MANUEL DE L'UTILISATEUR

KASPERSKY INTERNET SECURITY 2009 SPECIAL EDITION FOR ULTRA-PORTABLES

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 que vous pourriez avoir sur le logiciel.

+7 (495) 645-7939,
Téléphone, fax : +7 (495) 797-8700,
+7 (495) 956-7000

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

Date d'édition : 08.04.2009

TABLE DES MATIERES

INSTALLATION DE KASPERSKY INTERNET SECURITY

Kaspersky Internet Security 2009 Special Edition for Ultra-Portables peut être installé dans un des modes suivants :

- interactif, à l'aide de l'Assistant d'installation. Ce mode exige la participation de l'utilisateur ;
- non interactif. Le démarrage d'installation en ce mode s'effectue depuis la ligne de commande et ne requiert pas la participation de l'utilisateur.

Avant l'installation de Kaspersky Internet Security, il est recommandé de fermer toutes les applications actives.

DANS CETTE SECTION

OBTENTION D'INFORMATIONS SUR L'APPLICATION

Si vous avez des questions sur le choix de l'application, l'achat de celle-ci, son installation ou son utilisation, vous pouvez obtenir les réponses rapidement.

Kaspersky Lab propose de nombreuses sources d'informations sur l'application et vous pouvez choisir celle qui vous convient le mieux en fonction de l'importance et de l'urgence de la question.

SOURCES D'INFORMATIONS POUR LES RECHERCHES INDEPENDANTES

Vous pouvez utiliser le système d'aide en ligne.

L'aide contient des informations sur la gestion de la protection de l'ordinateur : consultation de l'état de la protection, recherche de virus dans divers secteurs de l'ordinateur, exécution d'autres tâches.

Pour ouvrir l'aide, cliquez sur le lien **Aide** dans la fenêtre principale de l'application ou appuyez sur la touche **<F1>** du clavier.

CONTACTER LE SERVICE COMMERCIAL

Si vous avez des questions sur le choix, sur l'achat d'une application ou sur le renouvellement de la licence, vous pouvez contacter notre service commercial à ce numéro :

0.825.888.612

Vous pouvez également contacter le service commercial par courrier électronique en écrivant à **info@fr.kaspersky.com**.

CONTACTER LE SERVICE D'ASSISTANCE TECHNIQUE

Si vous avez déjà acheté l'application, vous pouvez obtenir des renseignements sur celle-ci auprès des opérateurs du service d'assistance technique, par téléphone ou via Internet.

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 de votre ordinateur, ils vous aideront à surmonter les conséquences de l'action des programmes malveillants.

Assistance Technique en ligne

Vous pouvez retrouver toutes nos options de support à partir de notre portail de support :

http://support.kaspersky.fr/kis2009

Vous pouvez également accéder à notre banque de solution en vous rendant sur ce site :

http://kb.kaspersky.fr/kis2009

Requête électronique adressée au service d'assistance technique (pour les utilisateurs enregistrés)

Vous pouvez poser vos questions aux experts du service d'assistance technique via le formulaire en ligne :

http://support.kaspersky.fr/requete

Vous pouvez envoyer vos messages en russe, en anglais, en allemand, en français ou en espagnol.

Pour envoyer une requête par voie électronique, vous devez indiquer le **numéro de client** obtenu lors de l'enregistrement sur le site Internet du service d'assistance technique ainsi que le **mot de passe**.

Remarque

Si vous n'êtes pas un utilisateur enregistré des applications de Kaspersky Lab, vous pouvez remplir le formulaire d'inscription à la page https://support.kaspersky.com/fr/PersonalCabinet/Registration/Form/. Lors de l'enregistrement, saisissez le *code d'activation* de l'application ou le *nom du fichier de licence*.

L'opérateur du service d'assistance technique vous enverra sa réponse à l'adresse électronique que vous avez indiquée ainsi que dans votre **Espace personnel.**

Décrivez le plus exactement possible le problème que vous rencontrez. Dans les champs obligatoires, indiquez :

- Le **type de requête**. Les questions les plus souvent posées par les utilisateurs sont reprises dans des sujets distincts, par exemple "Problème d'installation/de suppression du logiciel" ou "Problème de recherche/de neutralisation de virus". Si vous ne trouvez pas un sujet qui se rapproche le plus de votre situation, choisissez "Question générale".

- **Nom et numéro de version de l'application**.

- **Texte de la demande**. Décrivez le problème rencontré avec le plus de détails possibles

- **Numéro de client et mot de passe**. Saisissez le numéro de client et le mot de passe que vous avez obtenu lors de l'enregistrement sur le site du service d'assistance technique.

- **Adresse de messagerie**. Il s'agit de l'adresse à laquelle les experts du service d'assistance technique enverront la réponse à votre question.

DISCUSSION SUR LES APPLICATIONS DE KASPERSKY LAB SUR LE FORUM

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

Sur le forum, vous pouvez consulter les sujets publiés, ajouter des commentaires, créer une nouvelle discussion ou lancer des recherches.

CONCEPTION DE LA PROTECTION DE L'APPLICATION

Kaspersky Internet Security protège votre ordinateur contre les menaces connues ou nouvelles, les attaques de pirates et les escroqueries, le courrier indésirable et d'autres données malveillantes. Chacune de ces menaces est traitée par un composant particulier de l'application. Cette conception du système de protection permet d'utiliser en souplesse et de configurer chaque composant en fonction des besoins d'un utilisateur particulier ou de l'entreprise dans son ensemble.

Kaspersky Internet Security comprend :

- Le contrôle de l'activité des applications dans le système empêche l'exécution d'actions dangereuses.

- Des composants de protection contre les programmes malveillants qui protègent tous les canaux de transfert de données de et vers votre ordinateur en temps réel.

- Les composants de la protection pendant l'utilisation d'Internet qui protègent votre ordinateur contre les attaques de réseau et les escroqueries en ligne connues à ce moment.

- Les composants du filtrage des données indésirables qui permettent de gagner du temps et d'économiser du trafic et de l'argent.

- Des tâches de recherche de virus qui procède à la recherche d'éventuels virus dans l'ordinateur ou dans des fichiers, des répertoires, des disques ou des secteurs particuliers. Ces tâches peuvent également être configurées pour identifier les vulnérabilités dans les applications installées.

- La mise à jour, garantit l'actualité des modules internes de l'application et des bases utilisées pour la recherche des programmes malveillants, l'identification des attaques de réseau et le filtrage du courrier indésirable.

- Assistants et instruments qui facilitent l'exécution des tâches pendant le fonctionnement de Kaspersky Internet Security.

- Des services qui garantissent le soutien information dans le cadre de l'utilisation du logiciel et qui permettent d'en élargir les fonctions.

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 d'analyse de la sécurité qui pose le diagnostic de la sécurité de l'ordinateur et qui recherche les vulnérabilités du système d'exploitation et des programmes installés.

- Assistant de configuration du navigateur qui analyse les paramètres du navigateur Microsoft Internet Explorer et qui les évalue avant tout du point de vue de la sécurité.

- L'Assistant de restauration après infection permet de liquider les traces de la présence d'objets malveillants dans le système.

- Assistant de suppression des traces d'activité qui recherche les traces d'activité de l'utilisateur dans le système et qui les supprime tout comme les paramètres du système d'exploitation qui permettent d'accumuler des informations sur l'activité de l'utilisateur.

- Analyse des paquets de réseaux qui intercepte les paquets de réseau et qui affiche des informations détaillées à leur sujet.

- Surveillance du réseau qui offre des informations détaillées sur l'activité de réseau sur votre ordinateur.

- Le clavier virtuel permet d'éviter l'interception des données saisies à l'aide du clavier traditionnel.

FONCTIONS DE SERVICE

L'application propose diverses fonctions de service. Ceux-ci visent à maintenir la protection de l'ordinateur à jour, à élargir les possibilités d'utilisation du programme et à fournir de l'aide pendant l'utilisation du programme.

Kaspersky Security Network

Kaspersky Security Network est un système de transfert automatique des rapports sur les menaces découvertes ou potentielles vers une base de données centralisée. Cette base de données permet de réagir encore plus vite aux menaces les plus répandues et de signaler les épidémies aux utilisateurs.

Licence

Lorsque vous achetez l'application, vous entrez dans un contrat de licence entre vous et Kaspersky Lab. Ce contrat vous permet d'utiliser l'application et d'accéder aux mises à jour de l'application et au service d'assistance technique pendant une certaine période. La durée de validité ainsi que d'autres informations indispensables au déblocage de toutes les fonctions de l'application sont reprises dans la licence.

Grâce à la fonction **Licence**, vous pouvez obtenir des informations détaillées sur la licence que vous utilisez ainsi qu'acheter une nouvelle licence ou renouveler la licence en cours.

Assistance technique

Tous les utilisateurs enregistrés de l'application peuvent faire appel au service d'assistance technique. Utilisez la fonction **Assistance technique** pour savoir où vous pouvez obtenir l'assistance technique dont vous avez besoin.

A l'aide des liens prévus à cet effet, vous pouvez accéder au forum des utilisateurs des logiciels de Kaspersky Lab et envoyer des commentaires au service d'assistance technique sur des erreurs ou sur le fonctionnement de l'application via le formulaire en ligne.

Le service d'assistance technique est accessible en ligne tout comme le service d'espace personnel de l'utilisateur et nos opérateurs sont toujours prêts à répondre à vos questions sur l'utilisation de l'application par téléphone.

ANALYSE HEURISTIQUE

Les méthodes d'analyse heuristique interviennent dans le fonctionnement de certains composants de la protection en temps réel tels que l'Antivirus Fichiers, l'Antivirus Courrier et l'Antivirus Internet ainsi que dans les tâches de recherche de virus.

Comme vous le savez, l'analyse sur la base des signatures à l'aide de bases constituées antérieurement et contenant les définitions des menaces connues ainsi que les méthodes de réparation, indique clairement si l'objet analysé est malveillant et la catégorie à laquelle il appartient. La méthode heuristique, au contraire de la méthode qui repose sur les signatures, ne vise pas à trouver la signature d'un code malveillant mais bien les séquences d'opérations typiques qui permettent de tirer, avec une certaine dose de certitude, des conclusions sur la nature d'un fichier.

L'avantage de la méthode heuristique tient au fait que son application ne requiert pas l'existence de bases. Ainsi, les nouvelles menaces peuvent être identifiées avant que leur activité ne soit remarquée par les spécialistes des virus.

Toutefois, il existe des méthodes qui permettent de contourner les méthodes heuristiques. L'une d'entre elles consiste à geler l'activité du code malveillant au moment de la découverte de l'application de méthodes heuristiques dans l'analyse.

Remarque

La combinaison de différentes méthodes d'analyse garantit une meilleure protection.

En cas de doute vis-à-vis d'une menace, l'analyseur heuristique émule l'exécution de l'objet dans un environnement virtuel sécurisé de l'application. Si des actions suspectes sont identifiées pendant l'exécution, l'objet est considéré comme suspect et soit, son exécution sur l'ordinateur est bloquée, soit un message s'affiche et invite l'utilisateur à déterminer la suite des événements :

- 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 que cet objet ne peut pas être malveillant.

Pour utiliser la méthode heuristique, cochez la case **Utiliser l'analyseur heuristique**. Vous pouvez, en plus, sélectionner le niveau d'analyse à l'aide du curseur : superficielle, moyenne ou en profondeur. Le niveau de détail de l'analyse garantit l'équilibre entre la minutie de la recherche des virus, c.-à-d. la qualité, et la charge imposée aux ressources du système d'exploitation et la durée de l'analyse. Plus le niveau de l'analyse est élevé, plus les ressources du système seront sollicitées et plus longtemps elle prendra.

