au-delà duquel un message est considéré comme courrier indésirable potentiel. Si la probabilité est inférieure à cette valeur, alors l'Anti-Spam considère le message comme un message normal.

Les experts de Kaspersky Lab ont configuré trois niveaux de protection :

- **Elevé.** Ce niveau de protection doit être utilisé si vous recevez souvent des messages non sollicités, par exemple lors de l'utilisation de service de messagerie en ligne gratuite. Si vous sélectionnez ce niveau, la fréquence d'identification d'un courrier normal en tant que courrier indésirable peut augmenter.

- **Moyen**. Ce niveau de protection doit être utilisé dans la majorité des cas.

- **Bas.** Ce niveau de protection doit être utilisé si vous recevez rarement du courrier indésirable, par exemple si vous travaillez dans un milieu protégé (système de messagerie d'entreprise). Si vous sélectionnez ce niveau, la fréquence d'identification d'un courrier normal en tant que courrier indésirable peut diminuer.

Pour modifier le niveau de protection prédéfini de l'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Définissez le niveau de protection requis pour le composant sélectionné.

SELECTION DE LA METHODE D'ANALYSE

La méthode d'analyse désigne l'analyse des liens, inclus dans les messages électroniques, pour savoir s'ils appartiennent à la liste des URL interdites et / ou à la liste des URL de phishing.

L'analyse des liens, s'ils appartiennent à la liste des adresses de phishing, permet d'éviter les attaques de phishing qui, en règle générale, se présentent sous les messages électroniques prétendument envoyés par une institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message amène le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche.

L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse authentique du site s'affiche ; dans la majorité des cas, il s'agit d'un site fictif. Toutes vos actions sur ce site sont suivies et pourraient servir au vol de votre argent.

Pour analyser les liens des messages selon la base des adresses suspectes, procédez comme suit :

1. Ouvrde l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des liens de la base des URL suspectes**.

Pour analyser les liens des messages selon la liste des adresses de phishing, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des liens de la base des URL de phishing**.

CONSTITUTION D'UNE LISTE D'ADRESSES DE CONFIANCE

Vous pouvez composer une liste d'adresses de confiance. L'Anti-Spam vérifiera si l'adresse du destinataire appartient à cette liste.

Pour constituer la liste des adresses de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, cochez la case **Dont je ne suis pas le destinataire** et cliquez sur **Mes adresses**.
5. Dans la fenêtre **Mes adresses** qui s'ouvre, cliquez sur le lien **Ajouter**.
6. Dans la fenêtre **Masque d'adresse de courrier électronique** qui s'ouvre, saisissez les adresses ou les masques d'adresse requis.

CONSTITUTION D'UNE LISTE D'EXPEDITEURS INTERDITS

La liste des expéditeurs interdits reprend les adresses des expéditeurs de messages que vous considérez comme indésirables. La liste est rédigée manuellement.

S'agissant des adresses de la liste, vous pouvez saisir soit une adresse, soit un masque. Les caractères ***** et **?** peuvent servir de masque (où ***** représente n'importe quel nombre de caractères et **?**, pour n'importe quel caractère). Exemples de masques d'adresse :

- *dupont@test.fr*. Les messages de cet expéditeur seront considérés comme du courrier indésirable.
- **@test.fr*. Les messages de n'importe quel expéditeur du domaine *test.fr* seront considérés comme du courrier indésirable ; exemple : *legrand@test.fr*, *dunant@test.fr*.
- *dupont@**. Les expéditeurs portant ce nom, quel que soit le domaine de messagerie, envoient toujours du courrier indésirable, par exemple : *dupont@test.fr*, *dupont@mail.fr*.
- **@test**. Les messages de n'importe quel expéditeur d'un domaine commençant par *test* appartiennent au courrier indésirable, par exemple : *dupont@test.fr*, *legrand@test.com*.
- *pierre.*@test.???*. Le courrier dont le nom de l'expéditeur commence par *pierre.* et dont le nom de domaine commence par *test* et se termine par une séquence quelconque de trois caractères sera toujours considéré comme du courrier indésirable; exemple : *pierre.dupont@test.com*, *pierre.legrand@test.org*.

Pour composer la liste des expéditeurs interdits et l'utiliser par la suite, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **D'expéditeurs interdits** puis cliquez sur le bouton **Sélection**.

5. Dans la fenêtre **Liste des expéditeurs interdits** qui s'ouvre, cliquez sur **Ajouter**.

6. Dans la fenêtre **Masque d'adresse de courrier électronique** qui s'ouvre, saisissez l'adresse ou le masque requis.

CONSTITUTION D'UNE LISTE D'EXPRESSIONS INTERDITES

La liste des expressions interdites contient des expressions clés des messages qui selon vous sont des messages non sollicités. La liste est rédigée manuellement.

Les masques peuvent être appliqués aux expressions. Les caractères ***** et **?** peuvent servir de masque (où ***** représente n'importe quel nombre de caractères et **?**, pour n'importe quel caractère). Exemples d'expressions et de masques d'expression :

- *Salut Pierre !*. Le message qui contient ce texte uniquement est considéré comme courrier indésirable. Il est déconseillé d'utiliser ce type d'expression.
- *Salut Pierre !**. Le message qui commence par *Salut Pierre !* est considéré comme du courrier indésirable.
- *Salut *! **. Le message qui débute par *Salut* et qui possède un point d'exclamation n'importe où dans le texte est considéré comme un courrier indésirable.
- ** Pierre? **. Le message adressé à *Pierre* suivi de n'importe quel caractère est considéré comme du courrier indésirable.
- ** Pierre\? **. Le message qui contient le texte *Pierre?* est considéré comme du courrier indésirable.

Si les caractères * et ? font partie d'une expression, il convient de les faire précéder du caractère \ afin d'éviter toute confusion de la part de l'Anti-Spam. Dans ce cas, au lieu d'utiliser un caractère, on en utilise deux : * et \?.

Pour composer la liste des expressions interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites** puis cliquez sur le bouton **Sélection**.

5. Dans la fenêtre **Liste des expressions interdites** qui s'ouvre, cliquez sur **Ajouter**.

6. Dans la fenêtre **Expression interdite** qui s'ouvre, saisissez l'expression ou le masque requis.

CONSTITUTION D'UNE LISTE D'EXPRESSIONS VULGAIRES

La liste contient les expressions vulgaires dont la présence dans un message permet d'affirmer avec beaucoup de certitude qu'il s'agit d'un message non sollicité.

Les experts de Kaspersky Lab ont constitué la liste d'expressions vulgaires utilisée par Kaspersky Internet Security. Vous pouvez l'enrichir.

Les masques peuvent être appliqués aux expressions. Les caractères ***** et **?** peuvent servir de masque (où ***** représente n'importe quel nombre de caractères et **?**, pour n'importe quel caractère).

Si les caractères * et ? font partie d'une expression, il convient de les faire précéder du caractère \ afin d'éviter toute confusion de la part de l'Anti-Spam. Dans ce cas, au lieu d'utiliser un caractère, on en utilise deux : * et \?.

Pour modifier la liste des expressions vulgaires, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier indésirable**, cochez la case **Contenant des expressions interdites** puis cliquez sur le bouton **Sélection**.
5. Dans la fenêtre **Liste des expressions interdites** qui s'ouvre, cochez la case **Considérer comme interdit les expressions vulgaires** puis cliquez sur le lien **les expressions vulgaires**.
6. Dans la fenêtre **Accord** qui s'ouvre, lisez le texte du contrat et si vous en acceptez les dispositions, cochez la case correspondante puis cliquez sur **OK**.
7. Dans la fenêtre **Liste de langage vulgaire** qui s'ouvre, cliquez sur le lien **Ajouter**.
8. Dans la fenêtre **Expression interdite** qui s'ouvre, saisissez l'expression ou le masque requis.

CONSTITUTION D'UNE LISTE D'EXPEDITEURS AUTORISES

La liste des expéditeurs autorisés reprend les adresses des expéditeurs qui, selon vous, ne devraient pas vous envoyer du courrier indésirable : Cette liste est remplie automatiquement lors de l'entraînement de l'Anti-Spam. Vous pouvez modifier cette liste.

S'agissant des adresses de la liste, vous pouvez saisir soit une adresse, soit un masque. Les caractères ***** et **?** peuvent servir de masque (où ***** représente n'importe quel nombre de caractères et **?**, pour n'importe quel caractère). Exemples de masques d'adresses :

- *dupont@test.fr.* Les messages de cet expéditeur seront considérés comme du courrier normal.
- **@test.fr.* Les messages de n'importe quel expéditeur du domaine *test.fr* seront considérés comme du courrier normal ; exemple : *legrand@test.fr*, *dunant@test.fr*.
- *dupont@*.* Les expéditeurs portant ce nom, quel que soit le domaine de messagerie, envoient toujours du courrier normal, par exemple : *dupont@test.fr*, *dupont@mail.fr*.
- **@test*.* Les messages de n'importe quel expéditeur d'un domaine commençant par *test* n'appartiennent pas au courrier indésirable, par exemple : *dupont@test.fr*, *legrand@test.com*.
- *pierre.*@test.???.* Le courrier dont le nom de l'expéditeur commence par *pierre.* et dont le nom de domaine commence par *test* et se termine par une séquence quelconque de trois caractères sera toujours considéré comme du courrier normal; exemple : *pierre.dupont@test.com*, *pierre.legrand@test.org*.

Pour composer la liste des expressions autorisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier utile**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

5. Dans la fenêtre **Liste des expéditeurs autorisés** qui s'ouvre, cliquez sur **Ajouter**.

6. Dans la fenêtre **Masque d'adresse de courrier électronique** qui s'ouvre, saisissez l'adresse ou le masque requis.

CONSTITUTION D'UNE LISTE D'EXPRESSIONS AUTORISEES

La liste d'expressions autorisées contient les expressions clés des messages que vous considérez comme des messages normaux. Vous pouvez composer une telle liste.

Les masques peuvent être appliqués aux expressions. Les caractères ***** et **?** peuvent servir de masque (où ***** représente n'importe quel nombre de caractères et **?**, pour n'importe quel caractère). Exemples d'expressions et de masques d'expression :

- *Salut Pierre !*. Le message qui contient ce texte uniquement est considéré comme courrier normal. Il est déconseillé d'utiliser ce type d'expression.
- *Salut Pierre !**. Le message qui commence par *Salut Pierre !* est considéré comme du courrier normal.
- *Salut *! **. Le message qui débute par *Salut* et qui possède un point d'exclamation n'importe où dans le texte n'est pas considéré comme un courrier indésirable.
- ** Pierre? **. Le message adressé à *Pierre* suivi de n'importe quel caractère n'est pas considéré comme du courrier indésirable.
- ** Pierre\? **. Le message qui contient le texte *Pierre?* est considéré comme du courrier normal.

Si les caractères * et ? font partie d'une expression, il convient de les faire précéder du caractère \ afin d'éviter toute confusion de la part de l'Anti-Spam. Dans ce cas, au lieu d'utiliser un caractère, on en utilise deux : * et \?.

Pour composer la liste des expressions autorisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général**, dans le groupe **Considérer les messages suivants comme du courrier utile**, cochez la case **Contenant des expressions autorisées** puis cliquez sur le bouton **Sélection**.

5. Dans la fenêtre **Liste des expressions autorisées** qui s'ouvre, cliquez sur **Ajouter**.

6. Dans la fenêtre **Expression autorisée** qui s'ouvre, saisissez l'expression ou le masque requis.

IMPORTATION DE LA LISTE DES EXPEDITEURS AUTORISES

Il est possible d'importer les adresses dans la liste des expéditeurs autorisés au départ d'un fichier **.txt*, **.csv* ou depuis le carnet d'adresses de Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail).

Pour importer la liste des expéditeurs autorisés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Général** dans le groupe **Considérer les messages suivants comme du courrier utile**, cochez la case **D'expéditeurs autorisés** et cliquez sur le bouton **Sélection**.

5. Dans la fenêtre **Liste des expéditeurs autorisés** qui s'ouvre, cliquez sur **Importer**.

6. Sélectionnez la source de l'importation dans le menu déroulant :

   - **Importer depuis un fichier**. Si vous choisissez cette source, la fenêtre de sélection du fichier s'ouvrira. L'application peut importer des fichiers *.csv* ou *.txt*.

   - **Importer depuis le carnet d'adresses**. Si vous choisissez cette source, la fenêtre de sélection du carnet d'adresses s'ouvrira. Sélectionnez le carnet d'adresses requis dans la fenêtre.

DEFINITION DES PARAMETRES DE COURRIER INDESIRABLE ET DE COURRIER INDESIRABLE POTENTIEL

Les experts de Kaspersky Lab s'efforcent de configurer l'Anti-Spam de la façon la plus précise qui soit afin qu'il identifie le courrier indésirable, confirmé ou potentiel.

L'identification du courrier indésirable repose sur l'utilisation de technologies modernes de filtrage qui permettent à l'Anti-Spam de séparer le courrier (potentiellement) indésirable du courrier normal. Cet entraînement est réalisé sur la base de l'analyse d'un nombre déterminé de messages de l'utilisateur.

L'entraînement de l'Anti-Spam est réalisé à l'aide le l'Assistant d'apprentissage, ainsi qu'à l'aide de l'entraînement via les clients de messagerie. Chaque élément de courrier normal ou de courrier indésirable se voit attribuer un certain coefficient. Quand un message arrive dans votre boîte aux lettres, l'Anti-Spam exploite la technologie iBayes pour voir si le message contient des éléments de courrier indésirable ou de courrier normal. Les coefficients de chaque élément de courrier indésirable (courrier normal) sont ajoutés pour obtenir l'indice de courrier indésirable et l'indice de courrier indésirable potentiel.

La valeur de l'indice de courrier indésirable potentiel est un indicateur qui, s'il est dépassé, entraîne l'octroi de l'état *Courrier indésirable potentiel* au message. Si vous avez opté pour le niveau **Recommandé** dans la configuration de l'Anti-Spam, tout message dont l'indice est supérieur à 60 % sera considéré comme un message indésirable potentiel. Un message est normal si la valeur de cet indice après l'analyse est inférieure à 60%. Vous pouvez modifier la valeur.

La valeur de l'indice de courrier indésirable est un indicateur qui, s'il est dépassé, entraîne l'octroi de l'état *Courrier indésirable* au message. Tout message dont l'indice est supérieur à l'indice défini sera considéré comme un courrier indésirable. Par défaut, au niveau **Recommandé**, l'indice de courrier indésirable est égal à 90%. Cela signifie que tout message dont l'indice est supérieur à 90% sera considéré comme un courrier indésirable. Vous pouvez modifier la valeur.

Pour modifier la valeur de l'indice de courrier indésirable (potentiel), procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Indice de courrier indésirable**, réglez les facteurs de courrier indésirable et de courrier indésirable potentiel.

SELECTION DE L'ALGORITHME D'IDENTIFICATION DU COURRIER INDESIRABLE

La recherche des messages non sollicités dans le courrier s'opère à l'aide d'algorithme d'identification :

- ☑ **Analyse heuristique**. L'Anti-Spam analyse les messages à l'aide des règles heuristiques. L'analyse heuristique est toujours utilisée.
- ☑ **Identification des images (GSG)**. L'Anti-Spam applique la technologie GSG pour identifier le courrier indésirable sous la forme d'images.
- ☑ **Analyse des documents .rtf joints**. L'Anti-Spam analyse les documents joints au message afin de voir s'ils présentent des éléments caractéristiques du courrier indésirable.
- ☑ **Algorithme d'auto-apprentissage d'analyse de texte (iBayes)**. L'algorithme iBayes décide si le message est normal ou non sur la base de la fréquence d'utilisation dans le texte de mots caractéristiques du courrier indésirable. Il faut impérativement entraîner (cf. section "Entraînement de l'Anti-Spam" à la page 106) l'algorithme d'iBayes avant de commencer à l'utiliser.

Afin d'utiliser/de ne pas utiliser un algorithme quelconque d'identification du courrier indésirable lors de l'analyse du courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** dans le groupe **Algorithmes d'identification**, cochez / décochez les cases correspondantes ☑.

UTILISATION D'INDICES COMPLEMENTAIRES POUR LE FILTRAGE DU COURRIER INDESIRABLE

Outre les éléments principaux sur la base desquels les messages sont filtrés (constitution de listes d'expéditeurs autorisés ou interdits, analyse à l'aide d'algorithme d'identification, etc.), vous pouvez définir d'autres critères. Sur la base de ces critères, le message sera considéré comme *indésirable* avec un niveau de certitude ou l'autre.

Afin de recourir ou non à l'utilisation de certains critères complémentaires pour filtrer le courrier indésirable, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé** cliquez sur le bouton **Options additionnelles**.
5. Dans la fenêtre **Avancé**, cochez / décochez la case ☑ en regard des critères requis pour les messages indésirables.

AJOUT DE COMMENTAIRES A L'OBJET DU MESSAGE

Vous pouvez ajouter les commentaires **[!! SPAM]** ou **[?? Probable Spam]** dans le champ **Objet** des messages considérés comme indésirables ou potentiellement indésirables après l'analyse.

Pour ajouter/ne pas ajouter de commentaires à l'objet des messages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Avancé** qui s'ouvre, dans le groupe **Actions**, cochez ou désélectionnez les cases requises ☑. Vous pouvez modifier le texte du commentaire.

FILTRAGE DES MESSAGES SUR LE SERVEUR. GESTIONNAIRE DE MESSAGES

Vous pouvez consulter la liste des messages sur le serveur sans devoir les télécharger sur votre ordinateur. Cela évite la réception de certains messages, ce qui vous fait gagner du temps et de l'argent lors de l'utilisation du courrier électronique et qui réduit la probabilité de recevoir du courrier indésirable et des virus.

Le **Gestionnaire de messages** permet de manipuler les messages sur le serveur. La fenêtre du Gestionnaire s'ouvre chaque fois avant la réception d'un message, pour autant que le Gestionnaire soit activé.

La fenêtre du Gestionnaire de messages s'ouvre lors de la réception de courrier via le protocole POP3. Le Gestionnaire de messages ne s'ouvre pas, si le serveur POP3 ne prend pas ne charge la consultation des en-têtes des messages électroniques, ou tout le courrier sur le serveur était envoyé par les utilisateurs de la liste des expéditeurs autorisés.

La liste des messages présents sur le serveur s'affiche dans la partie centrale de la fenêtre du gestionnaire. Sélectionnez le message dans la liste pour étudier son en-tête en détail. L'examen des en-têtes peut être utile dans les cas suivants : les spammeurs ont installé un programme malveillant sur l'ordinateur de votre collègue qui envoie du courrier indésirable en son nom en utilisant la liste des contacts de son client de messagerie. Il est fort probable que votre adresse se trouve dans les contacts de vos collègues. Par conséquent votre boîte aux lettres sera certainement remplie de courrier indésirable. Dans cette situation, l'adresse de l'expéditeur ne permet pas à elle seule de confirmer si le message a été envoyé par votre ami ou par un diffuseur de courrier indésirable. C'est précisément pour cette raison qu'il faut prêter attention aux en-têtes des messages. Il est conseillé de vérifier quand le message a été envoyé et par qui et il est important également de prêter attention à sa taille. Dans la mesure du possible, soyez attentif au trajet du message depuis l'expéditeur jusque votre serveur de messagerie. Ces informations doivent figurer dans l'en-tête du message. Toutes ces informations doivent être reprises dans l'en-tête du message. Les actions citées vous permettront de définir s'il faut vraiment charger ce message depuis le serveur ou s'il est préférable de le supprimer.

Pour utiliser le Gestionnaire de messages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Messages entrants**, cochez la case ☑ **Ouvrir le Gestionnaire de messages lors de la réception de courrier via le protocole POP3**.

Pour supprimer les messages du serveur à l'aide du Gestionnaire de messages, procédez comme suit :

1. Dans la fenêtre du Gestionnaire, cochez la case dans la colonne **Supprimer** en regard du message.
2. Dans la partie supérieure de la fenêtre, cliquez sur le bouton **Supprimer la sélection**.

Les messages seront supprimés du serveur. Vous recevrez un message accompagné de la note **[!! SPAM]** et traité selon les règles de votre client de messagerie.

EXCLUSION DES MESSAGES MICROSOFT EXCHANGE SERVER DE L'ANALYSE

Vous pouvez exclure de la recherche du courrier indésirable les messages envoyés dans le cadre du réseau interne (par exemple, le courrier d'entreprise). N'oubliez pas que les messages seront considérés comme des messages internes dans ce cas si Microsoft Office Outlook est utilisé sur tous les postes du réseau et que les boîtes aux lettres des utilisateurs se trouvent sur un même serveur Exchange ou que ces serveurs sont unis par des connecteurs X400.

Par défaut, l'Anti-Spam n'analyse pas les messages de Microsoft Exchange Server.

Pour que l'Anti-Spam analyse les messages, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre sous l'onglet **Avancé** dans le groupe **Exclusions**, décochez la case **Ne pas analyser les messages Microsoft Exchange Server**.

ACTIONS A REALISER SUR LE COURRIER INDESIRABLE

Si l'analyse indique que le message est un exemplaire de courrier indésirable ou de courrier indésirable potentiel, la suite des opérations réalisées par Anti-Spam dépendra de l'état de l'objet et de l'action sélectionnée. Par défaut, les messages électroniques classés comme courrier indésirable ou courrier indésirable potentiel sont modifiés : le texte **[!! SPAM]** ou **[?? Probable Spam]** est ajouté respectivement au champ **Objet** du message.

Vous pouvez sélectionner des actions complémentaires à exécuter sur le courrier indésirable et le courrier indésirable potentiel. Des modules externes spéciaux sont prévus dans les clients de messagerie Microsoft Office Outlook (cf. section "Configuration du traitement du courrier indésirable dans Microsoft Office Outlook" à la page 119) et Microsoft Outlook Express (Windows Mail) (cf. section "Configuration du traitement du courrier indésirable dans Microsoft Outlook Express (Windows Mail)" à la page 120). Pour les clients de messagerie The Bat! (cf. section "Configuration du traitement du courrier indésirable dans The Bat!" à la page 121) et Thunderbird (cf. section "Configuration du traitement du courrier indésirable dans Thunderbird" à la page 121) vous pouvez configurer des règles de filtrage.

VOIR EGALEMENT

CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE DANS MICROSOFT OFFICE OUTLOOK

La fenêtre de configuration du traitement du courrier indésirable s'ouvre automatiquement à la première ouverture du client de messagerie après le chargement de Kaspersky Internet Security.

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**.

Les règles de traitement suivantes sont prévues aussi bien pour le courrier indésirable que pour le courrier indésirable potentiel :

- **Placer dans le dossier** : le courrier indésirable est placé dans le dossier de la boîte aux lettres que vous aurez spécifié.
- **Copier dans le dossier** : une copie du message est créée et placée dans le dossier indiqué. La copie originale reste dans le dossier **Entrant**.
- **Supprimer** : supprime le courrier indésirable de la boîte aux lettres de l'utilisateur.
- **Ignorer** : laisse le message électronique dans le dossier **Entrant**.

Pour ce faire, sélectionnez la valeur souhaitée dans la liste déroulante du bloc **Courrier indésirable** ou **Courrier indésirable potentiel**.

En cas dentraînement de l'Anti-Spam à l'aide d'un client de messagerie (cf. section "Apprentissage à l'aide du client de messagerie" à la page 108) le message sélectionné est envoyé à Kaspersky Lab en tant qu'exemple de courrier indésirable. Cliquez sur le lien **Avancé lors de l'identification manuelle d'un message en tant que message non sollicité** afin de sélectionner le mode d'envoi des exemples de courrier indésirable dans la fenêtre qui s'ouvre. Cliquez sur le lien **Configurer l'envoi des échantillons de spam à Kaspersky Lab** pour sélectionner le mode d'envoi des échantillons de courrier normal (échantillons considérés par erreur comme du courrier indésirable).

Vous pouvez également indiquer l'algorithme de coopération entre Microsoft Office Outlook et l'Anti-Spam :

- **Analyser à la réception**. Tous les messages qui arrivent dans la boîte aux lettres de l'utilisateur sont d'abord analysés selon les règles définies de Microsoft Office Outlook. A la fin de ce traitement, les messages qui ne tombaient pas sous le coup de ces règles sont transmis au plug-in Anti-Spam. Le traitement se déroule dans un certain ordre. Cet ordre peut parfois ne pas être respecté, par exemple lors de la réception simultanée d'un grand nombre de messages dans la boîte aux lettres. Une telle situation peut faire que les informations relatives aux messages traités par les règles de Microsoft Outlook apparaissent comme *courrier indésirable* dans le rapport de l'Anti-Spam. Afin d'éviter une telle situation, nous vous conseillons de configurer le plug-in Anti-Spam en qualité de règle de Microsoft Office Outlook.
- **Utiliser la règle de Microsoft Office Outlook**. Dans ce cas, le traitement des messages qui arrivent dans la boîte aux lettres de l'utilisateur s'opère selon la hiérarchie des règles de Microsoft Office Outlook. Il faut créer en guise de règle le traitement des messages par l'Anti-Spam. Il s'agit de l'algorithme de travail optimal qui évite les conflits entre Microsoft Office Outlook et le plug-in Anti-Spam. Cet algorithme a un seul défaut : la création et la suppression des règles de traitement des messages via Microsoft Office Outlook s'opèrent manuellement.

➧ *Pour créer la règle de traitement d'un message à la recherche de courrier indésirable, procédez comme suit :*

1. Lancez Microsoft Office Outlook et utilisez la commande **Service** →**Règles et notifications** de la fenêtre principale du logiciel. La méthode à employer pour ouvrir l'Assistant dépend de la version de Microsoft Office Outlook que vous utilisez. Dans notre cas, nous envisageons la création d'une règle dans Microsoft Office Outlook 2003.
2. Dans la fenêtre **Règles et notification**, passez à l'onglet **Règles pour le courrier électronique** et cliquez sur **Nouvelle**. Cette action entraîne le lancement de l'Assistant de création de nouvelle règle. Il contient une succession de fenêtres (étapes) :

a. Vous devez choisir entre la création d'une règle à partir de zéro ou selon un modèle. Sélectionnez l'option **Créer une nouvelle règle** et en guise de condition de l'analyse, sélectionnez **Analyse des messages après la réception**. Cliquez sur **Suivant**.

b. Dans la fenêtre de sélection des conditions de tri des messages, cliquez sur **Suivant** sans cocher aucune case. Confirmez l'application de cette règle à tous les messages reçus dans la fenêtre de confirmation.

c. Dans la fenêtre de sélection des actions sur les messages, cochez la case **exécuter une action complémentaire** dans la liste des actions. Dans la partie inférieure de la fenêtre, cliquez sur **action complémentaire**. Dans la fenêtre qui s'ouvre, sélectionnez Kaspersky Anti-Spam dans la liste déroulante puis cliquez sur **OK**.

d. Dans la fenêtre des exclusions de la règle, cliquez sur **Suivant** sans cocher aucune case.

e. Dans la fenêtre finale de création de la règle, vous pouvez changer son nom (le nom par défaut est Kaspersky Anti-Spam). Assurez-vous que la case **Activer la règle** est cochée puis, cliquez sur **Terminer**.

3. Par défaut, la nouvelle règle sera ajoutée en tête de la liste des règles de la fenêtre **Règles et notifications**. Déplacez cette règle à la fin de la liste si vous voulez qu'elle soit appliquée en dernier lieu au message.

Tous les messages qui arrivent dans la boîte aux lettres sont traités sur la base des règles. L'ordre d'application des règles dépend de la priorité associée à chaque règle. Les règles sont appliquées dans l'ordre de la liste. Chaque règle a une priorité inférieure à la règle précédente. Chaque règle a une priorité inférieure à la règle précédente.

Si vous ne souhaitez pas que le message, après l'exécution d'une règle quelconque, soit traité par une règle d'Anti-Spam, il faudra cocher la case **arrêter le traitement ultérieur des règles** dans les paramètres de cette règle (cf. 3ème étape de la fenêtre de création des règles).

Si vous avez de l'expérience dans la création de règles de traitement des messages dans Microsoft Office Outlook, vous pouvez créer une règle propre à l'Anti-Spam sur la base de l'algorithme proposé ci-dessus.

Les paramètres de traitement du courrier indésirable et du courrier indésirable potentiel dans Microsoft Office Outlook sont repris sur l'onglet **Anti-Spam** du menu **Service** → **Paramètres**.

CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE DANS MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

La fenêtre de configuration du traitement du courrier indésirable s'ouvre à la première ouverture du client de messagerie après l'installation de l'application.

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par l'Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**.

Les règles de traitement suivantes sont prévues aussi bien pour le courrier indésirable que pour le courrier indésirable potentiel :

- **Placer dans le dossier** : le courrier indésirable est placé dans le dossier de la boîte aux lettres que vous aurez spécifié.
- **Copier dans le dossier** : une copie du message est créée et placée dans le dossier indiqué. La copie originale reste dans le dossier **Entrant**.
- **Supprimer** : supprime le courrier indésirable de la boîte aux lettres de l'utilisateur.
- **Ignorer** : laisse le message électronique dans le dossier **Entrant**.

Pour activer la règle de traitement requise, choisissez les valeurs souhaitées dans la liste déroulante du groupe **Courrier indésirable** ou **Courrier indésirable potentiel**.

En cas d'entraînement de l'Anti-Spam à l'aide d'un client de messagerie (cf. section "Apprentissage à l'aide du client de messagerie" à la page 108) le message sélectionné est envoyé à Kaspersky Lab en tant qu'exemple de courrier indésirable. Cliquez sur le lien **Avancé lors de l'identification manuelle d'un message en tant que message non sollicité** afin de sélectionner le mode d'envoi des exemples de courrier indésirable dans la fenêtre qui s'ouvre. Cliquez sur le lien **Configurer l'envoi des échantillons de spam à Kaspersky Lab** pour sélectionner le mode d'envoi des échantillons de courrier normal (échantillons considérés par erreur comme du courrier indésirable).

Pour ouvrir la fenêtre de configuration du traitement du courrier indésirable, cliquez sur le bouton **Configuration** situé à côté des autres boutons de l'Anti-Spam dans la barre des tâches : **Courrier indésirable** et **Courrier normal**.

CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE DANS THE BAT!

Les actions à exécuter sur le courrier indésirable et le courrier indésirable potentiel dans The Bat! sont définies à l'aide des outils du client.

Pour passer à la configuration des règles de traitement du courrier indésirable dans The Bat!, procédez comme suit :

1. Sélectionnez l'élément **Configuration** dans le menu **Propriétés** du client de messagerie.
2. Sélectionnez le nœud **Protection contre le courrier indésirable** dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable sont appliqués à tous les modules de l'Anti-Spam installés sur l'ordinateur compatibles avec The Bat!

Vous devez définir le niveau d'évaluation et indiquer comment agir sur les messages correspondant au niveau défini (pour l'Anti-Spam, la probabilité que le message est un exemple de courrier indésirable) :

- supprimer les messages dont le niveau d'évaluation est supérieur au niveau indiqué ;
- déplacer les messages du niveau défini dans un dossier spécial pour les messages non sollicités ;
- déplacer les messages non sollicités marqués d'un en-tête spécial dans le dossier du courrier indésirable ;
- laisser les messages non sollicités dans le dossier **Entrant**.

Suite au traitement des messages électroniques, Kaspersky Internet Security attribue le statut courrier indésirable ou courrier indésirable potentiel en fonction d'indice dont vous pouvez modifier la valeur. Dans The Bat!, on retrouve un algorithme spécial d'évaluation des messages qui repose également sur les facteurs de courrier indésirable. Afin d'éviter les écarts entre l'indice de courrier indésirable dans Kaspersky Internet Security et dans The Bat!, tous les messages analysés par l'Anti-Spam reçoivent une évaluation correspondant à l'état du message : courrier normal - 0%, courrier indésirable potentiel - 50%, courrier indésirable - 100%. Ainsi, l'évaluation du message dans The Bat! correspond non pas au facteur du message attribué par l'Anti-Spam mais bien au facteur correspondant à l'état.

Pour de plus amples informations sur l'évaluation du courrier indésirable et sur les règles de traitement, consultez la documentation relative au client de messagerie The Bat!

CONFIGURATION DU TRAITEMENT DU COURRIER INDESIRABLE DANS THUNDERBIRD

Par défaut, le courrier qui est considéré comme courrier indésirable ou courrier indésirable potentiel par Anti-Spam est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**. Dans Thunderbird, l'exécution des actions sur ces messages requiert l'utilisation des règles du menu **Outils**□✹ Filtres de messages (pour en savoir plus sur l'utilisation de ce client de messagerie, consultez l'aide de Mozilla Thunderbird).

Le module externe de l'Anti-Spam pour Thunderbird permet d'étudier les messages reçus et envoyés à l'aide de ce client de messagerie et de vérifier si le courrier contient des messages non sollicités. Le module est intégré à Thunderbird et

transmet les messages à l'Anti-Spam afin qu'ils puissent être analysés à l'aide de la commande du **Outils** ✹ Traquer les indésirables dans ce dossier. Donc, à la place de Thunderbird, c'est Kaspersky Internet Security effectue le contrôle du courrier. Les fonctions de Thunderbird ne sont en rien modifiées.

L'état du module d'extension de l'Anti-Spam se reflète sous la forme d'icône dans la ligne d'état de Thunderbird. Une icône grise indique qu'un problème s'est présenté dans le fonctionnement du module externe ou que le composant Anti-Spam (à la page 103) est désactivé. Double clique sur l'icône, la fenêtre de configuration des paramètres Kaspersky Internet Security s'ouvre. Pour passer à la configuration des paramètres de l'**Anti-Spam**, cliquez sur le bouton **Configuration** dans le groupe **Anti-Spam**.

RESTAURATION DES PARAMETRES DE L'ANTI-SPAM PAR DEFAUT

Lorsque vous configurez l'Anti-Spam, vous pouvez décider à n'importe quel moment de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de protection contre le courrier indésirable par défaut, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-Spam** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de protection**.

ANTI-BANNIERE

L'Anti-bannière bloque les messages publicitaires situés sur des bannières spéciales dans l'interface de divers programmes installés sur votre ordinateur ou sur Internet.

Non seulement ces bannières ne présentent aucune information utile, mais en plus elles sont sources de distraction et augmentent le volume téléchargé. L'Anti-bannière bloque les bannières les plus répandues à l'heure actuelle grâce aux masques livrés avec Kaspersky Internet Security. Vous pouvez désactiver le blocage des bannières ou créer vos propres listes de bannières autorisées et interdites.

La liste des masques des bannières publicitaires les plus répandues a été constituée par les experts de Kaspersky Lab sur la base d'une étude spéciale et elle est reprise dans l'installation de Kaspersky Internet Security. Les bannières publicitaires correspondantes aux masques de cette liste seront bloquées par l'Anti-Bannière, pour autant que cette fonction soit activée. Pour bloquer les bannières dont les masques d'adresse ne figurent pas dans la liste standard, il faut utiliser l'analyseur heuristique (cf. section "Utilisation de l'analyse heuristique" à la page 123).

De plus, vous pouvez créer des listes "blanche" (cf. section "Constitution de la liste des adresses de bannières autorisées" à la page 124) et "noire" (cf. section "Constitution de la liste des adresses de bannières interdites" à la page 125) de bannières qui serviront pour décider de l'affichage ou non de la bannière.

L'Anti-bannière est désactivé après l'installation de Kaspersky Internet Security.

➧ *Afin de modifier les paramètres de fonctionnement de l'Anti-bannière, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
3. Pour le composant sélectionné, introduisez les modifications requises dans les paramètres.

DANS CETTE SECTION

UTILISATION DE L'ANALYSE HEURISTIQUE

Les bannières dont l'adresse ne figure pas dans la liste standard peuvent être analysée via l'analyse heuristique. Dans ce cas, Kaspersky Internet Security analysera les images chargées afin de repérer les indices caractéristiques des bannières. Sur la base des résultats de cette analyse, l'image peut être identifiée comme une bannière et bloquée.

➧ *Afin d'utiliser l'analyse heuristique, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Analyse**, cochez la case ☑ **Activer l'analyse heuristique**.

LES PARAMETRES COMPLEMENTAIRES DE FONCTIONNEMENT DU COMPOSANT

La liste des masques des bannières publicitaires les plus répandues a été constituée par les experts de Kaspersky Lab sur la base d'une étude spéciale et elle est reprise dans l'installation de Kaspersky Internet Security. Les bannières publicitaires correspondantes aux masques de cette liste seront bloquées par l'Anti-Bannière, pour autant que cette fonction soit activée.

Lors de la création de la liste des bannières autorisées / interdites, il est possible de saisir soit l'adresse IP de la bannière, soit son nom symbolique. Pour éviter les doubles emplois, vous pouvez utiliser une fonction supplémentaire qui permet de traduire l'adresse IP saisie en nom de domaine et vice-versa.

- *Pour désactiver l'utilisation de la liste des bannières livrée avec Kaspersky Internet Security, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'applicationet cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, dans le groupe **Méthodes d'analyse**, décochez la case ☑ **Ne pas utiliser la liste standard des bannières**.

- *Afin de pouvoir traduire les adresses IP des bannières saisies en nom de domaine (ou inversement), procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, dans le groupe **Méthodes d'analyse**, cochez la case ☑ **Traduire les adresses IP en nom de domaine**.

CONSTITUTION DE LA LISTE DES ADRESSES DE BANNIERES AUTORISEES

La liste blanche des bannières est composée par l'utilisateur lors de l'utilisation de Kaspersky Internet Security lorsqu'il n'est pas nécessaire de bloquer certaines bannières. Cette liste contient les masques pour l'affichage des bannières autorisées.

- *Pour ajouter un nouveau masque à la liste "blanche", procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, dans le groupe **Avancé**, cochez la case ☑ **Utiliser la liste blanche des adresses** et cliquez sur le bouton **Configuration**.
  4. Dans la fenêtre **Liste "blanche"** qui s'ouvre, cliquez sur le lien **Ajouter**.
  5. Saisissez le masque de la bannière autorisée dans la fenêtre **Masque d'adresse (URL)**. Pour désactiver un masque saisi sans pour autant le supprimer de la liste, il vous suffira de désélectionner la case ☑ située en regard de ce masque.

CONSTITUTION DE LA LISTE DES ADRESSES DE BANNIERES INTERDITES

Vous pouvez créer la liste des adresses de bannières interdites, qui seront bloquées par l'Anti-Bannière lors de leur détection.

Pour ajouter un nouveau masque à la liste "noire", procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Avancé**, cochez la case **Utiliser la liste noire des adresses** et cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Liste "noire"** qui s'ouvre, cliquez sur le lien **Ajouter**.
5. Saisissez le masque de la bannière autorisée dans la fenêtre **Masque d'adresse (URL)**. Pour désactiver un masque saisi sans pour autant le supprimer de la liste, il vous suffira de désélectionner la case située en regard de ce masque.

EXPORTATION / IMPORTATION DES LISTES DES BANNIERES

Vous pouvez copier les listes de bannières autorisées / interdites d'un ordinateur sur un autre. Lors de l'exportation de la liste, vous serez invité à copier uniquement l'élément sélectionné de la liste ou toute la liste. Lors de l'importation, vous pouvez ajouter les nouvelles adresses à la liste ou écraser la liste existante par la liste importée.

Pour copier les listes de bannières autorisées / interdites, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Anti-bannière** dans la rubrique **Protection**.
3. Pour le composant sélectionné, dans le groupe **Avancé** de liste qu'il faut copier, cliquez sur **Configuration**.
4. Dans la fenêtre **Liste "blanche"** (ou dans la fenêtre **Liste "noire"**) qui s'ouvre, cliquez sur les liens **Importer** ou **Exporter**.

CONTROLE PARENTAL

Le *Contrôle Parental* est un composant de l'application qui permet de contrôler l'accès des utilisateurs aux ressources Internet. L'objectif principal du contrôle parental est de limiter l'accès principalement aux ressources suivantes :

- Les sites Internet pour adultes ou les sites web sur la pornographie, les armes, les drogues ou incitant à la cruauté ou à la violence, etc. ;
- Les sites Internet dont le contenu peut provoquer une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites d'enchères).

Généralement, ces sites abritent une certaine quantité de programmes malveillants et le téléchargement de données depuis ces ressources (sites de jeux par exemple) entraîne une augmentation sensible du trafic Internet.

La restriction de l'accès aux ressources Internet pour l'utilisateur s'opère en lui attribuant un des trois profilsprédéfinis (cf. page 128) pour l'utilisation d'Internet. Il est permis, pour chaque profil, de définir des limites au niveau de l'affichage (cf. page 130) et de la durée d'utilisation des sites Internet (cf. page 134).

Tous les utilisateurs reçoivent par défaut le profil **Enfant** qui contient le plus grand nombre de restrictions. Le profil peut être associé à un compte utilisateur de Microsoft Windows. Dans ce cas, l'utilisateur pourra accéder aux sites Internet qui correspondent aux paramètres de son profil.

Dans le cas d'utilisation de plusieurs profils sous le même compte, il est recommandé de purger régulièrement le contenu du cache de votre navigateur Web (les pages Web sauvegardées, les fichiers temporaires, les fichiers "cookie", les mots de passe mémorisés). Dans le cas contraire, l'utilisateur avec le profil, possédant les privilèges minimaux , recevra l'accès aux pages Web, parcourus par l'utilisateur avec le profil sans restrictions.

L'accès au profil **Parent** ou **Adolescent** doit être protégé par un mot de passe. La permutation vers un profil (cf. page 128) protégé par un mot de passe est possible uniquement après avoir saisi ce dernier.

Chaque profil réglemente l'accès aux sites Internet selon un des niveaux de restrictions prédéfinis (cf. page 129). Le niveau de restriction est un ensemble de paramètres qui régit l'accès aux sites d'un certain type.

Il est conseillé de configurer la protection par mot de passe de Kaspersky Internet Security (cf. section "Autodéfense de Kaspersky Internet Security" à la page 169) afin d'éviter une désactivation non autorisée du composant.

Après l'installation de Kaspersky Internet Security, le Contrôle Parental est désactivé.

➡ *Afin de modifier les paramètres de fonctionnement du Contrôle Parental, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Modifiez les paramètres du composant selon vos besoins.

DANS CETTE SECTION

ALGORITHME DE FONCTIONNEMENT DU COMPOSANT

Examinons l'algorithme de fonctionnement du composant **Contrôle Parental**.

1. Une fois que l'utilisateur s'est identifié dans le système, le profil correspondant à cet utilisateur est chargé.
2. Lorsque l'utilisateur tente d'accéder à un site Web, le Contrôle Parental exécute les actions suivantes :
   - vérification d'éventuelles restrictions selon l'heure (cf. page 134) ;
   - comparaison de l'URL de la page demandée la liste des adresses autorisées en mode d'accès exclusif à certains sites Internet ;
   - en mode restrictif, le composant effectue les actions suivantes :
     - comparaison de l'URL de la page demandée avec la liste des adresses autorisées et interdites ;
     - analyse du contenu de la page Internet pour vérifier une éventuelle concordance avec une catégorie interdite.

Si une de ces conditions n'est pas remplie, alors l'accès au site est bloqué. Dans le cas contraire, la page s'ouvre dans le navigateur.

Si dans votre réseau un serveur proxy est utilisé et qu'il utilise un port hors-série, alors il est nécessaire d'ajouter ce port à la liste des ports contrôlés (cf. section "Constitution de la liste des ports contrôlés" à la page 177). Autrement le Contrôle Parental peut fonctionner incorrectement et laisser passer les sites Web interdits.

Si à la fin de l'analyse, la page demandée est considérée comme interdite, vous ne pourrez pas y accéder. Dans le cas contraire, la page s'ouvre dans le navigateur.

UTILISATION DES PROFILS

Un profil est un ensemble de règles qui limitent l'accès de l'utilisateur à certains sites Internet. Vous pouvez choisir un des profils : **Enfant** (utilisé par défaut), **Adolescent** ou **Parent**.

Sur la base de l'âge, de l'expérience et d'autres caractéristiques de chaque groupe, une sélection optimale de règles a été définie pour chaque profil. Ainsi, le profil **Enfant** présente le maximum de restrictions tandis que le profil **Parent** n'en a aucune. Il est impossible de supprimer les profils prédéfinis ou d'en créer de nouveaux, mais vous pouvez modifier les paramètres des profils **Enfant** et **Adolescent** selon vos besoins.

Il faut obligatoirement définir un mot de passe pour les profils **Parent** et **Adolescent**. Le mot de passe devra être saisi pour pouvoir changer de profil (cf. page 128).

Pour utiliser les profiles Adolescent ou Adulte, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Adolescent** ou sous l'onglet **Parent** cochez la case **Utiliser le profil** et saisissez le mot de passe dans le champ du même nom.

Pour associer le profil au compte utilisateur Microsoft Windows, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Adolescent** ou sous l'onglet **Parent** dans le groupe **Liste des utilisateurs**, cliquez sur **Ajouter**.
5. Dans la fenêtre **Utilisateurs** qui s'ouvre, vous verrez la liste des comptes utilisateurs locaux. Sélectionnez le compte requis dans la liste puis cliquez sur **OK**.

   Si vous devez ajouter un compte qui ne figure pas dans la liste, utilisez les méthodes standards de Microsoft Windows. Pour ce faire, cliquez sur le bouton **Chercher** et dans la fenêtre Microsoft Windows standard qui s'ouvre, indiquez le compte utilisateur requis (pour de plus amples renseignements, consultez l'aide du système d'exploitation).

   Pour que le profil configuré ne s'applique pas au compte de l'utilisateur, sélectionnez cet utilisateur dans le groupe **Liste des utilisateurs** puis cliquez sur le lien **Supprimer**.

PERMUTATION DES PROFILS

Le profil actif peut être modifié. Ceci peut être utile si le profil actif possède des restrictions au niveau de l'accès à Internet et qu'il ne vous permet pas de naviguer en toute liberté.

Vous pouvez changer de profil de deux manières :

- depuis la fenêtre de configuration des paramètres de l'application (cf. section "Fenêtre de configuration des paramètres de l'application" à la page 46) ;
- depuis le menu contextuel (cf. section "Menu contextuel" à la page 42).

Le changement de profil est limité à l'aide d'un mot de passe. Aucun mot de passe n'est requis pour passer à l'onglet **Enfant**.

- *Pour changer le profil de l'utilisateur depuis la fenêtre de configuration de l'application, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
  3. Dans la liste déroulante, sélectionnez le nom du profil, cliquez sur **Appliquer** et, le cas échéant, indiquez le mot de passe.

- *Pour changer le profil de l'utilisateur depuis le menu contextuel de l'application, procédez comme suit :*

  1. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
  2. Sélectionnez l'option **Contrôle Parental** dans le menu déroulant.
  3. Sélectionnez le profil requis dans le menu déroulant.
  4. Dans la fenêtre **Permutation du profil** qui s'ouvre, saisissez le mot de passe. Cette fenêtre n'apparaît pas lors du passage au profil **Enfant**.

- *Pour modifier le mot de passe associé au profil de l'utilisateur, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
  4. Dans la fenêtre qui s'ouvre, sous l'onglet **Adolescent** ou sous l'onglet **Parent**, définissez le mot de passe dans le champ du même nom.

MODIFICATION DU NIVEAU DE RESTRICTION

Le Contrôle Parental assure le contrôle de l'accès des utilisateurs de l'ordinateur aux ressources Internet selon l'un des niveaux prédéfinis.

Si aucun des niveaux de restriction ne répond à vos attentes, vous pouvez procéder à une configuration complémentaire des paramètres de contrôle. Dans ce cas, sélectionnez le niveau le plus proche de vos souhaits en guise de point de départ et modifiez-en les paramètres.

Le profil **Parent** n'est contraint à aucune restriction.

- *Pour modifier le niveau de restriction, agissez de la manière suivante :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
  3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
  4. Dans la fenêtre qui s'ouvre, sous l'onglet du profil requis (**Enfant** ou **Adolescent**), réglez le niveau de restriction souhaité à l'aide du curseur dans le groupe **Niveau de restrictions**.

Pour modifier les paramètres du niveau de restriction, agissez de la manière suivante :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet du profil requis (**Enfant** ou **Adolescent**), réglez le niveau de restriction souhaité à l'aide du curseur dans le groupe **Niveau de restrictions** puis cliquez sur le bouton **Configuration**.

5. Dans la fenêtre qui s'ouvre, imposez des restrictions sur l'affichage des sites Internet (cf. page 130), sur la durée d'accès à Internet (cf. page 134), définissez le niveau d'analyse heuristique (cf. page 134) et composez la liste des catégories de sites Internet interdites (cf. page 133). Le niveau de restriction **Autre** est ainsi créé selon les paramètres de protection que vous aurez définis. Pour revenir aux paramètres de restriction standard, cliquez sur le bouton **Par défaut** dans le groupe **Niveau de restrictions**.

RESTRICTIONS SUR LA CONSULTATION DES SITES INTERNET

Vous pouvez associer des restrictions sur la consultation de certains sites aux profils **Enfant** et **Adolescent**. Le Contrôle Parental propose deux méthodes pour restreindre l'accès aux sites Internet :

- Le blocage de l'accès à tous les sites Internet, hormis certaines exceptions. Ces restrictions sont en vigueur si seul le mode d'accès à certaines URL a été activé. Dans ce mode, la configuration consiste à établir une liste d'adresses autorisées (cf. page131).

- Le blocage de l'accès aux sites Internet sur la base de divers paramètres. Le mode restrictif est activé et la décision d'autoriser ou non l'accès à un site est prise sur la base de diverses conditions :

  - Présence de l'URL de la page ouverte dans la liste des adresses autorisées (cf. page 131) ou interdites (cf. page 132) ;

  - Appartenance d'un site Internet à l'une des catégories interdites.

Pour activer le mode restrictif du Contrôle Parental pour le profil Enfant ou Adolescent, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, choisissez une des options proposées :

   - **Permettre uniquement la consultation des adresses Internet autorisées** : si nécessaire, activez le mode d'accès à certaines URL uniquement ;

   - **Définir les restrictions** : si nécessaire, activez le mode restrictif.

CONSTITUTION D'UNE LISTE D'URL AUTORISEES

Il est possible d'autoriser l'accès à certaines URL pour les profils **Enfant** et **Adolescent**. Pour ce faire, il suffit d'ajouter le site à la liste des URL autorisées.

Si le mode d'accès à des sites définis est activé (option **Permettre uniquement la consultation des adresses Internet autorisées**), alors l'accès à n'importe quel site qui ne figure pas dans la liste des URL autorisées sera bloqué.

Si le mode d'accès avec restrictions est activé (option **Définir les restrictions**), alors l'accès aux ressources peut être limité sur la base de leur appartenance à des catégories définies. Il est possible également de limiter clairement l'accès à des sites particuliers. Pour ce faire, il faut ajouter les adresses de ces ressources Internet dans la liste d'adresses interdites.

Le site ajouté à la liste des URL autorisées peut appartenir à une des catégories d'URL interdites (cf. page 133). Dans ce cas, la ressource sera accessible même si le filtre des sites de la catégorie correspondante est activé.

Exemple : vous ne souhaitez pas que votre enfant ait accès aux sites pour adultes ou aux sites qui pourraient entraîner une perte de temps ou d'argent. Mais vous devez pouvoir envoyer des messages électroniques à votre enfant.

Sélectionnez le profil **Enfant**. Dans ce cas, il est conseillé d'utiliser le niveau **Recommander** qui sera modifié de la manière suivante : ajout de restriction sur l'utilisation des chats et des messageries en ligne et ajout dans une liste des adresses Internet autorisées du service de messagerie où votre enfant possède un compte. Ainsi, votre enfant aura accès uniquement à cette messagerie.

- *Pour ajouter une nouvelle adresse ou un masque à la liste des adresses autorisées en mode d'accès exclusif à certains sites Internet, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.
5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, cliquez sur le bouton **Liste**.
6. Dans la fenêtre **Liste des URL autorisées** qui s'ouvre, cliquez sur **Ajouter**.
7. Dans la fenêtre **Masque d'adresse (URL)**, introduisez une adresse ou un masque.

   Si vous souhaitez exclure une adresse ou un masque de la liste sans la supprimer, désélectionnez la case en regard.

- *Pour ajouter une nouvelle adresse ou un masque à la liste des adresses autorisées en mode restrictif, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.
3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.
4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, cliquez sur le bouton **Exclusions**.

6. Dans la fenêtre **Liste des URL autorisées** qui s'ouvre, cliquez sur **Ajouter**.

7. Dans la fenêtre **Masque d'adresse (URL)**, introduisez une adresse ou un masque.

   Si vous souhaitez exclure une adresse ou un masque de la liste sans la supprimer, désélectionnez la case en regard.

CONSTITUTION D'UNE LISTE D'URL INTERDITES

Dans le mode restrictif, le Contrôle Parental (option **Utiliser les restrictions définies**) limite l'accès aux sites sur la base de l'appartenance de ceux-ci à des catégories définies (cf. section "Sélection des catégories d'URL interdites" à la page 133). Il est possible de limiter clairement l'accès à des sites particuliers. Pour ce faire, il faut ajouter l'adresse à la liste des URL interdites.

Pour ajouter une nouvelle adresse ou un masque à la liste des adresses interdites dans ce mode, procédez comme suit :

1. Ouvrez la fenêtre principale enêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, cliquez sur le bouton **Liste**.

6. Dans la fenêtre **Liste des URL interdites** qui s'ouvre, cliquez sur **Ajouter**.

7. Dans la fenêtre **Masque d'adresse (URL)**, introduisez une adresse ou un masque.

   Si vous souhaitez exclure une adresse ou un masque de la liste sans la supprimer, désélectionnez la case en regard.

EXPORTATION/IMPORTATION D'UNE LISTE D'URL

Si vous avez déjà constitué une liste d'URL autorisées ou interdites, vous pouvez l'enregistrer dans un fichier séparé. Par la suite, vous pourrez importer la liste depuis ce fichier afin de ne pas devoir la créer manuellement. L'exportation/l'importation de la liste peut être utile si vous souhaitez définir des paramètres similaires pour les profils **Enfant** et **Adolescent**.

L'exportation/l'importation sont accessibles uniquement en mode restrictif (option **Définir les restrictions**).

Pour enregistrer la liste des URL dans un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, ouvrez la liste requise :

   - Liste des URL autorisées en mode restrictif : cliquez sur le bouton **Exclusions** ;
   - Liste des URL interdites en mode restrictif : cliquez sur le bouton **Liste** ;

6. Dans la fenêtre qui s'ouvre contenant la liste d'URL, cliquez sur le lien **Exporter**.

7. Dans la fenêtre **Enregistrer sous** qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci.

Pour charger la liste des URL depuis un fichier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, ouvrez la liste requise :

   - Liste des URL autorisées en mode restrictif : cliquez sur le bouton **Exclusions** ;
   - Liste des URL interdites en mode restrictif : cliquez sur le bouton **Liste** ;

6. Dans la fenêtre qui s'ouvre contenant la liste d'URL, cliquez sur le lien **Importer**.

7. Dans la fenêtre **Ouvrir le fichier** qui s'ouvre, saisissez le chemin d'accès au fichier.

SELECTION DES CATEGORIES D'URL INTERDITES

Le Contrôle Parental analyse le contenu des sites Internet sur la base de mots clés en rapport avec un thème en particulier. Si le nombre de mots de la catégorie définie dépasse le seuil admis, l'accès à ce site est bloqué. La restriction de l'ouverture des URL en fonction de catégories n'est possible que si le mode imposant les restrictions (cf. page 130) a été activé.

La base des mots clés est livrée avec Kaspersky Internet Security et elle est actualisée en même temps que les bases et les modules de l'application.

La liste des catégories interdites se limite à la liste par défaut. La création de catégories interdites personnalisées n'est pas prise en charge.

Pour choisir les catégories de sites interdits pour les profils Enfant ou Adolescent, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Restrictions**, cochez la case **Bloquer les URL selon les catégories**.

6. Cochez les cases en regard des catégories souhaitées.

UTILISATION DE L'ANALYSE HEURISTIQUE

Par défaut, l'analyse des URL qui vise à déterminer si elles appartiennent aux catégories interdites repose sur la consultation de la base des mots clés. L'analyse heuristique est utilisée pour identifier les sites qui ne peuvent être reconnus à l'aide de ces bases. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Vous pouvez définir également le niveau de détail de l'analyse. Le niveau garantit l'équilibre entre la charge des ressources d'une part et la minutie et la durée de l'analyse d'autre part. Plus le niveau de détails est élevé, plus l'analyse utilise de ressources et plus longtemps elle dure.

Des faux positifs peuvent apparaître lors d'une analyse approfondie.

Pour commencer à utiliser l'analyse heuristique et définir le niveau de détail de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil (**Enfant** ou **Adolescent**) dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Avancé**, cochez la case **Activer l'analyse heuristique** et définissez le niveau de détail de l'analyse à l'aide du curseur.

SELECTION DE L'ACTION A EXECUTER EN CAS DE TENTATIVE D'ACCES A DES URL INTERDITES

Lorsque l'utilisateur tente d'accéder à la ressource Internet sollicité, le Contrôle Parental exécute l'action définie.

Afin de choisir l'action qui sera exécutée par le composant en cas de tentative d'accès à un site interdit, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet du profil requis (**Enfant** ou **Adolescent**), sélectionnez l'action dans le groupe du même nom.

RESTRICTION D'ACCES SELON L'HEURE

Vous pouvez limiter le temps que peut passer un utilisateur sur Internet. Avec cela, trois types de restrictions sont possibles. Par défaut, la restriction est établie selon les paramètres d'affichage. Vous pouvez modifier les paramètres de

restriction selon l'heure à 30 minutes près. Outre la définition de plages horaires, vous pouvez limiter la durée totale d'utilisation d'Internet.

Exemple :

Pour le profil **Enfant**, vous avez limité l'utilisation totale d'Internet par jour à 3 heures et vous avez en plus autorisé l'accès uniquement entre 14h00 et 15h00. En fin de compte, l'accès à Internet sera autorisé uniquement durant cet intervalle, quelle que soit la durée globale d'utilisation admise.

Pour limiter la durée d'utilisation d'Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Contrôle Parental** dans la rubrique **Protection**.

3. Pour le composant sélectionné, cliquez sur le bouton **Configuration**.

4. Sous l'onglet portant le nom du profil (**Enfant** ou **Adolescent**) dont vous allez modifier les paramètres, cliquez sur le bouton **Configuration**.

5. Dans la fenêtre **Configuration du profil** qui s'ouvre, sous l'onglet **Programmation**, définissez les paramètres requis.

   Pour établir des restrictions dans l'utilisation d'Internet par jour, cochez la case ☑ **Limiter l'utilisation quotidienne d'Internet** puis, définissez les restrictions.

   La programmation de l'accès à Internet s'opère via la sélection de plage horaire dans le tableau. Les lignes correspondent aux jours de la semaine, colonnes – intervalles de 30 minutes sur l'échelle du temps. En fonction des paramètres régionaux du système d'exploitation, l'heure peut être au format 12 heures ou 24 heures. Les couleurs des cellules du tableau reflètent les restrictions établies : la couleur rouge indique que l'accès aux ressources Internet est interdit et jaune – accès limité selon les restrictions d'affichage (cf. page 130).

Si vous utilisez les deux modes de restriction dans le temps et que la valeur d'un dépasse la valeur de l'heure au niveau du temps admis, c'est la durée la plus courte qui sera prise en compte.

ANALYSE DE L'ORDINATEUR

La recherche de virus et de vulnérabilités sur l'ordinateur est une des principales tâches qui garantira la protection de l'ordinateur. L'analyse met en évidence la diffusion d'un code malveillant qui, pour une raison quelconque, n'avait pas été découvert par la protection contre les programmes malveillants. La recherche de vulnérabilités détermine si les applications présentent des vulnérabilités qui pourraient être exploitées par les individus mal intentionnés pour diffuser des objets malveillants et accéder aux données personnelles.

Les experts de Kaspersky Lab ont élaboré des tâches d'analyse (cf. page 136), dont l'analyse des disques amovibles (cf. page 142), et la tâche de recherche de vulnérabilités dans le système et les applications (cf. page 146).

Pour modifier les paramètres d'une tâche d'analyse quelconque, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**, **Recherche de vulnérabilités**).
3. Introduisez les modifications requises dans les paramètres de la tâche sélectionnée.

DANS CETTE SECTION

RECHERCHE DE VIRUS

Les experts de Kaspersky Lab ont identifiés les tâches suivantes pour la recherche de virus sur votre ordinateur :

- **Analyse des Objets**.Les objets sélectionnés par l'utilisateur sont analysés. L'analyse peut porter sur n'import quel objet du système de fichiers de l'ordinateur. Dans le cadre de cette tâche, vous pouvez configurer l'analyse des disques amovibles.
- **Analyse Complète**. Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.
- **Analyse Rapide**. L'analyse porte sur les objets chargés au démarrage du système d'exploitation.

Les tâches d'analyse rapide et complète sont des tâches spécifiques. Il est déconseillé de modifier la liste des objets à analyser pour ces tâches.

Chaque tâche d'analyse est exécutée dans une zone définie et peut être lancée selon un horaire défini. L'ensemble des paramètres des tâches d'analyse définissent le niveau de protection. Il existe trois niveaux par défaut.

Après le lancement de la tâche d'analyse, la progression de cette dernière est présentée dans la rubrique **Analyse** de la fenêtre principale de Kaspersky Internet Security dans le champ sous le nom de la tâche exécutée. Quand l'application découvre une menace, elle exécute l'action définie.

Les informations sur les résultats de la recherche de menaces sont consignées dans le rapport de Kaspersky Internet Security.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (par exemple : via **l'Assistant** ou sur le **Bureau**, etc.). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel de Microsoft Windows d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

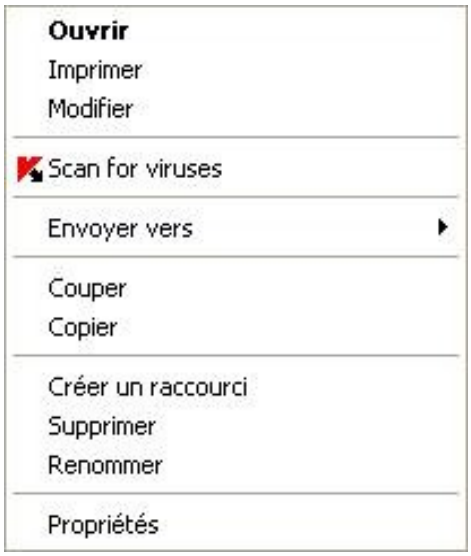


Illustration 9: Menu contextuel de Microsoft Windows

Vous pouvez également accéder au rapport sur l'analyse où vous pourrez voir des informations complètes sur les événements survenus durant l'exécution des tâches.

VOIR EGALEMENT

LANCEMENT DE L'ANALYSE

L'analyse peut être lancée des manières suivantes :

- depuis le menu contextuel (cf. section "Menu contextuel" à la page 42) de Kaspersky Internet Security ;
- depuis la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) de Kaspersky Internet Security ;
- via un raccourci créé (cf. page 139) au préalable.

Les informations relatives à l'exécution de la tâche sont affichées dans la fenêtre principale de Kaspersky Internet Security.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc.).

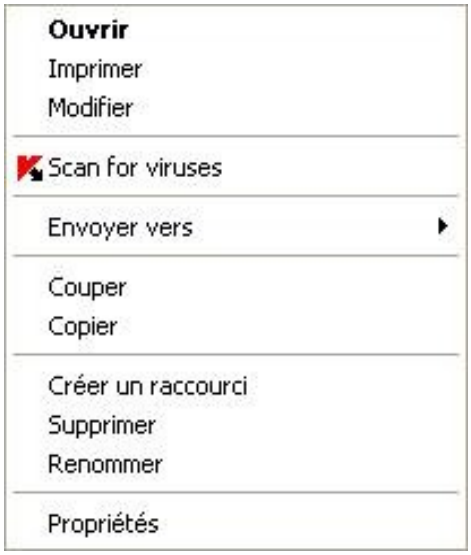


Illustration 10: Menu contextuel de Microsoft Windows

Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :

1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.
2. Double-cliquez sur le raccourci pour lancer la tâche. La progression de la tâche est illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**.

Pour lancer la recherche d'éventuels virus depuis le menu contextuel de l'application, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Rechercher d'éventuels virus**.
3. Dans la fenêtre principale de Kaspersky Internet Security qui s'ouvre, dans la rubrique **Analyse**, cliquez sur le bouton portant le nom de la tâche qui vous intéresse.

Pour lancer l'analyse complète de l'ordinateur, choisissez l'option **Analyse complète de l'ordinateur** dans le menu contextuel L'analyse complète de l'ordinateur sera lancée. La progression de la tâche est illustrée dans la fenêtre principale de Kaspersky Internet Security dans la rubrique **Analyse**.

- *Pour lancer la recherche d'éventuels virus depuis la fenêtre principale de l'application :*

  1. Ouvrez la fenêtre principale de l'application.
  2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
  3. Cliquez sur le bouton portant le nom de la tâche qui vous intéresse.

- *Pour lancer la recherche d'éventuels virus dans un objet sélectionné depuis le menu contextuel de Microsoft Windows, procédez comme suit :*

  1. Cliquez avec le bouton droit de la souris sur le nom de l'objet sélectionné.
  2. Dans le menu contextuel qui s'ouvre, sélectionnez le point **Rechercher d'éventuels virus**. La progression et le résultat d'exécution de la tâche sont illustrés dans la fenêtre ouverte.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'UNE TACHE

Il est possible de créer des raccourcis pour accélérer le lancement des analyses complètes et rapides. Il est ainsi possible de lancer la tâche d'analyse requise sans devoir ouvrir la fenêtre principale de l'application ou le menu contextuel.

- *Pour créer un raccourci pour le lancement de l'analyse, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
  3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le lien **Créer un raccourci** situé à côté du nom de la tâche envisagée (**Analyse Rapide** ou **Analyse Complète**).
  4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Une liste d'objets à analyser est associée par défaut à chaque tâche de recherche d'éventuels virus. Ces objets peuvent être des objets du système de fichiers de l'ordinateur (par exemple, les disques logiques, les **bases de messagerie**) ainsi que des objets d'autres types (par exemple, des disques de réseau). Vous pouvez introduire des modifications dans cette liste.

L'objet ajouté apparaît désormais dans la liste. Si au moment d'ajouter l'objet, vous avez coché la case **Sous-répertoires compris**, l'analyse se fera à tous les niveaux.

Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le lien **Supprimer**.

Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

Outre la suppression des objets, il est possible également de les exclure temporairement de l'analyse. Pour ce faire, sélectionnez l'objet dans la liste et désélectionnez la case située à gauche de son nom.

Si la couverture d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse !

Pour constituer la liste des objets de l'analyse des objets, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.
3. Cliquez sur le lien **Ajouter**.
4. Dans la fenêtre **Sélection de l'objet à analyser** qui s'ouvre, sélectionnez l'objet et cliquez sur le bouton **Ajouter**. Une fois que vous aurez ajoutés les objets requis, cliquez sur le bouton **OK**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

Pour composer la liste des objets pour les analyses complète ou rapide, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Analyse Complète** (**Analyse Rapide**).
3. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **<Nom de l'analyse>: liste des objets** qui s'ouvre, constituez la liste à l'aide des liens **Ajouter**, **Modifier**, **Supprimer**. Pour exclure un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

MODIFICATION DU NIVEAU DE PROTECTION

Le niveau de protection désigne un ensemble prédéfini de paramètres d'analyse. Les experts de Kaspersky Lab ont configuré trois niveaux de protection : Vous choisissez le niveau en fonction de vos préférences. Vous avez le choix parmi les niveaux de protection suivants :

- **Elevé.** Choisissez ce niveau si vous estimez que le risque d'infection de votre ordinateur est élevé.
- **Recommandé**. Ce niveau convient à la majorité des cas et son utilisation est conseillée par les experts de Kaspersky Lab.
- **Bas.** Si vous utilisez des applications gourmandes en mémoire vive, sélectionnez le niveau faible car la sélection de fichiers à analyser à ce niveau est moindre.

Si aucun des niveaux proposés ne répond à vos besoins, vous pouvez configurer vous-même les paramètres de fonctionnement. Le nom du niveau de protection devient **Utilisateur**. Pour restaurer les paramètres de fonctionnement par défaut de l'analyse, sélectionnez un des niveaux proposés.

Afin de modifier le niveau de protection, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée, dans le groupe **Niveau de protection**, définissez le niveau requis.

MODIFICATION DE L'ACTION A EXECUTER APRES LA DECOUVERTE D'UNE MENACE

Dès que Kaspersky Internet Security identifie une menace, il lui attribue un des états suivants :

- Etat de l'un des programmes malveillants (exemple, *virus*, *cheval de Troie*) ;

- *Probablement infecté* lorsqu'il est impossible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le fichier contient une séquence de code d'un virus inconnu ou le code modifié d'un virus connu.

Kaspersky Internet Security vous avertira s'il découvre des objets infectés ou potentiellement infectés suite à l'analyse. Il faut réagir à la menace découverte à l'aide d'une action sur l'objet. En cas de sélection de l'option **Confirmer l'action** pour les actions à réaliser sur l'objet identifié, le comportement de Kaspersky Internet Security sera le comportement par défaut. Vous pouvez modifier l'action. Par exemple, si vous êtes convaincu chaque objet découvert doit être soumis à une tentative de réparation et que vous ne souhaitez pas à chaque fois choisir l'option **Réparer** au moment de recevoir la notification sur la découverte d'un objet infecté ou suspect, choisissez l'option **Exécuter l'action. Réparer**.

Avant de réparer ou de supprimer un objet, Kaspersky Internet Security crée une copie de sauvegarde au cas où la restauration de l'objet serait requise par la suite ou si la possibilité de le réparer se présentait.

Si vous travaillez en mode automatique (cf. section "Etape. Sélection du mode de protection" à la page 31), Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. Pour les objets malveillants l'action sera **Réparer. Supprimer si la réparation est impossible** et pour les objets suspects : **Ignorer**.

➡ *Pour modifier l'action à exécuter sur les objets découverts, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée, dans le groupe **Action**, désignez l'action requise.

MODIFICATION DU TYPE D'OBJETS A ANALYSER

La définition du type d'objet à analyser est la fonction qui vous permet d'indiquer le format et la taille des fichiers qui seront analysés lors de l'exécution de la tâche d'analyse sélectionnée.

Il convient de ne pas oublier les caractéristiques suivantes des types de fichiers au moment de les sélectionner :

- La probabilité d'insertion d'un code malveillant dans les fichiers de certains formats (par exemple *txt*) et son activation ultérieure est relativement faible. Il existe également des formats de fichier qui contiennent ou qui pourraient contenir un code exécutable (par exemple, *exe*, *dll*, *doc*). Le risque d'infection par un code malveillant et d'activation est assez élevé pour ces fichiers.
- Il ne faut pas oublier qu'un individu mal intentionné peut envoyer un virus dans un fichier portant l'extension *txt* alors qu'il s'agit en fait d'un fichier exécutable renommé en fichier *txt*. Si vous sélectionnez l'option **Fichiers analysés selon l'extension**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Fichiers analysés selon le format**, la protection des fichiers et de la mémoire ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

➡ *Afin de modifier la priorité de la règle, exécutez l'opération suivante :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Types de fichiers** sélectionnez le paramètre requis.

OPTIMISATION DE L'ANALYSE

Vous pouvez réduire la durée d'analyse et accélérer le fonctionnement de Kaspersky Internet Security. Pour ce faire, il faut analyser uniquement les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse. Ce mode d'analyse s'applique aussi bien aux fichiers simples qu'aux fichiers composés.

Il est également possible de limiter la durée de l'analyse. Une fois la durée écoulée, l'analyse des fichiers sera suspendue.

Afin d'analyser uniquement les nouveaux fichiers et les fichiers modifiés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le groupe **Optimisation de l'analyse** cochez la case **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**.

Pour définir une restriction temporaire sur la durée de l'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sur l'onglet **Zone d'action**, groupe **Optimisation de l'analyse**, cochez la case **Ignorer les fichiers si l'analyse dure plus de**, et définissez la durée d'analyse dans le champ à côté.

ANALYSE DES DISQUES AMOVIBLES

Ces derniers temps, les objets malveillants qui exploitent les vulnérabilités du système d'exploitation pour se diffuser via les réseaux locaux et les disques amovibles se sont fort répandus.

Vous pouvez analyser les disques amovibles au moment où ils sont connectés à l'ordinateur. Pour ce faire, il faut sélectionner une des actions qu'exécutera Kaspersky Internet Security.

- **Ne pas analyser**. L'analyse automatique des disques amovibles connectés à l'ordinateur ne sera pas réalisée.
- **Confirmer auprès de l'utilisateur**. Par défaut, Kaspersky Internet Security demande à l'utilisateur de confirmer l'action à exécuter lorsque le disque amovible est connecté à l'ordinateur.
- **Analyse Complète**. Une fois que le disque amovible est connecté à l'ordinateur, les fichiers qu'il contient (selon les paramètres de la tâche Analyse complète) sont soumis à une analyse complète.
- **Analyse Rapide**. Lorsque les disques amovibles sont connectés, tous les fichiers sont analysés conformément aux paramètres de l'analyse rapide.

Afin de pouvoir analyser les disques amovibles lorsqu'ils sont connectés à l'ordinateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.

3. Dans le groupe **Analyse des disques amovibles à la connexion**, sélectionnez l'action et, le cas échéant, définissez la taille maximale du disque à analyser dans le champ inférieur.

ANALYSE DES FICHIERS COMPOSES

L'insertion de virus dans des fichiers composés (archives, bases de données, etc.) est une pratique très répandue. Pour identifier les virus dissimulés de cette façon, il faut décompacter le fichier composé, ce qui peut entraîner un ralentissement significatif de l'analyse.

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour ce faire, cliquez sur le lien situé en regard du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si vous sélectionnez le mode d'analyse uniquement des nouveaux fichiers et des fichiers modifiés (cf. page 142), il sera impossible de sélectionner un type de fichier composé.

Vous pouvez également définir la taille maximale du fichier composé à analyser. Les fichiers composés dont la taille dépasse la valeur limite ne seront pas analysés.

L'analyse des fichiers de grande taille au moment de l'extraction des archives aura lieu même si la case ☑ **Ne pas décompacter les fichiers composés de grande taille** est cochée.

➡ *Pour modifier la liste des fichiers composés à analyser, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Zone d'action** dans le bloc **Analyse des fichiers composés** sélectionnez les types de fichiers composés à analyser.

➡ *Pour définir la taille maximale des fichiers composés qui seront analysés, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, cliquez sur **Avancé** dans le groupe **Analyse des fichiers composés** de l'onglet **Zone d'action**.
5. Dans la fenêtre **Fichiers composés** qui s'ouvre, cochez la case ☑ **Ne pas décompacter les objets composés de grande taille** et définissez la taille maximale des objets à analyser dans le champ en dessous.

TECHNOLOGIE D'ANALYSE

Vous pouvez indiquer également la technologie qui sera utilisée lors de l'analyse. Vous avez le choix entre les technologies suivantes :

- **iChecker**. Cette technologie permet d'accélérer l'analyse en excluant certains objets. L'exclusion d'un objet de l'analyse est réalisée à l'aide d'un algorithme spécial qui tient compte de la date d'édition des signatures des menaces, de la date de l'analyse antérieure et de la modification des paramètres d'analyse.

Admettons que vous avez une archive qui a été analysée par Kaspersky Internet Security et auquel il a attribué l'état *non infecté*. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases de l'application, l'archive sera analysée à nouveau.

La technologie iChecker a ses limites : elle ne fonctionne pas avec les fichiers de grande taille et de plus, elle n'est applicable qu'aux objets dont la structure est connue de l'application (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

- **iSwift**. Cette technologie est un développement de la technologie iChecker pour les ordinateurs dotés d'un système de fichiers NTFS. Il existe certaines restrictions à la technologie iSwift : elle s'applique à l'emplacement particulier d'un fichier dans le système de fichiers et elle ne s'applique qu'aux objets des systèmes de fichiers NTFS.

Afin de modifier la technologie d'analyse des objets, exécutez l'opération suivante :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Technologies d'analyse**, définissez les paramètres requis.

MODIFICATION DE LA METHODE D'ANALYSE

Vous pouvez configurer certains paramètres d'analyse qui ont une influence sur la minutie de celle-ci. Le mode de recherche des menaces à l'aide des signatures des bases de l'application est toujours activé par défaut. De plus, il est possible d'agir sur diverses méthodes et technologies d'analyse (cf. page 143).

Le mode d'*analyse à l'aide des signatures* où Kaspersky Internet Security compare l'objet trouvé aux enregistrements de la base est toujours utilisé. Vous pouvez également choisir d'utiliser *l'analyse heuristique*. Cette méthode repose sur l'analyse de l'activité de l'objet dans le système. Si l'activité est caractéristique des objets malveillants, alors l'objet peut être considéré, avec forte probabilité, comme un objet malveillant ou suspect.

Il est également possible de choisir le niveau de détails de l'analyse heuristique : superficiel, moyen ou profond. Il suffit de déplacer le curseur sur la position souhaitée.

Outre ces méthodes d'analyse, vous pouvez également utiliser la recherche d'outils de dissimulation d'activité. Un outil de dissimulation d'activité est un utilitaire qui permet de dissimuler la présence de programmes malveillants dans le système d'exploitation. Ces utilitaires s'introduisent dans le système en masquant leur présence et celle des processus, des répertoires et des clés de registre de n'importe quel programme malveillant décrit dans la configuration de l'outil de dissimulation d'activité. Lorsque la recherche est activée, vous pouvez définir le niveau de détail d'identification des outils de dissimulation d'activité (Analyse approfondie). Dans ce cas, une recherche minutieuse de ces programmes sera lancée via l'analyse d'une grande quantité d'objets de divers types.

Pour utiliser les méthodes d'analyse requises, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Avancé**, dans le groupe **Méthodes d'analyse**, définissez les paramètres requis.

MODE DE LANCEMENT : PROGRAMMATION

Il est possible de programmer l'exécution automatique de l'analyse.

L'élément primordial à définir est l'intervalle selon lequel la tâche doit être exécutée. Pour ce faire, il faut définir les paramètres de la programmation pour l'option sélectionnée.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation** choisissez **Manuel** si vous souhaitez lancer la tâche d'analyse à l'heure qui vous convient. Pour lancer la tâche à intervalle régulier, sélectionnez l'option **Programmation** et définissez les paramètres d'exécution.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case **Lancer les tâches non exécutées**.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Vous pouvez définir le compte utilisateur sous les privilèges duquel la recherche de virus sera réalisée.

Pour définir le compte utilisé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

PARTICULARITE DU LANCEMENT PROGRAMME DES TACHES DE L'ANALYSE

Toutes les tâches d'analyse peuvent être lancées manuellement ou automatiquement selon un horaire défini.

Pour les tâches, lancées selon la programmation, vous pouvez utiliser la possibilité complémentaire : *suspendre l'analyse selon la programmation si l'écran de veille est actif ou l'ordinateur est débloqué*. Cette possibilité permet de reporter le lancement de la tâche jusqu'à ce que l'utilisateur ne termine pas son travail sur l'ordinateur. Ainsi, la tâche d'analyse ne va pas occuper les ressources de l'ordinateur pendant son fonctionnement.

Pour lancer l'analyse une fois que l'utilisateur terminera son travail, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Mode d'exécution**, cochez l'option ☑ **Suspendre l'analyse selon la programmation si l'écran de veille est actif et l'ordinateur est débloqué**.

RESTAURATION DES PARAMETRES D'ANALYSE PAR DEFAUT

Une fois que vous aurez configuré les paramètres d'exécution de la tâche, sachez que vous pourrez toujours revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de protection des fichiers par défaut, procédez comme suit :

1. Ouvrez la fenêtre principalede l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**).
3. Pour la tâche sélectionnée dans le groupe **Niveau de protection** cliquez sur le bouton **Par défaut**.

RECHERCHE DE VULNERABILITES

La tâche de recherche de vulnérabilités pose un diagnostic sur la sécurité du système et recherche les éventuelles vulnérabilités qui sont généralement exploitées par les individus mal intentionnés pour nuire.

Dans le cadre de cette étude, le système est analysé et l'application recherche les anomalies ou les corruptions dans les paramètres du système d'exploitation et du navigateur. Le diagnostic de la sécurité s'opère dans de nombreuses directions : par exemple, la recherche d'outils de dissimulation d'activité (programme pour le contrôle dissimulé d'un système compromis), recherche de services ou de paramètres vulnérables, collecte d'informations sur les processus, les pilotes, etc.

Le diagnostic des vulnérabilités peut prendre un certain temps. Une fois que le diagnostic est terminé, les informations recueillies sont analysées. L'analyse vise à évaluer les problèmes identifiés dans la sécurité du point de vue du danger qu'ils représentent pour le système.

Tous les problèmes identifiés au moment de l'analyse du système sont regroupés du point de vue du danger qu'il présente pour le système. Pour chaque groupe de problèmes, les experts de Kaspersky Lab proposent un ensemble d'actions dont l'exécution permettra de supprimer les vulnérabilités et les points problématiques du système. Trois groupes de problèmes et les actions correspondantes ont été identifiés :

- *Les actions vivement recommandées* permettent de supprimer les problèmes qui constituent une menace sérieuse pour la sécurité. Il est conseillé d'exécuter toutes les actions de ce groupe.

- *Les actions recommandées* visent à supprimer les problèmes qui peuvent présenter un danger potentiel. L'exécution des actions de ce groupe est également recommandée.

- *Les actions complémentaires* sont prévues pour supprimer les corruptions du système qui ne présentent actuellement aucun danger mais qui à l'avenir pourraient menacer la sécurité de l'ordinateur.

Les liens directs vers les correctifs critiques (mise à jour des applications) sont les résultats de la recherche des vulnérabilités potentielles dans le système d'exploitation et les applications installées.

Une fois la tâche de recherche de vulnérabilités lancées (cf. page 147), sa progression s'affiche dans la fenêtre principale de l'application et dans la fenêtre **Recherche de vulnérabilités** dans le champ **Fin**. Les vulnérabilités identifiées dans le système et dans les applications à la suite de l'analyse figurent dans cette même fenêtre sous les onglets **Vulnérabilités du système** et **Applications vulnérables**.