Attention !

Les nouvelles menaces, découvertes grâce à l'analyseur heuristique, sont étudiées par les spécialistes de Kaspersky Lab et les outils de réparation sont proposés dans les bases actualisées toutes les heures.

Si vous procédez régulièrement à la mise à jour des base de l'application, votre ordinateur jouira du niveau de protection optimal.

CONFIGURATION MATERIELLE ET LOGICIELLE REQUISES

Pour garantir le fonctionnement normal de l'application, l'ordinateur doit répondre aux exigences minimales suivantes :

Recommandations d'ordre général :

- 75 Mo d'espace disponible sur le disque dur.
- Périphérique de saisie et de manipulation (souris).
- Microsoft Internet Explorer 5.5 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 ou suivant), Microsoft Windows XP Professional (service pack 2 ou suivant) :

- Processeur Intel Atom, Intel Celeron-M ou VIA C7-M.
- 256 Mo de mémoire vive disponible.

MENACES SUR LA SECURITE INFORMATIQUE

Les programmes-menaces constituent la majeure partie du danger qui plane sur la sécurité informatique. Outre ces programmes, le courrier indésirable, les attaques de pirates informatiques et les bannières publicitaires peuvent également présenter un certain danger. Ces menaces sont liées à l'utilisation d'Internet.

DANS CETTE SECTION

PROGRAMMES MENACES

L'application de Kaspersky Lab est capable d'identifier des centaines de milliers de programmes dangereux sur l'ordinateur. Certains de ces programmes constituent une grande menace pour les ordinateurs des utilisateurs tandis que d'autres sont dangereux uniquement dans certaines conditions. Une fois que l'application a découvert un programme dangereux, elle le classe et lui attribue un niveau de danger (élevé ou moyen).

Les experts antivirus de Kaspersky Lab distinguent deux catégories principales : les *programmes malveillants* et les *programmes potentiellement malveillants*.

Les Programmes malveillants (cf. p. 15) (Malware) sont créés spécialement pour nuire à l'ordinateur et à son utilisateur, par exemple bloquer, voler, modifier ou détruire des données, perturber le fonctionnement de l'ordinateur ou du réseau.

Les Programmes potentiellement malveillants (cf. page 27) (PUP, potentially unwanted programs) à la différence des programmes malveillants ne sont pas développés dans le but de nuire mais ils peuvent malgré tout violer la sécurité de l'ordinateur.

L'Encyclopédie des virus (http://www.viruslist.com/fr/viruses/encyclopedia) propose une description détaillée de ces programmes.

PROGRAMMES MALVEILLANTS

Les programmes malveillants sont créés spécialement pour nuire aux ordinateurs et à leurs utilisateurs : voler, bloquer, modifier ou détruire des données, perturber le fonctionnement des ordinateurs ou des réseaux.

Les programmes malveillants sont scindés en trois groupes : les virus et les vers, les chevaux de Troie et les utilitaires malveillants.

Les Virus et vers (cf. page 15) (Viruses_and_Worms) peuvent créer leur copie capable de se propager vers d'autres machines. Certains sont exécutés sans intervention de l'utilisateur tandis que d'autres requièrent une action de l'utilisateur. Ces programmes commencent leur action malveillante dès le lancement.

Les Chevaux de Troie (cf. page 18) (Trojan_programs) ne créent pas leur copie, à la différence des vers. Ils s'infiltrent sur les ordinateurs via le courrier Internet ou via le navigateur lorsque l'internaute visite un site infecté. Leur exécution requiert l'intervention de l'utilisateur ; ils entament leur action malveillante au démarrage.

Les utilitaires malveillants (cf. page 24) (Malicious_tools) sont conçus spécialement pour nuire. Mais à la différence des autres programmes malveillants, ils n'exécutent pas d'actions malveillantes dès le lancement et peuvent être préservés et exécutés sans danger sur l'ordinateur de l'utilisateur. Ces programmes possèdent des fonctions qui interviennent dans la préparation de virus, de vers et de chevaux de Troie, l'organisation d'attaques de réseau sur des serveurs distants, l'intrusion dans des ordinateurs ou d'autres actions malveillantes.

VIRUS ET VERS

Sous-catégorie : virus et vers (Viruses_and_Worms)

Niveau de danger : élevé

Les virus et les vers classiques exécutent sur l'ordinateur des actions qui n'ont pas été autorisées par l'utilisateur et peuvent créer leur propre copie qui possède la capacité d'auto-reproduction.

Virus classique

Une fois que le virus classique s'est introduit dans un système, il infecte un fichier quelconque, s'y active, exécute son action malveillante puis ajoute sa copie à d'autres fichiers.

Le virus classique se multiplie uniquement sur les ressources locales de l'ordinateur ; il est incapable de s'introduire lui-même dans un autre ordinateur. Il peut pénétrer dans d'autres systèmes uniquement s'il ajoute sa copie dans un fichier enregistré dans un répertoire partagé ou sur un cédérom ou si l'utilisateur envoie un message avec le fichier infecté en pièce jointe.

Le code du virus classique peut s'introduire dans divers secteurs de l'ordinateur, du système d'exploitation ou de l'application. Sur la base de l'environnement d'exécution, on distingue les virus de *fichier*, les virus de *démarrage*, les virus de *script* et les virus de *macro*.

Les virus peuvent infecter des fichiers de diverses manières. Les virus *écraseurs* (overwriting) remplace le code du fichier infecté par leur propre code et supprime ainsi le contenu du fichier. Le fichier infecté n'est plus exploitable et il ne peut être réparé. Les virus *parasites* (Parasitic) modifient les fichiers, mais ceux-ci demeurent totalement ou partiellement fonctionnels. Les *virus compagnons* (Companion) ne modifient pas les fichiers mais créent des copies. Lorsque le fichier infecté est exécuté, son double est lancé, à savoir le virus. Il existe également des *virus-liens* (Link), des virus *qui infectent les modules objets* (OBJ), des virus *qui infectent les bibliothèques de compilateur* (LIB), les virus *qui infectent les textes source des programmes* et d'autres.

Ver

Le code du ver, à l'instar de celui du virus classique, s'active et exécute son action malveillante dès qu'il s'est introduit dans le système. Toutefois, le ver doit son nom à sa capacité à "ramper" d'ordinateur en ordinateur, sans que l'utilisateur n'autorise cette diffusion des copies via divers canaux d'informations.

La principale caractéristique qui distingue les vers entre eux, c'est le mode de diffusion. Le tableau suivant reprend une description des différents types de vers en fonction du mode de diffusion.

Tableau 1. Vers en fonction du mode de propagation

TYPE	NOM	DESCRIPTION
Email-Worm	Vers de messagerie	Ils se diffusent via le courrier électronique. Le message infecté contient un fichier joint avec la copie du ver ou un lien vers ce fichier sur un site compromis. Quand la pièce jointe est exécutée, le ver s'active ; lorsque vous cliquez sur le lien, téléchargez le fichier puis l'exécutez, le ver entame également son action malveillante. Ensuite, il continue à diffuser ses copies après avoir trouvé d'autres adresses électroniques, il envoie des messages infectés.
IM-Worm	Vers de messagerie instantanée	Ils se propagent via les messageries instantanées telles que ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ou Skype. En règle général, ce ver envoie un message aux contacts. Ce message contient un lien vers la copie du ver sur un site. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.
IRC-Worm	Vers de chats	Ils se diffusent via les canaux IRC, ces systèmes qui permettent de discuter en temps réel avec d'autres personnes. Ce ver publie un fichier avec sa copie ou un lien vers celle-ci dans le chat. Quand l'utilisateur télécharge le fichier et l'ouvre, le ver s'active.
Net-Worm	Vers de réseau (vers de réseaux informatiques)	Ils se diffusent via les réseaux informatiques. A la différence des autres types de vers, le ver de réseau se propage sans l'intervention de l'utilisateur. Il recherche une application vulnérable sur les ordinateurs du réseau local. Pour ce faire, il envoie un paquet de réseau spécial (un code d'exploitation) qui contient le code du ver ou une partie de celui-ci. Si le réseau abrite un ordinateur "vulnérable", celui-ci acceptera le paquet. Une fois qu'il a pénétré dans cet ordinateur, le ver s'active.

TYPE	NOM	DESCRIPTION
P2P-Worm	Vers de réseau d'échange de fichiers	Ils se diffusent via les réseaux d'échange de fichiers (P2P) tels que Kazaa, Grokster, EDonkey, FastTrack ou Gnutella. Afin d'infiltrer le réseau, le ver se copie dans le répertoire d'échange de fichiers qui se trouve normalement sur l'ordinateur de l'utilisateur. Le réseau d'échange de fichiers illustre les informations relatives à ce fichier et l'utilisateur peut "trouver" le fichier infecté comme n'importe quel autre fichier, le télécharger puis l'ouvrir. Les vers plus sophistiqués imitent le protocole d'un réseau d'échange de fichiers en particulier : ils répondent positivement aux recherches et proposent leur copie pour le téléchargement.
Worm	Autres vers	Parmi ces autres vers, citons : • les vers qui diffusent leur copie via les ressources de réseau. A l'aide des fonctions du système d'exploitation, ils consultent les répertoires de réseau disponibles, se connectent aux ordinateurs du réseau mondial et tentent d'ouvrir leur disque en libre accès. A la différence des vers de réseau informatique, l'utilisateur doit ouvrir le fichier contenant la copie du ver afin de l'activer. • Les vers qui n'adoptent aucun des moyens de propagation décrits dans ce tableau (par exemple, diffusion via les téléphones mobiles).

CHEVAUX DE TROIE

Sous-catégorie : chevaux de Troie (Trojan_programs)

Niveau de danger : élevé

A la différence des vers et des virus, les chevaux de Troie ne créent pas leur propre copie. Ils s'infiltrent sur les ordinateurs via le courrier Internet ou via le navigateur lorsque l'internaute visite un site infecté. Les chevaux de Troie sont

exécutés sur intervention de l'utilisateur ; ils entament leur action malveillante au démarrage.

Le comportement des chevaux de Troie sur l'ordinateur infecté varie. Parmi les fonctions principales des chevaux de Troie, citons le blocage, la modification ou la suppression d'informations, la perturbation du fonctionnement des ordinateurs ou des réseaux. De plus, les chevaux de Troie peuvent recevoir ou envoyer des fichiers, les exécuter, afficher des messages, contacter des pages Web, télécharger des programmes et les installer et redémarrer l'ordinateur.

Les individus mal intentionnés utilisent souvent des "sélections" composées de divers chevaux de Troie.

Le tableau ci-après offre une description des chevaux de Troie en fonction de leur comportement.

Tableau 2. Types de chevaux de Troie selon le comportement sur l'ordinateur infecté

TYPE	NOM	DESCRIPTION
Trojan-ArcBomb	Chevaux de Troie (bombes dans les archives)	Il s'agit d'archive qui, au moment du décompactage, atteigne un tel poids qu'elles perturbent le fonctionnement de l'ordinateur. Dès que vous tentez de décompacter une archive de ce genre, l'ordinateur peut commencer à ralentir, voire à s'arrêter et le disque peut se remplir de données "vides". Ces "bombes" sont particulièrement dangereuses pour les serveurs de fichiers et de messagerie. Si le serveur utilise un système de traitement automatique des données entrantes, ce genre de "bombe d'archive" peut entraîner l'arrêt du serveur.
Backdoor	Chevaux de Troie d'administration à distance	Considérés comme les chevaux de Troie les plus dangereux ; leurs fonctions rappellent celles des programmes d'administration à distance disponibles dans les magasins. Ces programmes s'installent à l'insu de l'utilisateur sur l'ordinateur et permettent à l'individu mal intentionné d'administrer l'ordinateur à distance.
Trojan	Chevaux de Troie	Cette catégorie reprend les programmes malveillants suivants : • **Chevaux de Troie traditionnels** ; ils exécutent uniquement les fonctions

TYPE	NOM	DESCRIPTION
		fondamentales des chevaux de Troie : blocage, modification ou suppression des informations, perturbation du fonctionnement des ordinateurs ou des réseaux informatiques ; ils ne possèdent pas les fonctions complémentaires caractéristiques d'autres chevaux de Troie décrits dans ce tableau ; • **Chevaux de Troie multicibles** ; ils possèdent des fonctions complémentaires appartenant à divers types de chevaux de Troie.
Trojan-Ransom	Chevaux de Troie exigeant le versement d'une rançon	Ces programmes "prennent en otage" les données de l'ordinateur après les avoir modifiées ou bloquées ou perturbent le fonctionnement de l'ordinateur de telle manière que l'utilisateur n'est plus en mesure d'exploiter les données. L'individu mal intentionné exige le paiement d'une somme d'argent en échange de l'envoi d'un programme qui rétablira le fonctionnement de l'ordinateur et les données qu'il abrite.
Trojan-Clicker	Chevaux de Troie qui cliquent	Ils accèdent à des pages Web depuis l'ordinateur de la victime : ils envoient des instructions au navigateur ou remplacent les adresses Internet conservées dans les fichiers systèmes. Grâce à ces programmes malveillants, les individus mal intentionnés organisent des attaques de réseau ou augmentent le nombre de visites sur le site afin d'augmenter le nombre d'affichage de publicité.
Trojan-Downloader	Chevaux de Troie qui téléchargent	Ils contactent la page Web de l'individu mal intentionné, y téléchargent d'autres programmes malveillants et les installent sur l'ordinateur de la victime ; ils peuvent conserver le nom du programme malveillant à télécharger ou le récupérer sur la page Web qu'ils contactent.

TYPE	NOM	DESCRIPTION
Trojan-Dropper	Chevaux de Troie qui procèdent à des installations	Ils enregistrent sur le disque puis installent d'autres chevaux de Troie présents dans le corps de ces programmes. Les individus mal intentionnés peuvent utiliser ce genre de chevaux de Troie pour : • Installer un programme malveillant à l'insu de l'utilisateur : ces chevaux de Troie n'affichent aucun message réel ou fictif (par exemple, messages relatifs à une erreur dans une archive ou à la version incorrecte du système d'exploitation) ; • Protéger un autre programme malveillant connu : tous les antivirus ne sont pas en mesure d'identifier un programme malveillant au sein d'un cheval de Troie qui réalise des installations.
Trojan-Notifier	Chevaux de Troie qui envoient des notifications	Ils signalent à l'individu mal intentionné que la communication avec l'ordinateur infecté est établie et transmettent des informations relatives à l'ordinateur : adresse IP, numéro du port ouvert ou adresse de courrier électronique. Ils contactent l'individu mal intentionné par courrier électronique ou via FTP (vers le site de ce dernier) ou par d'autres moyens. Ces programmes sont souvent utilisés dans les sélections de différents chevaux de Troie. Ils indiquent à l'individu mal intentionné que les autres chevaux de Troie ont bien été installé sur l'ordinateur de l'utilisateur.
Trojan-Proxy	Chevaux de Troie faisant office de proxy	Ils permettent à l'individu mal intentionné de contacter anonymement des pages Web via l'ordinateur de la victime ; le plus souvent, ils sont utilisés pour diffuser du courrier indésirable.

TYPE	NOM	DESCRIPTION
Trojan-PSW	Chevaux de Troie qui volent des mots de passe	Il s'agit de chevaux de Troie qui volent des mots de passe (Password Stealing Ware) ; ils volent les données des comptes des utilisateurs, les données d'enregistrement d'un logiciel. Ils recherchent les données confidentielles dans les fichiers systèmes et dans la base de registres et les transmettent à leur "maître" via courrier électronique ou via FTP sur la page Web de l'individu mal intentionné ou par d'autres méthodes. Certains de ces programmes appartiennent à des groupes particuliers décrits dans ce tableau. Il s'agit des chevaux de Troie qui volent les données d'accès aux services bancaires (Trojan-Banker), les chevaux de Troie qui volent les données des utilisateurs des services de messagerie instantanée (Trojan-IM) et les chevaux de Troie qui volent les données des adeptes de jeux en ligne (Trojan-GameThief).
Trojan-Spy	Chevaux de Troie espions	Ils mènent un espionnage électronique de l'utilisateur : ils recueillent des informations sur ses activités sur l'ordinateur ; par exemple, ils interceptent les données saisies à l'aide du clavier, réalisent des captures d'écran ou dressent des listes des applications actives. Une fois qu'ils ont obtenu ces informations, ils les transmettent à l'individu mal intentionné par courrier électronique ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Trojan-DDoS	Chevaux de Troie pour l'attaque de réseaux	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service). Ces programmes infectent généralement plusieurs ordinateurs pour attaquer simultanément un serveur.

TYPE	NOM	DESCRIPTION
Trojan-IM	Chevaux de Troie qui volent les données des utilisateurs de messagerie instantanée	Ils volent le numéro et le mot de passe des utilisateurs de messagerie instantanée telle que ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ou Skype. Ils transmettent ces informations à l'individu mal intentionné par courrier électronique ou via FTP (vers le site de ce dernier) ou par d'autres moyens.
Rootkit	Outils de dissimulation d'activité	Ils cachent les programmes malveillants et leurs activités et ce faisant, ils prolongent la présence de ceux-ci dans le système ; ils peuvent dissimuler des fichiers, des processus dans la mémoire de l'ordinateur infecté ou des clés de la base de registres qui lancent des programmes malveillants ; dissimulent l'échange de données entre les applications de l'ordinateur de la victime et d'autres ordinateurs du réseau.
Trojan-SMS	Chevaux de Troie qui envoient des SMS	Ils infectent des téléphones mobiles et les utilisent pour envoyer des SMS vers des numéros payants.
Trojan-GameThief	Chevaux de Troie qui volent les données des adeptes de jeux en ligne	Ils volent les données des comptes des adeptes de jeux en ligne ; ils transmettent les données à l'individu malveillant par courrier électronique, via FTP (sur le site de l'individu mal intentionné) ou via d'autres moyens.
Trojan-Banker	Chevaux de Troie qui volent les données de comptes en banque	Ils volent les données des comptes en banque ou les données des comptes de système de porte-monnaie électronique ; ils transmettent les données à l'individu malveillant par courrier électronique, via FTP (sur le site de l'individu mal intentionné) ou via d'autres moyens.
Trojan-Mailfinder	Chevaux de Troie qui récoltent des adresses électroniques	Ils recueillent les adresses de courrier électronique sur l'ordinateur et les envoient à l'individu mal intentionné par courrier électronique, via FTP (sur le site de l'individu mal intentionné) ou via d'autres moyens. Les individus mal intentionnés utilisent ensuite ces adresses

TYPE	NOM	DESCRIPTION
		pour diffuser des messages non sollicités.

UTILITAIRES MALVEILLANTS

Sous-catégorie : utilitaires malveillants (Malicious_tools)

Niveau de danger : moyen

Les utilitaires malveillants ont été créés spécialement pour nuire. Mais à la différence des autres programmes malveillants, ils n'exécutent pas d'actions malveillantes dès le lancement et peuvent être préservés et exécutés sans danger sur l'ordinateur de l'utilisateur. Ces programmes possèdent des fonctions qui interviennent dans la préparation de virus, de vers et de chevaux de Troie, l'organisation d'attaques de réseau sur des serveurs distants, l'intrusion dans des ordinateurs ou d'autres actions malveillantes.

Les utilitaires malveillants sont regroupés selon leur fonction. Le tableau ci-après fournit une description des différents types.

Tableau 3. Utilitaires malveillants selon les fonctions

TYPE	NOM	DESCRIPTION
Constructor	Constructeurs	Ils permettent de créer de nouveaux virus, vers ou chevaux de Troie Certains constructeurs sont dotés d'une interface standard qui permet, à l'aide de menus, de sélectionner le type de programme malveillant à créer, son mode de résistance face aux débogueurs ainsi que d'autres propriétés.
Dos	Attaques de réseau	Ils envoient de nombreuses requêtes vers un serveur distant au départ de l'ordinateur de la victime. Le serveur ne dispose pas de ressources suffisantes pour traiter les requêtes et il arrête de fonctionner (Denial-of-service (DoS), déni de service).

TYPE	NOM	DESCRIPTION
Exploit	Codes d'exploitation	Le code d'exploitation est un ensemble de données ou de code qui exploite une vulnérabilité de l'application dans laquelle il est exécuté et réalise une action malveillante quelconque sur l'ordinateur. Par exemple, un code d'exploitation peut écrire ou lire des fichiers ou contacter des pages Web "infectées". Divers codes d'exploitation exploitent les vulnérabilités de diverses applications et services de réseau. Le code d'exploitation sous la forme d'un paquet de réseau se transmet via le réseau vers de nombreux ordinateurs à la recherche d'ordinateurs possédant des services de réseau vulnérables. Le code d'exploitation d'un fichier DOS utilise la vulnérabilité de l'éditeur de test. Il peut commencer à exécuter les fonctions prévues par l'individu mal intentionné lorsque l'utilisateur ouvre le fichier infecté. Le code d'exploitation intégré à un message électronique recherche les vulnérabilités dans un client de messagerie quelconque ; il peut commencer à exécuter l'action malveillante dès que l'utilisateur ouvre le message infecté dans le programme. Les vers de réseau (Net-Worm) se diffusent grâce aux codes d'exploitation. Les codes d'exploitation *nuker* sont des paquets de réseau qui mettent l'ordinateur hors service.
FileCryptor	Encodeurs	Ils encodent d'autres programmes malveillants afin de les cacher pour les logiciels antivirus.
Flooder	Programmes de "pollution" du réseau	Ils envoient une multitude de messages via les canaux de réseau. Les programmes utilisés pour polluer les canaux IRC (Internet Relay Chats) appartiennent à cette catégorie. Il s'agit également des programmes qui "polluent" le courrier électronique, les messageries instantanées et les systèmes mobiles. Ces programmes sont regroupés

TYPE	NOM	DESCRIPTION
		en différentes catégories décrites dans ce tableau (Email-Flooder, IM-Flooder et SMS-Flooder).
HackTool	Outils de piratage	Ils permettent de s'emparer de l'ordinateur sur lequel ils sont installés ou d'attaquer un autre ordinateur (par exemple, ajout d'autres utilisateurs au système sans l'autorisation de la victime, purger des journaux du système afin de dissimuler les traces de leur présence). Il s'agit de quelques sniffers qui possèdent des fonctions malveillantes telles que l'interception des mots de passe. Les sniffers sont des programmes qui permettent de consulter le trafic de réseau.
not-virus:Hoax	Blagues de mauvais goût	Effraient l'utilisateur à l'aide de messages semblables à ceux que pourrait produire un virus : ils peuvent découvrir un virus dans un fichier sain ou annoncer le formatage du disque alors qu'il n'aura pas lieu.
Spoofer	Utilitaires d'imitation	Ils envoient des messages et des requêtes de réseau au départ d'adresses fictives. Les individus mal intentionnés les utilisent pour se faire passer pour l'expéditeur.
VirTool	Instruments pour la modification des programmes malveillants	Ils permettent de modifier d'autres programmes malveillants afin de les rendre invisibles pour les logiciels antivirus.
Email-Flooder	Programmes qui "inondent" le courrier électronique.	Ils envoient de nombreux messages aux adresses du carnet d'adresses ("pollution du courrier"). Ce flux important de messages empêche l'utilisateur de lire le courrier utile.
IM-Flooder	Programmes de "pollution" des messageries instantanées	Ils envoient de nombreux messages aux utilisateurs de messagerie instantanée telle que ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager ou Skype. Ce flux important de messages empêche l'utilisateur de lire les messages utiles.