Les informations sur les résultats de la recherche de menaces sont consignées dans le rapport de Kaspersky Internet Security.

A l'instar de ce qui se fait pour les tâches d'analyse, il est possible, dans la section **Recherche de vulnérabilités** de la fenêtre de configuration de l'application, de définir un horaire d'exécution (cf. page 149) et de composer une liste d'objets à analyser (cf. page 148) pour la recherche de vulnérabilités. Par défaut, les applications installées sont choisies en guise d'objets à analyser.

VOIR EGALEMENT

LANCEMENT DE LA RECHERCHE DE VULNERABILITES

La recherche de vulnérabilités peut être lancée d'une des manières suivantes :

- depuis la fenêtre principale (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43) de Kaspersky Internet Security ;

- via un raccourci créé (cf. page 148) au préalable.

Les informations relatives à l'exécution de la tâche sont affichées dans la fenêtre principale de Kaspersky Internet Security ainsi que dans la fenêtre **Recherche de vulnérabilités**.

Pour lancer une tâche à l'aide d'un raccourci, procédez comme suit :

1. Ouvrez le répertoire dans lequel vous avez créé le raccourci.

2. Double-cliquez sur le raccourci pour lancer la tâche. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

Pour lancer la tâche de recherche de vulnérabilités depuis la fenêtre de l'application, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.

3. Cliquez sur le bouton **Recherche de vulnérabilités**.

4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Recherche de vulnérabilités**. La progression de la tâche sera présentée dans le champ **Fin**. Pour arrêter l'exécution de la tâche, cliquez à nouveau sur le bouton.

CREATION DE RACCOURCIS POUR LE LANCEMENT D'UNE TACHE

Pour accélérer le lancement de la recherche de vulnérabilités, l'application offre la possibilité de créer un raccourci. Il est ainsi possible de lancer la tâche sans devoir ouvrir la fenêtre principale de l'application.

Pour créer un raccourci pour le lancement de la recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Analyse**.

3. Dans la partie droite de la fenêtre, dans le groupe **Lancement rapide des tâches**, cliquez sur le bouton **Créer un raccourci** à côté du nom de la tâche (**Recherche de vulnérabilités**).

4. Dans la fenêtre qui s'ouvre, saisissez le chemin d'accès pour l'enregistrement du fichier ainsi que le nom de celui-ci. Par défaut, le raccourci prend le nom de la tâche et est créé dans le répertoire *Poste de travail* de l'utilisateur actuel de l'ordinateur.

COMPOSITION DE LA LISTE DES OBJETS A ANALYSER

Par défaut, la recherche de vulnérabilités possède sa propre liste d'objets à analyser. Ces objets sont le système d'exploitation et les applications installées. Il est possible également de désigner des objets complémentaires tels que les objets du système de fichiers de l'ordinateur (par exemple, les disques logiques ou les **Bases de messagerie**) ou des objets d'autres types (par exemple, les disques de réseau).

L'objet ajouté apparaît désormais dans la liste. Si au moment d'ajouter l'objet, vous avez coché la case ☑ **Sous-répertoires compris**, l'analyse se fera à tous les niveaux. Les objets ajoutés manuellement seront également soumis à l'analyse.

Pour supprimer un objet de la liste, sélectionnez-le et cliquez sur le lien **Supprimer**.

Les objets ajoutés à la liste par défaut ne peuvent être modifiés ou supprimés.

Outre la suppression des objets, il est possible également de les exclure temporairement de l'analyse. Pour ce faire, sélectionnez l'objet dans la liste et désélectionnez la case située à gauche de son nom.

Si la couverture d'analyse est vide ou si aucun des objets qu'elle contient n'a été coché, il ne sera pas possible de lancer la tâche d'analyse !

Pour constituer la liste des objets de la recherche de vulnérabilités, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de vulnérabilités** dans la rubrique **Analyse**.

3. Pour la tâche sélectionnée, dans le groupe **Objets à analyser**, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre **Recherche des vulnérabilités: liste des objets** qui s'ouvre, composez la liste à l'aides des liens **Ajouter**, **Modifier**, **Supprimer**. Pour exclure temporairement un objet quelconque de la liste, désélectionnez la case située en regard de celui-ci.

MODE DE LANCEMENT : PROGRAMMATION

Il est possible de programmer le lancement automatique de la recherche de vulnérabilités.

L'élément principal à déterminer est l'intervalle selon lequel la tâche doit être exécutée.

Si l'exécution est impossible pour une raison quelconque (par exemple, l'ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique dès que cela est possible.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de vulnérabilités** dans la rubrique **Analyse**.

3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Programmation** choisissez **Manuel** si vous souhaitez lancer la tâche d'analyse à l'heure qui vous convient. Pour lancer la tâche à intervalle régulier, sélectionnez l'option **Programmation** et définissez les paramètres d'exécution.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de vulnérabilités** dans la rubrique **Analyse**.

3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, groupe **Programmation**, cochez la case **Lancer les tâches non exécutées**.

MODE DE LANCEMENT : CONFIGURATION DU COMPTE UTILISATEUR

Vous pouvez définir le compte utilisateur sous les privilèges duquel la recherche de vulnérabilité sera réalisée.

Pour définir le compte utilisé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre, sélectionnez la tâche **Recherche de vulnérabilités** dans la rubrique **Analyse**.

3. Pour la tâche sélectionnée dans le groupe **Mode d'exécution** cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

MISE A JOUR

L'actualité de la protection est le garant de la sécurité de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillant apparaissent. Il est donc primordial de s'assurer que vos données sont bien protégées. Les informations relatives aux menaces et aux moyens de les neutraliser sont reprises dans les bases de Kaspersky Internet Security et c'est la raison pour laquelle la mise à jour des bases de l'application constitue un élément fondamental pour maintenir la protection d'actualité.

Lors de la mise à jour de l'application, les objets suivants sont téléchargés et installés sur votre ordinateur :

- Bases de Kaspersky Internet Security.

  La protection des données est garantie par l'utilisation de bases de données qui contiennent les descriptions des signatures des menaces et des attaques de réseau ainsi que les méthodes de lutte contre celles-ci. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces bases sont enrichies régulièrement des définitions des nouvelles menaces et des moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

  En plus des bases de Kaspersky Internet Security, la mise à jour concerne également les pilotes de réseau qui assurent l'interception du trafic de réseau par les composants de la protection.

- Modules logiciels.

  En plus des bases de Kaspersky Internet Security, vous pouvez actualiser les modules logiciels. Ces paquets de mise à jour suppriment des vulnérabilités de Kaspersky Internet Security, ajoutent de nouvelles fonctions ou améliorent les fonctions existantes.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour de Kaspersky Internet Security.

Pour réussir à télécharger les mises à jour depuis les serveurs, il faut que votre ordinateur soit connecté à Internet. Les paramètres de connexion à Internet sont définis automatiquement par défaut. Si les paramètres du serveur proxy ne sont pas définis automatiquement, configurez les paramètres de connexion à ce dernier.

Au cours du processus, les modules logiciels et les bases installés sur votre ordinateur sont comparés à ceux du serveur. Si les bases et les composants installés sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les bases et les modules diffèrent, la partie manquante de la mise à jour sera installée. La copie des bases et des modules complets n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

Si les bases sont fortement dépassées, la taille du paquet de mise à jour peut être considérable, ce qui augmentera le trafic Internet (de quelques dizaines de Mo).

Avant de lancer la mise à jour des bases, Kaspersky Internet Security réalise une copie des bases installées au cas où vous souhaiteriez à nouveau les utiliser pour une raison quelconque.

La possibilité d'annuler une mise à jour est indispensable, par exemple si les bases que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

Parallèlement à la mise à jour de Kaspersky Internet Security, vous pouvez copier les mises à jour obtenues dans une source locale. Ce service permet d'actualiser les bases antivirus et les modules logiciels sur les ordinateurs du réseau en réduisant le trafic Internet.

Vous pouvez également configurer le mode de lancement automatique de la mise à jour.

La section **Mise à jour** de la fenêtre principale de l'application reprend les informations relatives à l'état actuel des bases de Kaspersky Internet Security :

- date et heure de diffusion ;
- Quantité et état des enregistrements dans les bases ;
- État des bases (à jour, dépassées ou corrompues).

Vous pouvez passer au rapport sur les mises à jour qui reprend les informations complètes relatives aux événements survenus lors de l'exécution de la tâche de mises à jour (lien **Rapport** dans la partie supérieure de la fenêtre). Vous pouvez également prendre connaissance de l'activité virale sur le site www.kaspersky.com/fr (lien **Examen de l'activité des virus**).

DANS CETTE SECTION

LANCEMENT DE LA MISE A JOUR

Vous pouvez lancer la mise à jour de Kaspersky Internet Security à n'importe quel moment. Celle-ci sera réalisée au départ de la source de la mise à jour (cf. section "Sélection de la source de mises à jour" à la page 152) que vous aurez choisie.

La mise à jour de Kaspersky Internet Security peut être lancée de deux façons :

- depuis le menu contextuel (cf. section "Menu contextuel" à la page 42) ;
- depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43).

Les informations relatives au processus sont affichées dans la rubrique **Mise à jour** de la fenêtre principale de l'application.

Pour lancer la mise à jour de Kaspersky Internet Security depuis le menu contextuel, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de l'application dans la zone de notification de la barre des tâches.
2. Dans le menu qui s'ouvre, sélectionnez le point **Mise à jour**.

Afin de lancer la mise à jour de la fenêtre principale Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.

3. Cliquez sur **Lancer la Mise à jour**. La progression de la tâche est illustrée dans la fenêtre principale de l'application.

ANNULATION DE LA DERNIERE MISE A JOUR

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Internet Security crée une copie de sauvegarde de la version actuelle des bases et des modules de l'application utilisés avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau les bases antérieures après une mise à jour ratée.

La possibilité de revenir à l'état antérieur de la mise à jour est utile, par exemple, si une partie de la base est corrompue. Les bases locales peuvent être corrompues par l'utilisateur ou par un programme malveillant, ce qui est possible uniquement lorsque l'autodéfense (cf. section "Autodéfense de Kaspersky Internet Security" à la page 169) de Kaspersky Internet Security est désactivée. Vous pouvez ainsi revenir aux bases antérieures et tenter de les actualiser à nouveau ultérieurement.

Pour revenir à l'utilisation de la version précédente des bases, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Cliquez sur le bouton **Restaurer les mises à jours précédentes**.

SELECTION DE LA SOURCE DE MISES A JOUR

La source des mises à jour est une ressource qui contient les mises à jour des bases et des modules de Kaspersky Internet Security. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Les serveurs de mise à jour de Kaspersky Lab constituent la source principale de mises à jour. Il s'agit de sites Internet spéciaux prévus pour la diffusion des bases et des modules logiciels pour tous les produits de Kaspersky Lab.

Si vous ne pouvez accéder aux serveurs de mise à jour de Kaspersky Lab, nous vous invitons à contacter notre service d'assistance technique à l'adresse suivante : http://support.kaspersky.com/fr/

Par défaut, la liste des sources de mises à jour contient uniquement les serveurs de mise à jour de Kaspersky Lab.

Si en guise de source de mises à jour vous avez sélectionné une ressource située hors de l'intranet, vous devrez être connecté à Internet pour télécharger la mise à jour.

Si plusieurs ressources ont été sélectionnées en guise de sources de mise à jour, Kaspersky Internet Security les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible.

Pour sélectionner la source de la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Ajouter**.
5. Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le site FTP ou HTTP ou saisissez son adresse IP, son nom symbolique ou son adresse URL.

UTILISATION DU SERVEUR PROXY

Si vous vous connectez à Internet via un serveur proxy, il faudra le configurer.

Pour configurer les paramètres du serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Serveur proxy**.
5. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, configurez les paramètres du serveur proxy.

PARAMETRES REGIONAUX

Si vous utilisez les serveurs de Kaspersky Lab en guise de serveur de mise à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Les serveurs de Kaspersky Lab sont répartis entre plusieurs pays. En choisissant le serveur situé le plus proche de vous géographiquement, vous pouvez augmenter la vitesse de la mise à jour et du téléchargement de celle-ci.

Pour sélectionner le serveur le plus proche, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre sous l'onglet **Source**, dans le groupe **Paramètres régionaux**, cochez la case **Choisir dans la liste** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

   Si vous choisissez l'option **Déterminer automatiquement**, la mise à jour utilisera les informations sur la région définie dans la base de registre du système d'exploitation.

ACTIONS EXECUTEES APRES LA MISE A JOUR

Kaspersky Internet Security permet également de définir les actions qui seront exécutées automatiquement après la mise à jour. Les actions suivantes peuvent être sélectionnées :

- **Analyser les fichiers en quarantaine**. La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infectés. Il se peut que les bases puissent identifier catégoriquement la menace après la mise à jour et la supprimer. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour. Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et être à nouveau utilisés.

- **Copier la mise à jour des bases dans le dossier**. Si les ordinateurs font partie d'un réseau local, il n'est pas nécessaire de télécharger et d'installer les mises à jour sur chacun des postes séparés car cela entraînerait une augmentation du trafic. Vous pouvez utiliser le mécanisme de copie des mises à jour qui permet de réduire le trafic en procédant une seule fois au téléchargement de la mise à jour.

- *Pour analyser les fichiers en quarantaine après la mise à jour, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
  3. Dans le groupe **Avancé**, cochez la case **Analyser les fichiers en quarantaine après mise à jour**.

MISE A JOUR DEPUIS UN REPERTOIRE LOCAL

La procédure de récupération des mises à jour depuis un répertoire local est organisée de la manière suivante :

1. Un des ordinateurs du réseau récupère les mises à jour pour Kaspersky Internet Security sur les serveurs de Kaspersky Lab ou sur tout autre serveur en ligne proposant les mises à jour les plus récentes. Les mises à jour ainsi obtenues sont placées dans un dossier partagé.
2. Les autres ordinateurs du réseau accèdent à ce dossier partagé afin d'obtenir les mises à jour de Kaspersky Internet Security.

- *Pour activer le mode de copie des mises à jour, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
  3. Dans le groupe **Avancé**, cochez la case **Copier la mise à jour des bases dans le dossier** et dans le champ en dessous, saisissez le chemin d'accès au dossier partagé où seront stockées les mises à jour récupérées. Vous pouvez aussi saisir le chemin dans la fenêtre qui s'ouvre dès que vous aurez cliqué sur **Parcourir**.

- *Afin que la mise à jour soit réalisée depuis le répertoire partagé sélectionné, réalisez les opérations suivantes sur tous les ordinateurs du réseau :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.
  3. Dans le groupe **Source des mises à jour**, cliquez sur le bouton **Configuration**.
  4. Dans la fenêtre qui s'affiche, sous l'onglet **Source** cliquez sur le bouton **Ajouter**.
  5. Dans la fenêtre **Sélection de la source des mises à jour** qui s'ouvre, sélectionnez le répertoire ou saisissez son chemin d'accès complet dans le champ **Source**.
  6. Dans l'onglet **Source** désélectionnez la case **Serveurs de mises à jour de Kaspersky Lab**.

MODIFICATION DU MODE DE LANCEMENT DE LA TACHE DE MISE A JOUR

Le mode de lancement de la tâche de mise à jour de Kaspersky Internet Security est sélectionné lors du fonctionnement de l'Assistant de configuration de Kaspersky Internet Security (cf. section "Etape 3. Configuration de la mise à jour de l'application" à la page 31). Si le mode d'exécution de la mise à jour sélectionné ne vous convient pas, vous pouvez le changer.

L'exécution de la tâche de mise à jour peut se dérouler selon l'un des modes suivants :

- **Automatique**. Kaspersky Internet Security vérifie selon une fréquence déterminée si les fichiers de mise à jour sont présents sur la source. L'intervalle de vérification peut être réduit en cas d'épidémie et agrandi en situation normale. Si le logiciel découvre des nouvelles mises à jour, il les télécharge et les installe sur l'ordinateur.

- **Selon la programmation** (l'intervalle peut changer en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini.

- **Manuel**. Dans ce cas, vous lancez vous-même la procédure de mise à jour de Kaspersky Internet Security.

Pour programmer l'exécution de la tâche d'analyse, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.

3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, onglet **Mode d'exécution**, groupe **Programmation**, sélectionnez le mode d'exécution de la mise à jour. Si vous avez choisi l'option **Selon la programmation**, définissez l'horaire.

   Si pour une raison quelconque le lancement de la mise à jour a été ignoré (par exemple, votre ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique des tâches ignorées dès que cela sera possible. Pour ce faire, cochez la case **Lancer les tâches non exécutées** dans la partie inférieure de la fenêtre. Cette case est accessible pour toutes les options de programmation à l'exception de **Heures**, **Minutes** et **Après le lancement de l'application**.

LANCEMENT DE LA MISE A JOUR AVEC LES PRIVILEGES D'UN AUTRE UTILISATEUR

La mise à jour est lancée par défaut sous le compte que vous avez utilisé pour ouvrir votre session. Il arrive parfois que la mise à jour de Kaspersky Internet Security se déroule depuis une source à laquelle vous n'avez pas accès (par exemple, le répertoire de réseau contenant des mises à jour) ou pour laquelle vous ne jouissez pas des privilèges d'utilisateur autorisé du serveur proxy. Vous pouvez lancer la mise à jour de Kaspersky Internet Security au nom d'un utilisateur qui possède de tels privilèges.

Pour lancer la mise à jour avec les privilèges d'un autre utilisateur, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.

3. Dans le groupe **Mode d'exécution**, cliquez sur le bouton **Configuration**.

4. Dans la fenêtre qui s'ouvre, sous l'onglet **Mode d'exécution**, dans le groupe **Utilisateur**, cochez la case **Lancer la tâche avec les privilèges d'un autre utilisateur**. Saisissez le nom de l'utilisateur et le mot de passe dans les champs en bas.

CONFIGURATION DES PARAMETRES DE L'APPLICATION

La fenêtre de configuration des paramètres de l'application vous permet d'accéder rapidement aux paramètres principaux de Kaspersky Internet Security.

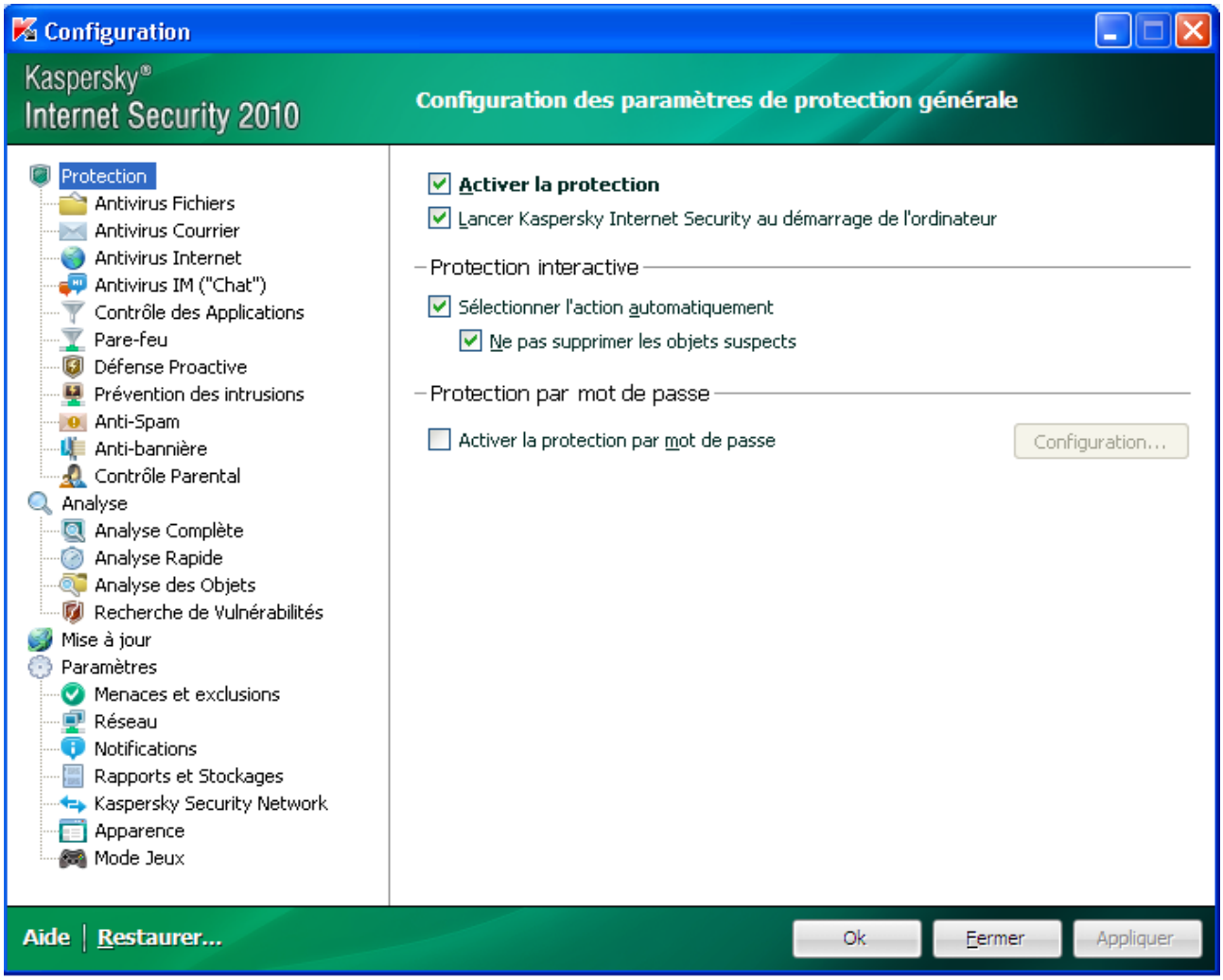


Illustration 11 : Fenêtre de configuration des paramètres de l'application

La fenêtre de configuration contient deux parties :

- la partie gauche permet d'accéder au composant de Kaspersky Internet Security, aux tâches de recherche de virus, à la mise à jour, etc. ;
- la partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionnés dans la partie gauche.

Vous pouvez ouvrir la fenêtre d'une des manières suivantes :

- Depuis la fenêtre principale de l'application (cf. section "Fenêtre principale de Kaspersky Internet Security" à la page 43). Pour ce faire, cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

- Depuis le menu contextuel (cf. section "Menu contextuel" à la page 42). Pour ce faire, sélectionnez l'élément **Configuration** dans le menu contextuel de l'application.

Illustration 12: Menu contextuel

DANS CETTE SECTION

PROTECTION

La fenêtre **Protection** vous permet d'utiliser les fonctions complémentaires suivantes de Kaspersky Internet Security :

- Activation / désactivation de la protection de Kaspersky Internet Security (cf. page 158).
- Lancement de Kaspersky Internet Security au démarrage du système d'exploitation (cf. page 158).
- Utilisation du mode de protection interactif (cf. page 159).
- Restriction de l'accès à Kaspersky Internet Security (cf. page 159).

ACTIVATION / DESACTIVATION DE LA PROTECTION DE L'ORDINATEUR

L'application est lancée par défaut au démarrage du système d'exploitation et protège votre ordinateur pendant la session. Tous les composants de la protection sont activés.

Vous pouvez désactiver la protection en temps réel offerte par Kaspersky Internet Security complètement ou partiellement.

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection** car cela pourrait entraîner l'infection de l'ordinateur et la perte de données.

Cette action entraînera l'arrêt de tous ses composants. Les éléments suivants en témoignent :

- l'icône de Kaspersky Internet Security (cf. section "Icône dans la zone de notification" à la page 41) dans la zone de notification de la barre des tâches est en grise ;
- la couleur rouge de l'indicateur de sécurité.

Notez que dans ce cas, la protection est envisagée dans le contexte des composants du logiciel. La désactivation ou la suspension du fonctionnement des composants du logiciel n'a pas d'influence sur la recherche de virus et la mise à jour du logiciel.

Pour désactiver complètement la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Désélectionnez la case **Activer la protection**.

LANCEMENT DE KASPERSKY INTERNET SECURITY AU DEMARRAGE DU SYSTEME D'EXPLOITATION

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Internet Security, sélectionnez le point **Terminer** dans le menu contextuel (cf. section "Menu contextuel" à la page 42) de Kaspersky Internet Security. Le programme sera déchargé de la mémoire vive de l'ordinateur. Cela signifie que votre ordinateur ne sera plus protégé pendant cette période.

Pour activer à nouveau la protection de l'ordinateur, vous pourrez charger Kaspersky Internet Security depuis le menu **Démarrer** → **Programmes** → **Kaspersky Internet Security 2010** → **Kaspersky Internet Security 2010**.

Il est possible également de lancer la protection automatiquement après le redémarrage du système d'exploitation.

Pour activer ce mode, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Cochez la case **Lancer Kaspersky Internet Security au démarrage de l'ordinateur**.

UTILISATION DU MODE DE PROTECTION INTERACTIF

Kaspersky Internet Security fonctionne selon deux modes :

- *Mode de protection interactif*. Kaspersky Internet Security prévient l'utilisateur de tous les événements dangereux et suspects survenus dans le système. L'utilisateur doit lui-même prendre la décision d'autoriser ou d'interdire une action quelconque.
- *Mode de protection automatique*. Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab lors d'événements dangereux.

Pour utiliser le mode automatique de la protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Protection interactive** cochez la case **Sélectionner l'action automatiquement**. Si vous ne souhaitez pas que Kaspersky Internet Security supprime les objets suspects en mode automatique, cochez la case **Ne pas supprimer les objets suspects**.

RESTRICTION DE L'ACCES A KASPERSKY INTERNET SECURITY

Plusieurs personnes peuvent utiliser un même ordinateur et le niveau de connaissances informatiques de celles-ci varie. L'accès ouvert à Kaspersky Internet Security et à ces paramètres peut considérablement réduire le niveau de la protection globale de l'ordinateur.

Pour renforcer la sécurité de l'ordinateur, imposez un mot de passe pour l'accès à Kaspersky Internet Security. Vous pouvez bloquer n'importe quelle action de Kaspersky Internet Security, à l'exception des notifications en cas de découverte d'objets dangereux ou interdire l'une des actions suivantes :

- modification des paramètres de fonctionnement de l'application ;
- arrêt de l'application ;

Pour protéger l'accès à Kaspersky Internet Security à l'aide d'un mot de passe, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Protection**.
3. Dans le groupe **Protection par mot de passe**, cochez la case **Activer la protection par mot de passe** puis cliquez sur le bouton **Configuration**.
4. Dans la fenêtre **Protection par un mot de passe** qui s'ouvre, saisissez le mot de passe et définissez le domaine d'application des restrictions. Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions que vous avez sélectionné, il devra saisir le mot de passe.

ANTIVIRUS FICHIERS

Cette fenêtre regroupe les paramètres du composant Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page 47). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Fichiers ;
- modifier le niveau de protection (cf. page 49) ;
- modifier l'action à appliquer aux objets identifiés (cf. page 49) ;
- constituer la couverture de protection (cf. page 50) ;
- optimiser l'analyse (cf. page 51) ;
- configurer l'analyse des fichiers composés (cf. page 52) ;
- modifier le mode d'analyse (cf. page 53) ;
- utiliser l'analyse heuristique (cf. page 51) ;
- suspendre le composant (cf. page 54) ;
- sélectionner la technologie d'analyse (cf. page 53) ;
- restaurer les paramètres de protection par défaut (cf. page 56), pour autant qu'ils aient été modifiés.

Pour désactiver l'utilisation de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Fichiers**.

Pour passer à la configuration des paramètres de l'Antivirus Fichiers, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Fichiers** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres de l'Antivirus Fichiers.

ANTIVIRUS COURRIER

Cette fenêtre regroupe les paramètres du composant Antivirus Courrier (cf. section "Protection du courrier" à la page 57). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Courrier ;
- modifier le niveau de protection (cf. page 58) ;
- modifier l'action à appliquer aux objets identifiés (cf. page 59) ;

- constituer la couverture de protection (cf. page 60) ;
- utiliser l'analyse heuristique (cf. page 61) ;
- configurer l'analyse des fichiers composés (cf. page 62) ;
- configurer les règles de filtrage à appliquer aux pièces jointes (cf. page 62) ;
- restaurer les paramètres de protection du courrier par défaut (cf. page 63).

Pour désactiver l'utilisation de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, cochez la case **Activer l'Antivirus Courrier**.

Pour passer à la configuration des paramètres de l'Antivirus Courrier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus Courrier** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres de l'Antivirus Courrier.

ANTIVIRUS INTERNET

Cette fenêtre regroupe les paramètres du composant Antivirus Internet (cf. section "Protection du trafic Internet" à la page 64). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Antivirus Internet ;
- modifier le niveau de protection (cf. page 66) ;
- modifier l'action à appliquer aux objets identifiés (cf. page 66) ;
- constituer la couverture de protection (cf. page 67) ;
- modifier les méthodes d'analyse (cf. page 67) ;
- utiliser le module d'analyse des liens (cf. page 68) ;
- optimiser l'analyse (cf. page 69) ;
- utiliser l'analyse heuristique (cf. page 69) ;
- restaurer les paramètres de protection Internet par défaut (cf. page 70).

Pour désactiver l'utilisation de l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection,** sélectionnez le composant **Antivirus Internet**.

3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus Internet**.

Pour passer à la configuration des paramètres de l'Antivirus Internet, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, dans la section **Protection,** sélectionnez le composant **Antivirus Internet**.

3. Dans la partie droite de la fenêtre, sélectionnez le niveau de protection et la réaction face à la menace pour le composant. Cliquez sur le bouton **Configuration** afin de passer à la configuration des autres paramètres de l'Antivirus Internet.

ANTIVIRUS IM ("CHAT")

Cette fenêtre regroupe les paramètres du composant Antivirus IM ("Chat") (cf. section "Protection du trafic des messageries instantanées" à la page 71). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver l'Antivirus IM ("Chat") ;
- constituer la couverture de protection (cf. page 72) ;
- modifier la méthode d'analyse (cf. page 72) ;
- utiliser l'analyse heuristique (cf. page 73).

Pour désactiver l'utilisation de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.

3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Antivirus IM ("Chat")**.

Pour passer à la configuration des paramètres de l'Antivirus IM, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Antivirus IM ("Chat")** dans la rubrique **Protection**.

3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

CONTROLE DES APPLICATIONS

Cette fenêtre regroupe les paramètres du composant Contrôle des Applications (à la page 74). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- Désactiver le Contrôle des Applications ;
- constituer la couverture de protection (cf. page 77) ;
- administrer la répartition des applications en groupes (cf. page 80) ;
- modifier la durée de définition de l'état de l'application (cf. page 80) ;

- modifier la règle pour l'application (cf. page 81) ;
- modifier la règle pour un groupe d'applications (cf. page 81) ;
- créer une règle de réseau pour l'application (cf. page 82) ;
- définir les exclusions (cf. page 82) ;
- administrer la suppression de règles pour les applications (cf. page 83).

Pour désactiver le contrôle des applications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection,** sélectionnez le composant **Contrôle des Applications**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer le Contrôle des Applications**.

Pour passer à la configuration des paramètres du Contrôle des Applications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection,** sélectionnez le composant **Contrôle des Applications**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

PARE-FEU

Cette fenêtre regroupe les paramètres du composant Pare-feu (à la page 89). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver le Pare-feu ;
- modifier l'état du réseau (cf. page 89) ;
- élargir la plage d'adresses du réseau (cf. page 90) ;
- sélectionner mode de notification sur les modifications du réseau (cf. page 90) ;
- indiquer les paramètres complémentaires de fonctionnement du composant (cf. page 91) ;
- définir les règles de fonctionnement du Pare-feu (cf. page 91) ;
  - créer une règle pour les paquets (cf. page 92) ;
  - créer une règle pour l'application (cf. page 93) ;
  - utiliser l'Assistant de création de règles (cf. page 94) ;
  - sélectionner l'action exécutée par la règle (cf. page 94) ;
  - configurer les paramètres du service de réseau (cf. page 94) ;
  - sélectionner la plage d'adresses (cf. page 95) ;
  - modifier la priorité de la règle.

Pour activer l'utilisation du Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer le Pare-Feu**.

Pour passer à la configuration des paramètres du Pare-feu, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Pare-feu**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration** et dans la fenêtrer qui s'ouvre, modifiez comme il se doit les paramètres du composant.

DEFENSE PROACTIVE

Cette fenêtre regroupe les paramètres du composant Défense Proactive (à la page 97). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver la Défense proactive ;
- gérer la liste de l'activité dangereuse (cf. page 97) ;
- modifier la réaction de l'application sur l'activité dangereuse dans le système (cf. page 98) ;
- constituer un groupe d'applications de confiance (cf. page 99) ;
- contrôler les comptes du système (cf. page 99).

Pour désactiver l'utilisation de la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Défense Proactive**.

Pour passer à la configuration des paramètres de la Défense Proactive, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Défense Proactive**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

PROTECTION CONTRE LES ATTAQUES DE RESEAU

La fenêtre regroupe les paramètres du composant Prévention des intrusions (cf. page 100). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver la Prévention des intrusions ;
- ajouter l'ordinateur à l'origine de l'attaque à la liste de blocage (cf. page 100).

Pour désactiver la Prévention des intrusions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Prévention des intrusions** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer la Prévention des intrusions**.

Pour accéder à la configuration des paramètres de la protection contre les attaques de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez le composant **Prévention des intrusions** dans la rubrique **Protection**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

ANTI-SPAM

Cette fenêtre regroupe les paramètres du composant Anti-Spam (à la page 103). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- arrêter l'Anti-Spam ;
- entraîner l'Anti-Spam (cf. page 106) :
  - à l'aide de l'Assistant d'apprentissage (cf. page 106) ;
  - sur la base du courrier sortant (cf. page 107) ;
  - à l'aide du client de messagerie (cf. page 108) ;
  - à l'aide des rapports (cf. page 109) ;
- modifier le niveau de protection (cf. page 109) ;
- modifier la méthode d'analyse (cf. page 110) ;
- constituer la liste :
  - des adresses de confiance (cf. page 111) ;
  - des expéditeurs interdits (cf. page 111) ;
  - des expressions interdites (cf. page 112) ;
  - des expressions vulgaires (cf. page 112) ;

  - des expéditeurs autorisés (cf. page 113) ;
  - des expressions autorisées (cf. page 114) ;
- importer une liste d'expéditeurs autorisés (cf. page 114) ;
- définir les facteurs de courrier indésirable et de courrier indésirable potentiel (cf. page 115) ;
- sélectionner l'algorithme d'identification du courrier indésirable (cf. page 116) ;
- utiliser les critères complémentaires de filtrage du courrier indésirable (cf. page 116) ;
- ajouter un commentaire à l'objet du message (cf. page 117) ;
- utiliser le Gestionnaire de messages (cf. page 117) ;
- exclure les messages Microsoft Exchange Server de l'analyse (cf. page 118) ;
- configurer le traitement du courrier indésirable :
  - dans Microsoft Office Outlook (cf. page 119) ;
  - dans Microsoft Outlook Express (Windows Mail) (cf. page 120) ;
  - dans The Bat! (cf. page 121) ;
  - dans Thunderbird (cf. page 121) ;
- restaurer les paramètres de protection par défaut contre le courrier indésirable (cf. page 122).

Pour désactiver l'utilisation de l'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Anti-Spam**.

Pour passer à la configuration des paramètres de l'Anti-Spam, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, dans la section **Protection**, sélectionnez le composant **Anti-Spam**.
3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration** et dans la fenêtrer qui s'ouvre, modifiez comme il se doit les paramètres du composant.

ANTI-BANNIERE

Cette fenêtre regroupe les paramètres du composant Anti-bannière (à la page 123). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver l'Anti-bannière ;
- utiliser l'analyse heuristique (cf. page 123) ;
- définir les paramètres avancés de fonctionnement du composant (cf. page 124) ;

- composer la liste des adresses autorisées (cf. page 124) ;
- composer la liste des adresses interdites (cf. page 125) ;
- exporter / importer la liste des bannières (cf. page 125).

Pour désactiver l'Anti-bannière, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre dans la section **Protection,** sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer l'Anti-bannière**.

Pour passer à la configuration des paramètres de l'Anti-bannière, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre dans la section **Protection,** sélectionnez le composant **Anti-bannière**.
3. Dans la partie droite de la fenêtre, modifiez les paramètres du composant comme vous le souhaitez.

CONTROLE PARENTAL

Cette fenêtre regroupe les paramètres du composant Contrôle Parental (à la page 126). La modification des paramètres vous permet d'exécuter les opérations suivantes :

- désactiver le Contrôle Parental ;
- gérer l'utilisation des profils (cf. page 128) ;
- changer le profil actif (cf. page 128) ;
- modifier le niveau de restriction (cf. page 129) ;
- limiter la consultation de sites Internet (cf. page 130) ;
- composer la liste des URL autorisées (cf. page 131) ;
- composer la liste des URL interdites (cf. page 132) ;
- exporter / importer la liste des URL (cf. page 132) ;
- sélectionner les catégories d'URL interdites (cf. page 133) ;
- utiliser l'analyse heuristique (cf. page 134) ;
- sélectionner l'action à exécuter en cas de tentative d'accès à des URL interdites (cf. page 134) ;
- limiter l'accès selon l'heure (cf. page 134).

Pour désactiver l'utilisation du Contrôle Parental, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre dans la section **Protection,** sélectionnez le composant **Contrôle Parental**.

3. Dans la partie droite de la fenêtre, désélectionnez la case **Activer le Contrôle Parental**.

Pour passer à la configuration des paramètres du Contrôle Parental, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre dans la section **Protection,** sélectionnez le composant **Contrôle Parental**.

3. Dans la partie droite de la fenêtre, cliquez sur le bouton **Configuration** et dans la fenêtrer qui s'ouvre, modifiez comme il se doit les paramètres du composant.

ANALYSE

L'ensemble de paramètres définis pour chaque tâche détermine le mode d'exécution de l'analyse des objets sur l'ordinateur.

Les experts de Kaspersky Lab ont élaboré des tâches d'analyse et de recherche de vulnérabilités. Les tâches de recherche d'éventuels virus sont :

- **Analyse des Objets**. Analyse des Objets sélectionnés par l'utilisateur. Vous pouvez analyser n'importe quel objet du système de fichiers de l'ordinateur.

- **Analyse Complète**. Analyse minutieuse de tout le système. Les objets suivants sont analysés par défaut : mémoire système, objets exécutés au démarrage du système, sauvegarde, bases de messagerie, disques durs, disques de réseau et disques amovibles.

- **Analyse Rapide**. Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

La fenêtre de configuration de chaque tâche d'analyse vous permet de réaliser les opérations suivantes :

- sélectionner le niveau de protection pour l'exécution de la tâche ;

- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou probablement infecté ;

- programmer le lancement automatique de la tâche.

- composer la liste des objets à analyser (pour les analyses complète et rapide) ;

- définir les types de fichiers soumis à l'analyse antivirus ;

- définir les paramètres d'analyse des fichiers composés ;

- sélectionner les méthodes et les technologies d'analyse.

Vous pouvez, dans la section **Analyse**, indiquer les paramètres d'analyse automatique des disques amovibles lorsqu'ils sont connectés à l'ordinateur et créer des raccourcis pour le lancement rapide des tâches d'analyse et de recherche de vulnérabilités.

Dans la fenêtre de configuration de la tâche de recherche de vulnérabilités, vous pouvez :

- programmer le lancement automatique de la tâche ;

- composer la liste des objets à analyser.

Pour passer à la configuration des paramètres de la tâche, procédez comme suit :

1. Ouvrez la fenêtre de configuration de l'application.

2. Dans la partie gauche de la fenêtre, sélectionnez dans la rubrique **Analyse** la tâche requise (**Analyse Complète**, **Analyse Rapide**, **Analyse des Objets**, **Recherche de vulnérabilités**).

3. Dans la partie droite de la fenêtre configurez les paramètres.

MISE A JOUR

La mise à jour de Kaspersky Internet Security s'opère conformément à la sélection de paramètres.

La fenêtre de configuration de la mise à jour vous permet de réaliser les opérations suivantes :

- modifier l'adresse de la ressource depuis laquelle les mises à jour de l'application seront copiées et installées ;
- indiquer le mode dans lequel la mise à jour de l'application sera lancée ;
- définir l'horaire de l'exécution de la tâche ;
- désigner le compte utilisateur sous lequel la mise à jour sera lancée ;
- indiquer les actions à exécuter après la mise à jour de l'application.

Pour passer à la configuration des paramètres de la mise à jour, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la partie gauche de la fenêtre sélectionnez la section **Mise à jour**.

3. Dans la partie droite de la fenêtre, indiquez le mode d'exécution requis et sélectionnez la source des mises à jour. Dans le groupe **Avancé**, définissez les autres paramètres de la tâche.

PARAMETRES

La fenêtre **Paramètres** vous permet d'utiliser les fonctions complémentaires suivantes de Kaspersky Internet Security :

- Autodéfense de Kaspersky Internet Security (cf. page 169).
- Utilisation de la technologie de réparation de l'infection active (cf. page 170).
- Service d'économie de la charge de la batterie (cf. page 170).
- Exécution différée des tâches d'analyse en cas de ralentissement du fonctionnement des autres programmes (cf. page 171).
- Exportation / importation des paramètres de fonctionnement de Kaspersky Internet Security (cf. page 171).
- Restauration des paramètres de fonctionnement de Kaspersky Internet Security par défaut (cf. page 172).