TYPE	NOM	DESCRIPTION
SMS-Flooder	Programmes de "pollution" par SMS	Ils envoient de nombreux sms vers les téléphones portables.

PROGRAMMES POTENTIELLEMENT MALVEILLANTS

Les **programmes potentiellement malveillants** à la différence des programmes malveillants ne sont pas développés dans le but de nuire. Toutefois, ils peuvent contribuer au viol de la sécurité de l'ordinateur.

Les programmes potentiellement malveillants regroupent les *logiciels publicitaires*, les *programmes à caractère pornographique* et les *autres applications potentiellement indésirables*.

Les logiciels publicitaires (cf. page 28) (Adware) sont liés à l'affichage de publicités sur l'écran de l'utilisateur.

Les logiciels à caractère pornographique (cf. page 28) (Pornware) sont liés à l'affichage d'informations à caractère pornographique sur l'écran de l'utilisateur.

Les autres applications présentant un risque potentiel (Riskware) (cf. page 29) (Riskware) sont le plus souvent des programmes utiles largement utilisés. Toutefois, si les individus mal intentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter leur fonction pour compromettre la sécurité.

Les programmes potentiellement malveillants sont installés à l'aide d'une des méthodes suivantes :

- ils peuvent être installés par l'utilisateur, séparément ou avec un autre programme (ainsi, les développeurs de programmes gratuits ou à contribution volontaire y intègrent des logiciels publicitaires).

- Ils peuvent être installés par des individus mal intentionnés, par exemple, ils les intègrent à des paquets contenant d'autres programmes malveillants, exploitent les vulnérabilités du navigateur Internet ou des chevaux de Troie de téléchargement et d'installation.

PROGRAMMES A CARACTERE PUBLICITAIRE

Sous-catégorie : programmes à contenu publicitaire (Adware)

Niveau de danger : moyen

Les programmes à caractère publicitaire montrent des publicités à l'utilisateur. Ils affichent des bandeaux publicitaires dans l'interface d'autres programmes ou réorientent les demandes vers les sites dont la publicité est assurée. Certains d'entre eux recueillent également des informations marketing sur l'utilisateur (par exemple, sujets des sites visités, mots clés utilisés dans les recherches) et les transmettent à leur auteur (à la différence des chevaux de Troie espion, ils transmettent ces informations avec l'autorisation de l'utilisateur).

PROGRAMMES A CARACTERE PORNOGRAPHIQUE

Sous-catégorie : programme à caractère pornographique (Pornware)

Niveau de danger : moyen

En général, l'utilisateur installe lui-même de tels programmes afin de chercher et de télécharger du contenu pornographique.

Les individus mal intentionnés peuvent également installer ces programmes sur l'ordinateur de la victime afin d'afficher, sans son consentement, des publicités pour des sites et des services pornographiques payants. Ils s'installent en exploitant des vulnérabilités du système d'exploitation ou du navigateur ou à l'aide de chevaux de Troie de téléchargement et des programmes d'installation.

On distingue trois types de programmes à caractère pornographique selon leur fonction. Le tableau ci-après fournit une description des différents types.

Tableau 4. Type de programmes à caractère pornographique selon les fonctions

TYPE	NOM	DESCRIPTION
Porn-Dialer	Numéroteurs automatiques	Etablissent une connexion avec des services pornographiques par téléphone (ils renferment les numéros de téléphone) ; à la différence des chevaux de Troie, ils informent l'utilisateur de leurs actions.

TYPE	NOM	DESCRIPTION
Porn-Downloader	Programmes pour le téléchargement de fichier depuis Internet	Ils téléchargent du contenu pornographique sur l'ordinateur ; à la différence des chevaux de Troie de numérotation automatique, ils préviennent l'utilisateur.
Porn-Tool	Outils	Ils permettent de rechercher et d'afficher du contenu pornographique ; par exemple, les barres d'outils spéciales pour les navigateurs et des lecteurs vidéo particuliers.

AUTRES PROGRAMMES POTENTIELLEMENT INDESIRABLES

Sous-catégorie : autres programmes potentiellement indésirables (Riskware)

Niveau de danger : moyen

La majorité de ces programmes sont des applications utiles employées par nombreux d'entre nous. Parmi ceux-ci, nous retrouvons les clients IRC, les numéroteurs automatiques (dialers), les programmes pour le chargement des fichiers, les dispositifs de surveillance de l'activité des systèmes informatiques, les utilitaires de manipulation de mots de passe, les serveurs Internet de services FTP, HTTP ou Telnet.

Toutefois, si les individus mal intentionnés mettent la main sur de tels programmes ou les infiltrent dans l'ordinateur de l'utilisateur, ils peuvent exploiter certaines de leur fonction pour compromettre la sécurité.

Les autres programmes potentiellement indésirables se distinguent par leurs fonctions. Le tableau ci-après fournit une description des différents types.

Tableau 5. Types d'autres programmes potentiellement indésirables selon les fonctions

TYPE	NOM	DESCRIPTION
Client-IRC	Clients de chats	Les utilisateurs installent ces programmes afin de pouvoir communiquer dans les canaux IRC (Internet Relay Chats). Les individus mal intentionnés les utilisent pour diffuser des programmes malveillants.
Dialer	Programmes de numérotation automatique	Ils peuvent établir des connexions téléphoniques par modem à l'insu de l'utilisateur.
Downloader	Programmes de téléchargement	Ils peuvent télécharger des fichiers depuis des pages Web en mode caché.
Monitor	Programmes de surveillance	Ils permettent de surveiller l'activité sur l'ordinateur sur lequel ils sont installée (observent les applications qui fonctionnent, comment elles échangent les données avec les applications sur d'autres ordinateurs).
PSWTool	Récupérateur de mots de passe	Ils permettent de consulter et de récupérer les mots de passe oubliés. C'est à cette fin que les individus mal intentionnés les installent à l'insu des utilisateurs.
RemoteAdmin	Programmes d'administration à distance	Ils sont utilisés par les administrateurs de système ; ils permettent d'accéder à l'interface de l'ordinateur distant afin de l'observer et de l'administrer. Les individus mal intentionnés les installent à l'insu des utilisateurs afin d'observer les ordinateurs distants et de les administrer. Les programmes potentiellement indésirables d'administration à distance se distinguent des chevaux de Troie de type Backdoor. Ces chevaux de Troie possèdent des

TYPE	NOM	DESCRIPTION
		fonctions qui leur permettent de s'introduire dans un système et de s'y installer ; les programmes potentiellement indésirable ne possèdent pas de telles fonctions.
Server-FTP	Serveurs FTP	Ils remplissent les fonctions d'un serveur FTP. Les individus mal intentionnés les insèrent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole FTP.
Server-Proxy	Serveurs proxy	Ils remplissent les fonctions d'un serveur proxy. Les individus mal intentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du courrier indésirable en leur nom.
Server-Telnet	Serveurs Telnet	Ils remplissent les fonctions d'un serveur Telnet. Les individus mal intentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole Telnet.
Server-Web	Serveurs Web	Ils remplissent les fonctions d'un serveur Web. Les individus mal intentionnés les introduisent sur l'ordinateur de la victime afin d'ouvrir l'accès à distance via le protocole HTTP.
RiskTool	Instruments utilisés sur l'ordinateur local	Ils offrent des possibilités complémentaires à l'utilisateur dans le cadre de l'utilisation de l'ordinateur (permettent de dissimuler des fichiers ou des fenêtres actives, arrêter des processus actifs).
NetTool	Instruments de réseau	Une fois installés, ils permettent à l'utilisateur d'exploiter des possibilités complémentaires en cas d'utilisation d'autres ordinateurs sur le réseau (redémarrage, identification des ports ouverts, exécution de programmes installés).

TYPE	NOM	DESCRIPTION
Client-P2P	Clients de réseaux d'échange de fichiers	Ils permettent aux réseaux P2P de fonctionner. Les individus mal intentionnés peuvent les utiliser pour diffuser des programmes malveillants.
Client-SMTP	Clients SMTP	Ils envoient des messages électroniques en mode discret. Les individus mal intentionnés les introduisent sur l'ordinateur des victimes afin de diffuser du courrier indésirable en leur nom.
WebToolbar	Barre d'outils Web	Ajout d'une barre d'outils dans l'interface d'autres applications en vue d'une utilisation de systèmes de recherche.
FraudTool	Pseudo-programme	Ils se font passer pour d'autres programmes. Par exemple, il existe des pseudo-antivirus ; ils affichent des messages sur la découverte de programmes malveillants alors qu'en réalité ils sont incapables d'identifier ou de réparer quoi que ce soit.

METHODE SUIVIE PAR L'APPLICATION POUR DECOUVRIR LES OBJETS INFECTES, SUSPECTS ET POTENTIELLEMENT DANGEREUX

L'application de Kaspersky Lab peut découvrir les objets malveillants dans les objets de deux manières : selon une méthode *réactive* (à l'aide de bases) ou selon une méthode *proactive* (à l'aide de l'analyse heuristique).

Les bases sont des fichiers contenant des signatures qui permettent d'identifier des centaines de milliers de programmes malveillants dans les objets analysés. Ces signatures contiennent des informations sur les segments de contrôle du code des programmes malveillants et des algorithmes de réparation des objets qui contiennent ces programmes. Les experts antivirus de Kaspersky Lab

découvrent chaque jour des centaines de nouveaux programmes malveillants, créent les signatures qui permettent de les identifier et les incluent dans les mises à jour des bases.

Si l'application de Kaspersky Lab découvre dans l'objet analysé un segment de code qui correspond parfaitement à un segment de contrôle du code d'un programme malveillant quelconque selon les informations reprises dans la base, il considère cet objet comme étant *infecté* et si l'équivalence du code n'est que partielle (dans des circonstances définies), il considère l'objet comme un objet *suspect*.

Grâce à la méthode proactive, l'application peut découvrir les programmes malveillants les plus récents qui ne figurent pas encore dans les bases.

L'application de Kaspersky Lab reconnaît les objets contenant de nouveaux programmes malveillants sur la base de leur comportement. Il est impossible de dire si le code de cet objet correspond parfaitement ou partiellement au code d'un programme malveillant connu mais il contient un série d'instructions propres aux programmes malveillants telles que l'ouverture d'un fichier, l'écriture dans un fichier ou l'interception des vecteurs d'interruption. Dans ce cas, l'application peut décider que le fichier ressemble à un fichier infecté par un virus inconnu.

Les objets découverts par la méthode proactive sont désignés comme étant *potentiellement dangereux*.

MENACES INTERNET

L'application de Kaspersky Lab utilise des technologies spéciales afin de lutter contre les menaces informatiques suivantes :

- Le spam ou courrier indésirable (cf. section «Spam ou courrier indésirable» à la page 33) ;
- L'hameçonnage (page 34);
- Les attaques de pirates informatiques (page 35);
- L'affichage de bannières (page 35).

SPAM OU COURRIER INDESIRABLE ENTRANT

L'application de Kaspersky Lab protège l'utilisateur contre le courrier indésirable. Le courrier indésirable ou *spam* a souvent un caractère publicitaire. Il encombre les canaux et les serveurs de messagerie du fournisseur. L'utilisateur paie pour

le trafic généré par le courrier indésirable et le courrier normal arrive plus lentement. C'est la raison pour laquelle le courrier indésirable est illégal dans de nombreux pays.

L'application de Kaspersky Lab vérifie les messages qui arrivent dans Microsoft Office Outlook, Microsoft Outlook Express et The Bat! et s'il identifie un message non sollicité, il exécute les actions que vous aurez sélectionnées (par exemple, le placer dans un répertoire distinct ou le supprimer).

L'application de Kaspersky Lab identifie le courrier indésirable avec un degré de précision élevé. Il applique simultanément plusieurs technologies de filtrage du courrier indésirable : identification du courrier en fonction de l'adresse de l'expéditeur et des mots et expressions dans l'en-tête des messages ; identifie le courrier indésirable sous la forme d'images et utilise l'algorithme d'auto-apprentissage pour identifier les messages non sollicités sur la base du texte.

Les bases d'Anti-Spam contiennent des listes "noire" et "blanche" d'adresses d'expéditeurs, des listes de mots et d'expressions qui appartiennent à différentes catégories de courrier indésirable telles que la publicité, les médicaments, la santé, les jeux de hasard et autres.

HAMEÇONNAGE

L'*hameçonnage* (phishing) est un type d'escroquerie sur Internet qui vise à "extraire" le numéro de carte de crédit, les codes d'identification personnelle et d'autres données privées de l'utilisateur dans le but de lui voler de l'argent.

L'hameçonnage est lié à l'émergence des services bancaires en ligne. Les individus mal intentionnés reproduisent une copie fidèle de la banque prise pour cible puis envoient aux clients de celle-ci un message qui a tous les attributs d'un message authentique en provenance de la banque. Ces messages invitent le client à confirmer ou à modifier ses données d'accès au site de la banque à la suite d'une panne ou d'un changement de système d'opérations bancaires en ligne qui a entraîné la perte de toutes les données. L'utilisateur clique sur le lien qui le mène au site créé par les individus mal intentionnés et il y saisit ses données.

Les bases d'Anti-Phishing contiennent une liste d'URL utilisées dans les attaques d'hameçonnage.

L'application de Kaspersky Lab analyse les messages qui arrivent dans Microsoft Office Outlook et Microsoft Outlook Express et si elle découvre un lien vers une des URL reprises dans les bases, elle traite ce message comme du courrier indésirable. Et si l'utilisateur ouvre le message et tente d'accéder au lien, l'application bloque la page.

ATTAQUES DE PIRATES INFORMATIQUES

Une *attaque de pirate* est une intrusion dans le système d'un ordinateur distant afin d'en prendre le contrôle, de le mettre hors service ou d'accéder aux informations protégées.

Les attaques de pirates peuvent être le fait d'individus mal intentionnés (par exemple, balayage des ports, collecte de mots de passe) ou de programmes malveillants qui exécutent des commandes au nom de l'utilisateur, transmettent les informations à leur "maître" et exécutent d'autres fonctions caractéristiques des attaques de pirates. Nos pouvons citer certains chevaux de Troie, les attaques par déni de service, les scripts malveillants et un multitude de vers de réseau.

Les attaques de pirate se diffusent sur les réseaux locaux et mondiaux via les vulnérabilités dans les systèmes d'exploitation et les applications. Ils se transmettent sous la forme de paquets de données IP distincts durant la connexion de réseau.

L'application de Kaspersky Lab est à l'affût des attaques de réseau sans perturber les connexions. Elle utilise des bases spéciales du Pare-feu. Ces bases contiennent des enregistrements qui identifient les paquets de données IP caractéristiques de différents programmes de pirates. L'application analyse les connexions de réseau et bloque les paquets IP qu'elle juge dangereux.

AFFICHAGE DES BANNIERES

Les *bannières* ou les bandeaux publicitaires qui jouent le rôle de lien vers des sites annonceurs se présentent le plus souvent sous la forme d'images. Leur affichage sur la page Web ne constitue pas une menace pour la sécurité mais elles nuisent à l'utilisation normale de l'ordinateur. Le clignotement des bannières à l'écran détériore les conditions de travail et réduit la productivité. L'utilisateur est déconcentré de son travail. De plus, cliquer sur les bannières augmente le trafic Internet.

De nombreuses entreprises ont adopté l'exclusion des bannières en tant qu'élément de leur stratégie de sécurité.

L'application de Kaspersky Lab bloque les bannières selon l'adresse URL de la page sur laquelle la bannière apparaît. Il utilise les bases actualisées d'Anti-bannière qui contiennent la liste des adresses URL des réseaux de bannières russes et étrangers. L'application analyse les liens sur la page Web téléchargée, compare les adresses aux adresses des bases et s'il en trouve, il supprime lien vers cette adresse sur la page et continue à charger la page.

INSTALLATION DE L'APPLICATION

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

> Attention !
>
> 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).

Vient ensuite la recherche du paquet d'installation de l'application (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 La via Internet. Si le fichier du paquet d'installation est introuvable, vous serez invité à le télécharger. L'installation de l'application 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.
- **Annule** : 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 du paquet.

DANS CETTE SECTION

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

Avant de lancer l'installation de l'application sur votre ordinateur, le système contacte les serveurs de mise à jour de Kaspersky Lab.

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 de la nouvelle version sera lancé automatiquement. Pour connaître la suite de l'installation de la version plus récente, lisez la documentation de la version correspondante de l'application.

ETAPE 2. VERIFICATION DE LA CONFORMITE DU SYSTEME AUX EXIGENCES MINIMUM 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 (cf. section "Configuration matérielle et logicielle requises" à la page 13). Le système vérifie également si l'ordinateur est doté des programmes requis et si vous jouissez des privilèges nécessaires pour réaliser l'installation.

Si une des conditions n'est pas remplie, le message de circonstance apparaîtra. Il est conseillé d'installer tous les Service Pack à l'aide du service **Windows Update** ainsi que les programmes requis avant de lancer l'installation de l'application de Kaspersky Lab.

ETAPE 3. ACCUEIL DE L'ASSISTANT D'INSTALLATION

Si votre système répond parfaitement aux exigences (cf. section "Configuration matérielle et logicielle requises" à la page 13), 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. La fenêtre d'accueil de l'Assistant d'installation s'ouvre. Elle contient les informations relatives au début de l'installation de l'application sur votre ordinateur.

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

ETAPE 4. LECTURE DU CONTRAT DE LICENCE

Cette fenêtre de l'Assistant d'installation contient le contrat de licence qui est conclu entre vous et Kaspersky Lab. Lisez-le attentivement et si vous n'avez

aucune objection à formuler, sélectionnez l'option **J'accepte les termes du contrat de licence** puis cliquez sur **Suivant**. L'installation se poursuit.

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

ETAPE 5. SELECTION DU TYPE D'INSTALLATION

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

- **Installation rapide**. Si vous choisissez cette option, 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 sera lancé à la fin de l'installation.

- **Installation personnalisée**. Dans ce cas de figure, vous êtes invité à sélectionner les composants de l'application que vous souhaitez installer, à désigner le répertoire dans lequel l'application sera installée (cf. section "Etape 6. Sélection du répertoire d'installation" à la page 39), à activer l'application et à la configurer à l'aide d'un Assistant spécial.

Si vous choisissez la première option, l'Assistant d'installation passe immédiatement à l'étape 8 (cf. section "Recherche d'autres logiciels antivirus" à la page 41). Dans le deuxième cas, vous devrez saisir ou confirmer certaines données à chaque étape de l'installation.

ETAPE 6. SELECTION DU REPERTOIRE D'INSTALLATION

> Remarque
>
> Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Etape 5. Sélection du type d'installation" à la page 39).

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 2009 Special Edition for Ultra-Portables** pour les systèmes 32 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.

Attention !

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 A INSTALLER

Remarque Cette étape de l'Assistant apparaît uniquement si vous avez sélectionné l'installation personnalisée (cf. section "Etape 5. Sélection du type d'installation" à la page 39).

En cas d'installation personnalisée, vous devez désigner les composants de l'application que vous souhaitez installer. Tous les composants de l'application sont désignés par défaut : composants de la protection, tâches d'analyse et de mise 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. 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 de les supprimer automatiquement ou manuellement.

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

ETAPE 9. 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 ou personnalisée (cf. rubrique « Etape 5. Sélection du type d'installation » à la page 39), il est déconseillé de désélectionner la case **Activer l'Autodéfense avant l'installation**. L'activation de l'autodéfense permet, en cas d'erreur lors de l'installation, de réaliser la procédure correcte de remise à l'état antérieur. En cas de nouvelle tentative d'installation, il est conseillé de désélectionner cette case.

Remarque

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

Pour poursuivre l'installation, cliquez sur **Suivant**. Cette action entraîne le lancement du processus de copie des fichiers de la distribution de l'application sur l'ordinateur.

Attention !

Les connexions de réseau ouvertes sont coupées durant l'installation si l'application contient des composants qui interceptent le trafic de réseau. La majorité des connexions interrompues seront rétablies après un certain temps.

ETAPE 10. FIN DE LA PROCEDURE D'INSTALLATION

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

Si le redémarrage de l'ordinateur est requis pour finaliser correctement l'installation, le message de circonstance sera affiché. L'Assistant de configuration sera lancé automatiquement après le redémarrage du système.

Si le redémarrage du système n'est pas requis, cliquez sur le bouton **Suivant** pour passer à l'Assistant de configuration de l'application.

INTERFACE DE L'APPLICATION

L'interface de l'application est simple et conviviale. Ce chapitre est consacré à ses principaux éléments.

En plus de l'interface principale du logiciel, il existe des plug-ins intégrés pour Microsoft Office Outlook (recherche de virus et recherche du courrier indésirable), Microsoft Outlook Express (recherche du courrier indésirable) et The Bat! (recherche de virus et recherche du courrier indésirable), Thunderbird (recherche du courrier indésirable), Microsoft Internet Explorer, Microsoft Windows Explorer. Ces modules externes élargissent les possibilités des programmes cités et permettent d'administrer et de configurer, depuis leur interface, les paramètres des composants **Antivirus Courrier** et **Anti-Spam**.

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 est un indice du fonctionnement de l'application. Elle reflète l'état de la protection et illustre également diverses tâches fondamentales exécutées par l'application.

Si l'icône est activée  (en couleur), cela signifie que la protection de l'ordinateur est complètement activée et que les composants fonctionnent. Si

l'icône n'est pas activée (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 :

- : l'analyse d'un message électronique est en cours.
- : la mise à jour des signatures des menaces et des modules du programme est en cours.
- : il faut redémarrer l'ordinateur pour appliquer les mises à jour.
- : un échec est survenu dans le fonctionnement d'un composant quelconque de l'application.

L'icône donne également accès aux éléments principaux de l'interface du logiciel : le menu contextuel (cf. section «Menu contextuel» à la page 44) et la fenêtre principale (cf. section «Fenêtre principale de l'application» à la page 46).

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

Pour ouvrir la fenêtre principale de l'application, double-cliquez avec le bouton gauche de la souris sur l'icône de l'application. La fenêtre principale s'ouvre à chaque fois à la rubrique **Protection**.