AUTODEFENSE DE KASPERSKY INTERNET SECURITY

Kaspersky Internet Security protège les ordinateurs contre les programmes malveillants et pour cette raison, il constitue une cible de choix pour les programmes malveillants qui tentent de le bloquer ou de le supprimer de l'ordinateur.

Pour garantir la stabilité du système de sécurité de votre ordinateur, Kaspersky Internet Security prévoit des mécanismes d'auto-défense et de protection contre les actions externes.

Sous les systèmes d'exploitation 64 bits et sous Microsoft Windows Vista, seule l'administration du mécanisme d'autodéfense de Kaspersky Internet Security contre la modification et la suppression des fichiers sur le disque ou des clés dans la base de registres est accessible.

Il arrive parfois que le recours à la protection contre les interventions à distance entraîne l'impossibilité d'utiliser les programmes d'administration à distance (par exemple, RemoteAdmin). Pour garantir leur fonctionnement, il faut ajouter ces applications à la liste des applications de confiance et activer le paramètre **Ne pas surveiller l'activité de l'application**.

Afin d'activer l'utilisation des mécanismes d'autodéfense de Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Autodéfense**, cochez la case **Activer l'Autodéfense** pour activer le mécanisme de protection de Kaspersky Internet Security contre la modification ou la suppression de ces propres fichiers sur le disque, des processus en mémoire et des enregistrements dans la base de registre système.

   Dans le groupe **Autodéfense**, cochez la case **Désactiver la possibilité d'administration externe du service système** pour bloquer toute tentative d'administration à distance des services de l'application.

   Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la zone de notification de la barre des tâches en cas de tentative d'exécution des actions citées (pour autant que le service n'ait pas été désactivé par l'utilisateur).

TECHNOLOGIE DE REPARATION DES INFECTIONS ACTIVES

Les programmes malveillants actuels peuvent s'introduire au niveau le plus bas du système d'exploitation, ce qui vous prive en pratique de la possibilité de les supprimer. En cas de découverte d'une action malveillante dans le système, Kaspersky Internet Security propose la réalisation d'une procédure élargie de réparation qui permet de neutraliser la menace ou de la supprimer de l'ordinateur.

L'ordinateur redémarrera à la fin de la procédure. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

Pour appliquer la procédure de réparation étendue, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité**, cochez la case **Appliquer la technologie de désinfection avancée**.

UTILISATION DE KASPERSKY INTERNET SECURITY SUR UN ORDINATEUR PORTABLE

Afin d'économiser les batteries des ordinateurs portables, vous pouvez reporter les tâches liées à la recherche de virus.

Etant donné que la recherche de virus et la mise à jour sont assez gourmandes en ressources et durent un certain temps, nous vous conseillons de désactiver le lancement programmé de celles-ci. Cela vous permettra d'économiser la batterie. Au besoin, vous pourrez mettre à jour vous-même Kaspersky Internet Security ou lancer l'analyse antivirus.

Pour utiliser le mode d'économie de la batterie, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité**, cochez la case **Ne pas lancer l'analyse programmée en cas d'alimentation via la batterie**.

PERFORMANCES DE L'ORDINATEUR PENDANT L'EXECUTION DES TACHES

Afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

L'exécution des tâches d'analyse augmente la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, Kaspersky Internet Security arrête par défaut l'exécution des tâches d'analyse et libère des ressources pour les applications de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Pour que l'analyse ne dépende pas du fonctionnement de tels programmes, il ne faut pas leur céder des ressources.

Remarquez que ce paramètre peut être défini individuellement pour chaque tâche d'analyse. Dans ce cas, la configuration des paramètres pour une tâche particulière à une priorité supérieure.

Pour reporter l'exécution des tâches d'analyse en cas de ralentissement d'autres programmes, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Compatibilité** cochez la case **Céder les ressources aux autres applications**.

EXPORTATION / IMPORTATION DES PARAMETRES DE KASPERSKY INTERNET SECURITY

Kaspersky Internet Security vous permet d'exporter et d'importer les paramètres de fonctionnement.

Cela est utile si vous avez installé Kaspersky Internet Security sur un ordinateur chez vous et au bureau. Vous pouvez configurer le logiciel selon un mode qui vous convient pour le travail à domicile, conserver ces paramètres sur le disque et à l'aide de la fonction d'importation, les importer rapidement sur votre ordinateur au travail. Les paramètres sont enregistrés dans un fichier de configuration spécial.

Pour exporter les paramètres actuels de fonctionnement de Kaspersky Internet Security, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.
3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Enregistrer**.
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

Pour importer les paramètres de fonctionnement depuis le fichier de configuration, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.

3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Importer**.

4. Dans la fenêtre qui s'ouvre, sélectionnez le fichier à utiliser pour importer les paramètres de Kaspersky Internet Security.

RESTAURATION DES PARAMETRES PAR DEFAUT

Vous pouvez toujours revenir aux paramètres recommandés de Kaspersky Internet Security. Ces paramètres sont les paramètres optimaux recommandés par les experts de Kaspersky Lab. La restauration des paramètres est exécutée par l'Assistant de configuration initiale (cf. section "Assistant de configuration de l'application" à la page 29) de l'application.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et les composants pour lesquels vous souhaitez les conserver ou non en plus de la restauration du niveau de protection recommandé.

La liste propose les composants de Kaspersky Internet Security dont les paramètres ont été modifiés par l'utilisateur ou assimilés par Kaspersky Internet Security durant l'entraînement des composants Pare-feu et Anti-Spam. Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la liste.

Parmi les paramètres que vous pouvez conserver, il y a les listes "blanche" et "noire" des expressions et des adresses utilisées par l'Anti-Spam, la liste des adresses Internet et des numéros d'accès de confiance, les règles d'exclusion pour les composants du programme, les règles de filtrage des paquets et les règles des applications du Pare-feu.

Ces listes sont constituées pendant l'utilisation de Kaspersky Internet Security et tiennent compte des tâches individuelles et des exigences de sécurité. La constitution de telles listes prend en général beaucoup de temps et pour cette raison, nous vous recommandons de les conserver en cas de rétablissements des paramètres du programme à leur valeur d'origine.

Lorsque vous aurez quitté l'Assistant, tous les composants de la protection fonctionneront selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidés de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

Pour restaurer les paramètres de protection, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Paramètres**.

3. Dans le groupe **Administration des paramètres de l'application**, cliquez sur le bouton **Restaurer**.

4. Dans la fenêtre qui s'ouvre, cochez les cases pour les paramètres qui doivent être enregistrés. Cliquez sur **Suivant**. Cette action entraîne le lancement de l'Assistant de configuration initiale. Suivez les instructions affichées.

MENACES ET EXCLUSIONS

La section **Menaces et exclusions** de la fenêtre de configuration de Kaspersky Internet Security vous permet de réaliser les tâches suivantes

- Sélectionner les catégories de menaces identifiées (cf. section "Sélection des catégories de menaces identifiées" à la page 173) ;

- composer la zone de confiance de l'application.

La Zone de confiance est en réalité une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par l'application. En d'autres termes, il s'agit des éléments exclus de la protection offerte par Kaspersky Internet Security.

La zone de confiance se forme à la base de la liste des applications de confiance (cf. section "Sélection des applications de confiance" à la page 173) et des règles d'exclusion (cf. section "Règles d'exclusion" à la page 174).

L'utilisateur compose la zone de confiance en fonction des particularités des objets qu'il manipule et des programmes installés. La constitution de cette liste d'exclusions peut s'avérer utile si l'application bloque l'accès à un objet ou un programme quelconque alors que vous êtes convaincu que celui-ci est tout à fait sain.

VOIR EGALEMENT

SELECTION DES CATEGORIES DE MENACES IDENTIFIEES

Kaspersky Internet Security vous protège contre divers types de programmes malveillants. Quels que soient les paramètres définis, l'application recherche toujours et neutralise les virus, les chevaux de Troie et les outils de pirates informatiques. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

Pour sélectionner les catégories de menaces à identifier, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**. Cliquez sur le bouton **Configuration** dans le groupe **Menaces**.
3. Dans la fenêtre **Menaces** qui s'ouvre, sélectionnez les catégories de menaces contre lesquelles vous souhaitez protéger votre ordinateur.

SELECTION DES APPLICATIONS DE CONFIANCE

Vous pouvez composer une liste d'applications de confiance dont l'activité au niveau des fichiers et du réseau (y compris toute activité suspecte) ou les requêtes envoyées à la base de registres système ne seront plus contrôlées.

Par exemple, vous estimez que les objets utilisés par le programme Bloc-notes de Microsoft Windows sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance aux processus de ce programme. Afin d'exclure de l'analyse les objets utilisés par ce processus, ajoutez le programme Bloc-notes à la liste des applications de confiance. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux règles d'exclusion.

De plus, certaines actions jugées dangereuses peuvent être tout à fait normales dans le cadre du fonctionnement de toute une série de programmes. Ainsi, l'interception des frappes au clavier est une action standard pour les programmes de permutation automatique de la disposition du clavier (Punto Switcher, etc.). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

Le recours aux exclusions d'applications de confiance de l'analyse permet de résoudre les éventuels problèmes de compatibilité entre Kaspersky Internet Security et d'autres applications (par exemple, le problème de la double analyse du trafic de réseau d'un ordinateur tiers par Kaspersky Internet Security et une autre application antivirus) et d'augmenter les performances de l'ordinateur ce qui est particulièrement important en cas d'utilisation d'applications de réseau.

Par défaut Kaspersky Internet Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère.

Pour ajouter une application à la liste des applications de confiance, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**.
3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Applications de confiance** cliquez sur le lien **Ajouter**.
5. Sélectionnez l'application dans le menu qui s'ouvre. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution.
6. Dans la fenêtre **Exclusions pour l'application** qui s'ouvre, définissez les paramètres des règles pour l'application.

N'oubliez pas que lorsque la case **Exclure l'analyse du trafic de réseau** est cochée, le trafic de l'application indiquée n'est pas analysé uniquement pour les virus et le courrier indésirable. Cela n'exerce aucune influence sur l'analyse du trafic réalisée par le Pare-feu qui analyse l'activité de réseau de cette application selon les paramètres.

Vous pouvez modifier ou supprimer l'application de confiance de la liste à l'aide des liens du même nom situé dans la partie inférieure de l'onglet. Pour exclure l'application de la liste sans toutefois la supprimer, décochez la case en regard de cette dernière.

REGLES D'EXCLUSION

Les applications qui présentent un danger potentiel n'ont aucune fonction malveillante mais elles peuvent être utilisées en tant qu'élément qui va aider un programme malveillant car elles contiennent des failles et des erreurs. Cette catégorie reprend les programmes d'administration à distance, les clients IRC, les serveurs FTP, les utilitaires d'arrêt des processus ou de dissimulation de ceux-ci, les enregistreurs de frappe de clavier, les programmes de décodage des mots de passe, les numéroteurs automatiques vers des numéros payants, etc. Ce genre d'application n'est pas considéré comme un virus (not-a-virus). Il peut s'agir d'un programme de type Adware, Joke, Riskware, etc. (pour obtenir de plus amples informations sur les applications malveillantes découvertes par l'application, consultez l'encyclopédie des virus à l'adresse www.viruslist.com/fr). Ces programmes peuvent être bloqués suite à l'analyse. Dans la mesure où l'utilisation de certains d'entre eux est très populaire, il est prévu de pouvoir les exclure de l'analyse.

Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'une application d'accès à distance qui permet de travailler sur un ordinateur distant. L'activité générée par cette application est considérée comme potentiellement dangereuse par Kaspersky Internet Security et peut être bloquée. Pour exclure le blocage de l'application, il faut créer une règle d'exclusion pour l'application qui la reconnaît comme *not-a-virus:RemoteAdmin.Win32.RAdmin.22* conformément à l'Encyclopédie des virus.

La règle d'exclusion est un ensemble de conditions qui, si elles sont vérifiées, entraîne l'exclusion de l'objet de l'analyse réalisée par Kaspersky Internet Security.

Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un type de menace conforme à la classification de l'encyclopédie des virus.

Le type de menace est l'état attribué à l'objet par Kaspersky Internet Security lors de l'analyse. Le type de menace est rendu sur la base du classement des programmes malveillants et des riskwares présentés dans l'encyclopédie des virus de Kaspersky Lab.

Lorsqu'une règle est ajoutée, une règle est créée. Celle-ci pourra être utilisée par la suite par certains composants de l'application (par exemple, l'Antivirus Fichiers (cf. section "Protection du système de fichiers de l'ordinateur" à la page 47), l'Antivirus Courrier (cf. section "Protection du courrier" à la page 57), l'Antivirus Internet (cf. section "Protection du trafic Internet" à la page 64), ainsi que lors de l'exécution des tâches d'analyse.

Pour créer une règle d'exclusion, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Menaces et exclusions**.
3. Dans la rubrique **Exclusions**, cliquez sur le bouton **Configuration**.
4. Dans la fenêtre qui s'ouvre, sous l'onglet **Règles d'exclusion**, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Règle d'exclusion** qui s'ouvre, définissez les paramètres des règles d'exclusion.

VOIR EGALEMENT

PARAMETRES D'EXCLUSION AVANCES

Pour certains objets selon le type de menace, il est possible de définir dans le champ **Paramètres complémentaires** des conditions supplémentaires pour l'application de la règle. L'indication de paramètres complémentaires peut être requise par exemple pour les verdicts suivants :

- *Invader (insertion dans les processus du programme)*. Pour ce verdict, il est possible d'ajouter en qualité de condition d'exclusion complémentaire pour ce verdict, le nom, le masque ou le chemin d'accès complet à l'objet victime de l'attaque (par exemple, un fichier dll).
- *Launching Internet Browser (lancement du navigateur selon les paramètres)*. Pour cette menace, en guise de condition d'exclusion avancée, vous pouvez indiquer les paramètres de lancement du navigateur. Par exemple, vous souhaitez autoriser le lancement du navigateur pour le domaine de www.kaspersky.com depuis un lien dans Microsoft Office Outlook. Pour ce faire, en guise d'**Objet** de l'exclusion, désignez le programme Microsoft Office Outlook et en guise de **Type de menace**, choisissez Launching Internet Browser puis, dans les **Paramètres avancés**, saisissez le masque du domaine autorisé.

MASQUES AUTORISES POUR L'EXCLUSION DES FICHIERS

Voici des exemples de masques autorisés que vous pouvez utiliser dans la composition de la liste des fichiers à exclure. Parmi ceux-ci, citons les éléments suivants :

1. Masques sans chemins d'accès aux fichiers :
   - ***.exe** : tous les fichiers avec extension *exe* ;
   - **tous les fichiers *.exe** : tous les fichiers avec extension *ex?*, où **?** peut représenter tout caractère singulier ;
   - **test** : tous les fichiers avec le nom *test*.
2. Masques avec chemins d'accès absolus aux fichiers :
   - **C:\dir*.*** ou **C:\dir*** ou **C:\dir** : tous les fichiers du répertoire *C:\dir* ;

- **C:\dir*.exe** : tous les fichiers avec l'extension exe dans le répertoire *C:\dir* ;
- **C:\dir*.ex?** : tous les fichiers portant l'extension *ex?* dans le répertoire *C:\dir*, où **?** peut représenter n'importe quel caractère unique ;
- **C:\dir\test** : uniquement le fichier *C:\dir\test*.

  Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case **Sous-répertoire compris** lors de la définition du masque.

3. Masques de chemins d'accès aux fichiers :
   - **dir*.*** ou **dir*** ou **dir** : tous les fichiers dans tous les répertoires *dir* ;
   - **dir\test** : tous les fichiers *test* dans les répertoires *dir* ;
   - **dir*.exe** : tous les fichiers portant l'extension *exe* dans tous les répertoires *dir* ;
   - **dir*.ex?** : tous les fichiers portant l'extension *ex?* dans tous les répertoires *dir*, où **?** peut représenter tout caractère singulier.

     Afin de ne pas analyser les fichiers dans tous les sous-répertoires du répertoire indiqué, désélectionnez la case **Sous-répertoire compris** lors de la définition du masque.

L'utilisation des masques d'exclusion *.* ou * est admissible uniquement lors de l'indication de la classification des menaces exclues selon l'Encyclopédie des virus. Dans ce cas, la menace indiquée ne sera pas décelée dans tous les objets. L'utilisation de ces masques sans indication de la classification revient à désactiver la protection. Aussi, il n'est pas recommandé de sélectionner, en tant qu'exclusion, le chemin d'accès appartenant au disque virtuel, généré sur la base du catalogue du système de fichiers par l'instruction subst, ou le disque qui est l'image du répertoire de réseau. Il se fait que pour divers utilisateurs d'un ordinateur, le même nom de disque peut désigner différentes ressources, ce qui entraîne inévitablement un dysfonctionnement de la règle d'exclusion.

MASQUES DE TYPES DE MENACES AUTORISES

Pour ajouter des menaces d'un verdict particulier (conforme au classement de l'encyclopédie des virus) en guise d'exclusion, vous pouvez indiquer les paramètres suivants :

- le nom complet de la menace, tel que repris dans l'Encyclopédie des virus sur http://www.viruslist.com/fr (ex. *not-a-virus:RiskWare.RemoteAdmin.RA.311* ou *Flooder.Win32.Fuxx*);
- Le nom de la menace selon un masque, par exemple :
  - **not-a-virus*** : exclut de l'analyse les logiciels licites mais potentiellement dangereux, ainsi que les jokewares ;
  - ***Riskware.*** : exclut de l'analyse tous les types de logiciels présentant un risque potentiel de type Riskware ;
  - ***RemoteAdmin.*** : exclut de l'analyse toutes les versions de logiciel d'administration à distance.

RESEAU

La section **Réseau** de la fenêtre de configuration de l'application vous permet de sélectionner les ports contrôlés par Kaspersky Internet Security et de configurer l'analyse des connexions sécurisées :

- composer la liste des ports contrôlés (cf. page 177) ;
- activer / désactiver le mode d'analyse des connexions sécurisées (via le protocole SSL) (cf. page 178) ;

- configurer les paramètres du serveur proxy (cf. page 180) ;
- donner l'accès à l'Analyse des paquets de réseau (cf. page 180).

VOIR EGALEMENT

CONSTITUTION DE LA LISTE DES PORTS CONTROLES

Les composants de la protection tels que l'Antivirus Courrier (cf. section "Protection du courrier" à la page 57), l'Antivirus Internet (cf. section "Protection du trafic Internet" à la page 64) et l'Anti-Spam (à la page 103) contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains ports ouverts de l'ordinateur. Ainsi, l'Antivirus Courrier analyse les données transmises via le protocole SMTP tandis que l'Antivirus Internet analyse les paquets HTTP.

Vous avez le choix entre deux modes de contrôle des ports :

- **Contrôler tous les ports de réseau** ;
- **Contrôler uniquement les ports sélectionnés**. La liste des ports qui sont normalement utilisés pour le courrier et le trafic http sont repris dans le logiciel.

Pour ajouter un port à la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cliquez sur le lien **Ajouter**.
5. Dans la fenêtre **Port de réseau** qui s'ouvre, saisissez les données requises.

Pour exclure un port de la liste des ports contrôlés, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, décochez la case en regard de la description du port.

Pour former la liste des applications dont l'ensemble des ports devra être analysé, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le bloc **Ports contrôlés**, cliquez sur **Sélection**.
4. Dans la fenêtre **Ports de réseau** qui s'ouvre, cochez la case **Contrôler tous les ports pour les applications indiquées** puis cliquez sur le lien **Ajouter** dans le groupe du dessous.
5. Sélectionnez l'application dans le menu qui s'ouvre. Si vous sélectionnez **Parcourir**, vous ouvrirez une fenêtre dans laquelle vous devrez saisir le chemin d'accès au fichier exécutable. Si vous sélectionnez **Applications**, vous ouvrirez la liste des applications en cours d'exécution.
6. Dans la fenêtre **Application** qui s'ouvre, saisissez une description pour l'application sélectionnée.

ANALYSE DES CONNEXIONS SECURISEES

Les connexions à l'aide du protocole SSL protègent le canal d'échange des données sur Internet. Le protocole SSL permet d'identifier les parties qui échangent les données sur la base de certificats électroniques, de crypter les données transmises et de garantir leur intégrité tout au long de la transmission.

Ces particularités du protocole sont exploitées par les individus mal intentionnés afin de diffuser leurs logiciels malveillants car la majorité des logiciels antivirus n'analyse pas le trafic SSL.

Kaspersky Internet Security analyse les connexions sécurisées à l'aide d'un certificat de Kaspersky Lab. Ce certificat sera toujours utilisé pour l'analyse de la sécurité de la connexion.

Par la suite, l'analyse du trafic SSL aura lieu à l'aide du certificat de Kaspersky Lab. Si un certificat non valide est découvert au moment d'établir la connexion avec le serveur (par exemple, il a été remplacé par un individu mal intentionné), un message s'affichera et invitera l'utilisateur à accepter ou non le certificat ou à consulter les informations relatives à ce dernier. Si l'application fonctionne en mode automatique, la connexion qui utilise le certificat incorrect sera coupée sans notification.

Pour activer l'analyse des connexions sécurisées, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans la fenêtre qui s'ouvre, cochez la case **Analyse des connexions sécurisées** puis cliquez sur le bouton **Installer le certificat**.
4. Dans la fenêtre qui s'affiche, cliquez sur **Installer le certificat**. Cela lancera l'Assistant. Suivez ses instructions pour l'installation du certificat.

L'installation automatique du certificat a lieu uniquement lors de l'utilisation de Microsoft Internet Explorer. Pour l'analyse des connexions sécurisées dans Mozilla Firefox et Opera, installez le certificat de Kaspersky Lab manuellement.

ANALYSE DES CONNEXIONS SECURISEES DANS MOZILLA FIREFOX

Le navigateur Mozilla Firefox n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions sécurisées à l'aide de Firefox, il faut installer manuellement le certificat de Kaspersky Lab.

Pour installer le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Dans le bloc **Certificats**, sélectionnez l'onglet **Sécurité** et cliquez sur **Consultation des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Restaurer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur le bouton **Consulter**.

Pour installer le certificat de Kaspersky Lab pour Mozilla Firefox version 3.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sous l'onglet **Cryptage** cliquez sur **Consultation des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Dans la fenêtre qui s'ouvre, cochez les cases afin de choisir les actions dont l'analyse sera soumise à l'application du certificat installé. Pour consulter les informations relatives au certificat, cliquez sur **Voir**.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera : *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

ANALYSE DES CONNEXIONS SECURISEES DANS OPERA

Le navigateur Opera n'utilise pas le référentiel de certificats de Microsoft Windows. Pour analyser les connexions sécurisées à l'aide d'Opera, il faut installer manuellement le certificat de Kaspersky Lab.

Pour installer le certificat de Kaspersky Lab, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez le point **Outils** → **Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Editeurs** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab :

%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé. Pour consulter les informations relatives au certificat et pour sélectionner les actions qui utiliseront le certificat, sélectionnez le certificat dans la liste et cliquez sur le bouton **Consulter**.

Pour installer le certificat de Kaspersky Lab pour Opera version 9.x, procédez comme suit :

1. Dans le menu du navigateur, sélectionnez le point **Outils** →**Configuration**.
2. Dans la fenêtre qui s'ouvre, cliquez sur l'onglet **Avancé**.
3. Sélectionnez l'onglet **Sécurité** dans la partie gauche de la fenêtre et cliquez sur le bouton **Administration des certificats**.
4. Dans la fenêtre qui s'ouvre, sélectionnez l'onglet **Centres de certifications** puis cliquez sur le bouton **Importer**.
5. Dans la fenêtre qui s'ouvre, sélectionnez le fichier de certificat de Kaspersky Lab. Chemin d'accès au fichier du certificat de Kaspersky Lab : *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Dans la fenêtre qui s'affiche, cliquez sur **Installer**. Le certificat de Kaspersky Lab sera installé.

Si votre ordinateur fonctionne sous le système d'exploitation Microsoft Windows Vista, alors le chemin d'accès au fichier du certificat de Kaspersky Lab sera : *%AllUsersProfile%\Kaspersky Lab\AVP9\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

PARAMETRES DU SERVEUR PROXY

Si la connexion à Internet s'opère via un serveur proxy, il faudra alors peut-être configurer les paramètres de connexion à ce dernier. Kaspersky Internet Security applique ces paramètres dans quelques composants de la protection ainsi que dans la mise à jour des bases et des modules de l'application.

Si votre réseau est doté d'un serveur proxy qui utilise un port inhabituel, il faudra l'ajouter à la liste des ports contrôlés (cf. section "Constitution de la liste des ports contrôlés" à la page 177).

Pour configurer les paramètres du serveur proxy, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le groupe **Serveur proxy**, cliquez sur le bouton **Paramètres du serveur proxy**.
4. Dans la fenêtre **Paramètres du serveur proxy** qui s'ouvre, modifiez les paramètres du serveur proxy.

ACCES A L'ANALYSE DES PAQUETS DE RESEAU.

L'instrument **Analyse des paquets de réseaux** a été développé pour les utilisateurs expérimentés qui possèdent des connaissances sur les principes de création de réseaux et sur les protocoles de réseau.

Kaspersky Internet Security propose l'instrument *Analyse des paquets de réseau*. Il vise à étudier et à analyser l'activité du réseau auquel appartient votre ordinateur.

Par défaut, l'Analyse des paquets de réseau n'est pas accessible dans la fenêtre principale de Kaspersky Internet Security.

Pour ouvrir l'accès à l'Analyse des paquets de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Réseau**.
3. Dans le groupe **Analyse des paquets de réseau** cochez la case **Afficher l'icône de l'Analyse des paquets de réseau**.

NOTIFICATIONS

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Internet Security. Elles peuvent avoir un caractère purement informatif ou présenter des informations cruciales. Par exemple, la notification peut signaler la réussite de la mise à jour ou signaler une erreur dans le fonctionnement d'un composant qu'il faudra rectifier au plus vite.

Pour rester au courant des événements qui surviennent dans le fonctionnement de Kaspersky Internet Security, utilisez le service de notifications.

Par défaut, l'utilisateur est prévenu à l'aide de fenêtres contextuelles et de signaux sonores.

La notification peut être réalisée de l'une des manières suivantes :

- messages contextuels au-dessus de l'icône de l'application dans la barre des tâches ;
- notification sonore ;
- messages électroniques.

Afin de désactiver la remise des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Décochez la case **Notifier les événements**.

Même si l'affichage de la notification est désactivé, les informations relatives aux événements qui surviennent pendant l'utilisation de Kaspersky Internet Security seront consignées dans le Rapports sur l'activité de l'application.

Afin de désactiver le moyen de remise des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Notifications** puis cliquez sur le bouton **Configuration**.
3. Dans la fenêtre **Notification** qui s'ouvre, sélectionnez le mode de notification.

VOIR EGALEMENT

DESACTIVATION DE LA SONORISATION DES NOTIFICATIONS

Par défaut, toutes les notifications sont accompagnées d'un son. Ces sons proviennent de Microsoft Windows. La case **Utiliser les sons standards de Windows par défaut** permet de modifier la sélection de sons utilisée. Si la case est décochée, c'est la sélection de sons de la version antérieure de l'application qui sera utilisée.

Pour désactiver l'accompagnement sonore, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Décochez la case **Activer les sons des notifications**.

ENVOI DES NOTIFICATIONS A L'AIDE DU COURRIER ELECTRONIQUE

Si vous choisissez de recevoir les notifications par courrier électronique, il faudra définir les paramètres de livraison.

Pour configurer les paramètres du courrier électronique pour l'envoi des notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Notifications**.
3. Cochez la case **Activer les notifications par courriers** puis cliquez sur le bouton **Configuration e-mail**.
4. Dans la fenêtre **Configuration des notifications par courrier** qui s'ouvre définissez les paramètres de livraison.

RAPPORTS ET STOCKAGES

La rubrique regroupe les paramètres qui régissent l'utilisation des fichiers de données de Kaspersky Internet Security.

Les fichiers de données de l'application sont les objets placés en quarantaine ou dans la sauvegarde pendant l'utilisation de Kaspersky Internet Security ainsi que les fichiers des rapports sur le fonctionnement des composants de l'application.

Dans cette section, vous pouvez :

- configurer les paramètres de création (cf. page 183) et de conservation des rapports (cf. page 183) ;
- configurer les paramètres de la quarantaine et du dossier de sauvegarde (cf. page 185).

VOIR EGALEMENT

AJOUT D'ENREGISTREMENTS RELATIFS AUX EVENEMENTS DANS LE RAPPORT

Vous pouvez ajouter au rapport de la protection des enregistrements sur les événements non critiques ou sur les événements de la base de registres et du système de fichiers. Ces enregistrements ne sont pas ajoutés par défaut.

- *Pour ajouter au rapport des enregistrements sur les événements non critiques, sur les événements de la base de registres et / ou du système de fichiers, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
  3. Dans le groupe **Rapports**, cochez la case ☑ requise.

PURGE DES RAPPORTS

Les informations relatives au fonctionnement de Kaspersky Internet Security sont consignées dans les rapports. Vous pouvez les purger.

- *Pour purger* les rapports*, procédez comme suit* :

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
  3. Dans le bloc **Rapports** cliquez sur **Purger**.
  4. Dans la fenêtre **Suppression des informations des rapports**, cochez les cases en regard des catégories de rapports que vous souhaitez purger.

CONSERVATION DES RAPPORTS

Vous pouvez définir la durée maximale de conservation des rapports des événements (case ☑ **Supprimer les rapports après**). Par défaut, cette valeur est égale à 30 jours. Une fois ce délai écoulé, les objets sont supprimés. La durée maximale de conservation peut être modifiée, voire complètement annulée. Il est également possible de définir la taille

maximale du fichier du journal (case **Taille maximale de fichier**). Par défaut, la taille maximale est limitée à 1024 Mo. Une fois que la taille maximale est atteinte, le contenu du fichier est remplacé par de nouveaux enregistrements. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

Afin de configurer les paramètres de conservation des rapports, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.

3. Dans la fenêtre qui s'ouvre, dans le groupe **Rapports**, cochez les cases requises et, le cas échéant, modifiez la taille maximale du journal et la durée de conservation.

QUARANTAINE POUR LES OBJETS POTENTIELLEMENT INFECTES

La *quarantaine* est un dossier spécial dans lequel on retrouve les objets qui ont peut être été infectés par des virus.

Les objets potentiellement infectés sont des objets qui ont peut-être été infectés par des virus ou leur modification.

L'objet potentiellement infecté peut-être identifié et mis en quarantaine par l'Antivirus Fichiers, l'Antivirus Courrier, lors de l'analyse antivirus ou par la Défense Proactive.

Les objets sont placés en quarantaine suite aux actions de l'Antivirus Fichiers ou de l'Antivirus Courrier ainsi qu'après l'analyse si :

- *Le code de l'objet analysé est semblable à celui d'une menace connue mais a été partiellement modifié*.

  Les bases de Kaspersky Internet Security contiennent les menaces qui ont été étudiées par les experts de Kaspersky Lab. Si l'application malveillante a été modifiée et que ces modifications ne figurent pas encore dans les bases, Kaspersky Internet Security considère l'objet comme étant infecté par une modification d'une application malveillante et le classe comme objet potentiellement infecté. Il indique obligatoirement à quelle menace cette infection ressemble.

- *Le code de l'objet infecté rappelle, par sa structure, celui d'un programme malveillant mais les bases de l'application ne recensent rien de similaire*.

  Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Internet Security le classe comme un objet potentiellement infecté.

L'analyseur heuristique de code détermine si un fichier est potentiellement infecté par un virus. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

S'agissant de la Défense Proactive, le composant met l'objet en quarantaine si l'analyse de la séquence d'actions qu'il réalise suscite des doutes.

Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

Après la mise à jour des bases de l'application, il se peut que Kaspersky Internet Security puisse identifier la menace et la neutraliser. C'est pour cette raison que le logiciel analyse les objets en quarantaine après chaque mise à jour (cf. page 153).

COPIE DE SAUVEGARDE DES OBJETS DANGEREUX

Il n'est pas toujours possible de préserver l'intégrité des objets lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de tenter de le restaurer au départ de sa copie de sauvegarde.

La copie de sauvegarde est une copie de l'objet dangereux original qui est créée lors de la première réparation ou suppression de l'objet en question et qui est conservée dans le dossier de sauvegarde.

Le dossier de sauvegarde est un dossier spécial qui contient les copies des objets dangereux traités ou supprimés. La principale fonction de la sauvegarde est de garantir la possibilité de restaurer l'objet original à n'importe quel moment. Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger.

MANIPULATION DES OBJETS EN QUARANTAINE

Vous pouvez réaliser les opérations suivantes sur les objets en quarantaine :

- mettre en quarantaine les fichiers qui selon vous sont infectés par un virus ;
- analyser et réparer à l'aide de la version actuelle des bases de Kaspersky Internet Security tous les objets potentiellement infectés qui se trouvent en quarantaine ;
- restaurer les fichiers dans un répertoire choisi par l'utilisateur ou dans le répertoire d'origine où ils se trouvaient avant d'être mis en quarantaine ;
- supprimer n'importe quel objet ou groupe d'objets de la quarantaine ;
- envoyer un objet de la quarantaine à Kaspersky Lab pour étude.

Pour réaliser une action quelconque sur les objets en quarantaine, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Quarantaine**.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Menaces détectées** exécutez les actions requises.

CONSERVATION DES OBJETS DE LA QUARANTAINE ET DE LA SAUVEGARDE.

Vous pouvez configurer les paramètres suivants de fonctionnement de la quarantaine et de la sauvegarde :

- Définir la durée de conservation maximum des objets en quarantaine et des copies des objets dans le dossier de sauvegarde (la case **Supprimer les objets après**). Par défaut, la durée de conservation des objets est 30 jours, après lesquels ils seront supprimés. Vous pouvez modifier la durée de conservation maximum des rapports ou ne pas imposer de limite.
- Indiquer la taille maximale de la quarantaine (case **Taille maximale**). Par défaut, la taille maximale est limitée à 100 Mo. Vous pouvez supprimer les restrictions sur la taille du rapport ou attribuer une autre valeur.

Pour configurer les paramètres de la quarantaine ou de la sauvegarde, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Rapports et Stockages**.
3. Dans le groupe **Quarantaine et sauvegarde**, cochez les cases requises et, le cas échéant, indiquez la taille maximale du dossier où seront conservées les données.

KASPERSKY SECURITY NETWORK

Chaque jour dans le monde, une multitude de nouveaux virus apparaissent. Pour accélérer la collecte de données statistiques sur les types de nouvelles menaces et leurs sources ainsi que dans le but de les neutraliser, Kaspersky Lab vous offre la possibilité d'utiliser les services du *Kaspersky Security Network*.

Le service Kaspersky Security Network suppose l'envoi à Kaspersky Lab de certaines informations. Les informations suivantes sont transmises :

- L'identifiant unique attribué à votre ordinateur par l'application de Kaspersky Lab. Cet identifiant définit les paramètres matériels de votre ordinateur et ne contient aucune donnée personnelle.
- Les informations relatives aux menaces découvertes par les composants du programme. Le contenu de ces informations dépend du type de menace identifiée.
- Les informations relatives au système : version du système d'exploitation, mises à jour installées, services et pilotes téléchargés, version des navigateurs et des clients de messagerie, modules externes des navigateurs, numéro de la version de l'application de Kaspersky Lab installée.

Pour activer l'envoi des statistiques dans Kaspersky Security Network, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Kaspersky Security Network**.
3. Cochez la case **J'accepte de rejoindre le Kaspersky Security Network**.

ASPECT EXTERIEUR DU RAPPORT

Vous pouvez également modifier l'apparence de l'application en créant et en utilisant vos propres éléments graphiques et la palette de couleurs. Il est aussi possible de configurer l'utilisation des éléments actifs de l'interface (icône de l'application dans la zone de notification de la barre des tâches de Microsoft Windows et messages contextuels).

VOIR EGALEMENT

ELEMENTS ACTIFS DE L'INTERFACE

Pour configurer les éléments actifs de l'interface (par exemple, l'icône de Kaspersky Internet Security dans la barre des tâches ou les messages contextuels), vous pouvez exploiter les possibilités suivantes de Kaspersky Internet Security :

Animer l'icône durant l'exécution des tâches.

L'aspect de l'icône change en fonction de l'opération exécutée par l'opération. Ainsi, lors de l'analyse d'un script, un pictogramme avec un script apparaît sur le fond de l'icône tandis qu'un pictogramme représentant un message apparaît pendant l'analyse d'un message. L'icône de Kaspersky Internet Security est animée. Dans ce cas, elle représentera uniquement l'état de la protection de votre ordinateur : si la protection est activée, l'icône sera en couleur. Si la protection est suspendue ou désactivée, l'icône sera grise.

Utiliser la transparence pour les fenêtres de notification.

Toutes les opérations de l'application qui requièrent une notification ou une prise de décision immédiate sont présentées dans un message contextuel qui apparaît au-dessus de l'icône de l'application dans la barre des tâches. Ces infobulles sont transparentes afin de ne pas vous perturber dans votre travail. Le fond de la fenêtre devient solide lorsque le curseur est déplacé sur celle-ci.

M'avertir des informations de Kaspersky Lab.

Par défaut, quand des informations sont obtenues, une icône spéciale apparaît dans la barre d'état. Il suffit de cliquer sur cette icône pour ouvrir une fenêtre contenant le texte des informations.

Afficher "Protected by Kaspersky Lab" sur l'écran de bienvenue de Microsoft Windows.

Par défaut, cet indicateur apparaît dans le coin supérieur droit de l'écran au démarrage de Kaspersky Internet Security. Il indique que votre ordinateur est protégé contre tout type de menace.

Si le programme est installé sur un ordinateur fonctionnant sous Microsoft Windows Vista, cette possibilité ne sera pas offerte.

Pour configurer les éléments actifs de l'interface, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Apparence**.
3. Dans le groupe **Icône de la barre des tâches**, cochez ou décochez les cases correspondantes ☑.

PRESENTATION GRAPHIQUE DE KASPERSKY INTERNET SECURITY

Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de Kaspersky Internet Security peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel et localiser l'interface dans la langue de votre choix.

Pour sélectionner un autre skin, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sélectionnez la rubrique **Apparence**.
3. Dans le groupe **Skins**, cochez la case ☑ **Utiliser un skin personnalisé** pour associer un skin. Dans le champ, saisissez le répertoire contenant les paramètres des thèmes. Cliquez sur **Parcourir** pour sélectionner le répertoire.

UTILISATION DES PROFILS DE KASPERSKY INTERNET SECURITY

L'utilisation de certaines applications (ex : jeux) en mode plein écran peut amener à la nécessité de désactiver quelques fonctions de Kaspersky Internet Security, notamment, du service de notifications. Souvent, de telles applications requièrent aussi des ressources considérables du système, et ce faisant, l'exécution de certaines tâches de Kaspersky Internet Security peut ralentir leur fonctionnement.

Pour désactiver les notifications et suspendre les tâches manuellement chaque fois lors de l'utilisation des applications en mode plein écran, la possibilité de modifier temporairement les paramètres à l'aide du profil de jeux est prévue dans Kaspersky Internet Security. Le Mode Jeux permet de modifier simultanément les paramètres de tous les composants lors du passage en mode plein écran et de remettre à l'état antérieur les modifications apportées après y avoir quitté.

Lors du passage en mode plein écran, les notifications sur les événements sont désactivées automatiquement. Outre cela, vous pouvez spécifier les paramètres suivants :

- ☑ **Sélectionner l'action automatiquement**. Si ce paramètre est sélectionné, alors, en tant que réaction, la sélection automatique de l'action sera appliquée pour tous les composants, même si dans leurs paramètres l'option ◉ **Confirmer l'action** est sélectionnée. Ce faisant, l'utilisateur ne va pas recevoir de propositions sur la sélection de l'action sur les menaces détectées, et l'application choisira l'action automatiquement.
- ☑ **Ne pas exécuter la mise à jour** et ☑ **Ne pas réaliser les analyses programmées**. L'utilisation de ces paramètres est recommandée pour éviter le ralentissement des applications en mode plein écran.

Pour activer l'utilisation du Mode Jeux, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Mode Jeux**.

3. Cochez la case **Activer le Mode Jeux** et saisissez les paramètres nécessaires.

POSSIBILITES COMPLEMENTAIRES

Garantir la protection de l'ordinateur est une tâche complexe qui requiert des connaissances sur les particularités de fonctionnement du système d'exploitation et sur les moyens d'exploiter ses points faibles. De plus, le volume important des informations sur la protection du système et la diversité de celles-ci complique l'analyse et le traitement.

Pour faciliter l'exécution de tâches spécifiques pour la sécurité de l'ordinateur, Kaspersky Internet Security contient plusieurs assistants et outils :

- Le Clavier virtuel (cf. page 189) qui permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.
- Le Contrôle Parental (cf. page 190) qui permet de contrôler l'accès des utilisateurs aux ressources Internet.
- L'Assistant de création de disque de dépannage (cf. page 190) qui rétablit le fonctionnement du système après une attaque de virus si les fichiers système du système d'exploitation ont été endommagés et que celui-ci ne peut être chargé.
- L'Assistant de configuration du navigateur (cf. page 193) qui analyse les paramètres du navigateur Microsoft Internet Explorer et qui les évalue avant tout du point de vue de la sécurité.
- L'Analyse des paquets de réseau (cf. page 194) qui intercepte les paquets de réseau et qui affiche des informations détaillées à leur sujet.
- L'Assistant de restauration après infection (cf. page 196) permet de liquider les traces de la présence d'objets malveillants dans le système.
- L'Assistant de suppression des traces d'activité (cf. page 196) qui permet de retrouver et d'éliminer les traces d'activité de l'utilisateur dans le système.