Quand Kaspersky Lab diffuse des informations, l'icône apparaît dans la zone de notification de la barre des tâches. Double-cliquez sur celle-ci avec le bouton gauche de la souris et lisez le contenu des informations dans la fenêtre qui s'ouvre.

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** - télécharge la mise à jour des bases et des modules de l'application et les installe sur l'ordinateur.
- **Analyse complète** - lance l'analyse complète de l'ordinateur à la recherche d'éventuels objets malveillants. Les objets de tous les disques, y compris sur les disques amovibles, seront analysés.

- **Recherche de virus** - passe à la sélection des objets et à la recherche d'éventuels virus parmi eux. La liste contient par défaut une série 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** - consultation de la liste des connexions établies, des ports ouverts et du trafic.

- **Clavier virtuel** - passage au clavier virtuel.

- **Kaspersky Internet Security** - ouvre la fenêtre principale de l'application (cf. section «Fenêtre principale de l'application» à la page 46).

- **Configuration** - permet d'examiner et de configurer les paramètres de fonctionnement de l'application.

- **Activation de la licence** - passe à l'activation de l'application. Pour obtenir le statut d'utilisateur enregistré, vous devez activer votre version de l'application. Ce point apparaît uniquement si le programme n'est pas activé.

- **A propos du programme** - affichage des informations relatives à l'application.

- **Suspension de la protection /Rétablissement de la protection** - désactive temporairement/active le fonctionnement des composants de la protection. Ce point du menu n'a aucune influence sur la mise à jour de l'application ou sur l'exécution de la recherche de virus.

- **Bloquer le trafic de réseau** - blocage temporaire de toutes les connexions réseau de l'ordinateur. Pour autoriser à nouveau la communication entre l'ordinateur et le réseau, sélectionnez ce même point dans le menu.

- **Quitter** : quitte l'application (lorsque vous sélectionnez ce point du menu, l'application sera déchargée de la mémoire vive de l'ordinateur).

Illustration1 : 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 L'APPLICATION

La fenêtre principale du logiciel se présente en trois parties :

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

Illustration2 : Etat actuel de la protection de l'ordinateur

Il existe trois types d'états de la protection et chacun est clairement indiqué par une couleur identique à celle d'un feu rouge. Le vert signale que la protection est assurée au bon niveau, tandis que le jaune et le rouge indiquent une menace pour la sécurité dans la configuration ou le fonctionnement de l'application. Les menaces regroupent non seulement les programmes malveillant, mais également les bases dépassées de l'application, certains composants désactivés, les paramètres minimum de fonctionnement de l'application, etc.

Il faut remédier aux menaces pour la sécurité au fur et à mesure qu'elles se présentent. Pour obtenir des informations détaillées sur ces menaces et sur les moyens de les résoudre rapidement, cliquez sur le lien **Corriger** (cf. ill. ci-dessus).

- La partie gauche de la fenêtre sert à la navigation. Elle permet de passer rapidement à l'utilisation de n'importe quelle fonction de l'application, à l'exécution d'une recherche de virus ou à l'analyse.

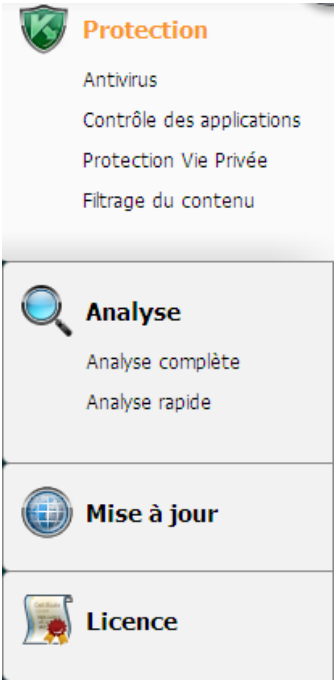

Illustration3 : La partie gauche de la fenêtre principale

- La partie droite de la fenêtre contient des informations relatives à la fonction de l'application sélectionnée dans la partie gauche. Elle permet de configurer les paramètres de chacune des fonctions, propose des outils pour l'exécution des tâches d'analyse, de mise à jour, etc.

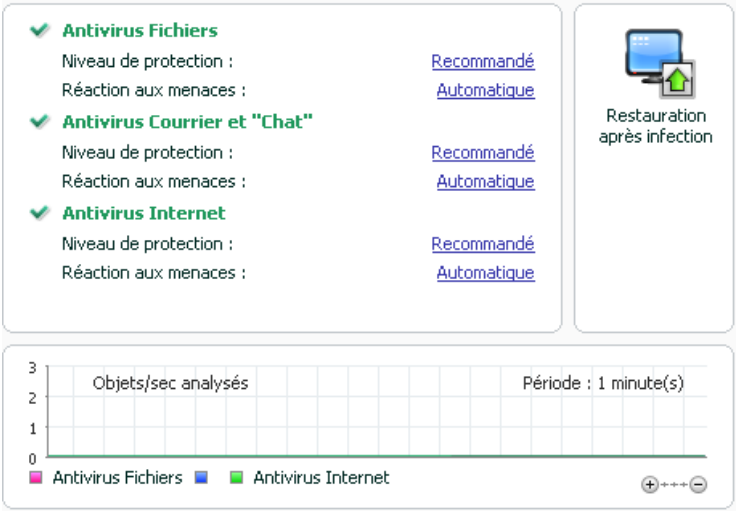

Illustration4 : Volet d'informations de la fenêtre principale

Vous pouvez également utiliser les boutons suivants :

- **Configuration** : ouvre la fenêtre de configuration des paramètres de l'application.
- **Aide** : ouvre le système d'aide de l'application.
- **Détectés** : passe à la liste des objets dangereux découverts par un composant quelconque ou par une recherche de virus exécutée et affiche des statistiques détaillées sur les résultats du fonctionnement de l'application.
- **Journaux** : passe à la liste des événements survenus pendant le fonctionnement de l'application.
- **Assistance** : ouvre la fenêtre reprenant les informations relatives au système et des liens vers les sources d'informations proposées par Kaspersky Lab (site du service d'assistance technique, forum).

> Remarque
>
> Vous pouvez également modifier l'apparence de l'application en créant et en utilisant vos propres éléments graphiques et la palette de couleurs.

NOTIFICATIONS

Lorsque des événements se produisent pendant l'utilisation de l'application, des notifications spéciales s'affichent à l'écran. Elles prennent la forme d'info-bulles au dessus de l'icône de l'application dans la barre des tâches de Microsoft Windows.

En fonction du niveau de gravité de l'événement (du point de vue de la sécurité de l'ordinateur), le message peut appartenir à l'une des catégories suivantes :

- **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. Ce type de message est de couleur 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 faut prendre une décision en fonction du danger que représente la menace à vos yeux. Ce type de message est de couleur 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 à caractère informatif ont une couleur verte.

FENETRE DE CONFIGURATION DES PARAMETRES DE L'APPLICATION

Vous pouvez ouvrir la fenêtre de configuration des paramètres de l'application depuis la fenêtre principale (cf. la section «Fenêtre principale de l'application» à la page 46) ou via le menu contextuel (cf. la section «Menu contextuel» à la page 44) de l'application. Pour ce faire, cliquez sur **Configuration** dans la partie supérieure de la fenêtre ou sélectionnez l'option équivalente dans le menu contextuel.

La fenêtre de configuration contient deux parties :

- la partie gauche permet d'accéder au composant de l'application, 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.

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 ces paramètres au sein d'une interface unique : l'assistant de configuration de l'application qui démarre à la fin de la procédure d'installation de l'application. Grâce aux instructions de l'Assistant, vous pouvez activer l'application, configurer les paramètres de la mise à jour, restreindre l'accès à l'application 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 (cf. la section "Recherche d'éventuels virus" à la page 54).

Les valeurs des paramètres de votre ordinateur peuvent être corrompues suite à l'action de programmes malveillants ou aux échecs du système. Lancez l'Assistant d'analyse de la sécurité (cf. la section "Assistant d'analyse de la sécurité" à la page 53) afin d'identifier les vulnérabilités des programmes installés ainsi que les anomalies dans la configuration du système.

Les bases livrées avec l'application peuvent être dépassées au moment de l'installation de celle-ci. Lancez la mise à jour du logiciel (page 53) (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 afin de configurer le composant pour votre correspondance.

Une fois que les actions ci-dessus auront été réalisées, l'application sera prête 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 60).

DANS CETTE SECTION

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 de fonctionnement interactif 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** : l'accès à votre ordinateur depuis l'extérieur est interdit pour les connexions de réseau de ce type. L'accès aux dossiers partagés et aux imprimantes est également 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** : toute activité est autorisée pour les connexions de réseau possédant 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 DU LOGICIEL

Attention !

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, au moment de l'installation, les bases de l'application peuvent être dépassées vu que 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. Kaspersky Internet Security vérifie automatiquement la présence des mises à jour sur les serveurs 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.

Pour maintenir la protection de votre ordinateur au niveau le plus actuel possible, 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**.

ANALYSE DE LA SECURITE

Les paramètres du système d'exploitation peuvent être corrompus par une activité indésirable sur l'ordinateur, résultat d'une panne du système ou 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 l'*Assistant d'analyse de la sécurité* après l'installation de l'application. L'Assistant d'analyse de la sécurité recherche les vulnérabilités dans les applications ainsi que les corruptions et les anomalies dans les paramètres du système d'exploitation et du navigateur.

- *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 section **Contrôle des applications**.

  3. Lancez la tâche **Analyse de la sécurité**

RECHERCHE DE VIRUS SUR L'ORDINATEUR

Les développeurs de programmes malveillants déploient de gros efforts pour dissimuler l'activité de leurs programmes et c'est la raison pour laquelle il peut arriver que vous ne remarquiez pas la présence de programmes malveillants 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/arrêter la tâche de recherche de virus :*

  1. Ouvrez la fenêtre principale de l'application.

  2. Dans la partie gauche de la fenêtre, sélectionnez la rubrique **Analyse** (**Analyse complète**, **Analyse rapide**).

  3. Cliquez sur **Lancer l'analyse** afin de lancer l'analyse. Cliquez sur **Arrêter l'analyse** pendant le fonctionnement de la tâche si vous devez interrompre son exécution.

ADMINISTRATION DE LA LICENCE

Kaspersky Internet Security fonctionne grâce à une clé. Elle vous est donnée lors de l'achat du logiciel et vous donne le droit d'utiliser celui-ci dès l'activation de la clé.

Sans clé, si la version d'évaluation n'a pas été activée, Kaspersky Internet Security ne procédera pas à la mise à jour des bases de l'application. ne procédera pas à la mise à jour des bases de l'application.

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 mettra à jour les bases de l'application. Vous pourrez toujours analyser le serveur 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 votre 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.

Les informations relatives à la clé installée sont reprises dans la rubrique **Licence** de la fenêtre principale de Kaspersky Internet Security : numéro de clé, son type (commerciale, commerciale avec abonnement, commerciale avec abonnement à la protection, évaluation, test bêta), le nombre maximum d'ordinateurs sur lesquels cette clé peut être utilisée, la fin de validité de la clé et le nombre de jour restant avant cette date. Les informations relatives à la fin de la validité de la licence n'apparaissent pas si une licence commerciale avec abonnement ou une licence commerciale avec abonnement à la protection a été installée (cf. section "Abonnement pour le renouvellement automatique de la licence" à la page 56).

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 une clé de la liste, cliquez sur le bouton **Supprimer** la licence.