DANS CETTE SECTION

CLAVIER VIRTUEL

Au cours de l'utilisation de l'ordinateur, il arrive souvent qu'il faille saisir des données personnelles ou un nom d'utilisateur et un mot de passe. C'est le cas lors de l'enregistrement sur certains sites Internet, lors de l'achat dans des boutiques en ligne, etc.

Le risque existe que ces données soient interceptées à l'aide d'outils d'interception ou d'enregistreurs de frappes.

Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

Le clavier virtuel ne peut protéger vos données si le site nécessitant la saisie de ces données a été compromis car dans ce cas, les données tombent directement entre les mains des individus mal intentionnés.

Plusieurs programmes-espions peuvent faire des captures d'écran qui se transmettent automatiquement au malfaiteur pour qu'il analyse et qu'il puisse récupérer les données personnelles de l'utilisateur. Le Clavier virtuel protège les données personnelles saisies contre l'interception par les captures d'écran.

Le clavier virtuel protège contre l'interception des données personnelles uniquement si les navigateurs Microsoft Internet Explorer et Mozilla Firefox fonctionnent.

Pour utiliser le clavier virtuel, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Clavier virtuel**.
3. Saisissez les données requises en appuyant sur les touches du clavier virtuel. Assurez-vous que les données sont saisies dans le champ requis. Si vous appuyez sur les touches de fonction (**Maj**, **Alt** ou **Ctrl**) du clavier virtuel, le mode de saisie spécial est activé (ainsi, si vous appuyez sur la touche **Maj**, tous les caractères seront saisis en majuscules). Pour annuler un mode spécial, appuyez à nouveau sur la touche de fonction.

Le changement de la langue pour le clavier virtuel se passe à l'aide de la combinaison des touches **Ctrl** + le clique sur **Maj** avec le bouton droit de la souris, ou **Ctrl** + le clique sur le **Left Alt** avec le bouton droit de la souris selon les paramètres installés.

CONTROLE PARENTAL

Le *Contrôle Parental* est un composant de l'application qui permet de contrôler l'accès des utilisateurs aux ressources Internet. L'objectif principal du contrôle parental est de limiter l'accès principalement aux ressources suivantes :

- Les sites Internet pour adultes ou les sites web sur la pornographie, les armes, les drogues ou incitant à la cruauté ou à la violence, etc. ;
- Les sites Internet dont le contenu peut provoquer une perte de temps (chats, jeux) ou d'argent (magasins en ligne, sites d'enchères).

Généralement, ces sites abritent une certaine quantité de programmes malveillants et le téléchargement de données depuis ces ressources (sites de jeux par exemple) entraîne une augmentation sensible du trafic Internet.

Le Contrôle Parental (cf. page 126) est désactivé après l'installation de Kaspersky Internet Security.

DISQUE DE DEPANNAGE

Kaspersky Internet Security propose la création d'un disque de démarrage.

Le disque de dépannage est prévu pour le contrôle et la réparation des ordinateurs (compatibles x86) infectés. Il est utilisé lors de tel degré d'infection, quand il n'est pas possible de réparer l'ordinateur par les applications antivirus ou par les utilitaires de réparation (par exemple, Kaspersky AVPTool), lancés sous le système d'exploitation. Avec cela, l'efficacité de réparation est augmentée grâce au fait que les programmes malveillants dans le système ne reçoivent pas d'administration pendant le démarrage du système d'exploitation.

Le disque de dépannage est créé à la base du noyau du système d'exploitation Linux et représente le fichier .iso qui inclut :

- les fichiers de système et de configuration Linux ;
- un ensemble d'utilitaires pour le diagnostic du système d'exploitation ;
- l'ensemble d'utilitaires auxiliaires (le gestionnaire de fichiers, etc.) ;
- les fichiers Kaspersky Rescue Disk ;
- les fichiers contenant les bases antivirus.

Le démarrage de l'ordinateur avec le système d'exploitation endommagé peut être effectué du périphérique CD/DVD-ROM. Pour cela le périphérique correspondant doit être installé sur l'ordinateur.

Afin de créer le disque de dépannage, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre sélectionnez la section **Utilitaires+**.
3. Cliquez sur **Disque de dépannage** afin de lancer l'assistant de création de disque.
4. Suivez les consignes de l'Assistant.
5. A l'aide du fichier obtenu à la fin de l'Assistant, créez un CD/DVD de dépannage. Vous pouvez utiliser pour ce faire un des programmes d'enregistrement de CD/DVD tel que Nero par exemple.

VOIR EGALEMENT

Création d'un disque de dépannage 191

Démarrage de l'ordinateur à l'aide du disque de dépannage 192

CREATION D'UN DISQUE DE DEPANNAGE

La création du disque de dépannage consiste à générer une image du disque (fichier .iso) à partir des bases antivirus actuelles ainsi que des fichiers de configuration.

L'image du disque de départ, en fonction de laquelle le nouveau fichier est généré, peut être téléchargée du serveur de Kaspersky Lab, ou copiée depuis une source locale.

Le fichier de l'image, généré par l'Assistant, est sauvegardé dans le dossier "*Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP9\Data\Rdisk*" ("*ProgramData\Kaspersky Lab\AVP9\Data\Rdisk*" : pour Microsoft Vista) avec le nom *rescuecd.iso*. Si l'Assistant a découvert le fichier de l'image, créé précédemment, dans le dossier, alors, en cochant la case **Utiliser l'image existante**, vous pouvez l'utiliser en guise de l'image du disque de départ, et passez tout d'un coup à l'étape 3 : mise à jour de l'image. Si l'Assistant n'a pas découvert le fichier de l'image, alors cette case n'existe pas.

La création du disque de dépannage s'opère à l'aide d'un assistant spécial qui contient une succession de fenêtres (étape) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Pour terminer le travail de l'assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

VOIR EGALEMENT

Disque de dépannage 190

Démarrage de l'ordinateur à l'aide du disque de dépannage 192

DEMARRAGE DE L'ORDINATEUR A L'AIDE DU DISQUE DE DEPANNAGE

S'il est impossible de charger le système d'exploitation suite à une attaque de virus, utilisez le disque de dépannage.

Pour charger le système d'exploitation, il vous faut absolument un fichier d'image (.iso) de disque de dépannage. Vous pouvez charger le fichier depuis le serveur de Kaspersky Lab ou actualiser le fichier existant.

Examinons en détails le fonctionnement du disque de dépannage. Les opérations suivantes se déroulent durant le chargement du disque :

1. Identification automatique de la configuration matérielle de l'ordinateur.

2. Recherche de systèmes de fichiers sur les disques durs. Les systèmes de fichiers trouvés sont identifiés par un nom commençant par *C*.

   Les noms attribués aux disques durs et aux disques amovibles peuvent ne pas correspondre à la dénomination dans le système d'exploitation.

   Si le système d'exploitation d'ordinateur démarré est en mode de veille, ou son système de fichiers est en mode *unclean*, en conséquence de l'arrêt incorrect du fonctionnement, il vous sera proposé de prendre une décision sur l'assemblage du système de fichiers ou de redémarrer l'ordinateur.

   L'assemblage du système de fichiers peut amener à sa panne.

3. Recherche d'un fichier de téléchargement Microsoft Windows *pagefile.sys*. Si ce fichier n'existe pas, la taille de la mémoire virtuelle est limitée par la taille de la mémoire vive.

4. Choix de la langue de la version. Si durant une certaine période de temps, aucune sélection n'a eu lieu, alors la langue anglaise est prise par défaut.

5. Recherche (création) des dossiers pour le placement des bases antivirus, des rapports, de la quarantaine et des fichiers auxiliaires. Les répertoires de l'application de Kaspersky Lab installée sur l'ordinateur infectés sont utilisés par défaut (*ProgramData/Kaspersky Lab/AVP9* – pour Microsoft Windows Vista, *Documents and Settings/All Users/Application Data/Kaspersky Lab/AVP9* – pour les versions antérieures de Microsoft Windows). Si les répertoires de l'application sont introuvables, une tentative de création sera réalisée. Si les dossiers n'ont pas été découverts et il n'a pas été possible de les créés, le dossier *kl.files* se crée sur un des disques.

6. La tentative de configurer les connexions de réseau en fonction des données, découvertes dans les fichiers de système de l'ordinateur démarré.

7. Chargement du sous-système graphique et lancement de Kaspersky Rescue Disk.

En mode de restauration, seules la recherche de virus et la mise à jour des bases depuis une source locale sont accessibles, aussi que l'annulation des mises à jour et la consultation des statistiques.

➧ *Pour lancer le système d'exploitation d'un ordinateur infecté, procédez comme suit :*

1. Dans les paramètres BIOS, activez le chargement depuis un CD/DVD (pour obtenir de plus amples informations, consultez la documentation de la carte mère de votre ordinateur).

2. Introduisez le disque contenant l'image du disque de dépannage dans le lecteur d'un ordinateur infecté.

3. Redémarrez l'ordinateur.

Le chargement est alors exécuté conformément à l'algorithme décrit ci-dessus. L'aide de Kaspersky Rescue Disk contient de plus amples informations sur les possibilités du disque de dépannage.

VOIR EGALEMENT

CONFIGURATION DU NAVIGATEUR

L'Assistant de configuration du navigateur analyse les paramètres de Microsoft Internet Explorer du point de vue de la sécurité car certaines valeurs attribuées par l'utilisateur ou définies par défaut peuvent engendrer des problèmes de sécurité.

L'Assistant vérifie si les mises à jour les plus récentes du navigateur sont installées et si les paramètres de ce dernier constituent des vulnérabilités qui pourraient être utilisées par des individus mal intentionnés dans le but de nuire à l'ordinateur. Voici des exemples d'objets analysés :

- **Cache de fonctionnement de Microsoft Internet Explorer**. Le cache contient des données confidentielles et permet de voir les sites visités par l'utilisateur. Nombreux sont les objets malveillants qui lors du balayage du disque balaient également le cache, ce qui signifie que les individus mal intentionnés peuvent obtenir les adresses de messagerie des utilisateurs. Il est conseillé de nettoyer le cache après l'utilisation du navigateur.

- **Affichage de l'extension pour les fichiers de format connu**. Il est utile pour l'utilisateur de voir l'extension réelle du fichier. De nombreux objets malveillants utilisent des extensions doubles. Dans ce cas, l'utilisateur voit uniquement une partie du nom du fichier sans l'extension réelle. Cette méthode est largement employée par les individus mal intentionnés. Il est conseillé d'activer l'affichage de l'extension pour les fichiers de format connu.

- **Liste des sites de confiance**. Les objets malveillants peuvent être ajoutés à la liste des liens vers des sites créés par des individus mal intentionnés.

Avant de lancer le diagnostic, fermez toutes les fenêtres de Microsoft Internet Explorer.

Une l'étude terminée, l'Assistant analyse les informations recueillies afin d'identifier les problèmes de sécurité dans les paramètres du navigateur qui doivent être réglés sur le champ. Le résultat de l'étude se présente sous la forme d'une liste d'action qu'il convient d'exécuter pour supprimer le problème. Les actions sont groupées en catégorie selon la gravité des problèmes identifiés.

Pour conclure, l'Assistant rédige un rapport qui peut être envoyé à Kaspersky Lab pour analyse.

Il ne faut pas oublier que certaines valeurs des paramètres peuvent entraîner des problèmes d'affichage de certains sites (par exemple, si ces sites utilisent des éléments ActiveX). Vous pouvez résoudre ce problème en ajoutant ces sites à la zone de confiance.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

➡ *Pour lancer l'Assistant, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Configuration du navigateur**.

ANALYSE DES PAQUETS DE RESEAU

L'instrument **Analyse des paquets de réseau** a été développé pour les utilisateurs expérimentés qui possèdent des connaissances sur les principes de création de réseaux et sur les protocoles de réseau.

Kaspersky Internet Security propose l'instrument *Analyse des paquets de réseau*. Il vise à étudier et à analyser l'activité du réseau auquel appartient votre ordinateur.

Une fois lancée, l'Analyse des paquets de réseau intercepte tous les paquets transmis via le réseau. Le nombre des paquets interceptés peut être très élevé. Pour faciliter l'analyse des informations recueillies, vous pouvez les filtrer selon les adresses de la source et la destination du paquet (cf. page 195) et selon le protocole du transfert (cf. page 195).

Après l'installation de Kaspersky Internet Security, l'analyse des paquets de réseau n'est pas accessible dans la fenêtre principale de l'application. Avant de pouvoir utiliser l'Analyse des paquets de réseau, il est essentiel d'y ouvrir l'accès (cf. page 194).

Pour lancer l'Analyse des paquets de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Analyse des paquets de réseau**.

VOIR EGALEMENT

ACCES A L'ANALYSE DES PAQUETS DE RESEAU.

Par défaut, l'Analyse des paquets de réseau n'est pas accessible dans la fenêtre principale de Kaspersky Internet Security.

Pour ouvrir l'accès à l'Analyse des paquets de réseau, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Configuration** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, choisissez la rubrique **Réseau** et dans le groupe **Analyse des paquets de réseau**, cochez la case **Afficher l'icône de l'analyse des paquets de réseau**.

LANCEMENT/ARRET DE L'INTERCEPTION DES PAQUETS

L'analyse des paquets de réseau fonctionne sur la base des statistiques récoltées sur les paquets interceptés.

Pour lancer l'interception des paquets, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Analyse des paquets de réseau**.
3. Dans la fenêtre **Statistique de l'analyse des paquets de réseau** qui s'ouvre, cliquez sur le bouton **Démarrer**. Il ne faut pas filtrer les données recueillies ou fermer la fenêtre de l'analyse des paquets de réseau avant l'arrêt de l'interception des paquets.

FILTRAGE DES PAQUETS SELON LES ADRESSES DE LA SOURCE ET DE LA DESTINATION

Le volume important de données recueillies par l'Analyse des paquets de réseau complique le traitement et l'analyse. Pour faciliter l'analyse des informations, vous pouvez les filtrer selon les adresses de la source et la destination des paquets.

Pour filtrer les paquets selon les adresses d'origine et de destination, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Analyse des paquets de réseau**.
3. Dans la fenêtre **Statistique de l'analyse des paquets de réseau** qui s'ouvre, cliquez sur le bouton **Démarrer**.
4. Dans les champs **Source** et **Cible**, indiquez les adresses IP requises puis cliquez sur le bouton **Filtrer** dans la partie supérieure de la fenêtre. Les résultats du filtrage apparaîtront dans la partie gauche de la fenêtre.

   Pour annuler le filtrage, effacez le contenu des champs **Source** et **Cible** puis cliquez sur le bouton **Filtrer** dans la partie supérieure de la fenêtre. Les données recueillies par l'analyse de l'activité reviendront à l'état en vigueur au moment de l'arrêt de l'interception des paquets.

FILTRAGE DES PAQUETS SELON LE PROTOCOLE DE TRANSFERT

Le volume important de données recueillies par l'Analyse des paquets de réseau complique le traitement et l'analyse. Pour simplifier l'analyse des informations, celles-ci peuvent être filtrées selon le protocole de transfert des paquets.

Pour filtrer les paquets selon le protocole de transfert, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Analyse des paquets de réseau**.
3. Dans la fenêtre **Statistique de l'analyse des paquets de réseau** qui s'ouvre, cliquez sur le bouton **Démarrer**.
4. Dans la liste déroulante **Protocole**, sélectionnez le protocole requis puis cliquez sur le bouton **Filtrer** dans la partie supérieure de la fenêtre. Les résultats du filtrage figurent dans la partie gauche de la fenêtre.

   Pour annuler le filtrage, effacez le contenu du champ **Protocole** puis cliquez sur le bouton **Filtrer** dans la partie supérieure de la fenêtre. Les données recueillies par l'analyse de l'activité reviendront à l'état en vigueur au moment de l'arrêt de l'interception des paquets.

RESTAURATION APRES INFECTION

L'Assistant de restauration après infection permet de liquider les traces de la présence d'objets malveillants dans le système. Les experts de Kaspersky Lab recommandent de lancer l'Assistant après la réparation de l'ordinateur afin de confirmer que toutes les menaces et les dégâts qu'elles ont causés ont été supprimés. De plus, l'Assistant peut être utilisé si vous pensez que l'ordinateur est infecté.

L'Assistant vérifie si le système a été modifié d'une manière ou d'une autre : blocage de l'accès à l'environnement de réseau, modification des extensions de fichiers de format connu, blocage du panneau d'administration, etc. Ces comportements peuvent être provoqués par divers éléments tels que l'activité de programmes malveillants, par des échecs du système ou par l'utilisation de logiciels d'optimisation du système qui ne fonctionnent pas correctement.

Après l'étude, l'Assistant analyse les informations recueillies afin d'identifier les dégâts dans le système qui requièrent une intervention immédiate. Le résultat de l'étude se présente sous la forme d'une liste d'action qu'il convient d'exécuter pour supprimer la corruption. Les actions sont groupées en catégorie selon la gravité des problèmes identifiés.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Restauration après infection**.

ASSISTANT DE SUPPRESSION DES TRACES D'ACTIVITE

Lorsque vous utilisez votre ordinateur, vos activités sont enregistrées dans le système. Dans ce contexte, les données suivantes sont enregistrées :

- Historique contenant des informations sur :
  - La visite de sites Internet ;
  - L'exécution de l'application ;
  - Les recherches ;
  - L'ouverture/l'enregistrement de fichiers par diverses applications.
- Les enregistrements dans le journal système de Microsoft Windows.
- Les fichiers temporaires, etc.

Toutes ces sources d'informations sur l'activité de l'utilisateur peuvent contenir des données confidentielles (y compris des mots de passe) que les individus mal intentionnés pourraient analyser. Bien souvent, l'utilisateur ne possède pas les connaissances suffisantes pour empêcher ce genre de vol d'informations de valeur.

Kaspersky Internet Security propose un assistant de **Suppression des traces d'activité**. Cet Assistant recherche les traces d'activité de l'utilisateur dans le système ainsi que les paramètres du système d'exploitation qui permettent de récolter des informations sur cette activité.

Le système ne cesse d'accumuler des informations sur l'activité de l'utilisateur. L'exécution du moindre fichier ou l'ouverture de n'importe quel document est enregistrée dans l'historique et le journal de Microsoft Windows enregistre une multitude d'événements qui surviennent dans le système. Ceci veut dire qu'une nouvelle exécution de l'assistant de **Suppression des traces d'activité** peut découvrir des traces supprimées lors de l'exécution antérieure de l'Assistant. Certains fichiers, par exemple le fichier de rapport de Microsoft Windows, peuvent être utilisés par le système au moment où ils sont supprimés par l'Assistant. Afin de pouvoir supprimer les fichiers, l'Assistant propose de redémarrer le système. Toutefois, ces fichiers peuvent être recréés lors du redémarrage, ce qui signifie qu'ils seront à nouveau découverts en tant que trace d'activité.

L'Assistant se présente sous la forme d'une succession de fenêtre (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.

2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Utilitaires+** puis cliquez sur le bouton **Suppression des traces d'activité**.

SURVEILLANCE DU RESEAU

La *Surveillance du réseau* est un outil conçu pour consulter les informations relatives à l'activité de réseau en temps réel. Pour lancer la Surveillance du réseau, cliquez sur l'option du même nom dans le menu contextuel.

La fenêtre qui s'ouvre propose des informations regroupées sous les onglets suivants :

- L'onglet *Connexions et ports* reprend tous les ports ouverts et les connexions de réseau actives établies en ce moment sur votre ordinateur.

- L'onglet *Pare-feu : journal de traitement des règles* reprend les informations relatives à l'application de règles de paquet pour les applications.

- L'onglet *Trafic de réseau* reprend les informations relatives à toutes les connexions entrantes et sortantes établies entre votre ordinateur et d'autres ordinateurs (y compris des serveurs Web, des serveurs de messagerie, etc.).

- L'onglet *Ordinateurs bloqués* reprend la liste des ordinateurs bloqués.

RAPPORTS

Le fonctionnement de chaque composant de Kaspersky Internet Security et l'exécution de chaque tâche de recherche de virus et de mise à jour sont consignés dans le rapport.

Lors de l'utilisation des rapports, vous pouvez réaliser les opérations suivantes :

- sélectionner le composant / la tâche (cf. page 198) au sujet duquel vous souhaitez consulter le rapport ;
- administrer les groupes de données (cf. page 199) et les présenter à l'écran (cf. page 201) ;
- composer l'horaire (cf. page 199) selon lequel Kaspersky Internet Security vous rappellera que le rapport est prêt ;
- sélectionner le type d'événement (cf. page 200) pour lequel il faut générer un rapport ;
- choisir la forme sous laquelle les statistiques seront présentées : tableau ou graphique (cf. page 202) ;
- enregistrer le rapport dans un fichier (cf. page 202) ;
- définir des conditions de filtrage complexes (cf. page 203) ;
- organiser la recherche d'événements (cf. page 203) survenus dans le système et traités par l'application.

DANS CETTE SECTION

SELECTION DU COMPOSANT OU DE LA TACHE POUR LA COMPOSITION DU RAPPORT

Vous pouvez obtenir des informations sur les événements survenus pendant le fonctionnement de chaque composant de l'application ou lors de l'exécution de tâches (par exemple, Antivirus Fichiers, mise à jour, etc.)

Pour obtenir un rapport sur un composant ou une tâche quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la liste déroulante située à gauche dans la fenêtre qui s'ouvre, choisissez le composant ou la tâche pour lequel vous souhaitez générer un rapport. Si vous choisissez l'option **Protection**, le rapport sera produit pour tous les composants de la protection.

ADMINISTRATION DES GROUPES D'INFORMATIONS DANS LE RAPPORT

Vous pouvez administrer le regroupement des données présentées dans le rapport ; dans ce cas, les informations seront regroupées selon divers critères. La sélection des critères varie en fonction des composants et des tâches. Vous avez le choix entre :

- **Sans regroupement**. Tous les événements seront présentés.
- **Regroupement par tâche**. Les données seront regroupées en fonction des tâches exécutées par les composants de Kaspersky Internet Security.
- **Regroupement par application**. Les données seront regroupées en fonction des applications actives dans le système et traitées par Kaspersky Internet Security.
- **Regroupement selon le résultat**. Les données seront regroupées en fonction des résultats de l'analyse ou du traitement de l'objet.

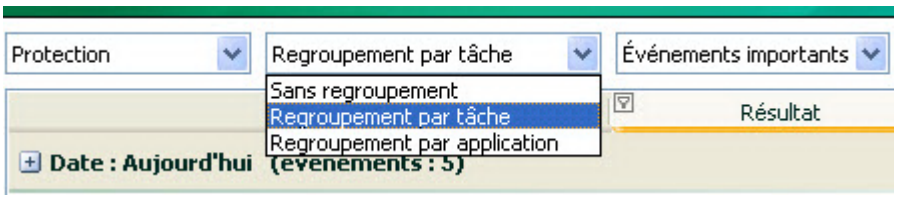


Illustration 13 : Critères de regroupement des informations dans le rapport

Afin d'obtenir rapidement les informations requises et de réduire la taille des groupes, il est possible de lancer une recherche (cf. section "Recherche d'événements" à la page 203) sur la base de mot clé. Vous pouvez définir également des critères de recherche.

Pour réaliser le regroupement selon un critère quelconque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le critère de regroupement dans le menu déroulant.

NOTIFICATION SUR LA DISPONIBILITE DU RAPPORT

Vous pouvez programmer la fréquence selon laquelle Kaspersky Internet Security vous rappellera la disponibilité des rapports.

Pour programmer l'envoi de notifications, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cochez la case **Rappeler le rapport**. Cliquez sur le lien avec l'heure définie.
3. Dans la fenêtre **Rapport: programmation** qui s'ouvre, programmez l'envoi.

SELECTION DU TYPE D'EVENEMENT

La liste complète de l'ensemble des événements survenus durant le fonctionnement du composant de la protection, de l'exécution de l'analyse ou de la mise à jour des bases de l'application figure dans le rapport. Vous pouvez sélectionner les types d'événement qui seront repris dans le rapport.

Les événements peuvent appartenir aux catégories suivantes :

- *Evénements critiques*. Evénements critiques qui indiquent un problème dans le fonctionnement de Kaspersky Internet Security ou une vulnérabilité dans la protection de l'ordinateur. Il s'agit par exemple de la découverte d'un virus ou d'un échec de fonctionnement.
- *Événements importants*. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation dans le fonctionnement du logiciel qui nécessite une intervention, par exemple l'événement **interrompu**.

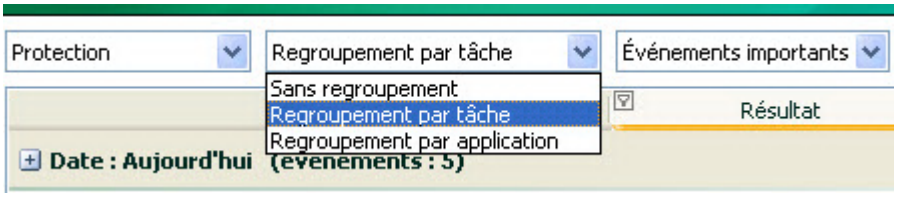


Illustration 14 : Sélection du type d'événement

Lors de la sélection du point **Tous les événements**, tous les événements seront reflétés dans le rapport, mais uniquement si dans la section **Rapports et Stockages**, groupe **Rapports** les cases sont cochées (cf. section "Ajout d'enregistrements relatifs aux événements dans le rapport" à la page 183) qui permettent de donner les informations dans le rapport d'écriture sur les événements non-critiques, de même du système de fichiers et du registre. Si les cases sont décochées, à côté de la liste avec le choix des types d'événements le lien **Désactivé** et un avertissement sont reflétés. Utilisez ce lien pour passer à la fenêtre de configuration des rapports et cochez les cases qu'il faut.

Pour sélectionner le type d'événement pour lequel il faut composer un rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, sélectionnez le type d'événement dans le menu. S'il faut générer un rapport pour l'ensemble des événements, sélectionnez l'option **Tous les événements**.

PRESENTATION DES DONNEES A L'ECRAN

Les événements repris dans le rapport sont présentés sous la forme d'un tableau. Vous pouvez sélectionner les informations en définissant des conditions de restriction. Pour ce faire, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne du tableau pour laquelle vous souhaitez introduire une restriction. La liste déroulante contient les restrictions, par exemple, **Hier** pour la colonne **Heure**, **Courrier électronique** pour la colonne **Objet**, etc. Faites votre choix. Choisissez l'option requise ; la sélection des données s'opèrera sur la base de la restriction définie. Si vous devez consulter l'ensemble des données, sélectionnez l'option **Tous** dans la liste des restrictions.

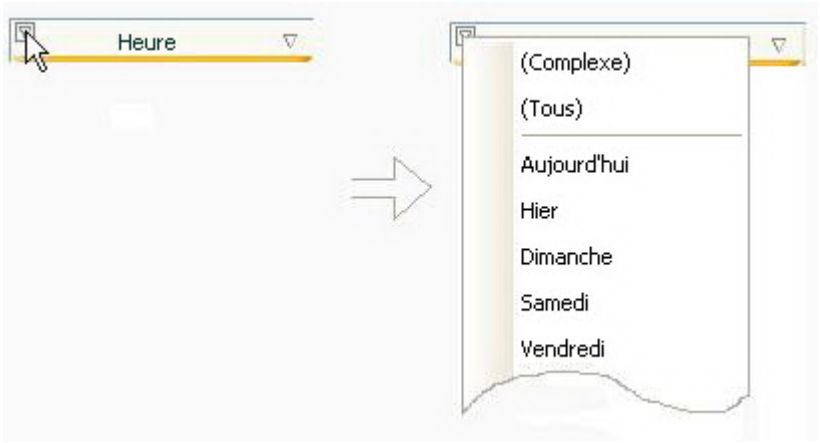


Illustration 15 : Définition d'une restriction

De plus, vous pouvez définir les paramètres de recherche complexe sous la forme d'une plage dans le cadre de laquelle il faudra sélectionner les données sur les événements survenus. Pour ce faire, dans la liste déroulante des restrictions, choisissez l'option **Complexe**. Dans la fenêtre qui s'ouvre définissez l'intervalle requis (cf. section "Utilisation du filtrage complexe" à la page 203).

Pour simplifier l'utilisation de l'onglet, il existe un menu contextuel qui permet d'accéder rapidement à n'importe quelle caractéristique permettant de regrouper et de sélectionner les événements.

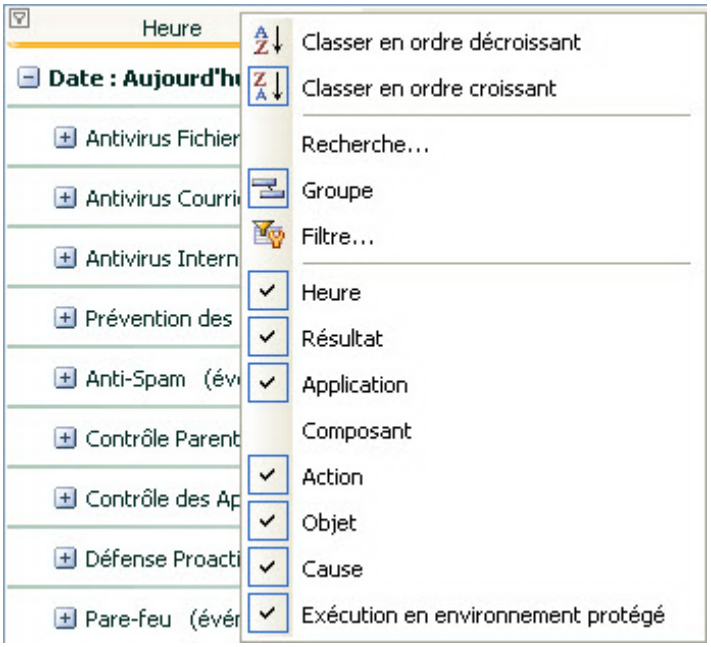


Illustration 16: Menu contextuel

- *Pour définir la condition de restriction, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
  3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne dans laquelle vous souhaitez introduire une restriction. Choisissez la restriction voulue dans la liste déroulante. Lors de la sélection du point **Complexe**, vous pouvez définir les conditions complexes du filtrage (cf. section "Utilisation du filtrage complexe" à la page 203).

- *Pour afficher / dissimuler les colonnes du tableau, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
  3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton droit de la souris à droite du titre de n'importe quelle colonne du tableau. Pour dissimuler certaines colonnes du tableau, décochez la case en regard du nom correspondant dans le menu contextuel.

PRESENTATION DES DONNEES STATISTIQUES DANS UN TABLEAU OU DANS UN GRAPHIQUE

La partie inférieure de la fenêtre des rapports reprend les statistiques de fonctionnement du composant ou de la tâche de Kaspersky Anti-Virus sélectionné. Vous pouvez consulter les statistiques élargies en mode graphique ou sous forme de tableau (selon l'élément ou la tâche). Le passage aux statistiques élargies se passe à l'aide du bouton  en haut de la fenêtre. Les statistiques présentées concernent la journée en cours ou toute la période pendant laquelle l'application a fonctionné sur l'ordinateur.

- *Afin de consulter les statistiques élargies, procédez comme suit :*

  4. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
  5. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
  6. Dans la fenêtre qui s'ouvre, sélectionnez le composant de l'application dont vous souhaitez consulter les statistiques élargies et utilisez le bouton  dans la partie supérieure de la fenêtre.

ENREGISTREMENT DU RAPPORT DANS UN FICHIER

Le rapport obtenu peut être enregistré dans un fichier.

- *Pour enregistrer le rapport dans un fichier, procédez comme suit :*

  1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
  2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
  3. Dans la fenêtre qui s'ouvre, rédigez le rapport requis, puis cliquez sur le bouton **Enregistrer**.
  4. Dans la fenêtre qui s'ouvre, désignez le répertoire dans lequel il faut enregistrer le fichier du rapport et saisissez le nom du fichier.

UTILISATION DU FILTRAGE COMPLEXE

La fenêtre **Filtre complexe** (cf. ill. ci-après) permet de définir les paramètres du filtrage complexe des données. Vous pouvez définir la plage de recherche des données pour n'importe quelle colonne du tableau. Nous allons étudier les principes de fonctionnement à l'aide de la colonne **Heure**.

La sélection des données à l'aide d'un filtre repose sur les opérations logiques de conjonctions (ET logique) et de disjonction (OU logique) qui permettent d'administrer la sélection des données.

Dans les champs situés dans la partie droite de la fenêtre, définissez les limites de la sélection (dans ce cas-ci, il s'agit de l'heure). Pour définir l'heure, vous pouvez utiliser les touches fléchées du clavier. Dans la partie gauche, la liste déroulante **Condition** vous permet de sélectionner la condition de sélection des événements, par exemple, **supérieur**, c.-à-d. supérieur à la limite définie dans le champ à droite.

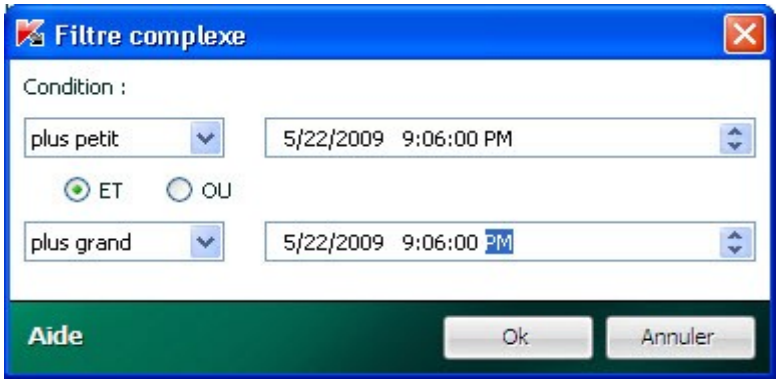


Illustration 17 : Définition des conditions de filtrage complexe

Si vous souhaitez que la sélection des données vérifie les deux conditions définies, sélectionnez **ET**. Si une condition minimum suffit, sélectionnez **OU**.

Pour toute une série de colonnes, les limites de la plage de recherche ne sont ni des chiffres, ni des heures, mais un mot (par exemple, résultat de l'analyse **OK** pour la colonne **Résultat**). Dans ce cas, le mot, défini en tant que limite, est comparé aux autres mots-valeurs pour la colonne sélectionnée par ordre alphabétique.

➧ *Pour définir les conditions complexes du filtrage, procédez comme suit :*

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.

2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.

3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton gauche de la souris à gauche du titre de la colonne pour laquelle vous souhaitez définir les conditions de filtrage complexe. Sélectionnez le point **Complexe** dans le menu déroulant. Vous pouvez également choisir l'option **Filtre** dans le menu contextuel (cf. section "Présentation des données à l'écran" à la page 201) accessible d'un clic avec le bouton droit de la souris sur la colonne souhaitée.

4. Dans la fenêtre **Filtre complexe** définissez les conditions nécessaires du filtrage.

RECHERCHE D'EVENEMENTS

Cette fenêtre (cf. ill. ci-dessous) est prévue pour la recherche des événements survenus dans le système et traités par l'application.

Examinons les principes de fonctionnement :

- Le champ **Ligne** est prévu pour la saisie du mot clé (par exemple, explorer). Pour lancer la recherche, cliquez sur le bouton .**Recherche avancée**. La recherche des données peut prendre un certain temps. A la fin de la

recherche, vous pourrez voir les événements qui correspondent au mot clé utilisé. Si vous cliquez sur le bouton **Marquer tout**, toutes les données qui satisfont le mot clé saisi seront mises en évidence.

- Le champ **Colonne** permet de sélectionner la colonne du tableau dans laquelle la recherche du mot clé aura lieu. Ce choix permet de réduire le temps consacré à la recherche (si, bien évidemment, la valeur **Tous** n'a pas été sélectionnée).

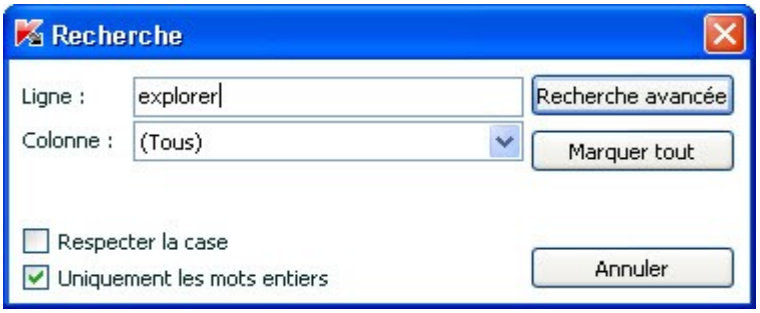


Illustration 18 : Recherche d'événements

Si vous souhaitez que la recherche tiennent compte de la case pour le mot clé, cochez la case **Respecter la case**. La case **Uniquement les mots entiers** permet de limiter les résultats de la recherche et d'afficher uniquement ceux correspondant aux mots entiers définis du mot clé.

Pour utiliser la recherche d'événements, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application et cliquez sur le lien **Rapport** dans la partie supérieure de la fenêtre.
2. Dans la fenêtre qui s'ouvre, sous l'onglet **Rapport** cliquez sur le bouton **Rapport complet**.
3. Dans la fenêtre qui s'ouvre, cliquez avec le bouton droit de la souris à droite du titre de n'importe quelle colonne du tableau. Dans le menu qui s'ouvre, sélectionnez le point **Recherche**.
4. Dans la fenêtre ouverte **Recherche** définissez le critère de recherche.

NOTIFICATIONS

Lorsqu'un événement se produit pendant l'utilisation de Kaspersky Internet Security, vous verrez apparaître un message spécial. En fonction de la gravité de l'événement pour la sécurité de l'ordinateur, les notifications peuvent appartenir aux catégories suivantes :

- **Alertes**. Un événement critique s'est produit, par exemple un objet malveillant ou une activité dangereuse a été découvert dans le système. Il faut immédiatement décider de la suite des événements. La fenêtre de ce genre de notification est rouge.

- **Attention**. Un événement qui présente un risque potentiel s'est produit, par exemple : découverte d'un objet potentiellement infecté ou d'une activité suspecte dans le système. Il est indispensable de décider, selon vous, à quel point cette action est dangereuse. La fenêtre de ce genre de notification est orange.

- **Informations**. Ce message vous signale un événement qui n'est pas critique. La fenêtre de ce genre de notification est verte.

La fenêtre de notification contient quatre parties :

1. *Titre de la fenêtre*. Le titre de la fenêtre fournit une brève description de l'événement, par exemple : demande de privilèges, activité suspecte, nouveau réseau, alerte, virus, etc.

2. *Description de l'événement*. Le groupe de description de l'événement fournit des détails sur la cause de la notification : nom de l'application à l'origine de l'événement, nom de la menace détectée, paramètres de la connexion de réseau détectée, etc.

3. *Zone de sélection de l'action*. Ce groupe vous propose de choisir entre plusieurs actions possibles pour ce type d'événement. Les options proposées dépendent du type d'événement, par exemple : **Réparer**, **Supprimer**, **Ignorer** en cas de découverte d'un virus, **Autoriser**, **Interdire** lorsque l'application demande des privilèges pour exécuter des actions présentant un danger potentiel. L'action recommandée par les experts de Kaspersky Lab est écrite en caractères gras.

   Lors de la sélection de l'action **Autoriser** ou **Interdire**, une fenêtre s'ouvre, où vous pouvez sélectionnez le *mode d'utilisation de l'action*. Pour l'action **Autoriser** vous pouvez sélectionner un des modes suivants :

   - **Autoriser toujours**. Cochez cette case pour résoudre l'activité découverte du programme par les changements dans la règle d'accès du programme vers les ressources du système.

   - **Autoriser maintenant**. Cochez cette case pour appliquer l'action sélectionnée à tous les événements identiques découverts pendant la session de fonctionnement de l'application. La session de fonctionnement d'une application désigne la période entre le moment où elle a été lancée et le moment où elle est arrêtée ou redémarrée.

   - **Rendre fiable**. Cochez cette case pour transmettre l'application dans le groupe **De confiance**.

   Pour l'action **Interdire** vous pouvez sélectionner un des modes suivants :

   - **Interdire toujours**. Cochez cette case pour interdire l'activité découverte du programme par les changements dans la règle d'accès du programme vers les ressources du système.

   - **Interdire maintenant**. Cochez cette case pour appliquer l'action sélectionnée à tous les événements identiques découverts pendant la session de fonctionnement de l'application. La session de fonctionnement d'une application désigne la période entre le moment où elle a été lancée et le moment où elle est arrêtée ou redémarrée.

   - **Quitter**. Cochez cette case pour interrompre le fonctionnement du programme.

4. *Zone de sélection de l'action complémentaire*. Ce groupe permet de sélectionner l'action complémentaire :

   - **Ajouter aux exclusions**. Si vous êtes persuadé que l'objet découvert ne présente aucun danger, vous pouvez l'ajouter à la zone de confiance afin d'éviter un nouveau déclenchement de l'application lors d'une nouvelle manipulation de cet objet.

   - **Appliquer à tous les objets**. Cochez cette case pour que l'action soit appliquée à tous les objets du même état dans des situations analogues.

DANS CETTE SECTION

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou une tâche d'analyse découvre un objet malveillant, un message spécial apparaît.

Il indique :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Réparer** : tentative de réparation de l'objet malveillant. Une copie de sauvegarde est créée avant la suppression au cas où il faudrait restaurer l'objet ou le scénario de l'infection.

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

LA REPARATION DE L'OBJET EST IMPOSSIBLE

Dans certains cas, il est impossible de réparer l'objet malveillant. Par exemple, si l'objet est corrompu à un tel point qu'il est impossible d'en supprimer le code malveillant ou de le restaurer. De plus il existe certains types d'objets malicieux comme les chevaux de Troie qui ne peuvent pas être réparés.

Dans ce cas, un message spécial contenant les informations suivantes s'affiche :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet malveillant tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet malveillant et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Effacer** : supprime l'objet malveillant. Une copie de sauvegarde de l'objet est créée avant la suppression au cas où il faudrait le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action, sauf consigner les informations à son sujet dans le rapport.

  Vous pourrez revenir au traitement des objets malveillants ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche d'analyse antivirus depuis son lancement jusque sa fin.

UNE PROCEDURE SPECIALE DE REPARATION EST REQUISE

Suite à la découverte d'une menace active en ce moment dans le système (par exemple, un processus malveillant dans la mémoire vive ou dans les objets de démarrage), un message vous invitant à lancer la procédure de réparation élargie s'affiche.

Les experts de Kaspersky Lab recommandent vivement d'accepter de lancer cette procédure de réparation. Pour ce faire, cliquez sur le bouton **OK**. Toutefois, n'oubliez pas que l'ordinateur sera redémarré à la fin de la procédure et par conséquent, il est conseillé d'enregistrer tous les travaux en cours et de quitter toutes les applications avant de lancer la procédure.

Lors de la procédure de réparation, il est interdit de lancer les clients de messagerie ou de modifier les bases de registres système du système d'exploitation. Une fois que l'ordinateur a redémarré, il est conseillé de lancer une analyse complète.

UN OBJET DANGEREUX A ETE DECOUVERT DANS LE TRAFIC

Lorsque l'Antivirus Internet découvre un objet dangereux dans le trafic, un message spécial s'affiche.

Celui-ci contient :

- Le type de menace (par exemple : *modification d'un virus*) et le nom de l'objet dangereux tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.

- Le nom complet de l'objet dangereux et le chemin vers la ressource Internet.

Vous aurez le choix entre les actions suivantes :

- **Autoriser** : continue à télécharger l'objet.

- **Interdire** : bloque le téléchargement de l'objet depuis le site Internet.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☑ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

UN OBJET SUSPECT A ETE DETECTE

Lorsque l'Antivirus Fichiers, l'Antivirus Courrier ou la recherche d'éventuels virus découvre un objet qui contient le code d'un virus inconnu ou le code modifié d'un virus connu, un message spécial s'affiche.

Il indique :

- Le type de menace (par exemple : *virus*, *cheval de Troie*) et le nom de l'objet tel que repris dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet malveillant se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte dans le système.

- Le nom complet de l'objet et son chemin d'accès.

Vous aurez le choix entre les actions suivantes :

- **Quarantaine** : place l'objet en quarantaine. Dans ce cas, l'objet est déplacé et non pas copié : l'objet est supprimé du disque ou du message et il est enregistré dans le répertoire de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

  Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

  > En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

- **Supprimer** : supprime l'objet. Avant la suppression une copie de sauvegarde de l'objet est créée au cas où il faudra par la suite le restaurer ou reproduire le scénario de l'infection.

- **Ignorer** : bloque l'accès à l'objet mais n'exécute aucune action sur ce dernier. L'application se contente de consigner les informations relatives à l'objet dans le rapport.

  Vous pourrez revenir au traitement des objets ignorés au départ de la fenêtre du rapport (le traitement différé d'un objet n'est pas possible lorsque l'objet découvert est joint à un message électronique).

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'objet découvert n'est pas malveillant, il est conseillé de l'ajouter à la zone de confiance pour éviter tout nouveau déclenchement de l'activation lors d'une prochaine manipulation de cet objet.

UNE ACTIVITE DANGEREUSE A ETE DECOUVERTE DANS LE SYSTEME

Lorsque la Protection proactive découvre une activité dangereuse en provenance d'une application quelconque du système, un message spécial apparaît avec les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du fichier du processus à l'origine de l'activité dangereuse et son chemin d'accès.
- Sélection des actions possibles :
  - **Quarantaine** : arrêter le processus et mettre son fichier exécutable en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

    Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

    > En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se passe uniquement si l'analyse a été réalisée (dans les trois jours maximum) après la mise en quarantaine du fichier.

  - **Terminer** : terminer le processus.
  - **Autoriser** : autoriser l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Internet Security.

UN PROCESSUS CACHE A ETE DECOUVERT

Lorsque la Protection proactive découvre un processus caché dans le système, un message spécial s'affiche et fournit les informations suivantes :

- Nom de la menace, tel qu'il figure dans l'Encyclopédie des virus de Kaspersky Lab. Le nom de l'objet se présente sous la forme d'un lien qui vous renvoie sur www.viruslist.com/fr où vous pourrez obtenir des informations complémentaires sur le type de menace découverte.
- Le nom complet du processus caché et son chemin d'accès.
- Sélection des actions possibles :
  - **Quarantaine** : place le fichier exécutable du processus en quarantaine. Un objet qui est mis en quarantaine est déplacé et non pas copié. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

    Lors des analyses ultérieures de la quarantaine à l'aide de signatures des menaces actualisées, il est possible que l'état de l'objet change. Par exemple, l'objet peut être identifié comme étant infecté et traité à l'aide de bases actualisées ou il peut recevoir l'état *sain* et dans ce cas, il pourra être restauré.

    > En cas de mise en quarantaine manuelle d'un fichier qui lors de l'analyse suivante ne sera pas considéré comme infecté, son statut après l'analyse ne deviendra pas automatiquement *OK*. Cela se produira uniquement si l'analyse a eu lieu un certain temps (au moins trois jours) après la mise du fichier en quarantaine.

  - **Terminer** : terminer le processus.
  - **Autoriser** : autoriser l'exécution du processus.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

Si vous êtes convaincu que l'application découverte ne représente aucun danger, il est conseillé de l'ajouter à la zone de confiance pour éviter un nouveau déclenchement de Kaspersky Internet Security.

UNE TENTATIVE D'ACCES A LA BASE DE REGISTRE SYSTEME A ETE DECOUVERTE

Lorsque la Défense Proactive découvre une tentative d'accès aux clés de la base de registre système, un message spécial s'affiche et fournit les informations suivantes :

- La clé du registre exposée à la tentative d'accès.
- Le nom complet du fichier du processus à l'origine de la tentative d'accès à la clé du registre et son chemin d'accès.
- Sélection des actions possibles :
  - **Autoriser** : autorise une fois l'exécution de l'action dangereuse ;
  - **Interdire** : interdit une fois l'exécution de l'action dangereuse.

Pour que l'action que vous avez sélectionnée soit exécutée automatiquement chaque fois qu'une telle activité sera lancée sur l'ordinateur, cochez la case **Créer une règle**.

Si vous estimez qu'aucune des actions lancées par l'application qui a tenté d'accéder à la base de registres système n'est dangereuse, vous pouvez ajouter l'application à la liste des applications de confiance.

UNE ACTIVITE DE RESEAU DE L'APPLICATION A ETE DECOUVERTE

Lors de la détection de l'activité de réseau de l'application (par défaut, pour les applications faisant parti du groupe (cf. section "Groupes d'applications" à la page 76) **Restrictions faibles** ou **Restrictions fortes**), un message s'affichera.

Le message s'affichera si Kaspersky Internet Security fonctionne dans le mode interactif (cf. section "Utilisation du mode de protection interactif" à la page 159), et pour l'application dont l'activité de réseau a été détectée, une règle pour un paquet (cf. page 92) n'a pas été créée.

Celui-ci contient :

- *Une description de l'activité* : nom de l'application et brèves caractéristiques de la connexion qu'elle tente d'établir. Sont également indiqués : le type de connexion, le port local à partir de laquelle elle est établie, le port distant et l'adresse de la connexion.
- *Séquence de lancement de l'application*.
- *Action* : la séquence d'opération que doit exécuter Kaspersky Internet Security par rapport à l'activité de réseau découverte.

Vous aurez le choix entre les actions suivantes :

- **Autoriser**.
- **Interdire**.
- **Créer une règle**. Le choix de cette sélection entraîne l'ouverture de *l'Assistant de rédaction de règles* (cf. page 94) qui vous aidera à créer la règle pour régir l'activité de réseau de l'application.

Vous pouvez :

- Exécuter l'action une fois. Pour ce faire, sélectionnez **Autoriser** ou **Interdire**.
- Enregistrer l'action pour la session de l'application qui montre l'activité de réseau. Pour ce faire, sélectionnez **Autoriser** ou **Interdire** et cochez la case **Enregistrer pour la session de l'application**.
- Enregistrer pour toujours l'action sélectionnée pour l'application. Pour ce faire, sélectionnez **Autoriser** ou **Interdire** et cochez la case **Enregistrer pour toujours**.
- Créer une règle pour régir l'activité de réseau de l'application. Pour ce faire, sélectionnez **Créer une règle**.

UN NOUVEAU RESEAU A ETE DECOUVERT

Chaque fois que l'ordinateur se connecte à une nouvelle zone (réseau), un message spécial s'affiche.

La partie supérieure de ce message reprend une brève description du réseau avec l'adresse IP et le masque de sous-réseau.

La partie inférieure de la fenêtre vous propose d'attribuer un état à la nouvelle zone. Cet état permettra d'autoriser ou non telle ou telle activité de réseau :

- **Réseau public (interdire l'accès à l'ordinateur de l'extérieur)**. Ce réseau présente un très grand risque car une fois qu'il y est connecté, l'ordinateur est exposé à toutes les menaces possibles et imaginables. Cet état doit être sélectionné pour les réseaux qui ne sont protégés par aucun logiciel antivirus, pare-feu, filtre, etc. Ce choix offre la protection maximale de l'ordinateur dans cet environnement.

- **Réseau local (autoriser l'accès aux fichiers et aux imprimantes)**. Cet état est recommandé pour les zones présentant un risque moyen (par exemple, le réseau interne d'une entreprise).

- **Réseau de confiance (autoriser n'importe quelle activité de réseau)**. Cet état doit être réservé aux zones qui, d'après vous, ne présentent aucun danger car l'ordinateur ne risque pas d'être attaqué ou victime d'un accès non autorisé.

UNE TENTATIVE DE PHISHING A ETE DECOUVERTE

Lorsque Kaspersky Internet Security découvre une tentative d'ouverture d'un site de phishing, un message spécial s'affiche.

Celui-ci contient :

- Le nom de la menace, *attaque de phishing*, sous la forme de lien qui vous renvoie à la description détaillée de la menace dans l'Encyclopédie des virus de Kaspersky Lab.

- L'URL du site de phishing.

- Sélection des actions possibles :

  - **Autoriser** : continue à télécharger le site de phishing.

  - **Interdire** : bloque le téléchargement du site de phishing.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☑ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

UN LIEN SUSPECT A ETE DECOUVERT

Lorsque Kaspersky Internet Security découvre une tentative d'ouverture d'un site Web dont l'adresse figure dans la liste des URL suspectes, il affiche un message spécial.

Celui-ci contient :

- URL du site

- Sélection des actions possibles :

  - **Autoriser** : poursuit le chargement du site Web.

  - **Interdire** : bloque le chargement du site Web.

Pour appliquer l'action sélectionnée à tous les objets portant le même état découvert dans la séance actuelle du composant de la protection ou de la tâche, cochez la case ☑ **Appliquer à tous les cas identiques**. Par session en cours, il faut entendre la durée de fonctionnement du composant depuis son lancement jusqu'à son arrêt ou jusqu'au redémarrage de l'application ainsi que la durée de l'exécution de la tâche de recherche de virus depuis son lancement jusque sa fin.

DECOUVERTE D'UN CERTIFICAT INCORRECT

L'analyse de la sécurité de connexion par le protocole SSL aura lieu à l'aide du certificat installé. En cas de tentative de connexion avec le serveur avec un certificat incorrect (par exemple, dans le cas de substitution par les malfaiteurs), un message spécial s'affiche.

L'information sur les causes possibles d'erreur, ainsi que le port et l'adresse à distance s'affichent dans la notification. Vous serez invité à décider de la nécessité d'établir la connexion en cas d'utilisation d'un certificat non valide.

- **Accepter le certificat** : poursuivre la connexion à une ressource en ligne ;
- **Rejeter le certificat** : rompre la connexion à une ressource en ligne ;
- **Consulter le certificat** : profiter de la possibilité de consulter l'information sur le certificat.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE KASPERSKY INTERNET SECURITY

Une fois que Kaspersky Internet Security a été installé et configuré, vous pouvez vérifier si la configuration est correcte à l'aide d'un virus d'essai et de ses modifications. La vérification doit être réalisée séparément pour chaque composant de la protection/protocole.

DANS CETTE SECTION

VIRUS D'ESSAI EICAR ET SES MODIFICATIONS

Ce "virus" d'essai a été développé spécialement par l'organisation eicar (The European Institute for Computer Antivirus Research) afin de tester les logiciels antivirus.

Le virus d'essai N'EST PAS UN VIRUS et il ne contient pas de code qui pourrait nuire à votre ordinateur. Toutefois, la majorité des logiciels antivirus le considère comme un virus.

N'utilisez jamais d'authentiques virus pour vérifier le fonctionnement de votre antivirus !

Vous pouvez télécharger le "virus" d'essai depuis le site officiel de l'organisation **EICAR** : http://www.eicar.org/anti_virus_test_file.htm.

Avant de lancer le téléchargement, il faut absolument désactiver la protection antivirus car le fichier *anti_virus_test_file.htm* sera identifié et traité par l'application comme un objet infecté transmis par le protocole HTTP. N'oubliez pas de réactiver la protection antivirus dès que le téléchargement du virus d'essai sera terminé.

L'application identifie le fichier téléchargé depuis le site de la société **EICAR** comme un objet infecté par un virus **qui ne peut être neutralisé et** exécute l'action définie pour ce genre d'objet.

Vous pouvez également utiliser une modification du virus d'essai standard afin de vérifier le bon fonctionnement de l'application. Pour ce faire, il faut modifier le contenu du virus standard en ajoutant un des préfixes présentés dans le tableau ci-après. Pour créer une modification du virus d'essai, vous pouvez utiliser n'importe quel éditeur de fichier texte ou éditeur hypertexte tel que le **Bloc-Notes de Microsoft** ou **UltraEdit32**, etc.

Vous pouvez vérifier le bon fonctionnement de votre logiciel antivirus à l'aide d'une modification du virus EICAR uniquement si vous possédez des bases antivirus dont la date de publication est postérieure au 24 octobre 2003 (mise à jour cumulée, octobre 2003).

La première colonne du tableau contient les préfixes qu'il faut ajouter en tête de la ligne du virus d'essai traditionnel. La deuxième colonne reprend toute les valeurs possibles de l'état attribué par l'antivirus à la fin de l'analyse. La troisième colonne contient les informations relatives au traitement que réservera l'application aux objets de l'état indiqué. N'oubliez pas que les actions à réaliser sur les objets sont définies par les paramètres de l'application.

Après avoir ajouté le préfixe au virus d'essai, enregistrez le fichier, par exemple sous le nom : *eicar_dele.com*. Nommez tous les virus modifiés selon le même principe.

Tableau 1. Modifications du virus d'essai

Préfixe	Etat de l'objet	Informations relatives au traitement de l'objet
Pas de préfixe, "virus" d'essai standard.	**Infecté**. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée.
CORR–	**Corrompu**.	L'application a pu accéder à l'objet mais n'a pas pu l'analyser car l'objet est corrompu (par exemple, sa structure est endommagée ou le format du fichier est invalide) Les informations relatives au traitement de l'objet figure dans le rapport sur le fonctionnement de l'application.
WARN–	**Suspect**. L'objet contient le code d'un virus inconnu. Réparation impossible.	L'analyseur heuristique attribue l'état suspect à l'objet. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
SUSP–	**Suspect**. L'objet contient le code modifié d'un virus connu. Réparation impossible.	L'application a découvert une équivalence partielle entre un extrait du code de l'objet et un extrait du code d'un virus connu. Au moment de la découverte, les bases de l'antivirus ne contenaient pas la description de la réparation de cet objet. Vous serez averti de la découverte d'un tel objet.
ERRO–	**Erreur d'analyse**.	Une erreur s'est produite lors de l'analyse de l'objet. L'application ne peut accéder à l'objet car l'intégrité de celui-ci a été violée (par exemple : il n'y a pas de fin à une archive multivolume) ou il n'y a pas de lien vers l'objet (lorsque l'objet se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figure dans le rapport sur le fonctionnement de l'application.
CURE–	**Infecté**. L'objet contient le code d'un virus connu. Réparable.	L'objet contient un virus qui peut être réparé. L'application répare l'objet et le texte du corps du « virus » est remplacé par CURE Vous serez averti de la découverte d'un tel objet.
DELE–	**Infecté**. L'objet contient le code d'un virus connu. Réparation impossible.	L'application identifie l'objet en tant que virus qui ne peut être réparé. Une erreur se produit en cas de tentative de réparation de l'objet ; l'action définie pour les objets qui ne peuvent être réparés est appliquée. Vous serez averti de la découverte d'un tel objet.

TEST DE LA PROTECTION DU TRAFIC HTTP

Pour vérifier l'identification de virus dans le flux de données transmises par le protocole HTTP :

essayez de télécharger le "virus" d'essai depuis le site officiel de l'organisation **EICAR** : http://www.eicar.org/anti_virus_test_file.htm.

Lors d'une tentative de téléchargement du virus d'essai, Kaspersky Internet Security découvre l'objet, l'identifie comme étant infecté et ne pouvant être réparé puis exécute l'action définie dans les paramètres d'analyse du trafic HTTP pour ce type d'objet. Par défaut, la connexion avec le site est coupée à la moindre tentative de téléchargement du virus d'essai et un message indiquera dans le navigateur que l'objet en question est infecté par le virus EICAR-Test-File.

TEST DE LA PROTECTION DU TRAFIC SMTP

Pour vérifier l'identification des virus dans le flux de données transmises via le protocole SMTP, vous pouvez utiliser le système de messagerie qui exploite ce protocole pour le transfert des données.

Il est conseillé de vérifier le fonctionnement d'Antivirus pour le courrier sortant aussi bien sur le corps des messages que les pièces jointes. Pour vérifier la découverte de virus dans le corps des messages, placer le texte du virus d'essai standard ou d'une de ses modifications dans le corps du message.

Pour ce faire, exécutez les actions suivantes :

1. Composez le message au format **Texte normal** à l'aide du client de messagerie installé sur l'ordinateur.

   Les messages contenant le virus d'essai dans le corps et rédigés au format RTF et HTML ne seront pas analysés !

2. Placez le texte du virus d'essai standard ou modifié au début du message ou joignez un fichier contenant le test d'essai.

3. Envoyez ce message à l'adresse de l'administrateur.

L'application découvre l'objet, l'identifie en tant qu'objet infecté et bloque l'envoie du message.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE L'ANTIVIRUS FICHIERS

Pour vérifier l'exactitude de la configuration de l'Antivirus Fichiers, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essairécupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.

2. Autorisez la consignation de tous les événements afin que le rapport reprenne les données sur les objets corrompus ou les objets qui n'ont pas été analysés suite à un échec.

3. Exécutez le fichier du virus d'essai ou une de ses modifications.

L'Antivirus Fichiers intercepte la requête adressée au fichier, la vérifie et exécute l'action définie dans les paramètres. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Les informations complètes sur les résultats du fonctionnement de l'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE ANTIVIRUS

Pour vérifier l'exactitude de la configuration de la tâche d'analyse, procédez comme suit :

1. Créez un répertoire sur le disque, copiez-y le virus d'essai récupéré sur le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm) ainsi que les modifications de ce virus que vous avez créées.

2. Créez une nouvelle tâche d'analyse antivirus et en guise d'objet à analyser sélectionnez le dossier, contenant la sélection de virus d'essai.

3. Autorisez la consignation de tous les événements dans le rapport afin de conserver les données relatives aux objets corrompus ou aux objets qui n'ont pas été analysés suite à l'échec.

4. Lancez la tâche d'analyse antivirus.

Lors de l'analyse, les actions définies dans les paramètres de la tâche seront exécutées au fur et à mesure que des objets suspects ou infectés sont découverts. En sélectionnant diverses actions à réaliser sur les objets infectés, vous pouvez vérifier le fonctionnement du composant dans son ensemble.

Toutes les informations relatives aux résultats de l'exécution de la tâche d'analyse sont consultables dans le rapport de fonctionnement du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA PROTECTION CONTRE LE COURRIER INDESIRABLE

Pour vérifier la protection contre le courrier indésirable, vous pouvez utiliser un message d'essai qui sera considéra comme indésirable par l'application.

Le message d'essai doit contenir dans le corps la ligne suivante :

```
Spam is bad do not send it
```

Une fois que ce message est arrivé sur l'ordinateur, Kaspersky Internet Security l'analyse, lui attribue l'état de courrier indésirable et exécute l'action définie pour les objets de ce type.

UTILISATION DE L'APPLICATION AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Internet Security à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- lancement et arrêt des composants de l'application ;
- lancement et arrêt de l'exécution des tâches d'analyse antivirus ;
- obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques;
- analyse des objets sélectionnés ;
- mise à jour des signatures des menaces et des modules de l'application ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;
- appel de l'aide relative à la syntaxe de la ligne de commande ;

Syntaxe de la ligne de commande :

```
avp.com <instruction> [paramètres]
```

La requête adressée à l'application via la ligne de commande doit être réalisée depuis le répertoire d'installation du logiciel ou en indiquant le chemin d'accès complet à avp.com.

Les instructions suivantes sont prévues :

START	lancement du composant ou de la tâche
STOP	arrêt du composant ou de la tâche (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)
STATUS	affichage de l'état actuel du composant ou de la tâche
STATISTICS	affichage des statistiques du composant ou de la tâche
HELP	aide sur la syntaxe de la commande ou la liste des commandes.
SCAN	analyse antivirus des objets
UPDATE	lance la mise à jour de l'application
ROLLBACK	annulation de la dernière mise à jour réalisée (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de Kaspersky Internet Security)
EXIT	quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mode passe défini via l'interface de l'application)
IMPORT	importation des paramètres de protection de Kaspersky Internet Security (l'exécution de la commande est possible uniquement après saisie du mot de passe défini via l'interface de l'application)

EXPORT	exporte les paramètres de la protection de l'application

Chaque instruction possède ses propres paramètres, propres à chaque composant de l'application.

DANS CETTE SECTION

ADMINISTRATION DES COMPOSANTS DE L'APPLICATION ET DES TACHES

Syntaxe de la commande :

```
avp.com <instruction> <profil|nom_de_la_tâche> [/R[A]:<fichier_de_rapport>]
avp.com STOP|PAUSE <profil|nom_de_la_tâche> /password=<votre_mot_de_passe>
[/R[A]:<fichier_de_rapport>]
```

<commande>	L'administration des composants et des tâches de Kaspersky Internet Security via la ligne de commande s'opère à l'aide des instructions suivantes : START : lancement du composant de la protection ou de la tâche. STOP : arrêt du composant de la protection ou de la tâche. STATUS : affichage de l'état actuel du composant de la protection ou de la tâche. STATISTICS : affichage des statistiques du composant de la protection ou de la tâche. N'oubliez pas que la commande STOP ne peut être exécutée sans la saisie préalable du mot de passe.

<profil|nom_de_la_tâche>	En guise de valeur pour le paramètre **<profil>**, vous pouvez indiquer n'importe quel composant de la protection en temps réel de Kaspersky Internet Security ainsi que les modules qui sont repris dans les composants des tâches d'analyse à la demande ou de mise à jour composées (les valeurs standard utilisées par l'application sont reprises dans le tableau ci-après). En guise de valeur pour le paramètre **<nom_de_la_tâche>**, vous pouvez indiquer le nom de n'importe quelle tâche d'analyse à la demande ou de mise à jour configurée par l'utilisateur.
<votre_mot_de_passe>	mot de passe d'accès à l'application, défini dans l'interface.
/R[A]:<fichier_de_rapport>	**/R:<fichier_de_rapport>** : consigner dans le rapport uniquement les événements importants. **/RA:<fichier_de_rapport>** : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.

En guise de valeur pour le paramètre **<profil>**, attribuez une des valeurs suivantes :

RTP	tous les composants de la protection. L'instruction **avp.com START RTP** lance tous les composants de la protection, si la protection avait été arrêtée. Si le composant a été arrêté via la commande **STOP** de la ligne de commande, il ne pourra être redémarré via la commande **avp.com START RTP**. Pour ce faire, il faut exécuter la commande **avp.com START <profil>** où le paramètre **<profil>** représente un composant concret de la protection, par exemple **avp.com START FM**.
FW	Pare-Feu
HIPS	Contrôle des Applications
pdm	Défense Proactive
FM	Antivirus Fichiers
EM	Antivirus Courrier
WM	Antivirus Internet Valeurs pour les sous-composants d'Antivirus Internet : **httpscan (HTTP)** : analyse du trafic HTTP ; **sc** : analyse des scripts.
IM	Antivirus IM ("Chat")
AB	Anti-bannière
AS	Anti-Spam
PC	Contrôle Parental

AP	Anti-phishing
ids	Protection contre les attaques de réseau
Updater	Mise à jour
Rollback	Annulation de la dernière mise à jour
Scan_My_Computer	Analyse de l'ordinateur
Scan_Objects	Analyse des Objets
Scan_Quarantine	Analyse de la quarantaine
Scan_Rootkits	Recherche de la présence éventuelle d'outils de dissimulation d'activité
Scan_Startup (STARTUP)	Analyse des objets de démarrage
Scan_Vulnerabilities (SECURITY)	Recherche de vulnérabilités

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples :

- *Pour activer l'Antivirus Fichiers, saisissez dans la ligne de commande :*

```
avp.com START FM
```

- *Pour rétablir le fonctionnement du contrôle parental, saisissez dans la ligne de commande :*

```
avp.com RESUME ParCtl
```

- *Pour arrêter la tâche d'analyse du poste de travail, saisissez dans la ligne de commande :*

```
avp.com STOP Scan_My_Computer /password=<votre_mot_de_passe>
```

RECHERCHE DE VIRUS

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>] [<types de fichiers>] [<exclusions>]
[<fichier de configuration>] [<paramètres du rapport>] [< paramètres complémentaires
>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans l'application en lançant la tâche requise via la ligne de commande. Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface de Kaspersky Internet Security.

Description des paramètres :

<objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
<files>	Liste des chemins d'accès aux fichiers et / ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste

	doivent être séparés par un espace. Remarques : • mettre le nom de l'objet entre guillemets s'il contient un espace ; • lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	Objets de la mémoire vive.
/STARTUP	Objets de démarrage.
/MAIL	Boîtes aux lettres.
/REMDRIVES	Tous les disques amovibles.
/FIXDRIVES	Tous les disques locaux.
/NETDRIVES	Tous les disques de réseau.
/QUARANTINE	Objets en quarantaine.
/ALL	Analyse du Poste de travail.
/@:<filelist.lst>	Chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi sans guillemets, même s'il contient un espace.
<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i8.** Si vous travaillez en mode automatique, alors Kaspersky Internet Security appliquera automatiquement l'action recommandée par les experts de Kaspersky Lab en cas de découverte d'objets dangereux. L'action définie par la valeur du paramètre <**action**>, sera ignoré.	
/i0	Aucune action n'est exécutée, les informations sont seulement consignées dans le rapport.
/i1	Réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	Réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx).
/i3	Réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	Supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i8	Confirmer l'action auprès de l'utilisateur en cas de découverte d'un objet infecté.
/i9	Confirmer l'action auprès de l'utilisateur à la fin de l'analyse.

Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.
/fa	Analyser tous les fichiers.
Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
-e:a	Ne pas analyser les archives.
-e:b	Ne pas analyser les bases de messagerie.
-e:m	Ne pas analyser les messages électroniques au format plain text.
-e:<filemask>	Ne pas analyser les objets en fonction d'un masque.
-e:<secondes>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre **<seconds>**.
-es:<taille>	Ignorer les objets dont la taille (en Mo) est supérieure à la valeur définie par le paramètre **<size>**.
Le paramètre **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour l'analyse antivirus. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de l'application qui seront utilisées.	
/C:<nom_du_fichier>	Utiliser les valeurs des paramètres définies dans le fichier **<nom_du_fichier>**.
Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.	
/R:<fichier_de_rapport>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<fichier_de_rapport>	Consigner tous les événements dans le rapport.
<paramètres complémentaires> : paramètres qui définissent l'utilisation de technologies de recherche de virus.	
/iChecker=<on|off>	Activer/désactiver l'utilisation de la technologie iChecker.
/iSwift=<on|off>	Activer / désactiver l'utilisation de la technologie iChecker.

Exemples :

- *Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des boîtes aux lettres et des répertoires My Documents, Program Files et du fichier test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents"
"C:\Program Files" "C:\Downloads\test.exe"
```

- *Suspendre l'analyse des objets sélectionnés, lancer une nouvelle analyse de l'ordinateur à la fin de laquelle il faudra poursuivre la recherche d'éventuels virus dans les objets sélectionnés :*

```
avp.com PAUSE Scan_Objects /password=<votre_mot_de_passe>
avp.com START Scan_My_Computer
avp.com RESUME Scan_Objects
```

- *Analyser les objets dont la liste est reprise dans le fichier object2scan.txt. Utiliser le fichier de configuration scan_setting.txt. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements :*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Exemple de fichier de configuration :

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

MISE A JOUR DE L'APPLICATION

L'instruction pour la mise à jour des modules de Kaspersky Internet Security et des bases de l'application possède la syntaxe suivante :

```
avp.com UPDATE [<source_de_la_mise_à_jour>] [/R[A]:<fichier_de_rapport>]
[/C:<nom_du_fichier>] [/APP=<on|off>]
```

Description des paramètres :

<source_de_la_mise_à_jour>	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Ce paramètre accepte en tant que valeur le chemin d'accès complet à la source des mises à jour ou une URL. Si le chemin d'accès n'est pas indiqué, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.
/R[A]:<fichier_de_rapport>	**/R:**<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants. **/RA:**<fichier_de_rapport> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.
/C:<nom_du_fichier>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de Kaspersky Internet Security pour la mise à jour. Le fichier de configuration est un fichier au format texte qui contient l'ensemble des paramètres de la ligne de commande pour la mise à jour de l'application. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs des paramètres définies dans l'interface de l'application qui seront utilisées.
/APP=<on|off>	Active / désactive la mise à jour des modules de l'application.

Exemples :

- *Actualiser les bases de l'application et consigner tous les éléments dans le rapport :*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Mettre à jour les modules de Kaspersky Internet Security en utilisant les paramètres du fichier de configuration updateapp.ini:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Exemple de fichier de configuration :

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt /app=on
```

ANNULATION DE LA DERNIERE MISE A JOUR

Syntaxe de la commande :

```
ROLLBACK [/R[A]:<fichier_de_rapport>][/password=<votre_mot_de_passe>]
```

Description des paramètres :

/R[A]:<fichier_de_rapport>	**/R:**<fichier_de_rapport> : consigner dans le rapport uniquement les événements importants. **/RA:**<fichier_de_rapport> : consigner tous les événements dans le rapport. Les chemins relatifs et absolus au fichier sont admis. Si le paramètre n'est pas indiqué, les résultats de l'analyse sont affichés à l'écran et portent sur tous les événements.
<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com ROLLBACK /RA:rollback.txt/password=<votre mot de passe>
```

EXPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com EXPORT <profil> <nom_du_fichier>
```

Description des paramètres :

<profil>	Composant ou tâche dont les paramètres sont exportés. Le paramètre **<profil>** peut prendre n'importe quelle des valeurs indiquées au point "Administration des composants de l'application et des taches".
<nom_du_fichier>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu. Le fichier de configuration est enregistré au format binaire (*dat*) si aucun autre format n'est indiqué ou si le format n'est pas précisé et il peut être ensuite utilisé pour transférer les paramètres de l'application vers d'autres ordinateurs. De plus, vous pouvez enregistrer le fichier de configuration au format texte. Dans ce cas, ajoutez l'extension *txt*. N'oubliez pas que l'importation de paramètres depuis un fichier texte n'est pas prise en charge. Ce fichier sert uniquement à consulter les paramètres de fonctionnement principaux de l'application.

Exemple :

```
avp.com EXPORT c:\settings.dat
```

IMPORTATION DES PARAMETRES DE PROTECTION

Syntaxe de la commande :

```
avp.com IMPORT <nom_du_fichier > [/password=< votre_mot_de_passe >
```

<nom_du_fichier>	Chemin d'accès au fichier d'où sont importés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu.
<votre_mot_de_passe>	Mot de passe pour Kaspersky Internet Security défini via l'interface de l'application. L'importation des paramètres de la protection est possible uniquement depuis un fichier au format binaire.

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

Exemple :

```
avp.com IMPORT c:\settings.dat /password=<mot de passe>
```

LANCEMENT DE L'APPLICATION

Syntaxe de la commande :

```
avp.com
```

ARRET DE L'APPLICATION

Syntaxe de la commande :

```
EXIT /password=<votre_mot_de_passe>
```

<votre_mot_de_passe>	Mot de passe d'accès à l'application, défini dans l'interface

N'oubliez pas que cette instruction ne s'exécutera pas sans la saisie du mot de passe.

OBTENTION DU FICHIER DE TRACE

La création du fichier de trace s'impose parfois lorsque des problèmes se présentent dans le fonctionnement de l'application. Il permettra aux spécialistes du service d'assistance technique de poser un diagnostic plus précis.

Syntaxe de la commande :

```
avp.com TRACE [file] [on|off] [<niveau_de_trace>]
```

Description des paramètres :

[on|off]	Active / désactive la création d'un fichier de trace
[file]	Recevoir la trace dans un fichier
<niveau_de_trace>	Pour ce paramètre, il est possible de saisir un chiffre compris entre 0 (niveau minimum, uniquement les événements critiques) et 700 (niveau maximum, tous les messages).

	Lorsque vous contactez le service d'assistance technique, l'expert doit vous préciser le niveau qu'il souhaite. S'il n'a rien recommandé en particulier, il est conseillé de choisir le niveau 500.

Il est conseillé d'activer la création de ces fichiers uniquement pour le diagnostic d'un problème particulier. L'activation permanente de cette fonction peut entraîner une réduction des performances de l'ordinateur et la saturation du disque dur.

Exemples :

- *Désactiver la constitution de fichiers de trace :*

```
avp.com TRACE file off
```

- *Créer un fichier de trace avec le niveau maximum de détails défini à 500 en vue d'un envoi à l'assistance technique :*

```
avp.com TRACE file on 500
```

CONSULTATION DE L'AIDE

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
avp.com [ /? | HELP ]
```

Pour obtenir de l'aide sur la syntaxe d'une commande particulière, vous pouvez utiliser une des commandes suivantes :