Pour acheter une clé ou pour prolonger sa durée de validité, procédez comme suit :

1. Achetez une nouvelle clé. Pour ce faire, cliquez sur le bouton **Acheter une licence** (si l'application n'a pas été activée) ou sur **Renouveler votre licence**. Dans la page Web qui s'ouvre, vous pourrez saisir toutes les informations relatives à l'achat de la clé via la boutique en ligne de Kaspersky Lab ou auprès des partenaires de la société. En cas d'achat via la boutique en ligne, vous recevrez, après confirmation du paiement, le fichier de clé ou le code d'activation de l'application dans un message envoyé à l'adresse indiquée dans le bon de commande.

2. Installez la clé. Pour ce faire, cliquez sur le bouton **Acheter la licence** dans la rubrique **Licence** de la fenêtre principale de l'application ou utilisez la commande **Activer** du menu contextuel de l'application. Cette action entraînera l'ouverture de l'Assistant d'activation.

Remarque. 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

Pour les licences avec abonnement, Kaspersky Internet Security contacte automatiquement le serveur d'activation après une durée déterminée pour préserver l'actualité de votre licence.

Si la durée de validité de la licence en cours est écoulée, Kaspersky Internet Security vérifie elle-même en arrière-plan s'il existe une licence actualisée sur le serveur et si tel est le cas, elle la télécharge et l'installe en remplaçant la licence précédente. Le renouvellement s'opère ainsi sans votre intervention. Si la période pendant laquelle l'application renouvelle automatiquement la licence est également écoulée, il est possible de réaliser un renouvellement manuel. Les fonctions de l'application sont préservées durant la période pendant laquelle vous pouvez renouveler l'application manuellement. A la fin de la période, si la licence n'a pas été renouvelée, l'application arrêtera de télécharger les mise à jour des bases (pour la licence commerciale avec abonnement), ainsi que cessera de réaliser la protection de votre ordinateur (pour la licence commerciale

avec abonnement à la protection). Si vous ne souhaitez pas utiliser le service d'abonnement au renouvellement automatique de la licence, vous devrez contacter le magasin en ligne où vous avez acheté Kaspersky Internet Security.

Attention !

Si Kaspersky Internet Security avait déjà été activée antérieurement à l'aide d'une licence commerciale au moment de l'activation de l'abonnement, la licence sera remplacée par la licence avec abonnement (par la licence avec abonnement à la protection). Afin de pouvoir utiliser à nouveau la licence commerciale, il faut supprimer la licence avec abonnement et activer à nouveau l'application à l'aide du code qui vous avait permis d'obtenir la licence commerciale.

L'abonnement se caractérise par 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 fait d'un délai déterminé, vous recevrez un message indiquant que l'abonnement n'a pas été réalisé. Les bases de l'application ne seront plus actualisées (pour la licence commerciale avec abonnement) et la protection de l'ordinateur sera également suspendue (pour la licence commerciale avec abonnement à la protection).

- *Activé*. L'abonnement pour le renouvellement automatique de la licence a été activé pour une durée indéterminée (pas de date finale) ou pour une durée déterminée (la date de fin de validité de l'abonnement a été définie).

- *Renouvelé*. L'abonnement a été renouvelé automatiquement ou manuellement pour une durée indéterminée (pas de date finale) ou pour une durée déterminée (la date de fin de validité de l'abonnement a été définie).

- *Erreur*. Le renouvellement de l'abonnement s'est soldé par une erreur.

- *Expiré*. La durée de validité de l'abonnement est écoulée. Vous pouvez utiliser un autre code d'activation ou prolonger l'abonnement en contactant le magasin en ligne ou vous avez acheté Kaspersky Internet Security.

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

- *Actualisation requise*. La clé pour le renouvellement de l'abonnement n'a pas été reçue à temps pour une raison quelconque. Cliquez sur le bouton **Actualiser l'état de l'abonnement** pour renouveller l'abonnement

Pour la licence commerciale avec abonnement à la protection, l'état de l'abonnement peut être :

- *Suspendu*. L'abonnement pour le renouvellement automatique de la licence a été suspendu (date de fin de l'abonnement : date de suspension de l'abonnement)

- *Rétabli*. L'abonnement pour le renouvellement automatique de la licence a été rétabli (la date de la fin de l'abonnement n'est pas définie).

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. Pour la licence commerciale avec abonnement, la fonction de l'application est préservée à l'exception de la mise à jour des bases de l'application. Pour la licence commerciale avec abonnement à la protection, la mise à jour des bases de l'application et la protection de l'ordinateur sont interrompues.

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. Pour ce faire, cliquez sur le bouton **Actualiser l'état de l'abonnement**. Tant que l'abonnement n'aura pas été renouvelé, Kaspersky Internet Security n'actualisera plus les bases de l'application (pour la licence commerciale avec abonnement) et il n'assurera plus également la protection de l'ordinateur (pour la licence commerciale avec abonnement à la protection).

Si vous utilisez l'abonnement, vous ne pouvez pas installer des licences d'un autre type ou utiliser un autre code d'activation dans le but de prolonger la durée de validité de la licence. Vous pouvez utiliser un autre code d'activation uniquement après l'expiration de la durée de l'abonnement (état *Expiré*).

Attention !

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

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 et leurs origines et pour développer le plus rapidement possible des moyens de neutralisation, Kaspersky Lab vous propose de participer au nouveau service 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 l'application. Cet identificateur définit les paramètres matériels de l'ordinateur et ne contient aucune information personnelle.
- Les informations relatives aux menaces découvertes par les composants de l'application. 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 récolte également des statistiques étendues qui porte sur :

- 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.

Attention !

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

- *Pour configurer les paramètres d'envoi des 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. Cochez la case **J'accepte d'envoyer les statistiques étendues dans le cadre de Kaspersky Security Network**, pour confirmer votre accord d'envoyer les statistiques étendues.

ADMINISTRATION DE LA SECURITE

L'état de la protection de l'ordinateur (cf. la section "Fenêtre principale de l'application" à la page 46) signale l'apparition d'un problème dans la protection de celui-ci en modifiant la couleur de l'icône de l'état de la protection et du panneau dans laquelle elle se trouve. Il est conseillé de résoudre les problèmes du système de protection dès qu'ils se manifestent.

Illustration5 : Etat actuel de la protection de l'ordinateur

L'onglet **Etat**, accessible en cliquant sur le lien **Corriger** (cf. ill. ci-dessus), vous permet de consulter la liste des problèmes survenus, leur description et les solutions éventuelles (cf. ill. ci-après).

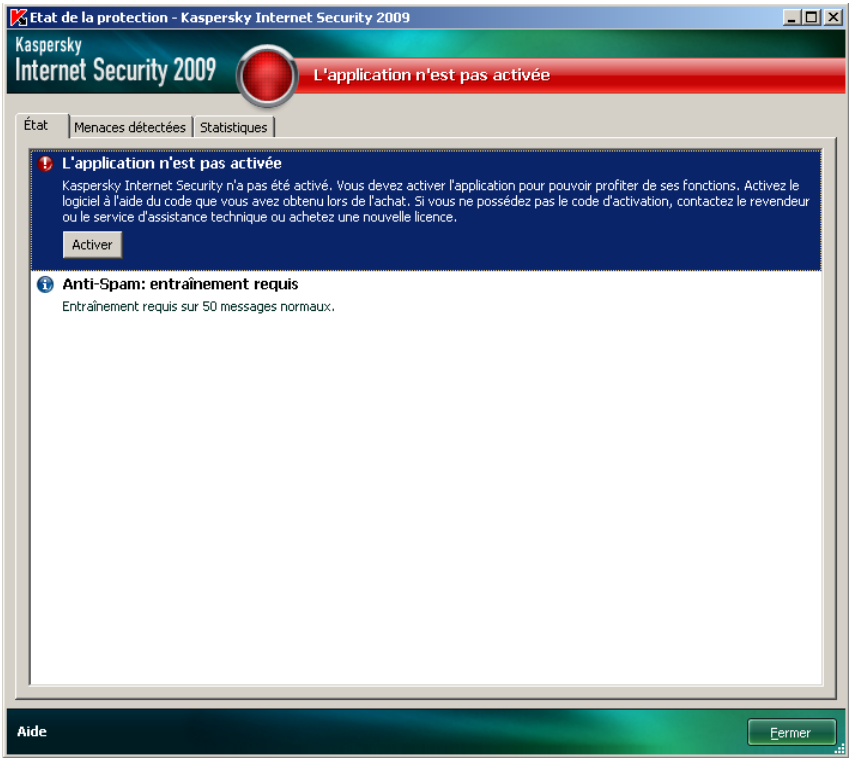

Illustration6 : Résolution des problèmes de sécurité

Vous pouvez consulter la liste des problèmes rencontrés. Les problèmes sont présentés par ordre d'urgence de la résolution : viennent en premier lieu les problèmes les plus importants, c.-à-d. ceux dont l'état est rouge, suivis par les problèmes moins importants (état orange) puis les messages d'information. 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 la suppression immédiate de la menace est impossible pour une raison quelconque, vous pouvez la reporter et y revenir plus tard. Pour ce faire, cliquez sur le bouton **Dissimuler le message**.

Sachez toutefois que cette possibilité n'est pas reprise pour les problèmes graves. Un problème grave peut être des objets malveillants non neutralisés, l'échec d'un ou de plusieurs composants de la protection ou la corruption des bases de l'application.

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

SUSPENSION DE LA PROTECTION

La suspension de la protection équivaut à la désactivation pendant un intervalle de temps donné de tous les composants de la protection.

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

1. Dans le menu contextuel (cf. la section "Menu contextuel" à la page 44) de l'application, sélectionnez le point **Suspension de la protection**.

2. Dans la fenêtre qui s'ouvre, sélectionnez la durée au terme de laquelle la protection sera réactivée :

   - **Dans <intervalle de temps>** : la protection sera activée au terme de l'intervalle indiqué. Pour sélectionner la valeur, utilisez la liste déroulante.

   - **Après le redémarrage** : la protection sera activée après le redémarrage du système (si le mode de lancement de l'activation de l'application à l'allumage de l'ordinateur a été sélectionné).

   - **Manuel** : 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 du programme.

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

- Le nom des composants désactivés apparaît en grise dans la section **Protection** de la fenêtre principale.

- Icône de l'application inactive (grise) (cf. la section "Icône dans la zone de notification" à la page 43 dans la barre d'état.

- Icône d'état et panneau de la fenêtre principale de l'application de couleur rouge.

Si des connexions de réseau étaient ouvertes au moment de l'arrêt de la protection, un message sur l'interruption des connexions s'affiche.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE L'APPLICATION

Une fois que vous aurez installé et configuré l'application, vous pourrez vérifier si la configuration des paramètres est optimale à l'aide du virus d'essai et de ses modifications. La vérification doit être réalisée pour chaque composant de la protection/chaque protocole séparément.

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.

Il NE S'AGIT PAS D'UN VIRUS et il ne contient aucun code qui puisse nuire à votre ordinateur. Néanmoins, la majorité des logiciels antivirus le considèrent comme un virus.

Attention !

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.

Remarque

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 l'organisation **EICAR** en tant qu'objet infecté contenant un virus **qui ne peut être réparé** et exécute l'action définie pour un tel 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.

Attention !

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 6. 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 cet objet comme un 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 figurent 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 n'a pas pu accéder à l'objet : l'intégrité de l'objet a été violée (par exemple, il n'y a pas de fin dans une archive multivolume) ou il n'y a pas de lien avec celui-ci (si l'objet analysé se trouve sur une ressource de réseau). Les informations relatives au traitement de l'objet figurent dans le rapport sur le fonctionnement de l'application.