```
avp.com <commande> /?
avp.com HELP <commande>
```

CODES DE RETOUR DE LA LIGNE DE COMMANDE

Cette rubrique décrit les codes de retour de la ligne de commande. Les codes généraux peuvent être renvoyés par n'importe quelle commande. Les codes de retour des tâches concernent les codes généraux et les codes spécifiques à un type de tâche en particulier.

CODES DE RETOUR GENERAUX	
0	Opération réussie
1	Valeur de paramètre invalide
2	Erreur inconnue
3	Erreur d'exécution de la tâche
4	Annulation de l'exécution de la tâche
CODES DE RETOUR DES TACHES D'ANALYSE ANTIVIRUS	
101	Tous les objets dangereux ont été traités
102	Des objets dangereux ont été découverts

SUPPRESSION DES PROBLEMES

Au cas où des problèmes se présenteraient durant l'utilisation de Kaspersky Internet Security, vérifiez si la solution n'est pas décrite dans l'aide ou dans la Banque des solutions de Kaspersky Lab (http://support.kaspersky.com/fr). La *banque des solutions* est une rubrique distincte du site du service d'assistance technique qui contient les recommandations sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées. Tentez de trouver la réponse à votre question ou la solution à votre problème dans cette ressource.

Pour consulter la banque de solutions, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique** cliquez sur le lien **Banque de solutions**.

Il existe une autre ressource où vous pouvez obtenir des informations sur l'utilisation des applications : le forum des utilisateurs des applications de Kaspersky Lab. Cette source est également une rubrique distincte du service d'assistance technique. Elle contient les questions, les commentaires et les suggestions des utilisateurs de l'application. Vous pouvez voir les principaux sujets de discussion, envoyer des commentaires sur l'application ou rechercher les réponses à votre question.

Pour ouvrir le forum des utilisateurs, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Accès direct aux FAQs**.

Si vous ne trouvez pas la solution à votre problème dans l'aide, la banque de solutions ou l'accès direct aux FAQ, nous vous conseillons de contacter le service d'assistance technique de Kaspersky Lab.

DANS CETTE SECTION

CREATION D'UN RAPPORT SUR L'ETAT DU SYSTEME

Afin de résoudre vos problèmes, il se peut que les experts du service d'assistance technique de Kaspersky Lab aient besoin d'un rapport sur l'état du système. Ce rapport contient des informations détaillées sur les processus exécutés, les modules et les pilotes chargés, les modules externes de Microsoft Internet Explorer et de l'Assistant Microsoft Windows, les ports ouverts, les objets suspects décelés, etc.

Aucune donnée personnelle relative à l'utilisateur n'est recueillie durant la création du rapport.

Pour créer un rapport sur l'état du système, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** cliquez sur le bouton **Créer le rapport sur l'état du système**.

Le rapport sur l'état du système est généré aux formats *htm* et *xml* et est enregistré dans l'archive *sysinfo.zip*. Une fois que la collecte des informations sur le système est terminée, vous pouvez consulter le rapport.

Pour parcourir le rapport, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** cliquez sur le bouton **Voir**.
5. Ouvrez l'archive *sysinfo.zip* contenant les fichiers du rapport.

CREATION D'UN FICHIER DE TRACE

Le système d'exploitation ou certaines applications peuvent rencontrer des problèmes après l'installation de Kaspersky Internet Security. Dans ce cas, il s'agit généralement d'un conflit entre Kaspersky Internet Security et des applications installées ou des pilotes sur l'ordinateur. Afin de résoudre ce problème, les experts du service d'assistance technique de Kaspersky Lab pourraient vous demander de créer un fichier de traçage.

Pour créer un fichier de trace, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre, utilisez la liste déroulante du bloc **Traçages** afin de sélectionner le niveau de traçage. Le niveau de traçage est indiqué par l'expert du service d'assistance technique. En cas d'absence de recommandations du service d'assistance technique, il est conseillé de choisir le niveau **500**.
5. Afin de lancer le traçage, cliquez sur le bouton **Activer**.
6. Reproduisez la situation qui entraîne le problème.
7. Pour arrêter le traçage, cliquez sur le bouton **Désactiver**.

Vous pouvez passer au transfert des résultats du traçage (cf. section "Envoi des fichiers de données" à la page 230) sur le serveur de Kaspersky Lab.

ENVOI DES FICHIERS DE DONNEES

Une fois que les fichiers de traçage et le rapport sur l'état du système ont été créés, il faut les envoyer aux experts du service d'assistance technique de Kaspersky Lab.

Pour charger les fichiers de données sur le serveur du service d'assistance technique, il faut obtenir un numéro de requête. Ce numéro est accessible dans votre Espace personnel sur le site du service d'assistance technique lorsque des requêtes actives sont présentes.

Pour télécharger les fichiers de données sur le serveur du service d'Assistance technique, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique**, dans le groupe **Actions** cliquez sur le bouton **Envoyer les informations pour le service d'assistance technique**.
5. Dans la fenêtre qui s'ouvre, cochez les cases en regard des fichiers que vous souhaitez envoyer au service d'assistance technique puis cliquez sur **Envoyer**.
6. Dans la fenêtre ouverte **Saisir le numéro de requête (numéro SRF)** indiquez le numéro attribué à votre requête au moment de remplir le formulaire en ligne sur le site du service d'Assistance technique.

Les fichiers de données sélectionnés seront compactés et envoyés sur le serveur du service d'assistance.

S'il n'est pas possible pour une raison quelconque de contacter le service d'assistance technique, vous pouvez enregistrer le fichier de données sur votre ordinateur.

Pour enregistrer les fichiers de données sur le disque, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique**, cliquez sur le lien **Outils d'assistance**.
4. Dans la fenêtre **Informations pour le service d'assistance technique**, dans le groupe **Actions** cliquez sur le bouton **Envoyer les informations pour le service d'assistance technique**.
5. Dans la fenêtre qui s'ouvre, cochez les cases en regard des fichiers de traçage que vous souhaitez envoyer au service d'assistance puis cliquez sur le bouton **Télécharger**.
6. Dans la fenêtre **Saisir le numéro de requête (numéro SRF)** cliquez sur le bouton **Non** et dans la fenêtre qui s'ouvre, confirmez l'enregistrement des fichiers sur le disque.
7. Dans la fenêtre qui s'ouvre définissez le nom d'archive.

Vous pourrez ensuite envoyer les fichiers enregistrés au service d'assistance technique via l'Espace personnel (https://my.kaspersky.com/fr/).

EXECUTION DU SCRIPT AVZ

Les experts de Kaspersky Lab analysent votre problème sur la base du fichier de trace et du rapport sur l'état du système. Cette analyse débouche sur une séquence d'actions à exécuter pour supprimer les problèmes identifiés. Le nombre de ces actions peut être très élevé.

Pour modifier la procédure de résolution des problèmes, des scripts AVZ sont utilisés. Le script AVZ est un ensemble d'instructions qui permettent de modifier les clés du registre, de mettre des fichiers en quarantaine, de lancer des recherches de catégories avec possibilité de mise en quarantaine des fichiers en rapport, de bloquer les intercepteurs UserMode et KernelMode, etc.

Pour exécuter les scripts inclus dans l'application, utilisez *l'Assistant d'exécution des scripts AVZ*. L'Assistant se présente sous la forme d'une succession de fenêtres (étapes) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Vous pouvez arrêter l'Assistant en cliquant sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Il est déconseillé de modifier le texte du script envoyé par les experts de Kaspersky Lab. En cas de problème lors de l'exécution du script, contactez le service d'assistance technique.

Pour lancer l'Assistant, procédez comme suit :

1. Ouvrez la fenêtre principale de l'application.
2. Dans la partie inférieure de la fenêtre de l'application, cliquez sur **Assistance technique**.
3. Dans la fenêtre **Assistance technique** qui s'ouvre, cliquez sur le lien **Outils d'assistance** dans la partie inférieure de la fenêtre.
4. Dans la fenêtre **Informations pour le service d'assistance technique** qui s'ouvre cliquez sur le bouton **Exécuter le script AVZ**.

Si l'exécution du script réussi, l'Assistant termine. Si un échec se produit durant l'exécution du script, l'Assistant affiche le message correspondant.

REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

Déclaration sur la collecte des données

A. INTRODUCTION

VEUILLEZ LIRE CE DOCUMENT ATTENTIVEMENT. IL CONTIENT DES INFORMATIONS IMPORTANTES DONT VOUS DEVEZ PRENDRE CONNAISSANCE AVANT DE CONTINUER À UTILISER NOS SERVICES OU NOTRE LOGICIEL. LA POURSUITE DE L'UTILISATION DU LOGICIEL ET DES SERVICES DE KASPERSKY LAB MARQUE VOTRE ACCEPTATION DE CETTE DÉCLARATION SUR LA COLLECTE DES DONNÉES PAR KASPERSKY LAB. Nous nous réservons le droit de modifier la présente déclaration sur la collecte des données en publiant les changements sur cette page. Veuillez vérifier la date de modification ci-dessous afin de voir si la politique a été amendée depuis votre dernière lecture. La poursuite de l'utilisation de n'importe lequel des services de Kaspersky Lab après la publication d'une déclaration actualisée sur la collecte des données marque votre acceptation des modifications introduites.

Kaspersky Lab et ses partenaires (ci-après « Kaspersky Lab ») ont rédigé cette déclaration sur la collecte des données afin de présenter les pratiques de collecte et de distribution de données pour Kaspersky Anti-Virus et Kaspersky Internet Security.

Propos de Kaspersky Lab

Kaspersky Lab est ouvertement engagée dans l'offre d'un service de qualité supérieure à tous ses clients et nous accordons une attention particulière à vos préoccupations sur la collecte de données. Nous sommes conscients des questions que vous pourriez avoir sur la manière dont Kaspersky Security Network rassemble et utilise les données et les informations et la présente déclaration (la « Déclaration sur la collecte des données » ou la « Déclaration » est née de notre volonté de vous présenter les principes qui régissent la collecte de données dans le cadre de Kaspersky Security Network.

Cette Déclaration sur la collecte des données reprend de nombreux détails généraux et techniques sur les procédures que nous avons mises en place pour répondre à vos préoccupations en la matière. Le présent document a été organisé selon les processus et les domaines afin que vous puissiez accéder rapidement aux informations qui vous intéressent le plus. Sachez que toutes nos actions, y compris la protection de vos données, sont gouvernées par la volonté de répondre à vos besoins et à vos attentes.

Les données et les informations sont recueillies par Kaspersky Lab. En cas de questions ou de doutes sur la collecte de données après la lecture de la présente déclaration, n'hésitez pas à envoyer un message électronique à l'adresse support@kaspersky.com.

Qu'est-ce que le Kaspersky Security Network ?

Le service Kaspersky Security Network permet à tous les utilisateurs des logiciels de sécurité informatique de Kaspersky Lab dans le monde entier de contribuer aux efforts d'identification des nouvelles menaces pour la sécurité de vos ordinateurs et de réduire de cette manière le temps de développement de la riposte adéquate. Afin de pouvoir identifier les nouvelles menaces et leurs sources et dans le but d'améliorer d'une part la sécurité de l'utilisateur et, d'autre part, les fonctions du logiciel, Kaspersky Security Network enregistre des données particulières sur la sécurité et les applications et les transmet à Kaspersky Lab où elles seront analysées. Ces informations ne contiennent aucun élément capable d'établir l'identité de l'utilisateur et elles sont exploitées par Kaspersky Lab dans l'unique but d'améliorer ses logiciels de sécurité et de renforcer les solutions contre les menaces malicieuses et les virus. Au cas où des données personnelles seraient recueillies par accident, Kaspersky Lab s'engage à les protéger conformément aux dispositions de cette Déclaration sur la collecte des données.

Votre participation au Kaspersky Security Network, conjointement aux autres utilisateurs des logiciels de sécurité informatique de Kaspersky Lab dans le monde entier, contribue énormément à la sécurisation d'Internet.

Questions légales

Il se peut que Kaspersky Security Network soit soumis aux lois de plusieurs juridictions dans la mesure où ses services peuvent être utilisés dans des juridictions différentes, y compris aux États-Unis. Kaspersky Lab dévoilera les informations

permettant d'établir votre identité sans votre autorisation dans les situations où la loi l'exige ou lorsqu'elle pense de bonne foi que cette action s'impose dans le cadre d'une enquête sur des activités qui nuisent aux biens, aux invités, aux visiteurs et aux partenaires de Kaspersky Lab ou à d'autres ou afin de les protéger contre les activités nuisibles. Comme nous l'avons déjà dit, la législation applicable aux données et aux informations recueillies dans le cadre du Kaspersky Security Network peut varier selon le pays. Ainsi, certaines données permettant d'établir l'identité d'un individu recueillies dans les États membres de l'Union européenne sont couvertes par les directives européennes relatives aux données personnelles, à la confidentialité et aux communications électroniques telles que la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et les législations ultérieures adoptées par les États membres ou la décision 497/2001/CE de la Commission européenne sur les clauses contractuelles types (transfert de données personnelles vers des pays tiers) et les législations ultérieures adoptées par les États membres de l'Union européenne.

Kaspersky Security Network informera comme il se doit les utilisateurs concernés au début de la collecte des informations citées ci-dessus ou avant de partager ces informations, notamment dans le cadre du développement commercial, et donnera la possibilité à ces utilisateurs d'Internet de marquer leur accord (dans les États membres de l'Union européenne et dans les autres pays qui requiert une procédure de confirmation volontaire) ou le désaccord (pour tous les autres pays) en ligne pour l'utilisation commerciale de ces données et/ou le transfert de celles-ci à des tiers.

Kaspersky Lab peut être obligée par les autorités judiciaires ou de police à fournir aux autorités publiques certaines données permettant d'établir l'identité d'un individu. En cas de demande introduite par les autorités judiciaires ou la police, nous fournirons ces informations dès que nous aurons reçu les documents adéquats. Kaspersky Lab pourra également fournir des informations à la police pour protéger ses biens ainsi que la santé et la sécurité de personnes dans les limites définies par les lois.

Les divulgations aux autorités de protection des données à caractère personnel des Etats membres seront réalisées conformément aux législations en vigueur dans les Etats membres de l'Union européenne. Les informations relatives à ces divulgations seront accessibles dans les services de Kaspersky Security Network.

B. INFORMATIONS RECUEILLIES

Les données que nous recueillons

Les utilisateurs ont le droit d'envoyer les données conformément à cette déclaration et le service Kaspersky Security Network est chargé de recueillir des données fondamentales et étendues sur les risques potentiels qui menacent votre ordinateur et de les transmettre à Kaspersky Lab. Ces données reprennent :

Données fondamentales

* Informations sur votre matériel et sur vos logiciels, y compris le système d'exploitation et les services pack installés, les objets du noyau, les pilotes, les services, les extensions Internet Explorer, les extensions d'impression, les extensions Windows Explorer, les fichiers de programme téléchargés, les éléments de configuration actifs, les applets du panneau de configuration, les enregistrements de l'hôte et du registre, les adresses IP, les types de navigateur, les clients de messagerie et le numéro de version du logiciel de Kaspersky Lab qui, en général, ne permettent pas d'établir l'identité ;

* Un identifiant unique généré par le logiciel de Kaspersky Lab pour identifier des machines individuelles sans identifier l'utilisateur et qui ne contient aucune information à caractère personnel ;

* Informations sur l'état de la protection antivirus de votre ordinateur et données sur tout fichier ou activité soupçonné de provenir d'un programme malveillant (exemple : nom de virus, date et heure de la détection, noms/chemin d'accès et taille des fichiers infectés, adresse IP et port de l'attaque de réseau, nom de l'application soupçonnée d'être malveillante). Notez que les données citées ci-dessus ne contiennent pas d'éléments d'information capables d'établir une identité.

Données étendues

* Informations relatives aux applications à signature numérique téléchargées par l'utilisateur (URL, taille de fichier, nom du signataire)

* Informations relatives aux applications exécutables (taille, attributs, date de création, informations sur les en-têtes PE, région, nom, emplacement et utilitaire de compression utilisé).

Fichiers et / ou leurs composants

Kaspersky Security network peut accumuler et confirmer les fichiers entiers et / ou leurs composants à propos de Kaspersky Lab pour l'analyse complémentaire. Le transfert des fichiers et / ou leurs composants est réalisé uniquement si vous avez accepté Kaspersky Lab Data Collection Statement.

Sécurisation de la transmission et du stockage des données

Kaspersky Lab s'engage à assurer la sécurité des données qu'elle recueille. Les informations recueillies sont stockées sur des serveurs auxquels l'accès est limité et contrôlé. Kaspersky Lab utilise des réseaux de données sécurisés protégés par des pare-feu conformes aux normes du secteur et des mots de passe. Kaspersky Lab utilise un large éventail de technologies et de procédures de sécurité pour protéger les informations recueillies contre les menaces telles que l'accès, l'utilisation ou la divulgation non autorisée. Nos politiques de sécurité sont revues à intervalle régulier et améliorées selon les besoins et seuls des individus autorisés ont accès aux données que nous recueillons. Kaspersky Lab veille à ce que vos données soient traitées en toute sécurité et conformément aux dispositions de cette Déclaration. Malheureusement, aucune transmission de données ne peut être sécurisée à 100%. Par conséquent, alors que nous entreprenons tout ce qui est en notre pouvoir pour protéger vos données, nous ne pouvons garantir la sécurité des données que vous nous envoyez depuis nos produits ou services, y compris, et sans limite, via le Kaspersky Security Network, et vous utilisez ces services à vos propres risques.

Les données qui sont recueillies peuvent être transmises aux serveurs de Kaspersky Lab et Kaspersky Lab a adopté les mesures de précaution nécessaire pour veiller à ce que les informations recueillies, si elles sont transmises, jouissent d'un niveau de protection adéquat. Nous traitons les données que nous recevons comme des données confidentielles, c.-à-d. conformément à nos procédures de sécurité et à nos politiques d'entreprise sur la protection et l'utilisation des données confidentielles. Une fois que les données recueillies sont arrivées chez Kaspersky Lab, elles sont stockées sur un serveur doté des mesures de protection physiques et électroniques habituelles dans le secteur, y compris le recours à des procédures d'ouverture de session/mot de passe et des pare-feu électroniques chargés de bloquer tout accès non autorisé depuis l'extérieur de Kaspersky Lab. Les données recueillies par le Kaspersky Security Network et couvertes par cette Déclaration sont traitées et stockées aux Etats-Unis et dans d'autres juridictions et dans d'autres pays où Kaspersky Lab est présente. Tous les employés de Kaspersky Lab connaissent nos politiques de sécurité. Vos données sont accessibles uniquement aux employés qui en ont besoin dans l'exercice de leur fonction. Aucune information stockée ne sera associée à des informations permettant d'établir une identité. Kaspersky Lab n'associe pas les données stockées par le Kaspersky Security Network à d'autres données, des listes de contact ou des informations d'abonnement recueillies par Kaspersky Lab à des fins de promotion ou autres.

C. UTILISATION DES DONNÉES RECUEILLIES

Utilisation de vos informations à caractère personnel

Kaspersky Lab recueille les données afin de les analyser et d'identifier les sources de risques pour la sécurité et dans le but d'améliorer la capacité des logiciels de Kaspersky Lab à détecter les comportements malveillants, les sites frauduleux, les programmes criminels et d'autres menaces présentes sur Internet afin de pouvoir offrir à l'avenir le meilleur niveau de protection possible aux clients de Kaspersky Lab.

Divulgation des informations aux tiers

Kaspersky Lab peut être amenée à divulguer des informations recueillies suite à une demande d'un représentant de la police si la loi l'exige ou l'autorise, suite à une citation à comparaître ou une autre procédure légale ou si nous croyons, en toute bonne foi, que nous devons agir de la sorte pour respecter la loi en vigueur, des règlements, une citation à comparaître ou d'autres procédures légales ou demandes imposées par les autorités publiques. Kaspersky Lab peut également dévoiler des informations permettant d'établir l'identité d'une personne lorsque nous avons des raisons de penser que la divulgation de ces informations s'impose pour identifier un individu, le contacter ou lancer des poursuites judiciaires contre celui-ci si il viole cette Déclaration, les dispositions du contrat avec la Société ou pour protéger la sécurité de nos utilisateurs et du public ou dans le cadre d'accord de confidentialité et de contrat de licence avec des tiers qui nous aident à développer, à faire fonctionner et à entretenir le Kaspersky Security Network. Afin de promouvoir la prise de conscience des risques que présente Internet et la détection et la prévention de ceux-ci, Kaspersky Lab peut partager certaines informations avec des organismes de recherche ou d'autres éditeurs de logiciels antivirus. Kaspersky Lab peut également utiliser les statistiques tirées des informations recueillies pour suivre les tendances au niveau des risques et rédiger des rapports.

Vos choix

La participation à Kaspersky Security Network est facultative. Vous pouvez activer et désactiver le service Kaspersky Security Network à tout moment dans la section Renvoi d'informations dans la page de configuration de votre logiciel Kaspersky Lab. Notez toutefois que si vous choisissez de désactiver le Kaspersky Security Network, nous ne serons peut-être pas en mesure de vous offrir certains des services qui dépendent de la collecte de ces données. Une fois que la période de service de votre logiciel Kaspersky Lab arrive à échéance, certaines des fonctions du logiciel peuvent continuer à fonctionner mais les informations ne seront pas envoyées automatiquement à Kaspersky Lab.

Nous nous réservons également le droit d'envoyer de temps à autre des messages d'alertes aux utilisateurs afin de les informer des modifications spécifiques qui pourraient avoir un impact sur leur capacité à utiliser les services auxquels ils ont souscrits. Nous nous réservons également le droit de vous contacter si une procédure légale nous y oblige ou si nous avons enregistré une violation des contrats de licence, d'achat ou de garantie.

Kaspersky Lab n'abandonne pas ces droits car en des cas restreints, nous pensons que nous pourrons avoir besoin de vous contacter pour une question légale ou pour d'autres questions qui pourraient être importantes pour vous. Ces droits ne nous autorisent pas à vous contacter pour vous présenter de nouveaux services ou des services existants si vous avez choisi de ne pas être contactés pour ce genre de communication et ce genre de publication est rare.

D. COLLECTE DE DONNÉES - QUESTIONS ET RÉCLAMATIONS

Kaspersky Lab prête la plus grande attention aux préoccupations des utilisateurs sur la collecte de données. Si vous estimez avoir été victime du non-respect de cette Déclaration quant à vos données ou vos informations ou si vous avez des questions, vous pouvez envoyer un courrier électronique à Kaspersky Lab : support@kaspersky.com.

Veuillez détailler le plus possible dans votre message la nature de votre demande. Nous étudierons votre demande ou votre réclamation dans les plus brefs délais.

L'envoi des informations est volontaire. L'option de collecte des données peut être désactivée par l'utilisateur à tout moment dans la rubrique « Renvoi d'informations » de la section « Configuration » du logiciel Kaspersky correspondant.

UTILISATION D'UN CODE TIERS

Du code développé par des éditeurs tiers a été utilisé dans Kaspersky Internet Security

DANS CETTE SECTION

Bibliotheque BLPI "Crypto-Sy"

La bibliothèque logicielle de protection des informations (BLPI) "Crypto-Sy", http://www.cryptoex.ru, développée par Crypto intervient dans la formation et la vérification de la signature numérique.

Bibliotheque FastScript 1.9

La bibliothèque FastScript copyright © Fast Reports Inc. All rights reserved a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

Bibliotheque pcre 7.4, 7.7

La bibliothèque pcre 7.4, 7.7 copyright © 1997-2008 University of Cambridge sous licence BSD a été utilisée dans le développement de l'application.

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Bibliotheque GNU bison parser

La bibliothèque bison parser skeleton 2,3 copyright © GNU Project http://ftp.gnu.org/gnu/bison/ dans le cadre d'une exclusion spéciale a été utilisée dans le développement de l'application.

As a special exception, you may create a larger work that containspart or all of the Bison parser skeleton and distribute that work under terms of your choice, so long as that work isn't itself a parser generator using the skeleton or a modified version thereof as a parser skeleton. Alternatively, if you modify or redistribute the parser skeleton itself, you may (at your option) remove this special exception, which will cause the skeleton and the resulting Bison output files to be licensed under the GNU General Public License without this special exception.

BIBLIOTHEQUE AGG 2.4

La bibliothèque AGG (Anti-Grain Geometry) 2,4 copyright © 2002-2005 Maxim Shemanarev a été utilisée dans le développement de l'application. All rights reserved, sous licence BSD modifiée.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘‘AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004 Alberto Demichelis

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

BIBLIOTHEQUE OPENSSL 0.9.8D

La bibliotèque OpenSSL 0,9.8d copyright © 1998-2007 The OpenSSL Project a été utilisée dans le développement de l'application. All rights reserved, sous les licences OpenSSL License et Original SSLeay License (http://www.openssl.org/).

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved a été utilisée dans le développement de l'application.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ‘‘AS IS’’ AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:"This product includes cryptographic software written byEric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ‘‘AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

BIBLIOTHEQUE GECKO SDK 1.8

La bibliothèque Gecko SDK 1.8 Copyright © Mozilla Foundation a été utilisée dans le développement de l'application. All rights reserved, sous licence MPL 1,1 (http://www.mozilla.org/MPL/MPL-1.1.html). Site Web et lien vers la distribution : http://developer.mozilla.org/en/docs/Gecko_SDK.

BIBLIOTHEQUE ZLIB 1.2

La bibliothèque zlib 1.2 copyright © 1995-2005 Jean-loup Gailly and Mark Adler a été utilisée dans le développement de l'application. All rights reserved sous licence zlib/libpng.

BIBLIOTHEQUE LIBPNG 1.2.8, 1.2.29

La bibliothèque libpng 1.2.8, 1.2.29 copyright © 2004, 2006-2008 Glenn Randers-Pehrson a été utilisée dans le développement de l'application. All rights reserved, sous licence zlib/libpng.

BIBLIOTHEQUE LIBNKFM 2.0.5

La bibliothèque libnkfm 2.0.5 Copyright (c) KUBO Takehiro a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE EXPAT 1.2, 2.0.1

La bibliothèque Expat 1,2, 2,0.1 Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd. All rights reserved, a été utilisée dans le développement de l'application dans les conditions suivantes :

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEQUE INFO-ZIP 5.51

La bibliothèque Info-ZIP 5.51 Copyright (c) 1990-2007 a été utilisée dans le développement de l'application. All rights reserved, sous licence Info-ZIP.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP", "Zip", "UnZip", "UnZipSFX", "WiZ", "Pocket UnZip", "Pocket Zip", and "MacZip" for its own source and binary releases.

BIBLIOTHÈQUE WINDOWS INSTALLER XML (WIX) 2.0

La bibliothèque Windows Installer XML (WiX) 2.0 Copyright (c) Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved, sous licence CPL 1.0 (http://sourceforge.net/projects/wix/).

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEQUE PASSTHRU

La bibliothèque Ndis Intermediate Miniport driver sample Copyright (c) 1992-2000 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE FILTER

La bibliothèque Ndis Sample NDIS Lightweight filter driver Copyright (c) 2004-2005 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE NETCFG

La bibliothèque Network Configuration Sample Copyright (c) 1997 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHEQUE PCRE 3.0

La bibliothèque pcre 3.0 copyright © 1997-1999 University of Cambridge, sous licence PCRE LICENCE a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application.

BIBLIOTHÈQUE RFC1321-BASED (RSA-FREE) MD5 LIBRARY

La bibliothèque RFC1321-based (RSA-free) MD5 library Copyright (c) 1999, 2002 Aladdin Enterprises a été utilisée dans le développement de l'application. All rights reserved a été utilisée dans le développement de l'application. Elle est diffusée sous licence zlib/libpng.

BIBLIOTHEQUE WINDOWS TEMPLATE LIBRARY (WTL 7.5)

La bibliothèque Windows Template Library 7,5 Copyright (c) 2005 Microsoft Corporation a été utilisée dans le développement de l'application. All rights reserved, sous licence Common Public license 1.0, http://sourceforge.net/projects/wtl/.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

   "Contribution" means:

   a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

   b) in the case of each subsequent Contributor:

   i) changes to the Program, and

   ii) additions to the Program;

   where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

   "Contributor" means any person or entity that distributes the Program.

   "Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

   "Program" means the Contributions distributed in accordance with this Agreement.

   "Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

   a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

   b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the

Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

BIBLIOTHEQUE LIBJPEG 6B

La bibliothèque libjpeg 6b copyright (c) 1991-1998, Thomas G. a été utilisée dans le développement de l'application. Lane. All Rights. Elle est utilisée dans les conditions suivantes :

LEGAL ISSUES

In plain English:

We don't promise that this software works. (But if you find any bugs, please let us know!)

You can use this software for whatever you want. You don't have to pay us.

You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining

code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

BIBLIOTHEQUE LIBUNGIF 3.0

La bibliothèque libungif 3.0 Copyright (c) 1997 Eric S a été utilisée dans le développpement de l'application. Raymond. Elle est utilisée dans les conditions suivantes :

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BIBLIOTHEQUE LIBXDR

La bibliothèque libxdr copyright © Sun Microsystems, Inc. a été utilisée dans le développement de l'application dans les conditions suivantes :

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

BIBLIOTHEQUE TINICONV - 1.0.0

La bibliothèque tiniconv – 1.0.0 Copyright (C) Free Software Foundation, Inc. author Roman Rybalko (http://sourceforge.net/projects/tiniconv/) sous licence GNU LGPL 2,1 (http://www.gnu.org/).

GNU LESSER GENERAL PUBLIC LICENSE v.2.1

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its

terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code

and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

BIBLIOTHÈQUE BZIP2/LIBBZIP2 1.0.5

La bibliothèque bzip2/libbzip2 1.0.5 a été utilisée dans le développement de l'application. copyright (C) 1996-2007 Julian R Seward. All rights reserved a été utilisée dans le développement de l'application. Elle est utilisée dans les conditions suivantes :

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyrightnotice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘‘AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

BIBLIOTHÈQUE LIBSPF2-1.2.9

La bibliothèque libspf2-1.2.9 Copyright 2005 by Shevek and Wayne Schlitt, all rights reserved, a été utilisée dans le développement de l'application sous les conditions The two-clause BSD license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ‘‘AS IS’’ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

BIBLIOTHEQUE PROTOCOL BUFFER

La bibliothèque Protocol Buffer Copyright 2008, Google Inc. All rights reserved, diffusée sous la licence New BSD License, a été utilisée dans le développement de l'application.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE

COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

GLOSSAIRE

Liste des masques et URL dont le contenu est jugé fiable par l'utilisateur. L'application de Kaspersky Lab ne recherche pas la présence éventuelle d'objets malveillants dans les pages qui correspondent à un élément de la liste.

Activation de l'application

La procédure d'activation de l'application consiste à saisir le code d'activation suite à la réception de la licence, ce qui permettra à l'application de définir les privilèges d'utilisation et la durée de validité de la licence.

Analyse du trafic

Analyse en temps réel des données transitant par tous les protocoles (exemple : HTTP, FTP etc.), à l'aide de la dernière version des bases d'objets.

Analyse heuristique

Technologie d'identification des menaces non reconnues par l'antivirus. Celle-ci permet d'identifier les objets soupçonnés d'être infectés par un virus inconnu ou par une nouvelle modification d'un virus connu.

L'analyseur heuristique permet d'identifier jusqu'à 92% des nouvelles menaces. Ce mécanisme est assez efficace et entraîne rarement des faux-positifs.

Les fichiers identifiés à l'aide de l'analyseur heuristique sont considérés comme des fichiers suspects.

Application incompatible

Application antivirus d'un autre éditeur ou application de Kaspersky Lab qui ne peut être administrée via Kaspersky Internet Security.

Archive

Fichier qui contient un ou plusieurs autres objets qui peuvent être des archives.

Attaque de virus

Tentatives multiples d'infection virale d'un ordinateur.

Base des URL de phishing

Liste des URL de sites identifiés par les experts de Kaspersky Lab comme des sites de phishing. La base est actualisée régulièrement et elle est livrée avec l'application de Kaspersky Lab.

Base des URL suspectes

Liste des URL dont le contenu pourrait constituer une menace. La liste est rédigée par les experts de Kaspersky Lab. Elle est actualisée régulièrement et est livrée avec l'application de Kaspersky Lab.

Bases

Les bases de données sont créées par les experts de Kaspersky Lab et elles contiennent une description détaillée de toutes les menaces informatiques qui existent à l'heure actuelle ainsi que les moyens de les identifier et de les neutraliser. Les bases sont actualisées en permanence par Kaspersky Lab au fur et à mesure que de nouvelles menaces sont découvertes. Pour améliorer la qualité de la découverte de menaces, nous vous conseillons de télécharger fréquemment les mises à jour des bases depuis les serveurs de mise à jour de Kaspersky Lab.

Bases de messagerie

Bases contenant les messages stockés sur votre ordinateur et possédant un format spécifique. Chaque message entrant/sortant est inscrit dans la base de données de messagerie après sa réception/son envoi. Ces bases sont analysées lors de l'analyse complète de l'ordinateur.

Si la protection en temps réel est activée, les messages entrants/sortants sont directement analysés lors de leur réception/envoi.

BLOCAGE D'UN OBJET

Interdiction de l'accès d'applications tiers à l'objet. L'objet bloqué ne peut être lu, exécuté, modifié ou supprimé.

CERTIFICAT DU SERVEUR D'ADMINISTRATION

Certificat qui intervient dans l'authentification du serveur d'administration lors de la connexion à celui-ci de la console d'administration et de l'échange de données avec les postes client. Le certificat du serveur d'administration est créé lors de l'installation du serveur d'administration et il est enregistré dans le sous-répertoire **Cert** du répertoire d'installation.

COMPTEUR D'EPIDEMIE DE VIRUS

Modèle qui sert à prévenir les utilisateurs en cas de menace d'épidémie de virus. Le compteur d'épidémie de virus renferme un ensemble de paramètres qui déterminent un seuil d'activité de virus, les modes de diffusions et le texte des messages.

COPIE DE SAUVEGARDE

Création d'une copie de sauvegarde du fichier avant sa réparation ou sa suppression et placement de cette copie dans la sauvegarde avec la possibilité de restaurer le fichier ultérieurement, par exemple pour l'analyse avec des bases actualisées.

COURRIER INDESIRABLE

Envoi massif non autorisé de messages électroniques, le plus souvent à caractère publicitaire.

DEGRE D'IMPORTANCE DE L'EVENEMENT

Caractéristique de l'événement consignée dans le fonctionnement de l'application de Kaspersky Lab. Il existe 14 degrés d'importance :

- **Evénement critique**.
- **Refus de fonctionnement**.
- **Avertissement**.
- **Information**.

Les événements de même type peuvent avoir différents degrés de gravité, en fonction du moment où l'événement s'est produit.

DOSSIER DE SAUVEGARDE

Le stockage spécial est conçu pour l'enregistrement des copies de sauvegarde des objets, créées avant leur première réparation ou suppression.

DUREE DE VALIDITE DE LA LICENCE

Durée pendant laquelle vous pouvez utiliser toutes les fonctions de l'application de Kaspersky Lab. Généralement, la durée de validité d'une licence est d'une année calendrier à partir de la date d'installation. Une fois que la durée de validité est écoulée, les fonctions de l'application sont bloquées : vous ne pourrez plus actualiser les bases de l'application.

ENREGISTREMENT DES OBJETS EN QUARANTAINE

Mode de traitement d'un objet potentiellement infecté empêchant tout accès à celui-ci et engendrant son déplacement vers le dossier de quarantaine où il est conservé de manière cryptée afin de prévenir toute action malveillante.

ETAT DE LA PROTECTION

État actuel de la protection caractérisé par le niveau de sécurité de l'ordinateur.

EXCLUSION

Objet exclu de l'analyse de l'application de Kaspersky Lab. Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple :un répertoire ou un programme), des processus ou

des objets selon un type de menace conforme à la classification de l'encyclopédie des virus. Des exclusions peuvent être définies pour chaque tâche.

FAUX POSITIF

Situation lors de laquelle un objet non infecté est considéré comme infecté par l'application Kaspersky Lab étant donné son code proche de celui d'un virus.

FICHIERS COMPACTE

Fichier d'archivage contenant un programme de décompactage ainsi que des instructions du système d'exploitation nécessaires à son exécution.

FICHIER DE LICENCE

Fichier portant l'extension **.key** et qui est votre "clé" personnelle, indispensable au fonctionnement de l'application de Kaspersky Lab. Ce fichier sera inclus dans le logiciel si celui-ci a été obtenu chez un distributeur Kaspersky Lab. En revanche, il vous sera envoyé par email si le produit provient d'une boutique Internet.

FLUX NTFS ALTERNATIFS

Flux de données du système de fichiers NTFS (alternate data streams), prévus pour contenir des attributs complémentaires ou des informations relatives au fichier.

Chaque fichier dans le système de fichiers NTFS présente un ensemble de flux (streams). Un des flux renferme le contenu du fichier que nous pouvons voir une fois que le fichier a été ouvert. Les autres flux (alternatifs) sont prévus pour les méta-informations et garantissent, par exemple, la compatibilité du système NTFS avec d'autres systèmes tels que l'ancien système de fichiers Macintosh - Hierarchical File System (HFS). Les flux peuvent être créés, supprimés, enregistrés séparément, renommer ou lancer comme processus.

Les flux alternatifs peuvent être exploités par des individus mal intentionnés dans le but de dissimuler l'envoi ou la réception de données de l'ordinateur.

INSTALLATION A L'AIDE D'UN SCRIPT DE LANCEMENT

Méthode d'installation à distance des applications de Kaspersky Lab qui permet d'associer le lancement d'une tâche d'installation à distance à un compte utilisateur particulier (ou pour plusieurs comptes). Lorsque l'utilisateur s'enregistre dans le domaine, une tentative d'installation de l'application sur le poste client d'où s'est connecté l'utilisateur est lancée. Cette méthode est conseillée pour l'installation d'applications sur des ordinateurs tournant sous Microsoft Windows 98 / Me.

INTERCEPTEUR

Sous-composant de l'application chargé de l'analyse de certains types de messages électroniques. La sélection d'intercepteurs installés dépend du rôle ou de la combinaison de rôles de l'application.

LICENCE ACTIVE

Licence en cours d'utilisation par l'application de Kaspersky Lab. La licence détermine la durée de validité du fonctionnement complet de l'application ainsi que la politique de licence de l'application. L'application ne peut avoir qu'une application active à la fois.

LICENCE DE RESERVE

Licence ajoutée pour le fonctionnement de l'application de Kaspersky Lab mais qui n'a pas été activée. La licence complémentaire entre en vigueur lorsque la licence active est arrivée à échéance.

LISTE DES EXPEDITEURS AUTORISES

(aussi la Liste "blanche" des adresses)

Liste des adresses électroniques, dont les messages ne sont pas analysés par l'application de Kaspersky Lab.

LISTE DES EXPEDITEURS INTERDITS

(aussi la Liste "noire" des adresses)

Liste des adresses électroniques dont les messages sont bloqués par l'application de Kaspersky Lab quel que soit leur contenu.

LISTE DES URL ANALYSEES

Liste des masques et des URL soumises obligatoirement à la recherche d'objets malveillants par l'application de Kaspersky Lab.

LISTE DES URL AUTORISEES

Liste des masques et des URL dont l'accès n'est pas bloqué par l'application de Kaspersky Lab. Liste des adresses est créée par l'utilisateur lors de la configuration des paramètres de l'application.

LISTE DES URL INTERDITES

Liste des masques et des URL dont l'accès est bloqué par l'application de Kaspersky Lab. Liste des adresses est créée par l'utilisateur lors de la configuration des paramètres de l'application.

LISTE NOIRE DES FICHIERS DE LICENCES

Base de données contenant des informations relatives aux clés de licence Kaspersky Lab préalablement bloquées, aux utilisateurs ayant transgressé les dispositions du contrat de licence et aux clés qui ont été émises mais qui, pour une quelconque raison, n'ont pas été vendue ou ont été échangées. Le fichier de la liste noire est indispensable au fonctionnement des applications de Kaspersky Lab. Le contenu du fichier est mis à jour en même temps que les bases.

MASQUE DE FICHIER

Représentation du nom et de l'extension d'un fichier par des caractères génériques. Les deux caractères principaux utilisés à cette fin sont ***** et **?** (où ***** représente n'importe quel nombre de caractères et **?** représente un caractère unique). A l'aide de ces caractères, il est possible de représenter n'importe quel fichier. Attention! le nom et l'extension d'un fichier sont toujours séparés par un point.

MASQUE DE SOUS-RESEAU

Le masque de sous-réseau et l'adresse réseau permettent d'identifier un ordinateur au sein d'un réseau informatique.

MESSAGE INDECENT

Message électronique contenant un vocabulaire non normatif.

MESSAGE SUSPECT

Message qui ne peut être catégorisé comme indésirable de manière certaine mais dont l'analyse donne lieu à des soupçons (par exemple, certains types d'envois et de messages publicitaires).

MISE A JOUR

Procédure de remplacement/d'ajout de nouveaux fichiers (bases ou modules logiciels), récupérés des serveurs de mise à jour de Kaspersky Lab.

MISE A JOUR ACCESSIBLE

Ensemble de mises à jour des modules de l'application de Kaspersky Lab qui reprend les mises à jour urgentes rassemblées au cours d'un intervalle de temps défini ainsi que les modifications de l'architecture de l'application.

MISE A JOUR DES BASES

Une des fonctions de l'application de Kaspersky Lab qui permet de garantir l'actualité de la protection. Dans ce scénario, les bases sont copiées depuis les serveurs de mise à jour de Kaspersky Lab sur l'ordinateur et elles sont installées automatiquement.

MISE A JOUR URGENTE

Mise à jour critique des modules de l'application de Kaspersky Lab.

MODELE DE NOTIFICATION

Modèle utilisé pour signaler la découverte d'objets infectés lors de l'analyse. Le modèle de notification contient un ensemble de paramètres qui définissent l'ordre des notifications, les moyens de diffusion et le texte du message.

MODULES LOGICIELS

Fichiers faisant partie de la distribution de l'application de Kaspersky Lab et responsables de ses principales tâches. Chaque type de tâche réalisée par l'application (Protection en temps réel, Analyse à la demande, Mise à jour) possède son propre module exécutable. En lançant l'analyse complète depuis la fenêtre principale, vous démarrez le module lié à cette tâche.

NIVEAU DE PROTECTION

Le niveau de protection est l'ensemble de paramètres prédéfinis de fonctionnement du composant.

NIVEAU RECOMMANDE

Niveau de protection qui repose sur les paramètres de fonctionnement définis par les experts de Kaspersky Lab et qui garantit la protection optimale de votre ordinateur. Ce niveau de protection est activé par défaut à l'installation.

OBJET A CONTROLER

Fichier transmis via le protocole HTTP, FTP ou SMTP par le pare-feu et envoyer à l'application de Kaspersky Lab pour analyse.

OBJET DANGEREUX

Objet contenant un virus. Nous vous déconseillons de manipuler de tels objets car ils pourraient infecter votre ordinateur. Suite à la découverte d'un objet infecté, il est conseillé de le réparer à l'aide d'une application de Kaspersky Lab ou de le supprimer si la réparation est impossible.

OBJET INFECTE

Objet contenant un code malveillant : l'analyse de l'objet a mis en évidence une équivalence parfaite entre une partie du code de l'objet et le code d'une menace connue. Les experts de Kaspersky Lab vous déconseillent de manipuler de tels objets car ils pourraient infecter votre ordinateur.

OBJET OLE

Objet uni ou intégré à un autre fichier. L'application de Kaspersky Lab permet de rechercher la présence éventuelle de virus dans les objets OLE. Par exemple, si vous insérez un tableau Excel dans un document Microsoft Office Word, ce tableau sera analysé comme un objet OLE.

OBJET INFECTE POTENTIELLEMENT

Objet qui, en raison de son format ou de sa structure, peut être utilisé par un individu mal intentionné en tant que "conteneur" pour abriter et diffuser un objet malveillant. En règle générale, il s'agit d'objets exécutables avec, par exemple, les extensions **com**, **exe**, **dll**, etc. Le risque d'infection par un code malveillant est très élevé pour ces fichiers.

OBJET POTENTIELLEMENT INFECTE

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets potentiellement infectés sont identifiés à l'aide de l'analyseur heuristique.

OBJET SUSPECT

Objet dont le code contient le code modifié d'un virus connu ou un code semblable à celui d'un virus mais inconnu de Kaspersky Lab. Les objets suspects sont détectés grâce à l'analyseur heuristique.

OBJETS DE DEMARRAGE

Série de programmes indispensables au lancement et au bon fonctionnement du système d'exploitation et des applications installés sur votre ordinateur. Ces objets sont exécutés à chaque démarrage du système d'exploitation. Il existe des virus qui s'attaquent en particulier à ces objets, ce qui peut par exemple provoquer le blocage du système d'exploitation.

PAQUET DE MISE A JOUR

Ensemble de fichiers provenant d'Internet et s'installant sur votre ordinateur afin de mettre à jour une application.

PARAMETRES DE L'APPLICATION

Paramètres de fonctionnement de l'application communs à tous les types de tâche, responsables du fonctionnement de l'application dans son ensemble, par exemple les paramètres de performance de l'application, les paramètres de création des rapports, les paramètres de la sauvegarde.

PARAMETRES DE LA TACHE

Paramètres de fonctionnement de l'application propres à chaque type de tâche.

PASSERELLE A DEUX CANAUX

Ordinateur doté de deux cartes de réseau, chacune d'entre elles connectée à un réseau différent et transmettant les informations d'un réseau à l'autre.

PORT DE RESEAU

Paramètre des protocoles TCP et UDP déterminant la destination des paquets de données IP transmis vers l'hôte via le réseau et permettant aux divers programmes utilisés sur ce même hôte de recevoir des données indépendamment les uns des autres. Chaque programme traite les données envoyées sur un port bien défini (en d'autres termes, le programme "écoute" ce port).

Certains ports standards sont destinés aux protocoles réseau les plus courants (par exemple, les serveurs Web réceptionnent généralement les données envoyées via le protocole HTTP sur le port TCP 80). Néanmoins, un programme peut utiliser n'importe quel protocole et n'importe quel port. Valeurs possibles: de 1 à 65535.

PORT ENTREE-SORTIE

Utilisé dans les microprocesseurs (par exemple Intel) lors de l'échange de données avec les périphériques. Le port entrée-sortie est comparé à l'un ou l'autre périphérique et permet aux applications de le contacter pour l'échange de données.

PORT MATERIEL

Connexion pour un périphérique matériel quelconque via un câble ou une fiche (port LPT, port série, USB).

PROCESSUS DE CONFIANCE

Processus d'une application dont les opérations sur les fichiers ne sont pas contrôlées par l'application de Kaspersky Lab dans le cadre de la protection en temps réel. Tous les objets lancés, ouverts ou conservés par un processus de confiance ne sont pas analysés.

PROTECTION EN TEMPS REEL

Mode de fonctionnement pendant lequel l'application analyse en temps réel la présence de code malveillant.

L'application intercepte toutes les tentatives d'ouverture d'un objet en lecture, écriture et exécution et recherche la présence éventuelle de menaces. Les objets sains sont ignorés alors que les objets (potentiellement) malveillants sont traités conformément aux paramètres de la tâche (réparation, suppression, mise en quarantaine).

PROTOCOLE

Ensemble de règles clairement définies et standardisées, régulant l'interaction entre un client et un serveur. Parmi les protocoles les plus connus et les services liés à ceux-ci, on peut noter: HTTP (WWW), FTP et NNTP (news).

PROTOCOLE D'INTERNET (IP)

Protocole de base du réseau Internet, inchangé depuis son lancement en 1974. Il exécute les opérations principales liées au transfert de données d'un ordinateur à un autre et est à la base de protocoles plus haut niveau tels que le TCP et l'UDP. Il gère la connexion ainsi que la correction d'erreurs. Grâce à des technologies tels que le NAT et le masquerading, il est possible de dissimuler d'importants réseaux privés derrière quelques adresses IP (parfois même derrière une seule adresse). Cela permet de satisfaire la demande sans cesse croissante d'adresses IP dont la plage IPv4 est relativement limitée.

REPARATION DES OBJETS

Mode de traitement des objets infectés qui débouche sur la restauration totale ou partielle des données ou sur le constat de l'impossibilité de réparer les objets. La réparation des objets s'opère sur la base des enregistrements des bases. Une partie des données peut être perdue lors de la réparation.

REPARATION DES OBJETS AU REDEMARRAGE

Mode de traitement des objets infectés utilisés par d'autres applications au moment de la réparation. Il consiste à créer une copie de l'objet infecté, à réparer cette copie et à remplacer l'objet original infecté par cette copie lors du redémarrage suivant de l'ordinateur.

RESTAURATION

Déplacement d'un objet original depuis le dossier de quarantaine ou de sauvegarde vers l'emplacement où il était avant sa mise en quarantaine, sa réparation ou sa suppression ou vers un dossier spécifié par l'utilisateur.

SCRIPT

Petit programme informatique ou partie indépendante d'un programme (fonction) écrit, en règle générale, pour exécuter une petite tâche particulière. Ils interviennent le plus souvent lors de l'exécution de programmes intégrés à de l'hypertexte. Les scripts sont exécutés, par exemple, lorsque vous ouvrez certains sites Web.

Si la protection en temps réel est activée, l'application surveille l'exécution des scripts, les intercepte et vérifie s'ils contiennent des virus. En fonction des résultats de l'analyse, vous pourrez autoriser ou bloquer l'exécution du script.

SECTEUR D'AMORÇAGE DU DISQUE

Le secteur d'amorçage est un secteur particulier du disque dur de l'ordinateur, d'une disquette ou d'un autre support de stockage informatique. Ilcontient des informations relatives au système de fichier du disque ainsi qu'un programme de démarrage s'exécutant au lancement du système d'exploitation.

Certains virus, appelés virus de boot ou virus de secteur d'amorçage, s'attaquent aux secteurs d'amorçage des disques. L'application de Kaspersky Lab permet d'analyser les secteurs d'amorçage afin de voir s'ils contiennent des virus et des les réparer en cas d'infection.

SERVEUR PROXY

Service dans les réseaux informatiques qui permet aux clients de réaliser des requêtes indirectes vers d'autres ressources du réseau. Le client se connecte d'abord au serveur proxy et envoi une requête vers une ressource quelconque (par exemple, un fichier) situé sur un autre serveur. Ensuite, le serveur proxy se connecte au serveur indiqué et obtient la ressource demandée ou récupère la ressource dans son cache (si le serveur proxy possède son propre cache). Dans certains cas, la requête du client ou la réponse du serveur peut être modifiée par le serveur proxy à des fins déterminées.

SERVEURS DE MISES A JOUR DE KASPERSKY LAB

Liste de serveurs HTTP et FTP de Kaspersky Lab d'où l'application peut récupérer les bases et les mises à jour des modules.

SERVICE DE NOMS DE DOMAINE (DNS)

Système partagé de traduction du nom d'hôte (ordinateur ou autre périphérique de réseau) en adresse IP. DNS fonctionne dans les réseaux TCP/IP. Dans certains cas particuliers, DNS peut enregistrer et traiter les requêtes de retour et définir le nom de l'hôte sur la base de son IP (enregistrement PTR). La résolution du nom DNS est généralement l'œuvre d'applications de réseau et non pas des utilisateurs.

SEUIL D'ACTIVITE VIRALE

Nombre d'événements d'un type donné et générés dans un intervalle de temps déterminé qui, une fois dépassé, permettra à l'application de considérer qu'il y a augmentation de l'activité virale et développement d'un risque d'attaque virale. Ce paramètre est d'une importance capitale en cas d'épidémie de virus car il permet à l'administrateur d'anticiper l'attaque.

SOCKS

Protocole de serveur proxy permettant une connexion à deux points entre des ordinateurs du réseau interne et des ordinateurs de réseaux externes.

SUPPRESSION D'UN MESSAGE

Mode de traitement d'un message électronique considéré comme indésirable. Il se caractérise par la suppression physique du message. Cette méthode est recommandée lorsque le message est indubitablement indésirable. Une copie du message supprimé est conservée dans le dossier de sauvegarde (pour autant que cette fonctionnalité ne soit pas désactivée).

SUPPRESSION D'UN OBJET

Mode de traitement de l'objet qui entraîne sa suppression physique de l'endroit où il a été découvert par l'application (disque dur, répertoire, ressource de réseau). Ce mode de traitement est recommandé pour les objets dangereux dont la réparation est impossible pour une raison quelconque.

TACHE

Fonctions exécutées par l'application de Kaspersky Lab sous la forme d'une tâche, par exemple : **Protection en temps réel des fichiers**, **Analyse complète de l'ordinateur**, **Mise à jour des bases**.

TECHNOLOGIE ICHECKER

Technologie qui permet d'accélérer l'analyse antivirus en excluant les objets qui n'ont pas été modifiés depuis l'analyse antérieure pour autant que les paramètres de l'analyse (bases antivirus et paramètres) n'aient pas été modifiés. Ces informations sont conservées dans une base spéciale. La technologie est appliquée aussi bien pendant la protection en temps réel que dans les analyses à la demande.

Admettons que vous possédez une archive qui a été analysée par une application de Kaspersky Lab et qui a reçu l'état *sain*. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez modifié le contenu de l'archive (ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases antivirus, l'archive sera analysée à nouveau.

Limitations technologiques **d'iChecker** :

- la technologie ne fonctionne pas avec les fichiers de grande taille car dans ce cas il est plus rapide d'analyser tout le fichier que de vérifier s'il a été modifié depuis la dernière analyse ;
- la technologie est compatible avec un nombre restreint de formats (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

TITRE

L'information, qui est contenue dans le début du fichier ou du message, se compose des données de faibles niveaux selon l'état et le traitement du fichier (message). En particulier, l'en-tête du courrier électronique contient des renseignements, tels que, les données de l'expéditeur, du destinataire et la date.

VIRUS DE DEMARRAGE

Virus affectant les secteurs d'amorçage du disque de l'ordinateur. Au redémarrage du système, le virus force le système à inscrire en mémoire et à exécuter du code malveillant au lieu du code d'amorçage original.

VIRUS INCONNU

Nouveau virus pour lequel aucune information ne figure dans les bases. En règle générale, les virus inconnus sont découverts dans les objets à l'aide de l'analyse heuristique et ces objets reçoivent l'état potentiellement infecté.

QUARANTAINE

Répertoire défini dans lequel sont placés tous les objets potentiellement infectés découverts pendant l'analyse ou par la protection en temps réel.

CONTRAT DE LICENCE D'UTILISATEUR FINAL DE KASPERSKY LAB

AVIS JURIDIQUE IMPORTANT À L'INTENTION DE TOUS LES UTILISATEURS : VEUILLEZ LIRE ATTENTIVEMENT LE CONTRAT SUIVANT AVANT DE COMMENCER À UTILISER LE LOGICIEL.

LORSQUE VOUS CLIQUEZ SUR LE BOUTON D'ACCEPTATION DE LA FENÊTRE DU CONTRAT DE LICENCE OU SAISISSEZ LE OU LES SYMBOLES CORRESPONDANTS, VOUS CONSENTEZ À LIÉ PAR LES CONDITIONS GÉNÉRALES DE CE CONTRAT. **CETTE ACTION EST UN SYMBOLE DE VOTRE SIGNATURE, ET VOUS CONSENTEZ PAR LA À VOUS SOUMETTRE AUX CONDITIONS DE CE CONTRAT ET À ÊTRE PARTIE DE CELUI-CI, ET CONVENEZ QUE CE CONTRAT A VALEUR EXÉCUTOIRE AU MÊME TITRE QUE TOUT CONTRAT ÉCRIT, NÉGOCIÉ SIGNÉ PAR VOS SOINS.** SI VOUS N'ACCEPTEZ PAS TOUTES LES CONDITIONS GÉNÉRALES DE CE CONTRAT, ANNULEZ L'INSTALLATION DU LOGICIEL ET NE L'INSTALLEZ PAS.

APRÈS AVOIR CLIQUÉ SUR LE BOUTON D'ACCEPTATION DANS LA FENÊTRE DU CONTRAT DE LICENCE OU AVOIR SAISI LE OU LES SYMBOLES CORRESPONDANTS, VOUS POUVEZ VOUS SERVIR DU LOGICIEL CONFORMÉMENT AUX CONDITIONS GÉNÉRALES DE CE CONTRAT.

1. Définitions

1.1. On entend par **Logiciel** le logiciel et toute mise à jour, ainsi que tous les documents associés.

1.2. On entend par **Titulaire des droits** (propriétaire de tous les droits exclusifs ou autres sur le Logiciel) Kaspersky Lab ZAO, une société de droit russe.

1.3. On entend par **Ordinateur(s)** le matériel, en particulier les ordinateurs personnels, les ordinateurs portables, les stations de travail, les assistants numériques personnels, les « téléphones intelligents », les appareils portables, ou autres dispositifs électroniques pour lesquels le Logiciel a été conçu où le Logiciel sera installé et/ou utilisé.

1.4. On entend par **Utilisateur final (vous/votre)** la ou les personnes qui installent ou utilisent le Logiciel en son ou en leur nom ou qui utilisent légalement le Logiciel ; ou, si le Logiciel est téléchargé ou installé au nom d'une entité telle qu'un employeur, *« Vous »* signifie également l'entité pour laquelle le Logiciel est téléchargé ou installé, et il est déclaré par la présente que ladite entité a autorisé la personne acceptant ce contrat à cet effet en son nom. Aux fins des présentes, le terme *« entité »,* sans limitation, se rapporte, en particulier, à toute société en nom collectif, toute société à responsabilité limité, toute société, toute association, toute société par actions, toute fiducie, toute société en coparticipation, toute organisation syndicale, toute organisation non constituée en personne morale, ou tout organisme public.

1.5. On entend par **Partenaire(s)** les entités, la ou les personnes qui distribuent le Logiciel conformément à un contrat et une licence concédée par le Titulaire des droits.

1.6. On entend par **Mise(s) à jour** toutes les mises à jour, les révisions, les programmes de correction, les améliorations, les patch, les modifications, les copies, les ajouts ou les packs de maintenance, etc.

1.7. On entend par **Manuel de l'utilisateur** le manuel d'utilisation, le guide de l'administrateur, le livre de référence et les documents explicatifs ou autres.

2. Concession de la Licence

2.1. Le Titulaire des droits convient par la présente de Vous accorder une licence non exclusive d'archivage, de chargement, d'installation, d'exécution et d'affichage (« l'utilisation ») du Logiciel sur un nombre spécifié d'Ordinateurs pour faciliter la protection de Votre Ordinateur sur lequel le Logiciel est installé contre les menaces décrites dans le cadre du Manuel de l'utilisateur, conformément à toutes les exigences techniques décrites dans le Manuel de l'utilisateur et aux conditions générales de ce Contrat (la « Licence ») et vous acceptez cette Licence :

Version de démonstration. Si vous avez reçu, téléchargé et/ou installé une version de démonstration du Logiciel et si l'on vous accorde par la présente une licence d'évaluation du Logiciel, vous ne pouvez utiliser ce Logiciel qu'à des fins d'évaluation et pendant la seule période d'évaluation correspondante, sauf indication contraire, à compter de la date d'installation initiale. Toute utilisation du Logiciel à d'autres fins ou au-delà de la période d'évaluation applicable est strictement interdite.

Logiciel à environnements multiples ; Logiciel à langues multiples ; Logiciel sur deux types de support ; copies multiples ; packs logiciels. Si vous utilisez différentes versions du Logiciel ou des éditions en différentes langues du Logiciel, si vous recevez le Logiciel sur plusieurs supports, ou si vous recevez plusieurs copies du Logiciel de quelque façon que ce soit, ou si vous recevez le Logiciel dans un pack logiciel, le nombre total de vos Ordinateurs sur lesquels toutes les versions du Logiciel sont autorisées à être installées doit correspondre au nombre de licences que vous avez obtenues auprès du Titulaire des droits, *sachant que,* sauf disposition contraire du contrat de licence, chaque licence achetée vous donne le droit d'installer et d'utiliser le Logiciel sur le nombre d'Ordinateurs stipulé dans les Clauses 2.2 et 2.3.

2.2. Si le Logiciel a été acheté sur un support physique, Vous avez le droit d'utiliser le Logiciel pour la protection du nombre d'ordinateurs stipulé sur l'emballage du Logiciel.

2.3. Si le Logiciel a été acheté sur Internet, Vous pouvez utiliser le Logiciel pour la protection du nombre d'Ordinateurs stipulé lors de l'achat de la Licence du Logiciel.

2.4. Vous ne pouvez faire une copie du Logiciel qu'à des fins de sauvegarde, et seulement pour remplacer l'exemplaire que vous avez acquis de manière légale si cette copie était perdue, détruite ou devenait inutilisable. Cette copie de sauvegarde ne peut pas être utilisée à d'autres fins et devra être détruite si vous perdez le droit d'utilisation du Logiciel ou à l'échéance de Votre licence ou à la résiliation de celle-ci pour quelque raison que ce soit, conformément à la législation en vigueur dans votre pays de résidence principale, ou dans le pays où Vous utilisez le Logiciel.

2.5. Vous pouvez transférer la licence non exclusive d'utilisation du Logiciel à d'autres personnes physiques ou morales dans la limite du champ d'application de la licence qui Vous est accordée par le Titulaire des droits, à condition que son destinataire accepte de respecter les conditions générales de ce Contrat et se substitue pleinement à vous dans le cadre de la licence que vous accorde le Titulaire des droits. Si Vous transférez intégralement les droits d'utilisation du Logiciel que vous accorde le Titulaire des droits, Vous devrez détruire toutes les copies du Logiciel, y compris la copie de sauvegarde. Si Vous êtes le destinataire du transfert d'une licence, Vous devez accepter de respecter toutes les conditions générales de ce Contrat. Si vous n'acceptez pas de respecter toutes les conditions générales de ce Contrat, Vous n'êtes pas autorisé à installer ou utiliser le Logiciel. Vous acceptez également, en qualité de destinataire de la licence transférée, de ne jouir d'aucun droit autre que ceux de l'Utilisateur final d'origine qui avait acheté le Logiciel auprès du Titulaire des droits.

2.6. À compter du moment de l'activation du Logiciel ou de l'installation du fichier clé de licence (à l'exception de la version de démonstration du Logiciel), Vous pouvez bénéficier des services suivants pour la période définie stipulée sur l'emballage du Logiciel (si le Logiciel a été acheté sur un support physique) ou stipulée pendant l'achat (si le Logiciel a été acheté sur Internet) :

- Mises à jour du Logiciel par Internet lorsque le Titulaire des droits les publie sur son site Internet ou par le biais d'autres services en ligne. Toutes les Mises à jour que vous êtes susceptible de recevoir font partie intégrante du Logiciel et les conditions générales de ce Contrat leur sont applicables ;
- Assistance technique en ligne et assistance technique par téléphone.

3. Activation et durée de validité

3.1. Si vous modifiez Votre Ordinateur ou procédez à des modifications sur des logiciels provenant d'autres vendeurs et installés sur celui-ci, il est possible que le Titulaire des droits exige que Vous procédiez une nouvelle fois à l'activation du Logiciel ou à l'installation du fichier clé de licence. Le Titulaire des droits se réserve le droit d'utiliser tous les moyens et toutes les procédures de vérification de la validité de la Licence ou de la légalité du Logiciel installé ou utilisé sur Votre ordinateur.

3.2. Si le Logiciel a été acheté sur un support physique, le Logiciel peut être utilisé dès l'acceptation de ce Contrat pendant la période stipulée sur l'emballage et commençant à l'acceptation de ce Contrat.

3.3. Si le Logiciel a été acheté sur Internet, le Logiciel peut être utilisé à votre acceptation de ce Contrat, pendant la période stipulée lors de l'achat.

3.4. Vous avez le droit d'utiliser gratuitement une version de démonstration du Logiciel conformément aux dispositions de la Clause 2.1 pendant la seule période d'évaluation correspondante (30 jours) à compter de l'activation du Logiciel conformément à ce Contrat, *sachant que* la version de démonstration ne Vous donne aucun droit aux mises à jour et à l'assistance technique par Internet et par téléphone.

3.5. Votre Licence d'utilisation du Logiciel est limitée à la période stipulée dans les Clauses 3.2 ou 3.3 (selon le cas) et la période restante peut être visualisée par les moyens décrits dans le Manuel de l'utilisateur.

3.6. Si vous avez acheté le Logiciel dans le but de l'utiliser sur plus d'un Ordinateur, Votre Licence d'utilisation du Logiciel est limitée à la période commençant à la date d'activation du Logiciel ou de l'installation du fichier clé de licence sur le premier Ordinateur.

3.7. Sans préjudice des autres recours en droit ou équité à la disposition du Titulaire des droits, dans l'éventualité d'une rupture de votre part de toute clause de ce Contrat, le Titulaire des droits sera en droit, à sa convenance et sans préavis, de révoquer cette Licence d'utilisation du Logiciel sans rembourser le prix d'achat en tout ou en partie.

3.8. Vous vous engagez, dans le cadre de votre utilisation du Logiciel et de l'obtention de tout rapport ou de toute information dans le cadre de l'utilisation de ce Logiciel, à respecter toutes les lois et réglementations internationales, nationales, étatiques, régionales et locales en vigueur, ce qui comprend, sans toutefois s'y limiter, les lois relatives à la protection de la vie privée, des droits d'auteur, au contrôle des exportations et à la lutte contre les outrages à la pudeur.

3.9. Sauf disposition contraire spécifiquement énoncée dans ce Contrat, vous ne pouvez transférer ni céder aucun des droits qui vous sont accordés dans le cadre de ce Contrat ou aucune de vos obligations de par les présentes.

4. Assistance technique

L'assistance technique décrite dans la Clause 2.6 de ce Contrat Vous est offerte lorsque la dernière mise à jour du Logiciel est installée (sauf pour la version de démonstration du Logiciel).

Service d'assistance technique : http://support.kaspersky.com

5. Recueil d'informations

5.1. Conformément aux conditions générales de ce Contrat, Vous consentez à communiquer au Titulaire des droits des informations relatives aux fichiers exécutables et à leurs sommes de contrôle pour améliorer Votre niveau de protection et de sécurité.

5.2. Pour sensibiliser le public aux nouvelles menaces et à leurs sources, et dans un souci d'amélioration de Votre sécurité et de Votre protection, le Titulaire des droits, avec votre consentement explicitement confirmé dans le cadre de la déclaration de recueil des données du réseau de sécurité Kaspersky, est autorisé à accéder à ces informations. Vous pouvez désactiver le réseau de sécurité Kaspersky pendant l'installation. Vous pouvez également activer et désactiver le réseau de sécurité Kaspersky à votre guise, à la page des options du Logiciel.

Vous reconnaissez par ailleurs et acceptez que toutes les informations recueillies par le Titulaire des droits pourront être utilisées pour suivre et publier des rapports relatifs aux tendances en matière de risques et de sécurité, à la seule et exclusive appréciation du Titulaire des droits.

5.3. Le Logiciel ne traite aucune information susceptible de faire l'objet d'une identification personnelle et ne combine les données traitées avec aucune information personnelle.

5.4. Si vous ne souhaitez pas que les informations recueillies par le Logiciel soient transmises au Titulaire des droits, n'activez pas ou ne désactivez pas le réseau de sécurité Kaspersky.

6. Limitations

6.1. Vous vous engagez à ne pas émuler, cloner, louer, prêter, donner en bail, vendre, modifier, décompiler, ou faire l'ingénierie inverse du Logiciel, et à ne pas démonter ou créer des travaux dérivés reposant sur le Logiciel ou toute portion de celui-ci, à la seule exception du droit inaliénable qui Vous est accordé par la législation en vigueur, et vous ne devez autrement réduire aucune partie du Logiciel à une forme lisible par un humain ni transférer le Logiciel sous licence, ou toute sous-partie du Logiciel sous licence, ni autoriser une tierce partie de le faire, sauf dans la mesure où la restriction précédente est expressément interdite par la loi en vigueur. Ni le code binaire du Logiciel ni sa source ne peuvent être utilisés à des fins d'ingénierie inverse pour recréer le programme de l'algorithme, qui est la propriété exclusive du Titulaire des droits. Tous les droits non expressément accordés par la présente sont réservés par le Titulaire des droits et/ou ses fournisseurs, suivant

le cas. Toute utilisation du Logiciel en violation du Contrat entraînera la résiliation immédiate et automatique de ce Contrat et de la Licence concédée de par les présentes, et pourra entraîner des poursuites pénales et/ou civiles à votre encontre.

6.2. Vous ne devrez transférer les droits d'utilisation du Logiciel à aucune tierce partie sauf aux conditions énoncées dans la Clause 2.5 de ce Contrat.

6.3. Vous vous engagez à ne communiquer le code d'activation et/ou le fichier clé de licence à aucune tierce partie, et à ne permettre l'accès par aucune tierce partie au code d'activation et au fichier clé de licence qui sont considérés comme des informations confidentielles du Titulaire des droits, et vous prendrez toutes les mesures raisonnables nécessaires à la protection du code d'activation et/ou du fichier clé de licence, étant entendu que vous pouvez transférer le code d'activation et/ou le fichier clé de licence à de tierces parties dans les conditions énoncées dans la Clause 2.5 de ce Contrat.

6.4. Vous vous engagez à ne louer, donner à bail ou prêter le Logiciel à aucune tierce partie.

6.5. Vous vous engagez à ne pas vous servir du Logiciel pour la création de données ou de logiciels utilisés dans le cadre de la détection, du blocage ou du traitement des menaces décrites dans le Manuel de l'utilisateur.

6.6. Le Titulaire des droits a le droit de bloquer le fichier clé de licence ou de mettre fin à votre Licence d'utilisation du Logiciel en cas de non-respect de Votre part des conditions générales de ce Contrat, et ce, sans que vous puissiez prétendre à aucun remboursement.

6.7. Si vous utilisez la version de démonstration du Logiciel, Vous n'avez pas le droit de bénéficier de l'assistance technique stipulée dans la Clause 4 de ce Contrat, et Vous n'avez pas le droit de transférer la licence ou les droits d'utilisation du Logiciel à une tierce partie.

7. Garantie limitée et avis de non-responsabilité

7.1. Le Titulaire des droits garantit que le Logiciel donnera des résultats substantiellement conformes aux spécifications et aux descriptions énoncées dans le Manuel de l'utilisateur, *étant toutefois entendu* que cette garantie limitée ne s'applique pas dans les conditions suivantes : (w) des défauts de fonctionnement de Votre Ordinateur et autres non-respects des clauses du Contrat, auquel cas le Titulaire des droits est expressément dégagé de toute responsabilité en matière de garantie ; (x) les dysfonctionnements, les défauts ou les pannes résultant d'une utilisation abusive, d'un accident, de la négligence, d'une installation inappropriée, d'une utilisation ou d'une maintenance inappropriée ; des vols ; des actes de vandalisme ; des catastrophes naturelles ; des actes de terrorisme ; des pannes d'électricité ou des surtensions ; des sinistres ; de l'altération, des modifications non autorisées ou des réparations par toute partie autre que le Titulaire des droits ; ou des actions d'autres tierces parties ou Vos actions ou des causes échappant au contrôle raisonnable du Titulaire des droits ; (y) tout défaut non signalé par Vous au Titulaire dès que possible après sa constation ; et (z) toute incompatibilité causée par les composants du matériel et/ou du logiciel installés sur Votre Ordinateur.

7.2. Vous reconnaissez, acceptez et convenez qu'aucun logiciel n'est exempt d'erreurs, et nous Vous recommandons de faire une copie de sauvegarde des informations de Votre Ordinateur, à la fréquence et avec le niveau de fiabilité adaptés à Votre cas.

7.3. Le Titulaire des droits n'offre aucune garantie de fonctionnement correct du Logiciel en cas de non-respect des conditions décrites dans le Manuel de l'utilisateur ou dans ce Contrat.

7.4. Le Titulaire des droits ne garantit pas que le Logiciel fonctionnera correctement si Vous ne téléchargez pas régulièrement les Mises à jour spécifiées dans la Clause 2.6 de ce Contrat.

7.5. Le Titulaire des droits ne garantit aucune protection contre les menaces décrites dans le Manuel de l'utilisateur à l'issue de l'échéance de la période indiquée dans les Clauses 3.2 ou 3.3 de ce Contrat, ou à la suite de la résiliation pour une raison quelconque de la Licence d'utilisation du Logiciel.

7.6. LE LOGICIEL EST FOURNI « TEL QUEL » ET LE TITULAIRE DES DROITS N'OFFRE AUCUNE GARANTIE QUANT À SON UTILISATION OU SES PERFORMANCES. SAUF DANS LE CAS DE TOUTE GARANTIE, CONDITION, DÉCLARATION OU TOUT TERME DONT LA PORTÉE NE PEUT ÊTRE EXCLUE OU LIMITÉE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS ET SES PARTENAIRES N'OFFRENT AUCUNE GARANTIE, CONDITION OU DÉCLARATION (EXPLICITE OU IMPLICITE, QUE CE SOIT DE PARLA LÉGISLATION EN VIGUEUR, LE « COMMON LAW », LA COUTUME, LES USAGES OU AUTRES) QUANT À TOUTE QUESTION DONT, SANS LIMITATION, L'ABSENCE D'ATTEINTE AUX DROITS DE TIERCES PARTIES, LE CARACTÈRE COMMERCIALISABLE, LA QUALITÉ SATISFAISANTE, L'INTÉGRATION OU L'ADÉQUATION À UNE FIN PARTICULIÈRE. VOUS ASSUMEZ TOUS LES DÉFAUTS, ET L'INTÉGRALITÉ DES RISQUES LIÉS À LA PERFORMANCE ET AU CHOIX DU LOGICIEL POUR ABOUTIR AUX RÉSULTATS QUE VOUS RECHERCHEZ, ET À L'INSTALLATION DU LOGICIEL, SON UTILISATION ET LES RÉSULTATS OBTENUS AU MOYEN DU LOGICIEL. SANS LIMITER LES DISPOSITIONS PRÉCÉDENTES, LE TITULAIRE DES DROITS NE FAIT AUCUNE DÉCLARATION ET N'OFFRE AUCUNE GARANTIE QUANT À L'ABSENCE D'ERREURS DU LOGICIEL, OU L'ABSENCE D'INTERRUPTIONS OU D'AUTRES PANNES, OU LA

SATISFACTION DE TOUTES VOS EXIGENCES PAR LE LOGICIEL, QU'ELLES SOIENT OU NON DIVULGUÉES AU TITULAIRE DES DROITS.

8. Exclusion et Limitation de responsabilité

DANS LA MESURE MAXIMALE PERMISE PAR LA LOI EN VIGUEUR, LE TITULAIRE DES DROITS OU SES PARTENAIRES NE SERONT EN AUCUN CAS TENUS POUR RESPONSABLES DE TOUT DOMMAGE SPÉCIAL, ACCESSOIRE, PUNITIF, INDIRECT OU CONSÉCUTIF QUEL QU'IL SOIT (Y COMPRIS, SANS TOUTEFOIS S'Y LIMITER, LES DOMMAGES POUR PERTES DE PROFITS OU D'INFORMATIONS CONFIDENTIELLES OU AUTRES, EN CAS D'INTERRUPTION DES ACTIVITÉS, DE PERTE D'INFORMATIONS PERSONNELLES, DE CORRUPTION, DE DOMMAGE À DES DONNÉES OU À DES PROGRAMMES OU DE PERTES DE CEUX-CI, DE MANQUEMENT À L'EXERCICE DE TOUT DEVOIR, Y COMPRIS TOUTE OBLIGATION STATUTAIRE, DEVOIR DE BONNE FOI OU DE DILIGENCE RAISONNABLE, EN CAS DE NÉGLIGENCE, DE PERTE ÉCONOMIQUE, ET DE TOUTE AUTRE PERTE PÉCUNIAIRE OU AUTRE PERTE QUELLE QU'ELLE SOIT) DÉCOULANT DE OU LIÉ D'UNE MANIÈRE QUELCONQUE À L'UTILISATION OU À L'IMPOSSIBILITÉ D'UTILISATION DU LOGICIEL, À L'OFFRE D'ASSISTANCE OU D'AUTRES SERVICES OU À L'ABSENCE D'UNE TELLE OFFRE, LE LOGICIEL, ET LE CONTENU TRANSMIS PAR L'INTERMÉDIAIRE DU LOGICIEL OU AUTREMENT DÉCOULANT DE L'UTILISATION DU LOGICIEL, OU AUTREMENT DE PAR OU EN RELATION AVEC TOUTE DISPOSITION DE CE CONTRAT, OU DÉCOULANT DE TOUTE RUPTURE DE CE CONTRAT OU DE TOUT ACTE DOMMAGEABLE (Y COMPRIS LA NÉGLIGENCE, LA FAUSSE DÉCLARATION, OU TOUTE OBLIGATION OU DEVOIR EN RESPONSABILITÉ STRICTE), OU DE TOUT MANQUEMENT À UNE OBLIGATION STATUTAIRE, OU DE TOUTE RUPTURE DE GARANTIE DU TITULAIRE DES DROITS ET DE TOUT PARTENAIRE DE CELUI-CI, MÊME SI LE TITULAIRE DES DROITS OU TOUT PARTENAIRE A ÉTÉ INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES.

VOUS ACCEPTEZ QUE, DANS L'ÉVENTUALITÉ OÙ LE TITULAIRE DES DROITS ET/OU SES PARTENAIRES SONT ESTIMÉS RESPONSABLES, LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES SERA LIMITÉE AUX COÛTS DU LOGICIEL. LA RESPONSABILITÉ DU TITULAIRE DES DROITS ET/OU DE SES PARTENAIRES NE SAURAIT EN AUCUN CAS EXCÉDER LES FRAIS PAYÉS POUR LE LOGICIEL AU TITULAIRE DES DROITS OU AU PARTENAIRE (LE CAS ÉCHÉANT).

AUCUNE DISPOSITION DE CE CONTRAT NE SAURAIT EXCLURE OU LIMITER TOUTE DEMANDE EN CAS DE DÉCÈS OU DE DOMMAGE CORPOREL. PAR AILLEURS, DANS L'ÉVENTUALITÉ OÙ TOUTE DÉCHARGE DE RESPONSABILITÉ, TOUTE EXCLUSION OU LIMITATION DE CE CONTRAT NE SERAIT PAS POSSIBLE DU FAIT DE LA LOI EN VIGUEUR, ALORS SEULEMENT, CETTE DÉCHARGE DE RESPONSABILITÉ, EXCLUSION OU LIMITATION NE S'APPLIQUERA PAS DANS VOTRE CAS ET VOUS RESTEREZ TENU PAR LES DÉCHARGES DE RESPONSABILITÉ, LES EXCLUSIONS ET LES LIMITATIONS RESTANTES.

9. Licence GNU et autres licences de tierces parties

Le Logiciel peut comprendre des programmes concédés à l'utilisateur sous licence (ou sous-licence) dans le cadre d'une licence publique générale GNU (General Public License, GPL) ou d'autres licences de logiciel gratuites semblables, qui entre autres droits, autorisent l'utilisateur à copier, modifier et redistribuer certains programmes, ou des portions de ceux-ci, et à accéder au code source (« Logiciel libre »). Si ces licences exigent que, pour tout logiciel distribué à quelqu'un au format binaire exécutable, le code source soit également mis à la disposition de ces utilisateurs, le code source sera être communiqué sur demande adressée à source@kaspersky.com ou fourni avec le Logiciel. Si une licence de Logiciel libre devait exiger que le Titulaire des droits accorde des droits d'utilisation, de reproduction ou de modification du programme de logiciel libre plus importants que les droits accordés dans le cadre de ce Contrat, ces droits prévaudront sur les droits et restrictions énoncés dans les présentes.

10. Droits de propriété intellectuelle

10.1 Vous convenez que le Logiciel et le contenu exclusif, les systèmes, les idées, les méthodes de fonctionnement, la documentation et les autres informations contenues dans le Logiciel constituent un élément de propriété intellectuelle et/ou des secrets industriels de valeur du Titulaire des droits ou de ses partenaires, et que le Titulaire des droits et ses partenaires, le cas échéant, sont protégés par le droit civil et pénal, ainsi que par les lois sur la protection des droits d'auteur, des secrets industriels et des brevets de la Fédération de Russie, de l'Union européenne et des Etats-Unis, ainsi que d'autres pays et par les traités internationaux. Ce Contrat ne vous accorde aucun droit sur la propriété intellectuelle, en particulier toute marque de commerce ou de service

du Titulaire des droits et/ou de ses partenaires (les « Marques de commerce »). Vous n'êtes autorisé à utiliser les Marques de commerce que dans la mesure où elles permettent l'identification des informations imprimées par le Logiciel conformément aux pratiques admises en matière de marques de commerce, en particulier l'identification du nom du propriétaire de la Marque de commerce. Cette utilisation d'une marque de commerce ne vous donne aucun droit de propriété sur celle-ci. Le Titulaire des droits et/ou ses partenaires conservent la propriété et tout droit, titre et intérêt sur la Marque de commerce et sur le Logiciel, y compris sans limitation, toute correction des erreurs, amélioration, mise à jour ou autre modification du Logiciel, qu'elle soit apportée par le Titulaire des droits ou une tierce partie, et tous les droits d'auteur, brevets, droits sur des secrets industriels, et autres droits de propriété intellectuelle afférents à ce Contrat. Votre possession, installation ou utilisation du Logiciel ne transfère aucun titre de propriété intellectuelle à votre bénéfice, et vous n'acquerrez aucun droit sur le Logiciel, sauf dans les conditions expressément décrites dans le cadre de ce Contrat. Toutes les reproductions du Logiciel effectuées dans le cadre de ce Contrat doivent faire mention des mêmes avis d'exclusivité que ceux qui figurent sur le Logiciel. Sauf dans les conditions énoncées par les présentes, ce Contrat ne vous accorde aucun droit de propriété intellectuelle sur le Logiciel et vous convenez que la Licence telle que définie dans ce document et accordée dans le cadre de ce Contrat ne vous donne qu'un droit limité d'utilisation en vertu des conditions générales de ce Contrat. Le Titulaire des droits se réserve tout droit qui ne vous est pas expressément accordé dans ce Contrat.

10.2 Vous convenez que le code source, le code d'activation et/ou le fichier clé de licence sont la propriété exclusive du Titulaire des droits et constituent des secrets industriels dudit Titulaire des droits. Vous convenez de ne pas modifier, adapter, traduire le code source du Logiciel, de ne pas en faire l'ingénierie inverse, ni le décompiler, désassembler, ni tenter de toute autre manière de découvrir le code source du Logiciel.

10.3 Vous convenez de ne modifier ou altérer le Logiciel en aucune façon. Il vous est interdit d'éliminer ou d'altérer les avis de droits d'auteur ou autres avis d'exclusivité sur tous les exemplaires du Logiciel.

11. Droit applicable ; arbitrage

Ce Contrat sera régi et interprété conformément aux lois de la Fédération de Russie sans référence aux règlements et aux principes en matière de conflits de droit. Ce Contrat ne sera pas régi par la Conférence des Nations Unies sur les contrats de vente internationale de marchandises, dont l'application est strictement exclue. Tout litige auquel est susceptible de donner lieu l'interprétation ou l'application des clauses de ce Contrat ou toute rupture de celui-ci sera soumis à l'appréciation du Tribunal d'arbitrage commercial international de la Chambre de commerce et d'industrie de la Fédération de Russie à Moscou (Fédération de Russie), à moins qu'il ne soit réglé par négociation directe. Tout jugement rendu par l'arbitre sera définitif et engagera les parties, et tout tribunal compétent pourra faire valoir ce jugement d'arbitrage. Aucune disposition de ce Paragraphe 11 ne saurait s'opposer à ce qu'une Partie oppose un recours en redressement équitable ou l'obtienne auprès d'un tribunal compétent, avant, pendant ou après la procédure d'arbitrage.

12. Délai de recours.

Aucune action, quelle qu'en soit la forme, motivée par des transactions dans le cadre de ce Contrat, ne peut être intentée par l'une ou l'autre des parties à ce Contrat au-delà d'un (1) an à la suite de la survenance de la cause de l'action, ou de la découverte de sa survenance, mais un recours en contrefaçon de droits de propriété intellectuelle peut être intenté dans la limite du délai statutaire maximum applicable.

13. Intégralité de l'accord ; divisibilité ; absence de renoncement.

Ce Contrat constitue l'intégralité de l'accord entre vous et le Titulaire des droits et prévaut sur tout autre accord, toute autre proposition, communication ou publication préalable, par écrit ou non, relatifs au Logiciel ou à l'objet de ce Contrat. Vous convenez avoir lu ce Contrat et l'avoir compris, et vous convenez de respecter ses conditions générales. Si un tribunal compétent venait à déterminer que l'une des clauses de ce Contrat est nulle, non avenue ou non applicable pour une raison quelconque, dans sa totalité ou en partie, cette disposition fera l'objet d'une interprétation plus limitée de façon à devenir légale et applicable, l'intégralité du Contrat ne sera pas annulée pour autant, et le reste du Contrat conservera toute sa force et tout son effet dans la mesure maximale permise par la loi ou en equity de façon à préserver autant que possible son intention originale. Aucun renoncement à une disposition ou à une condition quelconque de ce document ne saurait être valable, à moins qu'il soit signifié par écrit et signé de votre main et de celle d'un représentant autorisé du Titulaire des droits, étant entendu qu'aucune exonération de rupture d'une disposition de ce Contrat ne saurait constituer une exonération d'une rupture préalable, concurrente ou subséquente. Le manquement à la stricte application de toute disposition ou tout droit de ce Contrat par le Titulaire des droits ne saurait constituer un renoncement à toute autre disposition ou tout autre droit de par ce Contrat.

14. Service clientèle

Si vous souhaitez joindre le Titulaire des droits pour toute question relative à ce Contrat ou pour quelque raison que ce soit, n'hésitez pas à vous adresser à notre service clientèle aux coordonnées suivantes :

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moscou, 123060
Fédération de Russie

Tél. :+7-495-797-8700
Fax : +7-495-645-7939

E-mail : info@kaspersky.com

Site Internet : www.kaspersky.com

KASPERSKY LAB

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 1000 spécialistes, tous spécialistes des technologies antivirus : 10 d'entre eux possèdent un M.B.A, 16 autres un doctorat. Les experts principaux de Kaspersky Lab siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. Grâce à l'analyse en continu de l'activité virale, nous pouvons prévoir les tendances dans le développement des programmes malfaisants et fournir à temps à nos utilisateurs une protection optimale contre les nouveaux types d'attaques. Cet avantage est à la base des produits et des services proposés par Kaspersky Lab. Nous sommes toujours en avance sur la concurrence et nous fournissons à nos clients la meilleure protection possible.

Grâce à des années de travail assidu, la société est devenue leader en développement de systèmes de défense antivirus. Kaspersky Lab fut l'une des premières entreprises à mettre au point les standards de défense antivirale les plus exigeants. Le produit vitrine de la société est Kaspersky Antivirus® : il assure une protection complète de tous les périmètres réseau, et couvre les postes de travail, les serveurs de fichiers, les systèmes de messagerie, les pare-feu et passerelles Internet, ainsi que les ordinateurs portables. La convivialité de l'administration permet aux utilisateurs d'automatiser au maximum la protection des ordinateurs et des réseaux d'entreprise. De nombreux fabricants reconnus utilisent le noyau Kaspersky Anti-Virus : Nokia ICG (Etats-Unis), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en œuvre et accompagnons les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos clients une assistance technique en plusieurs langues.

Si vous avez des questions, vous pouvez les adresser au revendeur ou directement à Kaspersky Lab. Vous bénéficierez toujours de consultations détaillées par téléphone ou courrier électronique. Vous recevrez des réponses complètes à vos questions.

Site officiel de Kaspersky Lab : http://www.kaspersky.com/fr

Encyclopédie de virus : http://www.viruslist.com/fr/

Laboratoire antivirus : http://newvirus.kaspersky.fr

Forum de Kaspersky Lab : http://forum.kaspersky.com

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

Z