Préfixe	Etat de l'objet	Informations relatives au traitement de l'objet
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 cet objet comme un 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 tester la découverte de virus dans le flux de données transmises via le protocole HTTP, procédez comme suit :*

  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 de la tentative de téléchargement du virus d'essai, Kaspersky Interne Security découvre l'objet, le considère comme étant dangereux et irréparable et exécute l'action définie dans les paramètres de l'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.

> Remarque
>
> Il est conseillé de vérifier le fonctionnement de Kaspersky Internet Security sur le trafic sortant, aussi bien dans le corps du message que dans les pièces jointes. Pour tester l'identification des virus dans le corps du message, placer le texte du virus d'essai standard ou un version modifiée de celui-ci dans le corps du message.

- *Pour ce faire :*

  1. Composez le message au format **Texte normal** à l'aide du client de messagerie installé sur l'ordinateur.

     > Remarque
     >
     > Les messages contenant le virus d'essai 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 comme étant infecté et bloque l'envoi de messages.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION D'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'essai téléchargé depuis le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), ainsi que les versions modifiées du virus d'essai.

  2. 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.

  3. Exécutez le fichier du virus d'essai ou une de ses modifications.

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 d'Antivirus Fichiers sont consultables dans le rapport sur l'utilisation du composant.

VERIFICATION DE L'EXACTITUDE DE LA CONFIGURATION DE LA TACHE D'ANALYSE

- *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 téléchargé depuis le site officiel de l'organisation **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), ainsi que les versions modifiées du virus d'essai.

  2. Créez une nouvelle tâche de recherche de virus 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 de recherche de virus.

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 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, l'application l'analyse, lui attribue l'état de courrier indésirable et exécute l'action définie pour les objets de ce type.

REGLEMENT D'UTILISATION DE KASPERSKY SECURITY NETWORK

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 en rapport avec les risques potentiels qui menacent votre ordinateur 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

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).

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 ne pas partager les informations ou les données demandées, 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.

KASPERSKY LAB

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

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

Aujourd'hui, Kaspersky Lab emploie plus de 450 spécialistes, tous spécialistes des technologies antivirus : 9 d'entre eux possèdent un M.B.A, 15 autres un doctorat, et deux experts siègent en tant que membres de l'organisation pour la recherche antivirus en informatique (CARO).

Kaspersky Lab offre les meilleures solutions de sécurité, appuyées par une expérience unique et un savoir-faire accumulé pendant plus de 14 années de combat contre les virus d'ordinateur. 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. Kaspersky® Internet Security, le produit phare de la société, garantit la protection de tous les objets susceptibles d'être la proie d'un virus : 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 Antivirus® : Nokia ICG (Etats-Unis), F-Secure (Finlande), Aladdin (Israël), Sybari (Etats-Unis), G Data (Allemagne), Deerfield (Etats-Unis), Alt-N (Etats-Unis), Microworld (Inde) et BorderWare (Canada).

Les clients de Kaspersky Lab bénéficient d'un large éventail de services qui garantissent le fonctionnement ininterrompu des logiciels et qui répondent à la moindre de leurs attentes. Nous élaborons, mettons en oeuvre et accompagnons

les dispositifs de protection antivirale pour entreprise. La base antivirus de Kaspersky Lab est mise à jour en temps réel toutes les heures. Nous offrons à nos utilisateurs une assistance technique en plusieurs langues vingt-quatre heures sur vingt-quatre.

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 une réponse complète à vos questions.

Adresse :	Siège social France 2, rue Joseph Monier 92500 Rueil Malmaison France
Assistance pour les utilisateurs :	http://support.kaspersky.fr/kis2009
Forum de Kaspersky Lab :	http://grandpublic.kaspersky.fr/forum
Laboratoire antivirus :	newvirus@kaspersky.com (uniquement pour l'envoi de nouveaux virus sous forme d'archive)
Informations générales :	0.825.888.612 info@fr.kaspersky.com
WWW:	http://www.kaspersky.com/fr http://www.viruslist.com/fr

MOZILLA FOUNDATION

a été utilisée dans le développement des composants de l'application.La bibliothèque **Gecko SDK ver. 1.8** a été utilisée dans le développement des composants de l'application.

Ce programme est utilisé selon les termes de la licence MPL 1.1 http://www.mozilla.opg/MPL.

Pour obtenir de plus amples informations sur la bibliothиque **Gecko SDK**, consultez l'adresse : http://developer.mozilla.org/en/docs/Gecko_SDK.

Site Web de Mozilla Foundation : http://www.mozilla.org.

CONTRAT DE LICENCE

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

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

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

CE LOGICIEL KASPERSKY A ETE PREVU POUR DES PARTICULIERS. EN ACCORD AVEC LA LEGISLATION , SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE DE KASPERSKY LAB OU D'UN DE SES PARTENAIRES, VOUS BENEFICIEZ D'UNE POSSIBILITE DE RETOUR ET DE REMBOURSEMENT DURANT UN DELAI DE 7 JOURS. L 'EVENTUEL DROIT AU RETOUR ET AU REMBOURSEMENT NE S'APPLIQUE QU'A L'ACHETEUR INITIAL. CONTACTEZ LA BOUTIQUE EN LIGNE SUR LAQUELLE VOUS AVEZ EFFECTUE VOTRE ACHAT POUR PLUS DE RENSEIGNEMENTS. KASPERSKY N'EST NI TENU D'APPLIQUER, NI RESPONSABLE DU CONTENU ET DES CLAUSES CONTRACTUELLES DE SES PARTENAIRES.

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

1. Octroi de la Licence. Sous réserve que vous vous soyez acquitté(e) du prix des droits de licence et sous réserve d'acceptation des termes et conditions de ce Contrat, Kaspersky Lab vous offre le droit non-exclusif et non-transférable d'utiliser cette version du Logiciel et de la documentation jointe (la "Documentation") jusqu'au terme de ce Contrat uniquement à des fins commerciales internes. Vous pouvez installer ce Logiciel sur un ordinateur.

1.1 Utilisation. Le logiciel est inscrit en tant que produit seul; il ne peut être utilisé sur plus d'un ordinateur, sauf comme décrit ci-dessous dans cette section.

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

1.1.2 Si vous cédez l'ordinateur sur lequel le Logiciel est installé, vous devrez au préalable vous assurer que toutes les copies du Logiciel ont été désinstallées ainsi que les éléments associés.

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

1.1.4 Il est interdit de copier, d'apporter des corrections ou de modifier, adapter ou traduire le Logiciel, et de produire des applications dérivées ou de le permettre à un tiers.

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

1.1.6 Il est interdit de transmettre le code d'activation et le fichier de clé de licence à un tiers. Le code d'activation et le fichier de clé de licence sont des informations strictement confidentielles.

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

1.1.8 Vous avez le droit de fournir à Kaspersky Lab toute information sur des menaces potentielles et vulnérabilités de votre ordinateur ; L'information collectée est à usage général et utilisée dans le seul but d'améliorer les logiciels Kaspersky Lab.

1.1.9 En rapport avec le sujet de la clause précédente (1.1.8) , le logiciel collectera automatiquement les « checksum » des fichiers exécutés sur un computer, et les enverra à Kaspersky Lab.

2. Assistance technique[1].

(i) Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr ou bien pour une période spécifiée et indiquée dans la fenêtre service du logiciel, et à partir de l'activation du logiciel ; tout ceci en satisfaisant les conditions et en fournissant les éléments ci-après :

(a) Le paiement total du logiciel et les frais d'accès au service d'assistance

(b) Le formulaire de souscription aux services d'assistance correctement rempli. Ce formulaire est disponible sur le site WEB de Kaspersky Lab et requiert que vous entriez le code d'activation, lui aussi fourni par Kaspersky Lab avec cet agrément. Il restera à l'entière discrétion de Kaspersky Lab de déterminez si vous satisfaisiez ou non les conditions de recours aux services d'assistance technique.

Les services d'assistance seront disponibles après l'activation du logiciel. D'autres renseignements ou enregistrements complémentaires pourront vous être demandés pour vous identifier (Customer ID) afin d'obtenir le service d'assistance.

En utilisant les services de l'assistance technique, vous acceptez les termes de la politique de Kaspersky Lab concernant la vie privée et qui est déposé sur www.kaspersky.com/privacy, et vous consentez explicitement au transfert de données à d'autres pays que le vôtre comme exposé dans la politique de vie privée.

(iii) Les services s'arrêteront sauf à renouveler annuellement le paiement des services et de remplir à nouveau le formulaire de souscription aux services d'assistance.

(iv) Services signifie :

[1] Le support technique, tel que présenté en clause 2 de cet EULA ne vous concerne pas si vous utilisez ce programme en mode de démonstration ou d'essai. De même vous n'avez pas le droit de vendre les éléments de ce programme, ensembles ou séparément. Vous pouvez utilisez le logiciel pour des raisons de démonstration ou d'essai pour la période spécifiée dans la licence. La période d'essai ou de démonstration commence à l'activation de la licence ou dés son installation. La période est visible dans l'interface graphique windows du logiciel.

(a) Mises à jour régulières des bases anti-virales

(b) Mises à jour gratuites du logiciel, y compris mises à niveau (sauf OEM),

(c) Support Technique via Internet

(d) Détection des virus et désinfection sous 24 heures

(v) Les services sont fournis uniquement lorsque vous avez la dernière version du logiciel, y compris les maintenance packs disponibles sur le site officiel de Kaspersky Lab (www.kaspersky.fr), installée sur votre ordinateur.

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

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

5. Limites de Garantie.

(i) Kaspersky Lab garantit que pour une durée de 6 mois suivant le premier téléchargement ou la première 'installation d'un logiciel Kaspersky en version sur CD-ROM, le logiciel fonctionnera, en substance, comme décrit dans la documentation fournie, et ce, lors d'une utilisation conforme et selon la manière spécifiée dans la Documentation.

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

(iii) Kaspersky Lab ne garantit pas que ce Logiciel reconnaisse tous les virus et les spam connus ni qu'il n'affichera pas de message de détection erroné.

(iv) L'entière responsabilité de Kaspersky Lab ne sera engagée qu'en cas de manquement envers le paragraphe (i) de la garantie, et il restera à la discrétion de Kaspersky Lab de réparer, remplacer ou rembourser le logiciel si le

problème est signalé directement à Kaspersky Lab ou à un ayant-droit au cours de la période de garantie. Vous fournirez tous les renseignements nécessaires pour aider le Fournisseur à remédier à tout problème éventuel.

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

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

6. Limites de Responsabilité.

(i) Rien dans ce Contrat ne saurait engager la responsabilité de Kaspersky Lab en cas (a) de non-satisfaction de l'utilisateur, (b) de décès ou dommages physiques résultant d'infractions aux lois en vigueur et du non-respect des termes de ce Contrat, ou (c) d'autre responsabilité qui ne peut être exclue par la loi.

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

(a) Perte de revenus;

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

(c) Perte de moyens de paiement;

(d) Perte d'économies prévues;

(e) Perte de marché;

(f) Perte d'occasions commerciales;

(g) Perte de clientèle;

(h) Atteinte à l'image;

(i) Perte, endommagement ou corruption des données;

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

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

7. Ce Contrat constitue l'accord unique liant les parties et prévaut sur tout autre arrangement, promesse ou accord verbal ou écrit passé au préalable entre vous et Kaspersky Lab, et qui ont été donnés ou seraient impliqués de manière écrite ou verbale lors de négociations avec nous ou nos représentants avant ce Contrat et tous les contrats antérieurs entre les parties en rapport avec les thèmes susmentionnés cesseront d'avoir effet à partir de la Date d'effet.